



Application Notes for Configuring Bell Canada SIP Trunking with Avaya Aura® Communication Manager Evolution Server, Avaya Aura® Session Manager, and Avaya Aura® Session Border Controller – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell Canada SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller 6.0, Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager Evolution Server 6.0.1, and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Border Controller or Avaya Aura® Session Manager.

Bell Canada SIP Trunking service provides PSTN access via a SIP trunk between the enterprise and the Bell Canada network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Bell Canada is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction	4
2.	Test Scope and Results	4
2.1.	Interoperability Compliance Testing	4
2.2.	Test Results	5
2.3.	Support	7
3.	Reference Configuration	7
4.	Equipment and Software Validated	9
5.	Configure Communication Manager	10
5.1.	Licensing and Capacity	10
5.2.	System Features	12
5.3.	IP Node Names	13
5.4.	Codecs	13
5.5.	IP Network Region	14
5.6.	Signaling Group	16
5.7.	Trunk Group	19
5.8.	Calling Party Information	22
5.9.	Outbound Routing	23
5.10.	Vector Directory Numbers (VDNs) and Vectors for SIP NCR	25
5.10.1.	Post-Answer Redirection to a PSTN Destination	26
5.10.2.	Post-Answer Redirection With UI to a SIP Destination	26
5.11.	Saving Communication Manager Configuration Changes	28
6.	Configure Avaya Aura® Session Manager	29
6.1.	System Manager Login and Navigation	30
6.2.	Specify SIP Domain	32
6.3.	Add Location	33
6.4.	Add Adaptation Module	36
6.5.	Add SIP Entities	40
6.6.	Add Entity Links	44
6.7.	Add Routing Policies	46
6.8.	Add Dial Patterns	47
6.9.	Add/View Session Manager	50
7.	Configure Avaya Aura® Session Border Controller	51
7.1.	Installation Wizard	52
7.1.1.	Network Settings	52
7.1.2.	VPN Access	53
7.1.3.	SBC	54
7.1.4.	Confirm Installation	56
7.2.	Post Installation Configuration	57
7.2.1.	Options Frequency	58
7.2.2.	Blocked Headers	59
7.2.3.	Diversion Header Domain Mapping	61
7.2.4.	Contact Header Modification	63
7.2.5.	Max-Forwards Value	65
7.2.6.	Normalizing Calling Number in From Header	67

7.2.7. Digest Authentication	70
7.2.8. Third Party Call Control	72
7.2.9. Save the Configuration	73
8. Bell Canada SIP Trunking Configuration	73
9. Verification and Troubleshooting	74
10. Conclusion.....	76
11. References	77
Appendix A: Avaya Aura® SBC Configuration File	78

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell Canada SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller (AA-SBC) 6.0, Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager 6.0.1 configured as an Evolution Server, and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Border Controller or Avaya Aura® Session Manager.

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

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

2. Test Scope and Results

2.1. 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 Bell Canada SIP Trunking service Vendor Validation circuit through the public Internet.

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

- Incoming PSTN calls to various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phones.

- Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) were tested. 1XC also supports two signaling protocols (H.323 and SIP). Both protocols were tested.
- Various call types included: local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411), etc.
- G.729A Codec, G.711A and G.711MU Codec and proper codec negotiation.
- DTMF tone transmissions passed as out-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection using SIP REFER for transfer of inbound call back to PSTN.
- Network Call Redirection using SIP REFER that contains UUI (User-To-User Information).

Items not supported or not tested included the following:

- Inbound toll-free and outbound emergency calls (911) are supported but were not tested as part of the compliance test.
- Faxing between the enterprise site and PSTN was not tested as part of the compliance test since Bell Canada currently does not support T.38 FoIP (Fax over IP) on its SIP Trunking Vendor Validation circuit.

2.2. 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 Bell Canada SIP Trunking service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

- **Off-net call forwarding:** When INVITE from the enterprise to Bell Canada for forwarding an inbound call back to PSTN contains both Diversion and History-Info headers, Bell Canada would respond with "404 Not Found", then issue a CANCEL message to the enterprise, resulting failure of off-net call forward. This failure was addressed in the compliance test by turning off the History-Info header in the call-redirection INVITE from the enterprise.
- **EC500:** EC500 is the Communication Manager mobility feature which allows a user to have incoming calls ring the destination extension as well as a remote off-net number such as a mobile phone. When the INVITE from the enterprise to Bell Canada for the remote PSTN endpoint contains both Diversion and History-Info headers, Bell Canada

would respond with "404 Not Found", then issue a CANCEL message to the enterprise, causing the EC500 call to fail. This failure was addressed in the compliance test by turning off the History-Info header in the call-redirection INVITE from the enterprise.

- **Calling number format:** The inbound call INVITE from Bell Canada to the enterprise contains a "+" followed by 11 digits in the From header for the calling number. This prevents some of the EC500 mobility call features from working properly since the EC500 mobile number configured on Communication Manager (in **off-pbx-telephone station-mapping** form) is not allowed to contain non-digits like "+" to match the number in the inbound INVITE From header. The workaround is to have AA-SBC normalize the calling number contained in the From header to remove the plus sign (see **Section 7.2.6**).
- **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, Bell Canada 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 ring-back for 2 minutes then an announcement "Your party is not answering..." in this failure scenario. Network call redirection works successfully when the Communication Manager vector is programmed to redirect the inbound call to a PSTN number after answering the call first in the vector (using SIP REFER message for network call redirection instead of the 302 message).
- **No matching codec:** With no matching codec between the network and the enterprise, Bell Canada does not return a proper 48X status message on outbound call from the enterprise if no codec offered by the enterprise matches any of the codecs supported by the network. Bell Canada simply does not return an 18X message (for signaling normal call progression) to the outbound INVITE in this situation. On the PSTN destination phone, if the handset is picked up immediately there will be a couple of rings followed by fast busy tones. The PSTN phone plays dial tone if the handset is picked up after a couple of rings.
- **Media Format:** If the Initial IP-IP Direct Media setting on Communication Manager's SIP trunk groups configured for Bell Canada (e.g., "n") is different than the setting (e.g., "y") for the general SIP trunk group between Communication Manager and Session Manager used for phone connections and other applications, then outbound call to PSTN from enterprise SIP phones will have audio problem: PSTN phone will hear a series of tones and delayed audio path from the enterprise to PSTN. Traces would show that audio Media Format from the enterprise is different than the Media Format expected by the network even though it is configured to be the same. To avoid this problem, the Initial IP-IP Direct Media setting on Communication Manager must be set identically on trunk groups dedicated to Bell Canada and on the general trunk group between Communication Manager and Session Manager.
- **Calling number/ID display:** PSTN phone may display both calling party id/name and calling party number or just calling party number and no calling party id/name on outbound calls from the enterprise to the PSTN through Bell Canada, depending on the specific service provider the call routes through from Bell Canada to the endpoint.
- **Call display update:** Call display was not properly updated on PSTN phone to reflect the true connected party on calls that are transferred to the PSTN from the enterprise (see

related item below). After the call transfer was completed, the PSTN phone showed the party that initiated the transfer instead of the actual connected party.

- **Contact header from AA-SBC:** After a transfer of inbound PSTN call to a 2nd PSTN phone was completed, UPDATE from Communication Manager to Session Manager and from Session Manager to AA-SBC correctly contains Contact header with originating PSTN phone number (i.e. the number for the actual connected party); however, UPDATE from AA-SBC to network changed this Contact header with Bell Canada DID associated with the internal extension that is the transferring party. The configuration on AA-SBC for addressing this problem using an earlier version of AA-SBC software failed to work in the AA-SBC software used for the compliance test. This issue was reported to AA-SBC support/development and will be fixed in a later release of the AA-SBC software.

2.3. Support

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

For technical support on Bell Canada SIP Trunking, contact Bell Canada at http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the Bell Canada SIP Trunking service (Vendor Validation circuit) through a public Internet WAN connection.

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

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

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

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

Canada across the public IP network is UDP; the transport protocol between the AA-SBC and the enterprise Session Manager across the enterprise IP network is TCP.

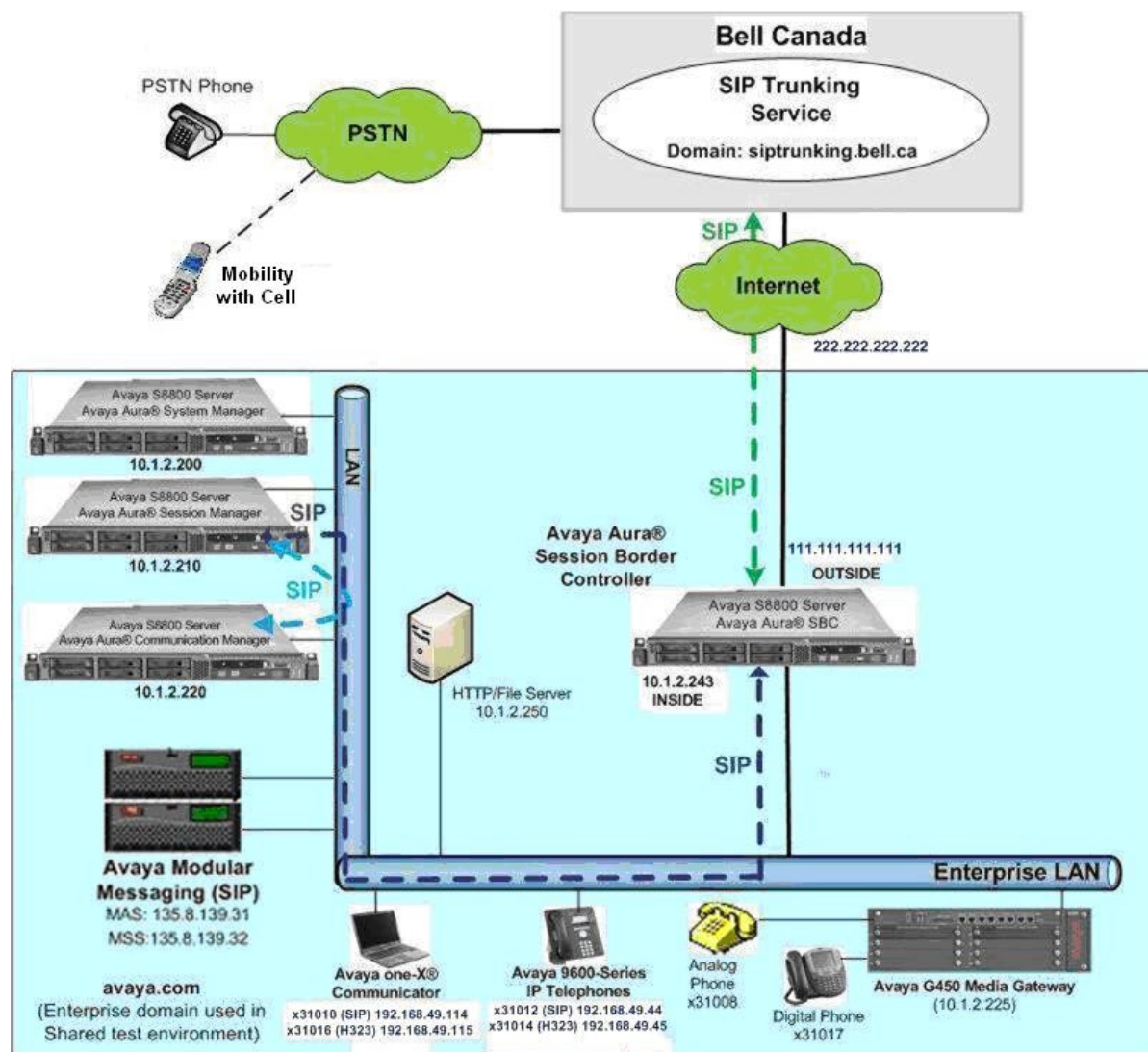


Figure 1: Avaya IP Telephony Network Connecting to Bell Canada SIP Trunking Service

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

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

treatment, such as incoming digit translations and class of service restrictions could be performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection 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 for egress to the Bell Canada network.

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

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on Avaya S8800 Server with Avaya G450 Media Gateway	6.0.1 (R016x.00.1.510.1-18621) 30.13.2
Avaya Aura® Session Manager running on Avaya S8800 Server	6.1.1.0.611023
Avaya Aura® System Manager running on Avaya S8800 Server	6.1.0 Build 6.1.0.0.7345-6.1.5.7
Avaya 96xx Series IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya 96xx Series IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.4
Avaya one-X Communicator (H.323 & SIP)	6.1.0.12-GA-30334
Avaya 8410D Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Avaya Aura® Session Border Controller running on Avaya S8800 Server	6.0.2.0.3 (sbc E362P4)
Avaya Modular Messaging (MAS) running on Avaya S8800 Server	5.2 SP6 Patch 2 (9.2.357.6022)
Avaya Modular Messaging (MSS) running on Avaya S8800 Server	5.2 SP6 Patch 2
Bell Canada SIP Trunking Solution Components	
Component	Release
Acme Packet Net-Net 4250 SBC	Firmware SC6.2.0 MR-4 Patch 1 (Build 718)
Broadsoft SoftSwitch	Rel16

Legacy Nortel CS2K Media Gateway	SN10 PVG/IW-SPM
----------------------------------	-----------------

Table 1: Equipment and Software Tested

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

5. Configure Communication Manager

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

It is assumed the general installation of the Communication Manager and the Avaya G450 Media Gateway has been previously completed and is not discussed here.

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **4000** licenses are available and **172** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options
OPTIONAL FEATURES

Page 2 of 11

IP PORT CAPACITIES	USED
Maximum Administered H.323 Trunks: 4000	0
Maximum Concurrently Registered IP Stations: 2400	4
Maximum Administered Remote Office Trunks: 4000	0
Maximum Concurrently Registered Remote Office Stations: 2400	0
Maximum Concurrently Registered IP eCons: 68	0
Max Concur Registered Unauthenticated H.323 Stations: 100	0
Maximum Video Capable Stations: 2400	2
Maximum Video Capable IP Softphones: 2400	2
Maximum Administered SIP Trunks: 4000	172
Maximum Administered Ad-hoc Video Conferencing Ports: 4000	0
Maximum Number of DS1 Boards with Echo Cancellation: 80	0
Maximum TN2501 VAL Boards: 10	0
Maximum Media Gateway VAL Sources: 50	1
Maximum TN2602 Boards with 80 VoIP Channels: 128	0
Maximum TN2602 Boards with 320 VoIP Channels: 128	0
Maximum Number of Expanded Meet-me Conference Ports: 300	0

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

5.2. System Features

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

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? y
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

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

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

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

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

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

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8800 Server running Communication Manager (**procr**) and Session Manager (**SM61**). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
SM61	10.1.2.210	
default	0.0.0.0	
procr	10.1.2.220	
procr6	::	

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Bell Canada SIP Trunking service currently supports G.729A, G.711A and G.711MU. Enter the codec to be used in priority order in the **Audio Codec** column of the table. Default values can be used for all other fields. The following screen shows the codec set configuration at a certain time of the compliance test. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time. Note that the G.722-64K codec was configured for use by intra-site calls between the enterprise IP phones.

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.722-64K	n	2	20
2: G.711MU	n	2	20
3: G.729A	n	2	20

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

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

5.5. IP Network Region

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

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.com** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region. Note that Session Manager adaptation configuration (**Section 6.4**) is used to convert this shared domain name to the specific CPE domain as assigned by Bell Canada and expected by the Bell Canada network.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```

change ip-network-region 2
                                     IP NETWORK REGION
                                     Page 1 of 20

Region: 3
Location:      Authoritative Domain: avaya.com
Name: Bell Canada Test
MEDIA PARAMETERS
  Codec Set: 2
  UDP Port Min: 2048
  UDP Port Max: 3329
  Intra-region IP-IP Direct Audio: yes
  Inter-region IP-IP Direct Audio: yes
  IP Audio Hairpinning? n
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5
H.323 IP ENDPOINTS
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
  AUDIO RESOURCE RESERVATION PARAMETERS
  RSVP Enabled? n

```

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

```

display ip-network-region 2
                                     Page 4 of 20

Source Region: 3      Inter Network Region Connection Management
dst codec direct WAN-BW-limits Video Intervening Dyn G A t
rgn set WAN Units Total Norm Prio Shr Regions CAC R L e
1 2 y NoLimit n t
2
3 2 all
4

```

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

For the compliance test, devices with IP addresses in the 10.1.2.0/24 subnet are assigned to network region 1. These include Communication Manager, Session Manager and AA-SBC that were set up for shared test environment. IP telephones used for the compliance test, including both the Avaya 9600 IP Telephones and the Avaya one-X® Communicator soft phones, are assigned to network region 2 with IP address in the 192.168.49.0/24 subnet. In production environments, different sites will typically be on different networks, and ranges of IP addresses

assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

change ip-network-map

Page 1 of 63

IP ADDRESS MAPPING

IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: 10.1.2.0	/24	1	n		
TO: 10.1.2.255					
FROM: 192.168.49.0	/24	2	n		
TO: 192.168.49.255					
FROM:	/		n		
TO:					

5.6. Signaling Group

Use the **add signaling-group** command to create 2 signaling groups between Communication Manager and the Session Manager for use by inbound calls from the service provider network and outgoing calls from the enterprise. The signaling group used for inbound calls from the service provider is shown below. For the compliance test, signaling group 27 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between the Communication Manager and Session Manager. The transport method used between the Session Manager and the AA-SBC is specified as TCP in **Sections 5.6** and **6.1.3**. Lastly, the transport method between the AA-SBC and Bell Canada is UDP. This is defined in **Section 7.1.3** when the service provider name is selected.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so the Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5064** (the well-known port value for TCP is 5060).
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and can not be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Avaya S8800 Server running Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM61**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to blank.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **DTMF over IP** field to **rtp-payload**. This setting enables Communication Manager to send DTMF transmissions using RFC 2833.
- Verify that the **Initial IP-IP Direct Media** is set to the same value as for the signaling group used for the enterprise site (signaling group 1 for the compliance test). The default setting for this field is **n**. See the **Media Format** bullet item in **Section 1.1** for more information about this setting.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **12**. This allows more time for outbound PSTN calls to complete through the Bell Canada SIP Trunking service.
- Default values may be used for all other fields.

```

add signaling-group 27                                     Page 1 of 1

                                SIGNALING GROUP

Group Number: 27                Group Type: sip
IMS Enabled? n                 Transport Method: tcp
    Q-SIP? n                                SIP Enabled LSP? n
    IP Video? n                       Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y  Peer Server: Others

Near-end Node Name: procr                Far-end Node Name: SM61
Near-end Listen Port: 5068              Far-end Listen Port: 5068
                                      Far-end Network Region: 2

Far-end Domain:

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

```

The trunk group for outbound calls from the enterprise to the PSTN was similarly configured except that the Far-end Domain is set to the service provider network domain as provided by Bell Canada. For the compliance test, signaling group 28 was used for this purpose and is shown below:

```
add signaling-group 28                                     Page 1 of 1
                                                    SIGNALING GROUP

Group Number: 28          Group Type: sip
IMS Enabled? n           Transport Method: tcp
    Q-SIP? n                                     SIP Enabled LSP? n
    IP Video? n                               Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: Others

Near-end Node Name: procr          Far-end Node Name: SM61
Near-end Listen Port: 5068        Far-end Listen Port: 5068
Far-end Network Region: 2

Far-end Domain: siptrunking.bell.ca

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    Initial IP-IP Direct Media? n
                                           Alternate Route Timer(sec): 12
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for each of the 2 signaling groups created in **Section 5.6**. For the compliance test, trunk group 27 and 28 were 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 **Direction** field to **incoming** for trunk group 27 and **outgoing** for trunk group 28
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 27                                     Page 1 of 21
                                     TRUNK GROUP

Group Number: 27                                     Group Type: sip      CDR Reports: y
Group Name: SP Trunk                                COR: 1              TN: 1              TAC: 127
Direction: incoming                                Outgoing Display? n
Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk                         Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 27
                                                Number of Members: 20
```

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

```
add trunk-group 27                                     Page 2 of 21
    Group Type: sip

TRUNK PARAMETERS

    Unicode Name: auto

                                                Redirect On OPTIM Failure: 5000

    SCCAN? n                                         Digital Loss Group: 18
                                                Preferred Minimum Session Refresh Interval(sec): 600

                                                Delay Call Setup When Accessed Via IGAR? n
```

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

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

add trunk-group 27		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
	UII Treatment: service-provider	
	Replace Restricted Numbers? y	
	Replace Unavailable Numbers? y	
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		

On **Page 4**, the **Network Call Redirection** field can be set to **n** (default setting) or **y**. Setting the **Network Call Redirection** flag to **y** enables use of the SIP REFER message for call transfer.

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

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

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

add trunk-group 27	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Network Call Redirection? y	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
 Convert 180 to 183 for Early Media? y	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Enable Q-SIP? n	

The screen below shows page 1 of trunk group 28 (the trunk group for outgoing calls from the enterprise) configuration. Note that settings for the **TAC**, **Direction** and **Signaling Group** fields as explained above.

add trunk-group 28	Page 1 of 21	
TRUNK GROUP		
Group Number: 28	Group Type: sip	CDR Reports: y
Group Name: SP Trunk	COR: 1	TN: 1
Direction: outgoing	Outgoing Display? n	TAC: 128
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 28	
	Number of Members: 20	

The configurations on other pages of trunk group 28 are identical to trunk group 27.

5.8. Calling Party Information

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

In the sample configuration, 3 DID numbers were assigned for testing. These 3 numbers were mapped to the 3 extensions 31012, 31014, and 31016. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 3 extensions.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	3	60		5	Total Administered: 10
5	31012	27-28	4167771111	10	Maximum Entries: 540
5	31014	27-28	4167771112	10	
5	31016	27-28	4167771113	10	

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 4 will send the calling party number as the **Private Prefix** plus the extension number.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	4	27-28	41677	10	Total Administered: 1
					Maximum Entries: 240

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

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	3			5	Total Administered: 12
5	31012	27-28	4167771111	10	Maximum Entries: 240
5	31014	27-28	4167771112	10	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.
5	31016	27-28	4167771113	10	

5.9. Outbound Routing

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 3		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	fac	9	1	fac			
00	3	fac	*	2	fac			
01	3	fac	#	2	fac			
1	3	dac						
2	5	ext						
3	5	ext						
4	5	ext						
44	5	ext						
5	5	ext						
50	4	ext						
6	5	ext						
7	5	ext						
732	10	udp						
777	7	udp						
8	1	fac						

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

```

change feature-access-codes                                     Page 1 of 10
                                FEATURE ACCESS CODE (FAC)
    Abbreviated Dialing List1 Access Code:
    Abbreviated Dialing List2 Access Code:
    Abbreviated Dialing List3 Access Code:
    Abbreviated Dial - Prgm Group List Access Code:
        Announcement Access Code: 001
        Answer Back Access Code:
        Attendant Access Code:
    Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
        Automatic Callback Activation:      Deactivation:
    Call Forwarding Activation Busy/DA: *2    All: *1    Deactivation: #1
    Call Forwarding Enhanced Status:      Act:      Deactivation:
        Call Park Access Code:
        Call Pickup Access Code:
    CAS Remote Hold/Answer Hold-Unhold Access Code:
        CDR Account Code Access Code:
        Change COR Access Code:

```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 1.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 28 which contains the SIP trunk to the service provider (as defined next).

```

change ars analysis 0                                     Page 1 of 2
                                ARS DIGIT ANALYSIS TABLE
                                Location: all                Percent Full: 2

```

	Dialed String	Total Min Max	Route Pattern	Call Type	Node Num	ANI Reqd
	0	1 1	28	op		n
	0	11 11	28	op		n
	00	2 2	28	op		n
	011	10 18	28	intl		n
	1800	11 11	28	fnpa		n
	1877	11 11	28	fnpa		n
	1908	11 11	28	fnpa		n
	411	3 3	28	svcl		n

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 28 for the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 28 was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk: 1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for the long distance North American Numbering Plan (NANP) numbers. All HNP 10 digit numbers are left unchanged.
- **Numbering Format: unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR: next**

change route-pattern 28															Page	1	of	3									
															Pattern Number: 2		Pattern Name: To Bell Canada										
															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:	28	0		1											n	user											
2:															n	user											
3:															n	user											
4:															n	user											
5:															n	user											
6:															n	user											
															BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR		
															0	1	2	M	4	W	Request					Dgts	Format
																							Subaddress				
1:	y	y	y	y	y	n	n	rest							unk-unk	next											
2:	y	y	y	y	y	n	n	rest								none											
3:	y	y	y	y	y	n	n	rest								none											
4:	y	y	y	y	y	n	n	rest								none											

5.10. Vector Directory Numbers (VDNs) and Vectors for SIP NCR

This section describes the basic commands used to configure Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke the Communication Manager SIP Network Call Redirection (NCR) functionality. These Application Notes provide rudimentary vector definitions to demonstrate and test the SIP NCR and UII functionalities. In general, call centers will use vector functionality that is more complex and tailored to individual needs. Call centers may also use customer hosts running applications used in conjunction with Avaya Aura® Application Enablement Services (AES) to define call routing and provide

associated UUI. The definition and documentation of those complex applications and associated vectors are beyond the scope of these Application Notes.

5.10.1. Post-Answer Redirection to a PSTN Destination

This section provides an example configuration of a vector that will use post-answer redirection to a PSTN destination. In this example, the inbound DID number is routed to VDN 36200 shown in the following abridged screen. The originally dialed DID number may be mapped to VDN 36200 by Session Manager digit conversion, or via the incoming call handling treatment for the inbound trunk group on Communication Manager.

display vdn 36200	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 36200	
Name*: Refer-Vector	
Destination: Vector Number	31
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	

VDN 36200 is associated with vector 31, which is shown below. Vector 31 plays an announcement (step 02) to answer the call. After the announcement, the **route-to number** (step 03) includes **~r19085551212** where the number 908-555-1212 is a PSTN destination. This step causes a REFER message to be sent where the Refer-To header includes 19085551212 as the user portion. If Refer triggered by step 03 fails, an announcement will be played and the call is disconnected (step 04).

display vector 31	Page 1 of 6
CALL VECTOR	
Number: 31	
Name: Refer-to-PSTN	
Multimedia? n	Attendant Vectoring? n
Basic? y	EAS? y
Prompting? y	LAI? y
Variables? y	3.0 Enhanced? y
01 wait-time 2 secs hearing ringback	
02 announcement 36000	
03 route-to number ~r19085551212 with cov n if unconditionally	
04 disconnect after announcement 36300	
05	
06	

5.10.2. Post-Answer Redirection With UUI to a SIP Destination

This section provides an example of post-answer redirection with UUI passed to a SIP destination. In this example, the inbound call is routed to VDN 36201 shown in the following abridged screen. The originally dialed DID number may be mapped to VDN 36201 by Session

Manager digit conversion, or via the incoming call handling treatment for the inbound trunk group on Communication Manager.

display vdn 36201	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 36201	
Name*: Refer-Vector-with-UUI	
Destination: Vector Number 32	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	

To facilitate testing of NCR with UUI, the following vector variables were defined.

change variables						Page 1 of 39
VARIABLES FOR VECTORS						
Var	Description	Type	Scope	Length	Start	Assignment VAC
A	Test1	asaiuui	L	16	1	
B						
C						
D						

VDN 36201 is associated with vector 32, which is shown below. Vector 32 sets data in the vector variable A (steps 01) and plays an announcement to answer the call (step 03). After the announcement, the **route-to** number step includes **~r18005551212**. This step causes a REFER message to be sent where the Refer-To header includes 18005551212 as the user portion. The Refer-To header will also contain the UII set in variables A. Service provider should include this UII in the INVITE ultimately sent to the SIP-connected target of the Refer. In practice, NCR with UII allows Communication Manager to send call or customer-related data along with the call to another contact center. If Refer triggered by step 04 fails, an announcement will be played and the call is disconnected (step 05).

```

display vector 32                                     Page 1 of
6
                                CALL VECTOR

    Number: 32                                Name: Refer-with-UII
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
    Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
    Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
    Variables? y      3.0 Enhanced? y01 wait-time      2      secs hearing ringback
01 set      A      = none      CATR 1234567890123456
02 wait-time      2      secs hearing ringback
03 announcement 36000
04 route-to      number ~r18005551212      with cov n if unconditionally
05 disconnect      after announcement 36300
06

```

5.11. Saving Communication Manager Configuration Changes

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

6. Configure Avaya Aura® Session Manager

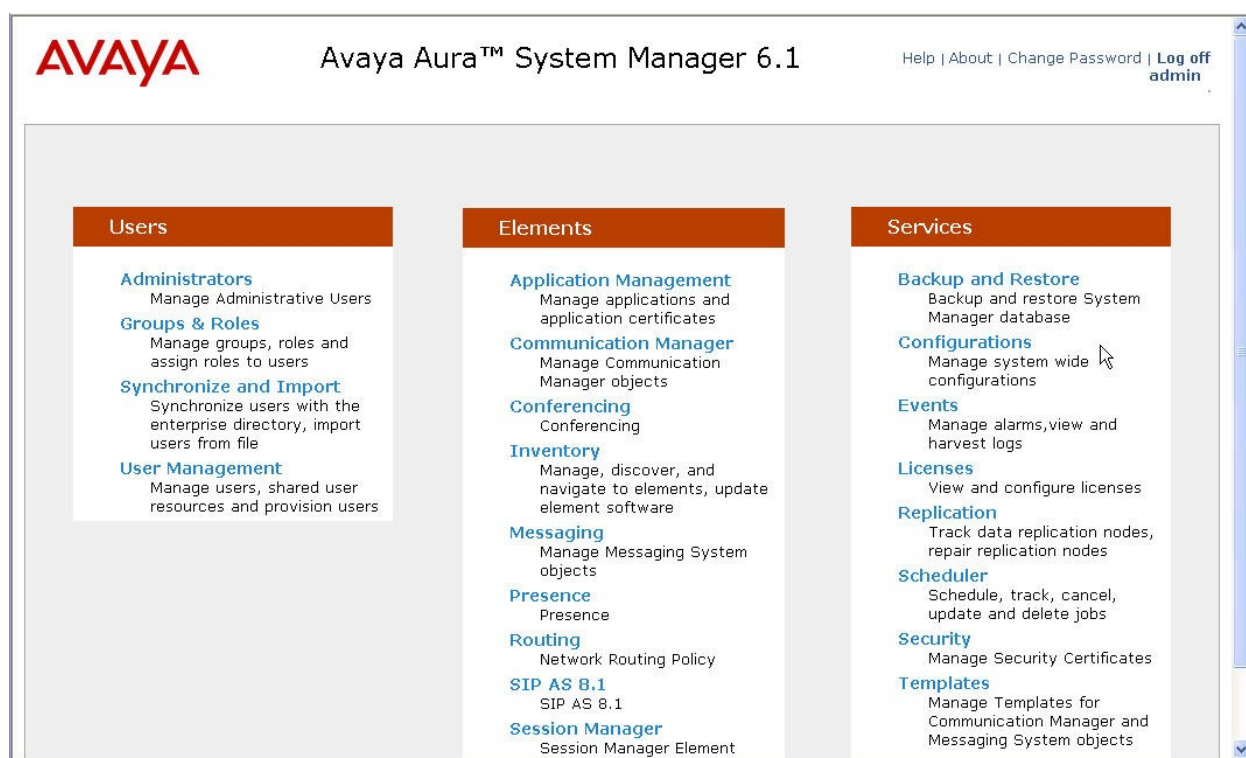
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

6.1. System Manager Login and Navigation

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



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

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

The screenshot displays the Avaya Aura™ System Manager 6.1 web interface. The top header includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off admin. A breadcrumb trail shows the path: Home /Elements / Routing- Introduction to Network Routing Policy. The left navigation pane lists various configuration categories under 'Routing', including Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Introduction to Network Routing Policy' and provides an overview of the network routing policy, listing several routing applications like Domains, Locations, SIP Entities, etc. It outlines a recommended order for configuration: Step 1: Create 'Domains' of type SIP; Step 2: Create 'Locations'; Step 3: Create 'Adaptations'; Step 4: Create 'SIP Entities' (with sub-points for Outbound Proxies, other SIP Entities, and Assigning Locations/Adaptations/Outbound Proxies); Step 5: Create 'Entity Links' (with sub-points for Session Managers and between Session Managers and other SIP Entities); Step 6: Create 'Time Ranges'.

AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home /Elements / Routing- Introduction to Network Routing Policy

Introduction to Network Routing Policy

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

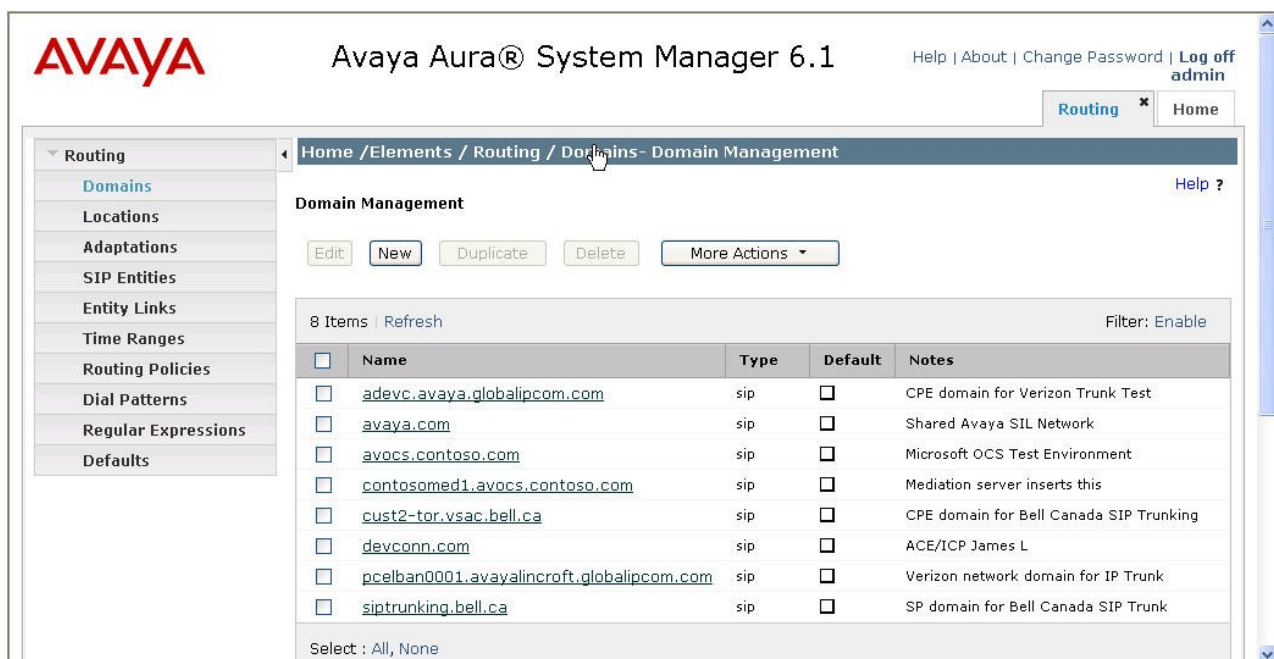
The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- 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"

6.2. Specify SIP Domain

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among many Avaya interoperability test efforts. The domain **avaya.com** was already being used for communication among a number of Avaya systems and applications, including an Avaya Modular Messaging system with SIP integration to Session Manager. The domain **avaya.com** is not known to the Bell Canada SIP Trunking service.



The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. The left sidebar shows a tree view with 'Routing' expanded, and 'Domains' selected. The main content area is titled 'Domain Management' and includes buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these buttons is a table with 8 items, showing a list of SIP domains. The table has columns for 'Name', 'Type', 'Default', and 'Notes'. The 'avaya.com' domain is highlighted in blue.

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	adevc.avaya.globalipcom.com	sip	<input type="checkbox"/>	CPE domain for Verizon Trunk Test
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>	Shared Avaya SIL Network
<input type="checkbox"/>	avocs.contoso.com	sip	<input type="checkbox"/>	Microsoft OCS Test Environment
<input type="checkbox"/>	contosomed1.avocs.contoso.com	sip	<input type="checkbox"/>	Mediation server inserts this
<input type="checkbox"/>	cust2-tor.vsac.bell.ca	sip	<input type="checkbox"/>	CPE domain for Bell Canada SIP Trunking
<input type="checkbox"/>	devconn.com	sip	<input type="checkbox"/>	ACE/ICP James L
<input type="checkbox"/>	pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon network domain for IP Trunk
<input type="checkbox"/>	siptrunking.bell.ca	sip	<input type="checkbox"/>	SP domain for Bell Canada SIP Trunk

Select : All, None

The domain **cust2-tor.vsac.bell.ca** is the domain known to Bell Canada as the enterprise SIP domain. For example, for calls from the enterprise to the network, this domain can appear in the P-Asserted-Identity header in the INVITE message sent to Bell Canada's SIP Trunking service.

The screenshot shows the 'Domain Management' interface. On the left is a navigation pane with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains - Domain Management' and a 'Help ?' link. Below the breadcrumb is a 'Domain Management' section with 'Commit' and 'Cancel' buttons. A table lists domains with columns 'Name', 'Type', 'Default', and 'Notes'. One item is shown: 'cust2-tor.vsac.bell.ca' with type 'sip' and note 'CPE domain for Bell Canada SIP Trunk'. Below the table is a red asterisk and the text '* Input Required', followed by 'Commit' and 'Cancel' buttons.

Name	Type	Default	Notes
* cust2-tor.vsac.bell.ca	sip	<input type="checkbox"/>	CPE domain for Bell Canada SIP Trunk

The domain **siptrunking.bell.ca** is associated with the Bell Canada network in the sample configuration. For example, for calls from the enterprise site to Bell Canada, this domain can appear in the Request-URI in the INVITE message sent to Bell Canada. The following screen shows the relevant configuration.

The screenshot shows the 'Domain Management' interface. On the left is a navigation pane with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains - Domain Management' and a 'Help ?' link. Below the breadcrumb is a 'Domain Management' section with 'Commit' and 'Cancel' buttons. A table lists domains with columns 'Name', 'Type', 'Default', and 'Notes'. One item is shown: 'siptrunking.bell.ca' with type 'sip' and note 'SP domain for Bell Canada SIP Trunk'. Below the table is a red asterisk and the text '* Input Required', followed by 'Commit' and 'Cancel' buttons.

Name	Type	Default	Notes
* siptrunking.bell.ca	sip	<input type="checkbox"/>	SP domain for Bell Canada SIP Trunk

6.3. Add Location

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

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

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

In the **Location Pattern** section (see 2nd screen below), click **Add** and enter the following values:

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

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

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

Routing Home

Home / Elements / Routing / Locations - Location Details

Location Details Commit Cancel Help ?

General

* **Name:** BaskingRidge HQ

Notes: CME, CS1K R5 & R7, AAC R6, CM

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* **Default Audio Bandwidth:** 80 Kbit/sec

Location Pattern

Add Remove

5 Items Refresh Filter: Enable

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

Select : All, None

* **Input Required** Commit Cancel

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

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

AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) * [Home](#)

Home / Elements / Routing / Locations - Location Details

Location Details [Help ?](#)

[Commit](#) [Cancel](#)

General

* **Name:** AA-SBC

Notes: SIP Trunking test

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* **Default Audio Bandwidth:** 80 Kbit/sec

Location Pattern

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

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

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

Select : All, None

* **Input Required** [Commit](#) [Cancel](#)

6.4. 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.

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

The following screen shows a portion of the list of adaptations in the sample configuration.

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	AcmeAdapt	DigitConversionAdapter odstd=138.210.71.242		Change RURI To Dest IP
<input type="checkbox"/>	Avaya-R6.0	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
<input type="checkbox"/>	BC AA-SBC	DigitConversionAdapter osrcd=cust2-tor.vsac.bell.ca odstd=siptrunking.bell.ca fromto=true		convert to BC's domains
<input type="checkbox"/>	BC CM-ES	DigitConversionAdapter odstd=avaya.com		avaya.com for shared SIL ntwk
<input type="checkbox"/>	BCM Adapter	DigitConversionAdapter avaya.com		Delete prefix
<input type="checkbox"/>	Cisco-ISR	CiscoAdapter avaya.com		
<input type="checkbox"/>	Cisco-UCM513	CiscoAdapter 192.45.130.105		
<input type="checkbox"/>	Cisco-UCM6	CiscoAdapter avaya.com		
<input type="checkbox"/>	Cisco-UCM7	CiscoAdapter avaya.com		
<input type="checkbox"/>	CiscoUCME	CiscoAdapter iosrcd=avaya.com odstd=192.45.131.1		
<input type="checkbox"/>	CM5-2-1 Adapt	DigitConversionAdapter osrcd=avaya.com		Tim For CLink Testing
<input type="checkbox"/>	CM-AE-VZ inbound	DigitConversionAdapter odstd=avaya.com		Avaya.com for shared SIL ntwk

The adaptations named **BC AA-SBC** and **BC CM-ES** were configured and used in the compliance test.

The **BC AA-SBC** adaptation will later be assigned to the AA-SBC SIP Entity. This adaptation uses the **DigitConversionAdapter** and specifies three parameters used to adapt the FQDN to the domains expected by the Bell Canada network in the sample configuration.

- **osrcd=cust2-tor.vsac.bell.ca**. This configuration enables the outbound source domain to be overwritten with **cust2-tor.vsac.bell.ca**. For example, for outbound PSTN calls from the Avaya CPE to Bell Canada, the PAI header will contain “cust2-tor.vsac.bell.ca” as expected by Bell Canada.
- **odstd=siptrunking.bell.ca**. This configuration enables the outbound destination domain to be overwritten with **siptrunking.bell.ca**. For example, for outbound PSTN calls from

the Avaya CPE to Bell Canada, the Request-URI will contain **siptrunking.bell.ca** as expected by Bell Canada.

- **fromto=true**. With this configuration, for an outbound call to Bell Canada, Session Manager 6.1 will set the host portion of both the PAI and the From headers to **cust2-tor.vsac.bell.ca**, and the host portion of the Request-URI and To headers to siptrunking.bell.ca

Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domains in this fashion. In the sample configuration, where **avaya.com** was already in use in a shared Avaya environment, Session Manager was used to adapt the domain from **avaya.com** to **cust2-tor.vsac.bell.ca** where the latter is the CPE domain known to Bell Canada.

The screen below shows the **BC AA-SBC** adaptation configured for the testing associated with these Application Notes:

The screenshot shows the 'Adaptation Details' page for 'BC AA-SBC'. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations (selected), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail: Home / Elements / Routing / Adaptations - Adaptation Details. Below this is the 'Adaptation Details' section with a 'General' tab. The 'General' tab contains the following fields: 'Adaptation name' (BC AA-SBC), 'Module name' (DigitConversionAdapter), 'Module parameter' (d=siptrunking.bell.ca fromto=true), 'Egress URI Parameters' (empty), and 'Notes' (convert to BC's domains). There are 'Commit' and 'Cancel' buttons at the top right. Below the 'General' tab is a section for 'Digit Conversion for Incoming Calls to SM' with 'Add' and 'Remove' buttons, a table with 0 items, and a 'Filter: Enable' button. The table has columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, and Notes. Below this is a similar section for 'Digit Conversion for Outgoing Calls from SM'. At the bottom, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

The adaptation named **BC CM-ES** shown below will later be assigned to the Communication Manager SIP Entity for calls to and from Bell Canada. This adaptation uses the **DigitConversionAdapter** and specifies the **odstd=avaya.com** parameter to adapt the domain to the domain expected by Communication Manager. More specifically, this configuration enables the destination domain to be overwritten with **avaya.com** for calls that egress to a SIP entity using this adapter. For example, for inbound PSTN calls from Bell Canada to the Avaya CPE, the Request-URI header sent to Communication Manager will contain **avaya.com** as expected by Communication Manager in the shared Avaya test Lab environment. Depending on the

Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.

The screenshot shows the 'Adaptation Details' page for 'BC CM-ES'. The left sidebar lists navigation options: Routing, Domains, Locations, Adaptations (selected), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail 'Home / Elements / Routing / Adaptations - Adaptation Details' and a 'Help ?' link. Below the breadcrumb is the 'Adaptation Details' section with a 'General' tab. The 'General' tab contains the following fields:

- * Adaptation name:** BC CM-ES
- Module name:** DigitConversionAdapter (dropdown menu)
- Module parameter:** odstd=avaya.com
- Egress URI Parameters:** (empty text field)
- Notes:** avaya.com for shared SIL ntwk

 At the top right of the main content area are 'Commit' and 'Cancel' buttons.

Scrolling down, the following screen shows a portion of the **BC CM-ES** adaptation that can be used to convert digits between the extension numbers used on Communication Manager and the 10 digit DID numbers assigned by Bell Canada. Since this adaptation will be applied to the Communication Manager SIP Entity later on, the settings for **incoming calls to SM** correspond with outgoing calls from Communication Manager to the PSTN using the Bell Canada SIP Trunking service. Similarly, the settings for **outgoing calls from SM** correspond to incoming calls from the PSTN that are routed by Session Manager to Communication Manager. In general, digit conversion such as this, that converts a Communication Manager extension (e.g., 31012) to a corresponding LDN or DID number known to the PSTN (e.g., 4167771111), can be performed in Communication Manager (e.g., using public unknown numbering and incoming call handling treatment for the Communication Manager trunk group) or in Session Manager as shown below.

The screenshot shows the 'Digit Conversion' configuration page, divided into two sections: 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM'. Each section has 'Add' and 'Remove' buttons and a table of conversion rules.

Digit Conversion for Incoming Calls to SM:

- Buttons: Add, Remove
- Table headers: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Notes
- Table content:

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 31012	* 5	* 5		* 5	4167771111	both	
<input type="checkbox"/>	* 31014	* 5	* 5		* 5	4167771112	both	
<input type="checkbox"/>	* 36200	* 5	* 5		* 5	4167771113	both	
- Footer: Select : All, None

Digit Conversion for Outgoing Calls from SM:

- Buttons: Add, Remove
- Table headers: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Notes
- Table content:

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 4167771111	* 10	* 10		* 10	31012	both	
<input type="checkbox"/>	* 4167771112	* 10	* 10		* 10	31014	both	
<input type="checkbox"/>	* 4167771113	* 10	* 10		* 10	36200	both	

In the example shown above, if a user on the PSTN dials 416-777-1111, Session Manager will convert the number to 31012 before sending the SIP INVITE to Communication Manager. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. For an outbound call, if extension 31012 dials the PSTN, and if Communication Manager sends the extension 31012 to Session Manager as the calling number, Session Manager would convert the calling number to 4167771111. Alternatively, the Communication Manager private-numbering form could have an entry to convert 31012 to 4167771111 before sending the call on the trunk group to Session Manager (as shown in **Section 5.8**).

Note that in the above screen, the DID number 4167771113 was mapped to 36200, a Vector Directory Number (VDN) on Communication Manager. In the compliance test, the digit conversions (or number mappings) in Session Manager **adaptation** as well as in **private-numbering** and **public-unknown-numbering** tables (see **Section 5.8**) were varied to route inbound calls to various destinations for different test cases.

6.5. Add SIP Entities

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

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for the AA-SBC.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation** name created in **Section 6.4** 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 SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

The screenshot shows a web application window titled "Home / Elements / Routing / SIP Entities - SIP Entity Details". On the left is a navigation pane with a tree view containing: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "SIP Entity Details" and has a "General" tab selected. At the top right of the main area are "Commit" and "Cancel" buttons, and a "Help ?" link. The form fields are as follows: "Name:" with a text box containing "SM1"; "* FQDN or IP Address:" with a text box containing "10.1.2.210"; "Type:" with a dropdown menu showing "Session Manager"; "Notes:" with a text box; "Location:" with a dropdown menu; "Outbound Proxy:" with a dropdown menu; "Time Zone:" with a dropdown menu showing "America/New_York"; "Credential name:" with a text box; and "SIP Link Monitoring:" with a dropdown menu showing "Use Session Manager Configuration".

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

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

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

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

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

- **5060** with **TCP** for connecting to AA-SBC
- **5064** with **TCP** for connecting to Communication Manager

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

Port

Add Remove

8 Items Refresh Filter: Enable

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

Select : All, None

* Input Required

Commit Cancel

The following screen shows the addition of Communication Manager SIP Entity. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of the Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for digit manipulation in **Section 6.4**.

The screenshot displays the 'SIP Entity Details' configuration page. On the left is a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), 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' and a 'Help ?' link. Below the breadcrumb is the 'SIP Entity Details' title and 'Commit'/'Cancel' buttons. The 'General' tab is active, showing the following fields:

- Name:** CM601-Evolution-procr-5064
- * FQDN or IP Address:** 10.1.2.220
- Type:** CM
- Notes:** CM 6.01-ES procr IP, different po
- Adaptation:** BC CM-ES
- Location:** BaskingRidge HQ
- Time Zone:** America/New_York
- Override Port & Transport with DNS SRV:** ☐
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

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

The screenshot displays the 'SIP Entity Details' configuration page for 'SIPTrunking-AuraSBC'. The left sidebar shows a navigation menu with 'Routing' expanded, containing sub-items: Domains, Locations, Adaptations, SIP Entities (highlighted), 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' and a 'Help ?' link. Below the breadcrumb is the 'SIP Entity Details' title and 'Commit'/'Cancel' buttons. The 'General' tab is active, showing fields for Name, FQDN or IP Address, Type, Notes, Adaptation, Location, Time Zone, and an 'Override Port & Transport with DNS SRV' checkbox. The 'SIP Link Monitoring' section is also visible, showing 'SIP Link Monitoring' set to 'Link Monitoring Enabled', 'Proactive Monitoring Interval' set to 60 seconds, 'Reactive Monitoring Interval' set to 30 seconds, and 'Number of Retries' set to 1.

Routing

- Domains
- Locations
- Adaptations
- SIP Entities**
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

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

SIP Entity Details

Commit Cancel Help ?

General

* Name: SIPTrunking-AuraSBC

* FQDN or IP Address: 10.1.2.243

Type: Other

Notes: AuraSBC connecting to SM6.1

Adaptation: BC AA-SBC

Location: AA-SBC

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 60

* Reactive Monitoring Interval (in seconds): 30

* Number of Retries: 1

6.6. Add Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.5**. For AA-SBC, select the AA-SBC SIP Entity defined in **Section 6.5**.
- **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 5.6**.
- **Trusted:** Check this box. Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** 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 5.6**.

Entity Link to Communication Manager:

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ? Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* CM601-ES-procr-506	* SM1	TCP	* 5064	* CM601-Evolution-procr-5064	* 5064	<input checked="" type="checkbox"/>

* Input Required Commit Cancel

Entity Link to the AA-SBC:

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ? Commit Cancel

1 Item | Refresh Filter: Enable

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

* Input Required Commit Cancel

Note that there existed a separate Entity Link between Communication Manager and Session Manager (not shown) in the shared configuration prior to adding the configuration related to Bell Canada SIP Trunking testing. This link, using port 5060, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Bell Canada, such as traffic related to SIP Telephones registered to Session Manager, or traffic related to Avaya Modular Messaging, which has SIP integration to Session Manager.

6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. 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:

- **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 'CM-ES-R601-BC-Inbound'. The left navigation pane is expanded to 'Routing Policies'. The 'General' section is active, showing the policy name, a 'Disabled' checkbox, and a note 'Inbound BC DID to CM port 5064'. The 'SIP Entity as Destination' section has a 'Select' button. Below is a table of available SIP entities.

Name	FQDN or IP Address	Type	Notes
CM601-Evolution-procr-5064	10.1.2.220	CM	CM 6.01-ES procr IP, different port

The screenshot shows the 'Routing Policy Details' page for a policy named 'SIPTrunking-AuraSBC'. The left navigation pane is expanded to 'Routing Policies'. The 'General' section is active, showing the policy name, a 'Disabled' checkbox, and a note 'To Service Provider SIP Trunking'. The 'SIP Entity as Destination' section has a 'Select' button. Below is a table of available SIP entities.

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

6.8. Add Dial Patterns

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

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

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

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

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

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

The first example shows that 11-digit dialed numbers that begin with **1908** and have a destination domain of **siptrunking.bell.ca** uses route policy **SIPTrunking-AuraSBC** as defined in **Section 6.7**.

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

Dial Pattern Details Help ? Commit Cancel

General

* **Pattern:** 1908

* **Min:** 11

* **Max:** 11

Emergency Call: ☐

SIP Domain: siptrunking.bell.ca

Notes: PSTN call through AuraSBC to Service Provider

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: Enable

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

Select : All, None

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

The second example shows that inbound 10-digit numbers that start with **416777** to domain **cust2-tor.vsac.bell.ca** and originating from Location **AA-SBC** uses route policy **CM-ES-R601-BC-Inbound** as defined in **Section 6.7**. These are the DID numbers assigned to the enterprise from Bell Canada. Location **AA-SBC** is selected because these calls come via AA-SBC.

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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

Help ?

Commit

Cancel

Dial Pattern Details

General

* Pattern:

416777

* Min:

10

* Max:

10

Emergency Call:

☐

SIP Domain:

cust2-tor.vsac.bell.ca

Notes:

Bell Canada DID to SM61-CM601

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	AA-SBC	SIP Trunking test	CM-ES-R601-BC-Inbound	0	<input type="checkbox"/>	CM601-Evolution-procr-5064	Inbound BC DID to CM port 5064

Select : All, None

6.9. Add/View Session Manager

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

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

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

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

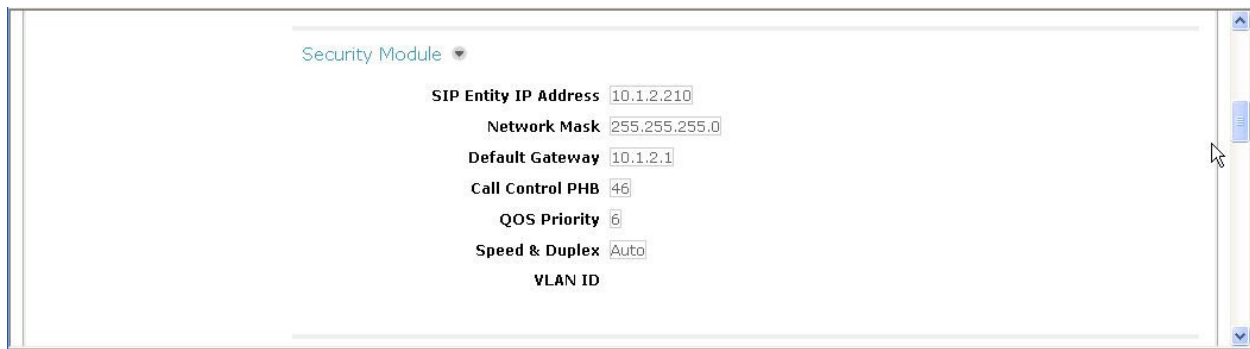
The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. A breadcrumb trail shows 'Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration'. The left navigation pane lists various configuration categories, with 'Session Manager Administration' selected. The main content area is titled 'View Session Manager' and contains a 'Return' button. Below this, a tabbed interface shows the 'General' tab selected, displaying the following configuration details:

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

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

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

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



The screenshot displays a configuration window titled "Security Module" with a dropdown arrow. Below the title, several configuration fields are listed, each with a text input box containing a default value:

- SIP Entity IP Address:** 10.1.2.210
- Network Mask:** 255.255.255.0
- Default Gateway:** 10.1.2.1
- Call Control PHB:** 46
- QOS Priority:** 6
- Speed & Duplex:** Auto
- VLAN ID:** (empty field)

7. Configure Avaya Aura® Session Border Controller

The AA-SBC configuration is done in two parts. The first part is done during the AA-SBC installation via the installation wizard. These Application Notes will not cover the AA-SBC installation in its entirety but will include the use of the installation wizard (invoked during the loading of AA-SBC template) for entering network and SBC settings. For information on installing the Avaya Aura® System Platform and the loading of the Avaya Aura® SBC template, see [1].

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

7.1. Installation Wizard

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

7.1.1. Network Settings

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

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

Click **Next Step** to continue.

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

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

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

7.1.2. VPN Access

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

Click **Next Step** to continue.

AVAYA

Home

Configuration

Installation

Network Settings

Logins

VPN Access

SBC

Summary

Finish

VPN Access

Configure VPN Access

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

☐ Yes ☒ No

VPN Access Configuration

VPN Router IP Address (Optional)

Remote Access Network

Remote Access Network Subnet Mask

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

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

If in doubt, please refer to the documentation.

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

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

7.1.3. SBC

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

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

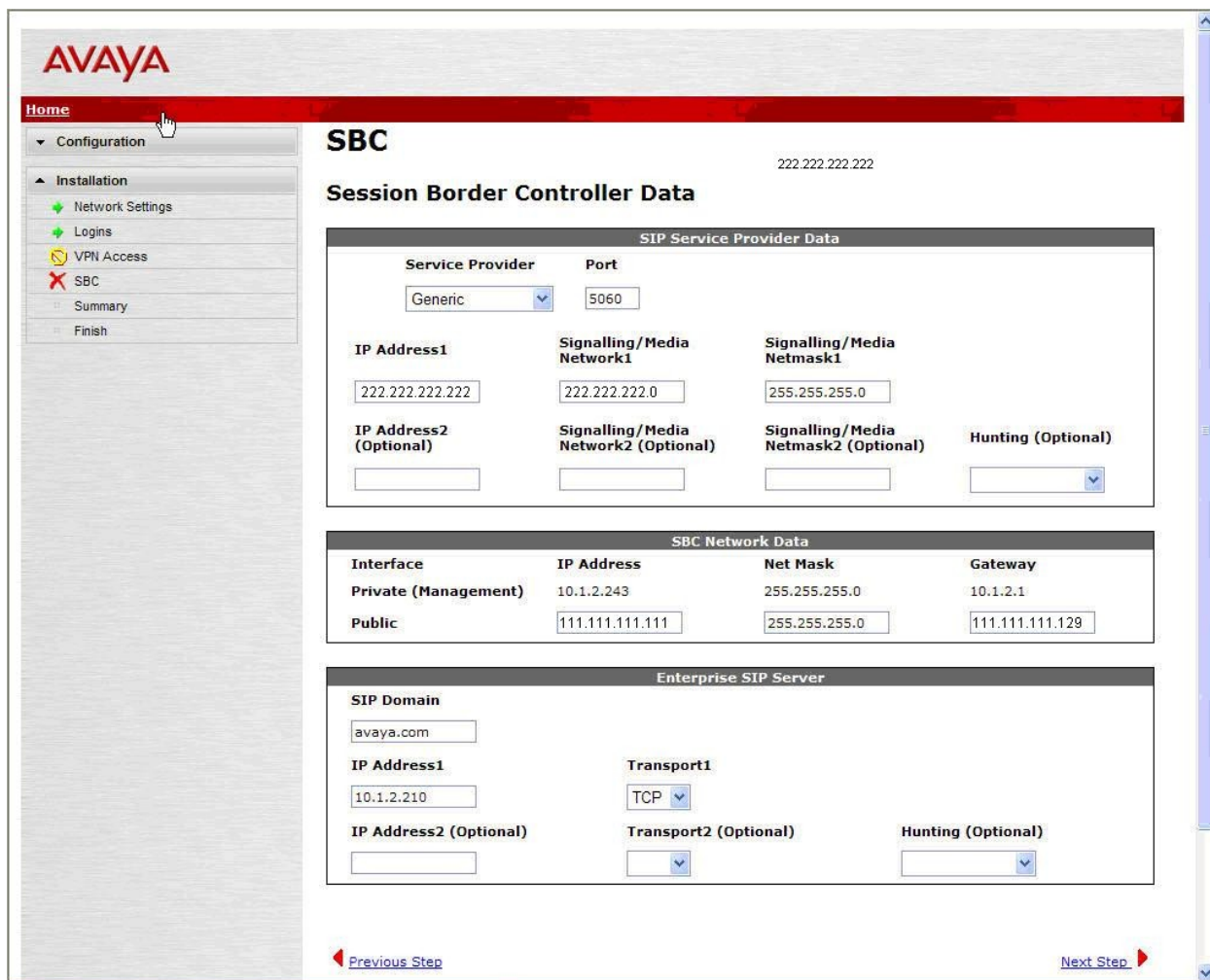
- **Service Provider:** From the pull-down menu, select the name of the service provider to which the AA-SBC will connect. This will allow the wizard to select a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for Bell Canada. 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 Bell Canada provided IP address of the Bell Canada SIP Proxy. If the service provider has multiple proxies, enter the primary proxy on this screen and additional proxies can be added after installation.
- **Signaling/Media Network1:** Enter the Bell Canada provided subnet where signaling/media traffic will originate. If signaling/media traffic can originate from multiple networks, enter one network address on this screen and additional networks can be added after installation.
- **Signaling/Media Netmask1:** Enter the netmask corresponding to **Signaling/Media Network1**.

In the **SBC Network Data** section:

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

In the **Enterprise SIP Server** section:

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



The screenshot shows the Avaya SBC configuration wizard. The left sidebar contains a navigation menu with 'Configuration' expanded, showing 'Installation' as the current step. The main area is titled 'SBC' and 'Session Border Controller Data'. It contains three sections: 'SIP Service Provider Data', 'SBC Network Data', and 'Enterprise SIP Server'. The 'SIP Service Provider Data' section has fields for 'Service Provider' (Generic), 'Port' (5060), 'IP Address1' (222.222.222.222), 'Signalling/Media Network1' (222.222.222.0), 'Signalling/Media Netmask1' (255.255.255.0), 'IP Address2 (Optional)', 'Signalling/Media Network2 (Optional)', 'Signalling/Media Netmask2 (Optional)', and 'Hunting (Optional)'. The 'SBC Network Data' section has a table with columns 'Interface', 'IP Address', 'Net Mask', and 'Gateway', containing data for 'Private (Management)' and 'Public' interfaces. The 'Enterprise SIP Server' section has fields for 'SIP Domain' (avaya.com), 'IP Address1' (10.1.2.210), 'Transport1' (TCP), 'IP Address2 (Optional)', 'Transport2 (Optional)', and 'Hunting (Optional)'. At the bottom, there are 'Previous Step' and 'Next Step' buttons.

AVAYA

Home

Configuration

Installation

Network Settings

Logins

VPN Access

SBC

Summary

Finish

SBC

222.222.222.222

Session Border Controller Data

SIP Service Provider Data

Service Provider	Port
Generic	5060

IP Address1	Signalling/Media Network1	Signalling/Media Netmask1
222.222.222.222	222.222.222.0	255.255.255.0

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

SBC Network Data

Interface	IP Address	Net Mask	Gateway
Private (Management)	10.1.2.243	255.255.255.0	10.1.2.1
Public	111.111.111.111	255.255.255.0	111.111.111.129

Enterprise SIP Server

SIP Domain	IP Address1	Transport1
avaya.com	10.1.2.210	TCP

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

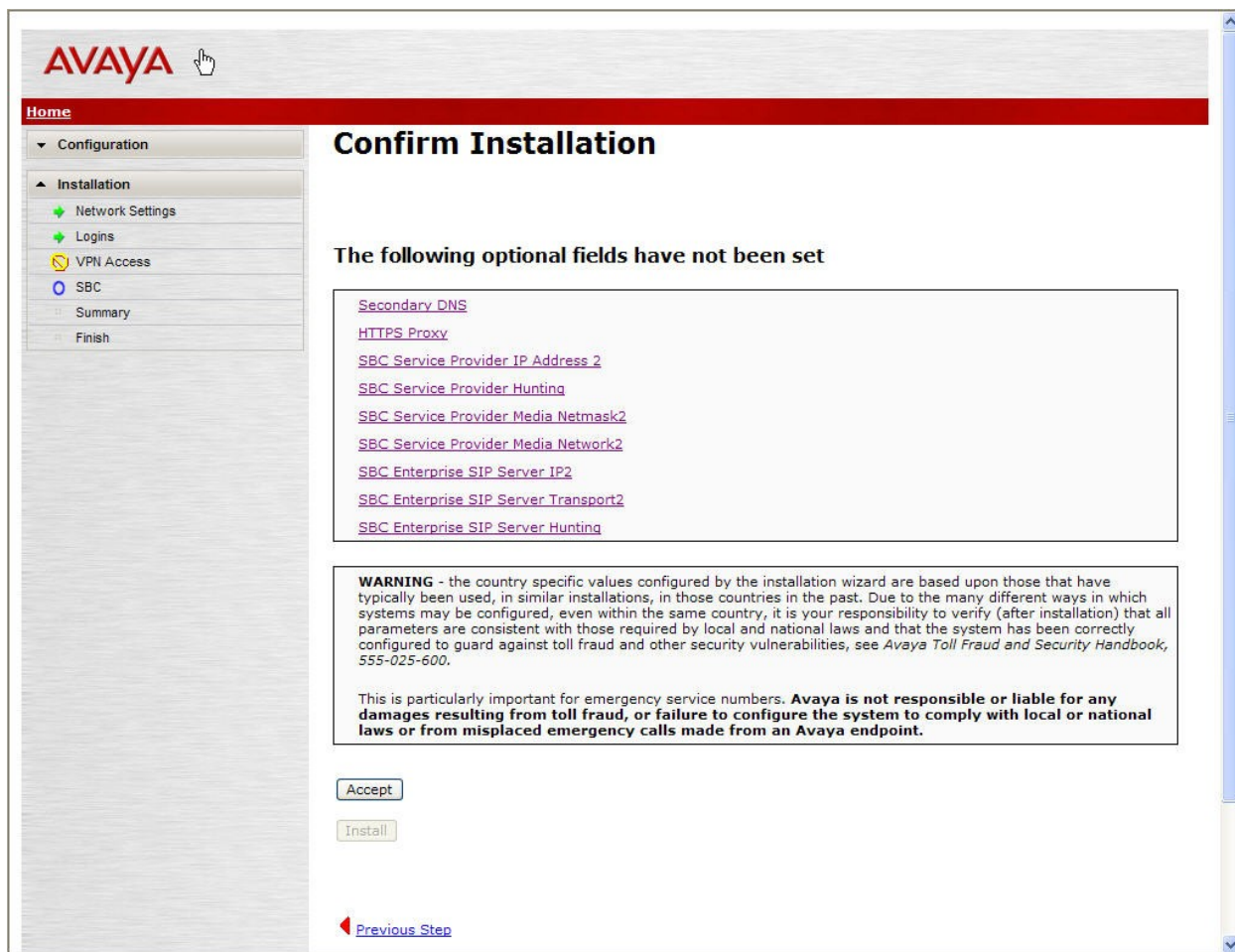
Previous Step

Next Step

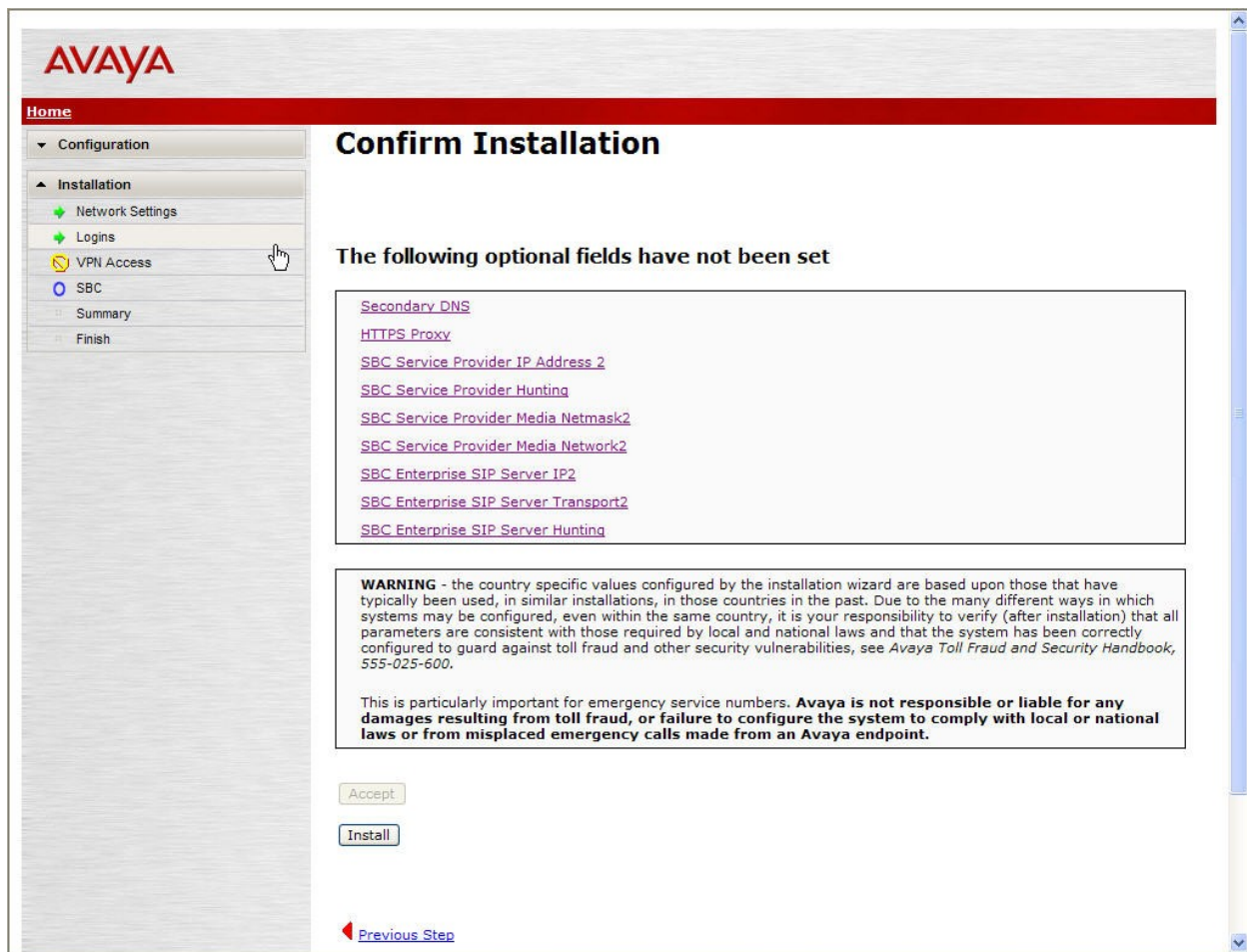
Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to continue to the final step.

7.1.4. Confirm Installation

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



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



Click **Install** to continue the overall template installation.

7.2. Post Installation Configuration

The installation wizard configures the Session Border Controller for use with the service provider chosen in **Section 7.1.3**. 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 7.1.1**. Log in with proper credentials.

Acme Packet Net-Net OS-E

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

Username:

Password:

7.2.1. Options Frequency

To set the frequency of the OPTIONS messages sent from the SBC to the service provider, first navigate to **vsp** → **enterprise** → **servers** → **sig-gateway Telco**. Click **Show Advanced**.

Configuration: all

Configuration Setup View

cluster

- box:AuraSBC.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - enterprise
 - servers
 - sig-gateway PBX
 - sig-gateway Telco
 - dns
 - settings

Configure vspenterprise\servers\sig-gateway Telco

Show advanced Help Index

Set Reset Back Copy Delete

Manage connections, Log instant messages, Record media, Record files, Set up accounting, Change "from:" URI, Change "to:" URI

general:

* name Telco

admin enabled (Resource is active)

domain

failover-detection ping (Use OPTIONS to detect failures)

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

Configuration: all

Configuration Setup View

cluster

- box:AuraSBC.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - enterprise
 - servers
 - sig-gateway PBX
 - sig-gateway Telco
 - dns
 - settings

servers:

server-type sip-proxy

server-pool [Delete]

routing:

routing-setting normalization

auto-tag-match

auto-domain-match

pstn-backup

Select All Unselect All

domain-alias Edit domain-alias

domain-subnet Edit domain-subnet

loop-detection tight (Compare source and destination address/port/transport)

service-type provider (Provider peer)

ping-interval 60 seconds

registration:

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

7.2.2. Blocked Headers

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

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 main content area is titled "Configure vsp/default-session-config/header-settings" and includes a "Show basic" button and links for Help and Index. Below the title are buttons for Set, Reset, Back, and Delete. The left sidebar shows a tree view of the configuration hierarchy, with "header-settings" selected. The main table lists various configuration options:

Configuration Option	Value / Action
pAssert-mode	disabled (Resource is inactive)
header-to-strip	Edit header-to-strip
allowed-header	Edit allowed-header
blocked-header	Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header
header-normalization	Add header-normalization
altered-body	Add altered-body
reg-ex-collector	Add reg-ex-collector
apply-allow-block-to	requests-and-responses (apply to requests and responses)
apply-to-allow-block-to-dialog	both (Apply to both inbound and outbound dialogs.)

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

Configuration: all

Configuration | Setup | View

- cluster
- vsp
 - default-session-config
 - media
 - sip-directive
 - log-alert
 - header-settings
 - third-party-call-control
 - tls
 - session-config-pool
 - dial-plan
 - enterprise
 - dns
 - settings

Configure vspdefault-session-configheader-settings blocked-header

Back

P-Site X

P-Location X

Add Remove All

OK

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

Configuration: all

Configuration | Setup | View

- cluster
- vsp
 - default-session-config
 - media
 - sip-directive
 - log-alert
 - header-settings
 - third-party-call-control
 - tls
 - session-config-pool
 - dial-plan
 - enterprise
 - dns
 - settings

Configure vspdefault-session-configheader-settings Show advanced Help

Index

Set Reset Back Delete

allowed-header	Edit allowed-header
blocked-header	P-Site P-Location Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header
header-normalization	Add header-normalization
altered-body	Add altered-body
reg-ex-collector	Add reg-ex-collector
apply-allow-block-to	requests-and-responses (apply to requests and responses)
apply-to-allow-block-to-dialog	both (Apply to both inbound and outbound dialogs.)

7.2.3. Diversion Header Domain Mapping

The configuration in this section is not required if the Avaya CPE domain configured in Communication Manager matches the domain configured in the Bell Canada network for the enterprise site. In the compliance test, the Avaya CPE domain configured in Communication Manager (avaya.com for shared use by various test projects) is different than the CPE domain expected by the Bell Canada network (cust2-tor.vvac.bell.ca), making this configuration necessary on AA-SBC for Diversion header domain mapping.

Session Manager can adapt the domain in Request-URI and various SIP headers such as From, To, and P-Asserted-Identity headers. As described in these Application Notes, the Session Manager's capability to adapt the domain in various headers allowed a shared Avaya test lab environment already configured for the CPE domain avaya.com to be used for Bell Canada SIP Trunking testing, even though the Bell Canada network understood the CPE domain to be cust2-tor.vvac.bell.ca. In the case of diverted calls like inbound calls to the enterprise forwarded back out to the PSTN, the domain in the Diversion header received at AA-SBC from Session Manager still contains avaya.com. To allow diverted calls to be processed properly in the shared configuration, the AA-SBC was used to convert the domain in the Diversion header to cust2-tor.vvac.bell.ca as expected by Bell Canada.

Navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. On the screen displayed on the right side (not shown), click **Add altered-header** link on the right (not shown).

The screen below shows the edit screen for a previously added altered-header.

In the **number** field, enter an appropriate unused number. Since this is the first altered-header rule, number 1 was used. In the **source-header** field, enter **Diversion**. In the source-field area,

- select **selection** from the **type** drop-down menu
- in the **value** field, either enter a value to match directly, or click the **regular expression** link for assistance in creating the proper **value**. In the sample configuration, the rule will match on **avaya.com** appearing in the Diversion header.
- in the **replacement** field, enter the domain to appear in the host portion of the Diversion header, in place of **avaya.com**. In the sample configuration, Bell Canada expects **cust2-tor.vvac.bell.ca** as shown below.

In the **destination** area, enter **Diversion**. In the **destination-field** area, select **host** from the **type** drop-down menu, since it is the host portion of the Diversion header that the change rule should apply.

Retain the default settings for other configuration fields. Click the **Create** button (not shown) if adding a new altered-header; click the **Set** button if editing an exiting altered-header.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar contains a tree view with the following structure:

- cluster
 - box: AuraSBC.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - entry ToTelco
 - to-uri-specification
 - from-uri-specification
 - request-uri-specification
 - p-asserted-identity-uri
 - contact-uri-settings-in
 - contact-uri-settings-out
 - authentication
 - header-settings
 - entry ToPBX
 - entry Discard
 - dial-plan
 - enterprise
 - dns
 - settings

The main configuration area is titled 'Configure vsp|session-config-pool|entry ToTelco|header-settings|altered-header 1'. It includes buttons for 'Show advanced', 'Help', 'Index', 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The configuration fields are as follows:

- admin**: enabled (Resource is active)
- * number**: 1
- * source-header**: enter Diversion or select from Diversion
- * source-field**:
 - * type**: selection (Regular expression based selection of portion of the URL.)
 - * value**: .*avaya\.com (regular expression)
 - * replacement**: cust2-tor.vsac.bell.ca
- * destination**: enter Diversion or select from Diversion
- * destination-field**:
 - * type**: host (Host portion of the URL.)
- apply-to-methods**: INVITE, REFER

If the **regular expression** link is clicked in the screen shown above, the screen shown below is presented for assistance in generating the regular expression using simple language choices like **Match Any**. Enter the string to match in the **Enter String Pattern** field, and click the appropriate radio button such as **Match Any**, and press **OK**.

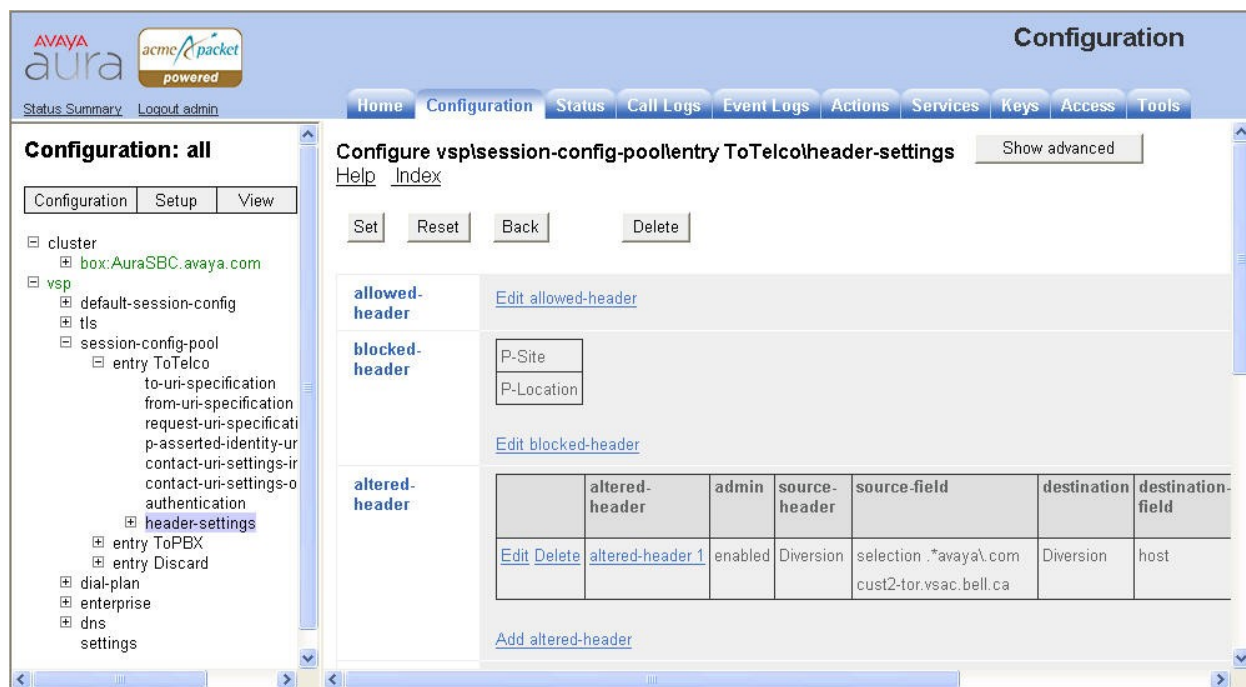
(regular expression)

You can set the match option so that the system matches the entire string, the beginning or end of the string, or any part of the string.

The 'Enter String Pattern' dialog box contains the following fields and options:

- Enter String Pattern**: avaya.com
- Match option**:
 - ☐ Exact Match
 - ☐ Match Beginning
 - ☐ Match End
 - ☒ Match Any
- OK** and **Cancel** buttons.

The following screen shows a summary of the altered-header rule configured in this section.



7.2.4. Contact Header Modification

Bell Canada SIP Trunking service requires the Contact header in the outbound call INVITE to be of a specific format. The following are the Contact header contents required for a sample outbound call:

```
Contact: <sip:4167771111;tgrp=VSAC_4167751396_01A;trunk-context=siptrunking.bell.ca@111.111.111.111:5060>
```

Where

- 4167771111 is the DID associated with the enterprise extension initiating the outbound call
- 4167751396 is the Authorization User name used for Digest Authentication for outbound calls (see **Section 7.2.6**)

However, the INVITE sent to AA-SBC from Session Manager for the same outbound call does not conform to the above requirement. It is necessary therefore to use header manipulation on AA-SBC to modify the Contact header to meet the requirement by the Bell Canada network.

Navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. On the screen displayed on the right side (not shown), click **Add reg-ex-header** link on the right (not shown).

The screen below shows the edit screen for a previously added reg-ex header.

In the **number** field, enter an appropriate unused number. Since this is the second header manipulation rule, number 2 was used. For **destination**, enter or select **Contact**. Expand **create** (by clicking the + sign to the left),

- Enter or select **Contact** for the **source** field
- For **expression**, enter `<sip:(.*)@(.*)5060;(.*)>`. This matches the Contact header contents from Session Manager.
- For **replacement**, enter `<sip:\1;tgrp=VSAC_4167751396_01A;trunk-context=siptrunking.bell.ca@\2:5060>`. This converts the Contact header contents as required.

Retain the default settings for other configuration fields. Click the **Create** button (not shown) if adding a new reg-ex-header; click the **Set** button if editing an exiting reg-ex-header.

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy: **Configuration: all** > **cluster** > **box: AuraSBC.avaya.com** > **vsp** > **default-session-config** > **tls** > **session-config-pool** > **entry ToTelco** > **header-settings** > **reg-ex-header 2**. The main content area is titled **Configure vsp|session-config-pool|entry ToTelco|header-settings|reg-ex-header 2**. It includes buttons for **Show advanced**, **Help**, **Index**, **Set**, **Reset**, **Back**, **Copy**, and **Delete**. The configuration fields are as follows:

- admin**: **enabled** (Resource is active)
- * number**: **2**
- * destination**: **enter** **or select from** **Contact**
- create** (expanded):
 - * source**: **enter** **or select from** **Contact**
 - * expression**: `<sip:(.*)@(.*)5060;(.*)>` (regular expression)
 - * replacement**: `<sip:\1;tgrp=VSAC_41677`
- append**: [Add append](#)
- apply-to-methods**: **INVITE**, **REFER**, **MESSAGE**, **INFO**

The following screen shows a summary of the header manipulations for SIP messages sent to the Bell Canada network, including the blocked-headers (Section 7.2.2), altered-header (Section 7.2.3) and reg-ex-header (Section 7.2.4).

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 main content area is titled 'Configure vsp\session-config-pool\entry ToTelco\header-settings'. On the left, a tree view shows the configuration hierarchy: cluster > box: AuraSBC.avaya.com > vsp > session-config-pool > entry ToTelco > header-settings. The main panel displays three sections: 'allowed-header' with an 'Edit allowed-header' link; 'blocked-header' with input fields for 'P-Site' and 'P-Location' and an 'Edit blocked-header' link; and 'altered-header' with a table of existing headers. Below the table is an 'Add altered-header' link. The 'reg-ex-header' section is also visible at the bottom.

	altered-header	admin	source-header	source-field	destination	destination-field	append
Edit Delete	altered-header 1	enabled	Diversion	selection .*avaya\.com cust2-tor.vtac.bell.ca	Diversion	host	

	reg-ex-header	admin	destination	create	append
Edit Delete	reg-ex-header 2	enabled	Contact	Contact <sip:(.*)@(.*)[:5060];(.*)> <sip:\1;trp=VSAC_4167751396_01A;trunk-context=siptrunking.bell.ca@2:5060>	

7.2.5. Max-Forwards Value

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

The screen below shows the edit screen for a previously added altered-header for Max-Forwards.

- **number:** Enter an unique number for this altered header.
- **source-header:** Specify the header from which the system initially derives the data that is to be written to the destination header. In this case, enter **Max-Forwards**.
- **source-field type:** Select “selection”. If **selection** is chosen, then the user may enter a value to match on and a replacement value.

- **source-field value:** Enter .* as the value. This is a regular expression that allows the system to match on any value.
- **source-field replacement:** Enter the replacement value. In this case, the value of **70** was used.
- **destination:** Specify the destination header. In this case, enter **Max-Forwards**.
- **destination-field:** Select **full**. This specifies that the full destination header will be over-written with the new one that was derived from the source header.

Click the **Create** button (not shown) if adding a new altered-header; click the **Set** button if editing an exiting altered-header.

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy, with 'header-settings' selected. The main content area is titled 'Configure vsplsession-config-poolentry ToPBX\header-settings\altered-header 3'. It includes a 'Show advanced' button and 'Help' and 'Index' links. Below these are buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The configuration fields are as follows:

- admin:** enabled (Resource is active)
- * number:** 3
- * source-header:** enter Max-Forwards or select from Max-Forwards
- * source-field:**
 - * type:** selection (Regular expression based selection of portion of the URI.)
 - * value:** .* (regular expression)
 - * replacement:** 70
- * destination:** enter Max-Forwards or select from Max-Forwards
- * destination-field:**
 - * type:** full (Entire value of the URI.)
- apply-to-methods:** INVITE, REFER, MESSAGE, INFO

7.2.6. Normalizing Calling Number in From Header

The inbound call INVITE from Bell Canada to the enterprise contains a + followed by 11 digits in the From header for the calling number. This prevents some of the EC500 mobility call features from working properly since the EC500 mobile number configured on Communication Manager (in **off-pbx-telephone station-mapping** form) is not allowed to contain non-digits like + to match the number in the inbound INVITE From header. To have the EC500 number configured on Communication Manager to exactly match the calling number contained in the INVITE From header, the calling number in the From header needs to be normalized to be 10-digits without the + sign.

To do this, navigate to **vsp → dial-plan** and click the **Add normalizaion** link on the right (not shown).

The screen below shows the edit screen for a previously added dial-plan normalization for stripping the calling number in the From header to 10-digits.

Under the **general:** heading, enter a descriptive text string for **name**.

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar shows a tree view with 'cluster' expanded, and 'vsp' selected. Under 'vsp', 'dial-plan' is highlighted. The main content area is titled 'Configure vsp\dial-plan\normalization StripPlusInFrom'. It has tabs for 'Configuration', 'Setup', and 'View'. Below the tabs are buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The 'general:' section contains fields for 'name' (StripPlusInFrom), 'description', 'match' (with a dropdown for 'type' set to 'default'), 'routing-tag' (with a link 'Add routing-tag'), 'priority' (100, with a note '(from 0 to 999,999,default=100)'), 'condition-list' (with a '[Delete]' link), and 'condition-list-match-secondary' (false). The 'other properties:' section has 'admin' set to 'enabled' (with a note '(Resource is active)') and 'apply-to-headers' with a checkbox for 'request-uri'.

Scroll down to the **other properties:** heading, check the **from-header** option box for **apply-to-headers**.

AVAYA

aura

acme

packet

powered

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

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

Configuration: all

Configuration

Setup

View

cluster

vsp

default-session-config

tls

session-config-pool

dial-plan

enterprise

dns

settings

other properties:

admin

enabled

(Resource is active)

apply-to-headers

request-uri

to-header

from-header

Select All

Unselect All

alter-tel-scheme

no

(Do not alter TEL scheme to SIP scheme)

alter-domain-name

enum-operation

disabled

(Resource is inactive)

enum-apply-request-result-to-contact

disabled

(Resource is inactive)

Scroll down further to **from user**. Select **strip-off-to** for **type**, then enter **10** for **resulting-string-length**. Verify that **INVITE** is selected (default) for **apply-to-methods**.

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 configuration options, with 'dial-plan' selected under the 'vsp' cluster. The main content area displays the configuration for the 'from-user' resource. The 'type' is set to 'strip-off-to' and the 'resulting-string-length' is set to '10'. The 'apply-to-methods' dropdown is set to 'INVITE'. The 'normalize-again' option is set to 'disabled'.

Resource	Configuration
enum-server	Add enum-server
synchronize-phone-group	type: no (Do not synchronize phone numbers in the same group)
apply-to-methods	INVITE, REFER, MESSAGE, INFO Select All, Unselect All
request-user	* type: no (No normalization applied to phone numbers)
to-user	* type: no (No normalization applied to phone numbers)
from-user	* type: strip-off-to (Strip off prefix to certain length) * resulting-string-length: 10
normalize-again	disabled (Resource is inactive)

Click the **Set** button (not shown) after making / verifying all the configuration changes.

7.2.7. Digest Authentication

Bell Canada SIP Trunk service uses Digest Authentication for outbound calls from the enterprise to the PSTN. On the CPE side, AA-SBC must be configured to

1. Enable proper response from AA-SBC to the Digest Authentication challenge from the network
2. Configure a user and password (provided by Bell Canada) used for Digest Authentication

To enable response from AA-SBC to Digest Authentication challenge, navigate to **vsp** → **session-config-pool** → **entry ToTelco** and click **authentication** under the **AAA:** heading on the right (not shown). In the resulting screen, select **enabled** for the **handle-challenge-locally** field. Retain default settings for other fields. Scroll to top of the screen and click **Set** (not shown).

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view of the configuration hierarchy, with 'session-config-pool' expanded to show 'entry ToTelco'. The main content area is titled 'AAA:' and contains the 'authentication' configuration for the selected entry. The configuration includes several fields with dropdown menus and checkboxes, all set to their default values except for 'handle-challenge-locally', which is set to 'enabled'. The 'apply-to-methods' field is a multi-select dropdown with 'INVITE', 'REFER', 'MESSAGE', and 'INFO' selected. The 'exclude-scheme-in-called-station-id' field is set to 'false'.

Field	Value	Description
mode	None	(Perform no authentication)
inbound-only	disabled	(Resource is inactive)
session-starter-only	disabled	(Resource is inactive)
handle-challenge-locally	enabled	(Resource is active)
challenge-response-code	401	(Unauthorized)
initial-challenge-state	True	
apply-to-methods	INVITE, REFER, MESSAGE, INFO	
exclude-scheme-in-called-station-id	false	

To configure a Digest Authentication user and password, navigate to **vsp** → **enterprise** → **sip-gateway Telco** and scroll down on the right to the **registration failover:** section. Enter the assigned user name for **user** and a descriptive text string for **password-tag**. Then click the **Manage Password** link to enter and confirm the assigned password in a pop-up Manage Password window (not shown). Scroll to top of the screen and click **Set** (not shown).

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, with 'sip-gateway Telco' selected under the 'enterprise' section. The main content area displays the 'registration failover:' configuration for the selected gateway. It includes fields for 'user' (4167751396), 'password-tag' (BC-Avaya), and 'add-user-to-contact' (disabled). A 'Manage Password' link is available next to the password-tag field. Below this, the 'servers:' section shows 'server-type' set to 'sip-proxy' and a 'server-pool' section with a 'Delete' link.

registration failover:	
user	4167751396
password-tag	BC-Avaya Manage Password
add-user-to-contact	disabled (Resource is inactive)

servers:	
server-type	sip-proxy
server-pool	
Delete	

7.2.8. Third Party Call Control

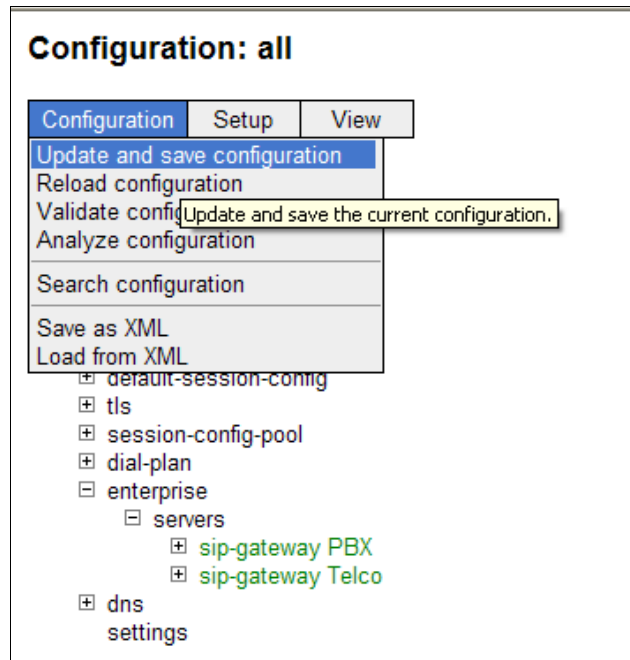
Disable third party call control. Navigate to **vsp** → **default-session-config** → **third-party-call-control**. Set the **admin** field to **disabled**.

The screenshot shows the Avaya Aura Configuration interface. The 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 vsp/default-session-config/third-party-call-control'. On the left, a tree view shows the configuration hierarchy: cluster > vsp > default-session-config > third-party-call-control. The main panel displays a list of configuration parameters for 'third-party-call-control'.

Parameter	Value	Status
admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	enabled	(Resource is active)
forward-unresolved-replaces	disabled	(Resource is inactive)
extract-refer-to-header-spec	disabled	(Resource is inactive)
refer-maintain-identity	false	
refer-notify-100-trying	disabled	(Resource is inactive)
refer-delayed-offer	disabled	(Resource is inactive)
ringback-file		Browse System Files
busy-file		Browse System Files
pre-call-announcement		Browse System Files

7.2.9. 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**.



8. Bell Canada SIP Trunking Configuration

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

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

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

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.
 - Using a network sniffing tool (e.g., Wireshark), monitor the SIP signaling messages between Bell Canada and AA-SBC on an outbound call from the enterprise to the PSTN, and verify the SIP signaling message exchanges for Digest Authentication:
 1. Bell Canada SIP Trunking service returned a **401 Unauthorized** status message to the initial INVITE from the AA-SBC. The 401 message contained a **WWW-Authenticate** Header posing challenge for Digest Authentication.

Example of **WWW-Authenticate** Header:

```
WWW-Authenticate: DIGEST qop="auth",  
nonce="BroadWorksXgmdj14a7T987am0BW",  
realm="siptrunking.bell.ca",  
algorithm=MD5
```

2. AA-SBC ACKed the above 401 message, then presented the Digest Authentication response by sending a second INVITE that contained an **Authorization** Header supplying the information for successful Digest Authentication. Note the username as configured in **Section 7.2.7**.

Example of **Authorization** Header:

```
Authorization: Digest username="4167751396",  
realm="siptrunking.bell.ca",  
nonce="BroadWorksXgmdj14a7T987am0BW",  
response="89f1e3b7c2d52ad7d13fb58c34aee1e3",  
uri="sip:19085551212@siptrunking.bell.ca",  
algorithm=MD5,  
qop=auth,  
nc=00000001,
```

cnonce="f8c60f3798082a2a6915"

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

2. Communication Manager:

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

3. Session Manager:

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

The screenshot displays the Session Manager Dashboard. The left sidebar contains navigation links: 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 shows the 'Session Manager Dashboard' with a description: 'This page provides the overall status and health summary of each administered Session Manager.' Below this, there are filters for 'Service State' and 'Shutdown System', and a timestamp 'As of 12:56 PM'. A table titled 'Session Manager Instances' shows one item, 'SM1', with columns for Session Manager, Type, Alarms, Tests Pass, Security Module, Service State, Entity Monitoring, Active Call Count, Registrations, and Version. The 'Tests Pass' column shows a green checkmark, and the 'Service State' column shows 'Accept New Service'.

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/> SM1	Core	76/3/1980	✓	Up	Accept New Service	24/46	0	15	6.1.1.0.611023

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

10. Conclusion

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

11. References

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

- [1]*Installing and Configuring Avaya Aura® System Platform*, Release 6.03, February 2011.
- [2]*Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [3]*Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509.
- [4]*Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.0, June 2010, Document Number 555-245-205.
- [5]*Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
- [6]*Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Number 03-603473.
- [7]*Administering Avaya Aura® Session Manager*, Release 6.1, May 2011, Document Number 03-603324.
- [8]*Avaya Aura® Session Border Controller System Administration Guide*, V.6.0, September 2010
- [9]*Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.
- [10]*Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
- [11]*Administering Avaya one-X® Communicator*, April 2011.
- [12]*Using Avaya one-X® Communicator*, April 2011.
- [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/>

Product documentation for Bell Canada SIP Trunking is available from Bell Canada.

Appendix A: Avaya Aura® SBC Configuration File

```
#
# Copyright (c) 2004-2011 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 18:21:02 Tue 2011-07-26
#
config cluster
config box 1
  set hostname AuraSBC.avaya.com
  set timezone America/New_York
  set name AuraSBC.avaya.com
  set identifier 00:ca:fe:66:67:63
config interface eth0
  config ip inside
    set ip-address static 10.1.2.243/24
    config ssh
    return
  config snmp
    set trap-target 10.1.2.242 162
    set trap-filter generic
    set trap-filter dos
    set trap-filter sip
    set trap-filter system
  return
  config web
  return
  config web-service
    set protocol https 8443
    set authentication certificate "vsp\tls\certificate ws-cert"
  return
  config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
  return
  config icmp
  return
  config media-ports
  return
  config routing
    config route Default
      set gateway 10.1.2.1
    return
    config route Static0
      set destination network 192.11.13.4/30
      set gateway 10.1.2.241
    return
    config route Static1
      set admin disabled
    return
    config route Static2
      set admin disabled
```

```

return
config route Static3
    set admin disabled
return
config route Static4
    set admin disabled
return
config route Static5
    set admin disabled
return
config route Static6
    set admin disabled
return
config route Static7
    set admin disabled
return
return
return
return
config interface eth2
config ip outside
    set ip-address static 111.111.111.111/24
config sip
    set udp-port 5060 "" "" any 0
return
config ntp-server
return
config media-ports
return
config routing
    config route Default
        set admin disabled
    return
    config route external-sip-media-1
        set destination network 222.222.222.0/24
        set gateway 111.111.111.129
    return
    config route "NTP TimeServer"
        set destination host 192.43.244.18
        set gateway 111.111.111.129
    return
return
config kernel-filter
    config allow-rule allow-sip-udp-from-peer-1
        set destination-port 5060
        set source-address/mask 222.222.222.0/24
        set protocol udp
    return
    config deny-rule deny-all-sip
        set destination-port 5060
    return
return
return
return
config ntp-client
    set server 192.43.244.18

```

```

    set poll-interval 2
    return
    config cli
    set prompt AuraSBC.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

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-Site
    set blocked-header P-Location
return
config third-party-call-control
    set handle-refer-locally disabled
return
return
config tls
    config default-ca
        set ca-file /cxc/certs/sipca.pem
    return
    config certificate ws-cert
        set certificate-file /cxc/certs/ws.cert
    return
    config certificate aasbc.p12
        set certificate-file /cxc/certs/aasbc.p12
        set passphrase-tag aasbc-cert-tag
    return
return
config session-config-pool
    config entry ToTelco
        config to-uri-specification
            set user request-uri
            set host request-uri
            set port request-uri
            set display request-uri
        return
        config from-uri-specification
            set user-param keep
        return
        config request-uri-specification
            set port next-hop
        return
        config p-asserted-identity-uri-specification
            set user-param keep
        return
        config contact-uri-settings-in-leg
        return
        config contact-uri-settings-out-leg
        return
        config authentication
            set handle-challenge-locally enabled
            set apply-to-methods INVITE

```

```

return
config header-settings
    set blocked-header P-Site
    set blocked-header P-Location
    config altered-header 1
        set source-header Diversion
        set source-field selection ".*avaya\.com" cust2-tor.vsacl.bell.ca
        set destination Diversion
        set destination-field host
    return
    config reg-ex-header 2
        set destination Contact
        set create Contact <sip:(.*)@(.*):5060;(.*)>
"<sip:\1;tgrp=VSAC_4167751396_01A;trunk-context=siptrunking.bell.ca@\2:5060>"
    return
    return
return
config entry ToPBX
    config to-uri-specification
        set host next-hop-domain
    return
    config from-uri-specification
    return
    config request-uri-specification
        set host next-hop-domain
    return
    config contact-uri-settings-in-leg
    return
    config contact-uri-settings-out-leg
    return
    config authentication
    return
    config header-settings
        set blocked-header P-Site
        set blocked-header P-Location
        config altered-header 3
            set source-header Max-Forwards
            set source-field selection .* 70
            set destination Max-Forwards
            set destination-field full
        return
    return
return
config entry Discard
    config sip-directive
    return
return
return
config dial-plan
    config normalization StripPlusInFrom
        set apply-to-headers from-header
        set apply-to-methods INVITE
        set from-user strip-off-to 10
    return
    config route Default
        set priority 500

```

```

    set location-match-preferred exclusive
    set session-config vsp\session-config-pool\entry Discard
return
config source-route FromTelco
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway Telco"
return
config source-route FromPBX
    set peer server "vsp\enterprise\servers\sip-gateway Telco"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
return
return
config enterprise
    config servers
        config sip-gateway PBX
            set domain cust2-tor.vsac.bell.ca
            set failover-detection ping
            set ping-interval 60
            set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
        config server-pool
            config server PBX1
                set host 10.1.2.210
                set transport TCP
            return
        return
return
        config sip-gateway Telco
            set failover-detection ping
            set ping-interval 60
            set user 4167751396
            set password-tag BC-Avaya
            set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
        config server-pool
            config server Telco1
                set host 222.222.222.222
            return
        return
return
return
return
config dns
    config resolver
        config server 192.168.1.200
    return
return
return
config settings
    set read-header-max 8191
return
return

config external-services
return

```

```

config preferences
  config gui-preferences
    set enum-strings SIPSourceHeader Diversion
    set enum-strings SIPSourceHeader Contact
    set enum-strings SIPSourceHeader Authorization
    set enum-strings SIPSourceHeader Max-Forwards
    set enum-strings Timezone America/New_York
  return
return

config access
  config permissions superuser
    set cli advanced
  return
  config permissions read-only
    set config view
    set actions disabled
  return
  config users
    config user admin
      set password 0x00709279d356502144245a519f7b8d3def7d85f6b35d763ed2ef9caa81
      set permissions access\permissions superuser
    return
    config user cust
      set password 0x005826490b28ed25073ca276419c8b4dfef00956d09e77514f79f33207
      set permissions access\permissions read-only
    return
    config user init
      set password 0x002956458de23a358a80cca0a201bec3a27537120662cc87111fd9efaf
      set permissions access\permissions superuser
    return
    config user craft
      set password 0x00e3ad966d252e8e31c36bd1644fdee2bc0d97a7980594b6ee94e7fe94
      set permissions access\permissions superuser
    return
    config user dadmin
      set password 0x0099af5ca1bbb074529637d750829aa668b1e1a7e274467badb0b8baa4
      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.