



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Border Controller 6.0 and Avaya Aura® Session Manager 6.1 with Qwest iQ® SIP Trunk (version 6.5.7R1) – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Qwest iQ® SIP Trunk (version 6.5.7R1) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 5.2.1, Avaya Aura Session Manager 6.1 and Avaya Aura® Session Border Controller 6.0 (SBC) with various Avaya endpoints.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Solutions and Interoperability Test Lab, utilizing Qwest iQ® SIP Trunk Services.

TABLE OF CONTENTS

1.	Introduction	4
1.1.	Interoperability Compliance Testing.....	4
1.2.	Support	5
1.3.	Test Results / Known Limitations	5
2.	Reference Configuration	7
2.1.	Interoperability Compliance Testing.....	7
3.	Equipment and Software Validated	8
4.	Configure Communication Manager	9
4.1.	Licensing and Capacity	9
4.2.	System Features.....	10
4.3.	IP Node Names	11
4.4.	Codecs	11
4.5.	IP Network Region	12
4.6.	Signaling Group.....	13
4.7.	Trunk Group	15
4.8.	Calling Party Information	17
4.9.	Outbound Routing	18
4.10.	Incoming Call Handling Treatment.....	21
5.	Configure Avaya Aura® Session Manager	22
5.1.	System Manager Login and Navigation	22
5.2.	Specify SIP Domain	23
5.3.	Add Location	25
5.4.	Add Adaptation Module	26
5.5.	Add SIP Entities	27
5.6.	Add Entity Links	30
5.7.	Add Routing Policies	32
5.8.	Add Dial Patterns	33
5.9.	Add/View Session Manager	36
6.	Avaya Aura SBC Configuration	38
6.1.	Initial Installation	38
6.1.1.	Network Settings.....	41
6.1.2.	Logins	42
6.1.3.	VPN Access	42
6.1.4.	SBC	43
6.1.5.	Confirm Installation.....	47
6.1.6.	Verify Installation	49
6.2.	Post Installation Configuration	51
6.2.1.	Add Additional SIP Gateways	51
6.2.2.	Blocked Headers	63
6.2.3.	Third Party Call Control.....	65
6.2.4.	Save the Configuration	65
7.	Qwest iQ® SIP Trunk Configuration	66
8.	General Test Approach and Test Results.....	66

9. Verification and Troubleshooting	66
10. Conclusion	67
11. References	67
Appendix A: Avaya Aura® SBC Configuration File	68

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Qwest iQ® SIP Trunk (version 6.5.7R1) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller (AA-SBC) 6.0, Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager 5.2.1 and various Avaya endpoints.

The Qwest iQ® SIP Trunk service referenced within these Application Notes is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

Qwest iQ® SIP Trunk will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE). SIP Trunk will also offer remote DID capability for a customer wishing to offer local numbers to their customers that can be aggregated in SIP format back to customer.

1.1. Interoperability Compliance Testing

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

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

- Incoming PSTN calls to various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from the Avaya one-X® Communicator (1XC) soft phone (H.323 version).
- 1XC supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. 1XC also supports two versions with different firmware (H.323 and SIP). Both versions of 1XC were tested.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411), emergency assistance (911), etc.
- Codecs G.711MU, G.729A and G.729AB.

- T.38 Fax
- DTMF tone transmissions passed out-band RTP events as per RFC 2833.
- Calling number presentation and calling number restriction.
- Voicemail navigation using DTMF for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection using SIP REFER for call transfer of inbound back to PSTN.
- Network Call Redirection of inbound call back to PSTN from Communication Manager vector.

1.2. Support

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

For technical support on the Qwest iQ® SIP Trunk services, contact Customer Service at <http://www.qwest.com/business/products/products-and-services/voip-adv-voice/sip-trunk.html>. Enter your phone number and click “Speak to us now” and Customer Service will call you or select the “Email us” link to send an e-mail inquiry or click “Contact a rep” and fill in the request information.

Note: CenturyLink acquired Qwest in April 2011. Over time Qwest branded services and web sites may be renamed by CenturyLink.

1.3. Test Results / Known Limitations

Interoperability testing of Qwest iQ® SIP Trunk (version 6.5.7R1) was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **No Error Indication if No Matching Codec Offered on Inbound Calls:** If the Communication Manager SIP trunk is improperly configured to have no matching codec with the service provider and an inbound call is placed, the service provider only returns a “488 Not Acceptable Here” response and the caller will hear a fast busy after 30 seconds. Codecs are normally agreed to upon turn-up so this condition should be discovered at that time.
- **No Error Indication if No Matching Codec Offered on Outbound Calls:** If the Communication Manager SIP trunk is improperly configured to have no matching codec with the service provider and an outbound call is placed, the service provider only returns a “487 Request Terminated” response. The caller will hear a fast busy and the called party will hear one ring before the call is terminated. Codecs are normally agreed to upon turn-up so this condition should be discovered at that time.

- **No Support for G.729B:** Qwest iQ® SIP Trunk does not support G.729B codec.
- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/Qwest SIP Trunk solution. It is listed here simply as an observation.
- **All Trunks Busy will ring from 7 – 40 seconds before fast busy:** When all Communication Manager trunk-group members are busy, the caller will hear ringing for anywhere from 7 seconds to 40 seconds before finally hearing a fast busy. Qwest iQ® SIP Trunk will send the call to the Avaya Communication Manager and it will return a “500 Service Unavailable” instead of a “503 Service Unavailable”. This only happens on the first call in after the trunk is busy. After the first call, the Avaya Communication Manager returns “403 Forbidden”. The workaround for this is to upgrade to one of the following loads: CM 5.2.1 SP9, CM 6.0.1 SP3, CM 6.2. Use of a 503 allows for a back-off time period and a retry by Qwest.
- **SIP Network REFER to an off-net extension is not supported:** When a Communication Manager vector is programmed to redirect an inbound call to a PSTN number after the call is answered by an announcement, Qwest iQ® SIP Trunk will send a “202 Accepted” to the REFER SIP message and the call will drop. Qwest iQ® SIP Trunk does not support REFER messages.
- **Network Call Redirection:** When a Communication Manager vector is programmed to redirect an inbound call to a PSTN number before answering the call in the vector, Qwest iQ® SIP Trunk will send an ACK to the “302 Moved Temporarily” SIP message from the enterprise but will not redirect the call to the new party in the Contact header of the 302 message. The inbound call initiator hears a recording from Qwest in this failure scenario.
- **SIP REFER with transfer (consultative or blind) is not supported in Qwest iQ® SIP Trunk (version 6.5.7R1):** When an extension receives a call from a PSTN number and attempts to transfer (either consultative or blind) the call to another PSTN extension, the call will initially connect and then will be dropped as soon as the transfer is completed on the enterprise user’s side. This is addressed in a future Qwest iQ® SIP Trunk release, meanwhile the work-around is to have the **Network Call Redirection** field to **n** on page 4 of the trunk group form, refer to **Section 5.7**.

2. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the Qwest iQ® SIP Trunk. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an SBC provides NAT functionality and SIP header manipulation. The SBC receives traffic from Qwest iQ® SIP Trunk on port 5060 and sends traffic to the Qwest iQ® SIP Trunk using destination port 5060, using the UDP protocol.

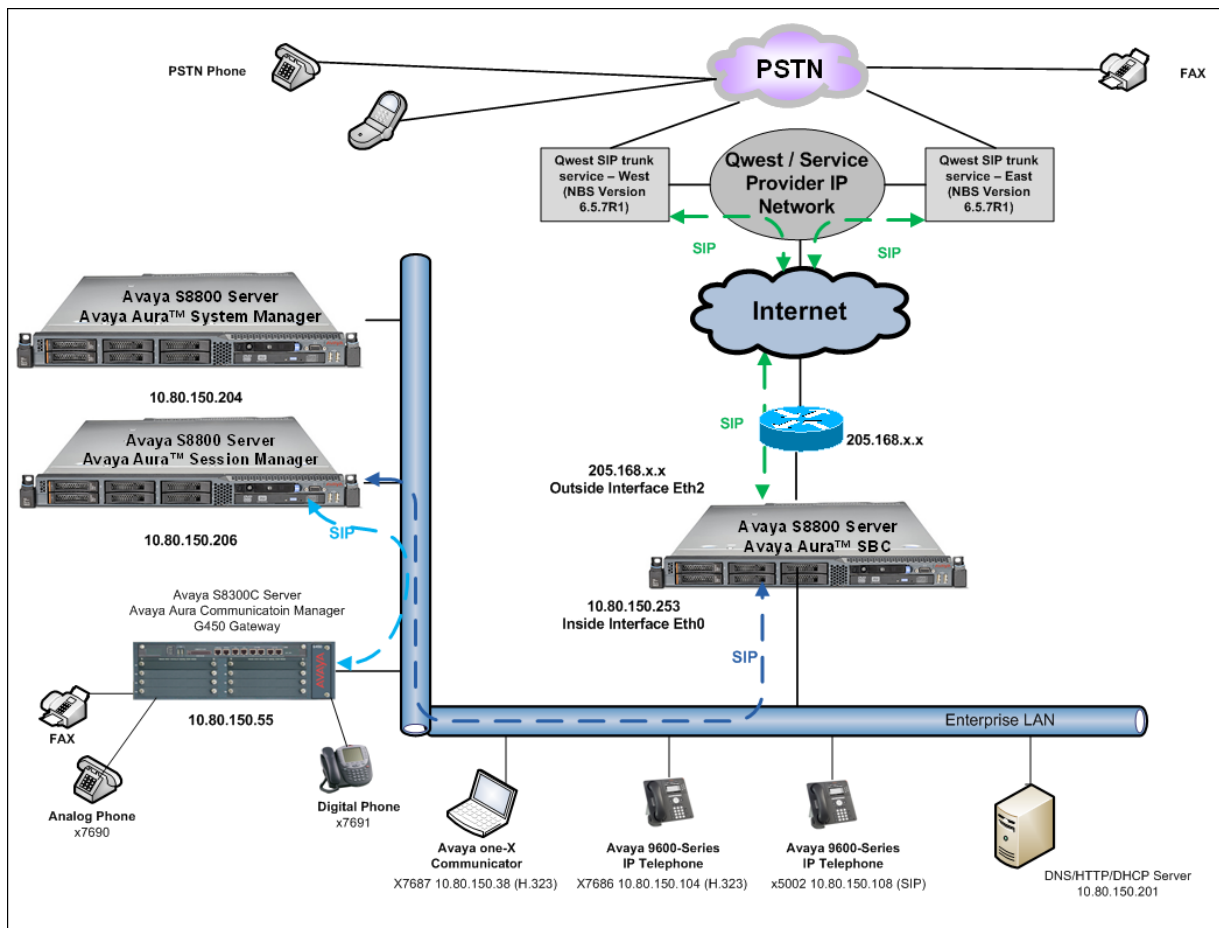


Figure 1: Avaya Interoperability Test Lab Configuration

2.1. Interoperability Compliance Testing

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

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

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

3. Equipment and Software Validated

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

Equipment:	Software:
Avaya Aura® Communication Manager running on Avaya S8300c Server with Avaya G430 Media Gateway	5.2.1 SP8 (R015x.02.1.016.4)
Avaya Aura® Session Manager running on HP DL360 Server	6.1 SP2 (Build 6.1.2.0.612004)
Avaya Aura® System Manager running on HP DL360 Server	6.1 SP2 (Build 6.1.0.4.5072) Patch 6.1.5.1087
Avaya 9641G IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.010f
Avaya 9621G IP Telephone (SIP)	Avaya one-X® Deskphone SIP 6.0.0
Avaya 4625 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 2.5
Avaya 9600 Series IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.102S
Avaya one-X Communicator (H.323)	6.0 with SP1 (6.0.1.16)
Avaya 2420D Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Avaya Aura® Session Border Controller running on Avaya S8800 Server	6.0.0.1.5

4. Configure Communication Manager

This section describes the procedure for configuring Communication Manager for Qwest iQ® SIP Trunk. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Qwest iQ® SIP Trunk. It is assumed the general installation of Communication Manager and Avaya G430 Media Gateway has been previously completed and is not discussed here.

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

4.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 450 SIP trunks are available and 20 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
	Maximum Administered H.323 Trunks:	450	18	
	Maximum Concurrently Registered IP Stations:	450	4	
	Maximum Administered Remote Office Trunks:	0	0	
	Maximum Concurrently Registered Remote Office Stations:	0	0	
	Maximum Concurrently Registered IP eCons:	68	0	
	Max Concur Registered Unauthenticated H.323 Stations:	450	0	
	Maximum Video Capable Stations:	450	0	
	Maximum Video Capable IP Softphones:	450	3	
	Maximum Administered SIP Trunks:	450	20	
	Maximum Administered Ad-hoc Video Conferencing Ports:	450	0	
	Maximum Number of DS1 Boards with Echo Cancellation:	80	0	
	Maximum TN2501 VAL Boards:	0	0	
	Maximum Media Gateway VAL Sources:	50	1	
	Maximum TN2602 Boards with 80 VoIP Channels:	0	0	
	Maximum TN2602 Boards with 320 VoIP Channels:	0	0	
	Maximum Number of Expanded Meet-me Conference Ports:	300	0	

4.2. System Features

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

```
change system-parameters features                               Page 1 of 18
                        FEATURE-RELATED SYSTEM PARAMETERS
                        Self Station Display Enabled? n
                        Trunk-to-Trunk Transfer: all
                        Automatic Callback with Called Party Queuing? n
Automatic Callback - No Answer Timeout Interval (rings): 3
                        Call Park Timeout Interval (minutes): 10
                        Off-Premises Tone Detect Timeout Interval (seconds): 20
                        AAR/ARS Dial Tone Required? y
```

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

```
change system-parameters features                               Page 9 of 18
                        FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

4.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the S8300 server's Processor Ethernet (procr) and for the Session Manager SM100 interface. These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip
```

Name	IP Address
ASM	10.80.150.206
CMM	10.80.150.56
default	0.0.0.0
procr	10.80.150.55

4.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, codecs G.729A and G.711MU were tested using ip-codec-set 2. To use these codecs, enter **G.729A** and **G.711MU** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields. Silence suppression is normally set to **n** and packet size is standard at **20ms**.

```
change ip-codec-set 2
```

Page 1 of 2

IP Codec Set

Codec Set: 2

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

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

```
change ip-codec-set 2
```

Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

	Mode	Redundancy
FAX	t.38-standard	0
Modem	pass-through	0
TDD/TTY	US	3
Clear-channel	n	

4.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 10 was chosen for the service provider trunk. Use the **change ip-network-region 10** command to configure region 10 with the following parameters:

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

```
change ip-network-region 10                                     Page 1 of 19
                                                                IP NETWORK REGION
Region: 10
Location: 1      Authoritative Domain: sip.avaya.com
Name: SIP Trunks
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 2          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? y
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS      RTCP Reporting Enabled? y
Call Control PHB Value: 46    RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46          Use Default Server Parameters? y
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS          RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

On **Page 3**, define the IP codec set to be used for traffic between region 10 and any other regions that are in use. Enter the desired IP codec set in the **codec set** column of the row with destination regions (**dst rgn**) 1 and 2. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls in region 10 (the service provider region) region 1 (the enterprise side) and region 2 (the IP phones). Creating this table entry for ip-network-region 1 will automatically create a complementary table entry on the ip-network-region 1 and 2 forms for destination region 10.

change ip-network-region 10										Page	3 of 19
Source Region: 10 Inter Network Region Connection Management										I	M
										G	A
dst	codec	direct	WAN-BW-limits		Video		Intervening		Dyn	A	G
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L
1	2	y	NoLimit							n	t
2	2	y	NoLimit							n	t
3											
4											
5											
6											
7											
8											
9											
10	2									all	
11											
12											
13											
14											
15											

4.6. Signaling Group

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

- Set the **Group Type** field to *sip*.
- Set the **Transport Method** to the recommended default value of *tls* (Transport Layer Security). For ease of troubleshooting during testing, part of 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.
- 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 and for TCP the well-known port value is 5060). The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5070**.
- Set the **Near-end Node Name** to *procr*. This node-name maps to the IP address of the S8300C as defined in the **node-names ip** screen shot in **Section 4.3**.

- Set the **Far-end Node Name** to *ASM*. This node name maps to the IP address of the Session Manager SM100 interface as defined in the **node-names-ip** screen shot in **Section 4.3**.
- Set the **Far-end Network Region** to the IP network region for the service provider in **Section 4.5**.
- Set the **Far-end Domain** to *qwest.com*. Communication Manager identifies incoming calls based on the P-Asserted Identity's host name, matching the value entered here. It is also used to populate the host field in the "To" header for outgoing calls.
- 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.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to *5*. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

change signaling-group 2		Page 1 of 1
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
IP Video? n		
Near-end Node Name: procr	Far-end Node Name: ASM	
Near-end Listen Port: 5070	Far-end Listen Port: 5070	
	Far-end Network Region: 10	
Far-end Domain: qwest.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 5	

4.7. Trunk Group

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

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

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: Qwest	COR: 1	TN: 1	TAC: *102
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Signaling Group: 2	
		Number of Members: 10	

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value comparable to the **Alternate Route Timer** on the signaling group form described in **Section 4.6**.

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

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

On **Page 3**, make sure the **Numbering Format** field is set to *public*. Set the **Replace Restricted Numbers?** and the **Replace Unavailable Numbers?** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 4.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

add trunk-group 2	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: public	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y

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

Set the **Telephone Event Payload Type** to **100**, the value preferred by Qwest iQ® SIP Trunk.

change trunk-group 2	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: 100	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Enable Q-SIP? n	

4.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 4.7**), use the **change public-numbering** command to create an entry for the DID range assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension. It is used to authenticate the caller.

In the sample configuration, Extensions were created matching the last 4 digits of the DID block. There is also extension numbers starting with a 4 and 5 that were mapped to the lead DID number as shown in **Figure 1**.

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	4	2	3035557686	10	Total Administered: 7
4	4	99		4	Maximum Entries: 240
4	5	2	3035557686	10	
4	5	99		4	
4	7	99		4	
4	76	2	303555	10	
4	5002	2	3035557692	10	

4.9. Outbound Routing

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

change dialplan analysis							Page 1 of 12		
DIAL PLAN ANALYSIS TABLE									
Location: all							Percent Full: 1		
	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1		3	dac						
2		4	ext						
4		4	ext						
5		4	ext						
6		4	ext						
7		4	ext						
8		1	fac						
9		1	fac						
*		4	dac						
#		4	fac						

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

change feature-access-codes		Page 1 of 9
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code: #110		
Abbreviated Dialing List2 Access Code: #111		
Abbreviated Dialing List3 Access Code: #112		
Abbreviated Dial - Prgm Group List Access Code: #113		
Announcement Access Code: #114		
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:		

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

change ars analysis 1							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
12	11	11	2	fnpa		n	
13	11	11	2	fnpa		n	
14	11	11	2	fnpa		n	
15	11	11	2	fnpa		n	
16	11	11	2	fnpa		n	
17	11	11	2	fnpa		n	
18	11	11	2	fnpa		n	
19	11	11	2	fnpa		n	
1xxx976	11	11	deny	fnpa		n	
303	10	10	2	hnpa		n	
411	3	3	2	svcl		n	
720	10	10	2	hnpa		n	
911	3	3	2	svcl		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 2 during the compliance test.

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

change route-pattern 2													Page	1 of	3
Pattern Number: 2													Pattern Name: Outbound 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:	2	3			1								n	user	
2:													n	user	
3:													n	user	
4:													n	user	
5:													n	user	
6:													n	user	
BCC		VALUE		TSC	CA-TSC	ITC		BCIE	Service/Feature	PARM	No.	Numbering	LAR		
0	1	2	M	4	W	Request					Dgts	Format			
										Subaddress					
1:	y	y	y	y	y	n	n	rest				none			
2:	y	y	y	y	y	n	n	rest				none			
3:	y	y	y	y	y	n	n	rest				none			

Use the **change ars digit-conversion** command to manipulate the routing of dialed digits that match the DID's to prevent the calls from going out the PSTN and routing to the proper extension. The example below shows the toll-free number being converted to a VDN and the DID block being converted to the extensions matching the last 4 digits.

change ars digit-conversion 0						Page	1 of	2
ARS DIGIT CONVERSION TABLE								
Location: all						Percent Full: 0		
Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI	Req
18775550751	11	11	11	7695	ext	y		n
3035557686	10	10	6		ext	y		n
3035557687	10	10	6		ext	y		n
3035557688	10	10	6		ext	y		n
3035557689	10	10	6		ext	y		n
303555769	10	10	6		ext	y		n
								n
								n
								n
								n
								n
								n

4.10. Incoming Call Handling Treatment

In general, the “incoming call handling treatment” for a trunk group can be used to manipulate the digits received for an incoming call if necessary. The toll-free number sent by Qwest iQ® SIP Trunk can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of toll-free number 8775550751 to extension 7695. It also shows the range of DID's being converted to 4 digit extensions.

change inc-call-handling-trmt trunk-group 2					Page	1 of	3
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del	Insert			
public-ntwrk	10	3035557692	10	5002			
public-ntwrk	10	6515555198	10	5002			
public-ntwrk	10	6785559410	10	7686			
public-ntwrk	10	8775550751	10	7695			
public-ntwrk	10	30355576	6				
public-ntwrk							
public-ntwrk							
public-ntwrk							
public-ntwrk							
public-ntwrk							
public-ntwrk							
public-ntwrk							

5. Configure Avaya Aura® Session Manager

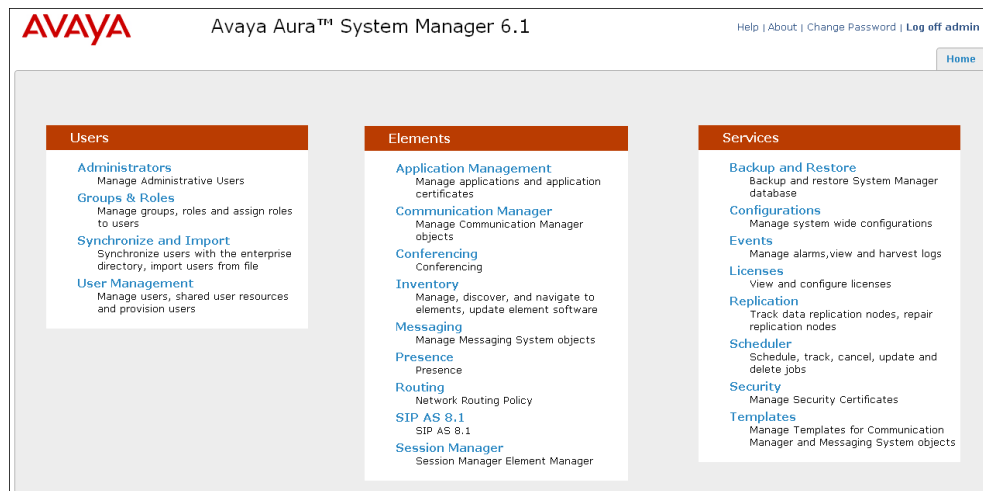
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

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

5.1. System Manager Login and Navigation

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



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

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

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

Routing x Home

Home / Elements / Routing - Introduction to Network Routing Policy Help ?

Introduction to Network Routing Policy

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

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

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers
- Step 7: Create "Routing Policies"
 - Assign the appropriate "Routing Destination" and "Time Of Day"
 - (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
- Step 8: Create "Dial Patterns"

5.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware of in order to route calls. For the compliance test, this includes the enterprise domain (*sip.avaya.com*) and the Qwest iQ® SIP trunk domain (*qwest.com*). Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

Home / Elements / Routing / Domains - Domain Management Help ?

Domain Management Commit Cancel

1 Item | Refresh Filter: Enable

Name	Type	Default	Notes
* qwest.com	sip	<input type="checkbox"/>	Qwest SIP Trunk

* Input Required Commit Cancel

The screen below shows both the enterprise domain and the Qwest domain after they have been created.

Home / Elements / Routing / Domains - Domain Management				
Domain Management				Help ?
<div>EditNewDuplicateDeleteMore Actions</div>				
2 Items RefreshFilter: Enable				
<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	qwest.com	sip	<input type="checkbox"/>	Qwest SIP Trunk
<input type="checkbox"/>	sip.avaya.com	sip	<input type="checkbox"/>	
Select : All, None				

5.3. Add Location

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

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

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

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

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

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

The screenshot shows the Avaya Aura™ System Manager 6.1 web interface. The left navigation pane is expanded to 'Routing' > 'Locations'. The main content area is titled 'Location Details' and shows the configuration for a location named 'Westminster'. The 'General' section has 'Name' set to 'Westminster'. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' as 'Kbit/sec' and 'Total Bandwidth' as an empty field. The 'Per-Call Bandwidth Parameters' section shows 'Default Audio Bandwidth' as '80 Kbit/sec'. The 'Location Pattern' section shows a table with one item: '10.80.*'. The 'Add' button is visible, and the 'Commit' button is at the bottom right.

IP Address Pattern	Notes
10.80.*	

Note: that call bandwidth management parameters should be set per customer requirement.

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

The screenshot displays the 'Locations- Location Details' configuration page. The left sidebar shows a navigation menu with 'Routing' selected. The main content area has a breadcrumb trail 'Home / Elements / Routing / Locations- Location Details'. Below this, there's a 'Location Details' section with a 'Commit' button and a 'Help' link. A message states: 'Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting'. The 'General' section contains a 'Name' field with 'AA-SBC' and a 'Notes' field with 'Aura SBC for Qwest SIP Trunks'. The 'Overall Managed Bandwidth' section has 'Managed Bandwidth Units' set to 'Kbit/sec' and an empty 'Total Bandwidth' field. The 'Per-Call Bandwidth Parameters' section has 'Default Audio Bandwidth' set to '80 Kbit/sec'. The 'Location Pattern' section has an 'Add' button and a table with one item: 'IP Address Pattern' with value '10.80.150.253' and 'Notes' with value 'Aura SBC For Qwest'. At the bottom, there's a 'Select : All, None' option and a '* Input Required' message. 'Commit' and 'Cancel' buttons are at the bottom right.

5.4. Add Adaptation Module

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

For Qwest iQ® SIP Trunk interoperability, one Adaptation is needed and maps inbound DID numbers from Qwest SIP Trunk to local Communication Manager extensions. The adaptation will later on be applied to the AA-SBC SIP Entity.

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

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

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter ***DigitConversionAdapter***.
- **Module parameter:** Enter ***iosrcd=qwest.com***. This setting adapts the incoming call (i.e., from SBC to Session Manager) destination domain to the

domain expected by Communication Manager in the sample configuration.

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

5.5. Add SIP Entities

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

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

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

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

The screenshot shows the 'SIP Entity Details' configuration page for a 'Session Manager' entity. The left sidebar lists navigation options: Routing, 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 'General'. It contains the following fields:

- Name:** ASM
- FQDN or IP Address:** 10.80.150.206
- Type:** Session Manager (dropdown)
- Notes:** Session Manager
- Location:** Westminster (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** America/Denver (dropdown)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

Below the main configuration area, there is a section for 'SIP Link Monitoring'.

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

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

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

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

The screenshot shows the 'Port' configuration section. It includes an 'Add' button and a 'Remove' button. Below them is a table with 3 items. The table has columns: Port, Protocol, Default Domain, and Notes. The 'Filter' is set to 'Enable'. The table contains three rows of data:

Port	Protocol	Default Domain	Notes
5060	UDP	sip.avaya.com	
5060	TCP	sip.avaya.com	
5061	TLS	sip.avaya.com	

Below the table, there is a 'Select' dropdown set to 'All, None'. At the bottom, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

The following screen shows the addition of Communication Manager. The **FQDN or IP Address** field is set to the IP address of the Processor Ethernet Interface of the Communication Manager S8300.

The screenshot displays the 'SIP Entity Details' configuration page. On the left is a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail: Home / Elements / Routing / SIP Entities - SIP Entity Details. Below this, the 'SIP Entity Details' section is titled 'General'. The configuration fields are as follows:

- Name:** S8300c_CM521
- * FQDN or IP Address:** 10.80.150.55
- Type:** CM
- Notes:** S8300C CM 5.2.1
- Adaptation:** (empty dropdown)
- Location:** Westminster
- Time Zone:** America/Denver
- Override Port & Transport with DNS SRV:** ☐
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

There is also a link for 'SIP Link Monitoring' in the bottom left of the configuration area.

The following screen shows the addition of the AA-SBC SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). **Link Monitoring Enabled** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 5.4**.

The screenshot displays the 'SIP Entity Details' configuration page for 'AA-SBC01'. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is divided into two sections: 'General' and 'SIP Link Monitoring'. In the 'General' section, fields include Name (AA-SBC01), FQDN or IP Address (10.80.150.253), Type (SIP Trunk), Notes (Avaya Aura SBC to Qwest), Adaptation (SIP_Trunking_in_from_Qwest), Location (AA-SBC), Time Zone (America/Denver), and an unchecked checkbox for 'Override Port & Transport with DNS SRV'. The 'SIP Timer B/F (in seconds)' is set to 4. In the 'SIP Link Monitoring' section, 'SIP Link Monitoring' is set to 'Link Monitoring Enabled', 'Proactive Monitoring Interval (in seconds)' is 900, 'Reactive Monitoring Interval (in seconds)' is 120, and 'Number of Retries' is 1.

5.6. Add Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 4.6**.

- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 5.5**. For AA-SBC, select the AA-SBC SIP Entity defined in **Section 5.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 4.6**.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 5.5** will be denied.*

Click **Commit** to save.

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

Entity Link to Communication Manager:

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

1 Item Refresh Filter: E

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ASM_s8300c_CM521	* ASM	TCP	* 5070	* S8300c_CM521	* 5070	<input checked="" type="checkbox"/>	

* Input Required

Entity Link to the AA-SBC:

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

1 Item Refresh Filter: t

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ASM_AA-SBC01_506	* ASM	TCP	* 5060	* AA-SBC01	* 5060	<input checked="" type="checkbox"/>	

* Input Required

5.7. Add Routing Policies

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

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

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

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

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

The screenshot shows the 'Routing Policy Details' page for a policy named 'To_S8300c_CM521'. The left navigation pane is expanded to 'Routing Policies'. The 'General' section is active, showing the policy name, a 'Disabled' checkbox, and a 'Notes' field. The 'SIP Entity as Destination' section shows a 'Select' button. Below these sections is a table with the following data:

Name	FQDN or IP Address	Type	Notes
S8300c_CM521	10.80.150.55	CM	S8300C CM 5.2.1

The screenshot shows the 'Routing Policy Details' page for a policy named 'To_AA-SBC01'. The left navigation pane is expanded to 'Routing Policies'. The 'General' section is active, showing the policy name, a 'Disabled' checkbox, and a 'Notes' field. The 'SIP Entity as Destination' section shows a 'Select' button. Below these sections is a table with the following data:

Name	FQDN or IP Address	Type	Notes
AA-SBC01	10.80.150.253	SIP Trunk	Avaya Aura SBC to Qwest

5.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Qwest and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing** → **Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

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

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

Two examples of the dial patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other dial patterns (e.g., 011 international calls, 411 directory assistance calls, etc.), were similarly defined.

The first example shows that 11 digit dialed numbers that begin with 1 uses route policy *To_AA-SBC01*.

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

Dial Pattern Details Commit

General

* Pattern: 1

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: -ALL-

Notes: 1+ Dialing Outbound

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: E

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing P Notes
<input type="checkbox"/>	Westminster		To_AA-SBC01	0	<input type="checkbox"/>	AA-SBC01	

Select : All, None

The second example shows that inbound 10 digit numbers that start with *30355576* and originating from Location *AA-SBC* uses route policy *To_S8300c_CM521*. These are the DID numbers assigned to the enterprise from Qwest.

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

Dial Pattern Details Commit

General

* Pattern: 30355576

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: DID Inbound to CM

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter:

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Notes
<input type="checkbox"/>	AA-SBC	Aura SBC for Qwest SIP Trunks	To_S8300c_CM521	0	<input type="checkbox"/>	S8300c_CM521	

Select : All, None

The screen below shows a list of dial patterns used for the compliance test.

<div>Routing</div> <div>Domains</div> <div>Locations</div> <div>Adaptations</div> <div>SIP Entities</div> <div>Entity Links</div> <div>Time Ranges</div> <div>Routing Policies</div> <div>Dial Patterns</div> <div>Regular Expressions</div> <div>Defaults</div>	Home / Elements / Routing / Dial Patterns - Dial Patterns						Help ?
	Dial Patterns						
	<div>Edit</div> <div>New</div> <div>Duplicate</div> <div>Delete</div> <div>More Actions</div>						
	12 Items Refresh						Filter: Enable
	<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
	<input type="checkbox"/>	0	1	36	<input type="checkbox"/>	-ALL-	0+ Dialing Outbound
	<input type="checkbox"/>	1	11	11	<input type="checkbox"/>	-ALL-	1+ Dialing Outbound
	<input type="checkbox"/>	303	10	10	<input type="checkbox"/>	-ALL-	Local area code 303 outbound
	<input type="checkbox"/>	30355576	10	10	<input type="checkbox"/>	-ALL-	DID Inbound to CM
	<input type="checkbox"/>	411	3	3	<input type="checkbox"/>	-ALL-	Special Service Outbound
	<input type="checkbox"/>	6515555198	10	10	<input type="checkbox"/>	-ALL-	RDID assigned for testing
	<input type="checkbox"/>	676	5	5	<input type="checkbox"/>	-ALL-	Endpoints on S8300D_CM601
	<input type="checkbox"/>	6785559410	10	10	<input type="checkbox"/>	-ALL-	RDID assigned for testing
	<input type="checkbox"/>	720	10	10	<input type="checkbox"/>	-ALL-	Local area code 720 outbound
	<input type="checkbox"/>	76	4	4	<input type="checkbox"/>	-ALL-	
	<input type="checkbox"/>	8775550751	10	10	<input type="checkbox"/>	-ALL-	Toll Free Inbound to CM
	<input type="checkbox"/>	911	3	3	<input type="checkbox"/>	-ALL-	Emergency
Select : All, None							

5.9. Add/View Session Manager

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

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

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

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

The screenshot shows 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 | Log off admin'. A breadcrumb trail indicates the current location: 'Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration'. The left sidebar contains a navigation menu with options like 'Session Manager', 'Dashboard', 'Session Manager Administration', 'Communication Profile Editor', 'Network Configuration', 'Device and Location Configuration', 'Application Configuration', 'System Status', and 'System Tools'. The main content area is titled 'View Session Manager' and includes a 'Return' button. Below this, there are tabs for 'General', 'Security Module', 'NIC Bonding', 'Monitoring', 'CDR', 'Personal Profile Manager (PPM)', 'Connection Settings', and 'Event Server'. The 'General' tab is active, showing the following configuration details:

SIP Entity Name	ASM
Description	
Management Access Point Host Name/IP	10.80.150.205
Direct Routing to Endpoints	Enable

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

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

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

The screenshot displays a web-based configuration interface for the 'Security Module'. The interface has a breadcrumb trail: 'System Tools' > 'Security Module'. Below the breadcrumb, there is a list of configuration fields for a Session Manager entity. The fields and their values are as follows:

Field	Value
SIP Entity IP Address	10.80.150.206
Network Mask	255.255.255.0
Default Gateway	10.80.150.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

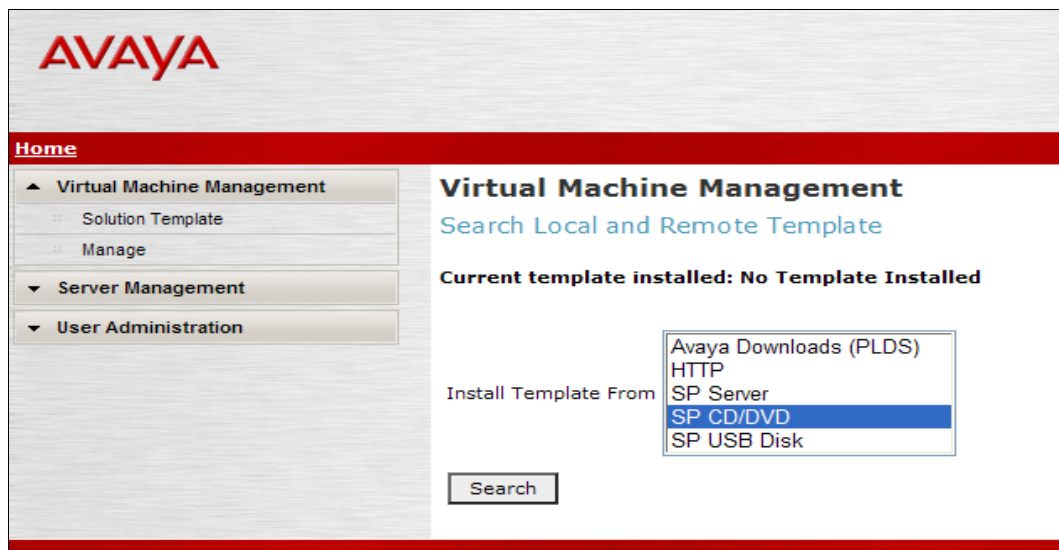
6. Avaya Aura SBC Configuration

6.1. Initial Installation

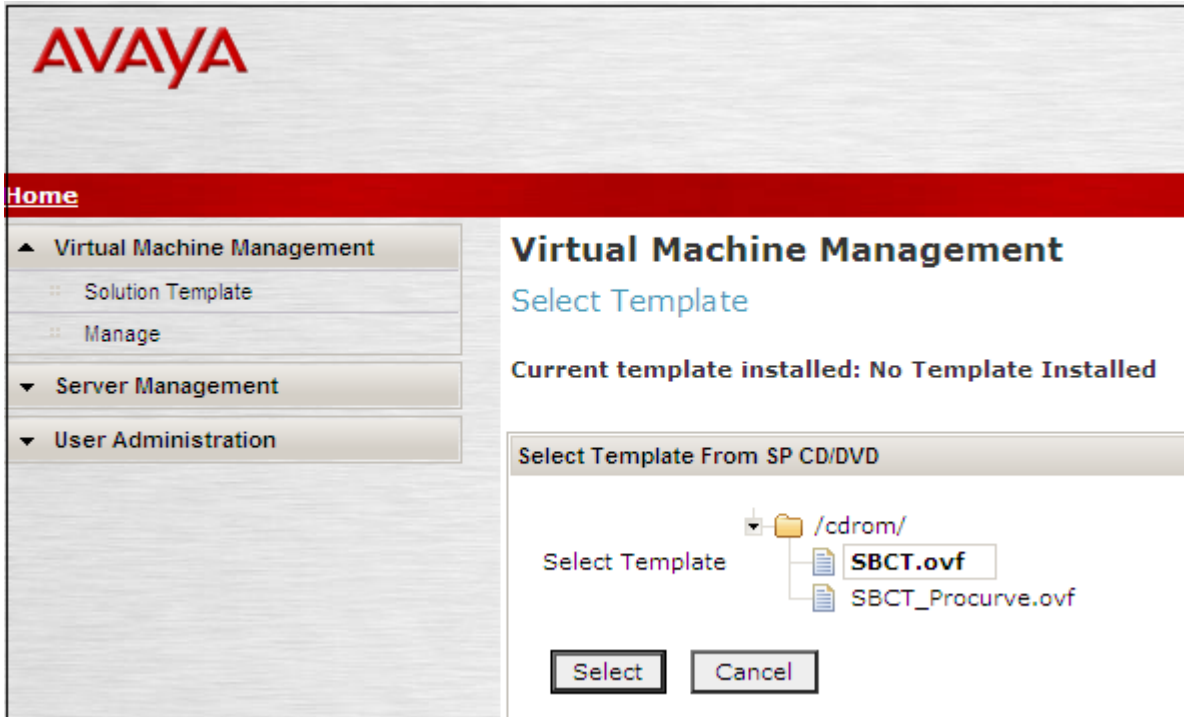
This section displays basic configuration of the SBC from the installation wizard. The initial configuration was completed by installing the Virtual Server Platform (VSP) 6.0.1.0.5 and then logging into the web interface of the server (cdom) address. This screen will verify the state of the dom-0 and cdom platforms (the State column below) and the Application State of the SBC after it has been installed.

Virtual Machine Management								
Virtual Machine List								
System Domain Uptime: 1 days, 21 hours, 44 minutes, 32 seconds								
Current template installed: SBCT 6.0.0.1.5 (sbc E362) <input type="button" value="Refresh"/>								
	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.1.0.5	205.3	512.0 MB	8	2h 15m 14s	Running	N/A
✓	cdom	6.0.1.0.5	205.3	1024.0 MB	1	54m 13s	Running	N/A

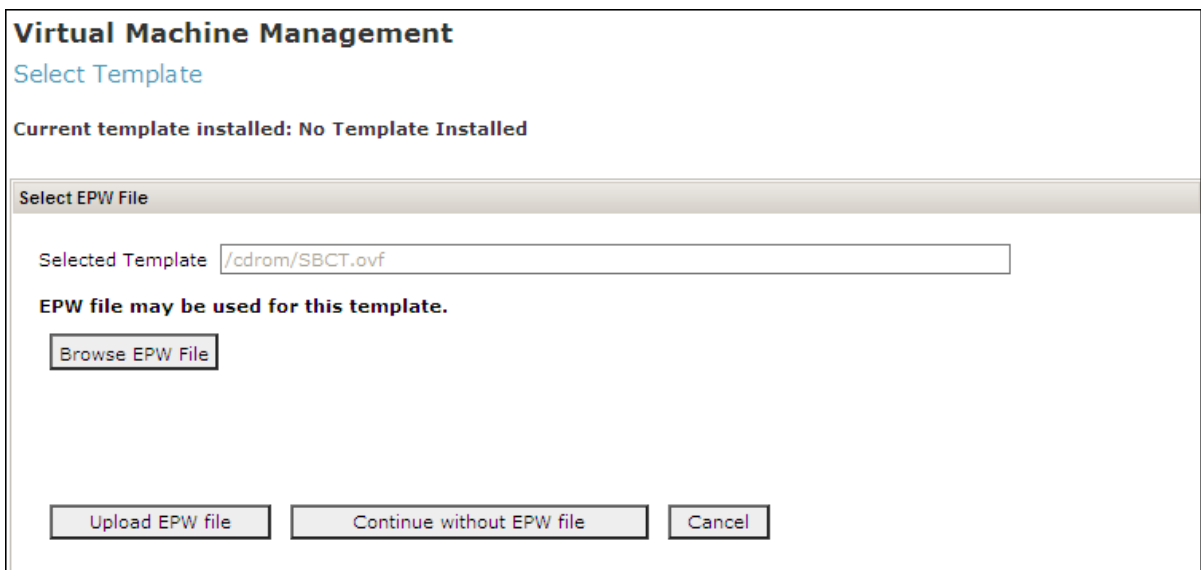
After Installation of VSP is complete open the web interface to the CDOM and go to Virtual Machine Management → Solution Template
Select the location of the template:



Select the correct template for your server hardware:



If an Electronic Preinstallation Worksheet has been created select “Browse EPW File” to select the location of the file then select “Upload EPW file”. Otherwise select “Continue without EPW file”.



Select “Install” after verifying:

Virtual Machine Management
Template Details

Current template installed: No Template Installed

Product ID: SBCT
Product Vendor: Avaya
Product Version: 6.0.0.1.5

Virtual Machines:

sbct

Product ID: sbc
Product Vendor: Avaya
Product Version: E362

Install

Cancel

At this point, it will open a log that will show the progress of the installation. When it gets to “Wait for User to Complete Data Entry”, it will open another window for input and you may have to enable pop-ups to view.

Virtual Machine Management						
Template Installation						
Cancel Installation						
Template Installation In Progress						
Workflow Status						
Start Time	Task Description	State	% Complete	Estimate	Actual	
12:26:33	Download disk image for sbc	In Progress	75	2m 39s		<div><div></div></div>
12:26:33	Download plugins for VMs	Complete	100		1m 7s	✓
12:27:40	Check Template for Web Application	Complete	100		14s	✓
12:27:55	Download pre-install web application	Complete	100		30s	✓
12:28:26	Pre-Install Web Application Deployment	Complete	100		3s	✓
12:28:29	Wait For User To Complete Data Entry	In Progress	0			<div><div></div></div>
	Undeploy Web Application	Not Started	0			✖
	Process EPW properties file if present	Not Started	0			✖
	Configure Network	Not Started	0			✖
	Install plugins	Not Started	0			✖
	Install sbc	Not Started	0	22m 0s		✖
	Restart network	Not Started	0			✖
	Start all VMs	Not Started	0			✖
	Wait until system and all VMs are stabilized	Not Started	0			✖
	Run post-install plugin if present	Not Started	0			✖
	Finalize Installation	Not Started	0			✖

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

6.1.1. Network Settings

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

- **IP Address:** Enter the IP address of the private side of the AA-SBC.
- **Hostname:** Enter a host name for the AA-SBC.
- **Domain:** Enter the domain used for the enterprise.
- **Default Domain:** Enter the domain used for the enterprise.

Click **Next Step** to continue.

Note: In this version the domain that is listed is NOT optional and must be populated or your install will fail, please refer to the release notes for further information.

The screenshot shows the Avaya Network Settings installation screen. The left sidebar contains a navigation menu with 'Configuration' and 'Installation' sections. The 'Installation' section is expanded, showing 'Network Settings' (marked with a red X), 'Logins', 'VPN Access', 'SBC' (marked with a red X), 'Summary', and 'Finish'. The main content area is titled 'Network Settings' and 'Enter network settings'. It contains several input fields for network configuration: Domain-0 IP Address (10.80.150.251), CDom IP Address (10.80.150.252), Gateway IP Address (10.80.150.1), Network Mask (255.255.255.0), Primary DNS (10.80.150.201), Secondary DNS (Optional), Default Search List (Optional), and HTTPS Proxy (Optional) [IP Address:Port Number]. Below these fields is a table for Virtual Machine settings:

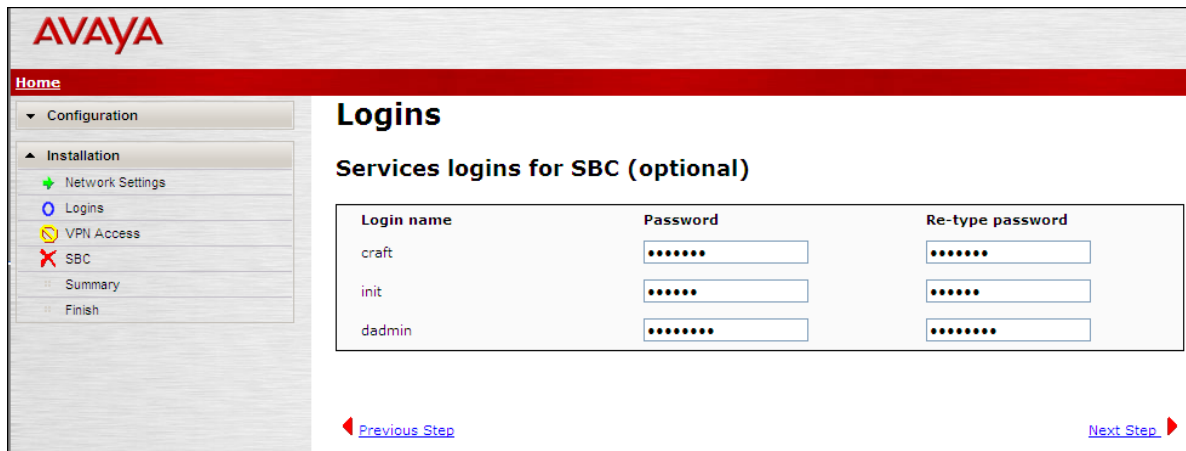
Virtual Machine	IP Address	Hostname	Domain
SBC	10.80.150.253	AASBC	sip.avaya.com (Optional)

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

6.1.2. Logins

Assign passwords for the different accounts.

Click **Next Step** to continue.



The screenshot shows the Avaya SBC configuration interface. The top bar is red with the Avaya logo. Below it is a navigation menu with options: Configuration, Installation, Network Settings, Logins, VPN Access, SBC, Summary, and Finish. The main content area is titled 'Logins' and 'Services logins for SBC (optional)'. It contains a table with three columns: Login name, Password, and Re-type password. The table has three rows: 'craft', 'init', and 'dadmin'. Each row has input fields for the password and re-type password, both masked with dots. At the bottom, there are 'Previous Step' and 'Next Step' buttons.

Login name	Password	Re-type password
craft	*****	*****
init	*****	*****
dadmin	*****	*****

6.1.3. VPN Access

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

Click **Next Step** to continue.

AVAYA

Home

Configuration

Installation

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

VPN Access

Configure VPN Access

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

☐ Yes ☒ No

VPN Access Configuration

VPN Router IP Address (Optional)

Remote Access Network

Remote Access Network Subnet Mask

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

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

If in doubt, please refer to the documentation.

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

6.1.4. SBC

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

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

- **Service Provider:** From the pull-down menu, select the name of the service provider to which the AA-SBC will connect. This will allow the wizard to select a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for Qwest. Thus, **Generic** was chosen instead and further customization was done manually after the wizard was complete.
- **Port:** Enter the port number that the service provider uses to listen for SIP traffic.
- **IP Address1:** Enter the Qwest provided IP address of the Qwest SIP Proxy.
- **Signaling/Media Network1:** Enter the Qwest provided subnet where signaling/media traffic will originate.
- **Signaling/Media Netmask1:** Enter the network mask corresponding to **Signaling/Media Network 1**.
- **IP Address2 (Optional):** If an additional network has been provided, enter the second Qwest provided IP address of the Qwest SIP Proxy. Any additional networks can be added after installation

- **Signaling/Media Network2 (Optional):** If an additional network is required, enter the second Qwest provided subnet where signaling/media traffic will originate. Any additional networks can be added after installation.
- **Signaling/Media Netmask2 (Optional):** Enter the network mask corresponding to **Signaling/Media Network 2**.

In the **SBC Network Data** section:

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

In the **Enterprise SIP Server** section:

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

Click **Next Step** to continue.

Home

Configuration

Installation

Network Settings

Logins

VPN Access

SBC

Summary

Finish

SBC

Session Border Controller Data

SIP Service Provider Data

Service Provider

Port

Generic

5060

IP Address1

67.148. .

Signalling/Media Network1

67.148. .

Signalling/Media Netmask1

255.255.255.240

IP Address2 (Optional)

67.148. .

Signalling/Media Network2 (Optional)

67.148. .

Signalling/Media Netmask2 (Optional)

255.255.255.240

Hunting (Optional)

Active/Standby

SBC Network Data

Interface

IP Address

Net Mask

Gateway

Private (Management)

10.80.150.253

255.255.255.0

10.80.150.1

Public

205.168. .

255.255.255.128

205.168. .

Enterprise SIP Server

SIP Domain

sip.avaya.com

IP Address1

10.80.150.206

Transport1

TCP

IP Address2 (Optional)

Transport2 (Optional)

Hunting (Optional)

Previous Step

Next Step

A summary screen will be displayed. Check the displayed values and click **Next Step** again to continue to the final step.

Summary

Network Settings	
Domain-0 Address	10.80.150.251
CDom Address	10.80.150.252
Gateway Address	10.80.150.1
Network Mask	255.255.255.0
Primary DNS	10.80.150.201
Secondary DNS	Not set
Default Search List	Not set
HTTPS Proxy	Not set

Virtual Machine	IP Address	Hostname	Domain
SBC	10.80.150.253	AASBC	sip.avaya.com
Default Domain			sip.avaya.com

Logins	
SBC craft Password	*****
SBC init Password	*****
SBC dadmin Password	*****

VPN Access	
VPN Access	Not Configured

SBC	
Service Provider	generic
Service Provider Port	5060
Service Provider IP Address	67.148. .
Service Provider Signalling/Media Network1	67.148. .
Service Provider Signalling/Media Netmask1	255.255.255.240
Service Provider IP Address2	67.148. .
Service Provider Signalling/Media Network2	67.148. .
Service Provider Signalling/Media Netmask2	255.255.255.240
Service Provider Hunting	ActiveStandby
Public IP Address	205.168. .
Public Netmask	255.255.255.128
Public Gateway	205.168. .
Enterprise SIP Server IP	10.80.150.206
Transport	TCP
Enterprise SIP Server IP2	Not set
Transport	Not set
Enterprise Hunting	Not set
Enterprise SIP Server Domain	sip.avaya.com

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

6.1.5. Confirm Installation

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

AVAYA

Home

Configuration

Installation

Network Settings

Logins

VPN Access

SBC

Summary

Finish

Confirm Installation

The following optional fields have not been set

- [Default Search List](#)
- [Secondary DNS](#)
- [HTTPS Proxy](#)
- [SBC Enterprise SIP Server IP2](#)
- [SBC Enterprise SIP Server Transport2](#)
- [SBC Enterprise SIP Server Hunting](#)

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook*, 555-025-600.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**


[Previous Step](#)

Wait until the template installation says **Template Installation Completed Successfully**.

Virtual Machine Management					
Template Installation					
Template Installation Completed Successfully					
Workflow Status					
Start Time	Task Description	State	% Complete	Estimate	Actual
12:26:33	Download disk image for sbc	Complete	100	10m 34s	✓
12:26:33	Download plugins for VMs	Complete	100	1m 7s	✓
12:27:40	Check Template for Web Application	Complete	100	14s	✓
12:27:55	Download pre-install web application	Complete	100	30s	✓
12:28:26	Pre-Install Web Application Deployment	Complete	100	3s	✓
12:28:29	Wait For User To Complete Data Entry	Complete	100	22m 53s	✓
12:51:22	Undeploy Web Application	Complete	100	0s	✓
12:51:23	Process EPW properties file if present	Complete	100	8s	✓
12:51:31	Configure Network	Complete	100	8s	✓
12:51:39	Install plugins	Complete	100	1s	✓
12:51:41	Install sbc	Complete	100	17m 28s	✓
13:09:09	Restart network	Complete	100	24s	✓
13:09:33	Start all VMs	Complete	100	14s	✓
13:09:48	Wait until system and all VMs are stabilized	Complete	100	46s	✓
	Run post-install plugin if present				
	- SBC:Creating SBC Configuration File				
	- SBC:Checking ssh connection to SBC				
	- SBC:Connecting to SBC web service				
	- SBC:Can't connect, trying again				
	- SBC:Connecting to SBC web service				
	- SBC:Copying configuration file to SBC				
	- SBC:Merging SBC configuration				
	- SBC:Saving SBC configuration file				
	- SBC:Restarting SBC				
	- SBC:Waiting for two minutes				
13:10:35	- SBC:Checking ssh connection to SBC	Complete	100	3m 35s	✓
	- SBC:Connecting to SBC web service				
	- SBC:Reading SBC configuration				
	- SBC:Adding user admin				
	- SBC:Adding user cust				
	- SBC:Adding user init				
	- SBC:Adding user craft				
	- SBC:Adding user dadmin				
	- SBC:Loading users				
	- SBC:Saving SBC configuration file				
	- SBC:Restarting SBC				
	- main:Wizard completed successfully				
13:14:10	Finalize Installation	Complete	100	17s	✓

6.1.6. Verify Installation

Click on **Home** screen to verify the SBC virtual machine is running.

Virtual Machine Management									
Virtual Machine List									
System Domain Uptime: 1 days, 21 hours, 44 minutes, 32 seconds									
Current template installed: SBCT 6.0.0.1.5 (sbc E362) Refresh									
	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State	
✓	Domain-0	6.0.1.0.5	205.3	512.0 MB	8	2h 15m 14s	Running	N/A	
✓	cdom	6.0.1.0.5	205.3	1024.0 MB	1	54m 13s	Running	N/A	
✓ 	sbc	E362	205.3	4.0 GB	4	4h 40m 49s	Running	Running	

Verify the proper IP interface is assigned to sbcPublic. Navigate to **Server Management** → **Network Configuration**.

AVAYA

Avaya Aura™ System Platform
admin
Previous successful login: Tue May 17 12:38:19 MDT 2011
Failed login attempts since: 0
Failover status: **Not configured**
[About](#) | [Help](#) | [Log Out](#)

Home

Virtual Machine Management

Server Management

Patch Management

Platform Upgrade

Log Viewer

Date / Time Configuration

Logging Configuration

System Configuration

Network Configuration

Static Route Configuration

Ethernet Configuration

Alarm Configuration

Certificate Management

License Management

SAL Gateway Management

Falover

Performance Statistics

Eject CD / DVD

File Manager

Security Configuration

Server Management

Network Configuration

Enable IPv6

Turn On IPv6 ☐ Requires System Reboot

General Network Settings

Default Gateway

Primary DNS

Secondary DNS

Domain Search List

Cdom Hostname

Dom0 Hostname

Scroll down to **Domain Network Interface**. Make sure the **sbcPublic** Interface is the same as the **Template Network Configuration** SBC Public Interface, eth2.

Domain Network Interface

Domain-0

Bridge	Interface	IP	Netmask	Gateway
avprivate	NA	172.20.10.1	255.255.255.0	no gateway defined for avprivate
avpublic	eth0	10.80.150.251	255.255.255.0	
sbcHA	eth3			
sbcPublic	eth2			
local service access	eth1	192.11.13.6		

Console Domain

Bridge	Interface	IP	Netmask	Gateway
avprivate	eth2	172.20.10.2	255.255.255.0	
avpublic	eth0	10.80.150.252	255.255.255.0	10.80.150.1

Template Network Configuration

Global Template Network Configuration

SBC Management and Private Interface IP address, eth0:
10.80.150.253

SBC hostname:
AASBC.sip.avaya.com

SBC Default Gateway interface, (eth0, eth2):
eth0

SBC Public Interface IP address, eth2:
205.168. .

SBC Public Interface Network Mask:
255.255.255.128

Save
Cancel

Please refer to SBC installation manuals and appropriate release notes for further assistance. Also note, this version of SBC is the first to require the license file be loaded via weblm instead of the SBC web interface.

6.2. Post Installation Configuration

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



Acme Packet Net-Net OS-E

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

Username:

Password:

Login

6.2.1. Add Additional SIP Gateways

Depending on the type of service, Qwest iQ® SIP Trunk may have multiple servers for redundancy purposes and remote DID's. During compliancy testing, three servers were used. Two servers were used for inbound/outbound dialing and one was used for inbound remote DID's and toll-free numbers. During the installation wizard the two used for inbound/outbound dialing were added. However, the two servers were in separate locations with separate subnets. When adding a new server that is in a separate subnet, it is necessary to add a route and a kernel-filter for it. To add a route, navigate to **cluster → box:<server_name> → interface eth2 → ip outside → routing**. Click on **Add route**.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The main content area is titled 'Configure clusterbox:AASBC.sip.avaya.com\interface eth2\ip outside\routing'. On the left, a tree view shows the configuration hierarchy: cluster > box:AASBC.sip.avaya.com > interface eth2 > ip outside > routing. The routing table contains two entries: 'route Default' (disabled) and 'route external-sip-media-1' (enabled). The 'Add route' button is highlighted with a yellow box. Below the table are buttons for Set, Reset, and Back, and links for Help and Index.

route	admin	destination	gateway	metric
Edit Delete route Default	disabled	default	0.0.0.0	1
Edit Delete route external-sip-media-1	enabled	network 67.148. /28	205. .1	1

Fill in the fields as described below and shown in the following screen:

- **route-name:** Enter a descriptive name. In the example below **external-sip-media-2** was used.
- **destination:** For **type** choose **network**. For **address/mask** enter the network and subnet mask provided by Qwest.
- **gateway:** Enter the IP address of the router connected to interface eth2.

Click **Set** to complete the configuration.

Configuration: all

Configuration | Setup | View

- cluster
 - box: AASBC.sip.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip
 - media-ports
 - routing
 - route Default
 - route external-sip-media-1
 - kernel-filter
- cli

- vsp
- default-session-config
- tls
- session-config-pool
- dial-plan
- enterprise
- dns
- settings

Create cluster | box 1 | interface eth2 | ip outside | routing | route - Step 1

Please provide some basic information for route. Then press "Create".

* route-name: external-sip-media-2

* destination

* type: network (network route)

* address/mask: 67.148. . /28

* gateway: 205.168. . (n.n.n.n)

Create | Reset | Cancel

In order for the AA-SBC to accept traffic from the new server a Kernel Filter needs to be added. Navigate to **cluster → box:<server_name> → interface eth2 → ip outside → kernel-filter** and click on **Add allow-rule**.

Configuration

Home | Configuration | Status | Call Logs | Event Logs | Actions | Services | Keys | Access | Tools

Configure cluster | box: AASBC.sip.avaya.com | interface eth2 | ip outside | kernel-filter | Help

Set | Reset | Back | Delete

allow-rule

	allow-rule	admin	destination-port	source-address/mask
Edit Delete	allow-rule allow-sip-udp-from-peer-1	enabled	5060	67.148. . /28

Add allow-rule

deny-rule

	deny-rule	admin	destination-port	source-address/mask	source-port
Edit Delete	deny-rule deny-all-sip	enabled	5060	0.0.0.0/0	0

Add deny-rule

Set | Reset | Back

Help | Index

Fill in the fields as described below and shown in the following screen:

- name:** Enter a descriptive name. In the example below **allow-sip-udp-from-peer-2** was used.
- admin:** Make sure it is set to **enabled**.

- **Destination-port:** Enter the port number provided by Qwest. Typically 5060.
- **source-address/mask:** Enter the network and subnet mask provided by Qwest.
- **source-port:** Enter 0.
- **protocol:** Choose the protocol provided by Qwest. Typically UDP.

Click **Set** to complete the configuration.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The main content area is titled 'Configuration: all' and shows a tree view on the left with the following structure:

- cluster
 - box: AASBC.sip.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip
 - media-ports
 - routing
 - kernel-filter
 - allow-rule allow-sip-udp-from
 - allow-rule allow-sip-udp-from
 - deny-rule deny-all-sip
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - enterprise
 - dns
 - settings

The right pane shows the configuration for 'clusterbox:AASBC.sip.avaya.com/interface eth2/ip outside/kernel-filter'. The configuration fields are:

- * name: allow-sip-udp-from-peer-2
- admin: enabled (Resource is active)
- destination-port: 5060 (from 0 to 65,535)
- * source-address/mask: 67.148. . /28 (n.n.n.n/n)
- source-port: 0 (from 0 to 65,535)
- protocol: udp (User Datagram Protocol)

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

The installation wizard only allows two servers to be added from Qwest so any additional servers will have to be added manually. To add a server, navigate to **vsp** → **enterprise** → **servers**. Click on **Add sip-gateway**.

Configuration: all

Configure vsplenterprise [Show advanced](#) [Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Delete](#)

other properties:

directories [Configure](#)

servers [Delete](#)

server	admin	domain	failover-detection	carrier
Edit Delete sip-gateway PBX	enabled	sip.avaya.com	ping	default
Edit Delete sip-gateway Telco	enabled		ping	default

[Add h323-server](#)
[Add sip-gateway](#)

3pcc-servers [Configure](#)

[Set](#) [Reset](#) [Back](#)

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

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

- **name:** Enter a descriptive name. In the example below **TelecoDID** was used.
- **admin:** Make sure it is set to **enabled**.
- **domain:** Leave blank.
- **Failover-detection:** Select **ping**. This sends SIP OPTIONS to detect failures.

In the **policy** section, set the **outbound-session-config-pool-entry** to **vsp\session-config-pool\entry ToTelco**.

Click **Set** to complete the configuration.

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The left sidebar shows a tree view of the configuration hierarchy: cluster > box: AASBC.sip.avaya.com > vsp > default-session-config > tls > session-config-pool > dial-plan > route Default > source-route FromTelco > source-route FromPBX > enterprise > servers > sip-gateway PBX > sip-gateway Telco > vsp\session-config-pool\entry To > server-pool > server Telco1 > server Telco2 > sip-gateway TelecoDID. The main content area is titled 'Configure vsp\enterprise\servers\sip-gateway TelecoDID' and includes a 'Show advanced' button. Below the title are buttons for Set, Reset, Back, Copy, and Delete. A link to 'Manage connections' is provided. A message states 'Press "Set" to keep these values.' The configuration is divided into sections: 'general:' with fields for * name (TelecoDID), admin (enabled), domain, and failover-detection (ping); 'servers:' with a 'server-pool' link; 'policy:' with dropdowns for inbound-session-config-pool-entry and outbound-session-config-pool-entry; and 'other properties:' with fields for carrier (default) and routing-tag. At the bottom are buttons for Set, Reset, Back, Copy, and links for Help and Index.

Configuration: all

Configuration Setup View

- cluster
 - box: AASBC.sip.avaya.com
 - vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - route Default
 - source-route FromTelco
 - source-route FromPBX
- enterprise
 - servers
 - sip-gateway PBX
 - sip-gateway Telco
 - vsp\session-config-pool\entry To
 - server-pool
 - server Telco1
 - server Telco2
 - sip-gateway TelecoDID

- dns
- settings

Configure vsp\enterprise\servers\sip-gateway TelecoDID Show advanced

Set Reset Back Copy Delete

[Manage connections](#), [Log instant messages](#), [Record media](#), [Record files](#), [Set up accounting](#), [Change "from:" URI](#), [Change "to:" URI](#)

Press "Set" to keep these values.

general:

* name	TelecoDID
admin	enabled (Resource is active)
domain	
failover-detection	ping (Use OPTIONS to detect failures)

servers:

server-pool [Configure](#)

policy:

inbound-session-config-pool-entry		Create
outbound-session-config-pool-entry	vsp\session-config-pool\entry ToTelco	Edit Create

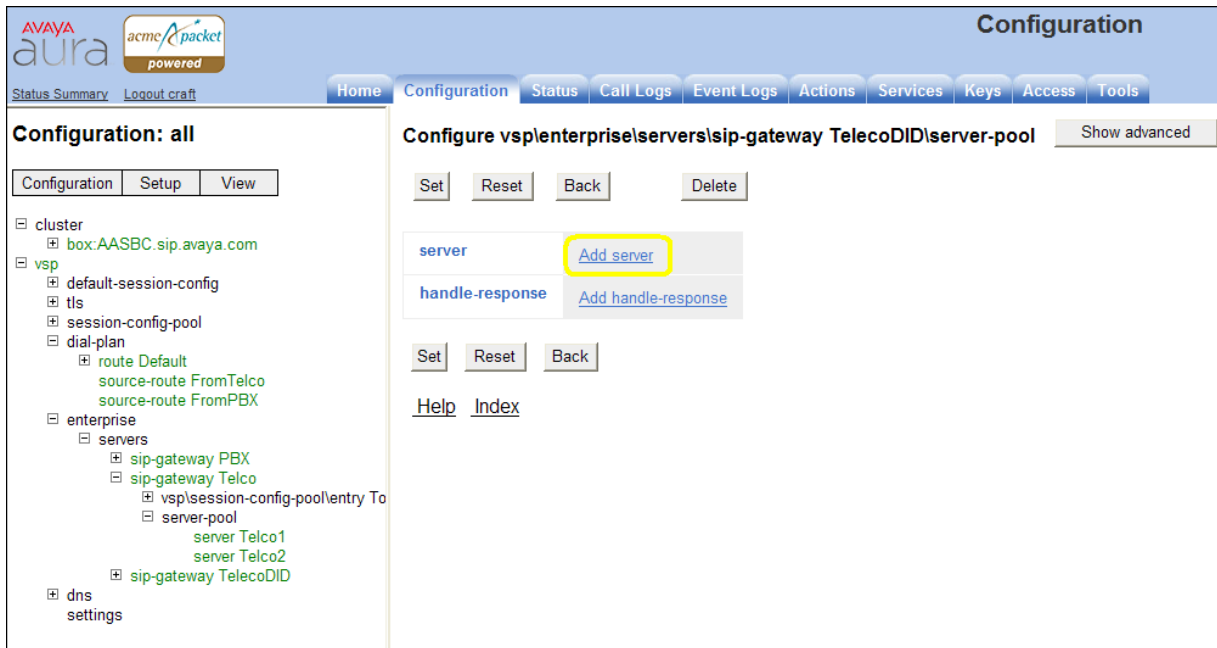
other properties:

carrier	default (Minimum 1 characters)
routing-tag	

Set Reset Back Copy

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

Next, in the **servers** section click on **configure** next to sever-pool. In the new right pane that appears click on **Add Server**.



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

- **server name:** Enter a descriptive name. In the example below **TelecoDID1** was used.
- **host:** Enter the IP address provided by Qwest.

Click on **Create**.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The 'Configuration' tab is active. On the left, a tree view shows the configuration hierarchy: 'cluster' (box: AASBC.sip.avaya.com), 'vsp' (default-session-config, tls, session-config-pool, dial-plan), 'enterprise' (servers: sip-gateway PBX, sip-gateway Telco, vsplsession-config-pool\entry To, server-pool: server Telco1, server Telco2, sip-gateway TelecoDID), and 'dns settings'. The main area displays the 'Create vsplenterprise\servers\sip-gateway TelecoDID\server-pool\server - Step 1 of 1' form. It prompts the user to 'Please provide some basic information for server. Then press "Create".' The 'General' section contains two fields: '* server-name' with the value 'TelcoDID1' and '* host' with the value '67.148. .'. A '(host name or n.n.n.n)' hint is shown next to the host field. At the bottom of the form are 'Create', 'Reset', and 'Cancel' buttons.

Next make sure the **transport** and **port** match what Qwest has provided. In this example the transport is set to **UDP** and the port is set to **5060**. Leave everything else default.

Click **Set** to complete the configuration.

Configure vsplenterprise\servers\sip-gateway TelcoDID\server-poolserver TelcoDID1
Show advanced
Help

Index

Set
Reset
Back
Copy
Delete

General:

* server-name	TelcoDID1
admin	enabled (Resource is active)
* host	67.148. (host name or n.n.n.n)
transport	transport UDP (User Datagram Protocol)
port	5060 (at minimum 1,default=5060)

Policy:

outbound-normalization	Add outbound-normalization
inbound-normalization	Add inbound-normalization

Call Admission Control:

admission-control	disabled (Resource is inactive)
emission-control	disabled (Resource is inactive)
max-bandwidth	enter unlimited kbits-per-second or select from unlimited (No limit to the minimum of bandwidth)
max-number-of-concurrent-calls	1000 (from 0 to 1,000,000,default=1000)
max-calls-in-setup	30 (from 0 to 10,000,default=30)

A dial plan needs to be created to route calls from the new Qwest inbound server to the Session Manager. Since the new server is for inbound only; a route to the server from Session Manager is not needed. Navigate to **vsp** → **dial-plan**. Click on **Add source-route**.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar lists the configuration tree under 'Configuration: all', with 'vsp' expanded to show 'dial-plan'. The main content area is titled 'source-route' and contains a table with the following data:

	source-route	description	source-match	peer	location-match-preferred
Add route					
Edit Delete	source-route FromTelco		server vsp\enterprise\servers\sip-gateway Telco	server vsp\enterprise\servers\sip-gateway PBX	up-to-outbound-peer
Edit Delete	source-route FromPBX		server vsp\enterprise\servers\sip-gateway PBX	server vsp\enterprise\servers\sip-gateway Telco	up-to-outbound-peer

Below the table is a yellow box containing the link [Add source-route](#). At the bottom of the page are buttons for 'Set', 'Reset', and 'Back', along with links for 'Help' and 'Index'.

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

- **name:** Enter a descriptive name. In the example below **FromTelecoDID** was used.
- **Source-match:** Set type to **server** and **source-server** to **vsp\enterprise\servers\sip-gateway TelcoDID**.

Click on **Create**.

Configuration

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configuration: all

Configuration Setup View

- cluster
 - box: AASBC.sip.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - route Default
 - source-route FromTelco
 - source-route FromPBX
- enterprise
 - servers
 - sip-gateway PBX
 - sip-gateway Telco
 - sip-gateway TelecoDID
- dns
 - settings

Create vsp\dial-plan\source-route - Step 1 of 1: Edit source-route [Help](#) [Index](#)

Please provide some basic information for source-route. Then press "Create".

general:

* name: From TelecoDID

* source-match

* type: server

* source-server: vsp\enterprise\servers\sip-gateway TelecoDID [Edit](#) [Create](#)

[Create](#) [Reset](#) [Cancel](#)

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

- **peer:** Set **type** to **server** and **server** to **vsp\enterprise\servers\sip-gateway PBX**.

Leave everything else default.

Click **Set** to complete the configuration.

AVAYA

aura

acme

packet

powered

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

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

Configuration: all

Configuration

Setup

View

cluster

box:AASBC.sip.avaya.com

vsp

default-session-config

tls

session-config-pool

dial-plan

route Default

source-route FromTelco

source-route FromPBX

source-route FromTelecoDID

enterprise

servers

sip-gateway PBX

sip-gateway Telco

sip-gateway TelecoDID

dns

settings

Configure vsp\dial-plan\source-route FromTelecoDID

Show advanced

Help

Index

Set

Reset

Back

Copy

Delete

general:

* name

FromTelecoDID

description

DID's From Qwest

* source-match

* type

server

* source-server

vsp\enterprise\servers\sip-gateway TelecoDID

Edit

Create

peer

type

server

(Peer is a SIP server)

server

vsp\enterprise\servers\sip-gateway PBX

Edit

Create

location-match-preferred

up-to-outbound-peer

(Outbound peer determines whether preferred)

priority

100

(from 0 to 999,999,default=100)

condition-list

Configure

condition-list-match-secondary

false

other properties:

admin

enabled

(Resource is active)

action

forward

(forward the INVITE to the server specified in the header)

apply-to-methods

INVITE

REFER

MESSAGE

INFO

Select All

Unselect All

6.2.2. Blocked Headers

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

The screenshot displays the Avaya Aura Configuration web interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The left sidebar shows a tree view of the configuration hierarchy, with 'vsp' expanded to show 'default-session-config' and 'header-settings'. The main content area is titled 'Configure vsp\default-session-config\header-settings' and includes a 'Show advanced' button and a 'Help' link. Below the title are buttons for Set, Reset, Back, and Delete. The configuration table lists various header settings, with 'blocked-header' highlighted and its 'Edit blocked-header' link circled in yellow. Other settings include 'allowed-header', 'altered-header', 'reg-ex-header', 'header-normalization', 'altered-body', 'reg-ex-collector', 'apply-allow-block-to', and 'apply-to-allow-block-to-dialog'. The 'apply-allow-block-to' dropdown is set to 'requests-and-responses' and the 'apply-to-allow-block-to-dialog' dropdown is set to 'both'.

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

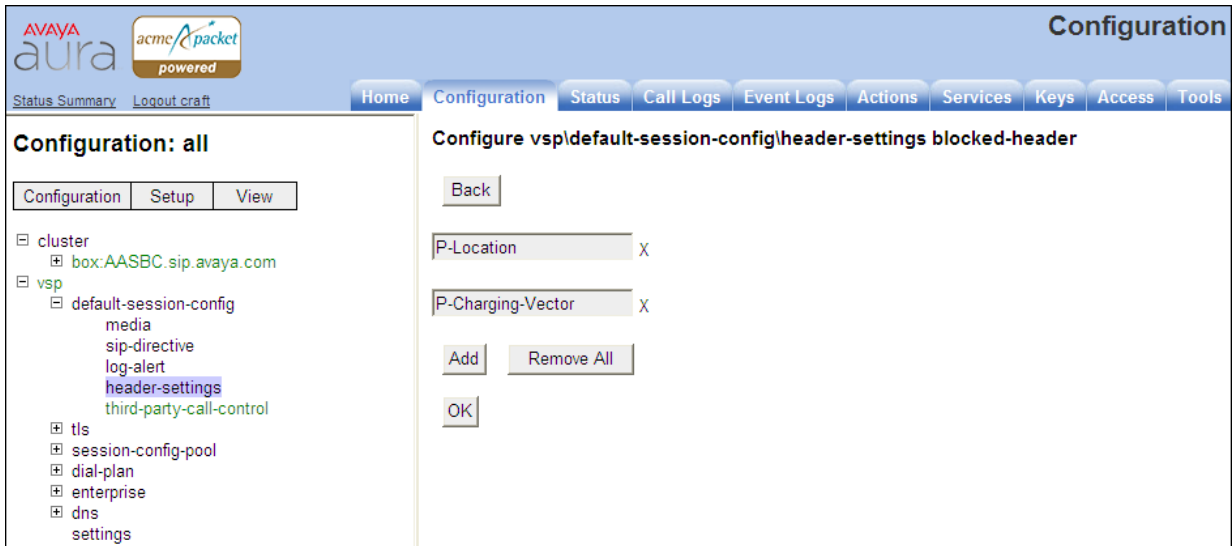
Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

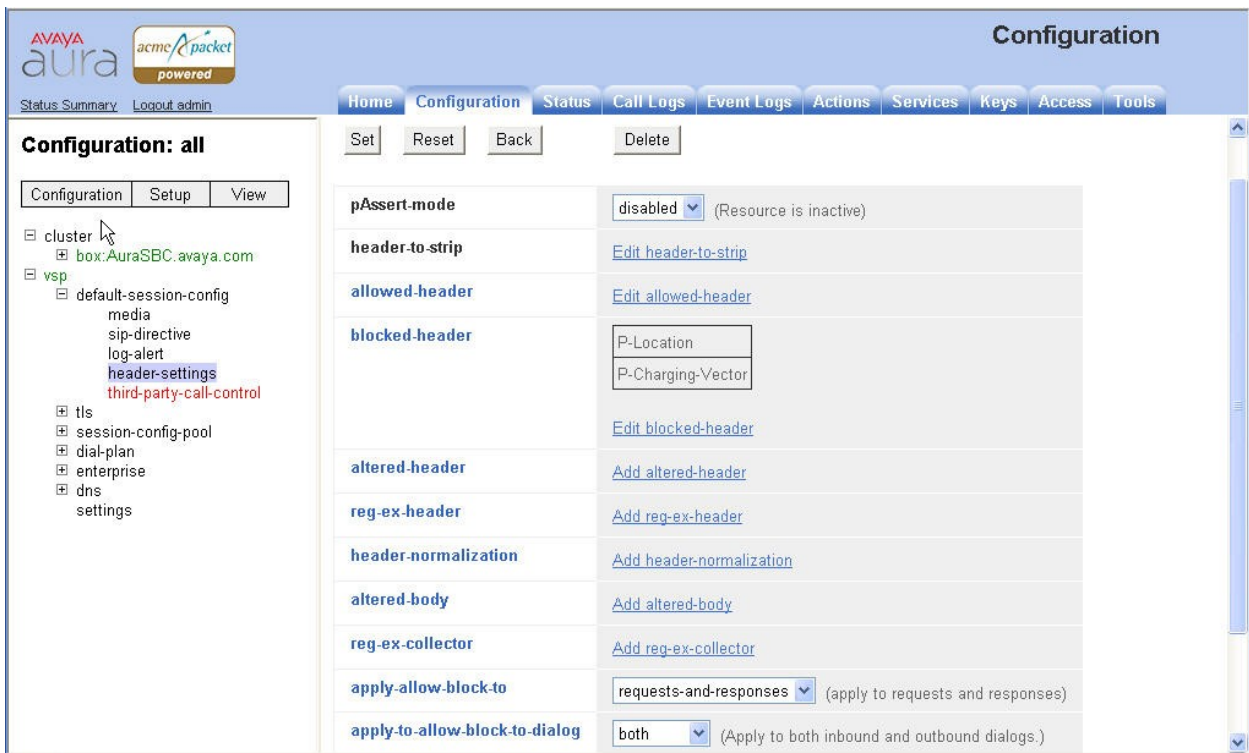
Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
cluster		
box:AASBC.sip.avaya.com		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
header-settings		

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



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



6.2.3. Third Party Call Control

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

The screenshot shows the AVAYA aura configuration interface. The left pane displays a tree structure under 'Configuration: all' with 'vsp' expanded, showing 'default-session-config' and 'third-party-call-control'. The right pane shows the configuration for 'third-party-call-control' with a 'Show advanced' button. The configuration table includes fields like 'admin' (set to 'disabled'), 'status-events' (set to 'both'), 'handle-refer-locally' (set to 'enabled'), and 'refer-maintain-identity' (set to 'false').

Field	Value	Resource Status
admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	enabled	(Resource is active)
refer-maintain-identity	false	
ringback-file		Browse System Files
busy-file		Browse System Files
pre-call-announcement		Browse System Files
terminate-after-pre-call-announcement	disabled	(Resource is inactive)
handle-replaces-locally	disabled	(Resource is inactive)
delayed-ack	disabled	(Resource is inactive)
include-reason-in-bye	enabled	(Resource is active)

6.2.4. Save the Configuration

To save the configuration, begin by clicking on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.

The screenshot shows the 'Configuration: all' menu in the AVAYA aura interface. The 'Configuration' tab is selected, and the 'Update and save configuration' option is highlighted. A tooltip for 'Update and save configuration' displays the text: 'Update and save the current configuration.' The menu also includes options like 'Reload configuration', 'Validate configuration', 'Analyze configuration', 'Search configuration', 'Save as XML', and 'Load from XML'.

7. Qwest iQ® SIP Trunk Configuration

To use the Qwest iQ® SIP Trunk Service, a customer must request service. The process can be started by accessing the corporate web site at www.qwest.com and requesting information via the online sales links or telephone numbers. The customer will need to provide the IP address used to reach the AA-SBC at the enterprise. Qwest will provide the customer with the necessary information to configure the SIP connection from the enterprise site to Qwest. The provided information from Qwest includes:

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

8. General Test Approach and Test Results

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

Qwest iQ® SIP Trunk passed compliance testing. Please refer to **Section 2.2** for any exceptions.

9. Verification and Troubleshooting

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

Verification Steps:

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

Troubleshooting:

1. Session Border Controller:
 - **Call Logs** - On the web user interface of the AA-SBC, the **Call Logs** tab can provide useful diagnostic or troubleshooting information.
2. Communication Manager:
 - **list trace station** <extension number> - Traces calls to and from a specific station.

- **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
 - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
 - **status trunk** <trunk access code number> - Displays trunk group information.
 - **status trunk** <trunk access code number/channel number> - Displays signaling and media information for an active trunk channel.
3. Session Manager:
- **traceSM -x** – Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.1 and Avaya Aura® Session Border Controller 6.0 to Qwest iQ® SIP Trunk service. Qwest iQ® SIP Trunk is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Qwest iQ® SIP Trunk provides a flexible, cost-saving alternative to traditional hardwired telephony trunks. Qwest iQ® SIP Trunk passed compliance testing. Please refer to **Section 2.2** for any exceptions.

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6, June 2010.
- [2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [3] *Administering Avaya Aura® Communication Manager*, Release 5.2, May 2009, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 5.2, May 2009, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
- [6] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, January 2011, Number 03-603473.
- [7] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Document Number 03-603324.
- [8] *Avaya Aura® Session Border Controller System Administration Guide*, V.6.0, September 2010
- [9] *Avaya Aura® Session Border Controller Release 6.0 Release Notes*
- [10] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.
- [11] *Avaya one-X® Communicator Getting Started*, August 2010.
- [12] *Avaya one-X® Communicator Quick Setup*, November 2009.
- [13] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>

- [14] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, <http://www.ietf.org/>
- [15] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, <http://www.ietf.org/>

Product documentation for Qwest iQ® SIP Trunking SIP is available from Qwest.

Appendix A: Avaya Aura® SBC Configuration File

```
#
# Copyright (c) 2004-2010 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 12:02:36 Wed 2011-05-18
#
config cluster
config box 1
  set hostname AASBC.sip.avaya.com
  set timezone America/Denver
  set name AASBC.sip.avaya.com
  set identifier 00:ca:fe:15:35:77
  config interface eth0
    config ip inside
      set ip-address static 10.80.150.253/24
    config ssh
    return
  config snmp
    set trap-target 10.80.150.252 162
    set trap-filter generic
    set trap-filter dos
    set trap-filter sip
    set trap-filter system
  return
  config web
  return
  config web-service
    set protocol https 8443
    set authentication certificate "vsp\tls\certificate ws-cert"
  return
  config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
  return
  config icmp
  return
  config media-ports
  return
  config routing
    config route Default
      set gateway 10.80.150.1
    return
```

```

config route Static0
    set destination network 192.11.13.4/30
    set gateway 10.80.150.251
return
config route Static1
    set admin disabled
return
config route Static2
    set admin disabled
return
config route Static3
    set admin disabled
return
config route Static4
    set admin disabled
return
config route Static5
    set admin disabled
return
config route Static6
    set admin disabled
return
config route Static7
    set admin disabled
return
return
return
return
config interface eth2
config ip outside
    set ip-address static 205.168.xxx.xxx/25
config sip
    set udp-port 5060 "" "" any 0
return
config media-ports
return
config routing
    config route Default
        set admin disabled
    return
    config route external-sip-media-1
        set destination network 67.xxx.xxx.0/28
        set gateway 205.168.xxx.xxx
    return
    config route external-sip-media-2
        set destination network 67.xxx.xxx.0/28
        set gateway 205.168.xxx.xxx
    return
return
config kernel-filter
    config allow-rule allow-sip-udp-from-peer-1
        set destination-port 5060
        set source-address/mask 67.xxx.xxx.0/28
        set protocol udp
    return
    config allow-rule allow-sip-udp-from-peer-2

```

```

        set destination-port 5060
        set source-address/mask 67.xxx.xxx.0/28
        set protocol udp
    return
    config deny-rule deny-all-sip
        set destination-port 5060
    return
return
return
return
return
config cli
    set prompt AASBC.sip.avaya.com
return
return
return

config services
config event-log
    config file access
        set filter access info
        set count 3
    return
    config file system
        set filter system info
        set count 3
    return
    config file errorlog
        set filter all error
        set count 3
    return
    config file db
        set filter db debug
        set filter dosDatabase info
        set count 3
    return
    config file management
        set filter management info
        set count 3
    return
    config file peer
        set filter sipSvr info
        set count 3
    return
    config file dos
        set filter dos alert
        set filter dosSip alert
        set filter dosTransport alert
        set filter dosUrl alert
        set count 3
    return
    config file krnlsys
        set filter krnlsys debug
        set count 3
    return
return
return
return

```

```

config master-services
    config database
        set media enabled
    return
return

config vsp
    set admin enabled
    config default-session-config
        config media
            set anchor enabled
            set rtp-stats enabled
        return
    config sip-directive
        set directive allow
    return
    config log-alert
        set apply-to-methods-for-filtered-logs
    return
    config header-settings
        set blocked-header P-Location
        set blocked-header P-Charging-Vector
    return
    config third-party-call-control
    return
return
config tls
    config default-ca
        set ca-file /cxc/certs/sipca.pem
    return
    config certificate ws-cert
        set certificate-file /cxc/certs/ws.cert
    return
    config certificate aasbc.pl2
        set certificate-file /cxc/certs/aasbc.pl2
        set passphrase-tag aasbc-cert-tag
    return
return
config session-config-pool
    config entry ToTelco
        config to-uri-specification
            set host next-hop
        return
        config from-uri-specification
            set host local-ip
        return
        config request-uri-specification
            set host next-hop
        return
        config p-asserted-identity-uri-specification
            set host local-ip
        return
    config forking-settings
        set outbound-arbiter-rule weighted-round-robin
    return

```

```

return
config entry ToPBX
  config to-uri-specification
    set host next-hop-domain
  return
  config request-uri-specification
    set host next-hop-domain
  return
return
config entry Discard
  config sip-directive
  return
return
return
config dial-plan
  config route Default
    set priority 500
    set location-match-preferred exclusive
    set session-config vsp\session-config-pool\entry Discard
  return
  config source-route FromTelco
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
    set peer server "vsp\enterprise\servers\sip-gateway Telco"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
  config source-route FromTelecoDID
    set description "DID's From Qwest"
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway TelecoDID"
  return
return
config enterprise
  config servers
    config sip-gateway PBX
      set domain sip.avaya.com
      set failover-detection ping
      set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
  config server-pool
    config server PBX1
      set host 10.80.150.206
      set transport TCP
    return
  return
  config sip-gateway Telco
    set domain 67.xxx.xxx.8
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
  config server-pool
    config server Telco1
      set host 67.xxx.xxx.8

```



```

        return
        config server Telco2
        set host 67.xxx.xxx.8
        return
    return
return
config sip-gateway TelecoDID
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
    config server TelcoDID1
    set host 67.xxx.xxx.9
    return
    return
    return
    return
return
config dns
    config resolver
    config server 10.80.150.201
    return
    return
return
config settings
    set read-header-max 8191
return
return

config external-services
return

config preferences
    config gui-preferences
        set enum-strings SIPSourceHeader Refer-To
        set enum-strings SIPSourceHeader next-hop
        set enum-strings SIPSourceHeader Status-Line
        set enum-strings SIPSourceHeader Contact
        set show-unlicensed-features false
    return
return

config access
    config permissions superuser
        set cli advanced
    return
    config permissions read-only
        set config view
        set actions disabled
        set debug disabled
    return
    config users
        config user admin
        set password
0x00a71fb02f708646e66100a735ab335e87007e76ea5d5fb60e3c608049
        set permissions access\permissions superuser

```

```
    return
    config user cust
    set password
0x0030135cb304c3146afeff64bc88d83b3687ef2827422da931aa12c796
    set permissions access\permissions read-only
    return
    config user init
    set password
0x00f363f7dffa7d071773c33bb32eefa55e080d99d8278bdde52ffadc8
    set permissions access\permissions superuser
    return
    config user craft
    set password
0x005f4d7e72e5cbb0aa13c121bcea9502dda0d1c857429cd2fecfe60307
    set permissions access\permissions superuser
    return
    config user dadmin
    set password
0x00eee65aec82446775d8f5ebd8db0dfe33f660175eff65beeaf0610d44
    set permissions access\permissions read-only
    return
    return
    return

config features
return
```

©2011 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.