



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

---

# **Application Notes for Configuring Broadvox SIP Trunking with Avaya Aura™ Communication Manager Evolution Server, Avaya Aura™ Session Manager, and Avaya Aura™ Session Border Controller – Issue 1.1**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the SIP service provider Broadvox and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura™ Session Border Controller, Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Evolution Server, and various Avaya endpoints.

Broadvox 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 the SIP service provider Broadvox and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura™ Session Border Controller (SBC), Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Evolution Server, and various Avaya H.323, SIP, digital and analog endpoints.

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

## 1.1. Interoperability Compliance Testing

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

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

- Incoming PSTN calls to various phone types  
Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types  
Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client)  
Avaya one-X Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Only the H.323 version of one-X Communicator was tested. The current GA SIP version (5.2) does not yet support Session Manager.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls and directory assistance (411)
- Codecs G.729A, and G.711MU.
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, transfer, and conference
- Off-net call forwarding and mobility (extension to cellular)

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls (911) are supported but were not tested as part of the compliance test.
- Network Call Redirection using the SIP REFER method or a 302 response with redirection is not supported.

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

- **T.38 Fax:** T.38 fax calls did not complete reliably. Thus, it is recommended that T.38 Fax is not used with this solution.
- **Media Shuffling:** Media shuffling must be disabled on Communication Manager for the SIP trunk used for Broadvox traffic. The call flow used by Communication Manager to perform media shuffling is not supported by Broadvox.
- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party.

## 1.2. Support

For technical support with Broadvox SIP Trunking, contact Broadvox by calling (888) 849-9608 opt. 3, or by sending an e-mail to [techsupport@broadvox.com](mailto:techsupport@broadvox.com). For all other inquiries you can contact customer service by calling (888) 849-9608 opt. 1, or [customerservice@broadvox.com](mailto:customerservice@broadvox.com) by e-mail.

## 2. Reference Configuration

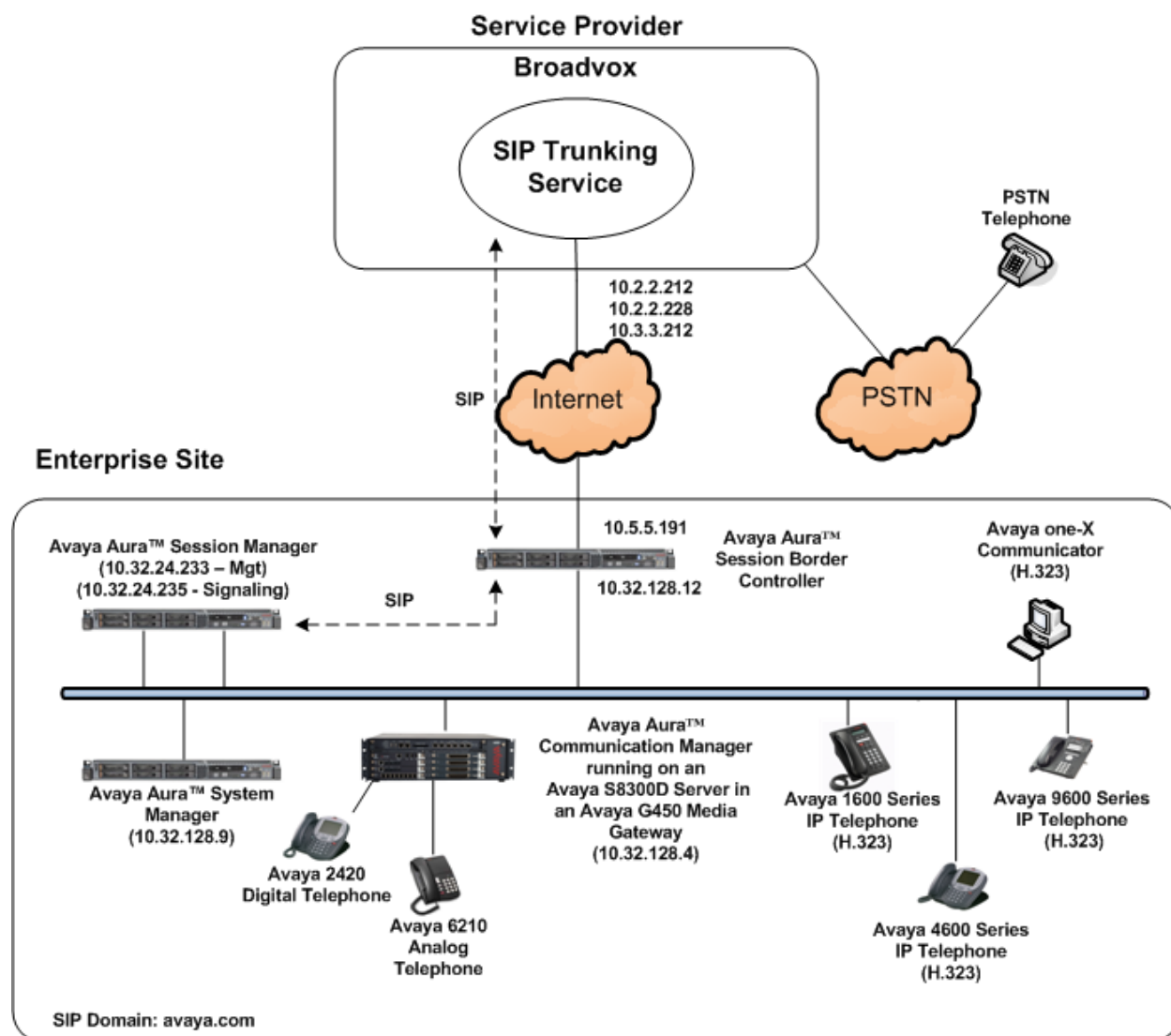
**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to Broadvox SIP Trunking. This is the configuration used for compliance testing.

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

- Avaya S8300D Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya 4600-Series IP telephones (H.323)
- Avaya 1600-Series IP telephones (H.323)
- Avaya one-X Communicator (H.323)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the SBC. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the

configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.



**Figure 1: Avaya IP Telephony Network using Broadvox SIP Trunking**

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

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

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

Broadvox has multiple SIP proxies that may answer or initiate SIP requests.

### 3. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura™ Communication Manager running on an Avaya S8300D Server	6.0 SP0 (R016x.00.0.345.0-18246)
Avaya G450 Media Gateway	30.10.4
Avaya Aura™ Session Manager running on an Avaya S8800 Server	6.0 (Build asm-6.0.0.0.600020)
Avaya Aura™ System Manager running on an Avaya S8800 Server	6.0 (Build 6.0.0.0.556-3.0.6.1)
Avaya 1608 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition 1.2.2
Avaya 4621SW IP Telephone (H.323)	2.9.1
Avaya 9640 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.1.1
Avaya 9630 IP Telephone (SIP)	Avaya one-X Deskphone SIP Edition 2.5
Avaya one-X Communicator (H.323)	5.2 SP3
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Avaya Aura™ Session Border Controller	6.0 (Build SBCT_6.0.0.1.4)
Broadvox SIP Trunking Solution Components	
Component	Release
Broadvox Softswitch - Fusion	v1.0

**Table 1: Equipment and Software Tested**

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

## 4. Configure Communication Manager

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

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

### 4.1. Licensing and Capacity

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

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	4000	36
Maximum Concurrently Registered IP Stations:	2400	3
Maximum Administered Remote Office Trunks:	4000	0
Maximum Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	2400	0
<b>Maximum Administered SIP Trunks:</b>	<b>4000</b>	<b>20</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0
Maximum TN2501 VAL Boards:	10	0
Maximum Media Gateway VAL Sources:	50	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0

## 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? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

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

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

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

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

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

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

### 4.3. IP Node Names

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

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

### 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. Broadvox SIP Trunking supports G.729A, and G.711MU. Thus, these codecs were included in this set in order of preference. The order of preference is defined by the end customer. Enter **G.729A**, and **G.711MU** in the **Audio Codec** column of the table. Default values can be used for all other fields.

change ip-codec-set 2

Page 1 of 2

IP Codec Set

Codec Set: 2

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

Since T.38 fax testing was not reliable, it is recommended to disable T.38 Fax by setting the **Fax Mode** field to **off** on **Page 2**. However, if T.38 fax is to be used, set the **Fax Mode** to **t.38-standard**.

change ip-codec-set 2		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? n		
FAX	Mode	Redundancy
	<b>off</b>	0
Modem	off	0
TDD/TTY	US	3



## 4.5. IP Network Region

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

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 4.4**.
- Default values can be used for all other fields.

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

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

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

## 4.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of *tls* (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to *5061*. For ease of troubleshooting, the compliance test was conducted with the **Transport Method** set to *tcp* and the **Near-end Listen Port** and **Far-end Listen Port** set to *5060*.
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field will initially be set to *Others* and can not be changed via administration. Later, the **Peer-Server** field will automatically change to *SM* once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Avaya S8300D Server running Communication Manager as defined in **Section 4.3**.
- Set the **Far-end Node Name** to *sessionMgr*. This node name maps to the IP address of Session Manager as defined in **Section 4.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 4.5**.
- Set the **Far-end Domain** to the domain of the service provider. This will be used to facilitate routing on Session Manager since the Request URI of outbound calls will contain this domain.

- Set **Direct IP-IP Audio Connections** to *n*. This field will disable media shuffling on the SIP trunk since Broadvox does not support the Avaya media shuffling call flow.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```

add signaling-group 2                                     Page 1 of 1
                                                    SIGNALING GROUP

Group Number: 2                Group Type: sip
IMS Enabled? n                Transport Method: tcp
    Q-SIP? n
    IP Video? n                SIP Enabled LSP? n
Peer Detection Enabled? y    Peer Server: SM            Enforce SIPS URI for SRTP? y

Near-end Node Name: procr                Far-end Node Name: sessionMgr
Near-end Listen Port: 5060                Far-end Listen Port: 5060
Far-end Domain: fs.broadvox.net            Far-end Network Region: 2

Incoming Dialog Loopbacks: eliminate        Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                    RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3            Direct IP-IP Audio Connections? n
    Enable Layer 3 Test? n                    IP Audio Hairpinning? n
                                                    Alternate Route Timer(sec): 6

```

## 4.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 4.6**. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

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

```
add trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2                                     Group Type: sip           CDR Reports: y
  Group Name: SP Trunk                               COR: 1           TN: 1           TAC: 1002
  Direction: two-way                               Outgoing Display? n
Dial Access? n                                       Night Service:
Queue Length: 0
Service Type: public-ntwrk                         Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 2
                                                Number of Members: 10
```

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

```
add trunk-group 2                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
SCCAN? n                                           Digital Loss Group: 18
  Preferred Minimum Session Refresh Interval(sec): 600
                                     Delay Call Setup When Accessed Via IGAR? n
```

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

**Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 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 2	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
<b>Numbering Format: public</b>	
	UI Treatment: service-provider
	<b>Replace Restricted Numbers? y</b>
	<b>Replace Unavailable Numbers? y</b>
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

On **Page 4**, set the **Network Call Redirection** field and **Send Diversion Header** field to **n**. Set the **Telephone Event Payload Type** to **101**, the value preferred by Broadvox.

add trunk-group 2	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
<b>Network Call Redirection? n</b>	
<b>Send Diversion Header? n</b>	
Support Request History? y	
<b>Telephone Event Payload Type: 101</b>	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Enable Q-SIP? n	

## 4.8. Calling Party Information

Public unknown numbering defines the calling party number to be sent to the far-end. This calling party number is sent in the SIP “From” header. Use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 40003, 40005 and 40010. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

Beginning with Communication Manager 6.0, numbers derived from this table are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity headers. The addition of the + sign did not impact interoperability with Broadvox.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	4			5	Total Administered: 4
5	40003	2	7325554489	10	Maximum Entries: 240
5	40005	2	7325554490	10	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.
5	40010	2	7325554491	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 public unknown 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 **CPN Prefix** plus the extension number.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	4	2	73255	10	Total Administered: 1
					Maximum Entries: 9999

## 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			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	4	dac							
4	5	ext							
8	1	fac							
<b>9</b>	<b>1</b>	<b>fac</b>							
*	3	fac							
#	3	fac							

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

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
<b>Auto Route Selection (ARS) – Access Code 1: 9</b>		Access Code 2:
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA: *01 All: *02		Deactivation: *03

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

change ars analysis 0					Page 1 of 2		
ARS DIGIT ANALYSIS TABLE					Percent Full: 2		
Location: all							
	Dialed String	Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
	0	1	1	2	op		n
	0	11	11	2	op		n
	00	2	2	2	op		n
	011	10	18	2	intl		n
	1732	11	11	2	fpna		n
	1800	11	11	2	fpna		n
	1877	11	11	2	fpna		n
	1908	11	11	2	fpna		n
	411	3	3	2	svcl		n



The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 2 was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk:** **1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **LAR:** *next*

change route-pattern 2													Page 1 of 3				
Pattern Number: 2													Pattern Name: SP route				
SCCAN? n													Secure SIP? n				
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC			
No			Mrk	Lmt	List	Del	Digits						QSIG				
													Intw				
1:	2	0	1									n	user				
2:												n	user				
3:												n	user				
4:												n	user				
5:												n	user				
6:												n	user				
BCC VALUE													TSC	CA-TSC	ITC BCIE Service/Feature		
0 1 2 M 4 W													Request		No. Numbering		
															Dgts Format		LAR
													Subaddress				
1:	y	y	y	y	y	n	n	rest					next				
2:	y	y	y	y	y	n	n	rest					none				
3:	y	y	y	y	y	n	n	rest					none				
4:	y	y	y	y	y	n	n	rest					none				

## 5. Configure Avaya Aura™ Session Manager

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

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

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

## 5.1. System Manager Login and Navigation

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

**AVAYA** Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 13, 2010 4:53 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

**Home Screen**

**Sub Pages**

Action	Description	Help
Elements	Interface to manage the application instances and contains the element managers for the different managed elements in the deployment.	<a href="#">Help for managing elements</a>
Events	Interface to view and administer logs and alarms.	<a href="#">Help for managing logs and alarms</a>
Groups & Roles	Interface to manage groups, resources and roles.	<a href="#">Help for managing groups and roles</a>
Licenses	Interface to manage licenses for individual applications of Avaya Aura (TM) Unified Communication Solution.	<a href="#">Help for managing licenses</a>
Routing	Interface to manage routing policies, adaptations, dial patterns, SIP elements.	<a href="#">Help for managing routing policies</a>
Security	Interface to manage certificates .Certificates help enable setting up secure communication between different elements in the Avaya Aura (TM) Unified Communication Solution.	<a href="#">Help for managing certificates</a>
System Manager Data	Interface to backup and restore System Manager data, manage data retention rules, list extension pack information, manage replication nodes, manage scheduled jobs and System Manager configuration.	<a href="#">Help for managing System Manager data and configuration</a>
Users	Interface to administer users, contact lists, shared addresses and Access Control Lists (ACLs).	<a href="#">Help for managing users</a>

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

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

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

Domain Management

CommitCancel

1 Item | RefreshFilter: Enable

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

\* Input Required

CommitCancel

The screen below shows the entry for the Broadvox domain.

Domain Management

CommitCancel

1 Item | RefreshFilter: Enable

Name	Type	Default	Notes
* fs.broadvox.net	sip	<input type="checkbox"/>	

\* Input Required

CommitCancel

### 5.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 5.1**) and click the **New** button in the right pane (not shown).

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

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

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

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

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

Location Details

Commit

Cancel

General

\* Name:

Location 1

Notes:

SP Subnet(s)

Managed Bandwidth:

Kbit/sec

\* Average Bandwidth per Call:

80

Kbit/sec

Location Pattern

Add

Remove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.128.*	

Select : All, None

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

Location Details

Commit

Cancel

General

\* Name:

Location 2

Notes:

Juan's Subnet(s)

Managed Bandwidth:

Kbit/sec

\* Average Bandwidth per Call:

80

Kbit/sec

Location Pattern

Add

Remove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.24.*	

Select : All, None

## 5.4. Add Adaptation Module

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

In the compliance test, two adaptations are needed. The first adaptation is applied to the Communication Manager SIP entity and maps inbound DID numbers from Broadvox to local Communication Manager extensions. The second adaptation is applied to the SBC SIP entity and converts the domain part of the incoming P-Asserted-Identity (PAI) header containing a Broadvox SIP proxy IP address to the Broadvox domain. This is necessary so that the PAI domain matches the value of the **Far-end Domain** configured on the Communication Manager signaling group in **Section 4.6**.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

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

**Adaptation Details**CommitCancel

**General**

\* **Adaptation name:**

**Module name:**

**Module parameter:**

**Egress URI Parameters:**

**Notes:**

To map inbound DID numbers from Broadvox 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

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--	------------------	-----	-----	---------------	---------------	-------------------	-------

### Digit Conversion for Outgoing Calls from SM

Add
Remove

3 Items | Refresh
Filter: Enable

	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 7325554489	* 10	* 10	* 10	40003	both ▼	
<input type="checkbox"/>	* 7325554490	* 10	* 10	* 10	40005	both ▼	
<input type="checkbox"/>	* 7325554491	* 10	* 10	* 10	40010	both ▼	

Select : All, None

\* Input Required
Commit
Cancel



To create the adaptation that will be applied to the SBC SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button in the right pane (not shown).

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter *DigitConversionAdapter*.
- **Module parameter:** Enter *iosrcd=fs.broadvox.net*. This is the IngressOverrideSourceDomain parameter. This parameter replaces the domain in the P-Asserted-Identity header and the calling part of the History-Info header with the given value for ingress only.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.

Adaptation Details

CommitCancel

General

\* Adaptation name: Broadvox Domain

Module name: DigitConversionAdapter

Module parameter: iosrcd=fs.broadvox.net

Egress URI Parameters:

Notes: Change IP to domain

Digit Conversion for Incoming Calls to SM

AddRemove

0 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes

Digit Conversion for Outgoing Calls from SM

AddRemove

0 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes

## 5.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and the SBC. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the SBC.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** created in **Section 5.4** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

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

**SIP Entity Details** Commit Cancel

**General**

\* **Name:**

\* **FQDN or IP Address:**

**Type:**

**Notes:**

**Location:**

**Outbound Proxy:**

**Time Zone:**

**Credential name:**

**SIP Link Monitoring**

**SIP Link Monitoring:**

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

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

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

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

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

**Port**

3 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP <input type="button" value="v"/>	avaya.com <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP <input type="button" value="v"/>	avaya.com <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS <input type="button" value="v"/>	avaya.com <input type="button" value="v"/>	<input type="text"/>

Select : All, None

**\* Input Required**

The following screen shows the addition of Communication Manager. The **FQDN or IP Address** field is set to the IP address of the Avaya S8300D Server running Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 5.4**.

SIP Entity Details

CommitCancel

General

\* Name:

sp3-cm

\* FQDN or IP Address:

10.32.128.4

Type:

CM

Notes:

Adaptation:

sp-cm3 Adaptation

Location:

Location 1

Time Zone:

America/New\_York

Override Port & Transport with DNS SRV:

☐

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

4

Credential name:

Call Detail Recording:

none

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

The following screen shows the addition of the SBC. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). For **Adaptation** field, select the adaptation module previously defined for modifying the domain in the PAI header in **Section 5.4**.

SIP Entity Details

CommitCancel

General

\* Name:

sp-sbc1

\* FQDN or IP Address:

10.32.128.12

Type:

SIP Trunk

Notes:

Adaptation:

Broadvox Domain

Location:

Location 1

Time Zone:

America/New\_York

Override Port & Transport with DNS SRV:

☐

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

4

Credential name:

Call Detail Recording:

egress

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

## 5.6. Add Entity Links

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

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

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

Entity Link to Communication Manager:

The screenshot shows the 'Entity Links' configuration page. At the top right are 'Commit' and 'Cancel' buttons. Below is a table with the following data:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* sp3-cm-link1	* devcon-asm	TCP	* 5060	* sp3-cm	* 5060	<input checked="" type="checkbox"/>	

Entity Link to the SBC:

The screenshot shows the 'Entity Links' configuration page. At the top right are 'Commit' and 'Cancel' buttons. Below is a table with the following data:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* toAuraSBC	* devcon-asm	TCP	* 5060	* sp-sbc1	* 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 SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

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

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

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

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

Routing Policy Details

CommitCancel

General

\* Name:

sp3-cm Route

Disabled:

☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
sp3-cm	10.32.128.4	CM	

Routing Policy Details

CommitCancel

General

\* Name:

SP Aura SBC route

Disabled:

☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
sp-sbc1	10.32.128.12	SIP Trunk	

## 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 Broadvox and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 5.1**) and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

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

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



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

Dial Pattern Details
Commit
Cancel

General

\* Pattern: 1

\* Min: 11

\* Max: 11

Emergency Call: ☐

SIP Domain: fs.broadvox.net

Notes: Orig: Loc1&2 Dest: sp-sbc1

Originating Locations and Routing Policies

Add Remove

2 Items Refresh Filter: Enable

<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"/>	Location 1	SP Subnet(s)	<a href="#">SP AuraSBC route</a>	0	<input type="checkbox"/>	sp-sbc1	
<input type="checkbox"/>	Location 2	Juan's Subnet(s)	<a href="#">SP AuraSBC route</a>	0	<input type="checkbox"/>	sp-sbc1	

Select : All, None

The second example shows that 10 digit numbers that start with 73255544 to any domain and originating from **Location 1** uses route policy **sp3-cm Route**. These are the DID numbers assigned to the enterprise from Broadvox. Location 1 is selected because these calls come from the SBC which resides in location 1.

Dial Pattern Details
Commit
Cancel

General

\* Pattern: 73255544  
\* Min: 10  
\* Max: 10  
Emergency Call: ☐  
SIP Domain: -ALL-  
Notes: Orig: Loc1 Dest: sp3-cm

Originating Locations and Routing Policies

Add
Remove

1 Item Refresh
Filter: Enable

<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"/>	Location 1	SP Subnet(s)	<a href="#">sp3-cm Route</a>	0	<input type="checkbox"/>	sp3-cm	

Select : All, None

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

Dial Patterns						
Edit New Duplicate Delete More Actions ▼ Commit						
6 Items Refresh Filter: Enable						
<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	<u>0</u>	1	11	<input type="checkbox"/>	fs.broadvox.net	Orig: Loc1&2 Dest: sp-sbc1
<input type="checkbox"/>	<u>011</u>	10	18	<input type="checkbox"/>	fs.broadvox.net	Orig: Loc1&2 Dest: sp-sbc1
<input type="checkbox"/>	<u>1</u>	11	11	<input type="checkbox"/>	fs.broadvox.net	Orig: Loc1&2 Dest: sp-sbc1
<input type="checkbox"/>	<u>411</u>	3	3	<input type="checkbox"/>	fs.broadvox.net	Orig: Loc1&2 Dest: sp-sbc1
<input type="checkbox"/>	<u>73255544</u>	10	10	<input type="checkbox"/>	-ALL-	Orig: Loc1 Dest: sp3-cm
Select : All, None						

## 5.9. Add/View Session Manager

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

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

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

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

### View Session Manager

Return

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |  
Expand All | Collapse All

**General** ▼

SIP Entity Name

devcon-asm

Description

Management Access Point Host Name/IP

10.32.24.233

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 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.

**Security Module** ▼

<b>SIP Entity IP Address</b>	10.32.24.235
<b>Network Mask</b>	255.255.255.0
<b>Default Gateway</b>	10.32.24.1
<b>Call Control PHB</b>	46
<b>QOS Priority</b>	6
<b>Speed &amp; Duplex</b>	Auto
<b>VLAN ID</b>	

## 6. Configure Avaya Aura™ Session Border Controller

This section describes the configuration of the Avaya Aura™ SBC. This configuration is done in two parts. The first part is done during the SBC installation via the installation wizard. These Application Notes will not cover the SBC installation in its entirety but will include the use of the installation wizard. For information on installing the Avaya Aura™ System Platform and the loading of the Avaya Aura™ SBC template see [1].

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

### 6.1. Installation Wizard

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

#### 6.1.1. Network Settings

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

- **IP Address:** Enter the IP address of the private side of the SBC.
- **Hostname:** Enter a host name for the SBC.

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

The screenshot shows the Avaya Aura Network Settings installation wizard. The left sidebar contains a navigation menu with the following items: Home, Configuration, Installation (expanded), Network Settings (with a red X icon), VPN Access (with a yellow icon), SBC (with a red X icon), 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	<input type="text" value="10.32.128.10"/>
CDom IP Address	<input type="text" value="10.32.128.11"/>
Gateway IP Address	<input type="text" value="10.32.128.254"/>
Network Mask	<input type="text" value="255.255.255.0"/>
Primary DNS	<input type="text" value="10.32.24.150"/>
Secondary DNS	<input type="text"/>
HTTPS Proxy (if required) [IP Address:Port Number]	<input type="text"/>

Below these fields is a table for Virtual Machine settings:

Virtual Machine	IP Address	Hostname
SBC	<input type="text" value="10.32.128.12"/>	<input type="text" value="sp-sbc1"/>

### 6.1.2. VPN Access

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

Click **Next Step** to continue.

**AVAYA**

Home

Configuration

Installation

- Network Settings
- 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

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](#)

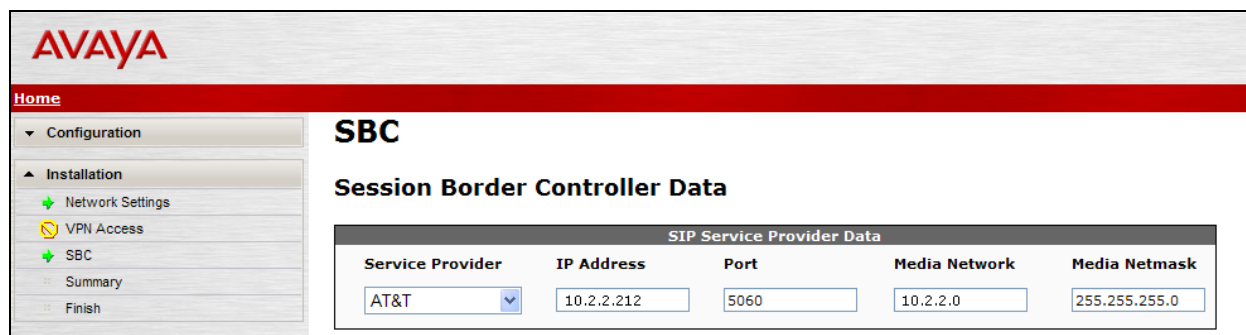
### 6.1.3. SBC

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

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

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

Scroll down to continue.



The screenshot shows the Avaya SBC configuration interface. On the left is a navigation menu with 'Home' at the top, followed by 'Configuration' and 'Installation'. Under 'Installation', there are links for 'Network Settings', 'VPN Access', 'SBC' (which is highlighted with a green plus icon), 'Summary', and 'Finish'. The main content area is titled 'SBC' and 'Session Border Controller Data'. Below this is a section titled 'SIP Service Provider Data' containing a table with five columns: 'Service Provider', 'IP Address', 'Port', 'Media Network', and 'Media Netmask'. The 'Service Provider' column has a dropdown menu with 'AT&T' selected. The 'IP Address' column contains the text '10.2.2.212'. The 'Port' column contains '5060'. The 'Media Network' column contains '10.2.2.0'. The 'Media Netmask' column contains '255.255.255.0'.

Service Provider	IP Address	Port	Media Network	Media Netmask
AT&T	10.2.2.212	5060	10.2.2.0	255.255.255.0

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

In the **SBC Network Data** section:

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

In the **Enterprise SIP Server** section:

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

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

SBC Network Data			
Interface	IP Address	Net Mask	Gateway
Private (Management)	10.32.128.12	255.255.255.0	10.32.128.254
Public	<input type="text" value="10.5.5.191"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="10.5.5.254"/>

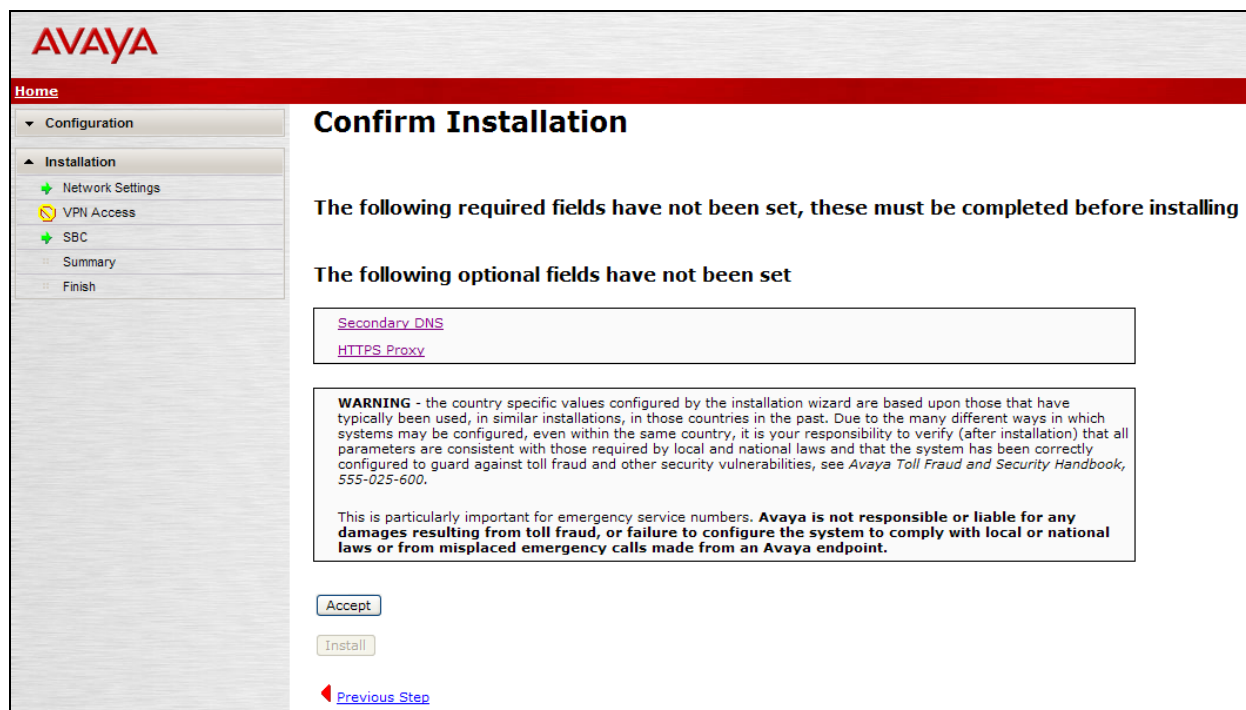
Enterprise SIP Server		
IP Address	Transport	SIP Domain
<input type="text" value="10.32.24.235"/>	<input type="text" value="TCP"/>	<input type="text" value="avaya.com"/>

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



### 6.1.4. Confirm Installation

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



The screenshot shows the Avaya web interface for the 'Confirm Installation' step. On the left is a navigation menu with 'Configuration' expanded, showing 'Installation' as the current section. The main content area is titled 'Confirm Installation'. It contains two sections: 'The following required fields have not been set, these must be completed before installing' and 'The following optional fields have not been set'. Below these are links for 'Secondary DNS' and 'HTTPS Proxy'. A 'WARNING' box states that country-specific values are based on past configurations and that users must verify local and national laws. At the bottom are buttons for 'Accept', 'Install', and a link for 'Previous Step'.

### 6.2. Post Installation Configuration

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



The screenshot shows the login screen for 'Acme Packet Net-Net OS-E'. The title is 'Acme Packet Net-Net OS-E'. Below it, a message says: 'To access the NNOS-E management interface, you must first log in. Please provide your user name and password.' There are two input fields: 'Username:' and 'Password:'. Below these fields is a 'Login' button.

### 6.2.1. Additional SIP Proxies

Broadvox has multiple SIP proxies which may process or initiate SIP requests. The installation wizard creates a single entry in the sip-gateway server pool based on the information provided in the wizard. Since Broadvox has multiple proxies, the additional proxies must be entered manually. To add a proxy to the server-pool list, begin by navigating to **vsp** → **enterprise** → **servers** → **sip-gateway Telco** → **server-pool** in the left-hand navigation pane. Click **Add server** in the right pane.

The screenshot shows the Avaya Aura Configuration interface. The left-hand navigation pane is expanded to show the path: **vsp** → **enterprise** → **servers** → **sip-gateway Telco** → **server-pool**. The right-hand pane displays the configuration for the selected server pool. At the top, there are tabs for **Set**, **Reset**, and **Back**, and a **Delete** button. Below these is a table with columns: **server**, **admin**, **host**, **transport**, **port**, **outbound-normalization**, **inbound-normalization**, **admission-control**, and **emission-control**. The table contains one entry: **server Telco1**, **enabled**, **10.2.2.212**, **UDP**, **5060**, **Configure**, **Configure**, **disabled**, and **disable**. Below the table, there are links for **Add server** and **Add handle-response**. At the bottom, there are tabs for **Set**, **Reset**, and **Back**.

In the right pane that appears, enter the following:

- **server-name:** Enter a descriptive name for the new proxy.
- **host:** Enter the IP address of the proxy.

Click **Create**. A SIP server will be created in the server-pool list with default values for all other parameters. The Edit screen for the server-pool entry will appear in the right pane (not shown). No other modifications are needed.

The screenshot shows the Avaya Aura Configuration interface. The left-hand navigation pane is expanded to show the path: **vsp** → **enterprise** → **servers** → **sip-gateway Telco** → **server-pool**. The right-hand pane displays the configuration for the selected server pool. At the top, there are tabs for **Home**, **Configuration**, **Status**, **Call Logs**, **Event Logs**, **Actions**, **Services**, **Keys**, **Access**, and **Tools**. Below these is a title bar: **Create vsplenterprise\servers\sip-gateway Telco\server-pool\server - Step 1 of 1: Edit server**. Below the title bar is a message: **Please provide some basic information for server. Then press "Create".** Below the message is a form with two fields: **\* server-name** (value: **Telco2**) and **\* host** (value: **10.2.2.228**, with a note: **(host name or n.n.n.n)**). Below the form are buttons for **Create**, **Reset**, and **Cancel**.

Repeat the procedure in this section to add each additional Broadvox SIP proxy. Navigating to **vsp** → **enterprise** → **servers** → **sip-gateway Telco** → **server-pool** in the left-hand navigation pane shows the complete list of Broadvox SIP proxies used for the compliance test.

The screenshot shows the Avaya Aura Configuration interface. The left-hand navigation pane is expanded to show the path: **cluster** → **box:sp-sbc1** → **vsp** → **enterprise** → **servers** → **sip-gateway Telco** → **server-pool**. The main content area is titled "Configure vspenterprise\servers\sip-gateway Telco\server-pool". It includes buttons for "Set", "Reset", "Back", and "Delete". Below these is a table with columns: "server", "admin", "host", "transport", "port", "outbound-normalization", "inbound-normalization", "admission-control", and "enabled". The table contains three rows of data for "server Telco1", "server Telco2", and "server Telco3". Each row has "Edit" and "Delete" links. Below the table is an "Add server" link. At the bottom, there are "Set", "Reset", and "Back" buttons, and "Help" and "Index" links.

server	admin	host	transport	port	outbound-normalization	inbound-normalization	admission-control	enabled
server Telco1	enabled	10.2.2.212	UDP	5060	Configure	Configure	disabled	di
server Telco2	enabled	10.2.2.228	UDP	5060	Configure	Configure	disabled	di
server Telco3	enabled	10.3.3.212	UDP	5060	Configure	Configure	disabled	di

## 6.2.2. Additional Media Paths

Media may originate from multiple subnets in the Broadvox network. The installation wizard creates a route for a single subnet based on the information provided in the wizard. Since Broadvox has multiple media subnets, additional routes must be entered manually. To add a route, begin by navigating to **cluster** → **box:sp-sbc1** → **interface eth2** → **ip outside** → **routing** in the left-hand navigation pane. Note that the box name **sp-sbc1** is the host name of the SBC and will differ between different SBC instances. Click **Add route** in the right pane.

The screenshot shows the Avaya Aura Configuration interface. The left-hand navigation pane is expanded to show the path: **cluster** → **box:sp-sbc1** → **interface eth2** → **ip outside** → **routing**. The main content area is titled "Configure cluster\box:sp-sbc1\interface eth2\ip outside\routing". It includes buttons for "Set", "Reset", "Back", and "Delete". Below these is a table with columns: "route", "admin", "destination", "gateway", and "metric". The table contains two rows of data: "route Default" (disabled, default, 0.0.0.0, 1) and "route external-sip-media" (enabled, network 10.2.2.0/24, 10.5.5.254, 1). Below the table is an "Add route" link. At the bottom, there are "Set", "Reset", and "Back" buttons, and "Help" and "Index" links.

route	admin	destination	gateway	metric
route Default	disabled	default	0.0.0.0	1
route external-sip-media	enabled	network 10.2.2.0/24	10.5.5.254	1

In the right pane that appears, enter the following:

- **route-name:** Enter a descriptive name for the new route.
- **type:** Select **network**.
- **address/mask:** Enter the destination network address and subnet mask that needs to be reached.
- **gateway:** Enter the gateway address to be used to reach the destination network.



Click **Create**. A route will be created with default values for all other parameters. The Edit screen for the route will appear in the right pane (not shown). No other modifications are needed.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The main content area is titled 'Configuration: all' and shows a tree view of the configuration hierarchy on the left. The right pane displays the 'Create clusterbox 1interface eth2ip outside\routing\route - Step 1 of 1: Edit route' screen. The form contains the following fields:

- \* route-name:** external-sip-media2
- \* destination:**
  - \* type:** network (network route)
  - \* address/mask:** 10.3.3.0/24
- \* gateway:** 10.5.5.254 (n.n.n.n)

At the bottom of the form are three buttons: Create, Reset, and Cancel.

Repeat the procedure in this section to add each additional route. Navigating to **cluster** → **box:sp-sbc1** → **interface eth2** → **ip outside** → **routing** in the left-hand navigation pane shows the complete list of routes used for the compliance test.

[Status Summary](#)
[Logout admin](#)

[Home](#)
[Configuration](#)
[Status](#)
[Call Logs](#)
[Event Logs](#)
[Actions](#)
[Services](#)
[Keys](#)
[Access](#)
[Tools](#)

**Configuration: all**

[Configuration](#)
[Setup](#)
[View](#)

cluster

box:sp-sbc1

interface eth0

interface eth2

ip outside

sip

media-ports

routing

cli

os

vsp

default-session-config

tls

session-config-pool

dial-plan

enterprise

dns

settings

Configure clusterbox:sp-sbc1interface eth2ip outsiderouting
[Help](#)
[Index](#)

Set

Reset

Back

Delete

route

	route	admin	destination	gateway	metric
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">route Default</a>	disabled	default	0.0.0.0	1
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">route external-sip-media</a>	enabled	network 10.2.2.0/24	10.5.5.254	1
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">route external-sip-media2</a>	enabled	network 10.3.3.0/24	10.5.5.254	1
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">route external-sip-media3</a>	enabled	network 10.11.1.0/24	10.5.5.254	1
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">route external-sip-media4</a>	enabled	network 10.11.7.0/24	10.5.5.254	1
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">route external-sip-media5</a>	enabled	network 10.12.20.0/24	10.5.5.254	1
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">route external-sip-media6</a>	enabled	network 10.12.21.0/24	10.5.5.254	1
<a href="#">Edit</a> <a href="#">Delete</a>	<a href="#">route external-sip-media7</a>	enabled	network 10.13.59.0/24	10.5.5.254	1

[Add route](#)

### 6.2.3. Domain and Options Frequency

To enter the domain for the Broadvox network, first navigate to **vsp** → **enterprise** → **server** → **sig-gateway Telco**. In the **domain** field, enter the Broadvox domain *fs.broadvox.net*.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view under 'Configuration: all' with the path: cluster > box:sp-sbc1 > interface eth0 > interface eth2 > cli > os > vsp > default-session-config > tls > session-config-pool > dial-plan > enterprise > servers > sip-gateway PBX > sip-gateway Telco. The main content area is titled 'Configure vspenterprise\servers\sip-gateway Telco'. It includes a 'Show advanced' button and links for 'Manage connections', 'Log instant messages', 'Record media', 'Record files', 'Set up accounting', 'Change "from:" URI', and 'Change "to:" URI'. Below these are buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The 'general' section contains fields for: '\* name' (Telco), 'admin' (enabled), 'domain' (fs.broadvox.net), and 'failover-detection' (ping). A 'servers' section shows a 'server-pool' with a 'Delete' link.

To set the frequency of the OPTIONS messages sent from the SBC to the service provider, click **Show Advanced** in the previous figure and scroll down to the **Routing** section of the form. Enter the desired interval in the **ping-interval** field. Click **Set** at the top of the form (shown in previous figure).

This screenshot shows the 'routing' section of the configuration page. The left sidebar is identical to the previous figure. The main content area shows the 'routing' section with a 'routing-setting' dropdown menu containing 'normalization', 'auto-tag-match', 'auto-domain-match', and 'pstn-backup'. Below this are 'Select All' and 'Unselect All' buttons. Other fields include: 'domain-alias' (Edit domain-alias), 'domain-subnet' (Edit domain-subnet), 'loop-detection' (tight), 'service-type' (provider), and 'ping-interval' (60 seconds).

## 6.2.4. Blocked Headers

Two SIP headers appearing in the SIP traffic between the Session Manager and the Broadvox network posed potential problems for interoperability. The first was the Allow-events header contained in messages sent from the Broadvox network to the Session Manager. Session Manager was not able to process this header. The second was the P-site header sent in SIP messages from the Session Manager to the Broadvox network. This header contained private IP addresses from the enterprise. These private IP addresses 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 → session-config-pool → entry ToTelco → header-settings**. Click **Edit blocked-header**.

Configuration: all

Configuration Setup View

- cluster
  - box:sp-sbc1
- vsp
  - default-session-config
  - tls
  - session-config-pool
    - entry ToTelco
      - header-settings
      - to-uri-specification
      - from-uri-specification
      - request-uri-specification
      - p-asserted-identity-uri-specification
      - header-settings
    - entry ToPBX
    - entry Discard
  - dial-plan
  - enterprise
  - dns
  - settings

Configure vspsession-config-poolentry ToTelcoheader-settings

Show advanced Help Index

Set Reset Back Delete

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

In the right pane that appears, click **Add**. In the blank field that appears, enter the name of the header to be blocked. To add another blocked header, click **Add** again and enter the next header. After all headers are entered, click **OK**. The screen below shows the **Allow-Events** and **P-Site** headers blocked for the compliance test.

### Configure vsp\session-config-pool\entry ToTelco\header-settings blocked-header

X

X

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

**Configuration**

[Home](#)
[Configuration](#)
[Status](#)
[Call Logs](#)
[Event Logs](#)
[Actions](#)
[Services](#)
[Keys](#)
[Access](#)
[Tools](#)

[Status Summary](#)
[Logout admin](#)

**Configuration: all**

- cluster
  - box:sp-sbc1
- vsp
  - default-session-config
  - tls
  - session-config-pool
    - entry ToTelco
      - sip-settings
        - to-uri-specification
        - from-uri-specification
        - request-uri-specification
        - p-asserted-identity-uri-specific
        - header-settings**
      - entry ToPBX
      - entry Discard
    - dial-plan
    - enterprise
    - dns
    - settings

**Configure vsp\session-config-pool\entry ToTelco\header-settings**

[Help](#)
[Index](#)

<b>allowed-header</b>	<a href="#">Edit allowed-header</a>
<b>blocked-header</b>	<input type="text" value="Allow-Events"/> <input type="text" value="P-Site"/> <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>	<input type="text" value="requests-and-responses"/> <small>(apply to requests and responses)</small>
<b>apply-to-allow-block-to-dialog</b>	<input type="text" value="both"/> <small>(Apply to both inbound and outbound dialogs.)</small>



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

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows the navigation tree with 'vsp' expanded, and 'session-config-pool' > 'entry ToPBX' > 'header-settings' selected. The main content area is titled 'Configure vsp|session-config-pool|entry ToPBX|header-settings'. It includes buttons for 'Set', 'Reset', 'Back', and 'Delete'. Below these are several configuration fields:

allowed-header	<a href="#">Edit allowed-header</a>
blocked-header	<input type="text" value="Allow-Events"/> <input type="text" value="P-Size"/> <a href="#">Edit blocked-header</a>
altered-header	<a href="#">Add altered-header</a>
reg-ex-header	<a href="#">Add reg-ex-header</a>
header-normalization	<a href="#">Add header-normalization</a>
altered-body	<a href="#">Add altered-body</a>
reg-ex-collector	<a href="#">Add reg-ex-collector</a>
apply-allow-block-to	requests-and-responses (apply to requests and responses)
apply-to-allow-block-to-dialog	both (Apply to both inbound and outbound dialogs.)

### 6.2.5. Third Party Call Control

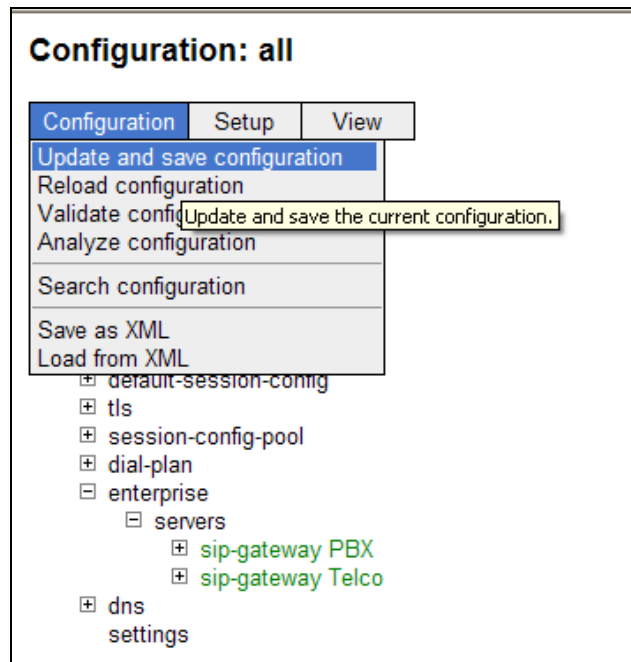
Disable third party call control. Navigate to **vsp** → **default-session-config** → **third-party-call-control**. Set the **admin** field to *disabled*.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows the navigation tree with 'vsp' expanded, and 'default-session-config' > 'third-party-call-control' selected. The main content area is titled 'Configure vsp|default-session-config|third-party-call-control'. It includes buttons for 'Set', 'Reset', 'Back', and 'Delete'. Below these are several configuration fields:

admin	disabled (Resource is inactive)
status-events	both (both call-legs)
handle-refer-locally	enabled (Resource is active)
refer-maintain-identity	false
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>

### 6.2.6. 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. Broadvox SIP Trunking Configuration

To use Broadvox SIP Trunking, a customer must request the service from Broadvox using their sales processes. The process can be started by contacting Broadvox via the corporate web site at [www.broadvox.com](http://www.broadvox.com) and requesting information via the online sales links or telephone numbers.

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

## 8. General Test Approach and Test Results

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

Broadvox SIP Trunking passed compliance testing.

## 9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

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.

## 10. Conclusion

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

## 11. References

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

- [1] *Installing and Configuring Avaya Aura™ System Platform*, Release 6, June 2010.
- [2] *Administering Avaya Aura™ System Platform*, Release 6, June 2010.
- [3] *Administering Avaya Aura™ Communication Manager*, May 2009, Document Number 03-300509.
- [4] *Avaya Aura™ Communication Manager Feature Description and Implementation*, May 2009, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura™ System Manager 5.2 GA Version*, January 2010.
- [6] *Installing Avaya Aura™ Session Manager*, January 2010.
- [7] *Administering Avaya Aura™ Session Manager*, March 2010, Document Number 03-603324.
- [8] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x*, February 2010, Document Number 16-601443.
- [9] *4600 Series IP Telephone LAN Administrator Guide*, October 2007, Document Number 555-233-507.
- [10] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, November 2009, Document Number 16-300698.
- [11] *Avaya one-X Communicator Getting Started*, November 2009.
- [12] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [13] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [14] RFC 4244, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

## 12. Appendix A: Avaya Aura™ SBC Configuration File

```
#
# Copyright (c) 2004-2010 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 16:46:38 Thu 2010-07-29
#
config cluster
config box 1
    set hostname sp-sbc1
    set timezone America/New_York
    set name sp-sbc1
    set identifier 00:ca:fe:09:42:38
config interface eth0
    config ip inside
        set ip-address static 10.32.128.12/24
    config ssh
    return
    config snmp
        set trap-target 10.32.128.11 162
        set trap-filter generic
        set trap-filter dos
        set trap-filter sip
        set trap-filter system
    return
    config web
    return
    config web-service
        set protocol https 8443
        set authentication certificate "vsp\tls\certificate ws-cert"
    return
    config sip
        set udp-port 5060 "" "" any 0
        set tcp-port 5060 "" "" any 0
        set tls-port 5061 "" "" any 0
    return
    config icmp
    return
    config media-ports
    return
    config routing
        config route Default
            set gateway 10.32.128.254
        return
        config route Static0
            set destination network 192.11.13.4/30
            set gateway 10.32.128.10
        return
        config route Static1
            set admin disabled
        return
```

```

config route Static2
    set admin disabled
return
config route Static3
    set admin disabled
return
config route Static4
    set admin disabled
return
config route Static5
    set admin disabled
return
config route Static6
    set admin disabled
return
config route Static7
    set admin disabled
return
config route internal-sip-media
    set destination host 10.32.24.235
    set gateway 10.32.128.254
return
return
return
config interface eth2
config ip outside
    set ip-address static 10.5.5.191/24
config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" any 0
return
config media-ports
return
config routing
    config route Default
        set admin disabled
    return
    config route external-sip-media
        set destination network 10.2.2.0/24
        set gateway 10.5.5.254
    return
    config route external-sip-media2
        set destination network 10.3.3.0/24
        set gateway 10.5.5.254
    return
    config route external-sip-media3
        set destination network 10.11.1.0/24
        set gateway 10.5.5.254
    return
    config route external-sip-media4
        set destination network 10.11.7.0/24
        set gateway 10.5.5.254
    return
    config route external-sip-media5

```

```

        set destination network 10.12.20.0/24
        set gateway 10.5.5.254
    return
    config route external-sip-media6
        set destination network 10.12.21.0/24
        set gateway 10.5.5.254
    return
    config route external-sip-media7
        set destination network 10.13.59.0/24
        set gateway 10.5.5.254
    return
    return
    return
    return
    config cli
        set prompt sp-sbc1
    return
    config os
    return
    return
    return
return

config services
config event-log
    config file access
        set filter access info
    return
    config file system
        set filter general info
        set filter system info
    return
    config file errorlog
        set filter all error
    return
    config file db
        set filter db debug
        set filter dosDatabase info
    return
    config file management
        set filter management info
    return
    config file peer
        set filter sipSvr info
    return
    config file cac
        set filter sipCAC warning
    return
    config file dos
        set filter dos alert
        set filter dosSip alert
        set filter dosTransport alert
        set filter dosUrl alert
    return
    config file krnlsys
        set filter krnlsys debug
    return

```

```

    config file acct
        set filter acct debug
    return
return

config master-services
config accounting
return
config database
    set media enabled
return
return

config vsp
set admin enabled
config default-session-config
    config media
        set anchor enabled
        set rtp-stats enabled
    return
config sip-directive
    set directive allow
return
config log-alert
    set apply-to-methods-for-filtered-logs
return
config third-party-call-control
return
return
config tls
    config certificate ws-cert
        set certificate-file /cxc/certs/ws.cert
    return
return
config session-config-pool
    config entry ToTelco
        config sip-settings
        return
        config to-uri-specification
            set host next-hop
        return
        config from-uri-specification
            set host local-ip
        return
        config request-uri-specification
            set host next-hop
        return
        config p-asserted-identity-uri-specification
            set host local-ip
        return
        config header-settings
            set blocked-header Allow-Events
            set blocked-header P-Site
        return
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 header-settings
    set blocked-header Allow-Events
    set blocked-header P-Site
  return
return
config entry Discard
  config sip-directive
  return
return
config dial-plan
  config route Default
    set priority 500
    set location-match-preferred exclusive
    set session-config vsp\session-config-pool\entry Discard
  return
  config source-route FromTelco
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
    set peer server "vsp\enterprise\servers\sip-gateway Telco"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
return
config enterprise
  config servers
    config sip-gateway PBX
      set domain avaya.com
      set failover-detection ping
      set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
  config server-pool
    config server PBX1
      set host 10.32.24.235
      set transport TCP
    return
  return
return
  config sip-gateway Telco
    set domain fs.broadvox.net
    set failover-detection ping
    set ping-interval 60
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
  config server-pool
    config server Telco1
      set host 10.2.2.212
    return

```

```

        config server Telco2
        set host 10.2.2.228
        return
        config server Telco3
        set host 10.3.3.212
        return
    return
return
config dns
    config resolver
    config server 10.32.24.150
    return
return
return
config settings
    set stack-socket-threads-max 2
return
return

config external-services
return

config preferences
    config gui-preferences
    return
return

config access
    config permissions superuser
    set cli advanced
    return
    config permissions read-only
    set config view
    set actions disabled
    return
    config users
    config user admin
    set password 0x002bdd5d9fea2fefeb97b0115854a47db2c8b27a2fe0187e0274977f4b
    set permissions access\permissions superuser
    return
    config user cust
    set password 0x004803cd9fae4ee1b2462598359d6c5e179008f9083caa7b30b9b19b43
    set permissions access\permissions read-only
    return
return
return

config features
return

```

---

**©2010 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).