



Application Notes for Configuring Broadconnect SIP trunking service with Avaya Aura® Communication Manager Evolution Server Release 6.0.1, Avaya Aura® Session Manager Release 6.1, and Avaya Session Border Controller for Enterprise Release 4.0.5 - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the Broadconnect SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, Avaya Session Border Controller for Enterprise 4.0.5, and various Avaya endpoints. During the interoperability testing, Avaya Communication Manager was able to interoperate with the Broadconnect via SIP trunk. This test was performed to verify SIP trunk features including basic call, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls are placed in both directions with various set types.

This documented solution does not extend to configurations without the Avaya Session Border Controller for Enterprise or Avaya Aura® Session Manager.

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.....	5
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results.....	6
2.2.1.	Network Call Redirection.....	6
2.2.2.	Calling number/ID display.....	6
2.2.3.	Call Display Update.....	6
2.2.4.	Call Termination.....	6
2.3.	Support.....	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated.....	10
5.	Configure Communication Manager.....	10
5.1.	Licensing and Capacity.....	11
5.2.	System Features.....	11
5.3.	IP Node Names.....	13
5.4.	Codecs.....	13
5.5.	IP Network Region.....	14
5.6.	Signaling Group.....	16
5.7.	Trunk Group.....	19
5.8.	Calling Party Information.....	22
5.9.	Outbound Routing.....	23
5.10.	Saving Communication Manager Configuration Changes.....	25
6.	Administer Avaya Aura® Session Manager.....	26
6.1.	Create a SIP domain name.....	26
6.2.	Create a Location.....	28
6.3.	Create SIP Entity for Avaya Aura® Session Manager.....	29
6.4.	Create SIP Entity for Avaya Aura® Communication Manager SIP Gateway.....	31
6.5.	Create SIP Entity for Avaya Session Border Controller for Enterprise.....	32
6.6.	Create Adaptation Module.....	33
6.7.	Create Routing Policy for inbound call.....	36
6.8.	Create Routing Policy for outbound call.....	37
6.9.	Create Dial Pattern for inbound call.....	37
6.10.	Create Dial Pattern for outbound call.....	39
7.	Configure Avaya Session Border Controller for Enterprise.....	43
7.1.	Avaya Session Border Controller For Enterprise Login.....	44
7.2.	Global Profiles.....	46
7.2.1.	Uniform Resource Identifier (URI) Groups.....	46
7.2.2.	Routing Profiles.....	47
7.2.3.	Topology Hiding.....	50
7.2.4.	Server Interworking.....	51
7.2.5.	Signaling Manipulation.....	55
7.2.6.	Server Configuration.....	59
7.3.	Domain Policies.....	64

7.3.1.	Application Rules	64
7.3.2.	Media Rules.....	65
7.3.3.	Signaling Rules	68
7.3.4.	Endpoint Policy Groups	70
7.3.5.	Session Policy	71
7.4.	Device Specific Settings	74
7.4.1.	Network Management	74
7.4.2.	Media Interface	75
7.4.3.	Signaling Interface	76
7.4.4.	End Point Flows - Server Flow	76
7.4.5.	Session Flow	79
8.	Configure Broadconnect SIP Trunking.....	80
9.	Verification Steps	81
10.	Conclusion	83
11.	Additional References	84

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Broadconnect SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager 6.0.1 configured as an Evolution Server, Avaya SBC for Enterprise (Avaya SBCE) 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Session Manager or Avaya SBCE.

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

The Broadconnect SIP Trunking service uses Digest Authentication for outbound calls from the enterprise, using challenge-response authentication for each call to the Broadconnect network based on a configured user name and password (provided by Broadconnect and configured on Avaya SBCE). This call authentication scheme as specified in SIP RFC 3261 provides security and integrity protection for SIP signaling.

The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in

Figure 3.1. For confidentiality purposes, the IP addresses in these Application notes have been modified to show 111.x.x.x for Avaya internal addresses, 222.x.x.x for Avaya external address and 333.x.x.x for Broadconnect external address. Broadconnect customers will use their own FQDNs and IP addresses as required.

2. General Test Approach and Test Results

Broadconnect is a member of the Avaya DevConnect Service Provider program. 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

A simulated enterprise site comprised of Communication Manager, Session Manager and the Avaya SBCE was connected to the public Internet using a broadband connection. The enterprise site was configured to connect to the Broadconnect SIP Trunking service Vendor Validation circuit through the public Internet.

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

- Incoming PSTN calls to various phone types.
- Phone types included H.323, digital and analog telephones at the enterprise. All inbound calls from 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, digital and analog telephones at the enterprise. All outbound calls to 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 (1XC) soft phones.
- Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) were tested. 1XC was tested using SIP and H.323 protocols.
- Various call types included: local, long distance, international, outbound toll-free, operator assisted calls and local directory assistance (411).
- G.729A Codec and G.711MU Codec and proper codec negotiation.
- DTMF tone transmissions passed as out-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Network Call Redirection using SIP INVITE for transfer of inbound call back to PSTN.
- Incoming and Outgoing fax over IP with codec G.711.

- EC500 mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection using reINVITE for transfer of inbound call back to PSTN.
- Session Timers implementation from both ends of enterprise and service provider.

Items not supported or not tested included the following:

- Inbound toll-free and outbound emergency calls (911) are supported but were not tested as part of the compliance test.
- Network Call Redirection using SIP REFER that contains UUI (User-To-User Information).

2.2. Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager, Session Manager and Avaya SBCE to connect to the Broadconnect SIP Trunking service. This configuration (shown in **Figure 3.1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

2.2.1. Network Call Redirection

In order for the blind transfer off-net call scenarios to function properly the CM must be setup to use reINVITE method and NOT the REFER method. The Network Call Redirection setting on the trunk as shown in **Section Error! Reference source not found.** should be turned OFF. This will ensure the reINVITE method for blind transfers is used and calls function properly.

2.2.2. Calling number/ID display

PSTN phone may display both calling party id/name and calling party number or just calling party number and no calling party id/name on outbound calls from the enterprise to the PSTN through Broadconnect, depending on the specific service provider the call routes through from Broadconnect to the endpoint.

2.2.3. Call Display Update

Call display was not properly updated on PSTN phone to reflect the true connected party on calls that are transferred to the PSTN from the enterprise. After the call transfer was completed, the PSTN phone showed the party that initiated the transfer instead of the actual connected party.

2.2.4. Call Termination

In certain call scenarios involving call forward, the BYE from the PSTN network is not passed by the Avaya SBCE to the next hop which is the Session Manager, resulting in a failure to properly terminate the call. The problem was addressed in this compliance test with the

application of a patch to the Avaya SBCE software version 4.0.5.Q02. Software versions later than 4.0.5.Q.02 will include this fix.

2.3. Support

For technical support on Broadconnect system, please contact Broadconnect technical support at:

- Toll Free: 1 866 228 6616
- <http://support.broadconnect.ca/>

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

3. Reference Configuration

Error! Reference source not found.

Figure 3.1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the Broadconnect SIP Trunking service (Vendor Validation circuit) through a public Internet WAN connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are masked in these Application Notes.

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

- Avaya S8300 Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya S8800 Servers running Messaging
- Avaya Session Border Controller for Enterprise
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Broadconnect 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.

Two separate SIP trunk groups were created between Communication Manager and Session Manager to carry traffic to and from the service provider respectively. Any specific trunk or codec settings required by the service provider were applied only to these dedicated trunks so as not to affect other enterprise SIP traffic.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE then to Session Manager. Session Manager used the routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions could be performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager.

The Session Manager once again used the routing policies to determine the route to the Avaya SBCE for egress to the Broadconnect network.

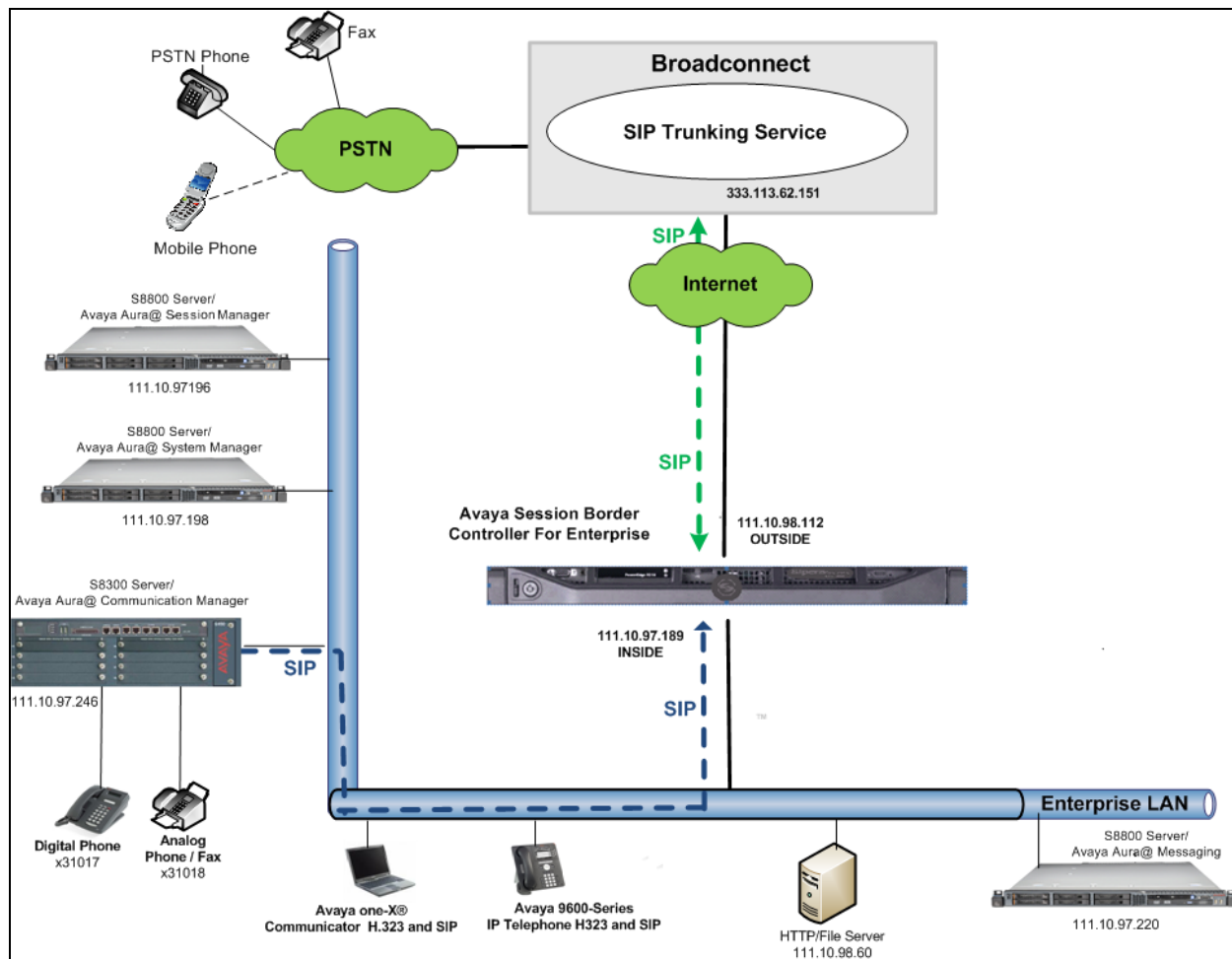


Figure 3.1 Network Diagram for Avaya CM – Broadconnect System

For efficiency, the Avaya CPE environment utilizing Session Manager Release 6.1 and Communication Manager Release 6.0.1 was shared among various ongoing test efforts at the Avaya test lab. Access to the Broadconnect network was added to a configuration that already used enterprise domain “avaya.com”. As such, Session Manager was used to adapt the “avaya.com” domain to the domain known to Broadconnect. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to the Broadconnect network.

4. Equipment and Software Validated

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

Avaya system:

Equipment	Software
Avaya G450 Media Gateway	31.20.1
Avaya S8300 Server running Avaya Aura [®] Communication Manager	Avaya Aura [®] Communication Manager R6.0.1 Build: R016x.00.1.510.1 Patch: 00.1.510.1-19350
Avaya S8800 Server	Avaya Aura [®] System Manager R6.1.0 6.1.0.0.7345-6.1.5.606
Avaya S8800 Server	Avaya Aura [®] Session Manager R6.1 6.1.6.0.616008
Dell R210 Server	Avaya Aura [®] Session Boarder Controller for Enterprise 4.0.5 Q2
Avaya one-X Communicator (H.323 and SIP)	6.1.2.01-SP2-33739
Avaya 9620 IP Telephone (H.323)	Avaya one-X [®] Deskphone Edition 3.1 S3.102S
Avaya 9404 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a

Broadconnect system:

System	Software
Broadsoft BroadWorks	R17.0
Acme Packet SBC	Net-Net 4250 R5.1.1 Patch 28 (Build 629)

5. Configure Communication Manager

This section describes the procedure for configuring Communication Manager for inter-operating with the Broadconnect SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to the enterprise from Broadconnect (for inbound calls to the enterprise from the PSTN); similarly a separate SIP trunk is created for carrying signaling traffic to the network from the enterprise (for outbound calls to the PSTN from the enterprise).

It is assumed the general installation of the Communication Manager and the Avaya G450 Media Gateway has been previously completed.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged for brevity and clarity in presentation.

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 **96** 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 0
      Maximum Concurrently Registered IP Stations: 18000 5
      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: 18000 2
      Maximum Video Capable IP Softphones: 18000 3
      Maximum Administered SIP Trunks: 24000 96
      Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 522 0
      Maximum TN2501 VAL Boards: 128 1
      Maximum Media Gateway VAL Sources: 250 0
      Maximum TN2602 Boards with 80 VoIP Channels: 128 0
      Maximum TN2602 Boards with 320 VoIP Channels: 128 0
      Maximum Number of Expanded Meet-me Conference Ports: 300 0

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

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. The compliance test used the values of **AV-Restricted** for restricted calls and **AV-Unavailable** for unavailable calls.

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

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

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

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

ENBLOC DIALING PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

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

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 the G450 CLAN card hosted by Communication Manager (**procr**) and Session Manager (**DevASM**). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
DevASM	111.10.97.198	
default	0.0.0.0	
procr	111.10.97.246	
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 1 was used for this purpose. Broadconnect SIP Trunking service currently supports G.729 and G.711MU. Enter the codec to be used in priority order in the **Audio Codec** column of the table. Default values can be used for all other fields. The following screen shows the codec set configuration at a certain time of the compliance test. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

change ip-codec-set 1		Page 1 of 2
		IP Codec Set
Codec Set: 1		
Audio Codec	Silence Suppression	Frames Per Pkt Packet Size(ms)
1: G.711MU	n	2 20
2: G.729AB	n	2 20
3:		

On **Page 2**, set the **Fax Mode** to **off**.

change ip-codec-set 1		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? n		
	Mode	Redundancy
FAX	off	0
Modem	off	0
TDD/TTY	off	3
Clear-channel	n	0

5.5. IP Network Region

Create a separate IP network region for the service provider trunk groups. 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 1** was created for the service provider trunks. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.com** 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. Note that Session Manager adaptation configuration (**Section 6.6**) is used to convert this shared domain name to the specific CPE domain as assigned by Broadconnect and expected by the Broadconnect network.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```

change ip-network-region 1                                     Page 1 of 20
                                     IP NETWORK REGION

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

```

On **Page 4**, define the IP codec set to be used for traffic between region 1 and other regions. In this testing, the Communication Manager, G450 Gateway, Session Manager, IP phone and Avaya SBCE were assigned to the same region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 1 will be used for calls between region 1 (the service provider region) and other regions.

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

Non-IP telephones (e.g., analog, digital) derive network region from the Avaya gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes.

For the compliance test, devices with IP addresses in the 111.10.97.0/24 subnet are assigned to network region 1. These include Communication Manager, G450 Gateway, Session Manager and Avaya SBCE that were set up for shared test environment. IP telephones used for the compliance test, including both the Avaya 9600 IP Telephones and the Avaya one-X® Communicator soft phones, are assigned to network region 1 with IP address in the

110.10.98.0/24 subnet. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

change ip-network-map				Page 1 of 63	
IP ADDRESS MAPPING					
IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: 111.10.97.0	/24	3	n		
TO: 111.10.97.255					
FROM: 111.10.98.0	/24	3	n		
TO: 111.10.98.255					
FROM:	/		n		
TO:					

5.6. Signaling Group

Use the **add signaling-group** command to create 2 signaling groups between Communication Manager and the Session Manager for use by inbound calls from the service provider network and outgoing calls from the enterprise. The signaling group used for inbound calls from the service provider is shown below. For the compliance test, signaling group 10 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between the Communication Manager and Session Manager. The transport method used between the Session Manager and Avaya SBCE is specified as TCP in **Section 6.5**. Lastly, the transport method between the Avaya SBCE and Broadconnect is UDP. This is defined in **Section 7.2.6.1** when the service provider name is selected.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so the Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5060** (the well-known port value for TCP is 5060).
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **Session Manager** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of G450 CLAN card IP address as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **DevASM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to blank.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **DTMF over IP** field to **rtp-payload**. This setting enables Communication Manager to send DTMF transmissions using RFC 2833.
- Verify that the **Initial IP-IP Direct Media** is set to the same value of to the signaling group used for the enterprise site. The default setting for this field is **n**. See the **Media Format** bullet item in **Section 2.2** for more information about this setting.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **12**. This allows more time for outbound PSTN calls to complete through the Broadconnect SIP Trunking service.
- Default values may be used for all other fields.

add signaling-group 10		Page 1 of 1
SIGNALING GROUP		
Group Number: 10 Group Type: sip		
IMS Enabled? n Transport Method: tcp		
Q-SIP? n		SIP Enabled LSP? n
IP Video? n		Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM		
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Near-end Node Name: procr Near-end Listen Port: 5060 </div> <div style="width: 45%;"> Far-end Node Name: DevASM Far-end Listen Port: 5060 Far-end Network Region: 1 </div> </div>		
Far-end Domain:		
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? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n
		Alternate Route Timer(sec): 12

The trunk group for outbound calls from the enterprise to the PSTN was similarly configured except that the Far-end Domain is set to “**broadconnect.ca**”, this domain is known to the service provider network domain as provided by Broadconnect. For the compliance test, signaling group 11 was used for this purpose and is shown below:

```
add signaling-group 11                                     Page 1 of 1
                                                         SIGNALING GROUP

Group Number: 11          Group Type: sip
IMS Enabled? n           Transport Method: tcp
    Q-SIP? n
    IP Video? n
Peer Detection Enabled? y Peer Server: SM
                                     SIP Enabled LSP? n
                                     Enforce SIPS URI for SRTP? y

Near-end Node Name: procr          Far-end Node Name: DevASM
Near-end Listen Port: 5060         Far-end Listen Port: 5060
Far-end Network Region: 1

Far-end Domain: broadconnect.ca
Incoming Dialog Loopbacks: eliminate
    DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
    Enable Layer 3 Test? y
H.323 Station Outgoing Direct Media? n
                                     Bypass If IP Threshold Exceeded? n
                                     RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
                                     IP Audio Hairpinning? n
Initial IP-IP Direct Media? n
Alternate Route Timer(sec): 12
```

5.7. Trunk Group

Use the **add trunk-group** command to create trunk group for the 2 signaling groups created in **Section 5.6**. For the compliance test, trunk group 10 was configured for incoming call and trunk group 11 was configured for outgoing calls and trunk group 20 was configured for two-way calling 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 **Direction** field to **incoming** for trunk group 10 and **outgoing** for trunk group 11.
- Set the Outgoing Display to **y** to enable name display on the trunk.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

add trunk-group 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: Broadconnect_PSTN_incomming	COR: 1	TN: 1	TAC: *010
Direction: incoming	Outgoing Display? y	Night Service:	
Dial Access? n			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 10		
	Number of Members: 32		

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

```

add trunk-group 10                                     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

```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with Broadconnect. Thus, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```

add trunk-group 10                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                               Measured: none
                                                    Maintenance Tests? y

    Numbering Format: private
                                                    UI Treatment: service-provider

    Replace Restricted Numbers? y
    Replace Unavailable Numbers? y

  Show ANSWERED BY on Display? y

```

On **Page 4**, the **Network Call Redirection** field can be set to **y**. This setting enables use of the SIP REFER message for incoming call transfer to a vector number. Notes: the outgoing trunk group 11 in the later discussion will have Network Call Redirection is set to n, this setting is to use reINVITE to off-net transfer an incoming call back to PSTN.

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

Set the **Support Request History** field to **n**. This parameter determines whether the SIP History-Info header will be included in the call-redirection INVITE from the enterprise.

Set the **Telephone Event Payload Type** to **101**, the value preferred by Broadconnect. Set the **Convert 180 to 183 for Early Media** field to **y**.

add trunk-group 10	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
 Convert 180 to 183 for Early Media? y	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Enable Q-SIP? n	

Trunk group 11 configuration, the screen below shows **Page 1**, the trunk group for outgoing calls from the enterprise.

add trunk-group 11	Page 1 of 21	
TRUNK GROUP		
Group Number: 11	Group Type: sip	CDR Reports: y
Group Name: Broadconnect_PSTN_outbound	COR: 1	TN: 1 TAC: *011
Direction: outgoing	Outgoing Display? y	
Dial Access? n		
Queue Length: 0		
Service Type: public-ntwrk		
	Member Assignment Method: auto	
	Signaling Group: 11	
	Number of Members: 32	

On **Page 4** of trunk group 11, the **Network Call Redirection** is set to “n”.

Notes: Network Call Redirection is set to “n”, Communication Manager will use reINVITE for off-net call transfer. This setting is used when service providers do not support the REFER method of call redirection.

add trunk-group 11	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? y	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Enable Q-SIP? n	

The configurations on other pages of trunk group 11 are identical to trunk group 10.

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). It is used to authenticate the caller.

Normally DID numbers are comprised of the local extension plus a prefix. A single private numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with 11 or 21 will send the calling party number as the **Private Prefix** plus the extension number.

change private-numbering 0					Page	1 of	2
NUMBERING - PRIVATE FORMAT							
Ext	Ext	Trk	Private	Total			
Len	Code	Grp(s)	Prefix	Len			
4	11	11	905346	10	Total Administered: 9		
4	11	20	555	7	Maximum Entries: 540		
4	21	11	780643	10			
4	21	20	555	7			

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

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
4	11	11	905346	10	Total Administered: 9
4	11	20	555	7	Maximum Entries: 240
4	14	11	604638	10	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.
4	14	20	555	7	
4	21	11	780643	10	
4	21	20	555	7	
4	33	11	514228	10	
4	33	20	555	7	

5.9. Outbound Routing

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

change dialplan analysis									Page 1 of 12
DIAL PLAN ANALYSIS TABLE									
Location: all									Percent Full: 3
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call	
String	Length	Type	String	Length	Type	String	Length	Type	
0	3	fac	#	2	fac				
11	4	ext	#	3	fac				
14	4	ext	8	1	fac				
2	4	ext	9	1	fac				
3	4	ext							
444	7	ext							
5	4	ext							
555	7	ext							

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

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *500		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA:	All:	Deactivation:
Call Forwarding Enhanced Status:	Act:	Deactivation:
Call Park Access Code:		
Call Pickup Access Code:		
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		Conditional Call Extend
Activation:	Deactivation:	

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 11 for outbound calls.

change ars analysis 0		Page 1 of 2
ARS DIGIT ANALYSIS TABLE		
Location: all		Percent Full: 0
Dialed String	Total Min Max	Route Pattern
0	11 11	11
011	11 18	11
1	11 11	11
411	3 3	11
		Call Type
		Node Num
		ANI Req'd
		op
		intl
		pubu
		svcl
		n
		n
		n
		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 11 for outgoing call.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 11 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.
- **Numbering Format:** **unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR:** next

change route-pattern 11													Page	1 of	3		
Pattern Number: 11													Pattern Name: outgoing PSTN				
SCCAN? n													Secure SIP? n				
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC			
No			Mrk	Lmt	List	Del	Digits						QSIG				
							Dgts						Intw				
1:	11	0										n	user				
2:												n	user				
3:												n	user				
4:												n	user				
5:												n	user				
6:												n	user				
BCC		VALUE		TSC	CA-TSC		ITC		BCIE	Service/Feature		PARM	No.	Numbering	LAR		
0		1	2	M	4	W	Request									Dgts	Format
													Subaddress				
1:	y	y	y	y	y	n	n	rest					unk-unk		next		
2:	y	y	y	y	y	n	n	rest							none		
3:	y	y	y	y	y	n	n	rest							none		
4:	y	y	y	y	y	n	n	rest							none		

5.10. Saving Communication Manager Configuration Changes

The command “**save translation all**” can be used to save the configuration changes made on Communication Manager.

6. Administer Avaya Aura® Session Manager

In this section, it shows how to configure the routing on Session Manager. It is assumed that the Session Manager has been successfully deployed and connected to System Manager. The System Manager is the web interface to configure the Session Manager.

6.1. Create a SIP domain name

This section shows how to create a new SIP domain name for this test configuration. The Session Manager uses this domain name to route the call from Broadconnect to CM and vice versa.

a) Login to System Manager. Open the web browser, then login with user “admin” and appropriate password as show in **Figure 6.1**.

AVAYA Avaya Aura® System Manager 6.1

Home / Log On

Log On

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account.
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification 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.

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.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

[Change Password](#)

Figure 6.1 Login to System Manager

The System Manager home page displays as **Figure 6.2**. Select **Routing** to configure the **Network Routing Policy**.

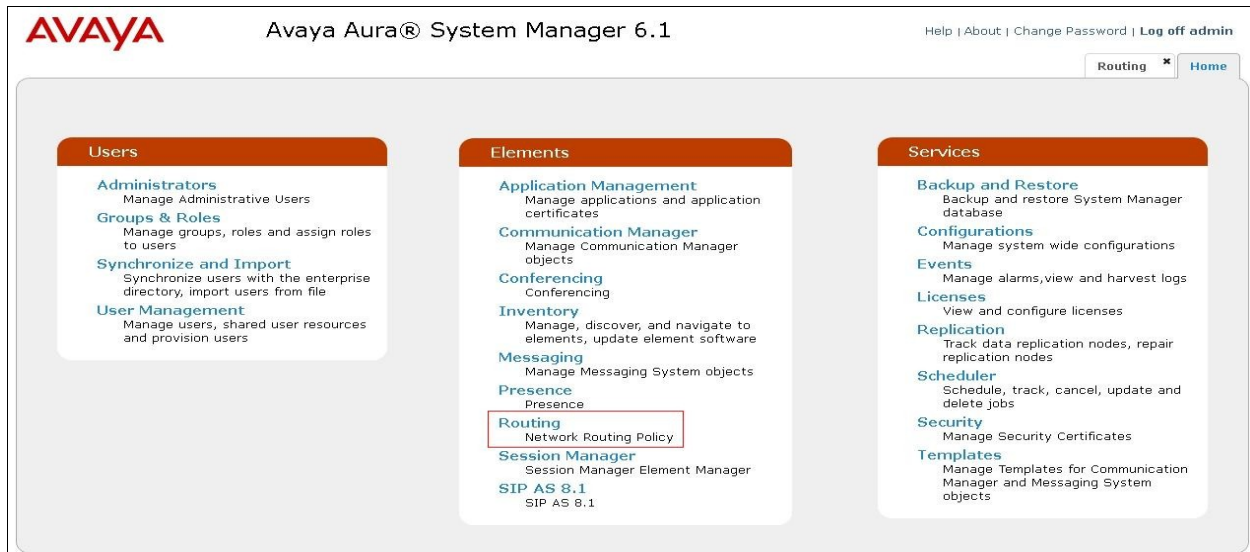


Figure 6.2 Select Routing to configure Network Routing Policy

c) In the **Introduction to Network Routing Policy** page (not shown), click **Domains** link on the left menu to open **Domains - Domain Management** page. Then click button **New** (not shown) to add a new test domain. **Figure 6.3** shows domain **broadconnect.ca** was successfully added.

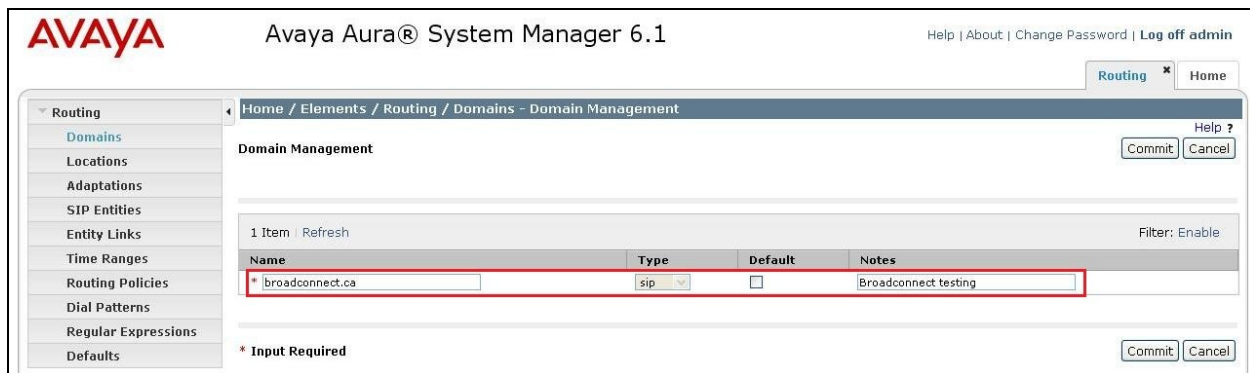


Figure 6.3 Adding SIP domain broadconnect.ca

d) Click **Commit**.

6.2. Create a Location

Other than domain name, Session Manager binds a SIP Entity to a Location for bandwidth and location management purposes. It inserts SIP header “P-Location” to tell the Service Provider where the call is made from.

The procedure to configure a location is as follows.

a) In the **Introduction to Network Routing Policy** page (not shown), click **Locations** link on the left menu to open **Locations - Location** page. Then click button **New** (not shown) to add a new test location. **Figure 6.4** shows location **Belleville,Ont,Ca** was successfully added with default settings in the red boxes.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for Help, About, Change Password, and Log off admin. A breadcrumb trail shows 'Home / Elements / Routing / Locations - Location Details'. The left sidebar contains a tree view with 'Routing' expanded, showing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and contains several sections: 'General' with a required field for Name (filled with 'Belleville,Ont,Ca') and a Notes field; 'Overall Managed Bandwidth' with a dropdown for Managed Bandwidth Units (set to Kbit/sec) and a Total Bandwidth field (filled with 1000000); 'Per-Call Bandwidth Parameters' with a required field for Default Audio Bandwidth (set to 80 Kbit/sec); and 'Location Pattern' with an 'Add' button and a table showing 0 items. At the bottom, there is a 'Commit' button and a 'Cancel' button. Red boxes are drawn around the Name, Total Bandwidth, and Default Audio Bandwidth fields to indicate they are the focus of the configuration.

Figure 6.4 Adding a Location

b) Click **Commit**.

6.3. Create SIP Entity for Avaya Aura® Session Manager

This section shows how to configure System Manager to add a **SIP Entity** for Session Manager as a static gateway.

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for Session Manager. **Figure 6.5** shows entity **DevASM** was successfully added. The Session Manager was configured to use transport protocol UDP with port 5060.

- Name: **DevASM**
- FQDN or IP Address: **111.10.97.198**
- Type: **Session Manager**
- Location: **Belleville,Ont,Ca**
- Port: **5060**
- Protocol: **UDP**
- SIP Link Monitoring: **Use Session Manager Configuration**

Routing / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: DevASM

* FQDN or IP Address: 111.10.97.198

Type: Session Manager

Notes: For Session Manager

Location: Belleville,Ont,Ca

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

19 Items | Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	UDP	* 5060	car1-cores1-Cust_0	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	CS1K60	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	AA-SBC	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	*		* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	*		* 5060	<input checked="" type="checkbox"/>

Select : All, None < Previous | Page 1 of 4 | Next >

Port

Add Remove

4 Items | Refresh Filter: Enable

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP		

Figure 6.5 Adding SIP Entity for Session Manager

b) Click **Commit**.

Note: The IP Address used for SIP Entity - Session Manager has to be different than the IP address used for management interface of Session Manager. The management IP was associated to physical interface eth0 and was defined during software installation. While the IP for SIP Entity was associated to physical interface eth2.

6.4. Create SIP Entity for Avaya Aura® Communication Manager SIP Gateway

This section shows how to configure System Manager to add a SIP Entity for CM SIP Gateway.

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for CM SIP Gateway.

The **Entity Links** configuration is to define the network connection between Session Manager and CM SIP Gateway. In this testing, the trusted link was configured with protocol TCP and port 5060. The **Figure 6.6** shows SIP Entity **CM2_REL-6_G450 PUBLIC** was successfully added.

- Name: **CM2_Rel-6_G450 Public**
- FQDN or IP Address: **111.10.97.246**
- Type: **CM**
- Adaptation: **CM_Broadconnect_Inbound**, as shown in **Section 6.6**.
- Location: **Belleville,Ont,Ca**
- SIP Link Monitoring: **Use Session Manager Configuration**

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The left sidebar contains a menu with options: Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The 'General' tab contains the following fields:

- Name:** CM2_Rel-6_G450 Public
- FQDN or IP Address:** 111.10.97.246
- Type:** CM
- Notes:** Broadconnect
- Adaptation:** CM_Broadconnect_Inbound
- Location:** Belleville,Ont,Ca
- Time Zone:** America/Toronto
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

Below the 'General' tab is the 'Entity Links' section, which includes 'Add' and 'Remove' buttons. A table below shows the configuration for the 'CM2_Rel-6_G450 Public' entity:

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
DevASM	TCP	* 5060	CM2_Rel-6_G450 Public	* 5060	<input checked="" type="checkbox"/>

Figure 6.6 Adding SIP Entity for CM SIP Gateway

b) Click **Commit**.

Note: In the **Entity Links** configuration, the option “**Trusted**” is mandatory.

6.5. Create SIP Entity for Avaya Session Border Controller for Enterprise

This section shows how to configure System Manager to add a SIP Entity for Avaya SBCE.

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for Avaya SBCE.

The **Entity Links** configuration is to define the network connection between Session Manager and Avaya SBCE. In this testing, the trusted link was configured with protocol TCP and port 5060. The **Figure 6.7** shows SIP Entity **Avaya SBCE** was successfully added.

- Name: **Avaya SBCE**
- FQDN or IP Address: **111.10.97.189**
- Type: **Other**
- Adaptation: **CM_Broadconnect_Outbound**, as shown in **Section 6.6**.
- Location: **Belleville,Ont,Ca**
- SIP Link Monitoring: **Use Session Manager Configuration**

The screenshot displays the 'SIP Entity Details' configuration page in the Avaya Aura System Manager 6.1 interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The configuration fields are as follows:

- Name:** Avaya SBCE
- FQDN or IP Address:** 111.10.97.189
- Type:** Other
- Notes:** Avaya SBCE
- Adaptation:** CM_Broadconnect_Outbound
- Location:** Belleville,Ont,Ca
- Time Zone:** America/New_York
- Override Port & Transport with DNS SRV:** ☐
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Link Monitoring Enabled
- * Proactive Monitoring Interval (in seconds):** 900
- * Reactive Monitoring Interval (in seconds):** 120
- * Number of Retries:** 1

Below the configuration fields is the 'Entity Links' section, which includes an 'Add' button and a 'Remove' button. A table shows the configured entity links:

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
DevASM	TCP	* 5060	Avaya SBCE	* 5060	<input checked="" type="checkbox"/>

Figure 6.7 Adding SIP Entity for Avaya SBCE

b) Click **Commit**.

Note: In the **Entity Links** configuration, the option “**Trusted**” is mandatory.

6.6. Create Adaptation Module

Session Manager can be configured with Adaptation modules that modify SIP messages before or after routing decisions have been made. A generic Adaptation module

DigitConversionAdapter supports digit conversion of telephone numbers in specific headers of SIP messages. Other Adaptation modules are built on this generic module, and can modify other headers to permit interoperability with third party SIP products.

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

The adaptations named **CM_Broadconnect_Inbound** and **CM_Broadconnect_Outbound** were configured and used in the compliance test.

The **CM_Broadconnect_Outbound** adaptation will later be assigned to the Avaya SBCE SIP Entity. This adaptation uses the **DigitConversionAdapter** and specifies three parameters used to adapt the FQDN to the domains expected by the Broadconnect network in the sample configuration.

- **osrcd=broadconnect.ca**. This configuration enables the outbound source domain to be overwritten with **broadconnect.ca**. For example, for outbound PSTN calls from the Avaya CPE to Broadconnect, the PAI header will contain “broadconnect.ca” as expected by Broadconnect.
- **odstd=broadconnect.ca**. This configuration enables the outbound destination domain to be overwritten with **broadconnect.ca**. For example, for outbound PSTN calls from the Avaya CPE to Broadconnect, the Request-URI will contain **broadconnect.ca** as expected by Broadconnect.
- **fromto=true**. With this configuration, for an outbound call to Broadconnect, Session Manager 6.1 will set the host portion of both the PAI and the From headers to **broadconnect.ca**, and the host portion of the Request-URI and To headers to **broadconnect.ca**.

Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domains in this fashion. In the sample configuration, where **avaya.com** was already in use in a shared Avaya environment, Session Manager was used to adapt the domain from **avaya.com** to **broadconnect.ca** where the latter is the CPE domain known to Broadconnect.

The screen below shows the **CM_Broadconnect_Outbound** adaptation configured for the testing associated with these Application Notes:

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details

General

* Adaptation name: CM_Broadconnect_Outbound

Module name: DigitConversionAdapter

Module parameter: osrcd=broadconnect.ca odstd=br

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

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

Digit Conversion for Outgoing Calls from SM

Add Remove

0 Items Refresh Filter: Enable

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

* Input Required

Commit Cancel

Figure 6.8 Outbound Adaptations

The adaptation named **CM_Broadconnect_Inbound** shown below will later be assigned to the Communication Manager SIP Entity for calls to and from Broadconnect. This adaptation uses the **DigitConversionAdapter** and specifies the **odstd=avaya.com** parameter to adapt the domain to the domain expected by Communication Manager. More specifically, this configuration enables the destination domain to be overwritten with **avaya.com** for calls that egress to a SIP entity using this adapter. For example, for inbound PSTN calls from Broadconnect to the Avaya CPE, the Request-URI header sent to Communication Manager will contain **avaya.com** as expected by Communication Manager in the shared Avaya test Lab environment. Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.

- **osrcd=avaya.com.** This configuration enables the inbound source domain to be overwritten with **avaya.com**. For example, for inbound PSTN calls from Broadconnect to the Avaya CPE, the PAI header will contain “avaya.com” as expected by Broadconnect.
- **odstd= avaya.com.** This configuration enables the inbound destination domain to be overwritten with **avaya.com**. For example, for inbound PSTN calls from Broadconnect to the Avaya CPE, the Request-URI will contain **avaya.com** as expected by CM.
- **fromto=true.** With this configuration, for an inbound call from Broadconnect, Session Manager 6.1 will set the host portion of both the PAI and the From headers to **avaya.com**, and the host portion of the Request-URI and To headers to **avaya.com**.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Adaptations

Adaptation Details

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Adaptation Details

Commit

Cancel

General

* Adaptation name:

CM_Broadconnect_Inbound

Module name:

DigitConversionAdapter

Module parameter:

odstd=avaya.com osrcd=avaya.c

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add

Remove

0 Items

Refresh

Filter: Enable

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

Digit Conversion for Outgoing Calls from SM

Add

Remove

0 Items

Refresh

Filter: Enable

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

* Input Required

Commit

Cancel

Figure 6.9 Inbound Adaptations

6.7. Create Routing Policy for inbound call

This section shows how to configure Session Manager to add a **Routing Policy** for inbound calls from Broadconnect to CM. As part of the dialing plan configuration, the **Routing Policy** instructs the Session Manager to route the SIP call from PSTN to the CM SIP Gateway to terminate.

The “**Time of Day**” setting defines the range to apply the **Routing Policy** during the day. In this testing, just simply select the default name **24/7**. It means the **Routing Policy** is always in effect.

Figure 6.10 shows policy **Broadconnect to CM2** was created.

- Name: **Broadconnect to CM2**
- SIP Entity as Destination: **CM2_REL-6_G450 PUBLIC**
- Time of Day: **24/7**

The screenshot displays the Avaya Aura System Manager 6.1 interface. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'General' tab. A red box highlights the 'Name' field, which contains 'Broadconnect to CM2', and the 'Notes' field, which contains 'Broadconnect to CM2 Rel 6'. Below this, the 'SIP Entity as Destination' section shows a table with one entry: 'CM2_Rel-6_G450 Public' with FQDN '111.10.97.246' and Type 'CM'. The 'Time of Day' section shows a table with one entry: '24/7' with a time range from '00:00' to '23:59'. The 'Dial Patterns' section shows a table with four entries: '514', '604', and two others, all with a time range from '10' to '10'.

Name	FQDN or IP Address	Type	Notes
CM2_Rel-6_G450 Public	111.10.97.246	CM	Broadconnect

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	Time Range 24/7

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
514	10	10	✓	broadconnect.ca	Belleville,Ont,Ca	broadconnect inbound
604	10	10	✓	broadconnect.ca	Belleville,Ont,Ca	broadconnect inbound

Figure 6.10 Adding Routing Policy for inbound call

6.8. Create Routing Policy for outbound call

Please refer to **Section 6.5** to create a **Routing Policy** for an outbound call. Based on the policy, the Session Manager routes the call from the CM to the SIP Entity AVAYA SBCE as the destination, then the Avaya SBCE sends the request to Broadconnect.

Figure 6.11 shows policy **CM2 to Broadconnect** was created.

- Name: **CM2 to Broadconnect**
- SIP Entity as Destination: **Avaya SBCE**
- Time of Day: **24/7**

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing Policy Details

General

* Name: CM2 to Broadconnect

Disabled: ☐

Notes: CM2 Rel 6 to Broadconnect

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	111.10.97.189	Other	Avaya SBCE

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select: All, None

Dial Patterns

Add Remove

5 Items Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
0	11	36	<input type="checkbox"/>	broadconnect.ca	Belleville,Ont,Ca	broadconnect outbound call, operator call
011	14	14	<input type="checkbox"/>	broadconnect.ca	Belleville,Ont,Ca	broadconnect outbound call, international

Figure 6.11 Adding Routing Policy for outbound call

6.9. Create Dial Pattern for inbound call

In this testing, Broadconnect assigns DID numbers with prefix **514** to the CM. The DIDs are in 10 digits format. The Dial Pattern **514** on Session Manager is configured as an entry of Routing Policy **Broadconnect to CM2**. It means when Session Manager receives inbound call with prefix **514**, it will routes the call to the CM SIP Gateway **Broadconnect to CM2** as the destination. **Figure 6.12** shows policy **Dial Pattern 514** was created.

a) In the **Introduction to Network Routing Policy** page (not shown), click **Dial Patterns** link on the left menu to open **Dial Patterns – Dial Pattern Details** page. Then click button **New** (not shown) to add a new Dial Pattern for inbound call with prefix **514**.

b) Under **Originating Locations and Routing Policy**, click **Add** (not shown). In the **Dial Patterns – Originating Locations and Routing Policy List** page (not shown), select **Originating Location** entry **Belleville,Ont,Ca** and **Routing Policies** entry **Broadconnect to CM2**.

- Pattern: **514**
- Min: **10** (digits)
- Max: **10** (digits)
- SIP Domain: **broadconnect.ca**
- Originating Location Name: **Belleville,Ont,Ca**
- Routing Policy Name: **Broadconnect to CM2**
- Routing Policy Destination: **CM2_REL-6_G450 PUBLIC**

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a menu with options like Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main area is titled 'Dial Pattern Details' and has a 'General' tab selected. In the 'General' tab, there are input fields for 'Pattern' (514), 'Min' (10), 'Max' (10), 'Emergency Call' (unchecked), 'SIP Domain' (broadconnect.ca), and 'Notes' (broadconnect inbound). Below this, the 'Originating Locations and Routing Policies' section has an 'Add' button and a table with one entry: 'Belleville,Ont,Ca' as the Originating Location Name, 'Broadconnect to CM2' as the Routing Policy Name, Rank 0, 'CM2_Rel-6_G450 Public' as the Routing Policy Destination, and 'Broadconnect to CM2 Rel 5' as the Routing Policy Notes. The 'Denied Originating Locations' section is empty and has an 'Add' button. At the bottom, there are 'Commit' and 'Cancel' buttons.

Figure 6.12 Adding Dial Pattern for inbound call

c) Click **Commit**.

The above example shows a prefix or area code starting with 514, however other DID numbers provided by Broadconnect had prefixes or area codes starting with 403, 604, 613, 780 and 905. A Dial Pattern must be created for each of those prefixes in the same manner as described above.

6.10.Create Dial Pattern for outbound call

The **Dial Pattern** for outbound call is associated to the **Routing Policy CM2 to Broadconnect**. The **Dial Pattern** configuration on Session Manager has to match the dialing plan configure on the CM.

a) Dial Pattern with prefix **1**. For long distance calls, CM sends 11 digits with prefix **1** to Broadconnect system via Avaya SBCE. To create the Dial Pattern **1**, the detail configuration is shown in **Figure 6.13**.

- Pattern: **1**
- Min: **11** (digits)
- Max: **36** (default)
- SIP Domain: **broadconnect.ca**
- Originating Location Name: **Belleville,Ont,Ca**
- Routing Policy Name: **CM2 to Broadconnect**
- Routing Policy Destination: **Avaya SBCE**

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 1

* Min: 11

* Max: 36

Emergency Call: ☐

SIP Domain: broadconnect.ca

Notes: broadconnect outbound call, long distance

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CM2 to Broadconnect	0	<input type="checkbox"/>	Avaya SBCE	CM2 Rel 6 to Broadconnect

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit Cancel

Figure 6.13 Adding Dial Pattern for outbound long distance call with prefix 1

b) Dial Pattern with prefix **0**. CM sends **0** or **0+10** digits to reach operator at Broadconnect. Broadconnect also uses the same prefix **011** for the outbound international call. Thus, the Dial

Pattern **0** should have flexible length. To create the Dial Pattern **0**, the detail configuration is shown in **Figure 6.14**.

- Pattern: **0**
- Min: **11** (digits)
- Max: **36** (default)
- SIP Domain: **broadconnect.ca**
- Originating Location Name: **Belleville,Ont,Ca**
- Routing Policy Name: **CM2 to Broadconnect**
- Routing Policy Destination: **Avaya SBCE**

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 0

* Min: 11

* Max: 36

Emergency Call: ☐

SIP Domain: broadconnect.ca

Notes: broadconnect outbound call, operator call

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CM2 to Broadconnect	0	<input type="checkbox"/>	Avaya SBCE	CM2 Rel 6 to Broadconnect

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit Cancel

Figure 6.14 Adding Dial Pattern for outbound special call with prefix 0

c) Dial Pattern with prefix **411**. As part of the dialing plan, the **Dial Pattern 411** routes the call from CM to 411 directory services hosted by Broadconnect. To create the Dial Pattern **411**, the detail configuration is shown in **Figure 6.15**.

- Pattern: **411**
- Min: **3** (digits)
- Max: **3** (digits)
- SIP Domain: **broadconnect.ca**
- Originating Location Name: **Belleville,Ont,Ca**
- Routing Policy Name: **CM2 to Broadconnect**
- Routing Policy Destination: **Avaya SBCE**

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 411

* Min: 3

* Max: 3

Emergency Call: ☐

SIP Domain: broadconnect.ca

Notes: broadconnect outbound call, directory assist

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville, Ont, Ca		CM2 to Broadconnect	0	<input type="checkbox"/>	Avaya SBCE	CM2 Rel 6 to Broadconnect

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit Cancel

Figure 6.15 Adding Dial Pattern for outbound 411 calls

d) Dial Pattern with prefix **911**. As part of the dialing plan, the **Dial Pattern 911** routes the call from CM to 911 emergency services hosted on Broadconnect. To create the Dial Pattern **911**. The detail configuration is shown in **Figure 6.16**.

- Pattern: **911**
- Min: **3** (digits)
- Max: **3** (digits)
- SIP Domain: **broadconnect.ca**
- Originating Location Name: **Belleville, Ont, Ca**
- Routing Policy Name: **CM2 to Broadconnect**
- Routing Policy Destination: **Avaya SBCE**

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern:

911

* Min:

3

* Max:

3

Emergency Call:

☐

SIP Domain:

broadconnect.ca

Notes:

broadconnect outbound call, emergency

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CM2 to Broadconnect	0	<input type="checkbox"/>	Avaya SBCE	CM2 Rel 6 to Broadconnect

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit

Cancel

Figure 6.16 Adding Dial Pattern for outbound 911 calls

STB; Reviewed:
SPOC 6/25/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

42 of 85
BroadCtCMSMSBCE

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Reference** [9] and [10].

This compliance test comprised the configuration for two major components, trunk server for service provider and call server for enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings, the configuration is defined in the Avaya SBCE web user interface as described in the following sections.

Trunk server configuration elements for service provider Broadconnect:

- Global Profiles:
 - o URI Groups.
 - o Routing.
 - o Topology Hiding.
 - o Server Interworking.
 - o Signaling Manipulation.
 - o Server Configuration.
- Domain Policies
 - o Application Rules.
 - o Media Rules.
 - o Signaling Rules.
 - o Endpoint Policy Group.
 - o Session Policy.
- Device Specific Settings:
 - o Network Management.
 - o Media Interface.
 - o Signaling Interface.
 - o End Point Flows → Server Flows.
 - o Session Flows.

Call server configuration elements for enterprise Session Manager:


- Global Profiles:
 - o URI Groups.
 - o Routing.
 - o Topology Hiding.
 - o Server Interworking.
 - o Server Configuration
- Domain Policies
 - o Application Rules.
 - o Media Rules.
 - o Signaling Rules
 - o Endpoint Policy Group.

- Session Policy
- Device Specific Settings:
 - Network Management.
 - Media Interface.
 - Signaling Interface.
 - End Point Flows → Server Flows.
 - Session Flows.

7.1. Avaya Session Border Controller For Enterprise Login

Use a WEB browser to access the UC-Sec web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser, where `<ip-addr>` is the management LAN IP address of UCSec.

Log in with appropriate credentials. Click **Sign In**.



The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

[Visit the Sipera Systems website to learn more.](#)

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

The main page of the **UC-Sec Control Center** will appear.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 12:48:21 AM EDT

Alarms **Incidents** **Statistics** **Logs** **Diagnostics** **Users** **Logout** **Help**

UC-Sec Control Center

Welcome

Securing your real-time unified communications

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail support@sipera.com.

Alarms (Past 24 Hours)	Incidents (Past 24 Hours)
None found.	sipera: No Routing Rule matched
	sipera: No Routing Rule matched
	sipera: No Routing Rule matched
	sipera: No Routing Rule matched

Administrator Notes [Add]

No notes posted.

Quick Links

- Sipera Website
- Sipera VIPER Labs
- Contact Support

UC-Sec Devices	Network Type
sipera	DMZ_ONLY

To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **sipera** is shown. To view the configuration of this device, click the **View Config** icon (the third icon from the right).

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 12:58:46 AM EDT

Alarms **Incidents** **Statistics** **Logs** **Diagnostics** **Users** **Logout** **Help**

UC-Sec Control Center

System Management

Installed **Updates**

Device Name	Serial Number	Version	Status
sipera	IPCS31020134	4.0.5.Q02	Commissioned

The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

The screenshot shows a window titled "System Information: sipera". Inside, there are three main sections:

- Network Configuration** (header):
 - General Settings**:

Appliance Name	sipera
Box Type	SIP
Deployment Mode	Proxy
 - Device Settings**:

HA Mode	NO
Secure Channel Mode	NONE
Two Bypass Mode	NO
- Network Settings**:

IP	Public IP	Netmask	Gateway	Interface
111.10.97.189	111.10.97.189	255.255.255.192	111.10.97.129	A1
111.10.98.98	111.10.98.98	255.255.255.224	111.10.98.97	B1
111.10.98.112	111.10.98.112	255.255.255.224	111.10.98.97	B1
- DNS Configuration**:

Primary DNS	110.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	110.10.97.189
- Management IP(s)**:

IP	110.10.98.85
----	--------------

7.2. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.2.1. Uniform Resource Identifier (URI) Groups

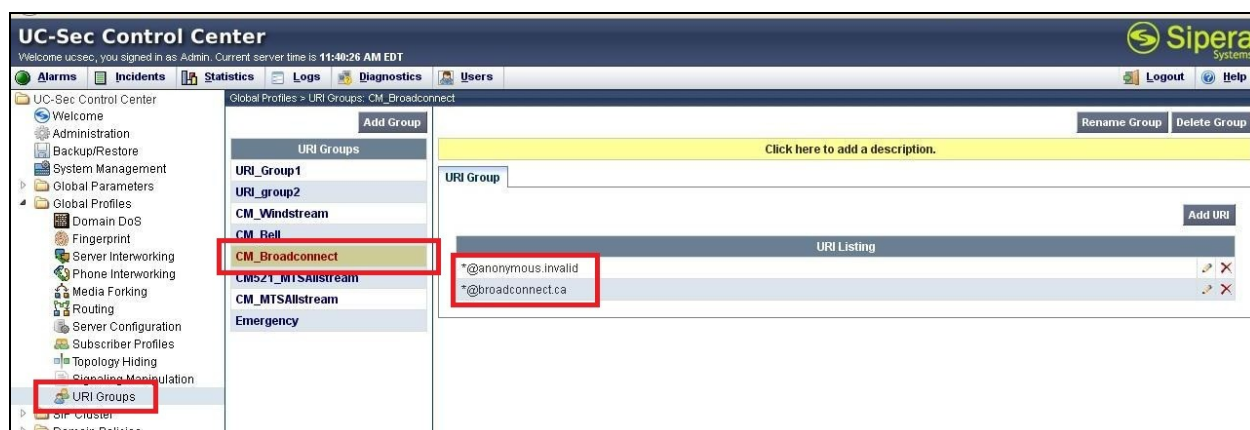
The **URI Group** feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be taken for a given call flow.

To add an **URI Group**, select **UC-Sec Control Center** → **Global Profiles** → **URI Groups**. Click on **Add Group** (not shown).

In this compliance test, a URI Group named “**CM_Broadconnect**” was added with plain URI type and consists of two domains [*@anonymous.invalid](#) and [*@broadconnect.ca](#) . This group

was used to match the From and To headers in SIP call dialogs received from Session Manager and Broadconnect SIP Trunk. If there is a match, then the Avaya SBCE applies the appropriate **Routing Profile** and **Server Flow** to route the inbound and outbound call to the right destinations. The **Routing Profile** and **Server Flow** are configured in next steps.

The screenshots below illustrate the **Global Profiles > URI Groups: CM_Broadconnect**.



7.2.2. Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by **Routing Profiles** include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

To create a **Routing Profile**, select **UC-Sec Control Center > Global Profiles > Routing**. Click on **Add Profile** (not shown).

In this compliance test, a **Routing Profile** named **To_Broadconnect** is created to be used in conjunction with the server flow defined for Session Manager. This entry is to route the outgoing enterprise SIP call to Broadconnect as a destination. On the opposite direction, a **Routing Profile** named **To_SM_fr_Broadconnect** is created to be used in conjunction with the server flow

defined for Broadconnect. This entry is to route the incoming SIP call from Broadconnect to enterprise as a destination.

7.2.2.1 Routing Profile for Broadconnect

The screenshots below illustrate the **UC-Sec Control Center > Global Profiles > Routing: To_Broadconnect**. The Broadconnect SIP Trunk is connected with transportation protocol **UDP**. If there is a match in To header with the **URI Group** named **CM_Broadconnect** defined in **Section 7.2.1**, then the call will be routed to the **Next Hop Server 1** which is the IP address of Broadconnect SIP Trunk.

The screenshot shows the UC-Sec Control Center interface. On the left, the 'Routing' menu item is highlighted. In the center, the 'Routing Profiles' list shows 'To_BroadConnect' selected. On the right, the 'Routing Profile' configuration for 'To_BroadConnect' is displayed. It includes a table with one routing rule:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	CM_Broadconnect	333.113.62.151	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

The 'Edit Routing Rule' dialog box is shown. It contains the following fields and options:

- URI Group:** CM_Broadconnect
- Next Hop Server 1:** 333.113.62.151
- Next Hop Server 2:** (empty)
- Routing Priority based on Next Hop Server:** ☒
- Use Next Hop for In Dialog Messages:** ☐
- Ignore Route Header for Messages Outside Dialog:** ☐
- NAPTR:** ☐ **SRV:** ☐
- Outgoing Transport:** ☐ TLS ☐ TCP ☒ UDP

A 'Finish' button is located at the bottom right.

7.2.2.2 Routing Profile for Session Manager

The Routing Profile “To_SM_fr_Broadconnec” is also defined to route the matching SIP call to **Next Hop Server 1** which is the IP address of Session Manager as a destination. As shown in **Figure 1**, Session Manager SIP entity is connected with transportation protocol TCP.

The screenshot shows the UC-Sec Control Center interface. On the left is a navigation tree with 'Routing' highlighted. The main panel displays the 'Global Profiles > Routing: To_SM_fr_BroadConnec' configuration. A table lists routing profiles, with 'To_SM_fr_BroadConnec' selected. Below, the 'Routing Profile' configuration is shown with a table of routing rules.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Disable	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	CM_Broadconnect	111.10.97.198:5060	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

The 'Edit Routing Rule' dialog box is shown. It contains a warning message and a 'Next Hop Routing' section. The 'URI Group' is set to 'CM_Broadconnect'. 'Next Hop Server 1' is '111.10.97.198:5060'. The 'Routing Priority based on Next Hop Server' checkbox is checked. 'Outgoing Transport' is set to 'TCP'. A 'Finish' button is at the bottom.

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group: CM_Broadconnect

Next Hop Server 1: 111.10.97.198:5060

Next Hop Server 2:

☒ Routing Priority based on Next Hop Server

☐ Use Next Hop for In Dialog Messages

☐ Ignore Route Header for Messages Outside Dialog

☐ NAPTR ☐ SRV

Outgoing Transport: ☐ TLS ☒ TCP ☐ UDP

Finish

7.2.3. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

To create a **Topology Hiding** profile, select **UC-Sec Control Center > Global Profiles > Topology Hiding**. Click on **Add Profile** (not shown).

In this compliance test, two **Topology Hiding** profiles were created, named **To_Broadconnect** and **To_Communication Manager**.

7.2.3.1 Topology Hiding Profile for Broadconnect.

Profile **To_Broadconnect** is defined to mask the enterprise SIP domain **avaya.com** in the From header to **broadconnect.ca** (the domain name defined here for From header is to meet the SIP specification require by Broadconnect); delete Record-Route and Via entries added by Session Manager and replace internal IP addresses in SDP by external IP address known to Broadconnect. It secures the enterprise network topology and also to meet the SIP requirement from the service provider.

The screenshots below illustrate the **UC-Sec Control Center > Global Profiles > Topology Hiding: To_Broadconnect**.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'Global Profiles' expanded and 'Topology Hiding' selected. The main content area shows the configuration for the 'To_BroadConnect' profile. A table titled 'Topology Hiding' lists the headers, criteria, replace actions, and overwrite values for the profile.

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	broadconnect.ca

Edit Topology Hiding Profile
Add Header

Header	Criteria	Replace Action	Overwrite Value	
SDP	IP/Domain	Auto		✗
Via	IP/Domain	Auto		✗
Record-Route	IP/Domain	Auto		✗
From	IP/Domain	Overwrite	broadconnect.ca	✗

Finish

7.2.3.2 Topology Hiding Profile for Session Manager.

Profile **To_SM_fr_BroadC** passes the Broadconnect SIP domain **broadconnect.ca** in all headers straight through to the Session Manager where they are manipulated to match the enterprise network domain.

The screenshots below illustrate the **UC-Sec Control Center > Global Profiles > Topology Hiding: To_SM_fr_BroadC**.

The screenshot shows the UC-Sec Control Center interface. On the left is a navigation tree with categories like Administration, System Management, Global Profiles, and Subscriber Profiles. Under Global Profiles, 'Topology Hiding' is selected and highlighted with a red box. The main area shows the configuration for the 'To_SM_fr_BroadC' profile, which is also highlighted with a red box in the list. The 'Topology Hiding' tab is active, displaying a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

Buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible.

7.2.4. Server Interworking

Interworking Profile features are configured based on different Call and Trunk Servers.

To create a **Server Interworking** profile, select **UC-Sec Control Center > Global Profiles > Server Interworking**. Click on **Add Profile** (not shown).

In this compliance testing, two profiles were created for Session Manager and Broadconnect trunk server, named **SM** and **Broadconnect**.

7.2.4.1 Server Interworking profile for Broadconnect

Profile **Broadconnect** is defined to match the specification of the Broadconnect SIP Trunk. The General settings are configured with the following parameters while the other options for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

General settings:

- Hold Support = **None**. Avaya SBCE will not modify the hold/ resume signaling from Communication Manager to send to Broadconnect.
- 18X Handling = **None**. Avaya SBCE will not handle 18X, it will keep the 18X messages from Communication Manager unchanged to send to Broadconnect.
- Refer Handling = **unchecked**. Avaya SBCE will not handle Refer, it will keep the Refer messages from Communication Manager unchanged to send to Broadconnect.
- Privacy Enabled = **unchecked**. Avaya SBCE will not mask the FROM header with anonymous for outbound call to Broadconnect. It depends on the Communication Manager to enable/ disable privacy on individual call basis.
- DTMF Support = **None**. Avaya SBCE will send original DTMF supported by Communication Manager to Broadconnect.

The screenshots below illustrate the **UC-Sec Control Center > Global Profiles > Server Interworking: Broadconnect**.

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 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

Next

Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

Back Finish

7.2.4.2 Server Interworking profile for Session Manager

Profile **SM** is defined to match the specification on Communication Manager. The General settings are configured with the following parameters while the other options for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

General settings:

- Hold Support = **RFC3264**. Communication Manager supports hold/ resume as per RFC3264.
- 18X Handling = **None**. Avaya SBCE will not handle 18X, it will keep the 18X messages from Broadconnect unchanged to send to Communication Manager via Session Manager.
- Refer Handling = **unchecked**. Avaya SBCE will not handle Refer, it will keep the Refer messages from Broadconnect unchanged to send to Communication Manager via Session Manager.
- Privacy Enabled = **unchecked**. Avaya SBCE will not mask the From header with anonymous for inbound call from Broadconnect. It depends on the Broadconnect to enable/ disable privacy on individual call basis.
- DTMF Support = **None**. Avaya SBCE will send original DTMF supported by Broadconnect to Communication Manager via Session Manager.

The screenshots below illustrate the **UC-Sec Control Center > Global Profiles > Server Interworking: SM**.

Editing Profile: SM

General

Hold Support	<input type="radio"/> None <input type="radio"/> RFC2543 - c=0 0 0 0 <input checked="" 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 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

Next

Editing Profile: SM

Privacy

Privacy Enabled	<input type="checkbox"/>
User Name	
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	

DTMF

DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
--------------	---

Back

Finish

7.2.5. Signaling Manipulation

The **Signaling Manipulation** feature allows the ability to add, change and delete any of the headers in a SIP message. This feature adds the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa. Using this language, a script can be written and tied to a given **Server Configuration** which will be configured in the next steps through the EMS GUI.

To create a **Signaling Manipulation** script, select **UC-Sec Control Center > Global Profiles > Signaling Manipulation**. Click on **Add Script** (not shown).

In this compliance testing, the script named **Broadconnect** was created. The detail is as following:


```

within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    // the PAI will be used to create RemoteParty-ID but first check if privacy is
    active
    // if privacy is active then use the PAI user, if not use the From user for
    all other cases
    if (%HEADERS["From"][1].URI.USER.regex_match("anonymous")) then
    {
      remove(%HEADERS["Alert-Info"][1]);
    }
    else
    {
      %HEADERS["P-Asserted-Identity"][1].URI.USER = %HEADERS["From"][1].URI.USER;
      remove(%HEADERS["Alert-Info"][1]);
    }

    // create a Remote-Party-ID using the information from the PAI header
    %HEADERS["Remote-Party-ID"][1] = %HEADERS["P-Asserted-Identity"][1];

    // hardcode the user to be the Pilot DID
    %HEADERS["From"][1].URI.USER = "4167758782";

    // remove unwanted headers
    remove(%HEADERS["P-Asserted-Identity"][1]);
    remove(%HEADERS["P-Location"][1]);
    remove(%HEADERS["P-Charging-Vector"][1]);
    remove(%HEADERS["Accept-Language"][1]);

    // set the Max-Forwards to one less than the service provider sent to Avaya
    %HEADERS["Max-Forwards"][1] = "8";

  }

  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    // increase the Max-Forwards so the Avaya network can process the call
    %HEADERS["Max-Forwards"][1] = "60";

    // hardcode the host.
    %HEADERS["From"][1].URI.HOST = "broadconnect.ca";

    if (%HEADERS["Request_Line"][1].regex_match("4167758782")) then
    {
      // the incoming R-URI.USER will always be the Pilot DID, so it must be
      stripped off

      %HEADERS["Request_Line"][1].regex_replace("sip:4167758782@135.10.98.112:5060;tra
      nsport=udp SIP/2.0","sip:");
      // use the To.USER to replace the R-URI.USER
      %To_USER = %HEADERS["To"][1].URI.USER;
      append(%HEADERS["Request_Line"][1], %To_USER);
      append(%HEADERS["Request_Line"][1], "@broadconnect.ca:5060;transport=udp
      SIP/2.0");
    }

  }

}

```


In the Signaling Manipulation script named **Broadconnect** above, the statement **act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"** specifies the portion of the script that will take effect on all type of SIP messages for outbound call and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

For outbound calls, the Contact header originated from Communication Manager should be manipulated as per request from Broadconnect, all unnecessary headers will be deleted i.e. P-Location, P-Charging-Vector, Accept-Language, Alert-Info headers.

- SigMa rules to create Remote-Party-ID header. The SigMa script has four main areas of focus. The first rule is to create the Remote-Party-ID for authentication on the Broadconnect network. The Remote-Party-ID should be a valid DID number on the Broadconnect and should reflect the originator of the call. The structure of the Remote-Party-ID header is the same as the P-Asserted-Identity header, so the easiest approach is to use the PAI header and copy its contents into the Remote-Party-ID. The caller DID is usually in the From header, with the only exception being when privacy is turned on. To make a rule for all cases an “if” statement is used to use the URI.USER from the From header in all cases except when the user is “anonymous” or has privacy enabled.

```
// the PAI will be used to create RemoteParty-ID but first check if privacy is active
// if privacy is active then use the PAI user, if not use the From user for all other cases
if (%HEADERS["From"][1].URI.USER.regex_match("anonymous")) then
{
    remove(%HEADERS["Alert-Info"][1]);
}
else
{
    %HEADERS["P-Asserted-Identity"][1].URI.USER = %HEADERS["From"][1].URI.USER;
    remove(%HEADERS["Alert-Info"][1]);
}

// create a Remote-Party-ID using the information from the PAI header
%HEADERS["Remote-Party-ID"][1] = %HEADERS["P-Asserted-Identity"][1];
```

The Alert-Info header is removed in the if statement because there must be an executable line in the if statement and the Header must be removed anyway.

- SigMa rules to populate the Pilot DID in the From header. All calls must have the Pilot DID in the From header in order to be authenticated on the Broadconnect network.

```
// hardcode the user to be the Pilot DID
%HEADERS["From"][1].URI.USER = "4167758782";
```

- SigMa rules to delete unnecessary headers, including P-Location, P-Charging-Vector, Accept-Language, and P-Asserted-Identity. The Alert-Info was removed above.

```
remove(%HEADERS["P-Asserted-Identity"][1]);  
remove(%HEADERS["P-Location"][1]);  
remove(%HEADERS["P-Charging-Vector"][1]);  
remove(%HEADERS["Accept-Language"][1]);
```

- **SigMa rules to set the Max-Forwards**, to one less than the 9 that Broadconnect sends out. This will make it appear that the one hop was used to traverse the Avaya network.

```
// set the Max-Forwards to one less than the service provider sent to Avaya  
%HEADERS["Max-Forwards"][1] = "8";
```

In the Signaling Manipulation script named **Broadconnect** further above, the statement **act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"** specifies the portion of the script that will take effect on all type of SIP messages for inbound call and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement.

- **SigMa rules to increase the Max-Forwards value.** The original value sent by Broadconnect is 9, which is not enough to traverse the Avaya network in certain call scenarios. Increasing the value to 60 will ensure that the message can be processed with no chance of experiencing too many hops.

```
// increase the Max-Forwards so the Avaya network can process the call  
%HEADERS["Max-Forwards"][1] = "60";
```

- **SigMa rule to set the host domain in the From header**, to ensure the From domain is that of Broadconnect.

```
// hardcode the host.  
%HEADERS["From"][1].URI.HOST = "broadconnect.ca";
```

- **SigMa rules to manipulate the calling number in Request URI header.** For incoming calls the Request URI will always be the Pilot DID as defined by Broadconnect. The Pilot DID needs to be removed and the actual called number should be populated in its place. The called number is populated in the To header. The if statement below will copy the To URI.USER into the Request URI header so the call can be properly processed by the Avaya network.

```

        if (%HEADERS["Request_Line"][1].regex_match("4167758782")) then
        {
            // the incoming R-URI.USER will always be the Pilot DID, so it must be
            stripped off

%HEADERS["Request_Line"][1].regex_replace("sip:4167758782@135.10.98.112:5060;transpo
rt=udp SIP/2.0","sip:");
            // use the To.USER to replace the R-URI.USER
            %To_USER = %HEADERS["To"][1].URI.USER;
            append(%HEADERS["Request_Line"][1], %To_USER);
            append(%HEADERS["Request_Line"][1], "@broadconnect.ca:5060;transport=udp
SIP/2.0");
        }

```

7.2.6. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

To create a Server Configuration entry, select **UC-Sec Control Center > Global Profiles > Server Configuration**. Click on **Add Profile** (not shown).

In this compliance testing, two separate Server Configurations were created, server entry **Broadconnect** for Broadconnect; and server entry **SM** for Session Manager.

7.2.6.1 Server Configuration for Broadconnect.

The **Server Configuration** named **Broadconnect** was added for Broadconnect will be discussed in detail as below. Following **General**, **Authentication**, **Heartbeat** and **Advanced** tabs will be provisioned; the other tabs e.g. **DoS Whitelist** and **DoS Protection** are kept as default.

The screenshot shows the UC-Sec Control Center web interface. The left sidebar contains a navigation tree with 'Server Configuration' highlighted. The main content area shows the 'Global Profiles > Server Configuration: Broadconnect' page. The 'General' tab is active, displaying the following configuration:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	333.113.62.151
Supported Transports	UDP
UDP Port	5060

Buttons for 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible at the bottom right of the configuration area.

In the **General** tab, specify Server Type for Broadconnect is a Trunk Server; the IP connectivity has also been defined here. In this compliance testing, Broadconnect supports UDP and listens on port 5060.

Edit Server Configuration Profile - General	
Server Type	Trunk Server
IP Addresses / Supported FQDNs <small>Comma seperated list</small>	333.113.62.151
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
Finish	

Broadconnect requests to have Digest Authentication supported on SIP Trunk. In this compliance testing, the authentication will be implemented by Avaya SBCE. In the **Authentication** tab, click on the checkbox to **Enable Authentication**; provide the **Realm** as **Broadworks**, **User Name** is the Pilot DID and correct **Password** provided by Broadconnect.

Edit Server Configuration Profile - Authentication	
Enable Authentication	<input checked="" type="checkbox"/>
User Name	4167758782
Realm	Broadworks
Password <small>(Leave blank to keep existing password)</small>
Confirm Password
Finish	

In **Heartbeat** tab, the Avaya SBCE is configured **Enable Heartbeat** is checked to send REGISTER messages in 60 seconds intervals to check for the SIP trunk status, input From header as **4137758782@broadconnect.ca** and To header as **4137758782@broadconnect.ca** as expected by Broadconnect. **TCP Probe** is kept unchecked as default.

Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER ▼
Frequency	60 seconds
From URI	4167758782@broadconni
To URI	4167758782@broadconni
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
<input type="button" value="Finish"/>	

Under **Advanced** tab, in **Interworking Profile** drop down list select entry **Broadconnect** as defined in **Section 7.2.4**, in **Signaling Manipulation Script** drop down list select entry **Broadconnect** as defined in **Section 7.2.5**. This configuration is to apply the specific SIP profile and Sigma script rules to the traffic from Broadconnect. The other settings are kept as default.

Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Broadconnect ▼
Signaling Manipulation Script	Broadconnect ▼
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<input type="button" value="Finish"/>	

7.2.6.2 Server Configuration for Avaya Aura® Session Manager.

The **Server Configuration** named **SM** was added for Session Manager will be discussed in detail as below. Following **General**; **Authentication**; **Heartbeat** and **Advanced** tabs will be provisioned; the other tabs e.g. **DoS Whitelist** and **DoS Protection** are kept as default.



In the **General** tab, specify Server Type for Session Manager is a Call Server; the IP connectivity has also been defined here. In this compliance testing, Session Manager link is TCP and listens on port 5060.

The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. It contains the following fields and controls:

- Server Type:** A dropdown menu set to 'Call Server'.
- IP Addresses / Supported FQDNs:** A text area containing '110.10.97.198'.
- Supported Transports:** A section with three checkboxes: ☒ TCP, ☐ UDP, and ☐ TLS.
- TCP Port:** A text field containing '5060'.
- UDP Port:** An empty text field.
- TLS Port:** An empty text field.
- Finish:** A button at the bottom.

In **Authentication** tab, uncheck the checkbox **Enable Authentication**. Session Manager was configured as a trusted link in **Section 6.5**, and does not require authentication.



In **Heartbeat** tab, uncheck the checkbox **Enable Heartbeat**. Session Manager does not require a heartbeat mechanism for this testing.



Under **Advanced** tab, in **Interworking Profile** drop down list select entry **SM** as defined in **Section 7.2.4**, in **Signaling Manipulation Script** drop down list select **None** since there is no manipulation on Session Manager. The other settings are kept as default.

Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SM
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<input type="button" value="Finish"/>	

7.3. Domain Policies

The **Domain Policies** feature configures, applies, and manages various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the UC-Sec security device to aggregate, monitor, control, and normalize call flows. There are default policies available to use, or a custom domain policy can be created.

7.3.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, it is possible to determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Create an **Application Rule** to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

To clone an application rule, navigate to **UC-Sec Control Center > Domain Policies > Application Rules**. With the default rule chosen, click on **Clone Rule** as shown below.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 12:45:58 AM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Domain Policies > Application Rules: default

Filter By Device...

Clone Rule

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

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	1000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None		
IM Logging	No		
RTCP Keep-Alive	No		

Edit

Enter a descriptive name **Broadconnect_AppR** for the new rule and click **Finish**.

Clone Rule

Rule Name default

Clone Name BroadConnect_AppR

Finish

Modify the rule by clicking the **Edit** button. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified **Application Rule** with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to 1000. In the sample configuration, Communication Manager was programmed to control the concurrent sessions by setting the number of members in the trunk group (**Section 5.7**) to the allotted amount. Therefore, the values in the **Application Rule** named **Broadconnect_AppR** were set high enough to be considered non-blocking.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	1000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	<input checked="" type="radio"/> None <input type="radio"/> CDR w/ RTP <input type="radio"/> CDR w/o RTP
IM Logging	<input type="checkbox"/>
RTCP Keep-Alive	<input type="checkbox"/>

Finish

7.3.2. Media Rules

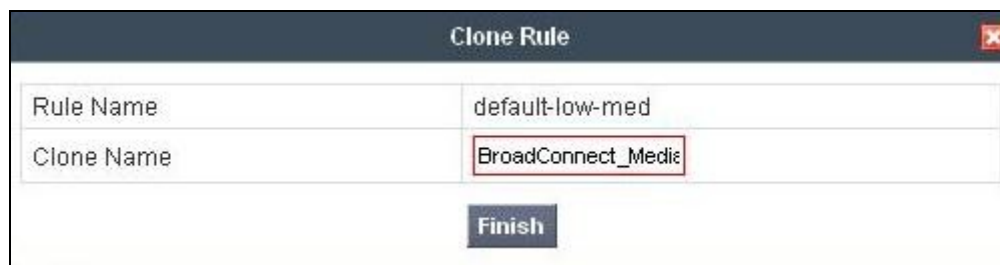
Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the UC-Sec security product.

Create a custom **Media Rule** to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration shows a custom **Media Rule Broadconnect_MediaR** created for the enterprise and Broadconnect.

To create a custom **Media Rule**, navigate to **UC-Sec Control Center > Domain Policies > Media Rules**. With **default-low-med** selected, click **Clone Rule** as shown below.



Enter a descriptive name **Broadconnect_MediaR** for the new rule and click **Finish**.



When the RTP packets of a call are shuffled from Communication Manager to an IP Phone, Avaya SBCE will interpret this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created during an audio shuffle.

To modify the rule, select the **Media Anomaly** tab and click **Edit**, uncheck **Media Anomaly Detection** and click **Finish**.



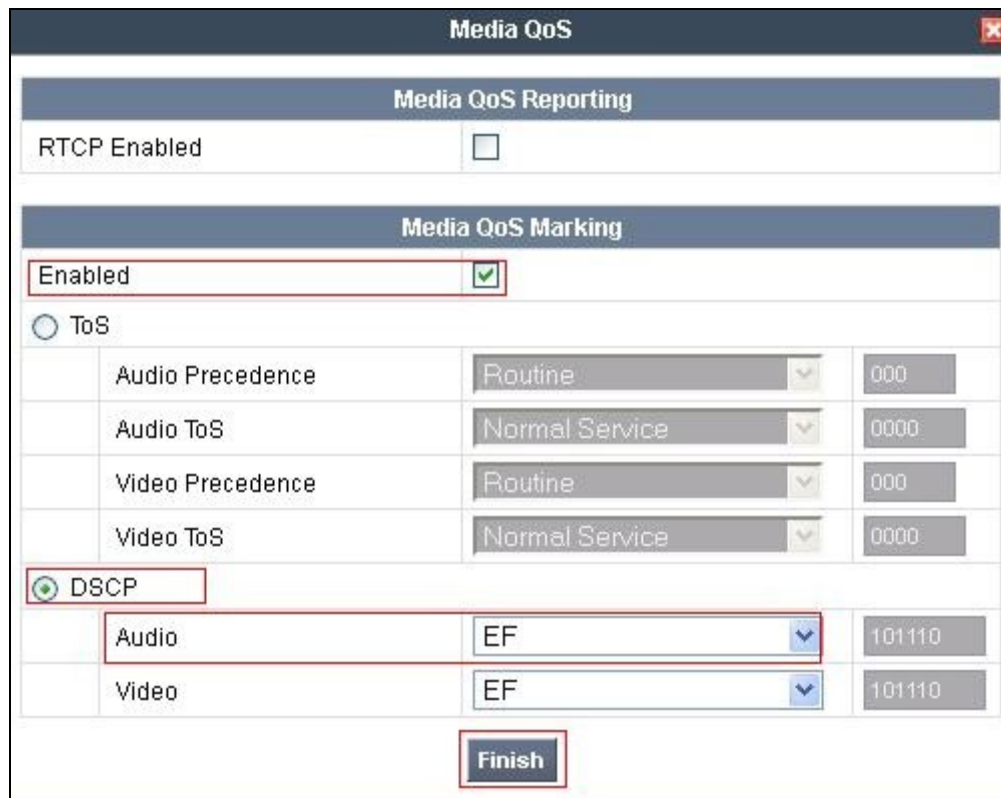
The **Media Silencing** feature detects the silence when the call is in progress. If the silence is detected and exists the allowed duration, Avaya SBCE generates alert in Incidents Log. In this sample configuration, the Media Silencing detection is disabled due to the RTP packets could be lost in part on public WAN.

To modify the rule, select the **Media Silencing** tab and click **Edit**, uncheck **Media Silencing** and click **Finish**.



The screenshot shows the 'Media Silencing' configuration window. It has a title bar with a close button. Below the title bar is a section header 'Media Silencing'. Under this header, there is a checkbox labeled 'Media Silencing' which is currently unchecked. Below the checkbox is a text input field labeled 'Timeout (seconds)'. At the bottom of the window is a 'Finish' button.

On the **Media QoS** tab select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for compliance testing.



The screenshot shows the 'Media QoS' configuration window. It has a title bar with a close button. Below the title bar is a section header 'Media QoS Reporting'. Under this header, there is a checkbox labeled 'RTCP Enabled' which is currently unchecked. Below this is another section header 'Media QoS Marking'. Under this header, there is a checkbox labeled 'Enabled' which is currently checked. Below the 'Enabled' checkbox is a radio button labeled 'ToS'. Below the 'ToS' radio button is a table with four rows: 'Audio Precedence', 'Audio ToS', 'Video Precedence', and 'Video ToS'. Each row has a dropdown menu and a text input field. The values in the dropdown menus are 'Routine' for 'Audio Precedence' and 'Video Precedence', and 'Normal Service' for 'Audio ToS' and 'Video ToS'. The values in the text input fields are '000' for 'Audio Precedence' and 'Video Precedence', and '0000' for 'Audio ToS' and 'Video ToS'. Below the table is a radio button labeled 'DSCP' which is currently selected. Below the 'DSCP' radio button is a table with two rows: 'Audio' and 'Video'. Each row has a dropdown menu and a text input field. The values in the dropdown menus are 'EF' for 'Audio' and 'Video'. The values in the text input fields are '101110' for 'Audio' and '101110' for 'Video'. At the bottom of the window is a 'Finish' button.

7.3.3. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Clone and modify the default signaling rule to apply for both enterprise and Broadconnect. To clone a signaling rule, navigate to **UC-Sec Control Center > Domain Policies > Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.

The screenshot displays the UC-Sec Control Center interface. On the left, a navigation tree shows 'Domain Policies' expanded, with 'Signaling Rules' selected. The 'default' rule is highlighted. The main content area shows the configuration for the 'default' rule. A warning banner states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The 'General' tab is active, showing 'Inbound' and 'Outbound' rule settings. All actions are set to 'Allow'. A 'Clone Rule' button is visible in the top right corner of the main panel.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks		<input checked="" type="checkbox"/>	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

On the **General** tab, accept the defaults as shown in following screenshot.

General Control

Inbound

Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

Outbound

Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

Content-Type Policy

Enable Content-Type Checks

☒

Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	

Finish

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS values used for compliance testing.

Signaling QoS			
Enabled <input checked="" type="checkbox"/>			
<input type="radio"/> ToS			
	Precedence	Routine	000
	ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP			
	Value	EF	101110
Finish			

7.3.4. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section.

This sample configuration, create a separate **Endpoint Policy Group** for the enterprise and the Broadconnect SIP Trunk.

To create a new policy group, navigate to **UC-Sec Control Center > Domain Policies > Endpoint Policy Groups** and click on **Add Group** (not shown).

7.3.4.1 Endpoint Policy Group for Broadconnect.

The following screen shows **Broadconnect_PolicyG** created for Broadconnect SIP Trunk. Set the **Application**, **Media** and **Signaling** rules to the ones previously created. Set the **Border**, and **Time of Day** rules to **default** and set the **Security** rule to **default-high**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar has 'End Point Policy Groups' selected. The main area displays the configuration for 'BroadConnect_PolicyG'. The table below shows the rules assigned to this policy group.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	BroadConnect_AppR	BroadConnect_BorderR	BroadConnect_MediaR	BroadConnect_SecR	BroadConnect_SigR	BroadConnect-ToDR

7.3.4.2 Endpoint Policy Group for Session Manager.

The following screen shows **SM_PolicyG** created for Session Manager. Set the **Application**, **Media** and **Signaling** rules to the ones previously created. Set the **Border**, and **Time of Day** rules to **default** and set the **Security** rule to **default-low**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar has 'End Point Policy Groups' selected. The main area displays the configuration for 'SM_PolicyG'. The table below shows the rules assigned to this policy group.

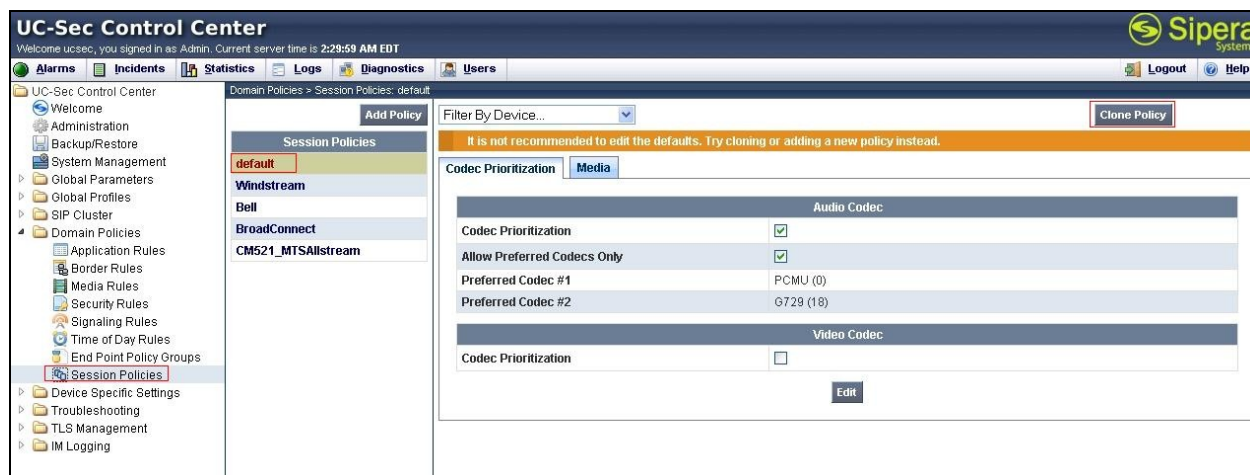
Order	Application	Border	Media	Security	Signaling	Time of Day
1	BroadConnect_AppR	default	BroadConnect_MediaR	default-med	BroadConnect_SigR	default

7.3.5. Session Policy

The Session Policy applies based on the source and destination of a media session. e.g. which codec to be applied to the media session between its source and destination. The source and destination are defined in URI Group in **Section 7.2.1**.

In this sample configuration, the Session Policy named Broadconnect is created to match to codec configuration on Broadconnect SIP Trunk. The policy also allows Avaya SBCE to anchor media, which is used for off-net call transfer scenarios.

Clone and modify the default Session Policy to apply for both enterprise and Broadconnect. To clone a Session Policy, navigate to **UC-Sec Control Center > Domain Policies > Session Policies**. With the **default** rule chosen, click on **Clone Rule** as shown below.



Enter a descriptive name **Broadconnect** for the new policy and click **Finish**.

Broadconnect supports voice codec G.729, G.711 in prioritized order with payload 101 for RFC2833/DTMF. To define **Codec Prioritize** for Audio Codec, select the profile **Broadconnect**, click on **Edit**. Then check the Codec Prioritization, select Preferred Codec #1 is G.711U, Preferred Codec #2 is G.729, Preferred Codec #3 is 101. Check on the checkbox of **Allow Preferred Codecs Only** is to prevent the unsupported codec from being sent to both ends.

This **Session Policy** prioritizes voice codec G.711 to establish the voice call. It is mandatory for a G.711 fax call can be successful because CM cannot switch the voice call using a different codec to G.711 for fax.

Codec Prioritization	
Audio Codec	
Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input checked="" type="checkbox"/>
Preferred Codec #1	PCMU (0) ▼
Preferred Codec #2	G729 (18) ▼
Preferred Codec #3	Dynamic (101) ▼
Preferred Codec #4	None ▼
Preferred Codec #5	None ▼
Video Codec	
Codec Prioritization	<input type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
Preferred Codec #1	CelB (25) ▼
Preferred Codec #2	None ▼
Preferred Codec #3	None ▼
Preferred Codec #4	None ▼
Preferred Codec #5	None ▼
Finish	

To enable **Media Anchoring** on Avaya SBCE, select **Session Policy Broadconnect** then select tab **Media**, click **Edit**. Check on **Media Anchoring**.

Media	
Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None ▼
Finish	

7.4. Device Specific Settings

The **Device Specific Settings** feature allows aggregate system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

7.4.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. This information populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center > Device Specific Settings > Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Device Specific Settings' expanded, showing 'Network Management' selected. The main content area is titled 'Device Specific Settings > Network Management: sipera'. It has two tabs: 'Network Configuration' and 'Interface Configuration'. The 'Interface Configuration' tab is active, displaying a table of IP addresses and their associated interfaces. A warning message at the top states: '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.' Below this, there are fields for 'A1 Netmask' (255.255.255.192), 'A2 Netmask', 'B1 Netmask' (255.255.255.224), and 'B2 Netmask'. The 'Add IP' button is visible. The table below has columns for 'IP Address', 'Public IP', 'Gateway', and 'Interface'. The first three rows are highlighted with red boxes.

IP Address	Public IP	Gateway	Interface
111.10.97.189		111.10.97.129	A1
111.10.98.98		111.10.98.97	B1
222.10.98.112		222.10.98.97	B1

Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click it's **Toggle State** button.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, Global Profiles, SIP Cluster, Domain Policies, and Device Specific Settings. Under Device Specific Settings, 'Network Management' is expanded, and 'Interface Configuration' is selected. The main pane displays a table of network interfaces for the device 'sipera'.

Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

7.4.2. Media Interface

The **Media Interface** screen is where the media ports are defined. Avaya SBCE will listen for RTPs on the defined ports.

Create a **Media Interface** for both the inside and outside IP interfaces.

To create a new **Media Interface**, navigate to **UC-Sec Control Center > Device Specific Settings > Media Interface** and click **Add Media Interface**.

The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces.

Notes: After the media interfaces are created, an application restart is necessary before the changes will take effect.

The screenshot shows the UC-Sec Control Center interface with the 'Media Interface' tab selected. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below the warning is a table of media interfaces for the device 'sipera'.

Name	Media IP	Port Range	
InsideMedia	111.10.97.189	35000 - 40000	✎ ✕
OutsideMedia_SBCE	122.10.98.112	35000 - 40000	✎ ✕
OutsideMedia	111.10.98.98	35000 - 40000	✎ ✕

7.4.3. Signaling Interface

The **Signaling Interface** screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports.

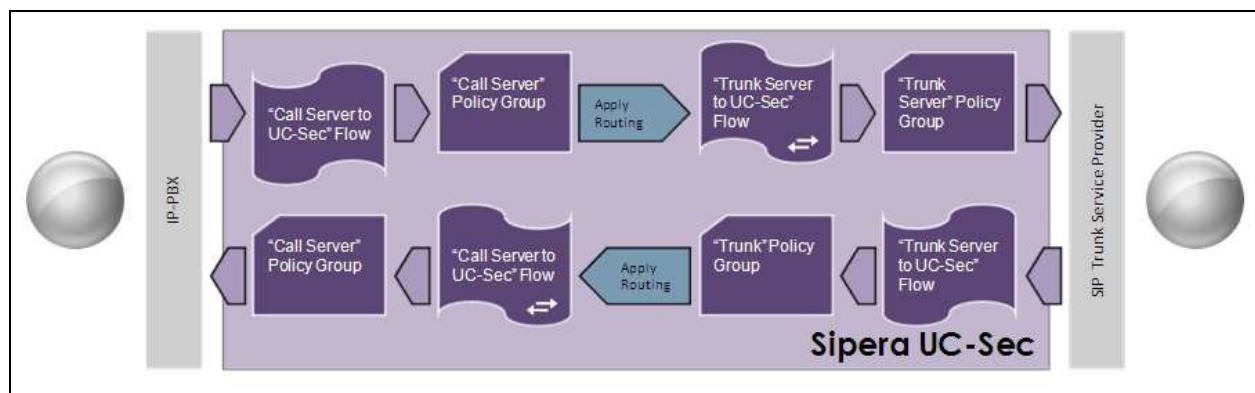
Create a **Signaling Interface** for both the inside and outside IP interfaces. To create a new **Signaling Interface**, navigate to **UC-Sec Control Center > Device Specific > Settings > Signaling Interface** and click **Add Signaling Interface**.

The following screen shows the signaling interfaces created in the sample configuration with TCP and UDP ports 5060 used for the inside and outside IP interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	111.10.97.189	5060	5060	---	None	
OutsideSIP_SBCE	222.10.98.112	5060	5060	---	None	
OutsideSIP	222.10.98.98	5060	5060	---	None	
InsideSIP_TCP_5080	111.10.97.189	5080	---	---	None	
InsideSIP_TCP_5090	111.10.97.189	5090	---	---	None	

7.4.4. End Point Flows - Server Flow

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through Avaya SBCE to secure a SIP Trunk call.



Create a separate Server Flow for Session Manager and the Broadconnectd SIP Trunk.

To create a Server Flow, navigate to **UC-Sec Control Center > Device Specific Settings > End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown).

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.6** to assign to the Flow.
- **URI Group:** Select the URI Group created in **Section 7.2.1** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration.
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration.
- Click **Finish** to save and exit.

The following screen shows the **Sever Flow** named **Broadconnect** for Broadconnect.

Edit Flow: Broadconnect	
Criteria	
Flow Name	Broadconnect
Server Configuration	Broadconnect
URI Group	CM_Broadconnect
Transport	*
Remote Subnet	*
Received Interface	InsideSIP
Signaling Interface	OutsideSIP_SBCE
Media Interface	OutsideMedia_SBCE
End Point Policy Group	BroadConnect_PolicyG
Routing Profile	To_SM_fr_BroadConnec
Topology Hiding Profile	To_BroadConnect
File Transfer Profile	None
Finish	

The following screen shows the **Sever Flow** named **SM** for Session Manager.

Criteria	
Flow Name	SM_to_BroadConnect
Server Configuration	SM
URI Group	CM_Broadconnect
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_SBCE
Signaling Interface	InsideSIP
Media Interface	InsideMedia
End Point Policy Group	CMBell_PolicyG
Routing Profile	To_BroadConnect
Topology Hiding Profile	To_SM_fr_BroadC
File Transfer Profile	None
<input type="button" value="Finish"/>	

7.4.5. Session Flow

The **Session Flows** features allow to define certain parameters that pertain to the media portions of a call, whether it originates from within the enterprise or from without. These features provide the complete and unparalleled flexibility to monitor, identify, and control very specific types of calls based upon these user-definable parameters. **Session Flows** profiles SDP media parameters, to completely identify and characterize a call placed through the network.

Create a common **Session Flow** for both enterprise and the Broadconnectd SIP Trunk.

To create a **Session Flow**, navigate to **UC-Sec Control Center > Device Specific Settings > Session Flows**. Click **Add Flow** (not shown).

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Flow Name:** Enter a descriptive name.
- **URI Group #1:** Select the URI Group created in **Section 7.2.1** to assign to the Flow as the source URI Group.
- **URI Group #2:** Select the URI Group created in **Section 7.2.1** to assign to the Flow as the destination URI Group.
- **Session Policy:** Select the Session Policy created in **Section 7.3.5** to assign to the Flow.

Click **Finish** to save and exit.

Notes: A unique URI Group was used for source and destination, since it contains multiple URIs defined for the source as well as the destination.

The following screen shows the **Session Flow** named **Broadconnect** was created.

Criteria	
Flow Name	BroadConnect
URI Group #1	CM_Broadconnect ▼
URI Group #2	CM_Broadconnect ▼
Subnet #1	* Ex: 192.168.0.1/24
Subnet #2	* Ex: 192.168.0.1/24
Session Policy	BroadConnect ▼

Finish

8. Configure Broadconnect SIP Trunking

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

- IP address of the Broadconnect SIP proxy.
- Broadconnect SIP domain.
- CPE SIP domain.
- User and password for Digest Authentication.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.

The sample configuration between Broadconnect and the enterprise for the compliance test is a static configuration. There is no registration of the SIP trunk or enterprise users to the Broadconnect network.

9. Verification Steps

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

Verification Steps:

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

Protocol Traces:

The following SIP headers are inspected using Wireshark traces:

- RequestURI: verify the request number and either SIP domain
- From: verify the display name and display number.
- To: verify the display name and display number.
- History-Info: verify the call forward information and reason code.
- P-Assert-Identity: verify the display name and display number.
- Privacy: verify the "user, id" masking.

The following attributes in SIP message body are inspected using Wireshark traces:

- Connection Information (c): verify IP address of far end endpoint
- Time Description (t): verify session timeout of far end endpoint
- Media Description (m): verify audio port, codec, DTMF event description
- Media Attribute (a): verify specific audio port, codec, ptime, send/ receive ability, DTMF event and fax attributes.

Troubleshooting:

1. Avaya SBCE:
 - Using a network sniffing tool (e.g., Wireshark), monitor the SIP signaling messages between Broadconnect and Avaya SBCE.
 - Verify the SIP signaling message exchanges for Digest Authentication:
 - Broadconnect SIP Trunking service returned a **401 Unauthorized** status message to the initial INVITE from the Avaya SBCE. The 401 message contained a **WWW-Authenticate** Header posing challenge for Digest Authentication.

Example of **WWW-Authenticate** Header:

```
WWW-Authenticate: DIGEST  
qop="auth", nonce="BroadWorksXh0e4vu4oTvvk3z3BW", realm="BroadWo  
rks", algorithm=MD5
```

- Avaya SBCE ACKed the above 401 message, and then presented the Digest Authentication response by sending a second INVITE that contained an **Authorization** Header supplying the information for successful Digest Authentication. Note the username as configured in **Section 7.2.6.1**.

Example of **Authorization** Header:

```
Authorization: Digest username="4167758782",
realm="BroadWorks",
nonce="BroadWorksXh0e4vu4oTvkv3z3BW",
uri="sip:208.113.62.151",
response="906d631c91b62af658bac1ec07c4463d", algorithm=MD5,
cnonce="0a4f113b", qop=auth, nc=00000001
```

- Broadconnect SIP Trunking service returned **100 Trying** and subsequent 18X call ringing or session progress messages signaling normal call progression.

2. Communication Manager:

- **list trace station** <extension number> - Traces calls to and from a specific station.
- **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
- **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
- **status trunk** <trunk group number> - Displays trunk group information.
- **status trunk** <trunk group number/channel number> - Displays signaling and media information for an active trunk channel.

3. Session Manager:

- **System State** – Navigate to **Home** → **Elements** → **Session Manager**, as shown below. Verify that a green check mark is placed under **Tests Pass** and the **Service State** is **Accept New Service**.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Home

Home / Elements / Session Manager - Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State Shutdown System As of 3:29 AM

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
DevaSM	Core	22111/2169/2003	✓	Up	Accept New Service	11/37	0	9	6.1.1.0.611023

Select : All, None

- **traceSM -x** – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.

- Call Routing Test - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to Home → Elements → Session Manager → System Tools → Call Routing Test. Enter the requested data to run the test.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller for Enterprise 4.0.5 to the Broadconnect SIP Trunking service. Broadconnect SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Broadconnect SIP Trunking provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

All of the test cases have been executed. Noting the observations seen during testing as described in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The Broadconnect SIP Trunking service is considered **compliant** with Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller for Enterprise 4.0.5.

11. Additional 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 6.03, February 2011.
- [2]Administering Avaya Aura® System Platform, Release 6, June 2010.
- [3]Installing and Configuring Avaya Aura® Communication Manager, Release 6.0 June, 2010, Document Number 03-603558
- [4]Administering Avaya Aura® Communication Manager, Release 6.0, June 2010, Document Number 03-300509.
- [5]Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.0, June 2010, Document Number 555-245-205.
- [6]Installing and Upgrading Avaya Aura® System Manager, Release 6.1, November 2010.
- [7]Installing and Configuring Avaya Aura® Session Manager, Release 6.1, April 2011, Number 03-603473.
- [8]Administering Avaya Aura® Session Manager, Release 6.1, May 2011, Document Number 03-603324.
- [9]UC-Sec Install Guide (102-5224-400v1.01)
- [10]UC-Sec Administration Guide (010-5423-400v106)
- [11]Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide, Release 3.1, November 2009, Document Number 16-300698.
- [12]Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.6, June 2010, Document Number 16-601944.
- [13]Administering Avaya one-X® Communicator, April 2011.
- [14]Using Avaya one-X® Communicator, April 2011.
- [15]RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>
- [16]RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, <http://www.ietf.org/>

©2012 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.