



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring CenturyLink 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 CenturyLink SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller 6.0, Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager Evolution Server 6.0.1, and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya Aura® Session Border Controller or Avaya Aura® Session Manager.

CenturyLink 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 CenturyLink SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller (AA-SBC) 6.0, Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager 6.0.1 configured as an 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.

The CenturyLink SIP Trunking service referenced within these Application Notes is designed for enterprise business customers. Customers using CenturyLink SIP Trunking service with the Avaya SIP-enabled enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

## 1.1. Interoperability Compliance Testing

A simulated enterprise site comprised of Communication Manager, Session Manager and the AA-SBC was connected to the public Internet using a broadband connection. The enterprise site was configured to connect to the CenturyLink SIP Trunking service through the public Internet.

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 (1XC) soft phones.
- 1XC supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. 1XC also supports two versions with different firmware (H.323 and SIP). Both versions of 1XC were tested.
- Various call types included: local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411), etc.
- G.711MU Codec.
- DTMF tone transmission passed in-band or as out-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.

- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection using SIP REFER for call transfer of inbound call back to PSTN.
- Network Call Redirection of inbound call to PSTN from Communication Manager vector.

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.
- Faxing between the enterprise site and PSTN were not tested as part of the compliance test since CenturyLink currently does not support T.38 FoIP (Fax over IP) on SIP Trunking.
- Codec negotiation of multiple codecs between CenturyLink and Avaya was not tested since CenturyLink currently supports only one codec (G.711MU) for SIP Trunking.

Interoperability testing of CenturyLink SIP Trunking service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Off-net call forwarding:** When INVITE from the enterprise to CenturyLink for forwarding inbound call back to PSTN contains both Diversion and History-Info headers, CenturyLink would respond with "604 Does not exist anywhere" resulting failure of off-net call forward. This failure was addressed in the compliance test by turning off the History-Info header in the call-redirection INVITE from the enterprise.
- **EC500:** EC500 is the Communication Manager mobility feature which allows a user to have incoming calls ring the destination extension as well as a remote off-net number such as a mobile phone. When the INVITE from the enterprise to CenturyLink for the remote PSTN endpoint contains both Diversion and History-Info headers, CenturyLink would respond with "604 Does not exist anywhere" causing the EC500 call to fail. This failure was addressed in the compliance test by turning off the History-Info header in the call-redirection INVITE from the enterprise.
- **Network Call Redirection:** When a Communication Manager vector is programmed to redirect an inbound call to a PSTN number before answering the call in the vector, CenturyLink 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 inbound call initiator hears fast busy in this failure scenario. Network call redirection works successfully when the Communication Manager vector is programmed to redirect the inbound call to a PSTN number after answering the call first in the vector (using SIP REFER message for network call redirection instead of the 302 message). Using REFER for transferring inbound calls to PSTN from the enterprise phones works properly.
- **Calling number/ID display:** PSTN phone may display both calling party id/name and calling party number or just calling party number and no calling party id/name on

outbound calls from the enterprise to the PSTN through CenturyLink, depending on the specific service provider the call routes through from Century Link to the endpoint.

- **Call display update:** Call display was not properly updated on PSTN phone to reflect the true connected party on calls that are transferred to the PSTN from the enterprise (see related item below). After the call transfer was completed, the PSTN phone showed the party that initiated the transfer instead of the actual connected party.
- **Contact header from AA-SBC:** After a transfer of inbound PSTN call to a 2<sup>nd</sup> PSTN phone was completed, UPDATE from Communication Manager to Session Manager and from Session Manager to AA-SBC correctly contains Contact header with originating PSTN phone number (i.e. the number for the actual connected party); however, UPDATE from AA-SBC to network changed this Contact header with CenturyLink DID associated with the internal extension that is the transferring party. The configuration on AA-SBC for addressing this problem using an earlier version of AA-SBC software failed to work in the AA-SBC software used for the compliance test. This issue was reported to AA-SBC support/development and will be fixed in a later release of the AA-SBC software.

## 1.2. Support

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

For technical support on CenturyLink SIP Trunking, contact CenturyLink using the Support link at <http://www.CenturyLink.com>.

## 2. Reference Configuration

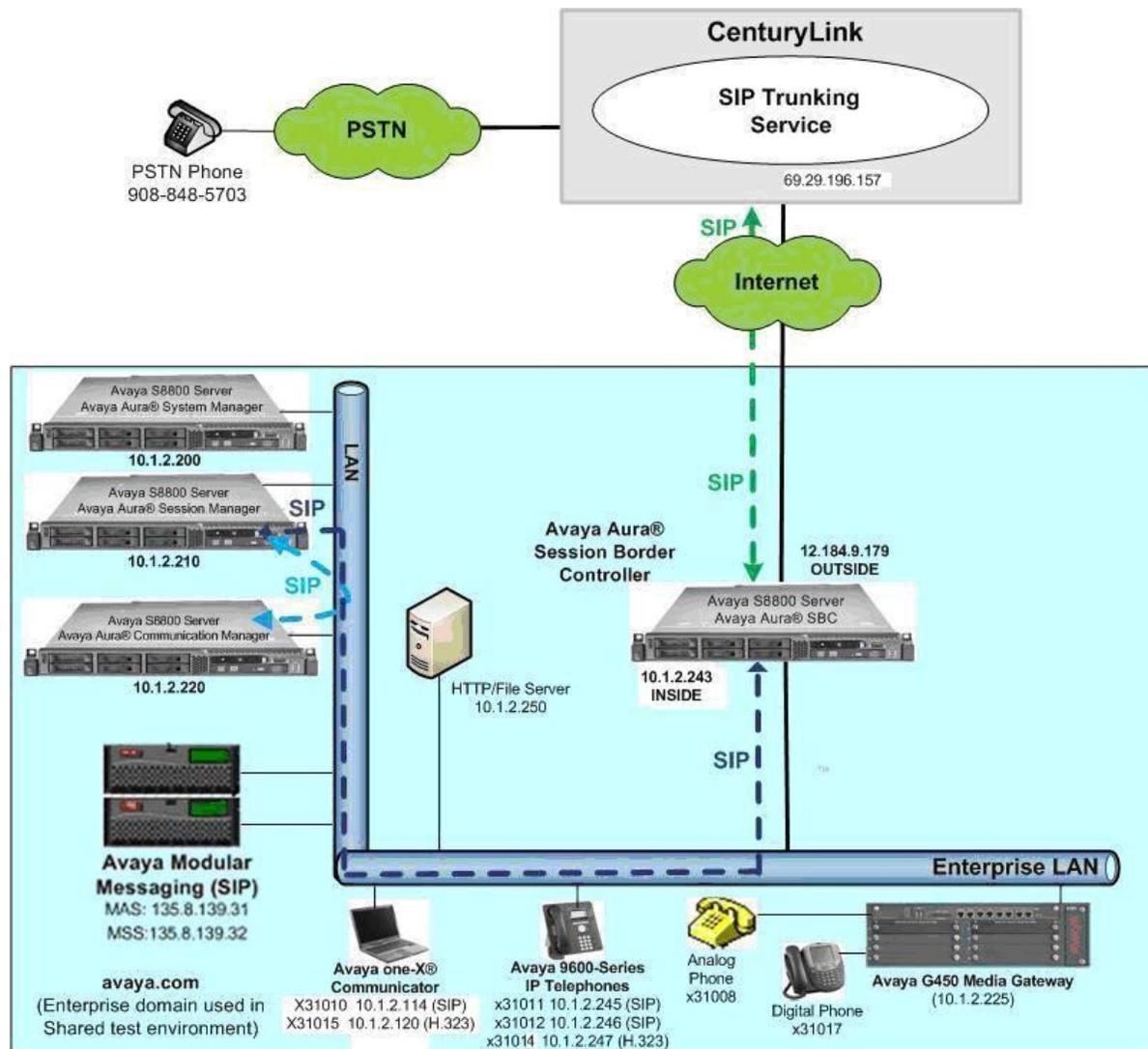
**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to the CenturyLink SIP Trunking service through a public Internet WAN connection.

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

- Avaya S8800 Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya S8800 Server running AA-SBC
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP)
- Avaya digital and analog telephones
- Avaya S8800 Servers running Avaya Modular Messaging Message Application Server (MAS) and Message Storage Server (MSS)

Located at the edge of the enterprise is the AA-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 AA-SBC. In this way, the AA-SBC can protect the enterprise against any SIP-based attacks. The AA-SBC provides network address

translation at both the IP and SIP layers. The transport protocol between the AA-SBC and CenturyLink across the public IP network is UDP; the transport protocol between the AA-SBC and the enterprise Session Manager across the enterprise IP network is TCP.



**Figure 1: Avaya IP Telephony Network Connecting to CenturyLink SIP Trunking Service**

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

For inbound calls, the calls flowed from the service provider to the AA-SBC then to Session Manager. Session Manager used 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 arrived at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions could be performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. The Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the AA-SBC. From the AA-SBC, the call was sent to the CenturyLink SIP Trunking service via the public Internet.

### 3. Equipment and Software Validated

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

<b>Avaya IP Telephony Solution Components</b>	
<b>Component</b>	<b>Release</b>
Avaya Aura® Communication Manager running on Avaya S8800 Server with Avaya G450 Media Gateway	6.0.1 (R016x.00.1.510.1-18621)
Avaya Aura® Session Manager running on Avaya S8800 Server	6.1.0.0.610023
Avaya Aura® System Manager running on Avaya S8800 Server	6.1.4.0 Build 6.1.0.4.5072 Patch 6.1.4.113
Avaya 96xx Series IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya 96xx Series IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.4
Avaya one-X Communicator (H.323 & SIP)	6.0 with SP1 (6.0.1.16)
Avaya 8410D Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Avaya Aura® Session Border Controller running on Avaya S8800 Server	6.0.0.1.5
Avaya Modular Messaging (MAS) running on Avaya S8800 Server	5.2 SP6 Patch 2 (9.2.357.6022)
Avaya Modular Messaging (MSS) running on Avaya S8800 Server	5.2 SP6 Patch 2
<b>CenturyLink SIP Trunking Solution Components</b>	
<b>Component</b>	<b>Release</b>
Acme Packet Net-Net 4250 SBC	R6.1
Broadsoft SoftSwitch	R16 sp1
Sonus GSX9000 Media Gateway	v07.02.07 r001

**Table 1: Equipment and Software Tested**

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

## 4. Configure Communication Manager

This section describes the procedure for configuring Communication Manager for inter-operating with the CenturyLink SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from CenturyLink. It is assumed the general installation of the Communication Manager and the Avaya G450 Media Gateway 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 for brevity and clarity in presentation.

### 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 172 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 0
    Maximum Concurrently Registered IP Stations: 2400 4
      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 2
      Maximum Video Capable IP Softphones: 2400 2
      Maximum Administered SIP Trunks: 4000 172
Maximum Administered Ad-hoc Video Conferencing Ports: 4000 0
  Maximum Number of DS1 Boards with Echo Cancellation: 80 0
      Maximum TN2501 VAL Boards: 10 0
      Maximum Media Gateway VAL Sources: 50 1
  Maximum TN2602 Boards with 80 VoIP Channels: 128 0
  Maximum TN2602 Boards with 320 VoIP Channels: 128 0
  Maximum Number of Expanded Meet-me Conference Ports: 300 0

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

```

## 4.2. System Features

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

```
change system-parameters features                               Page 1 of 19
                    FEATURE-RELATED SYSTEM PARAMETERS
                    Self Station Display Enabled? n
                    Trunk-to-Trunk Transfer: all
                    Automatic Callback with Called Party Queuing? y
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 values of **AV-Restricted** for restricted calls and **AV-Unavailable** for unavailable calls.

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

CPN/ANI/ICLID PARAMETERS
                    CPN/ANI/ICLID Replacement for Restricted Calls: AV-Restricted
                    CPN/ANI/ICLID Replacement for Unavailable Calls: AV-Unavailable

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 S8800 Server running Communication Manager (*procr*) and Session Manager (*SM61*). 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
<b>SM61</b>	10.1.2.210
default	0.0.0.0
<b>procr</b>	10.1.2.220
procr6	::

### 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. CenturyLink SIP Trunking service currently supports G.711MU only. Thus, the G.711MU was the only codec included in this set. Enter **G.711MU** in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

IP Codec Set				
Codec Set: 2				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)	
1: <b>G.711MU</b>	n	2	20	
2:				
3:				

On **Page 2**, set the **Fax Mode** to *off*. T.38 faxing is not currently supported by CenturyLink.

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

IP Codec Set		
Allow Direct-IP Multimedia? n		
FAX	Mode	Redundancy
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

## 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 3 was chosen for the service provider trunk. Use the **change ip-network-region 3** command to configure region 3 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 3                                     Page 1 of 20
                                                           IP NETWORK REGION
Region: 3
Location:                Authoritative Domain: avaya.com
Name: CenturyLink Test
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 3 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 3 (the service provider region) and region 1 (the rest of the enterprise).

display ip-network-region 3										Page	4 of	20
Source Region: 3										Inter Network Region Connection Management		
<b>dst</b>	<b>codec</b>	direct	WAN-BW-limits	Video	Intervening	Dyn	G	A	I	M		
<b>rgn</b>	<b>set</b>	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e		
1	2	y	NoLimit				n			t		
2												
3	2								all			
4												

## 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 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 AA-SBC is specified as TCP in **Sections 5.6 and 6.1.3**. Lastly, the transport method between the AA-SBC and CenturyLink 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 Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to *5068* (the well-known port value for TCP 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 S8800 Server running Communication Manager as defined in **Section 4.3**.

- Set the **Far-end Node Name** to *SM61*. 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 setting enables Communication Manager to send DTMF transmissions using RFC 2833.
- Change default setting of *6* for **Alternate Route Timer (sec)** to *12*. This allows more time for outbound PSTN calls to complete through the CenturyLink SIP Trunking service.
- Verify that the **Initial IP-IP Direct Media** is set to the same value as for the signaling group used for the enterprise site (signaling group 1 for the compliance test). The default setting for this field is *n*.
- 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: SM61
Near-end Listen Port: 5068                Far-end Listen Port: 5068
                                           Far-end Network Region: 3

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate        Bypass If IP Threshold Exceeded? n
                                           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): 12

```

## 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 **Section 4.6**.
- 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: 103
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: 20
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** 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 CenturyLink. 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**, the **Network Call Redirection** field can be set to *n* (default setting) or *y*. Setting the **Network Call Redirection** flag to *y* enables use of the SIP REFER message for call transfer. In the compliance test, transfer testing using INVITE was successfully completed with the **Network Call Redirection** flag set to *n*. Transfer with the **Network Call Redirection** flag set to *y* was also tested.

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 **Support Request History** field to *n*. This parameter determines whether the SIP History-Info header will be included in the call-redirection INVITE from the enterprise. Call-redirection of inbound call from PSTN back to PSTN failed in the compliance test when the call re-direction INVITE contains the History-Info header.

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

```
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? n
                    Telephone Event Payload Type: 101

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

## 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 numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension. It is used to authenticate the caller.

In the sample configuration, 5 DID numbers were assigned for testing. These 5 numbers were mapped to the 5 extensions 31010, 31011, 31012, 31014 and 31017. 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 5 extensions.

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

Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	3	60		5	Total Administered: 10
5	31010	3	9133245980	10	Maximum Entries: 540
5	31011	3	9133245977	10	
5	31012	3	9133245978	10	
5	31014	3	9133245979	10	
5	31017	3	9133245981	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 Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	4	3	91332	10	Total Administered: 1
					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						
<b>Ext</b>	<b>Ext</b>	<b>Trk</b>	<b>CPN</b>	<b>Total</b>		
<b>Len</b>	<b>Code</b>	<b>Grp(s)</b>	<b>Prefix</b>	<b>CPN</b>		
				<b>Len</b>		
5	3			5	Total Administered: 12	
5	31010	3	9133245980	10	Maximum Entries: 240	
5	31011	3	9133245977	10	Note: If an entry applies to	
5	31012	3	9133245978	10	a SIP connection to Avaya	
5	31014	3	9133245979	10	Aura(tm) Session Manager,	
5	31017	3	9133245981	10	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: 3

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	fac	<b>9</b>	<b>1</b>	<b>fac</b>			
00	3	fac	*	2	fac			
01	3	fac	#	2	fac			
1	3	dac						
2	5	ext						
3	5	ext						
4	5	ext						
44	5	ext						
5	5	ext						
50	4	ext						
6	5	ext						
7	5	ext						
732	10	udp						
777	7	udp						
8	1	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: 001
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: *2 All: *1
Deactivation: #1
Call Forwarding Enhanced Status: Act:
Deactivation:
Call Park Access Code:
Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
CDR Account Code Access Code:
Change COR Access Code:

```

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 3 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0		ARS DIGIT ANALYSIS TABLE					Page 1 of 2	
		Location: all					Percent Full: 2	
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI	Reqd	
0	1	1	3	op		n		
0	11	11	3	op		n		
00	2	2	3	op		n		
011	10	18	3	intl		n		
1800	11	11	3	fnpa		n		
1877	11	11	3	fnpa		n		
1908	11	11	3	fnpa		n		
411	3	3	3	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 3 for the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 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 the long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **Numbering Format:** *unk-unk* All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 4.7**.
- **LAR:** *next*

```

change route-pattern 3                                     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   No   Mrk Lmt List Del  Digits          QSIG
                Dgts                          Intw
1: 3    0    1
2:
3:
4:
5:
6:
                DCS/ IXC
                QSIG
                Intw
                n user
                n user
                n user
                n user
                n user
                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

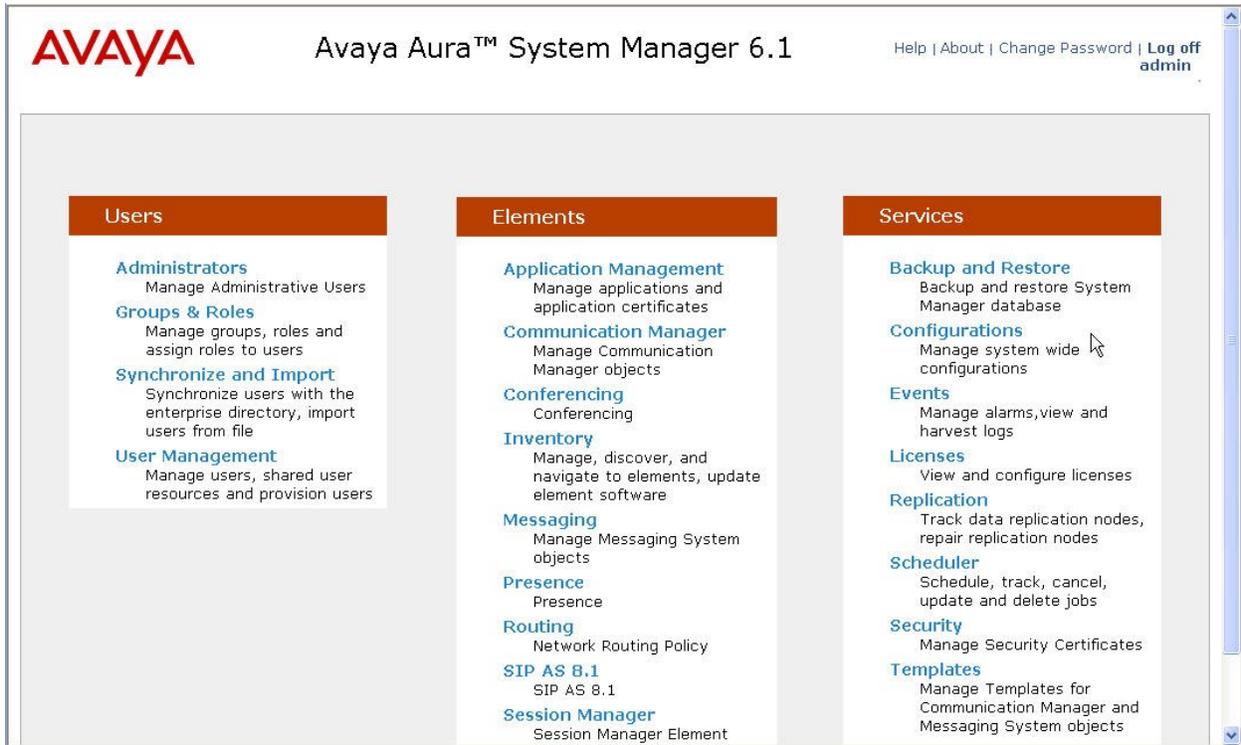
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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 AA-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.

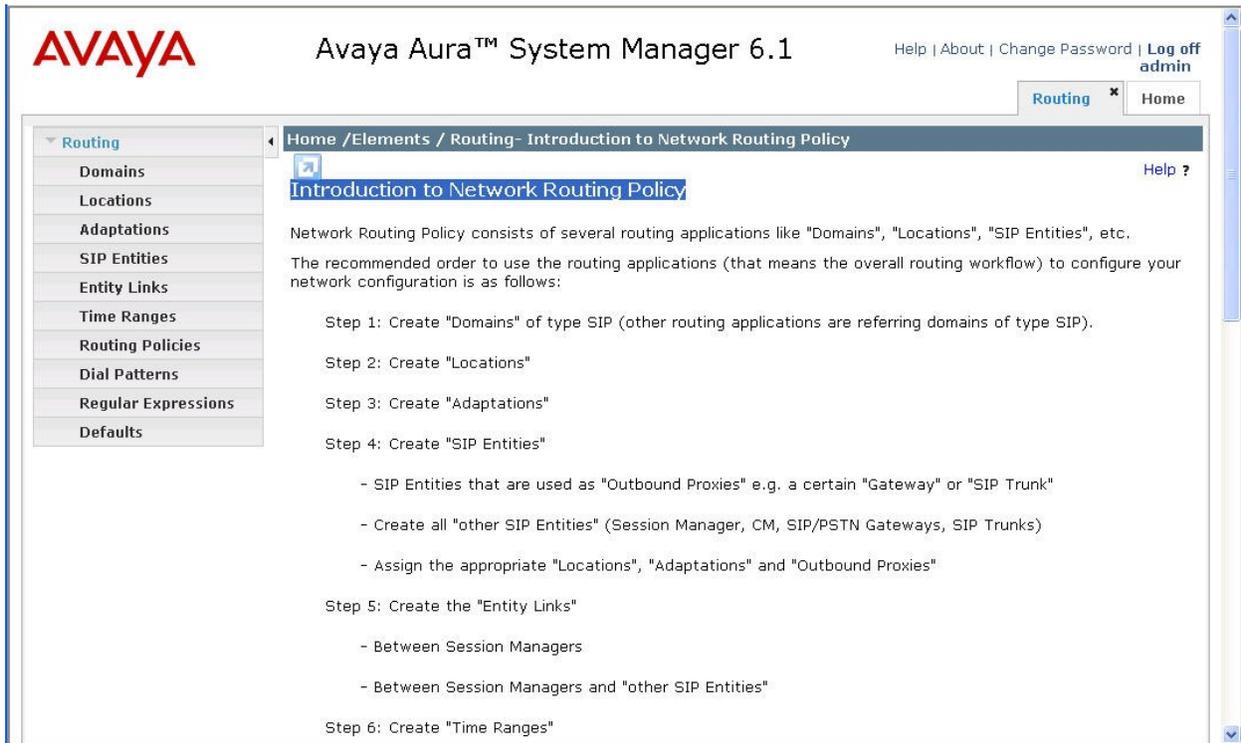
## 5.1. System Manager Login and Navigation

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. At the **Session Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



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

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



**AVAYA** Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing- Introduction to Network Routing Policy

[Introduction to Network Routing Policy](#) Help ?

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

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

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
  - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
  - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
  - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
  - Between Session Managers
  - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"

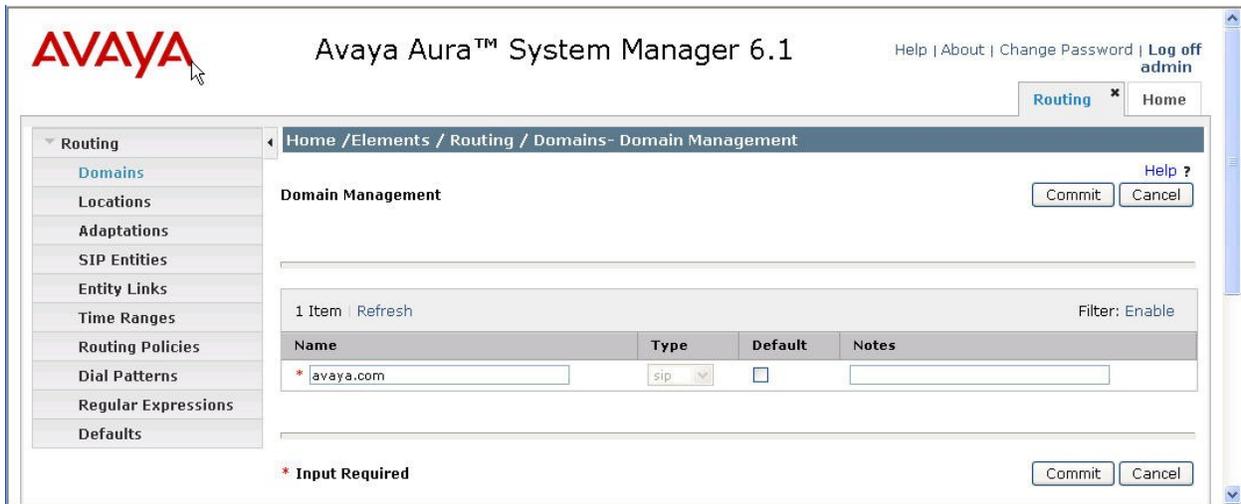
## 5.2. Specify SIP Domain

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 navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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



The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is expanded to 'Routing' > 'Domains'. The main content area is titled 'Domain Management' and contains a table with one entry. The table has columns for Name, Type, Default, and Notes. The entry for 'avaya.com' has 'sip' selected in the Type dropdown and an unchecked checkbox in the Default column. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the form area. A red asterisk indicates that the Name field is required.

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

### 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 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 (see 2<sup>nd</sup> screen below), 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).

Displayed below are the top and bottom halves of the screen for addition of the **BaskingRidge HQ** Location, which includes all equipment on the **10.1.2.x** subnet including Communication Manager, the IP phones, and the Session Manager itself. Click **Commit** to save.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. The main content area is titled 'Location Details' and is divided into sections: 'General' and 'Overall Managed Bandwidth'. In the 'General' section, the 'Name' field is filled with 'BaskingRidge HQ' and the 'Notes' field contains 'CME, CS1K R5 & R7, AAC R6, CM I'. The 'Overall Managed Bandwidth' section includes a dropdown for 'Managed Bandwidth Units' set to 'Kbit/sec', and empty input fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. A checkbox for 'Audio Calls Can Take Multimedia Bandwidth' is checked. The left-hand navigation pane shows 'Routing' selected, with sub-items like 'Domains', 'Locations', 'Adaptations', etc. Buttons for 'Commit' and 'Cancel' are visible at the top right of the form area.

**Per-Call Bandwidth Parameters**

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

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

Minimum Multimedia Bandwidth:  Kbit/Sec

\* Default Audio Bandwidth:  Kbit/sec

**Location Pattern**

5 Items Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.1.2.*	SM/CM R5.2.x, R6.0, R6.1
<input type="checkbox"/>	* 10.7.7.*	CS1K R7
<input type="checkbox"/>	* 10.32.1.*	
<input type="checkbox"/>	* 10.32.2.*	
<input type="checkbox"/>	* 172.28.43.*	

Select : All, None

\* Input Required

Note that call bandwidth management parameters should be set per customer requirement. Also note that the compliance test only used the IP Address Pattern **10.1.2.\*** ; other IP addresses in the screen above were configured for use by other projects.

Repeat the preceding procedure to create a separate Location for AA-SBC. Displayed below are the top and bottom halves of the screen for addition of the **AA-SBC** Location, which specifies the specific IP address for the AA-SBC. Click **Commit** to save.

**AVAYA** Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Locations - Location Details

**Location Details** Help ?

Commit Cancel

**General**

\* Name:

Notes:

**Overall Managed Bandwidth**

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

**Per-Call Bandwidth Parameters**

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

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

Minimum Multimedia Bandwidth:  Kbit/Sec

\* Default Audio Bandwidth:

**Location Pattern**

Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.1.2.243	Inside IP Address of AA-SBC

Select : All, None

\* Input Required Commit Cancel

## 5.4. Add Adaptation Module

Session Manager can be configured with Adaptation modules that 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 module, and can modify other headers to permit interoperability with third party SIP products.

For CenturyLink interoperability, one Adaptation is needed and maps inbound DID numbers from CenturyLink to local Communication Manager extensions. The adaptation will later on be applied to the Communication Manager SIP entity.

To create the adaptation, navigate to **Routing** → **Adaptations** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter *DigitConversionAdapter*.
- **Module parameter:** Enter *odstd=avaya.com*. This setting adapts the outgoing call (i.e., from Session Manager to Communication Manager) destination domain to the domain expected by Communication Manager in the sample configuration.

The screenshot displays the Avaya Aura™ System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off admin. The left-hand navigation pane lists various configuration categories, with 'Routing' expanded to show 'Adaptations'. The main content area is titled 'Adaptation Details' and contains a 'General' section with the following fields: 'Adaptation name' (text input with value 'SIPTrunking CM-ES-601'), 'Module name' (dropdown menu with value 'DigitConversionAdapter'), 'Module parameter' (text input with value 'odstd=avaya.com'), 'Egress URI Parameters' (empty text input), and 'Notes' (empty text input). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

To map inbound DID numbers from CenturyLink 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.

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 9133245977	* 10	* 10		* 10	31011	both	
<input type="checkbox"/>	* 9133245978	* 10	* 10		* 10	31012	both	
<input type="checkbox"/>	* 9133245979	* 10	* 10		* 10	31014	both	
<input type="checkbox"/>	* 9133245980	* 10	* 10		* 10	31010	both	
<input type="checkbox"/>	* 9133245981	* 10	* 10		* 10	31017	both	

Select : All, None

\* Input Required

Commit Cancel

## 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 AA-SBC. Navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select *Session Manager* for Session Manager, *CM* for Communication Manager and *Other* for the AA-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 Session Manager signaling interface is entered for **FQDN or IP Address**.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb navigation is "Home /Elements / Routing / SIP Entities- SIP Entity Details". The left navigation pane is expanded to "SIP Entities". The main content area is titled "SIP Entity Details" and has a "General" section. The fields are as follows:

- Name:** SM1
- FQDN or IP Address:** 10.1.2.210
- Type:** Session Manager (dropdown)
- Notes:** (empty text box)
- Location:** (empty dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** America/New\_York (dropdown)
- Credential name:** (empty text box)

Below the General section is the "SIP Link Monitoring" section, which contains a dropdown menu set to "Use Session Manager Configuration". At the top right of the form area are "Commit" and "Cancel" buttons, and a "Help ?" link.

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 the **Session Manager** SIP Entity.

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

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

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

The compliance test used 2 **Port** entries:

- **5060** with **TCP** for connecting to AA-SBC
- **5068** with **TCP** for connecting to Communication Manager

In addition, port 5060 with TCP was also used by a separate SIP Link between Session Manager and Communication Manager for Avaya SIP telephones and SIP soft clients. This SIP Link was part of the standard configuration on Session Manager and was not directly relevant to the interoperability with CenturyLink.

The screenshot shows the 'Port' configuration section of a SIP Entity. It features an 'Add' button and a 'Remove' button. Below these is a table with 8 items, a 'Refresh' button, and a 'Filter: Enable' option. The table has columns for 'Port', 'Protocol', 'Default Domain', and 'Notes'. Each row includes a checkbox, a text input for the port number, a dropdown for the protocol, a dropdown for the default domain, and a text input for notes. A mouse cursor is pointing at the 'Default Domain' dropdown for the row with port 5068. At the bottom, there is a 'Select: All, None' option, a '\* Input Required' warning, and 'Commit' and 'Cancel' buttons.

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	avaya.com	
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5061	TLS	avocs.contoso.com	
<input type="checkbox"/>	5062	TCP	adevc.avaya.globalipcom.com	Verizon testing CPE-domain
<input type="checkbox"/>	5064	TCP	cust2-tor.vtac.bell.ca	Bell Canada testing CPE-domain
<input type="checkbox"/>	5065	TCP	avaya.com	
<input type="checkbox"/>	5068	TCP	avaya.com	CenturyLink SIP Trunking test
<input type="checkbox"/>	5070	TCP	adevc.avaya.globalipcom.com	

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, it is necessary to create a separate SIP entity for Communication Manager in addition to 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 Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 5.4**.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura™ System Manager 6.1", and utility links for "Help | About | Change Password | Log off admin". A breadcrumb trail shows the path: "Home /Elements / Routing / SIP Entities- SIP Entity Details".

The left sidebar contains a menu with the following items: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults.

The main content area is titled "SIP Entity Details" and includes "Commit" and "Cancel" buttons. Below this is a "General" section with the following fields:

- Name:** CM601-Evolution-procr-5068
- FQDN or IP Address:** 10.1.2.220
- Type:** CM
- Notes:** CM 6.01-ES procr IP, different po
- Adaptation:** SIPTrunking CM-ES-601
- Location:** BaskingRidge HQ
- Time Zone:** America/New\_York

Below the "General" section is an "Override Port & Transport with DNS SRV:" checkbox, which is unchecked. This is followed by:

- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none

The "SIP Link Monitoring" section at the bottom contains:

- SIP Link Monitoring:** Use Session Manager Configuration

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

The screenshot displays the 'SIP Entity Details' configuration page for 'SIP Entities - SIP Entity Details'. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'Help ?' link, 'Commit', and 'Cancel' buttons. The 'General' section contains the following fields:

- \* Name: SIPTrunking-AuraSBC
- \* FQDN or IP Address: 10.1.2.243
- Type: Other
- Notes: AuraSBC connecting to SM6.1
- Adaptation: (dropdown menu)
- Location: AA-SBC
- Time Zone: America/New\_York
- Override Port & Transport with DNS SRV:
- \* SIP Timer B/F (in seconds): 4
- Credential name: (text input field)
- Call Detail Recording: none

The 'SIP Link Monitoring' section contains the following fields:

- SIP Link Monitoring: Link Monitoring Enabled
- \* Proactive Monitoring Interval (in seconds): 60
- \* Reactive Monitoring Interval (in seconds): 30
- \* Number of Retries: 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 AA-SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **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 Communication Manager, select the Communication Manager SIP Entity defined in **Section 5.5**. For AA-SBC, select the AA-SBC 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 AA-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:

The screenshot shows the 'Entity Links' configuration page in a web interface. The left sidebar contains a navigation menu with 'Entity Links' selected. The main content area has a breadcrumb trail 'Home /Elements / Routing / Entity Links- Entity Links' and a 'Help ?' link. Below the breadcrumb are 'Commit' and 'Cancel' buttons. The main area displays a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The row contains: \* CM601-ES-procr-506, \* SM1, TCP, \* 5068, \* CM601-Evolution-procr-5068, \* 5068, and a checked checkbox. Below the table is a '\* Input Required' label and another set of 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* CM601-ES-procr-506	* SM1	TCP	* 5068	* CM601-Evolution-procr-5068	* 5068	<input checked="" type="checkbox"/>

## Entity Link to the AA-SBC:

The screenshot shows the 'Entity Links' configuration page in a web interface, similar to the first one. The left sidebar contains a navigation menu with 'Entity Links' selected. The main content area has a breadcrumb trail 'Home /Elements / Routing / Entity Links- Entity Links' and a 'Help ?' link. Below the breadcrumb are 'Commit' and 'Cancel' buttons. The main area displays a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The row contains: \* \_SIPTrunking-AuraSI, \* SM1, TCP, \* 5060, \* SIPTrunking-AuraSBC, \* 5060, and a checked checkbox. Below the table is a '\* Input Required' label and another set of 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* _SIPTrunking-AuraSI	* SM1	TCP	* 5060	* SIPTrunking-AuraSBC	* 5060	<input checked="" type="checkbox"/>

## 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 AA-SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. 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 AA-SBC.

Routing Policy Details

General

\* Name: SIPTrunking-CM-ES-R601-Inbound

Disabled:

Notes: inbound service provider DID to C

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM601-Evolution-procr-5068	10.1.2.220	CM	CM 6.01-ES procr IP, different port

Routing Policy Details

General

\* Name: SIPTrunking-AuraSBC

Disabled:

Notes: To Service Provider SIP Trunking

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SIPTrunking-AuraSBC	10.1.2.243	Other	AuraSBC connecting to SM6.1

## 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 CenturyLink and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values. 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, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other dial patterns (e.g., 011 international calls, 411 directory assistance calls, etc.), were similarly defined.

The first example shows that 11 digit dialed numbers that begin with 1908 and have a destination domain of *avaya.com* uses route policy *SIPTrunking-AuraSBC*.

The screenshot displays the 'Dial Pattern Details' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Dial Patterns - Dial Pattern Details'. The 'General' section contains the following fields:

- Pattern:** 1908
- Min:** 11
- Max:** 11
- Emergency Call:**
- SIP Domain:** avaya.com
- Notes:** PSTN call through AuraSBC to Service Provid

The 'Originating Locations and Routing Policies' section includes an 'Add' and 'Remove' button, a 'Filter: Enable' option, and a table with one item:

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	<a href="#">SIPTrunking-AuraSBC</a>	0	<input type="checkbox"/>	SIPTrunking-AuraSBC	To Service Provider SIP Trunking Service

At the bottom of the table, it says 'Select : All, None'.

Note that the compliance test restricted outbound calls to the US 908 area code. In real deployments, this restriction should be relaxed (e.g., use Pattern “1” with 11 digits) or otherwise adjusted per customer business policies.

The second example shows that inbound 10 digit numbers that start with **91332459** to domain **avaya.com** and originating from Location **AA-SBC** uses route policy **SIPTrunking-CM-ES-R601-Inbound**. These are the DID numbers assigned to the enterprise from CenturyLink. Location **AA-SBC** is selected because these calls come from AA-SBC.

The screenshot displays the 'Dial Pattern Details' configuration page. The breadcrumb trail is 'Home /Elements / Routing / Dial Patterns- Dial Pattern Details'. The left sidebar shows a navigation menu with 'Dial Patterns' selected. The main area contains the following fields:

- Pattern:** 91332459
- Min:** 10
- Max:** 10
- Emergency Call:**
- SIP Domain:** avaya.com
- Notes:** Service Provider DID to SM61-CM601

Below the form is the 'Originating Locations and Routing Policies' section, which includes an 'Add' button, a 'Remove' button, and a table with one item. The table has columns for 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The single entry is for location 'AA-SBC' with routing policy 'SIPTrunking-CM-ES-R601-Inbound' and rank 0.

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	AA-SBC	SIP Trunking test	SIPTrunking-CM-ES-R601-Inbound	0	<input type="checkbox"/>	CM601-Evolution-procr-5068	inbound service provider DID to CM port 5068

At the bottom of the table, it says '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 **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

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

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

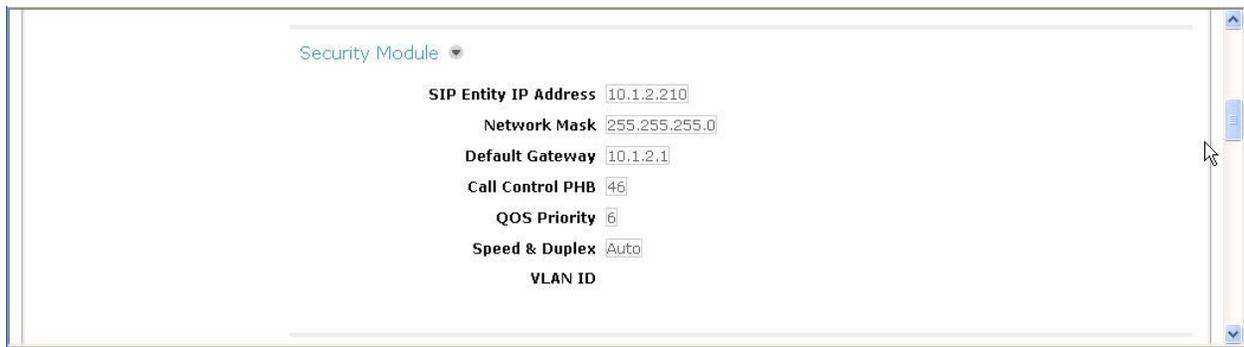
The screenshot displays the Avaya Aura™ System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off admin. The left sidebar shows a navigation tree with 'Session Manager Administration' selected. The main content area is titled 'View Session Manager' and shows the configuration for a Session Manager element. The configuration is organized into sections: General, Security Module, NIC Bonding, Monitoring, CDR, Personal Profile Manager (PPM), and Connection Settings. The 'General' section is expanded, showing the following configuration details:

SIP Entity Name	SM1
Description	R6.1 SM
Management Access Point Host Name/IP	10.1.2.211
Direct Routing to Endpoints	Enable

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.



The screenshot displays a configuration window titled "Security Module" with a dropdown arrow. Below the title, several configuration fields are listed with their respective values:

SIP Entity IP Address	10.1.2.210
Network Mask	255.255.255.0
Default Gateway	10.1.2.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

## 6. Configure Avaya Aura® Session Border Controller

This section describes the configuration of AA-SBC (Avaya Aura® SBC). This configuration is done in two parts. The first part is done during the AA-SBC installation via the installation wizard. These Application Notes will not cover the AA-SBC installation in its entirety but will include the use of the installation wizard (invoked during the loading of AA-SBC template) for entering network and SBC settings. 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 AA-SBC web interface. The resulting AA-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 AA-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 AA-SBC.
- **Hostname:** Enter a host name for the AA-SBC.
- **Domain:** Enter the domain used for the enterprise.
- **Default Domain:** Enter the domain used for the enterprise.

Click **Next Step** to continue.

The screenshot shows the Avaya Network Settings installation wizard. The interface includes a navigation pane on the left with options like Configuration, Installation, Network Settings, Logins, VPN Access, SBC, Summary, and Finish. The main content area is titled 'Network Settings' and 'Enter network settings'. It contains several input fields for network configuration: Domain-0 IP Address (10.1.2.241), CDom IP Address (10.1.2.242), Gateway IP Address (10.1.2.1), Network Mask (255.255.255.0), Primary DNS (192.168.1.200), Secondary DNS (Optional), Default Search List (Optional) (avaya.com), and HTTPS Proxy (Optional) [IP Address:Port Number]. Below these fields is a table for Virtual Machine settings:

Virtual Machine	IP Address	Hostname	Domain
SBC	10.1.2.243	AuraSBC	avaya.com (Optional)

Below the table, there is a 'Default Domain' field set to 'avaya.com (Optional)' and an 'Apply to all VMs' button. A 'Next Step' button with a red arrow is located at the bottom right of the screen.

## 6.1.2. VPN Access

VPN remote access to the AA-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.

**AVAYA**

Home

Configuration

Installation

- Network Settings
- Logins
- VPN Access
- SBC
- Summary
- Finish

### VPN Access

#### Configure VPN Access

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

Yes  No

**VPN Access Configuration**

VPN Router IP Address  (Optional)

Remote Access Network

Remote Access Network Subnet Mask

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

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

If in doubt, please refer to the documentation.

[Previous Step](#) [Next Step](#)

Copyright © 2010 Avaya Inc. All Rights Reserved.  
Avaya Aura™ Session Border Controller, powered by Acme Packet.  
Version 5273

### 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 AA-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 CenturyLink. Thus, **Generic** was chosen instead and further customization was done manually after the wizard was complete.
- **Port:** Enter the port number that the service provider uses to listen for SIP traffic.
- **IP Address1:** Enter the CenturyLink provided IP address of the CenturyLink SIP Proxy. If the service provider has multiple proxies, enter the primary proxy on this screen and additional proxies can be added after installation.
- **Signaling/Media Network1:** Enter the CenturyLink provided subnet where signaling/media traffic will originate. If signaling/media traffic can originate from multiple networks, enter one network address on this screen and additional networks can be added after installation.
- **Signaling/Media Netmask1:** Enter the netmask corresponding to **Signaling/Media Network1**.

In the **SBC Network Data** section:

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

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

**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	5060

IP Address1	Signalling/Media Network1	Signalling/Media Netmask1
69.29.196.157	69.29.196.0	255.255.255.0

IP Address2 (Optional)	Signalling/Media Network2 (Optional)	Signalling/Media Netmask2 (Optional)	Hunting (Optional)

#### SBC Network Data

Interface	IP Address	Net Mask	Gateway
Private (Management)	10.1.2.243	255.255.255.0	10.1.2.1
Public	12.184.9.179	255.255.255.0	12.184.9.129

#### Enterprise SIP Server

SIP Domain			
avaya.com			

IP Address1	Transport1
10.1.2.210	TCP

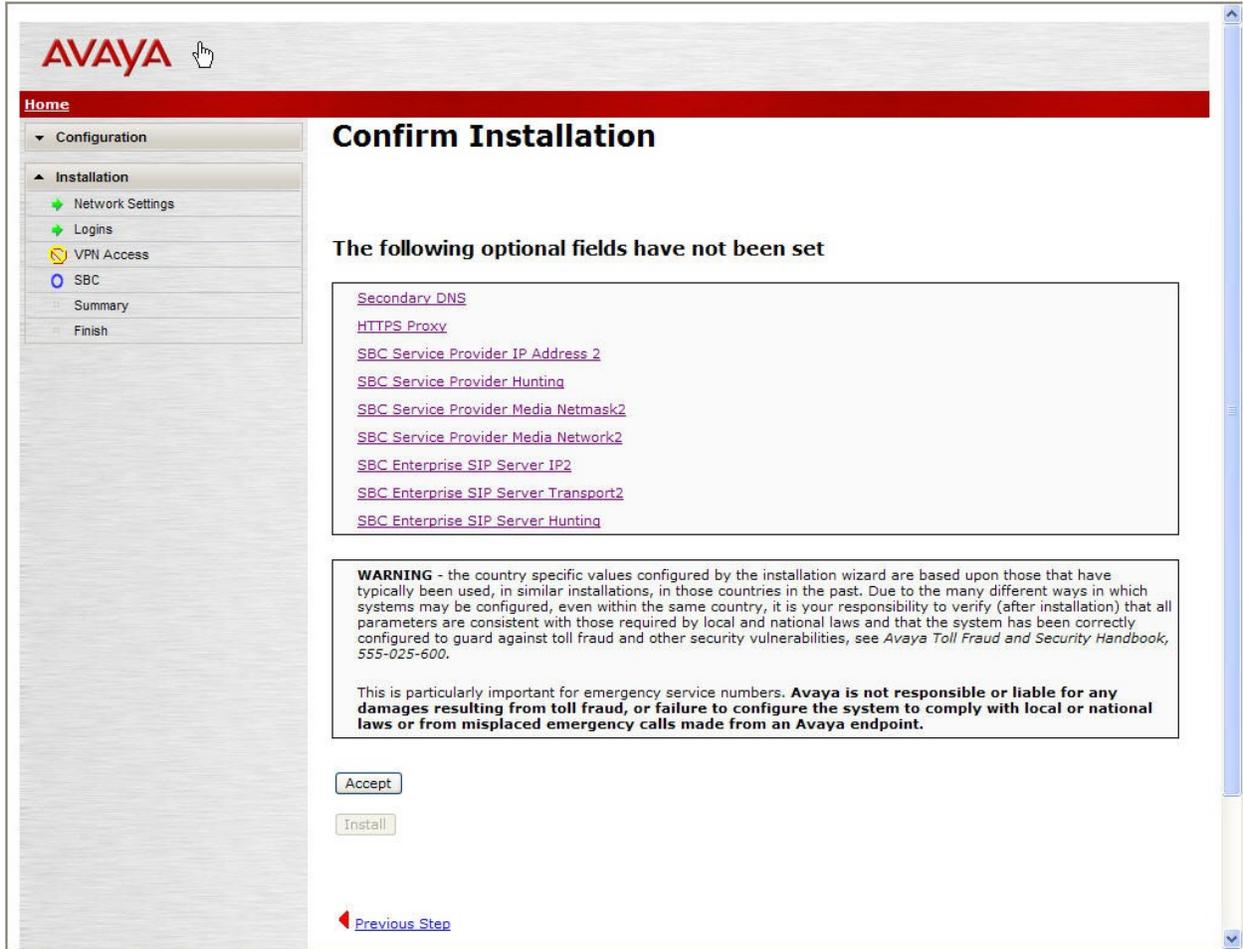
IP Address2 (Optional)	Transport2 (Optional)	Hunting (Optional)

[Previous Step](#) [Next Step](#)

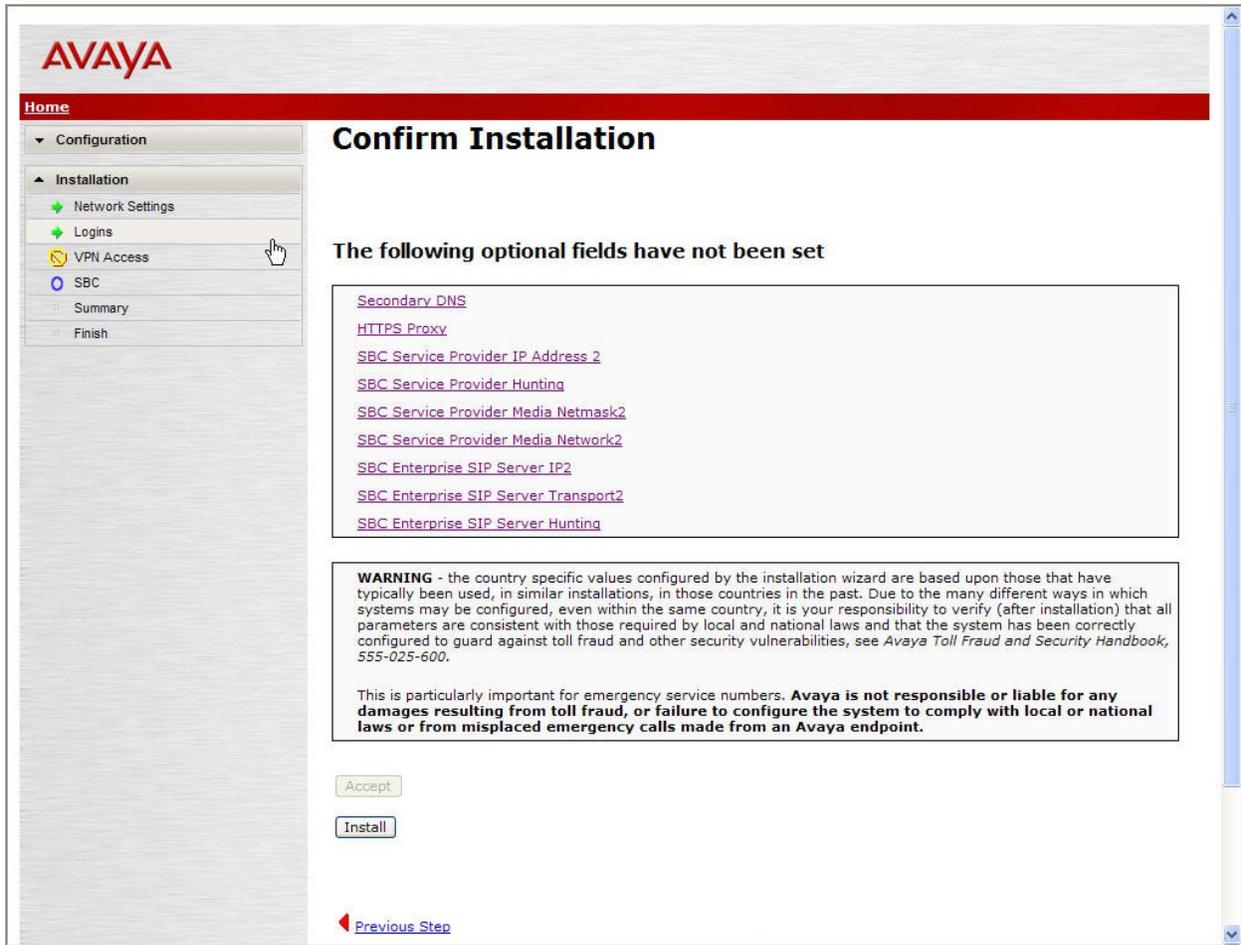
Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to continue to the final step.

### 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 relevant screen to set the required fields.



Otherwise, click **Accept** to bring up the second **Confirm Installation** screen as shown below.



Click **Install** 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 the *Generic* service provider was selected in the installation wizard, additional manual changes need to be performed. These changes are performed by accessing the browser-based GUI of the AA-SBC, using the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 6.1**. Log in with proper credentials.

**Acme Packet Net-Net OS-E**

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

Username:

Password:

## 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** → **servers** → **sig-gateway Telco**. Click **Show Advanced**.

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar shows a tree view under 'Configuration: all' with 'vsp' expanded to 'enterprise' → 'servers' → 'sip-gateway Telco'. The main content area is titled 'Configure vsplenterprise\servers\sip-gateway Telco' and includes a 'Show advanced' button. Below this are buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. A 'general' section contains the following fields:

- \* name**: Text input field containing 'Telco'.
- admin**: Dropdown menu set to 'enabled' with the note '(Resource is active)'.
- domain**: Empty text input field.
- failover-detection**: Dropdown menu set to 'ping' with the note '(Use OPTIONS to detect failures)'.

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

The screenshot shows the 'routing' section of the configuration form. The 'server-type' is 'sip-proxy'. The 'routing-setting' dropdown is expanded, showing options: 'normalization', 'auto-tag-match', 'auto-domain-match', and 'pstn-backup'. Below the dropdown are 'Select All' and 'Unselect All' buttons. Other fields in the routing section include:

- domain-alias**: Link to 'Edit domain-alias'.
- domain-subnet**: Link to 'Edit domain-subnet'.
- loop-detection**: Dropdown menu set to 'tight' with the note '(Compare source and destination address/port/transport)'.
- service-type**: Dropdown menu set to 'provider' with the note '(Provider peer)'.
- ping-interval**: Text input field containing '60' followed by 'seconds'.

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

## 6.2.2. Blocked Headers

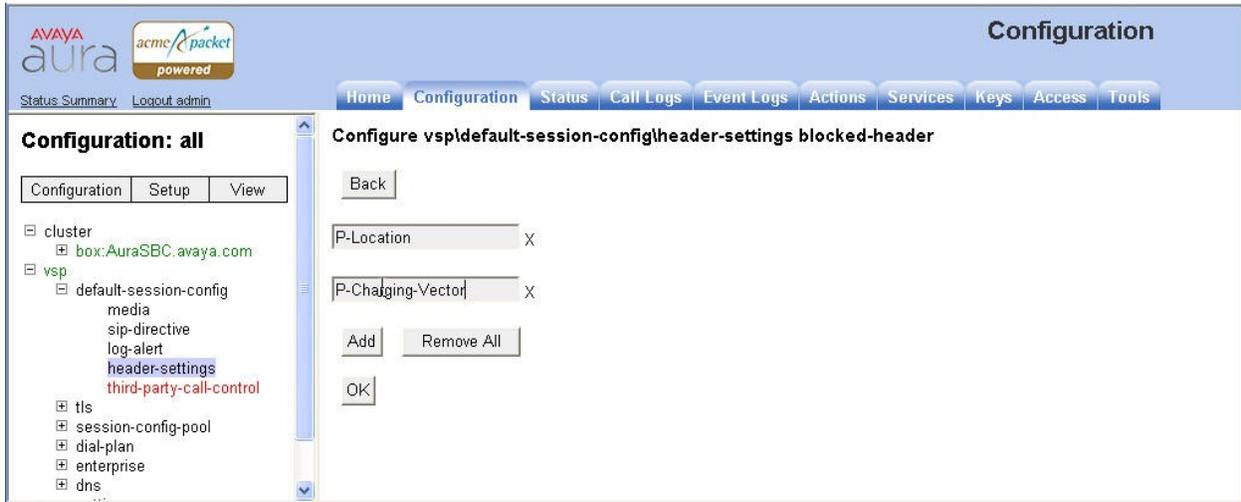
The P-Location and P-Charging-Vector headers are sent in SIP messages from the Session Manager. These headers should not be exposed external to the enterprise. For simplicity, these headers were simply removed (blocked) from both requests and responses for both inbound and outbound calls. To create a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

The screenshot displays the Avaya Aura Configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The main content area is titled 'Configure vspdefault-session-configheader-settings' and includes a 'Show basic' button and links for 'Help' and 'Index'. Below the title are 'Set', 'Reset', 'Back', and 'Delete' buttons. The configuration is presented as a table with various settings and their current values or actions:

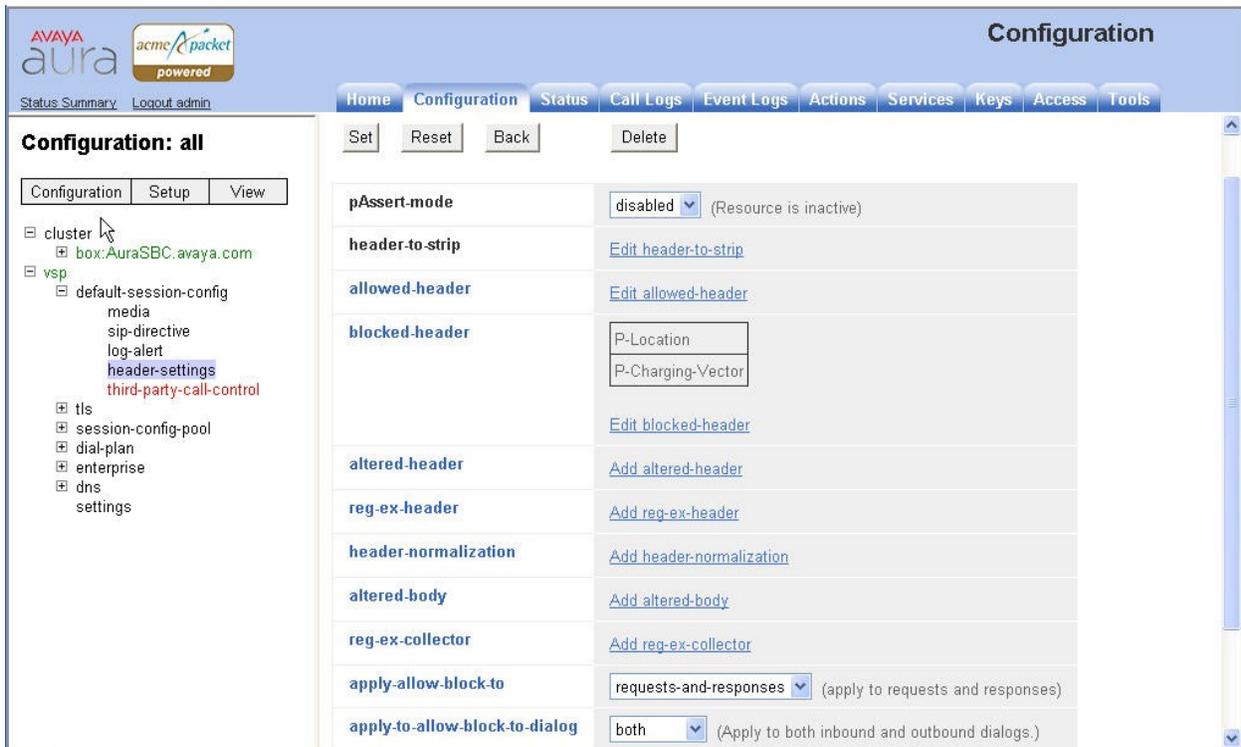
<b>pAssert-mode</b>	disabled (Resource is inactive)
<b>header-to-strip</b>	<a href="#">Edit header-to-strip</a>
<b>allowed-header</b>	<a href="#">Edit allowed-header</a>
<b>blocked-header</b>	<a href="#">Edit blocked-header</a>
<b>altered-header</b>	<a href="#">Add altered-header</a>
<b>reg-ex-header</b>	<a href="#">Add reg-ex-header</a>
<b>header-normalization</b>	<a href="#">Add header-normalization</a>
<b>altered-body</b>	<a href="#">Add altered-body</a>
<b>reg-ex-collector</b>	<a href="#">Add reg-ex-collector</a>
<b>apply-allow-block-to</b>	requests-and-responses (apply to requests and responses)
<b>apply-to-allow-block-to-dialog</b>	both (Apply to both inbound and outbound dialogs.)

The left sidebar shows a tree view of the configuration hierarchy: Configuration, Setup, View, cluster, box:AuraSBC.avaya.com, vsp, default-session-config, media, sip-directive, log-alert, header-settings (highlighted), third-party-call-control, tls, session-config-pool, dial-plan, enterprise, dns, settings.

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



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



### 6.2.3. Max-Forwards Value

On incoming PSTN calls to an enterprise SIP phone, increase the Max-Forwards value in the incoming SIP INVITE to allow the message to traverse all the SIP hops internal to the enterprise to reach the SIP phone. The AA-SBC was used to increase this value when the INVITE arrived at the AA-SBC from the network. To do this, navigate to **vsp** → **session-config-pool** → **entry ToPBX** → **header-settings** and click the **Add altered-header** link on the right (not shown).

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:** Select **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:** Select **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 screenshot shows the Avaya Aura Configuration interface. The main content area displays the configuration form for 'altered-header 0'. The form includes the following fields:

- \* number:** A text input field containing the value '1'.
- \* source-header:** A dropdown menu with 'Max-Forwards' selected.
- \* source-field type:** A dropdown menu with 'selection' selected. A note indicates: '(Regular expression based selection of portion of the URI.)'
- \* source-field value:** A text input field containing '.\*' with a note: '(regular expression)'
- \* source-field replacement:** A text input field containing '70'.
- \* destination:** A dropdown menu with 'Max-Forwards' selected.
- \* destination-field type:** A dropdown menu with 'full' selected. A note indicates: '(Entire value of the URI.)'

At the bottom of the form are three buttons: 'Create', 'Reset', and 'Cancel'. The left sidebar shows a tree view of the configuration hierarchy, with 'header-settings' selected under 'entry ToPBX'.

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.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The main content area is titled 'Configure vsp\session-config-pool\entry ToPBX\header-settings\altered-header 1'. On the left, a tree view shows the configuration hierarchy: cluster > box:AuraSBC.avaya.com > vsp > session-config-pool > entry ToPBX > header-settings. The main configuration pane contains the following fields:

- admin**: enabled (Resource is active)
- \* number**: 1
- \* source-header**: enter Max-Forwards or select from Max-Forwards
- \* source-field**:
  - \* type**: selection (Regular expression based selection of portion of the URI.)
  - \* value**: \* (regular expression)
  - \* replacement**: 70
- \* destination**: enter Max-Forwards or select from Max-Forwards
- \* destination-field**:
  - \* type**: full (Entire value of the URI.)
- apply-to-methods**: INVITE, REFER, MESSAGE, INFO

Buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete' are located at the top of the configuration pane.

## 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*.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The main content area is titled 'Configure vsp/default-session-config/third-party-call-control'. On the left, a tree view shows the configuration hierarchy: cluster > vsp > default-session-config > third-party-call-control. The main configuration area contains a table of settings:

Field	Value	Notes
admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	enabled	(Resource is active)
forward-unresolved-replaces	disabled	(Resource is inactive)
extract-refer-to-header-spec	disabled	(Resource is inactive)
refer-maintain-identity	false	
refer-notify-100-trying	disabled	(Resource is inactive)
refer-delayed-offer	disabled	(Resource is inactive)
ringback-file	<input type="text"/>	<a href="#">Browse System Files</a>
busy-file	<input type="text"/>	<a href="#">Browse System Files</a>
pre-call-announcement	<input type="text"/>	<a href="#">Browse System Files</a>

## 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**.

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar shows a tree view under 'Configuration: all' with 'vsp' expanded to 'session-config-pool' and 'entry ToPBX' selected. The main content area displays a table of configuration items for 'uri:':

uri:	
to-uri-specification	[Delete]
from-uri-specification	Configure
request-uri-specification	[Delete]
p-asserted-identity-uri-specification	Configure
contact-uri-settings-in-leg	Configure
contact-uri-settings-out-leg	Configure

In the right pane that appears, set the **add-maddr** field to *disabled*. Verify that the **use-incoming-contact** field is set to *disabled* (default setting).

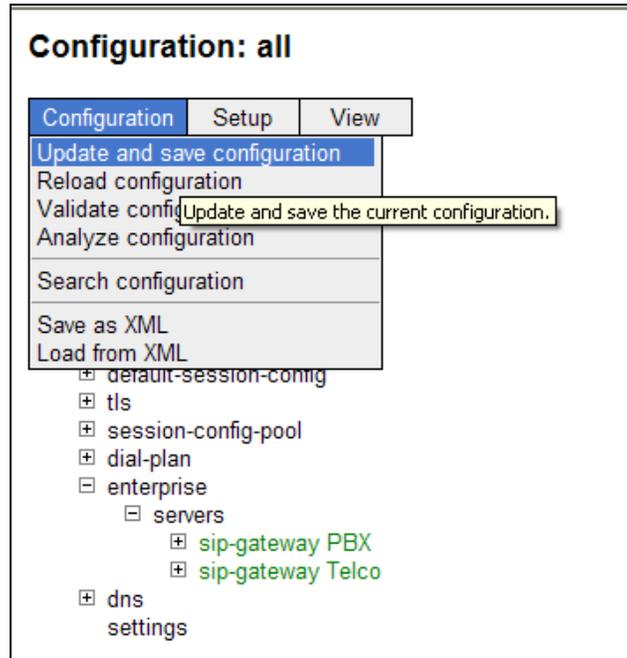
The screenshot shows the Avaya Aura Configuration interface with the configuration details for 'vsp|session-config-pool|entry ToPBX|contact-uri-settings-in-leg'. The left sidebar shows the tree view with 'entry ToPBX' selected. The main content area displays the configuration form with the following fields:

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

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

### 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. CenturyLink SIP Trunking Configuration

CenturyLink is responsible for the configuration of CenturyLink SIP Trunking service. The customer will need to provide the IP address used to reach the AA-SBC at the enterprise. CenturyLink will provide the customer with the necessary information to configure the SIP connection from the enterprise site to CenturyLink. The provided information from CenturyLink includes:

- IP address of the CenturyLink SIP proxy
- Supported codecs
- DID numbers
- IP addresses and port numbers used for signaling or media through any security devices

The sample configuration between CenturyLink and the enterprise for the compliance testing is a static configuration. There is no registration of the SIP trunk or enterprise users to the CenturyLink 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 AA-SBC to connect to the CenturyLink SIP Trunking service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 1.1**.

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

requested data to run the test. Displayed below are screens for the Call Routing Test for one inbound call to enterprise and one outbound call from enterprise:

Inbound call from PSTN phone (908) 848-5703 to DID number (913) 324-5977 (associated with enterprise extension x31011):

<ul style="list-style-type: none"> <li>Dashboard</li> <li>Session Manager</li> <li>Administration</li> <li>Communication Profile</li> <li>Editor</li> <li>▶ Network Configuration</li> <li>▶ Device and Location</li> <li>Configuration</li> <li>▶ Application</li> <li>Configuration</li> <li>▶ System Status</li> <li>▼ System Tools</li> <li>Maintenance Tests</li> <li>SIP Tracer</li> <li>Configuration</li> <li>SIP Trace Viewer</li> <li>Call Routing Test</li> </ul>	<h2 style="margin: 0;">Call Routing Test</h2> <p style="font-size: small; margin: 0;">This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.</p> <h3 style="margin: 0;">SIP INVITE Parameters</h3> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none;"> <p><b>Called Party URI</b>  <input type="text" value="9133245977@avaya.com"/></p> <p><b>Calling Party URI</b>  <input type="text" value="9088485703@10.1.2.243"/></p> <p><b>Day Of Week</b>  <input type="text" value="Monday"/></p> <p><b>Time (UTC)</b>  <input type="text" value="18:49"/></p> <p><b>Called Session Manager Instance</b>  <input type="text" value="SM1"/></p> </td> <td style="width: 50%; border: none;"> <p><b>Calling Party Address</b>  <input type="text" value="10.1.2.243"/></p> <p><b>Session Manager Listen Port</b>  <input type="text" value="5060"/></p> <p><b>Transport Protocol</b>  <input type="text" value="TCP"/></p> <p style="text-align: right;"><input type="button" value="Execute Test"/></p> </td> </tr> </table> <hr/> <h3 style="margin: 0;">Routing Decisions</h3> <div style="border: 1px solid gray; padding: 5px; font-size: small;"> Route &lt; sip:31011@avaya.com &gt; to SIP Entity CM601-Evolution-procr-5068 (10.1.2.220). Terminating Location is BaskingRidge HQ. </div> <hr/> <h3 style="margin: 0;">Routing Decision Process</h3> <div style="border: 1px solid gray; padding: 5px; font-size: x-small;"> NRP Adaptations: no Incoming Adaptation administered.  BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.  Originating Location is AA-SBC. Using digits &lt; 9133245977 &gt; and host &lt; avaya.com &gt; for routing.  NRP Dial Patterns: Found a Dial Pattern match for pattern &lt; 91332459 &gt; Min/Max length 10/10 and domain &lt; avaya.com &gt;.  NRP Routing Policies: Ranked destination NRP Sip Entities: CM601-Evolution-procr-5068.  NRP Routing Policies: Removing disabled routes.  NRP Routing Policies: Ranked destination NRP Sip Entities: CM601-Evolution-procr-5068.  END EMERGENCY CALL CHECK: This is not an emergency call.  Adapting and proxying for SIP Entity CM601-Evolution-procr-5068.  NRP Entity Links: Found direct link to destination. Link uses TCP to port 5068.  NRP Adaptations: SIPTrunking CM-ES-601 applied.  NRP Adaptations: Request-URI set to sip:31011@avaya.com  NRP Adaptations: Request URI set to sip:31011@avaya.com  Route &lt; sip:31011@avaya.com &gt; to SIP Entity CM601-Evolution-procr-5068 (10.1.2.220). Terminating Location is BaskingRidge HQ. </div>	<p><b>Called Party URI</b>  <input type="text" value="9133245977@avaya.com"/></p> <p><b>Calling Party URI</b>  <input type="text" value="9088485703@10.1.2.243"/></p> <p><b>Day Of Week</b>  <input type="text" value="Monday"/></p> <p><b>Time (UTC)</b>  <input type="text" value="18:49"/></p> <p><b>Called Session Manager Instance</b>  <input type="text" value="SM1"/></p>	<p><b>Calling Party Address</b>  <input type="text" value="10.1.2.243"/></p> <p><b>Session Manager Listen Port</b>  <input type="text" value="5060"/></p> <p><b>Transport Protocol</b>  <input type="text" value="TCP"/></p> <p style="text-align: right;"><input type="button" value="Execute Test"/></p>
<p><b>Called Party URI</b>  <input type="text" value="9133245977@avaya.com"/></p> <p><b>Calling Party URI</b>  <input type="text" value="9088485703@10.1.2.243"/></p> <p><b>Day Of Week</b>  <input type="text" value="Monday"/></p> <p><b>Time (UTC)</b>  <input type="text" value="18:49"/></p> <p><b>Called Session Manager Instance</b>  <input type="text" value="SM1"/></p>	<p><b>Calling Party Address</b>  <input type="text" value="10.1.2.243"/></p> <p><b>Session Manager Listen Port</b>  <input type="text" value="5060"/></p> <p><b>Transport Protocol</b>  <input type="text" value="TCP"/></p> <p style="text-align: right;"><input type="button" value="Execute Test"/></p>		

Outbound call from enterprise extension x31016 to PSTN number (908) 848-5703:

**Session Manager Administration**

- Administration
- Communication Profile Editor
- Network Configuration
- Device and Location Configuration
- Application Configuration
- System Status
- System Tools
  - Maintenance Tests
  - SIP Tracer
  - Configuration
  - SIP Trace Viewer
  - Call Routing Test**

### Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

#### SIP INVITE Parameters

<b>Called Party URI</b> 19088485703@avaya.com	<b>Calling Party Address</b> 10.1.2.220
<b>Calling Party URI</b> 31016@avaya.com	<b>Session Manager Listen Port</b> 5068
<b>Day Of Week</b> Monday	<b>Time (UTC)</b> 18:49
<b>Called Session Manager Instance</b> SM1	<b>Transport Protocol</b> TCP

---

#### Routing Decisions

Route < sip:19088485703@avaya.com > to SIP Entity SIPTrunking-AuraSBC (10.1.2.243). Terminating Location is AA-SBC.

---

#### Routing Decision Process

NRP Adaptations: SIPTrunking CM-ES-601 applied.

BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.

Originating Location is BaskingRidge HQ. Using digits < 19088485703 > and host < avaya.com > for routing.

NRP Dial Patterns: Found a Dial Pattern match for pattern < 19088485703 > Min/Max length 11/11 and domain < avaya.com >.

NRP Routing Policies: Ranked destination NRP Sip Entities: SIPTrunking-AuraSBC.

NRP Routing Policies: Removing disabled routes.

NRP Routing Policies: Ranked destination NRP Sip Entities: SIPTrunking-AuraSBC.

END EMERGENCY CALL CHECK: This is not an emergency call.

Adapting and proxying for SIP Entity SIPTrunking-AuraSBC.

NRP Entity Links: Found direct link to destination. Link uses TCP to port 5060.

NRP Adaptations: no Outgoing Adaptation administered.

Route < sip:19088485703@avaya.com > to SIP Entity SIPTrunking-AuraSBC (10.1.2.243). Terminating Location is AA-SBC.

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Aura® Session Border Controller 6.0 to CenturyLink SIP Trunking service. CenturyLink SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. CenturyLink SIP Trunking provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

## 11. References

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

- [1]*Installing and Configuring Avaya Aura® System Platform*, Release 6, June 2010.
- [2]*Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [3]*Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509.
- [4]*Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.0, August 2010, Document Number 555-245-205.
- [5]*Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
- [6]*Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, January 2011, Number 03-603473.
- [7]*Administering Avaya Aura® Session Manager*, Release 6.1, March 2011, Document Number 03-603324.
- [8]*Avaya Aura® Session Border Controller System Administration Guide*, V.6.0, September 2010
- [9]*Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.
- [10]*Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
- [11]*Avaya one-X® Communicator Getting Started*, August 2010.
- [12]*Avaya one-X® Communicator Quick Setup*, November 2009.
- [13]RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [14]RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [15]RFC 4244, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

Product documentation for CenturyLink SIP Trunking is available from CenturyLink.

## Appendix A: Avaya Aura® SBC Configuration File

```
#
# Copyright (c) 2004-2010 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 10:46:04 Mon 2011-02-21
#
config cluster
config box 1
  set hostname AuraSBC.avaya.com
  set timezone America/New_York
  set name AuraSBC.avaya.com
  set identifier 00:ca:fe:12:44:73
config interface eth0
  config ip inside
    set ip-address static 10.1.2.243/24
  config ssh
  return
  config snmp
    set trap-target 10.1.2.242 162
    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 10.1.2.1
    return
    config route Static0
      set destination network 192.11.13.4/30
      set gateway 10.1.2.241
    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
return
config interface eth2
config ip outside
  set ip-address static 12.184.9.179/24
config sip
  set udp-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 69.29.196.0/24
    set gateway 12.184.9.129
  return
return
config kernel-filter
  config allow-rule allow-sip-udp-from-peer-1
    set destination-port 5060
    set source-address/mask 69.29.196.0/24
    set protocol udp
  return
  config deny-rule deny-all-sip
    set destination-port 5060
  return
return
return
return
config cli
  set prompt AuraSBC.avaya.com
return
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 P-Charging-Vector
return
config third-party-call-control
return
return
config tls
config default-ca
    set ca-file /cxc/certs/sipca.pem
return
config certificate ws-cert
    set certificate-file /cxc/certs/ws.cert
return
config certificate aasbc.p12
    set certificate-file /cxc/certs/aasbc.p12
    set passphrase-tag aasbc-cert-tag
return
return
config session-config-pool
config entry ToTelco
    config to-uri-specification
        set host next-hop
    return
    config from-uri-specification
        set host local-ip
    return
    config request-uri-specification
        set host next-hop
    return
    config p-asserted-identity-uri-specification
        set host local-ip
    return
    config contact-uri-settings-in-leg
        set add-maddr disabled
    return
    config contact-uri-settings-out-leg
        set add-maddr disabled
    return
    config header-settings
    return
return
config entry ToPBX
    config to-uri-specification
        set host next-hop-domain
    return
    config request-uri-specification
        set host next-hop-domain
    return
    config contact-uri-settings-in-leg
        set add-maddr disabled
    return
    config contact-uri-settings-out-leg
        set add-maddr disabled

```

```

return
config header-settings
  config altered-header 1
    set source-header Max-Forwards
    set source-field selection .* 70
    set destination Max-Forwards
    set destination-field full
  return
return
return
config entry Discard
  config sip-directive
  return
return
return
config dial-plan
  config 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 ping-interval 60
      set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
      config server PBX1
        set host 10.1.2.210
        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 69.29.196.157
      return
    return
return

```

```

    return
return
config dns
    config resolver
        config server 192.168.1.200
        return
    return
return
config settings
    set read-header-max 8191
return
return

config external-services
return

config preferences
    config gui-preferences
        set enum-strings SIPSourceHeader Max-Forwards
    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 0x00630b556106ab6753185ad86a7dc06c2407ca2f6763efcb98d464acf9
            set permissions access\permissions superuser
        return
        config user cust
            set password 0x00b7c1912eb14049c66cb38128cd6a3857d7761119de7127cb28046d2c
            set permissions access\permissions read-only
        return
        config user init
            set password 0x009f6a2a9ad23ec6f7975a500921a893c6ffd0776159fc0160bdf2da6f
            set permissions access\permissions superuser
        return
        config user craft
            set password 0x005e51741b361f9e3f9475b2fff167da34ae5aa7f33d498db01484129e
            set permissions access\permissions superuser
        return
        config user dadmin
            set password 0x006135219ce7c515f159595c84aa5de9229379fc193c2e2cb8c74ea8a3
            set permissions access\permissions read-only
        return
    return
return

config features

```

---

**©2011 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ® are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).