



Application Notes for Configuring Broadvox SIP Trunking Service with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 6.2 – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the Broadvox SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.

The Broadvox SIP Trunking service offered by Broadvox provides customers with PSTN access via a SIP trunk between the enterprise and the Broadvox network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	6
2.3.	Support	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager.....	11
5.1.	Licensing and Capacity	11
5.2.	System Features.....	12
5.3.	IP Node Names.....	13
5.4.	Codecs	13
5.5.	IP Network Regions	14
5.6.	Signaling Group	15
5.7.	Trunk Group.....	17
5.8.	Calling Party Information.....	19
5.9.	Inbound Routing.....	19
5.10.	Outbound Routing	20
6.	Configure Avaya Aura® Session Manager	22
6.1.	System Manager Login and Navigation.....	23
6.2.	SIP Domain	24
6.3.	Locations	24
6.4.	SIP Entities	26
6.5.	Entity Links	30
6.6.	Routing Policies	31
6.7.	Dial Patterns	32
7.	Configure Avaya Session Border Controller for Enterprise	35
7.1.	System Access.....	35
7.2.	System Management	36
7.3.	Global Profiles.....	37
7.3.1.	Server Interworking	37
7.3.2.	Server Configuration.....	43
7.3.3.	Routing Profiles	47
7.3.4.	Topology Hiding.....	49
7.4.	Domain Policies	51
7.4.1.	Signaling Rules	51
7.4.2.	End Point Policy Groups.....	54
7.5.	Device Specific Settings.....	56
7.5.1.	Network Management.....	56
7.5.2.	Media Interface	57
7.5.3.	Signaling Interface	58
7.5.4.	End Point Flows.....	60

8.	Broadvox SIP Trunking Service Configuration.....	62
9.	Verification and Troubleshooting	62
9.1.	General Verification Steps	62
9.2.	Communication Manager Verification.....	62
9.3.	Session Manager Verification	63
9.4.	Avaya SBCE Verification	64
10.	Conclusion	66
11.	References.....	66

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the Broadvox SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2 and various Avaya endpoints.

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

2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Broadvox SIP Trunk service via a broadband connection to the public Internet.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

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

- SIP trunk registration with the service provider.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN 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 calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones in the “This Computer” and “Other Phone” modes. (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Flare® Experience for Windows softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 deskphones, Avaya one-X® Communicator and Flare® Experience for Windows.
- Various call types, including: local, long distance and international.
- Codecs G.711U and G729A and proper codec negotiation.
- DTMF tone transmissions passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- T.38 fax.

Items not supported or not tested included the following:

- Inbound toll-free and emergency (911) calls are supported but were not tested as part of the compliance test.
- Network Call Redirection methods using REFER or 302 Temporarily Unavailable messages are not supported by Broadvox and were not tested.
- Operator services such as dialing 0 or 0 + 10 digits are not supported.

2.2. Test Results

Interoperability testing of the Broadvox SIP Trunking service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observation described below:

- **Media Shuffling:** Direct IP-IP Audio Connections (media shuffling) must be disabled on the Communication Manager signaling group used by the SIP trunk connected to the Broadvox SIP Trunking service. The re-INVITEs used by Communication Manager to perform media shuffling are not supported by Broadvox.

2.3. Support

For technical support on the Broadvox SIP Trunking service, contact Broadvox by calling (888) 849-9608 options 2 or 3, or by sending an e-mail to techsupport@broadvox.com.

For all other inquiries visit <http://www.broadvox.com/products/sip-trunking>, or contact customer service by calling (888) 849-9608 opt. 1, or by email to customerservice@broadvox.com.

3. Reference Configuration

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

For security purposes, references to any public IP addresses used during the compliance test have been replaced in these Application Notes with private addresses. Also, PSTN routable phone numbers used in the test have been changed to non-routable numbers.

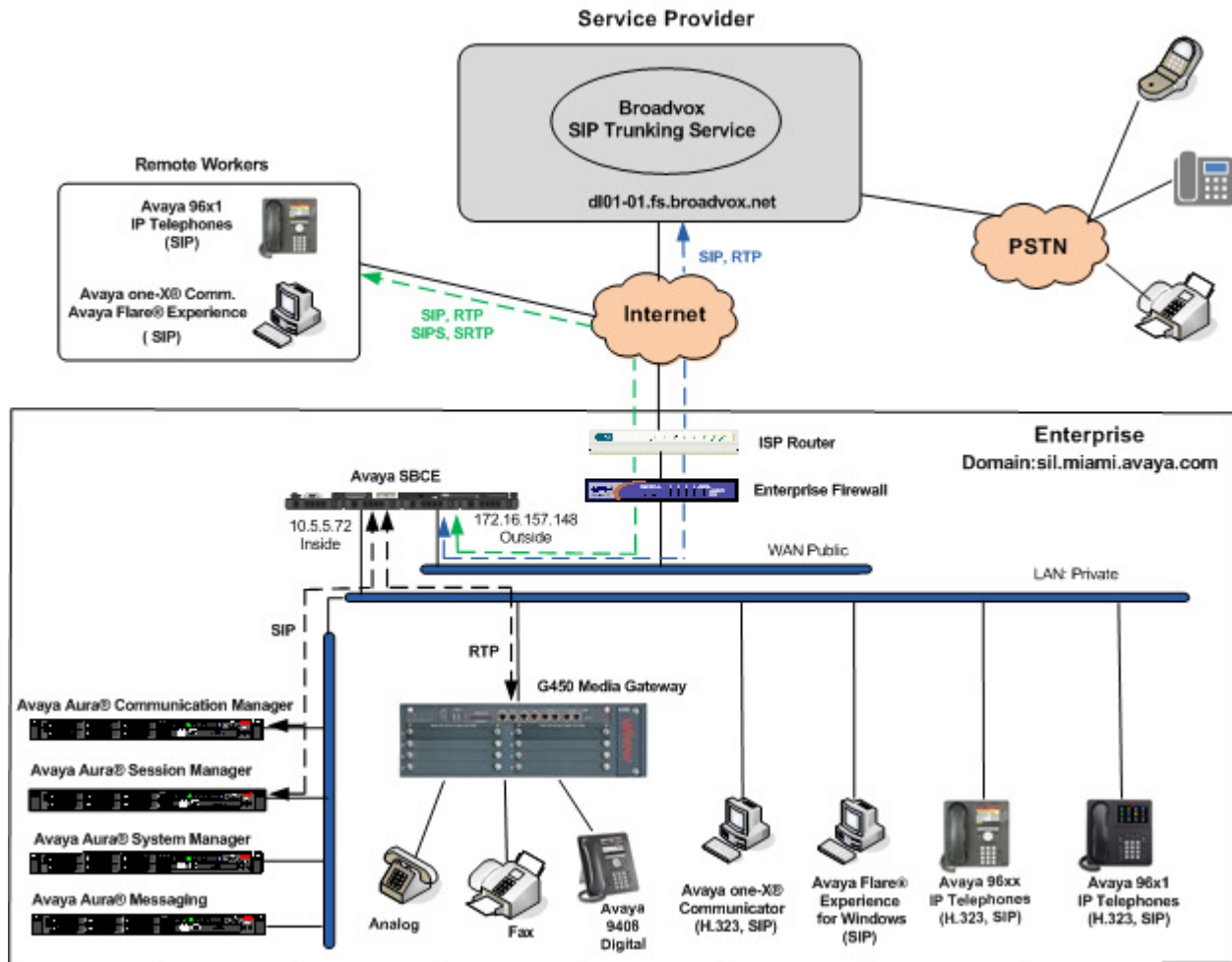


Figure 1: Avaya SIP Enterprise Solution connected to the Broadvox SIP Trunking service

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

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Aura® Messaging.
- Avaya G450 Media Gateway.
- Avaya 96x0 and 96x1 Series IP Telephones (H.323 and SIP).
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya Flare® Experience for Windows softphones.
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality, introduced with Avaya Aura® 6.2 Feature Pack 2. A remote worker is a SIP endpoint that resides in the untrusted network, registered to the Session Manager at the enterprise via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test, using the following endpoints and protocols:

- Avaya 96x1 SIP Deskphones (using TLS and SRTP).
- Avaya one-X® Communicator SIP (using TCP and RTP).
- Avaya Flare® Experience for Windows (using TCP and RTP).

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [7] in the **References** section for more information on this topic.

The Avaya SBCE is located at the edge of the enterprise. It has a public side that connects to the external network and a private side that connects to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flows through the Avaya SBCE, which in this way can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides the registration capability of the SIP trunk with the service provider, and also performs network address translation at both the IP and SIP layers.

The SIP Proxy server assigned by Broadvox during the compliance test used the fully qualified domain name (FQDN) “dl01-01.fs.broadvox.net”. The Avaya SBCE was configured to use an external DNS server to resolve the IP addresses of the Broadvox SIP Proxy servers used to route outbound signaling traffic.

The transport protocol between the Avaya SBCE and Broadvox across the public IP network is UDP. The transport protocol between the Avaya SBCE and the enterprise Session Manager across the enterprise IP network is TCP.

For inbound calls, the calls flow from the service provider to the external firewall, to the Avaya SBCE, 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 were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Broadvox network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. The trunk carried both inbound and outbound traffic.

Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of MWI (Message Waiting Indicator) messages to the enterprise telephones. Messaging was installed on a single standalone server located on the enterprise network, administered as a separate SIP entity in Session Manager. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the Broadvox SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager on HP® Proliant DL360 G7 Server	6.3-03.0.124.0
Avaya Aura® Session Manager on HP® Proliant DL360 G7 Server	6.3.3.0633004
Avaya Aura® System Manager on HP® Proliant DL360 G7 Server	6.3.3 Software Update Rev. 6.3.3.5.1719
Avaya Session Border Controller for Enterprise on a Dell R210 V2 Server	6.2.0.Q48
Avaya Aura® Messaging on a Dell PowerEdge R610 server	6.2.SP3
Avaya G450 Media Gateway	33.13.0
Avaya 96xx Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 3.2
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 6.2.2.17
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 6.2.2 (SP2)
Avaya one-X Communicator (H.323, SIP)	6.1.8.06-SP8-40314
Avaya Flare Experience for Windows	1.1.3.14
Broadvox SIP Trunking service	
Broadvox Fusion softswitch	Version 1.0

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Broadvox SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Broadvox. It is assumed that the general installation of Communication Manager, the 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.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **391** 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:		12000	10
Maximum Concurrently Registered IP Stations:		18000	3
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		41000	2
Maximum Video Capable IP Softphones:		18000	6
Maximum Administered SIP Trunks:		24000	391
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		128	0
Maximum Media Gateway VAL Sources:		250	1
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	0
Maximum Number of Expanded Meet-me Conference Ports:		100	0
(NOTE: You must logoff & login to effect the permission changes.)			

5.2. System Features

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

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

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

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

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

```
change system-parameters features                               Page 9 of 20
FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

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

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and the Session Manager Security Module (**asm**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
Acme_s1p0	192.168.10.52	
HG_CM	172.16.5.12	
HG_SM	172.16.5.32	
asm	192.168.10.32	
default	0.0.0.0	
ip_office	192.168.10.60	
msgserver	192.168.10.12	
procr	192.168.10.12	
procr6	::	

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 4 was used for this purpose. The Broadvox SIP Trunking service used codecs G.711MU and G.729A, in this order of preference. Enter **G.711MU** and **G.729A** in the **Audio Codec** column of the table. Default values can be used for all other fields.

change ip-codec-set 4		Page 1 of 2
IP Codec Set		
Codec Set: 4		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.711MU	<u>n</u>	<u>2</u>
2: G.729A	<u>n</u>	<u>2</u>
3:		

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

change ip-codec-set 4		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? <u>n</u>		
FAX	Mode	Redundancy
FAX	t.38-standard	<u>0</u>
Modem	off	<u>0</u>
TDD/TTY	US	<u>3</u>
Clear-channel	<u>n</u>	<u>0</u>

5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. 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 4 was chosen for the service provider trunk. Use the **change ip-network-region 4** command to configure region 4 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is *sil.miami.avaya.com* as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to *yes*, the default setting. This will 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. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

change ip-network-region 4		Page 1 of 20
IP NETWORK REGION		
Region: 4		
Location: 1	Authoritative Domain: <u>sil.miami.avaya.com</u>	
Name: <u>Broadvox SIP Trunk</u>	Stub Network Region: <u>n</u>	
MEDIA PARAMETERS		
Codec Set: <u>4</u>	Intra-region IP-IP Direct Audio: <u>yes</u>	
	Inter-region IP-IP Direct Audio: <u>yes</u>	
UDP Port Min: <u>2048</u>	IP Audio Hairpinning? <u>n</u>	
UDP Port Max: <u>3329</u>		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: <u>46</u>		
Audio PHB Value: <u>46</u>		
Video PHB Value: <u>26</u>		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: <u>6</u>		
Audio 802.1p Priority: <u>6</u>		
Video 802.1p Priority: <u>5</u>		
AUDIO RESOURCE RESERVATION PARAMETERS		
H.323 IP ENDPOINTS	RSUP Enabled? <u>n</u>	
H.323 Link Bounce Recovery? <u>y</u>		
Idle Traffic Interval (sec): <u>20</u>		
Keep-Alive Interval (sec): <u>5</u>		
Keep-Alive Count: <u>5</u>		

On **Page 4**, define the IP codec set to be used for traffic between region 4 and region 1 (the rest of the enterprise). 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 following example shows the settings used for the compliance test. It indicates that codec set **4** will be used for calls between region 4 (the service provider region) and region 1 (the rest of the enterprise).

change ip-network-region 4										Page	4 of 20
Source Region: 4 Inter Network Region Connection Management										I	M
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr Regions	Dyn CAC	A	G	L	A	t
1	4	y	NoLimit			n					t
2											
3											
4	4									all	
5											

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 4 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 transport protocol to be used between Communication Manager and Session Manager. For the compliance test, *tcp* was used.
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field will initially be set to *Others* and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to *SM* once Communication Manager detects its peer is a Session Manager.

Note: Once the **Peer-Server** field is updated to *SM*, the system changes the default values of the following fields, setting them to display-only:

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to *y*.
- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to *n*.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *asm*. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.

change signaling-group 4 Page 1 of 2

SIGNALING GROUP

Group Number: 4 Group Type: sip

IMS Enabled? n Transport Method: tcp

Q-SIP? n

IP Video? n Enforce SIPS URI for SRTP? y

Peer Detection Enabled? y Peer Server: SM

Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y

Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Near-end Node Name: procr Far-end Node Name: asm

Near-end Listen Port: 5075 Far-end Listen Port: 5075

Far-end Network Region: 4

Far-end Secondary Node Name: _____

Far-end Domain: sil.miami.avaya.com

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? y IP Audio Hairpinning? n

Alternate Route Timer(sec): 6

- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TCP, the well-known port value is 5060). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. For the compliance test both the **Near-end Listen Port** and **Far-end Listen Port** were set to **5075**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **n**. This setting will effectively disable media shuffling on the SIP trunk. Broadvox does not support the re-INVITEs used by Communication Manager when performing media shuffling, as previously mentioned in **Section 2.2**.
- Default values may be used for all other fields.

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 4 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 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.

```
change trunk-group 4                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 4      Group Type: sip      CDR Reports: y
Group Name: Broadvox      COR: 1      TN: 1      TAC: 604
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: 4
                                     Number of Members: 6
```

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 default value of **600** seconds was used.

```
change trunk-group 4                                     Page 2 of 21
      Group Type: sip
TRUNK PARAMETERS
      Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
      SCCAN? n      Digital Loss Group: 18
      Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
```

On **Page 3**, set the **Numbering Format** field to *public*. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity headers. The addition of the + sign did not impact interoperability with Broadvox. Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to *y*. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block.

change trunk-group 4		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? <u>n</u>	Measured: <u>none</u>	Maintenance Tests? <u>y</u>
Numbering Format: <u>public</u>		UUI Treatment: <u>service-provider</u>
Replace Restricted Numbers? <u>y</u>		Replace Unavailable Numbers? <u>y</u>

On **Page 4**, set the **Telephone Event Payload Type** to *101*, and **Convert 180 to 183 for Early Media** to *y*. Default values were used for all other fields.

change trunk-group 4		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? <u>n</u>		
Prepend '+' to Calling/Alerting/Diverting/Connected Number? <u>n</u>		
Send Transferring Party Information? <u>n</u>		
Network Call Redirection? <u>n</u>		
Send Diversion Header? <u>n</u>		
Support Request History? <u>n</u>		
Telephone Event Payload Type: <u>101</u>		
Convert 180 to 183 for Early Media? <u>y</u>		
Always Use re-INVITE for Display Updates? <u>n</u>		
Identity for Calling Party Display: <u>P-Asserted-Identity</u>		
Block Sending Calling Party Location in INVITE? <u>n</u>		
Accept Redirect to Blank User Destination? <u>n</u>		
Enable Q-SIP? <u>n</u>		

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the sample configuration, three DID numbers were assigned for testing. These DID numbers, preceded by the country code “1” and the “+” sign which is automatically inserted by Communication Manager, were used as the outbound calling party information on the service provider trunk when calls were originated from these extensions.

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2			4	Total Administered: 5
4	3			4	Maximum Entries: 9999
4	3001	4	17325551234	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	3002	4	17325551235	11	
4	3003	4	17325551236	11	

5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the 10 digit DID number sent by Broadvox is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 4					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	7325551234	10	3001	
public-ntwrk	10	7325551235	10	3002	
public-ntwrk	10	7325551236	10	3003	
public-ntwrk					

5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below 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								
Location: all								
Percent Full: 2								
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	attd						
1	5	ext						
2	5	ext						
3	4	ext						
4	5	ext						
5	5	ext						
6	3	dac						
7	5	ext						
8	5	ext						
9	1	fac						
*	3	dac						
#	3	dac						

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: <u>*10</u>				
Abbreviated Dialing List2 Access Code: <u>*12</u>				
Abbreviated Dialing List3 Access Code: <u>*13</u>				
Abbreviated Dial - Prgm Group List Access Code: <u>*14</u>				
Announcement Access Code: <u>*19</u>				
Answer Back Access Code: <u> </u>				
Auto Alternate Routing (AAR) Access Code: <u>*00</u>				
Auto Route Selection (ARS) - Access Code 1: <u>9</u>			Access Code 2: <u> </u>	
Automatic Callback Activation: <u>*33</u>			Deactivation: <u>#33</u>	
Call Forwarding Activation Busy/DA: <u>*30</u>			Deactivation: <u>#30</u>	
Call Forwarding Enhanced Status: <u> </u>			Act: <u> </u>	
			Deactivation: <u> </u>	

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 4 which contains the SIP trunk group to the service provider.

change ars analysis 0							Page	1 of	2
ARS DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 0		
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd			
011	10	14	4	intl		n			
1786	11	11	4	fnpa		n			
1800	11	11	4	fnpa		n			
732	10	10	4	hnpa		n			
411	3	3	4	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 4 for the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 4 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:** Setting the prefix mark (**Pfx Mrk**) to **1** will prefix any FNPA 10-digit number with a "1" and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance calls.
- Default values were used for all other fields.

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

6. Configure Avaya Aura® Session Manager

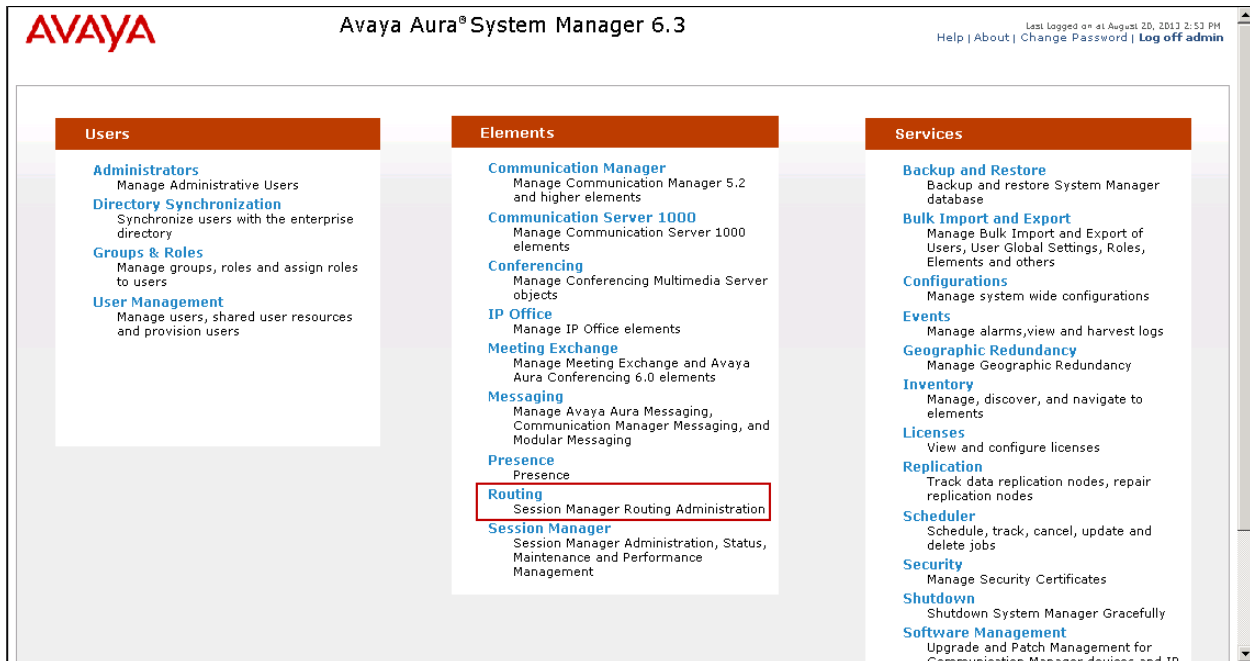
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- 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.

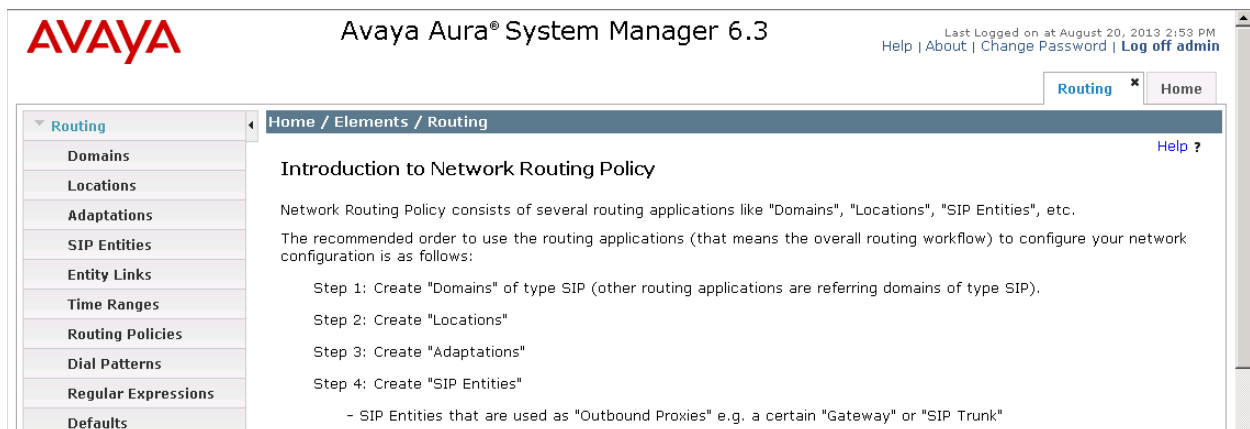
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

6.1. System Manager Login and Navigation

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



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



6.2. 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 will be the enterprise domain, **sil.miami.avaya.com**. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) 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.

The screenshot shows the 'Domain Management' interface. On the left is a navigation pane with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the breadcrumb is a 'Domain Management' section with 'Commit' and 'Cancel' buttons. A table below shows one item with columns 'Name', 'Type', and 'Notes'. The 'Name' column contains 'sil.miami.avaya.com', the 'Type' column contains 'sip', and the 'Notes' column contains 'MA Lab Domain'. There are 'Commit' and 'Cancel' buttons at the bottom right of the table.

Name	Type	Notes
* sil.miami.avaya.com	sip	MA Lab Domain

6.3. Locations

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

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

Defaults can be used for all other parameters.

The following screen shows the location details for the location named “MA Session Manager”. Later, this location will be assigned to the SIP Entity corresponding to Session Manager.

Home / Elements / Routing / Locations
[Help ?](#)

Location Details
Commit Cancel

General

* Name: MA Session Manager
Notes: Session Manager

Dial Plan Transparency in Survivable Mode

Enabled: ☐
Listed Directory Number:
Associated CM SIP Entity:

Overall Managed Bandwidth

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

Per-Call Bandwidth Parameters

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

Alarm Threshold

Overall Alarm Threshold: 80 %
Multimedia Alarm Threshold: 80 %
* Latency before Overall Alarm Trigger: 5 Minutes
* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove
0 Items Refresh Filter: Enable

☐ IP Address Pattern Notes

Commit Cancel

The following screen shows the location details for the location named “MA Communication Manager”. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.

The screenshot shows a web interface with a breadcrumb trail: Home / Elements / Routing / Locations. Below this is a section titled 'Location Details' with 'Commit' and 'Cancel' buttons. Under the 'General' tab, there are two input fields: '* Name:' with the value 'MA Communication Manager' and 'Notes:' with the value 'HP DL360'.

The following screen shows the location details for the location named “MA SBCE”. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.

The screenshot shows a web interface with a breadcrumb trail: Home / Elements / Routing / Locations. Below this is a section titled 'Location Details' with 'Commit' and 'Cancel' buttons. Under the 'General' tab, there are two input fields: '* Name:' with the value 'MA SBCE' and 'Notes:' with the value 'Avaya SBCE 6.2'.

6.4. 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 Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager Security Module is entered for **FQDN or IP Address**.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* **Name:** MA_Session Manager

* **FQDN or IP Address:** 192.168.10.32

Type: Session Manager

Notes: Security Module

Location: MA Session Manager

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

To define the ports that Session Manager will use to listen for SIP requests, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. The screen below shows the ports used by Session Manager in the shared lab environment. TCP ports 5060 and 5075 are the ones directly relevant to the SIP trunk to Broadvox in the reference configuration.

Port

TCP Failover port:

TLS Failover port:

Add Remove

7 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	sil.miami.avaya.com	
<input type="checkbox"/>	5060	UDP	sil.miami.avaya.com	
<input type="checkbox"/>	5061	TLS	sil.miami.avaya.com	
<input type="checkbox"/>	5070	TCP	sil.miami.avaya.com	
<input type="checkbox"/>	5075	TCP	sil.miami.avaya.com	
<input type="checkbox"/>	5080	TCP	sil.miami.avaya.com	
<input type="checkbox"/>	6060	TCP	sil.miami.avaya.com	

The following screen shows the addition of the SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different to the one created during the Session Manager installation, to be used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager.

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#)

SIP Entity Details

Commit

Cancel

General

* Name:

MA_CM Trunk 4

* FQDN or IP Address:

192.168.10.12

Type:

CM

Notes:

Adaptation:

Location:

MA Communication Manager

Time Zone:

America/New_York

Override Port & Transport with DNS SRV:

☐

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

Loop Detection

Loop Detection Mode:

Off

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

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#)

SIP Entity Details

CommitCancel

General

* Name:

MA_SBCE

* FQDN or IP Address:

10.5.5.72

Type:

SIP Trunk

Notes:

Avaya SBCE

Adaptation:

Location:

MA SBCE

Time Zone:

America/New_York

Override Port & Transport with DNS SRV:

☐

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

Loop Detection

Loop Detection Mode:

Off

MAA; Reviewed:
SPOC 11/5/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

29 of 67
BrdvoxCMSMASBCE

6.5. Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **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 from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.

Click **Commit** to save.

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Entity Links'. There are 'Commit' and 'Cancel' buttons. Below the title, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The values in the table are: Name: *MA SM to CM Tr 4, SIP Entity 1: *MA_Session Manager, Protocol: TCP, Port: *5075, SIP Entity 2: *MA_CM Trunk 4, Port: *5075, and Connection Policy: trusted.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
*MA SM to CM Tr 4	*MA_Session Manager	TCP	*5075	*MA_CM Trunk 4	*5075	trusted

Entity Link to the Avaya SBCE:

The screenshot shows the 'Entity Links' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Entity Links'. There are 'Commit' and 'Cancel' buttons. Below the title, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The values in the table are: Name: *MA SM to ASBCE, SIP Entity 1: *MA_Session Manager, Protocol: TCP, Port: *5060, SIP Entity 2: *MA_SBCE, Port: *5060, and Connection Policy: trusted.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
*MA SM to ASBCE	*MA_Session Manager	TCP	*5060	*MA_SBCE	*5060	trusted

6.6. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added; one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose 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 Avaya SBCE

Home / Elements / Routing / Routing Policies [Help ?](#)

Routing Policy Details [Commit](#) [Cancel](#)

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
MA_CM Trunk 4	192.168.10.12	CM	

Home / Elements / Routing / Routing Policies [Help ?](#)

Routing Policy Details [Commit](#) [Cancel](#)

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
MA_SBCE	10.5.5.72	SIP Trunk	Avaya SBCE

6.7. Dial Patterns

Dial Patterns are needed to route specific 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 navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, or select “**ALL**” to route incoming calls to all SIP domains.
- **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.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with **732555**, which is the DID range assigned by Broadvox to the SIP trunk, arriving from location **MA SBCE**, under **Originating Location Name**, will use route policy **To CM Trunk 4** to Communication Manager.

Home / Elements / Routing / Dial Patterns
[Help ?](#)

Dial Pattern Details
[Commit](#) [Cancel](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	MA SBCE	Avaya SBCE 6.2	To CM Trunk 4	0	<input type="checkbox"/>	MA_CM Trunk 4	

Repeat this procedure as needed to define additional dial patterns for other numbers assigned by Broadvox to the enterprise, to be routed to Communication Manager.

The example in this screen shows that 11 digit dialed numbers for outbound calls, beginning with a number such as **1786** used for test purposes during the compliance test, arriving from the **MA Communication Manager** location, under **Originating Location Name**, will use route policy **Outbound to MA ASBCE**, which sends the call out to the PSTN via the Avaya SBCE to the Broadvox SIP Trunk.

Home / Elements / Routing / Dial Patterns
Help ?

Dial Pattern Details
Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	MA Communication Manager	HP DL360	Outbound to MA ASBCE		<input type="checkbox"/>	MA_SBCE	Outbound to MA_SBCE

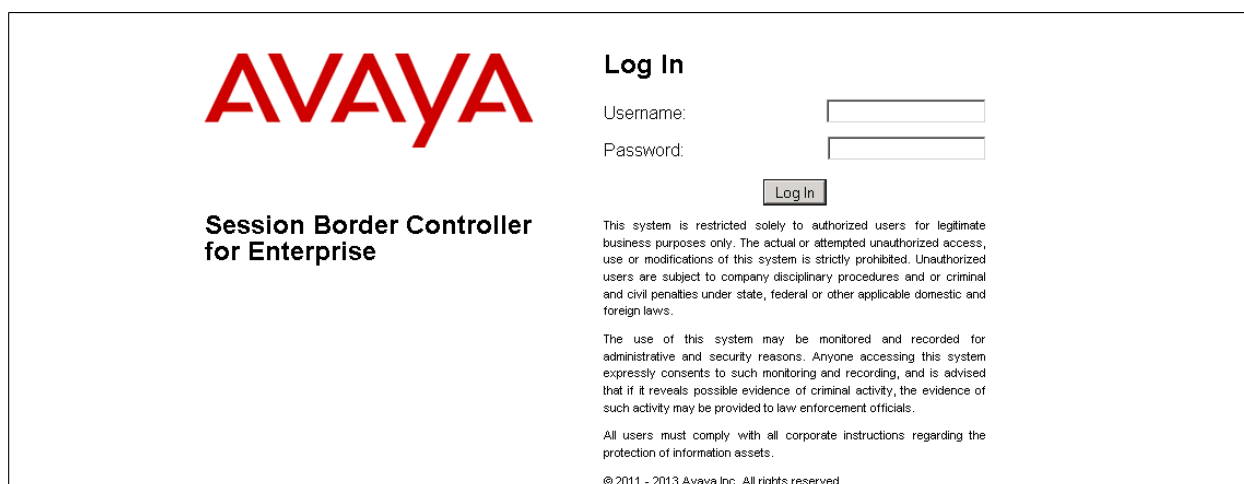
Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the Broadvox network via the Avaya SBCE.

7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Broadvox SIP Trunking service. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For more information on the SBC installation and initial provisioning, consult the Avaya SBCE documentation listed in the **References** section.

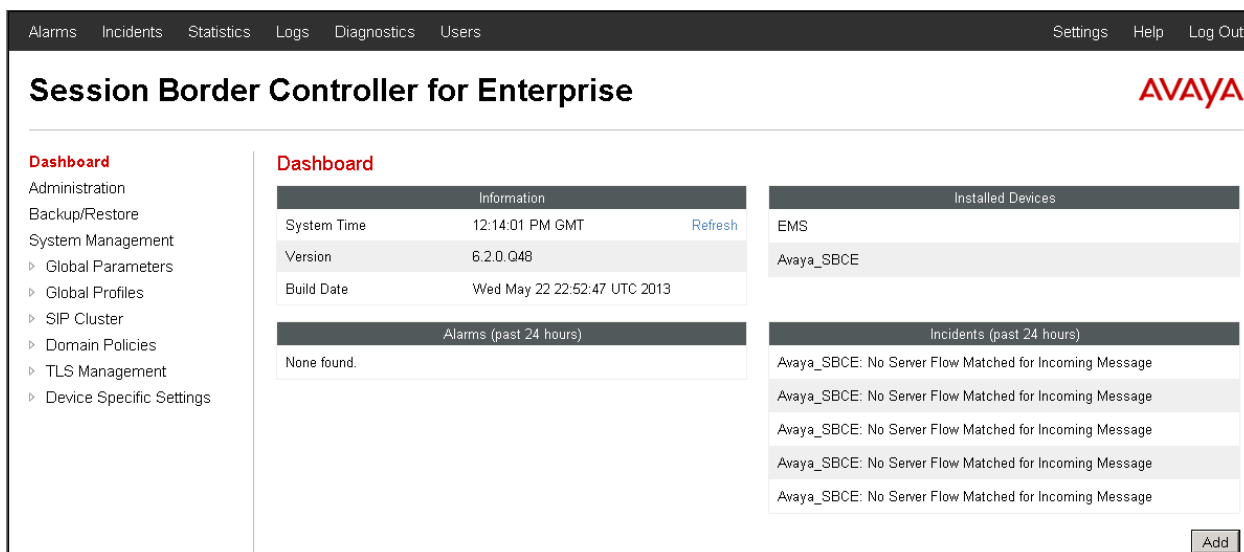
7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The login page features the Avaya logo in red on the left. To the right, under the heading "Log In", are two input fields for "Username:" and "Password:". Below these is a "Log In" button. Further down, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." This is followed by a statement: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." Below that is another statement: "All users must comply with all corporate instructions regarding the protection of information assets." At the very bottom, it says "© 2011 - 2013 Avaya Inc. All rights reserved."

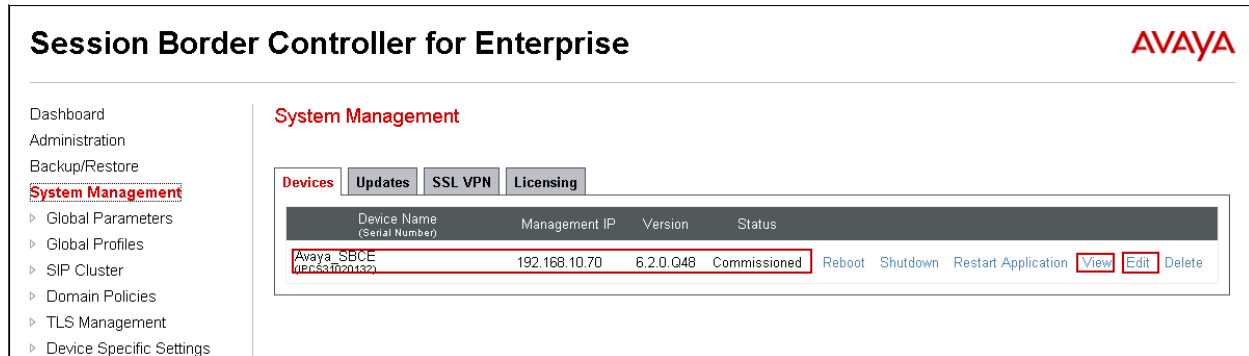
Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.



The dashboard has a top navigation bar with links: Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left is a navigation pane with "Dashboard" selected, and sub-items: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is divided into four sections: "Information" (System Time: 12:14:01 PM GMT, Version: 6.2.0.Q48, Build Date: Wed May 22 22:52:47 UTC 2013), "Installed Devices" (listing EMS and Avaya_SBCE), "Alarms (past 24 hours)" (showing "None found."), and "Incidents (past 24 hours)" (listing five incidents, each with the message "Avaya_SBCE: No Server Flow Matched for Incoming Message"). An "Add" button is at the bottom right.

7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named **Avaya_SBCE** is shown. The management IP address that was configured during installation and the current software version are shown here. Note that the management IP address needs to be on a subnet separate from the ones used in the other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



Session Border Controller for Enterprise

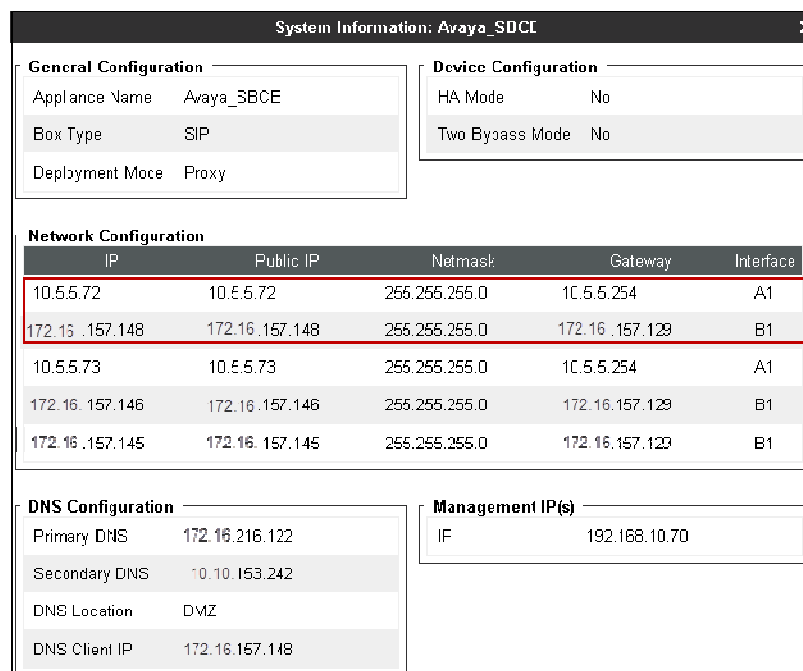
System Management

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings

Devices Updates SSL VPN Licensing

Device Name (Serial Number)	Management IP	Version	Status	
Avaya_SBCE (version132)	192.168.10.70	6.2.0.Q48	Commissioned	Reboot Shutdown Restart Application View Edit Delete

To view the network information assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device and the network settings. Note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces for the Avaya SBCE. The highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Broadvox. Other IP addresses assigned to these interfaces on the screen below are used to support remote workers and they are not discussed in this document.



System Information: Avaya_SBCE

General Configuration

Appliance Name: Avaya_SBCE
Box Type: SIP
Deployment Mode: Proxy

Device Configuration

HA Mode: No
Two Bypass Mode: No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.5.5.72	10.5.5.72	255.255.255.0	10.5.5.254	A1
172.16.157.148	172.16.157.148	255.255.255.0	172.16.157.129	B1
10.5.5.73	10.5.5.73	255.255.255.0	10.5.5.254	A1
172.16.157.146	172.16.157.146	255.255.255.0	172.16.157.129	B1
172.16.157.145	172.16.157.145	255.255.255.0	172.16.157.129	B1

DNS Configuration

Primary DNS: 172.16.216.122
Secondary DNS: 10.10.153.242
DNS Location: DMZ
DNS Client IP: 172.16.157.148

Management IP(s)

IP: 192.168.10.70

DNS server information can be entered or modified if needed, by clicking **Edit** on the **System Management/Devices** tab shown on the previous page. On the screen below, note that even though public DNS servers were used in the reference configuration, for security reasons the public IP addresses of the **Primary** and **Secondary** DNS servers have been masked, and private IP addresses are shown. The **DNS client IP**, also masked, corresponds to the **B1** interface used for SIP trunking. Click **Finish** when done.

Edit Device: Avaya_SBCE	
Address and interface changes must be made in Network Management.	
General Settings	
Appliance Name	Avaya_SBCE
Device Settings	
High Availability (HA)	<input type="checkbox"/>
DNS Settings	
Primary Ex: 202.201.192.1	172.16.216.122
Secondary Optional, Ex: 202.201.192.1	10.10.153.242
DNS Client IP	172.16.157.148
Finish	

7.3. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all UC-Sec appliances.

7.3.1. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server). In the reference configuration, Session Manager functions as the Call Server and the Broadvox SIP Proxy as the Trunk Server.

To configure the interworking profile in the enterprise direction, select **Global Profiles** → **Server Interworking** on the left navigation pane. Click **Add**.

Interworking Profiles: cs2100

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General | Timers | URI Manipulation | Header Manipulation | Advanced

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No

Enter a descriptive name for the new profile. Click **Next**.

Interworking Profile X

Profile Name

Next

On the **General** screen, check the **T.38 Support** box. All other parameters retain their default values. Click **Next**.

Interworking Profile

X

General

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

BackNext

Click **Next** on the **Privacy/DTMF** and **SIP Timers/Transport Timers** tabs (not shown). On the **Advanced Settings** tab, uncheck the **Topology Hiding: Change Call-ID** box and check the **AVAYA Extensions** box. Click **Finish** to save and exit.

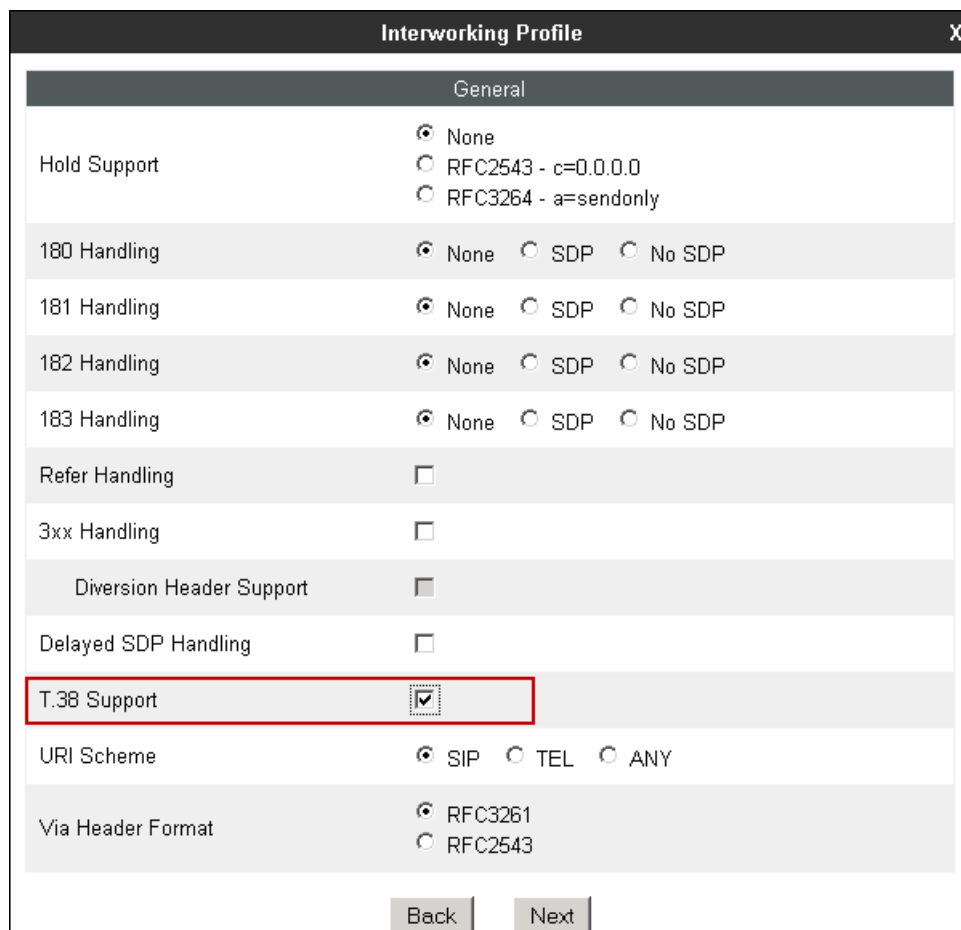
Interworking Profile	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input checked="" type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

A second interworking profile named ***Service Provider*** in the direction of the SIP trunk to Broadvox was similarly created. For this profile default values were used for all parameters except for **T.38 Support**, which was enabled.



The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Service Provider". Below the input field is a "Next" button.

General tab:



The screenshot shows the "Interworking Profile" dialog box with the "General" tab selected. The dialog contains several configuration options:

- Hold Support:** Radio buttons for None (selected), RFC2543 - c=0.0.0.0, and RFC3264 - a=sendonly.
- 180 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 181 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 182 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 183 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- Refer Handling:** A checkbox that is unchecked.
- 3xx Handling:** A checkbox that is unchecked.
- Diversion Header Support:** A checkbox that is unchecked.
- Delayed SDP Handling:** A checkbox that is unchecked.
- T.38 Support:** A checkbox that is checked, highlighted with a red box.
- URI Scheme:** Radio buttons for SIP (selected), TEL, and ANY.
- Via Header Format:** Radio buttons for RFC3261 (selected) and RFC2543.

At the bottom of the dialog are "Back" and "Next" buttons.

Advanced Settings tab:

Interworking Profile

X

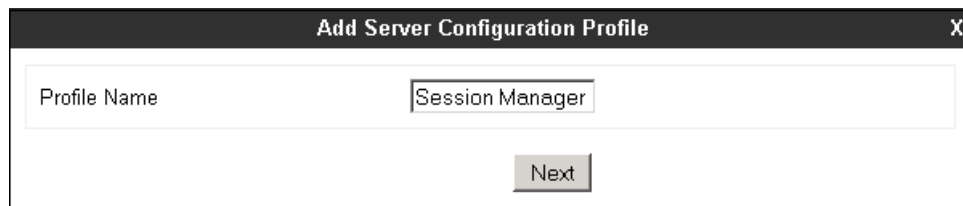
Record Routes	<div><input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides</div>
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Back

Finish

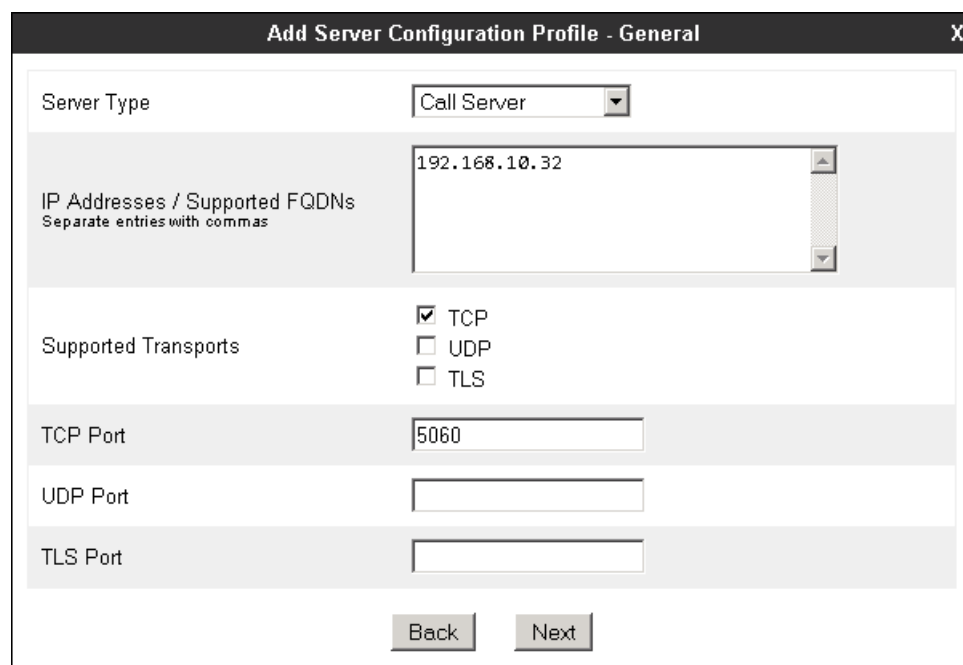
7.3.2. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE two peers, i.e., Session Manager (Call Server) and the SIP Proxy at the service provider's network (Trunk Server). From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server. Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



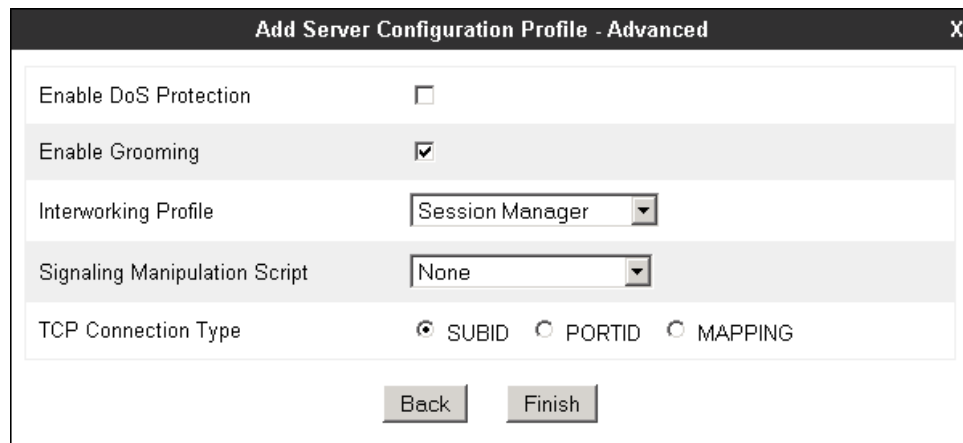
The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "Session Manager". Below this field is a "Next" button.

On the **Add Server Configuration Profile - General** Tab select **Call Server** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter the IP address of the Session Manager Security Module. Select **TCP** for **Supported Transports**, and enter **5060** under **TCP Port**. The transport protocol and port selected here must match the values defined for the Session Manager SIP entity in **Section 6.4**. Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and a list of supported transports. The "Server Type" dropdown is set to "Call Server". The "IP Addresses / Supported FQDNs" field, which has a sub-label "Separate entries with commas", contains the IP address "192.168.10.32". Under "Supported Transports", the "TCP" checkbox is checked, while "UDP" and "TLS" are unchecked. The "TCP Port" field contains the value "5060". The "UDP Port" and "TLS Port" fields are empty. At the bottom of the dialog are "Back" and "Next" buttons.

Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, since TCP is used, check the **Enable Grooming** box. Select *Session Manager* from the **Interworking Profile** drop down menu. Click **Finish**.

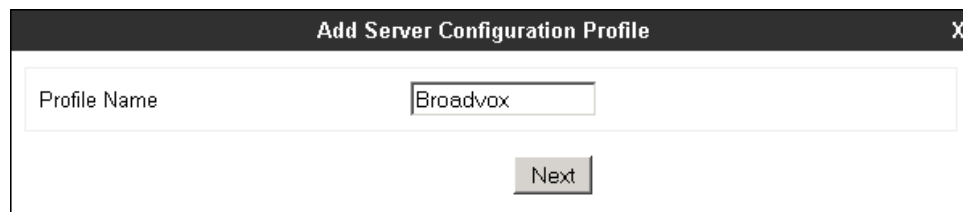


The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The dialog contains several configuration options:

- Enable DoS Protection**: A checkbox that is currently unchecked.
- Enable Grooming**: A checkbox that is checked.
- Interworking Profile**: A dropdown menu with "Session Manager" selected.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- TCP Connection Type**: Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". "SUBID" is selected.

At the bottom of the dialog, there are two buttons: "Back" and "Finish".

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown). Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. The dialog contains a single text input field labeled "Profile Name" with the text "Broadvox" entered. Below the input field is a "Next" button.

On the **Add Server Configuration Profile-General** Tab select **Trunk Server** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter **dl01-01.fs.broadvox.net**, the fully qualified domain name of the Broadvox SIP proxy server. Select **UDP** for **Supported Transports**, and enter **5060** under **UDP Port**, as specified by Broadvox.

Add Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs
Separate entries with commas: dl01-01.fs.broadvox.net

Supported Transports:
☐ TCP
☒ UDP
☐ TLS

TCP Port:

UDP Port: 5060

TLS Port:

Back Next

On the **Authentication** tab, check the **Enable Authentication** box. Enter the **User Name**, and **Password** credential information supplied by Broadvox for the authentication of the SIP trunk. Leave the **Realm** field blank. Click **Next**.

Add Server Configuration Profile - Authentication

Enable Authentication: ☒

User Name: 7325551234

Realm
(Leave blank to detect from server challenge):

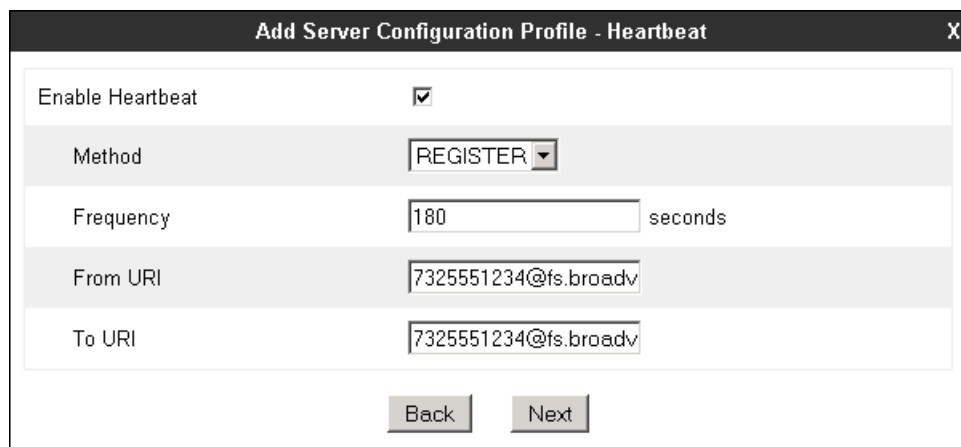
Password:

Confirm Password:

Back Next

On the **Heartbeat** tab:

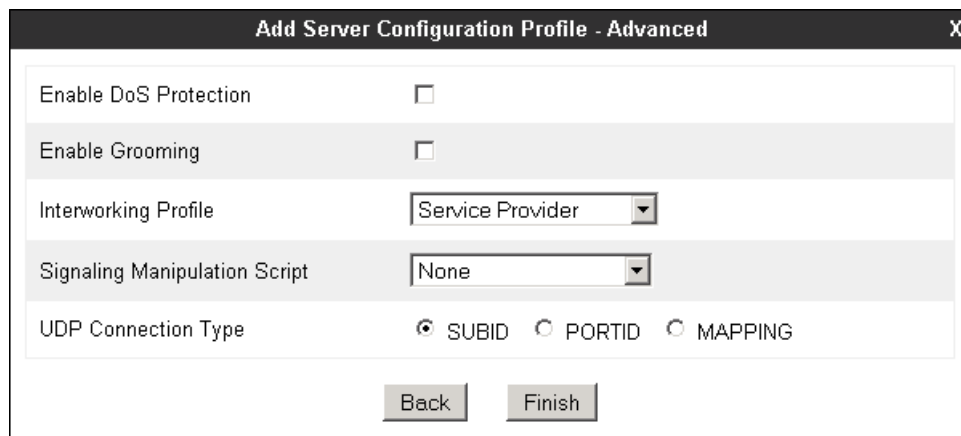
- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Broadvox proxy server in order to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **180** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the **User Name** entered in the **Authentication** screen, and the service's provider domain **fs.broadvox.net**, like shown on the example below.
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Heartbeat" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Enable Heartbeat**: A checkbox that is checked.
- Method**: A dropdown menu with "REGISTER" selected.
- Frequency**: A text input field containing "180" followed by the label "seconds".
- From URI**: A text input field containing "7325551234@fs.broadv".
- To URI**: A text input field containing "7325551234@fs.broadv".
- At the bottom, there are two buttons: "Back" and "Next".

On the **Advanced** tab, select **Service Provider** from the **Interworking Profile** drop down menu.
Click **Finish**



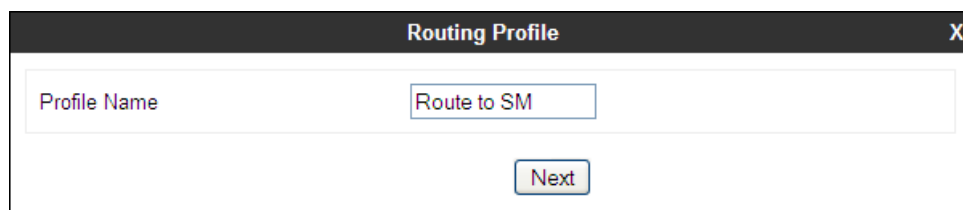
The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Enable DoS Protection**: A checkbox that is unchecked.
- Enable Grooming**: A checkbox that is unchecked.
- Interworking Profile**: A dropdown menu with "Service Provider" selected.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- UDP Connection Type**: Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". The "SUBID" radio button is selected.
- At the bottom, there are two buttons: "Back" and "Finish".

7.3.3. Routing Profiles

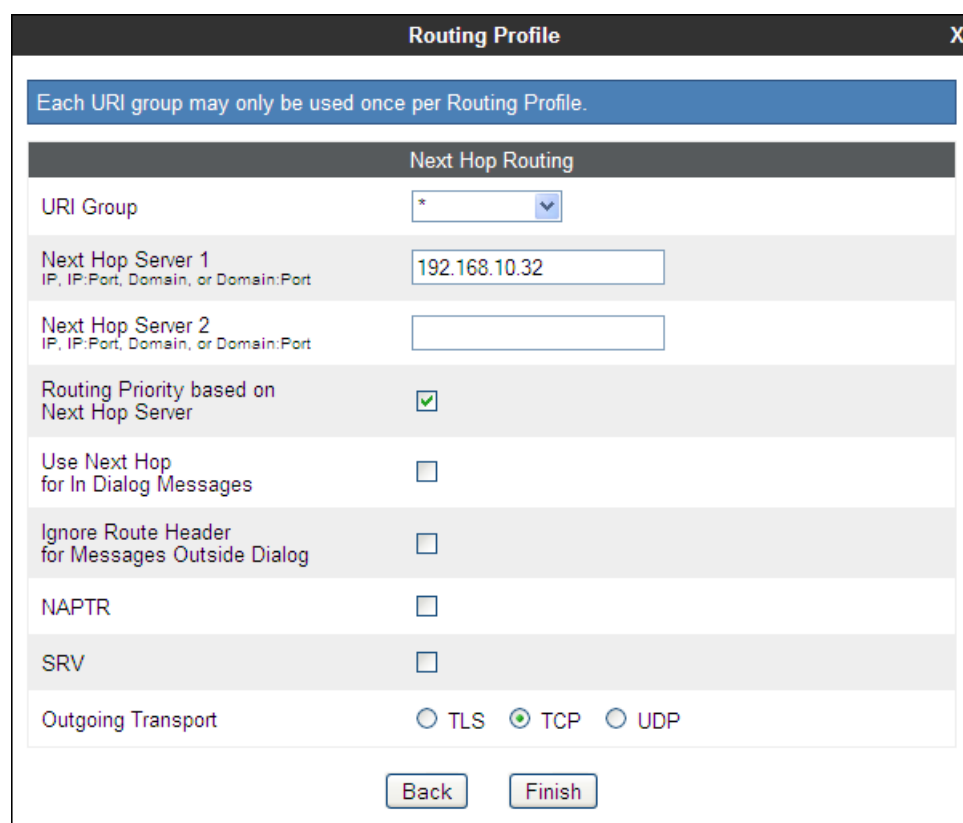
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces.

Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the Broadvox SIP trunk. To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown). Enter an appropriate **Profile Name** similar to the example below. Click **Next**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Route to SM". Below this field is a button labeled "Next".

On the **Next Hop Routing** tab, enter the IP Address of Session Manager as **Next Hop Server 1**. Since the default well-known port value of 5060 for TCP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **TCP** for **Outgoing Transport**. Click **Finish**.

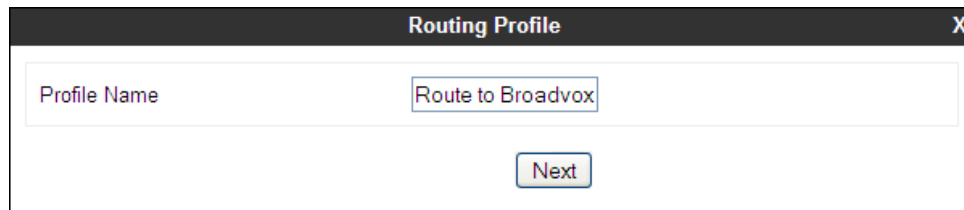


The screenshot shows the "Routing Profile" window with the "Next Hop Routing" tab selected. At the top, a blue banner reads "Each URI group may only be used once per Routing Profile." Below this, the "Next Hop Routing" section contains the following fields and options:

- URI Group:** A dropdown menu with an asterisk (*) selected.
- Next Hop Server 1:** A text input field containing "192.168.10.32". Below the field is the label "IP, IP:Port, Domain, or Domain:Port".
- Next Hop Server 2:** An empty text input field. Below the field is the label "IP, IP:Port, Domain, or Domain:Port".
- Routing Priority based on Next Hop Server:** A checkbox that is checked.
- Use Next Hop for In Dialog Messages:** An unchecked checkbox.
- Ignore Route Header for Messages Outside Dialog:** An unchecked checkbox.
- NAPTR:** An unchecked checkbox.
- SRV:** An unchecked checkbox.
- Outgoing Transport:** Three radio buttons: "TLS" (unchecked), "TCP" (checked), and "UDP" (unchecked).

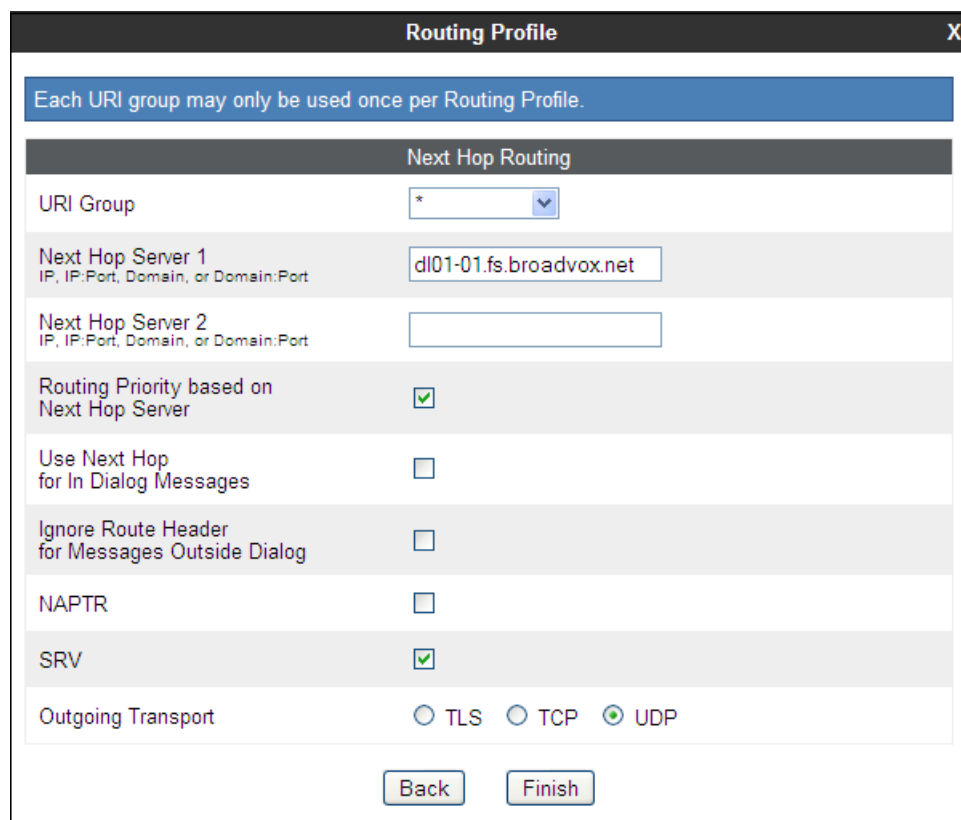
At the bottom of the window are two buttons: "Back" and "Finish".

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route. Enter an appropriate **Profile Name**. Click **Next**.



The image shows a 'Routing Profile' dialog box. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text input field labeled 'Profile Name' containing the text 'Route to Broadvox'. Below the input field is a 'Next' button.

On the Next Hop Routing tab, enter the FQDN of the service provider SIP proxy server as **Next Hop Server 1**. Since the default well-known port value of 5060 for UDP was used, it is not necessary to enter the port number here. Check the **Routing Priority based on Next Hop Server**. Check the **SRV** box. Choose **UDP** for **Outgoing Transport**. Click **Finish**.



The image shows the 'Routing Profile' dialog box with the 'Next Hop Routing' tab selected. At the top, a blue banner reads 'Each URI group may only be used once per Routing Profile.' Below this is a table-like structure with the following fields:

Next Hop Routing	
URI Group	* (dropdown)
Next Hop Server 1 <small>IP, IP:Port, Domain, or Domain:Port</small>	dl01-01.fs.broadvox.net
Next Hop Server 2 <small>IP, IP:Port, Domain, or Domain:Port</small>	
Routing Priority based on Next Hop Server	<input checked="" type="checkbox"/>
Use Next Hop for In Dialog Messages	<input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog	<input type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input checked="" type="checkbox"/>
Outgoing Transport	<input type="radio"/> TLS <input type="radio"/> TCP <input checked="" type="radio"/> UDP

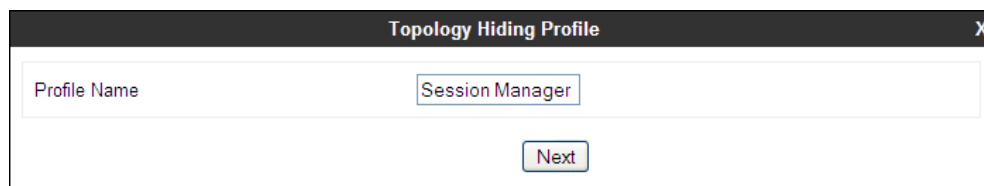
At the bottom of the dialog are 'Back' and 'Finish' buttons.

7.3.4. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

To add the **Topology Hiding Profile** in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side and click the **Add** button (not shown). Enter a **Profile Name** such as the one shown below. Click **Next**.



On the **Topology Hiding Profile** screen, click the **Add Header** button repeatedly to show the rest of the headers in the profile.



Header	Criteria	Replace Action	Overwrite Value
RequestLine	IP/Domain	Auto	

For the **Request-Line**, **From** and **To** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain known by the Session Manager, *sil.miami.avaya.com*, in the **Overwrite Value** column of these headers, as shown below. Default values were used for all other fields. Click **Finish**.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	sil.miami.avaya.com
From	IP/Domain	Overwrite	sil.miami.avaya.com
To	IP/Domain	Overwrite	sil.miami.avaya.com
Record-Route	IP/Domain	Auto	
Via	IP/Domain	Auto	
SDP	IP/Domain	Auto	

A Topology Hiding profile named **Service Provider** was similarly configured in the direction of the SIP trunk to Broadvox. During the compliance tests, IP addresses were used in the domain part of headers in messages between the Broadvox SIP Proxy and the Avaya SBCE. For the **Request-Line** and **To** headers, **Destination IP** was selected under the **Replace Action** column.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Destination IP	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Destination IP	---
SDP	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

7.4. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, only a new Signaling Rule was defined. All other rules under Domain Policies, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

7.4.1. Signaling Rules

A Signaling Rule was created in the sample configuration to remove (block) the following headers:

- AV-Global-Session-ID
- Alert-Info
- Endpoint-View
- P-AV-Message-ID
- P-Location
- P-Charging-Vector

These headers are sent in SIP messages from the Session Manager to the Avaya SBCE. They contain private IP addresses and SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries.

In the **Domain Policies** menu on the left-hand side, select **Signaling Rules**, then **Add Rule** (not shown). Enter an appropriate name like in the example below. Click **Next**.



On the next three pages (not shown), leave sections **Inbound**, **Outbound** and **Content-Type Policies** with their default values. Click **Next**. On the **Signaling QoS** tab, default values were used. Click **Finish**.

On the newly created **Remove_headers** Signaling Rule, select the **Request Headers** tab to create the manipulations performed on request messages. Select **Add In Header Control**.

The screenshot shows the 'Signaling Rules' configuration page. In the left sidebar, the 'Remove_headers' rule is selected. The main area has tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'Request Headers' tab is active, and the 'Add In Header Control' button is highlighted. Below the tabs is a table with columns: Row, Header Name, Method Name, Header Criteria, Action, Proprietary, and Direction. The table is empty, with a message 'No request header controls exist.' at the bottom.

In the **Add Header Control** screen select the following:

- **Header Name: Alert-Info**
- **Method Name: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

The screenshot shows the 'Add Header Control' dialog box. It contains the following fields and options:

- Proprietary Request Header:** ☐
- Header Name:** Alert-Info (dropdown)
- Method Name:** INVITE (dropdown)
- Header Criteria:**
 - ☒ Forbidden
 - ☐ Mandatory
 - ☐ Optional
- Presence Action:** Remove header (dropdown)
- 486:** Busy Here (text input)
- Finish:** (button)

Select **Add In Header Control** as needed to configure the remaining header control rules. For these headers, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Request Headers** tab should look like the following screen.

General Requests Responses Request Headers Response Headers Signaling QoS							
				Add In Header Control		Add Out Header Control	
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
4	P-AV-Message-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
5	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
6	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete

Select the **Response Headers** tab to similarly create the manipulations performed on response messages. Select **Add In Header Control** (not shown).

The screen below shows the settings for the Alert-Info header on response messages.

Add Header Control
X

Proprietary Response Header
☐

Header Name
Alert-Info

Response Code
200

Method Name
INVITE

Header Criteria
☒ Forbidden
☐ Mandatory
☐ Optional

Presence Action
Remove header

486
Busy Here

Finish

Select **Add In Header Control** as needed to configure the remaining header control rules. For these headers, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Response Headers** tab should look like the following screen.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS				
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
4	Endpoint-View	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Charging-Vector	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	P-Location	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.4.2. End Point Policy Groups

End Point Policy Groups associate the different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu. Select **Add** (not shown).

Enter an appropriate name in the **Group Name** field. *Enterprise* was used. Click **Next**.

Policy Group

X

Group Name

Enterprise

Next

In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, with the exception of the **Signaling Rule**, where the *Remove_headers* rule created in **Section 7.4.1** was selected. Click **Finish**.

Policy Group

X

Application Rule	default-trunk
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Remove_headers
Time of Day Rule	default

Back

Finish

The screen below shows the **Enterprise** End Point Policy Group after the configuration was completed.

Policy Group								Summary		Add	
Order	Application	Border	Media	Security	Signaling	Time of Day					
1	default-trunk	default	default-low-med	default-low	Remove_headers	default		Edit	Clone		

A second End Point Policy Group was created for the service provider, repeating the steps described above. Defaults were used in this case for all fields. The screen below shows the **Service Provider** End Point Policy Group after the configuration was completed.

Policy Group

Summary Add

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	default-trunk	default	default-low-med	default-low	default	default	Edit Clone

7.5. Device Specific Settings

The **Device Specific Settings** determine server specific parameters that determine how the device will work when deployed on the network. Among the parameters defined here are IP addresses, media and signaling interfaces, call flows, etc.

7.5.1. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be made here.

Select **Network Management** from **Device Specific Settings** on the left-side menu (not shown). Under **Devices** in the center pane, select the device being managed, **Avaya_SBCE** in the sample configuration. On the **Network Configuration** tab, verify or enter the network information as needed. Note that the **A1** interface is used for the internal side and **B1** is used for the external side of the Avaya SBCE.

Network Management: Avaya_SBCE

Devices

Avaya_SBCE

Network Configuration Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.0 B2 Netmask

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.5.5.72		10.5.5.254	A1	Delete
172.16.157.148		172.16.157.129	B1	Delete

On the **Interface Configuration** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. Click the **Toggle** buttons if necessary to enable the interfaces.

Devices	Network Configuration	Interface Configuration
Avaya_SBCE		
Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

7.5.2. Media Interface

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address and one of the ports in this range as the listening IP address and port in which it will accept media from the Call or Trunk Server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.

Add Media Interface
X

Name	Private_med
IP Address	10.5.5.72
Port Range	35000 - 40000

Finish

A second Media Interface facing the public network side was similarly created with the name **Public_med**, as shown below. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. The **Port Range** was left at the default values.

Add Media Interface
X

Name	Public_med
IP Address	172.16.157.148
Port Range	35000 - 40000

Finish

Once the configuration is complete, the **Media Interface** screen will appear as follows.

Media Interface: Avaya_SBCE

Devices

Avaya_SBCE

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP	Port Range	
Private_med	10.5.5.72	35000 - 40000	Edit Delete
Public_med	172.16.157.148	35000 - 40000	Edit Delete

7.5.3. Signaling Interface

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in both the inside and outside networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. Enter **5060** for **TCP Port**, since TCP port 5060 is used to listen to signaling traffic from Session Manager in the sample configuration. Click **Finish**.

Add Signaling Interface

Name: Private_sig

IP Address: 10.5.5.72

TCP Port: 5060
Leave blank to disable

UDP Port:
Leave blank to disable

Enable Stun: ☐

TLS Port:
Leave blank to disable

TLS Profile: AvayaSBCServer

Enable Shared Control: ☐

Shared Control Port:

Finish

A second Signaling Interface with the name **Public_sig** was similarly created in the network direction. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. **UDP Port 5060** was selected since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.

Add Signaling Interface
X

Name

IP Address

172.16.157.148 ▼

TCP Port
Leave blank to disable

UDP Port
Leave blank to disable

Enable Stun
☐

TLS Port
Leave blank to disable

TLS Profile

AvayaSBCEServer ▼

Enable Shared Control
☐

Shared Control Port

Finish

Once the configuration is complete, the **Signaling Interface** screen will appear as follows:

Devices

Avaya_SBCE

Signaling Interface

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	10.5.5.72	5060	---	---	None	<a>Edit <a>Delete
Public_sig	172.16.157.148	---	5060	---	None	<a>Edit <a>Delete

7.5.4. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named *Session Manager Flow* created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.

Edit Flow: Session Manager Flow	
Flow Name	Session Manager Flow
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
End Point Policy Group	Enterprise
Routing Profile	Route to Broadvox
Topology Hiding Profile	Session Manager
File Transfer Profile	None
Finish	

A second Server Flow with the name ***SIP Trunk Flow*** was similarly created in the network direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.

Edit Flow: SIP Trunk Flow
X

Flow Name	<input type="text" value="SIP Trunk Flow"/>
Server Configuration	<input type="text" value="Broadvox"/>
URI Group	<input type="text" value="*"/>
Transport	<input type="text" value="*"/>
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="Private_sig"/>
Signaling Interface	<input type="text" value="Public_sig"/>
Media Interface	<input type="text" value="Public_med"/>
End Point Policy Group	<input type="text" value="Service Provider"/>
Routing Profile	<input type="text" value="Route to SM"/>
Topology Hiding Profile	<input type="text" value="Service Provider"/>
File Transfer Profile	<input type="text" value="None"/>

The two Server Flows created in the sample configuration are summarized on the screen below:

Devices

Avaya_SBCE

Subscriber Flows

Server Flows

Click here to add a row description.

Server Configuration: Broadvox

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SIP Trunk Flow	*	Private_sig	Public_sig	Service Provider	Route to SM	View Clone Edit Delete

Server Configuration: Session Manager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Session Manager Flow	*	Public_sig	Private_sig	Enterprise	Route to Broadvox	View Clone Edit Delete

8. Broadvox SIP Trunking Service Configuration

Broadvox is responsible for the configuration of the Broadvox SIP Trunking service on its network. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Broadvox will provide the customer the necessary information to configure the SIP connection from the enterprise site to the Broadvox network, including:

- Credentials for SIP trunk registration (username and password).
- Fully qualified domain name of the Broadvox SIP Proxy server.
- Supported codecs and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

This information is used to complete the configuration of Communication Manager, Session Manager and the Avaya SBCE discussed in the previous sections.

9. Verification and Troubleshooting

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

9.1. General Verification Steps

- 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.
- 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.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.2. Communication Manager Verification

The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- **list trace station** <extension number>
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
Displays signaling group service state.
- **status trunk** <trunk group number>
Displays trunk group service state.

- **status station** <extension number>
Displays signaling and media information for an active call on a specific station.

9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Verify that the state of the Session Manager links under the **Conn. Status** and **Link Status** columns to Communication Manager and the Avaya SBCE is **UP**, like shown on the screen below.

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: MA_Session Manager

Status Details for the selected Session Manager:

Summary View

10 Items Refresh Filter: Disable, Apply, Clear

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	MA C.M. Trunk 2	192.168.10.12	5070	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	AA-Messaging	192.168.10.92	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	MA C.M. Trunk 1	192.168.10.12	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	MA SBCE	10.5.5.72	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	MA AA-SBC	192.168.10.42	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	MA C.M.Trunk 10	192.168.10.12	5080	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	MA CM Trunk 98	192.168.10.12	5062	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	MA CM Trunk 4	192.168.10.12	5075	TCP	FALSE	UP	200 OK	UP

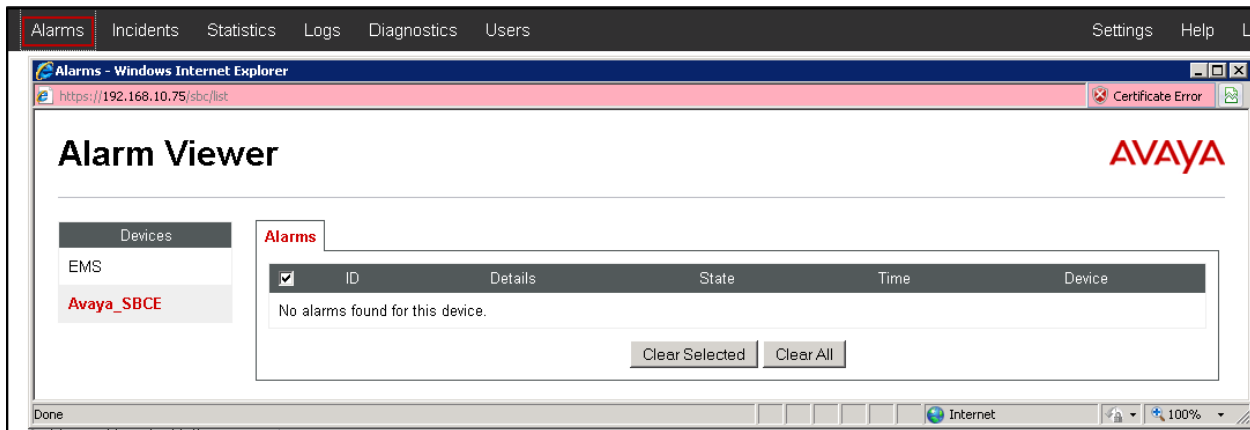
Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** – The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test

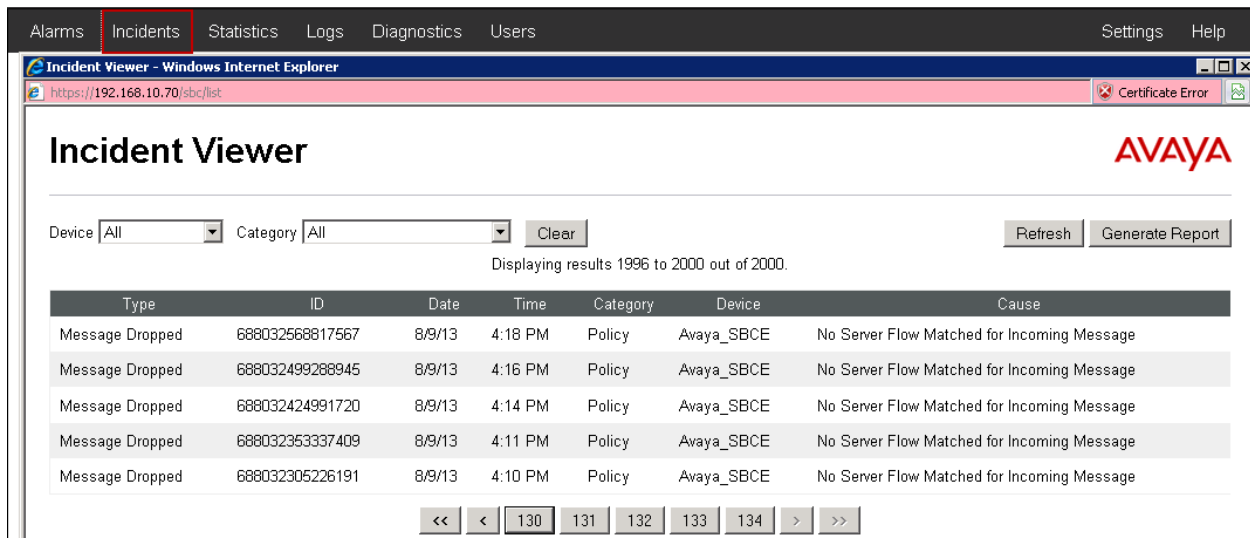
9.4. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

Alarms: Provides information about the health of the SBC.



Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.



Diagnostics: This screen provides a variety of tools to test and troubleshoot the SBC network connectivity.

Diagnostics AVAYA

Devices
Avaya_SBCE

Full Diagnostic Ping Test Application Protocol

Start Diagnostic

Task Description	Status
EMS Link Check	
SDC Link Check: A1	
SDC Link Check: D1	
Ping: SBC (10.5.5.72) to Ping: Gateway (10.5.5.254)	
Ping: SBC (10.5.5.72) to Ping: Primary DNS (172.16.216.122)	
Ping: SBC (10.5.5.72) to Ping: Secondary DNS (172.16.153.242)	
Ping: SBC (172.16.167.148) to Ping: Gateway (172.16.167.129)	

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

Session Border Controller for Enterprise AVAYA

Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options
Troubleshooting
Debugging
Trace
DoS

Trace: Avaya_SBCE

Devices
Avaya_SBCE

Call Trace Packet Capture Captures

Packet Capture Configuration

Status Ready

Interface Any

Local Address All

Remote Address *, *:Port, IP, IP:Port

Protocol All

Maximum Number of Packets to Capture 10000

Capture Filename test1.pcap
Using the name of an existing capture will overwrite it.

Start Capture Clear

Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

Call Trace

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified
test1_20130830102339.pcap	393,216	August 30, 2013 10:24:04 AM GMT Delete

10. Conclusion

These Application Notes describe the procedures required to configure an Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2, to connect to the Broadvox SIP Trunking service, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the exception of the observations/limitations described in **Section 2.2**.

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 6.3, May 2013.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2013.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.3, May 2013, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, May 2013, Document Number 555-245-205.
- [5] *Administering Avaya Aura® Session Manager*, Release 6.3, June 2013.
- [6] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013
- [7] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, May 2013
- [8] *Avaya Session Border Controller for Enterprise Release Notes*. Release 6.2, June 2013
- [9] *Administering Avaya one-X® Communicator*, December 2012.
- [10] *Using Avaya one-X® Communicator, Release 6.1*, October 2011.
- [11] *Implementing Avaya Flare® Experience for Windows*. Release 1.1 February 2013.
- [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/>

©2013 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.