



Avaya Solution & Interoperability Test Lab

Application Notes for Bell Canada SIP Trunking Service with Avaya Aura® Communication Manager Evolution Server R6.0.1, Avaya Aura® Session Manager R6.1, and Acme Packet Session Border Controller R6.2 – Issue 1.1

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® Communication Manager Evolution Server 6.0.1, Avaya Aura® Session Manager 6.1, Acme Packet Session Border Controller 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager or Acme Packet Session Border Controller.

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	5
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results	6
2.3.	Support.....	8
3.	Reference Configuration	9
4.	Equipment and Software Validated	11
5.	Configure Avaya Aura® Communication Manager	12
5.1.	Licensing and Capacity	12
5.2.	System Features	13
5.3.	IP Node Names	14
5.4.	Codecs.....	14
5.5.	IP Network Region	15
5.6.	Signaling Group	17
5.7.	Trunk Group.....	19
5.8.	Calling Party Information	23
5.9.	Outbound Routing.....	24
5.10.	Vector Directory Numbers (VDNs) and Vectors for SIP NCR.....	Error! Bookmark not defined.
5.11.	Post-Answer Redirection to a PSTN Destination	Error! Bookmark not defined.
5.12.	Post-Answer Redirection With UI to a SIP Destination.....	Error! Bookmark not defined.
5.13.	Saving Communication Manager Configuration Changes	26
6.	Configure Avaya Aura® Session Manager	27
6.1.	System Manager Login and Navigation	28
6.2.	Specify SIP Domain.....	29
6.3.	Add Location	31
6.4.	Add Adaptation Module	32
6.5.	Add SIP Entities.....	35
6.6.	Add Entity Links.....	37
6.7.	Add Routing Policies	39
6.8.	Add Dial Patterns.....	40
6.9.	Add/View Session Manager	42
7.	Configure Acme Packet Net-Net 3800 Session Border Controller	44
7.1.	Acme Packet Command Line Interface	44
7.2.	Physical and Network Interfaces	45
7.3.	Realm	46
7.4.	Session Agent.....	47
7.5.	Digest Authentication Configuration	48
7.6.	SIP Configuration	49
7.7.	SIP Interface.....	49
7.8.	SIP Manipulation	50
7.9.	Steering Pools	56
7.10.	Local Policy	56
8.	Bell Canada SIP Trunking Configuration.....	59
9.	Verification and Troubleshooting.....	60

10.	Conclusion	65
11.	References	66

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® Communication Manager Evolution Server 6.0.1, Avaya Aura® Session Manager 6.1, Acme Packet Session Border Controller (SBC) 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager or Acme Packet Session Border Controller.

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 connection. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

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 the SBC). This call authentication scheme as specified in SIP RFC 3261 provides security and integrity protection for SIP signaling.

2. Test Scope and Results

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

Bell Canada is a member of the Avaya DevConnect Service Provider program. The general test approach is to connect a simulated enterprise to Bell Canada SIP Trunking Service via the public internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise is comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Acme Packet Session Border Controller and various Avaya endpoints.

2.1. Interoperability Compliance Testing

To verify SIP Trunk interoperability, following features and functionalities are covered during the compliance test:

- Response to SIP OPTIONS heartbeat.
- Incoming PSTN calls to various phone types. Phone types include H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types include H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Incoming and outgoing 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) are tested. 1XC also supports two signaling protocols (H.323 and SIP). Both protocols are tested.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411), etc.
- G.729 and G.711MU codec and proper codec negotiation.
- DTMF tone transmission as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for incoming and outgoing calls.
- Incoming and outgoing fax over IP with G.711MU codec.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding with SIP Diversion method.
- EC500 mobility (extension to cellular).
- Routing incoming PSTN calls to call center agent queues.

- Network Call Redirection using reINVITE to transfer inbound calls to extension back to PSTN.
- .
- Session Timers implementation from both ends of the enterprise and the service provider.
- Digest Authentication on SIP trunk group implemented by Acme Packet Session Border Controller.

Items are not supported by Bell Canada or not tested as part of the compliance testing are listed as the following:

- Inbound toll-free and outbound emergency calls (911) are supported but are not tested as part of the compliance test because Bell Canada does not provide the necessary configuration.
- T.38 fax is not supported.
- Off-net calls transfer using REFER method is not supported.
- Vector call redirection before answering using “302 Moved Temporarily” method is not supported.
- Vector call redirection after answering using REFER method is not supported.
- Off-net call forwarding is not tested with History-Info method. Bell Canada SIP Trunking Service natively supports Diversion method; it also supports History-Info header by converting History-Info into Diversion header. Communication Manager has capability to support both methods but only Diversion is tested.

2.2. Test Results

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

01. Calling number format in off-net call forward an inbound call to EC500 number to PSTN: The inbound call INVITE from Bell Canada to the enterprise contains a "+" followed by 11 digits in the From header for the calling number. The EC500 mobility call features does not work 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 configure the Header Manipulation Rule on SBC to normalize the calling number in the From header to remove the plus sign (see **Section 7.8**).

02. Off-net blind transfer by a SIP phone with REFER method: Communication Manager SIP phone blind transfers off-net of an inbound call back to PSTN. When Communication Manager sends REFER to complete the transferring the calling PSTN party does not hear the ring back tone. This issue is corrected by turning off the **Network Call Redirection** flag on outgoing trunk group setting, then Communication Manager successfully transfers the call with reINVITE method. Please refer to **Section 5.7** for configuration.

03. Blind transfer by a SIP phone to local extension: Communication Manager SIP phone blind transfers an inbound PSTN call to local H.323 phone. The transfer fails

because Communication Manager does not respond ACK to Bell Canada. This issue is corrected by turning off the **Network Call Redirection** flag on both private outgoing trunk group which connects to Session Manager for internal SIP phone configuration and public outgoing trunk group which connects to Bell Canada for PSTN calls. Then Communication Manager successfully transfers the call.

04. Off-net blind transfer by one-X® Communicator SIP soft phone: Communication Manager one-X® Communicator SIP soft phone blind transfers off-net of an inbound call back to PSTN. Communication Manager sends REFER to complete the transfer. But Bell Canada responds 404 Not Found then the transfer call fails. This issue is corrected by turning off the **Network Call Redirection** flag on outgoing trunk group setting, then Communication Manager successfully transferred the call with reINVITE method. Please refer to **Section 5.7** for configuration.

05. Network Call Redirection with “302 Moved Temporarily”: A vector DN on Communication Manager is programmed to redirect an inbound call to PSTN before answering. Communication Manager sends a “302 Moved Temporarily” SIP message to redirect the call. Bell Canada responds with an ACK but it does not handle the 302 properly. The call is not redirected to the new PSTN party in the Contact header of the 302 message. There is no resolution currently available.

06. No matching codec: For an outbound call from enterprise, if the codec does not match any of the codec supported by Bell Canada, Bell Canada responds with a “480 Temporary Unavailable” which is improper. The response should be a “488 Not Acceptable Here”. However, the call is still dropped as expected. This is listed here just simply as an observation.

07. G.711MU fax over IP: In inbound/ outbound fax call scenarios with G.711MU codec between enterprise and PSTN, the SIP call dialog looks identical to a regular G.711MU voice call. The fax document is received with acceptable quality. Communication Manager does not officially support G.711MU fax. However, incoming and outgoing G.711MU fax calls appear to work during testing when configuring fax = off. Communication Manager handles the call like a regular voice call and only supports G.711MU fax in best effort.

08. Calling Call Party Name (CPN) display for outbound call: For outbound call scenario, Communication Manager sends both calling CPN name and number to Bell Canada. In some cases, PSTN phone displays just only CPN number and no CPN name. In some other cases, PSTN phone displays both calling CPN name and number. The calling CPN may be overridden by the intermediate service provider that routes the call through from Bell Canada to the PSTN endpoint. This issue has low user impact and it is listed here just simply as an observation.

09. Call display in consultative call transfer of an inbound call to local extension: A Communication Manager SIP phone performs a consultative transfer of an inbound PSTN call to a local H.323 phone. The local H.323 phone displays the trunk-group name

and TAC instead of the CPN of PSTN. This issue low user impact and it is listed here just simply as an observation.

10. Call display update in off-net call transfer scenario: Communication Manager transfers off-net of an incoming call back to PSTN. After completing the transfer, Communication Manager sends UPDATE to update the true connected CPN of PTSN parties. However, the CPN is not being updated. It depends on either Bell Canada or the intermediate service provider which routes the call from Bell Canada to the PSTN endpoint to support the display update. This issue low user impact and it is listed here just simply as an observation.

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 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 G650 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya S8800 Server running Messaging
- Avaya Session Border Controller for Enterprise
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP)
- Avaya digital and analog telephones

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

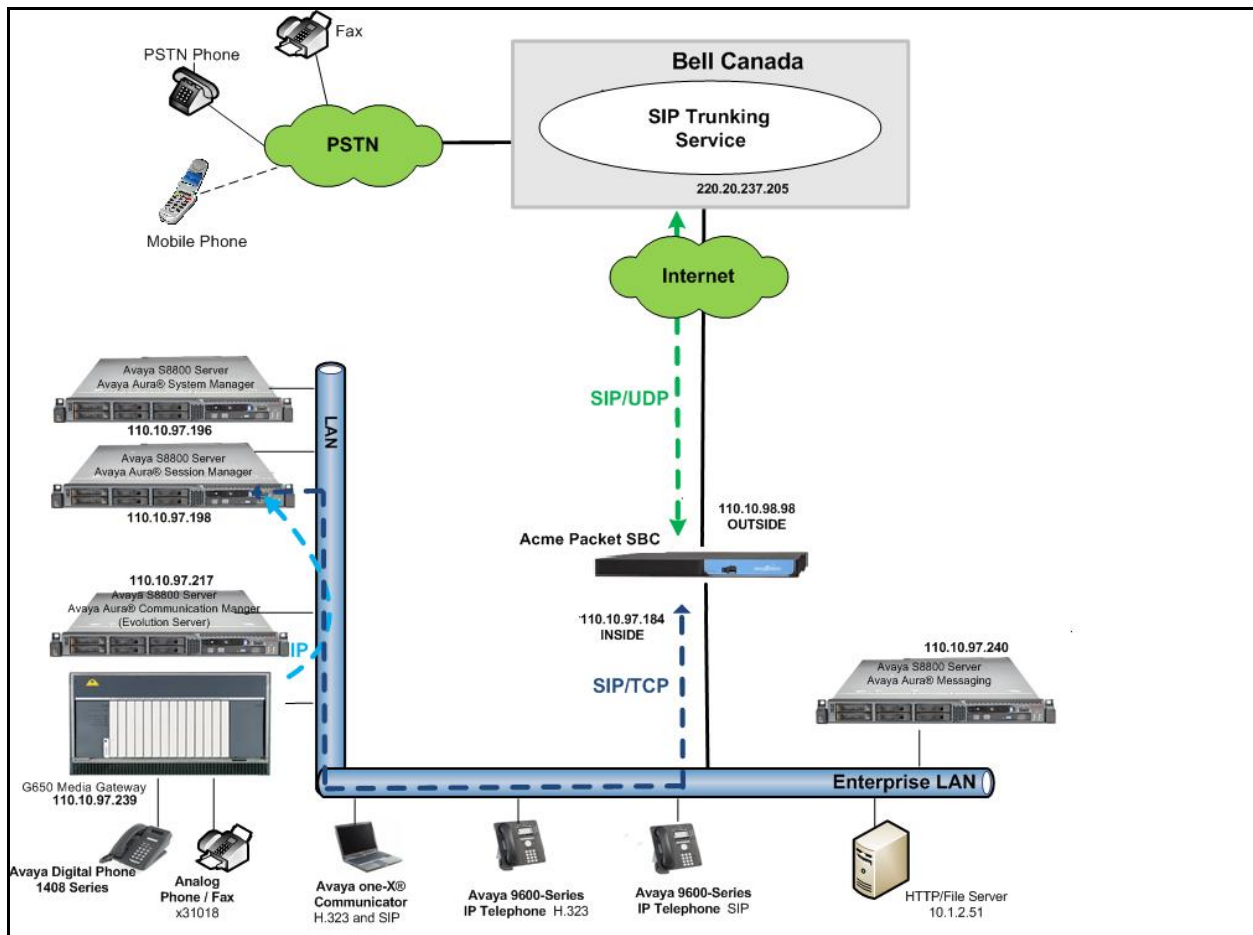


Figure 1: Avaya IP Telephony Network Connecting to Bell Canada SIP Trunking Service

Two separate SIP trunk groups are 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 are applied only to these dedicated trunks so as not to affect other enterprise SIP traffic.

For inbound calls, the calls flow from the service provider to the SBC then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case 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 are 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 is routed to Session Manager. The Session Manager once again uses the configured dial patterns (or regular expressions) and routing policies to determine the route to the SBC for egress to the Bell Canada network.

4. Equipment and Software Validated

The following equipment and software are used for the sample configuration:

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	6.0.1 (R016x.00.1.510.1-18621)
Avaya G650 Media Gateway IPSI TN2312BP Control-LAN TN799DP Medpro TN2302 Digital Line TN2224 Analog Line TN746B	HW06 FW043 HW01 FW026 HW20 FW117 000006 000019
Avaya Aura® Session Manager running on Avaya S8800 Server	6.1.1.0.611023
Avaya Aura® System Manager running on Avaya S8800 Server	6.1.5.0 Build number 6.1.0.0.7345 Patch 6.1.5.9
Avaya Aura® Messaging running on Avaya S8800 Server	6.1-11.0
Avaya 96xx Series IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.0.1
Avaya 96xx Series IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition R6_0_3-120511
Avaya one-X Communicator (H.323&SIP)	6.1.3.08-SP3-Patch2-35791
Avaya 1408 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Acme Packet Net-Net 3800 SBC	Firmware SCX6.2.0 MR-9 GA (Build 1014)
Bell Canada SIP Trunking Service Components	
Equipment/Software	Release/Version
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 are used for the compliance testing. Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

5. Configure Avaya Aura® Communication Manager

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

It is assumed the general installation of Communication Manager has been previously completed.

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **96** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

```
display system-parameters customer-options                               Page 2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 0
      Maximum Concurrently Registered IP Stations: 18000 5
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 18000 2
      Maximum Video Capable IP Softphones: 18000 3
      Maximum Administered SIP Trunks: 24000 96
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
Maximum Number of DS1 Boards with Echo Cancellation: 522 0
      Maximum TN2501 VAL Boards: 128 1
      Maximum Media Gateway VAL Sources: 250 0
      Maximum TN2602 Boards with 80 VoIP Channels: 128 0
      Maximum TN2602 Boards with 320 VoIP Channels: 128 0
Maximum Number of Expanded Meet-me Conference Ports: 300 0

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

5.2. System Features

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

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

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. The compliance test uses 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 C-LAN card hosted by Communication Manager (**CLAN01A02**); Medpro card hosted by Communication Manager (**IPMedia01A08**) and Session Manager (**DevASM**). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
CLAN01A02	110.10.97.217	
DevASM	110.10.97.198	
IPMedia01A08	110.10.97.239	
default	0.0.0.0	
procr	10.1.1.5	
procr6	::	

Note: The **CLAN01A02** is used as an alternative to node-name **procr**. It is recommended to use **procr** for signaling group provisioning if the CLAN card is not present on G650 Media Gateway or when Communication Manager is configured to work with G450 Media Gateway.

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codec to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 3 is used for this purpose. Bell Canada SIP Trunking service currently supports G.729 and G.711MU. Enter the codec to be used in priority order in the **Audio Codec** column of the table. Default values can be used for all other fields. The following screen shows the codec set configuration at a certain time of the compliance test. During testing, the codec set specifications are varied to test for individual codec as well as codec negotiation between the enterprise and the network.

change ip-codec-set 3		Page 1 of 2
		IP Codec Set
Codec Set: 3		
Audio Codec	Silence Suppression	Frames Per Pkt Packet Size (ms)
1: G.711MU	n	2 20
2: G.729	n	2 20
3:		
4:		

Bell Canada does not support T.38 fax in this compliance test. It only supports G.711MU fax. Even Communication Manager does not recommend G.711MU fax, however with the setting **FAX:off** as shown in the following screen the G.711 fax appears to work. Communication Manager seems to support G.711MU fax in best effort, it treats the fax call like a regular G.711MU voice call.

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

change ip-codec-set 3			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 separate codec or quality of service settings to be used for calls between the enterprise and the service provider. For the compliance test, ip-network-region 3 is created.

Use the **change ip-network-region 3** command to configure region 3 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 test environment in the Avaya test lab. This domain name appears in the From header of SIP messages originating from this IP region. Note: Session Manager adaptation configuration (**Section 6.4**) is used to convert this domain name to the specific CPE domain as assigned by Bell Canada and expected by the Bell Canada SIP Trunking Service.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (Media 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. Media 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 3                                     Page 1 of 20
                                                              IP NETWORK REGION
Region: 3
Location: 1           Authoritative Domain: avaya.com
Name: Bell Canada
MEDIA PARAMETERS
Codec Set: 3           Intra-region IP-IP Direct Audio: yes
                      Inter-region IP-IP Direct Audio: yes
                      IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS
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 3 and other regions. In this testing, Communication Manager, Session Manager, IP phone and SBC are assigned to the same region 3. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 3. Default values may be used for all other fields. The screen below shows the settings used for the compliance test. It indicates that codec set 3 will be used for calls between region 3 (the service provider region) and other regions.

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

Non-IP telephones (e.g., analog, digital) derive network region from the Avaya Media Gateway to which the device is connected. IP telephones can be assigned to a network region based on an IP address mapping.

For the compliance test, devices with IP addresses in the 110.10.97.0/24 subnet are assigned to network region 3 including Communication Manager, Session Manager and. IP telephones used for the compliance test, including both the Avaya 9600 IP Telephones and the Avaya one-X® Communicator soft phones, are also assigned to network region 3 with IP address in the 110.10.98.0/24 subnet. The following screen illustrates a subset of the IP address mapping configuration.

change ip-network-map				Page 1 of 63	
IP ADDRESS MAPPING					
IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: 110.10.97.0	/24	3	n		
TO: 110.10.97.255					
FROM: 110.10.98.0	/24	3	n		
TO: 110.10.98.255					
FROM:	/		n		
TO:					

5.6. Signaling Group

Use the **add signaling-group** command to create two signaling groups between Communication Manager and the Session Manager for use by inbound and outbound calls.

For the compliance test, the signaling group 3 is used for inbound calls. It is 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** set to **tcp**. The transport method specified here is used between Communication Manager and Session Manager. The transport method used between the Session Manager and SBC is specified as TCP in **Section 6.6**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to **5060**.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others**. 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 **CLAN01A02**. This node name maps to the IP address of C-LAN card IP address as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **DevASM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to blank.
- Set the **Enable Layer 3 Test?** to **y**. This field will enable OPTIONS heartbeat from Session Manager toward the SBC. By default, SBC does not respond to OPTIONS. It rather forwards the OPTIONS to the service provider to query for the status of SIP Trunk. In the compliance test, Bell Canada sends 200OK response to the OPTIONS. SBC also forwards the 200OK response to Session Manager to maintain the SIP Trunk status as in service.
- 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 service provider 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.
- Set the **Initial IP-IP Direct Media** to **n**.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **12**. This allows more time for PSTN calls to complete through the Bell Canada SIP Trunking Service.
- Default values may be used for all other fields.

```
add signaling-group 3                                     Page 1 of 1
                                                         SIGNALING GROUP

Group Number: 4                      Group Type: sip
  IMS Enabled? n                    Transport Method: tcp
    Q-SIP? n                                     SIP Enabled LSP? n
    IP Video? n                               Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM

Near-end Node Name: CLAN01A02          Far-end Node Name: DevASM
Near-end Listen Port: 5060              Far-end Listen Port: 5060
                                         Far-end Network Region: 3

Far-end Domain:

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

The trunk group for outbound calls from the enterprise to PSTN is similarly configured except that the **Far-end Domain** is set to **siptrunking.bell.ca**, this domain is network domain as provided by Bell Canada. For the compliance test, signaling group 4 is used for this purpose and is shown below:

```

add signaling-group 4
                                     Page 1 of 1

                                     SIGNALING GROUP

Group Number: 3                     Group Type: sip
IMS Enabled? n                     Transport Method: tcp
    Q-SIP? n                               SIP Enabled LSP? n
    IP Video? n                         Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM

Near-end Node Name: CLAN01A02        Far-end Node Name: DevASM
Near-end Listen Port: 5060            Far-end Listen Port: 5060
                                     Far-end Network Region: 3

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? y              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 trunk group for the two signaling groups created in **Section 5.6**. For the compliance test, trunk group 3 is configured for incoming call and trunk group 4 is configured for outgoing call 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 3 and **outgoing** for trunk group 4.
- Set the **Outgoing Display** to **y** to enable name display on the trunk.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the appropriate signaling group shown in **Section 5.6**, i.e. signaling group 3 for incoming trunk group 3 and signaling group 4 for outgoing trunk group 4.
- Set the **Number of Members** field to **32**. It is 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 are used for all other fields.

add trunk-group 3		Page 1 of 21
TRUNK GROUP		
Group Number: 3	Group Type: sip	CDR Reports: y
Group Name: Bell Canada Outbound Trunk	COR: 1	TN: 1 TAC: 8003
Direction: incoming	Outgoing Display? y	
Dial Access? n	Night Service:	
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 3	
	Number of Members: 32	

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

add trunk-group 3		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
Redirect On OPTIM Failure: 5000		
SCCAN? n	Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 600		
Disconnect Supervision - In? y		

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with Bell Canada. Thus, the **Numbering Format** is set to **private** and the **Numbering Format** in the route pattern 4 is 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 CPN of inbound calls is blocked. Default values are used for all other fields.

```

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

                                Numbering Format: private
                                UI Treatment: service-provider
                                Replace Restricted Numbers? y
                                Replace Unavailable Numbers? y

Show ANSWERED BY on Display? y

```

On **Page 4**, set the **Network Call Redirection** field to **n**. This setting disables the use of the SIP REFER message to transfer off-net of an incoming call to a vector DN back to PSTN as this method is not supported by Bell Canada. Note: the outgoing trunk group 4 in the later discussion will also have **Network Call Redirection** set to **n**, this setting allows Communication Manager to use reINVITE to transfer off-net of an incoming call to extension back to PSTN. For more information, please refer to **Section 2.2**, observation #02 and #04.

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 off-net of inbound calls back to the PSTN and Extension to Cellular (EC500) call scenarios.

Set the **Support Request History** field to **n**. This parameter determines the SIP History-Info header will not be included in the call-redirection INVITE from the enterprise.

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 3	Page 4 of 21
<p style="text-align: center;">PROTOCOL VARIATIONS</p> <p> Mark Users as Phone? n Prepend '+' to Calling Number? n Send Transferring Party Information? n Network Call Redirection? n Send Diversion Header? y Support Request History? n Telephone Event Payload Type: 101 </p> <p> 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 </p>	

For the configuration of outgoing trunk group 4, the **Direction** is set to “outgoing” and **Signaling Group** is set to 4. **Page 1** of the trunk group form is shown below:

add trunk-group 4	Page 1 of 21
<p style="text-align: center;">TRUNK GROUP</p> <p> Group Number: 4 Group Type: sip CDR Reports: y Group Name: Bell Canada Trunk COR: 1 TN: 1 TAC: 8004 Direction: outgoing Outgoing Display? y Dial Access? n Queue Length: 0 Service Type: public-ntwrk </p> <p style="text-align: right;"> Member Assignment Method: auto Signaling Group: 4 Number of Members: 32 </p>	

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

Note: When **Network Call Redirection** is set to “n”, Communication Manager uses reINVITE for off-net call transfer. This setting is to work around the issues as specified in **Section 2.2**, observation #02 and #04.

```

add trunk-group 4
                                Page 4 of 21
                                PROTOCOL VARIATIONS

                                Mark Users as Phone? n
                                Prepend '+' to Calling Number? n
                                Send Transferring Party Information? n
                                Network Call Redirection? n
                                Send Diversion Header? y
                                Support Request History? n
                                Telephone Event Payload Type: 101

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

```

The configurations on other pages of trunk group 4 are identical to trunk group 3.

5.8. Calling Party Information

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

The normal DID number is comprised of the local extension plus a prefix. A single private numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with 188X will send the calling party number as the **Private Prefix** plus the extension number to be as 416775188X.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
4	188	3-4	416775	10	Total Administered: 1
					Maximum Entries: 540

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

change public-unknown-numbering 0				Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT				
Ext	Ext	Trk	CPN	Total
Len	Code	Grp(s)	Prefix	CPN
				Len
4	188	3-4	416775	10
				Total Administered: 1
				Maximum Entries: 240
				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.

5.9. Outbound Routing

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

change dialplan analysis				Page 1 of 12			
				DIAL PLAN ANALYSIS TABLE			
				Location: all			
				Percent Full: 2			
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total
String	Length	Type	String	Length	Type	String	Length
18	4	ext					
6	1	fac					
8	4	dac					
9	1	fac					
*	4	dac					
#	4	dac					

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


```

change feature-access-codes                                     Page 1 of 10
                                FEATURE ACCESS CODE (FAC)
    Abbreviated Dialing List1 Access Code:
    Abbreviated Dialing List2 Access Code:
    Abbreviated Dialing List3 Access Code:
    Abbreviated Dial - Prgm Group List Access Code:
        Announcement Access Code: *100
        Answer Back Access Code:
        Attendant Access Code:
    Auto Alternate Routing (AAR) Access Code: 6
    Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
        Automatic Callback Activation:      Deactivation:
    Call Forwarding Activation Busy/DA:      All:      Deactivation:
    Call Forwarding Enhanced Status:      Act:      Deactivation:
        Call Park Access Code:
        Call Pickup Access Code:
    CAS Remote Hold/Answer Hold-Unhold Access Code:
        CDR Account Code Access Code:
        Change COR Access Code:
        Change Coverage 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 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 4 for outbound call via 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: 0

```

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
0	1	18	4	op		n
011	11	18	4	intl		n
1	11	11	4	fnpa		n
411	3	3	4	svcl		n

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

The example below shows the values used for route pattern 4 for outgoing call.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 4 is used.
- **FRL:** Set the Facility Restriction Level (FRL) field to 0. It is the least restrictive level.
- **Pfx Mrk:** The prefix mark (Pfx Mrk) of 1 will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for the long distance North American Numbering Plan (NANP) numbers. All HNPA 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: none.**

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

5.10. Saving Communication Manager Configuration Changes

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

6. Configure Avaya Aura® Session Manager

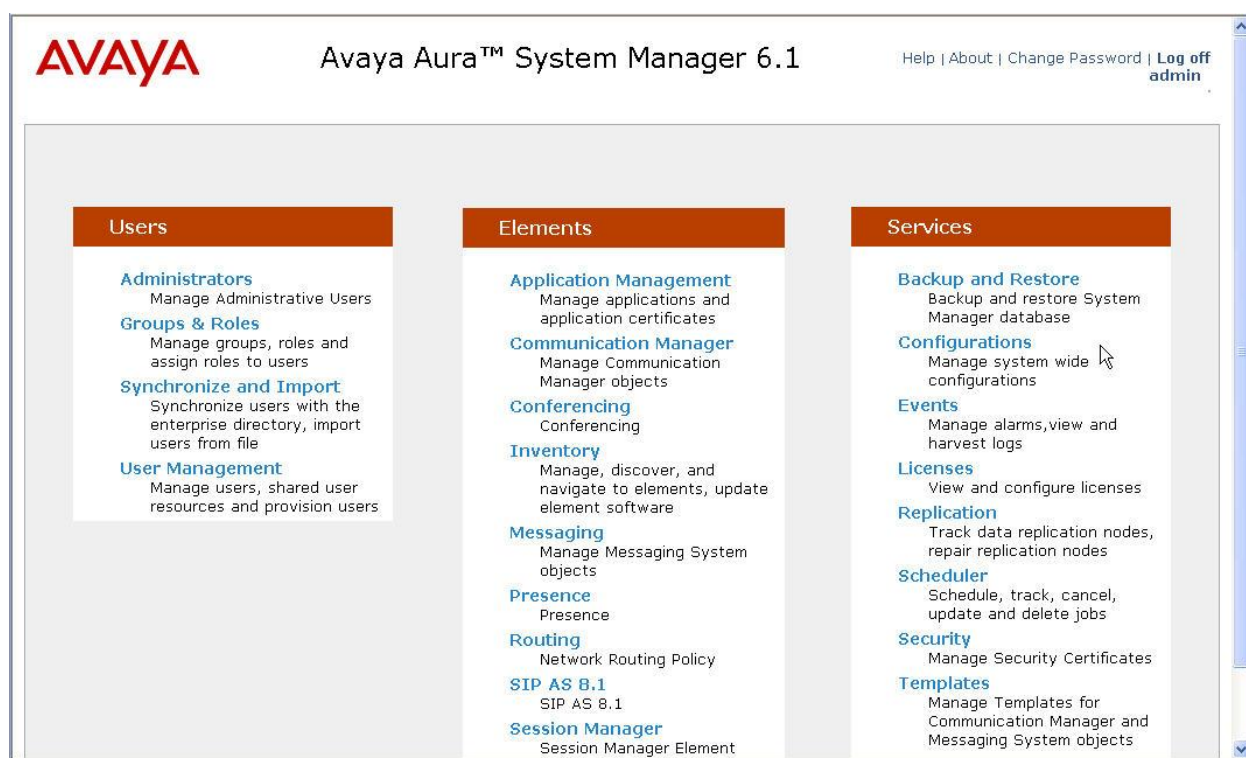
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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, Session Manager and SBC
- 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.

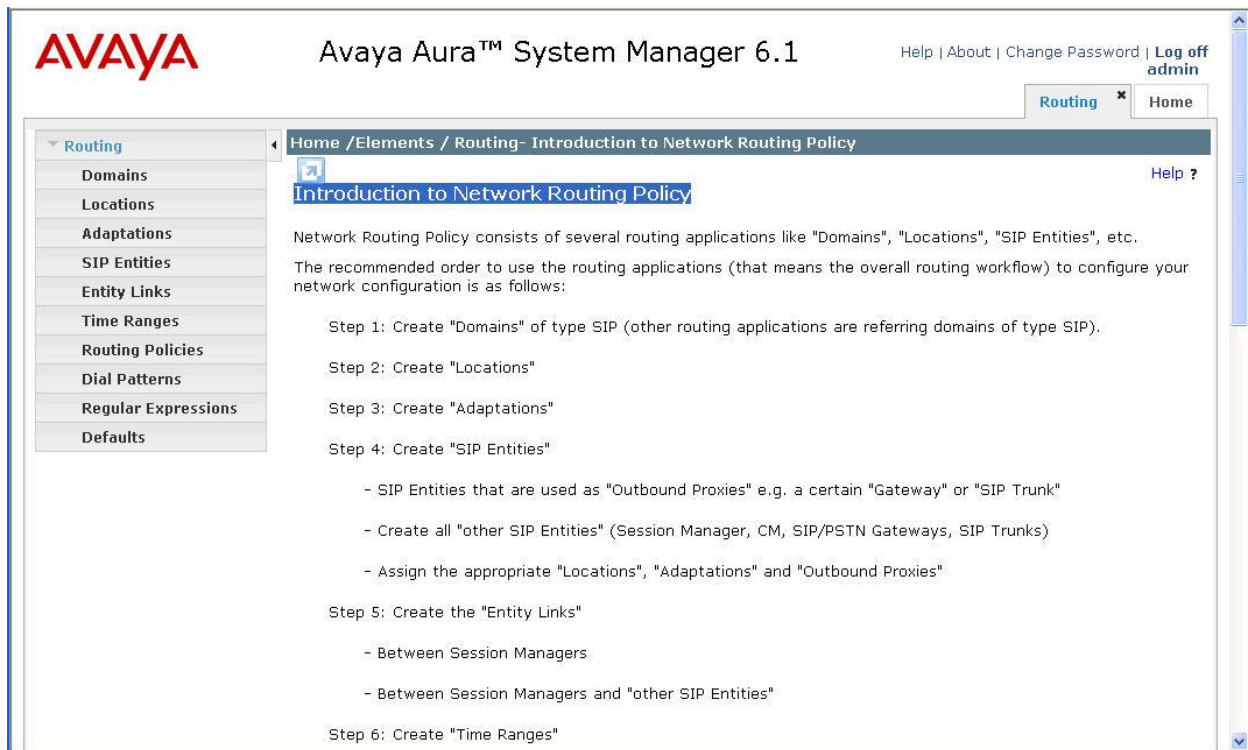
6.1. System Manager Login and Navigation

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.

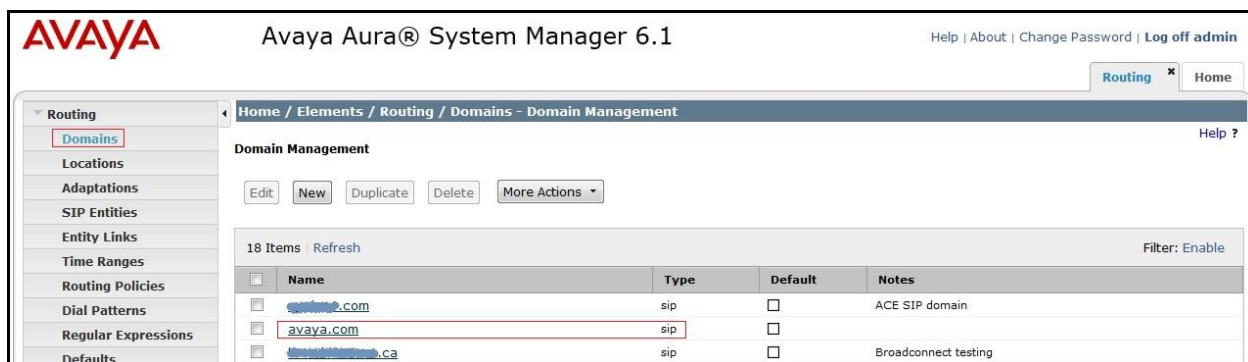
The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



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 domain **avaya.com** is already being used for communication among a number of Avaya systems and applications, including an Avaya Aura® Messaging system with SIP integration to Session Manager. The domain **avaya.com** is not known to the Bell Canada SIP Trunking Service.



The domain **cust6-tor.vtac.bell.ca** is the domain known to Bell Canada as the enterprise SIP domain. For example, for calls from the enterprise to the service provider, this domain appears in the P-Asserted-Identity header in the INVITE message sent to Bell Canada's SIP Trunking Service.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Domains - Domain Management

Domain Management

Edit New Duplicate Delete More Actions

17 Items Refresh Filter: Enable

Name	Type	Default	Notes
acebvw.com	sip	<input type="checkbox"/>	ACE SIP domain
avaya.com	sip	<input type="checkbox"/>	for Cisco UCM Testing
broadconnect.ca	sip	<input type="checkbox"/>	Broadconnect testing
bwdev7.com	sip	<input type="checkbox"/>	For PAETEC Communication SIP
bwdev7.com	sip	<input type="checkbox"/>	For SIP
cm521.mtsallstream.com	sip	<input type="checkbox"/>	
cm601.avaya.com	sip	<input type="checkbox"/>	Enterprise domain for CM601
cust2-tor.vtac.bell.ca	sip	<input type="checkbox"/>	Bell Canada Circuit 2
cust6-tor.vtac.bell.ca	sip	<input type="checkbox"/>	BellCanada Circuit 1
level3.com	sip	<input type="checkbox"/>	
level-3.voip.com	sip	<input type="checkbox"/>	level3 testing
mtsallstream.com	sip	<input type="checkbox"/>	mtsallstream.com
sip.ipc.com	sip	<input type="checkbox"/>	IPC Testing domain
sip.mvpx.movitas.com	sip	<input type="checkbox"/>	For testing with Movitas
sip.skype.com	sip	<input type="checkbox"/>	skype service provider testing
siptrunking.bell.ca	sip	<input type="checkbox"/>	Bell Canada
telus.com	sip	<input type="checkbox"/>	telus testing

Select : All, None

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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Domains - Domain Management

Domain Management

Edit New Duplicate Delete More Actions

17 Items Refresh Filter: Enable

Name	Type	Default	Notes
acebvw.com	sip	<input type="checkbox"/>	ACE SIP domain
avaya.com	sip	<input type="checkbox"/>	for Cisco UCM Testing
broadconnect.ca	sip	<input type="checkbox"/>	Broadconnect testing
bwdev7.com	sip	<input type="checkbox"/>	For PAETEC Communication SIP
bwdev7.com	sip	<input type="checkbox"/>	For SIP
cm521.mtsallstream.com	sip	<input type="checkbox"/>	
cm601.avaya.com	sip	<input type="checkbox"/>	Enterprise domain for CM601
cust2-tor.vtac.bell.ca	sip	<input type="checkbox"/>	Bell Canada Circuit 2
cust6-tor.vtac.bell.ca	sip	<input type="checkbox"/>	BellCanada Circuit 1
level3.com	sip	<input type="checkbox"/>	
level-3.voip.com	sip	<input type="checkbox"/>	level3 testing
mtsallstream.com	sip	<input type="checkbox"/>	mtsallstream.com
sip.ipc.com	sip	<input type="checkbox"/>	IPC Testing domain
sip.mvpx.movitas.com	sip	<input type="checkbox"/>	For testing with Movitas
sip.skype.com	sip	<input type="checkbox"/>	skype service provider testing
siptrunking.bell.ca	sip	<input type="checkbox"/>	Bell Canada
telus.com	sip	<input type="checkbox"/>	telus testing

Select : All, None

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 the 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 screenshot for **Belleville,Ont,Ca** location, which includes all equipment on the **110.10.x.x** subnet including Communication Manager, Session Manager and SBC. Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. The left-hand navigation pane shows a tree structure with 'Routing' expanded, containing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Locations - Location Details' and features a 'Location Details' section with 'Commit' and 'Cancel' buttons. Below this, a 'General' section contains fields for '* Name:' (filled with 'Belleville,Ont,Ca') and 'Notes:' (filled with 'Belleville DevConnect lab'). The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units:' as 'Kbit/sec' and 'Total Bandwidth:' as '1000000'. The 'Per-Call Bandwidth Parameters' section has '* Default Audio Bandwidth:' set to '80 Kbit/sec'. The 'Location Pattern' section includes 'Add' and 'Remove' buttons, a table with one item, and a 'Filter: Enable' option. The table has columns for 'IP Address Pattern' and 'Notes', with the first row showing '* 110.10.*.*'. At the bottom, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

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](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* **Name:** Belleville,Ont,Ca

Notes: Belleville DevConnect lab

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 1000000

Per-Call Bandwidth Parameters

* **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"/>	* 110.10.*.*	

Select : All, None

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

6.4. Add Adaptation Module

Session Manager can be configured with Adaptation module that modifies 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.

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.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left sidebar shows a navigation menu with 'Routing' selected, and 'Adaptations' highlighted under the 'Routing' section. The main content area is titled 'Home / Elements / Routing / Adaptations - Adaptations'. It features a table of 12 items, with a 'Filter: Enable' option. The table has columns for 'Name', 'Module name', 'Egress URI Parameters', and 'Notes'. The first two items, 'BC_Avaya_SBC' and 'BC_CM-ES', are highlighted with red boxes. The 'BC_Avaya_SBC' row shows 'DigitConversionAdapter' with parameters 'osrcd=cust6-tor.vsac.bell.ca' and 'odstd=siptrunking.bell.ca fromto=true'. The 'BC_CM-ES' row shows 'DigitConversionAdapter' with parameters 'odstd=avaya.com' and 'osrcd=avaya.com fromto=true'. Other items include 'ChangeDomainName', 'CSIK75Bottom', 'CSIK Adaptation', 'Diversion for Level 3', 'Movitas', 'MSUM2010', 'Paetec Diversion Header', 'skypeadap', 'Star_Telecom', and 'StarTelecom2'.

Name	Module name	Egress URI Parameters	Notes
BC_Avaya_SBC	DigitConversionAdapter	osrcd=cust6-tor.vsac.bell.ca odstd=siptrunking.bell.ca fromto=true	
BC_CM-ES	DigitConversionAdapter	odstd=avaya.com osrcd=avaya.com fromto=true	
ChangeDomainName	IPCAAdapter	osrcd=sip.ipc.com odstd=sip.ipc.com	
CSIK75Bottom	DigitConversionAdapter		
CSIK Adaptation	CS1000Adapter		CS1000 Adapter
Diversion for Level 3	DiversionTypeAdapter	odstd=135.10.98.104 osrcd=4.55.35.85 MIME=no	Outbound Diversion for Level3
Movitas	number_2_text		
MSUM2010	DigitConversionAdapter	131.107.5.62	
Paetec Diversion Header	DiversionTypeAdapter		
skypeadap		osrcd=135.10.97.198 odstd=sip.skype.com	
Star_Telecom	DigitConversionAdapter	osrcd=bvwddev7.com odstd=bvwddev7.com iodstd=bvwddev7.com iosrcd=bvwddev7.com	
StarTelecom2	DigitConversionAdapter	iodstd=135.10.97.184	

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

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

- **osrcd=cust6-tor.vsac.bell.ca**. This configuration enables the outbound source domain to be overwritten with **cust6-tor.vsac.bell.ca**. For example, for outbound PSTN calls from the Avaya CPE to Bell Canada, the PAI header will contain “**cust6-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**.
- **fromto=true**. With this configuration, for an outbound call to Bell Canada, Session Manager will set the host portion of both the PAI and the From headers to **cust6-tor.vsac.bell.ca**, and the host portion of the Request-URI and To headers to **siptrunking.bell.ca**.

In the sample configuration, Session Manager is used to adapt the domain **avaya.com** from Communication Manager to **cust6-tor.vsac.bell.ca** and **siptrunking.bell.ca** which are the domains known to Bell Canada.

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

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations (highlighted), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Adaptations - Adaptation Details'. It shows the 'Adaptation Details' for 'BC SBC'. The 'General' tab is active, displaying the following configuration:

- * Adaptation name:** BC SBC
- Module name:** DigitConversionAdapter
- Module parameter:** osrcd=cust6-tor.vsac.bell.ca odst
- Egress URI Parameters:** (empty field)
- Notes:** (empty field)

Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

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** specifies three parameters used to adapt the FQDN to the domains expected by Communication Manager in the sample configuration.

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

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 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 **Digit Conversion 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 **Digit Conversion for Outgoing Calls from SM** correspond to incoming calls from the PSTN that are routed by Session Manager to Communication Manager. The digit conversion that converts a Communication Manager extension (e.g., 188X) to a corresponding LDN or DID number known to the PSTN (e.g., 416775188X) is configured in Session Manager as shown below.

AVAYA

Avaya Aura® System Manager 6.1

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

Routing

Home

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details

General

* Adaptation name:

BC CM-ES

Module name:

DigitConversionAdapter

Module parameter:

pdstd=avaya.com osrcd=avaya.cd

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*188	*4	*4		*0	416775	origination	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*416775	*10	*10		*6		destination	

Select : All, None

* Input Required

Commit

Cancel

In the example shown above, if a user on the PSTN dials 416-777-188X, Session Manager will convert the number to 188X before sending the SIP INVITE to Communication Manager. For an outbound call, if extension 188X dials the PSTN, Communication Manager sends the extension 188X to Session Manager as the calling number, Session Manager will convert the calling number to 416777188X.

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 SBC.

To add a new SIP Entity, 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 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 the entity.
- **Location:** Select one of the locations defined previously in **Section 6.3**.
- **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 displays the Avaya Aura System Manager 6.1 web interface. The left navigation pane shows the 'Routing' menu expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and shows the 'General' tab. The form contains the following fields and values:

- Name:** DevASM
- FQDN or IP Address:** 110.10.97.198
- Type:** Session Manager (dropdown)
- Notes:** For Session Manager
- Location:** Belleville, Ont, Ca (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** America/Toronto (dropdown)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

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 **Port** entry **5060** with **TCP** for connecting to Communication Manager and SBC.

Port

Add Remove

9 Items Refresh Filter: Enable

Port	Protocol	Default Domain	Notes
15060	TLS	acebvw.com	
5060	TCP	avaya.com	
5060	UDP	bvwdev.com	
5061	TLS	sip.ipc.com	SIPL 5061
5062	TCP	sip.ipc.com	
5071	TLS	bvwdev.com	SIPL 5071
5080	TCP	bvwdev.com	To_Sipera
5081	TCP	siptrunking.bell.ca	BellCanada_CM_SM_Acme
5090	TCP	bvwdev.com	

Select : All, None

* Input Required

Commit Cancel

The following screen shows the addition of Communication Manager SIP Entities. In order for Session Manager to send SIP service provider traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of Communication Manager. Select **Type** is **CM**. For the **Adaptation** field, select the adaptation module “**BC CM-ES**” which is previously defined in **Section 6.4**.

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

- Name:** DevCM217
- FQDN or IP Address:** 110.10.97.217
- Type:** CM (dropdown)
- Notes:** (empty text field)
- Adaptation:** BC EM-ES (dropdown)
- Location:** Belleville, Ont, Ca (dropdown)
- Time Zone:** America/Toronto (dropdown)
- Override Port & Transport with DNS SRV:** (unchecked checkbox)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

 Buttons for 'Commit' and 'Cancel' are located at the top right of the form area.

The following screen shows the addition of the SIP Entity for SBC. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** is **Other**. Select **Adaptation** as **BC SBC** as created in **Section 6.4**.

The screenshot shows the Avaya Aura System Manager 6.1 interface for configuring a SIP Entity named ACME_SBC. The layout is identical to the previous screenshot, but with the following field values:

- Name:** ACME_SBC
- FQDN or IP Address:** 110.10.97.184
- Type:** Other (dropdown)
- Notes:** Acme_SBC
- Adaptation:** BC SBC (dropdown)
- Location:** Belleville, Ont, Ca (dropdown)
- Time Zone:** America/New_York (dropdown)
- Override Port & Transport with DNS SRV:** (unchecked checkbox)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

 The 'Commit' and 'Cancel' buttons are also present.

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links are created for Communication Manager and for the 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 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 SBC, select the 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**.
- **Connection Policy:** Select **Trusted**. Note: If this is selected, 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 SBC. For the compliance test, transport protocol TCP and port 5060 are used to match the values used on the Communication Manager signaling group form in **Section 5.6** and in **Figure 1**.

Entity Link to Communication Manager:

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Commit Cancel Help ?

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* DevASM_DevCM217_50	* DevASM	TCP	* 5060	* DevCM217	* 5060	Trusted	

* Input Required

Commit Cancel

Entity Link to SBC:

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Commit Cancel Help ?

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* DevASM_Acme_SBC	* DevASM	TCP	* 5060	* ACME_SBC	* 5060	Trusted	

* Input Required

Commit Cancel

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 for Communication Manager and for the 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 **BellCanada_To_CM601** for Communication Manager.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Commit Cancel Help ?

General

* Name: BellCanada_To_CM601

Disabled: ☐

Notes: BellCanada_To_CM601

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DevCM217	110.10.97.217	CM	

The following screens show the Routing Policies **CM601_To_BellCanada** for the SBC.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Commit Cancel Help ?

General

* Name: CM601_To_BellCanada

Disabled: ☐

Notes: CM601_To_BellCanada

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACME_SBC	110.10.97.184	Other	Acme_SBC

6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns are 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.) are similarly defined.

The first example shows that 11-digit dialed numbers that begin with **1** and has a destination domain of **siptrunking.bell.ca** uses route policy **CM601_To_BellCanada** as defined in **Section 6.7**.

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

Routing Home

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

Dial Pattern Details Help ? Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca	Belleville DevConnect lah	CM601_To_BellCanada	0	<input type="checkbox"/>	ACME_SBC	CM601_To_BellCanada

The second example shows that inbound 10-digit numbers that start with **416** to domain **cust6-tor.vsaac.bell.ca** uses route policy **BellCanada_To_CM601** as defined in **Section 6.7**. These are the DID numbers assigned to the enterprise by Bell Canada.

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

Routing Home

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

Dial Pattern Details Help ? Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		BellCanada_To_CM601	0	<input type="checkbox"/>	DevCM217	BellCanada_To_CM601

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

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

* Input Required Commit Cancel

6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is 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 shows the Avaya logo and the title 'Avaya Aura® System Manager 6.1'. On the right, there are links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below the header, a breadcrumb trail reads 'Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration'. The left navigation pane is expanded to show 'Session Manager Administration'. The main content area is titled 'Edit Session Manager' and includes 'Commit' and 'Cancel' buttons. Below this, there are tabs for 'General', 'Security Module', 'NIC Bonding', 'Monitoring', 'CDR', 'Personal Profile Manager (PPM)', 'Connection Settings', and 'Event Server'. The 'General' tab is active, showing the following fields: 'SIP Entity Name' (set to 'DevASM'), 'Description' (empty), '*Management Access Point Host Name/IP' (set to '110.10.97.197'), and '*Direct Routing to Endpoints' (set to '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.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

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

Security Module ▼

SIP Entity IP Address

110.10.97.198

*Network Mask

255.255.255.192

*Default Gateway

110.10.97.193

*Call Control PHB

46

*QOS Priority

6

*Speed & Duplex

Auto ▼

VLAN ID

7. Configure Acme Packet Net-Net 3800 Session Border Controller

This section describes the configuration of the Acme Packet Session Border Controller (SBC) necessary for interoperability with Avaya SIP-enabled enterprise solution and Bell Canada SIP Trunking Service. The SBC is configured via the Acme Packet Command Line Interface (ACLI).

This section will not attempt to describe each component in its entirety, but instead will highlight fields in each component which relates to the functionality in these Application Notes. The remaining fields are generally the default/standard value pre-defined by the SBC.

In the compliance test, according to the recommended configuration in **Figure 1**, the enterprise network resides on the inside and the service provider resides on the outside of the SBC.

7.1. Acme Packet Command Line Interface

The SBC is configured using the ACLI. The following are the generic ACLI steps for configuring various elements.

1. Access to the console port of the SBC using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the SBC for cable connection).

Use the following settings for the serial port on the PC.

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

2. Log into the SBC with the proper user password.
3. Enable the super user mode by entering **enable** command with a proper super user password. The command prompt will change to include a “#” instead of a “>” while in super user mode. This level of system access (i.e. at the “acmesystem#” prompt) will be referred to as the *main* level of the ACLI.
4. In super user mode, enter **configure terminal** command to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the *configuration* level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface**).
7. Enter the name of an element parameter followed by its value (e.g., **name INSIDE**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat **Steps 5 - 9** to configure all other elements.
11. Enter **exit** to return to the main level.

12. Type **save-config** to save the configuration.
13. Type **activate-config** to activate the configuration.

After accessing different levels of the ACLI to configure elements and parameters, it is necessary to return to the main level in order to run certain tasks such as saving the configuration, activating the configuration, and rebooting the system.

Note: Acme Packet Net-Net 3800 SBC provisioning applicable to the reference configuration is shown in **bold** text. Other parameters and setting are shown for informational purposes.

7.2. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface of slot 01/port 0 of the SBC as shown below. It connects to the external public internet which is an un-trusted network.

```
phy-interface
  name                INSIDE
  operation-type      Media
  port                0
  slot                0
  virtual-mac
  admin-state         enabled
  auto-negotiation     enabled
  duplex-mode         FULL
  speed               100
  overload-protection disabled
```

The Ethernet interface slot 0/port 0 is connected to the internal corporate LAN as shown in the screen below:

```
phy-interface
  name                OUTSIDE
  operation-type      Media
  port                0
  slot                1
  virtual-mac
  admin-state         enabled
  auto-negotiation     enabled
  duplex-mode         FULL
  speed               100
  overload-protection disabled
```

Define a logical network interface for each physical interface to assign it a routable IP address. As described in **Figure 1**, the network interface below defines the IP addresses on physical interface **INSIDE** which connects to the enterprise network.

```
network-interface
  name                INSIDE
  sub-port-id         0
  description
  hostname
  ip-address          110.10.97.184
  pri-utility-addr
```

```

sec-utility-addr
netmask                255.255.255.192
gateway                110.10.97.129
sec-gateway
gw-heartbeat
    state                disabled
    heartbeat            0
    retry-count          0
    retry-timeout        1
    health-score         0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout            11
hip-ip-list            110.10.97.184
ftp-address
icmp-address          110.10.97.184
snmp-address
telnet-address

```

The network interface below defines the IP addresses on physical interface OUTSIDE which connects to Bell Canada.

```

network-interface
    name                OUTSIDE
    sub-port-id          0
    description
    hostname
    ip-address          110.10.98.98
    pri-utility-addr
    sec-utility-addr
    netmask              255.255.255.224
    gateway              110.10.98.97
    sec-gateway
    gw-heartbeat
        state                disabled
        heartbeat            0
        retry-count          0
        retry-timeout        1
        health-score         0
    dns-ip-primary
    dns-ip-backup1
    dns-ip-backup2
    dns-domain
    dns-timeout          11
    hip-ip-list          110.10.98.98
    ftp-address
    icmp-address          110.10.98.98
    snmp-address

```

7.3. Realm

A realm represents a group of related SBC components.

For the compliance test, two realms are created. The realm names INSIDE below represents the internal network on which contains the elements configured for the enterprise.

realm-config	
identifier	INSIDE
description	
addr-prefix	0.0.0.0
network-interfaces	
	INSIDE:0
<Text removed for brevity>	

The realm names OUTSIDE below represents the external network which contains the elements configured for Bell Canada

realm-config	
identifier	OUTSIDE
description	
addr-prefix	0.0.0.0
network-interfaces	
	OUTSIDE:0
<Text removed for brevity>	

7.4. Session Agent

A session agent defines the characteristics of signaling from a peer gateway endpoint such as Session Manager (as known as Call Server) or Bell Canada (as known as Trunk Server).

The **session agent** in the screen below represents the configuration for Bell Canada. As described in **Figure 1**, the IP interface of Bell Canada SIP Trunking Service is defined with transport protocol is UDP and port 5060.

- Set **state** to **enabled**.
- Set **app-protocol** to **SIP**.
- Set **realm-id** to **OUTSIDE**.
- Set **in-manipulationid** to **BellCanada_To_CM**. This profile is defined in SIP Header Manipulation Section as discussed later in **Section 7.7**. It is a set of rules to manipulate the SIP signaling for inbound call from Bell Canada such as to normalize the From, To, Request-URI headers etc. to be known to Communication Manager.
- Set **out-manipulationid** to **CM_To_BellCanada**. This profile is defined in SIP Header Manipulation Section as discussed later in **Section 7.7**. It is a set of rules to manipulate the SIP signaling for outbound call to Bell Canada such as to normalize the From, To, Request-URI headers etc. to be known to Bell Canada.

```

session-agent
  hostname                220.20.237.205
  ip-address              220.20.237.205
  port                    5060
  state                   enabled
  app-protocol            SIP
  app-type
  transport-method        UDP
  realm-id                OUTSIDE
  egress-realm-id
  description              CM_To_BellCanada
    <Text removed for brevity>

  ping-method
  ping-interval
    <Text removed for brevity>

  in-manipulationid       BellCanada_To_CM
  out-manipulationid      CM_To_BellCanada
    <Text removed for brevity>

```

The **session agent** in the screen below represents the configuration for Session Manager. As described in **Figure 1**, the IP interface of Session Manager is defined with transport protocol is TCP and port 5060.

- Set **state** to **enabled**.
- Set **app-protocol** to **SIP**.
- Set **realm-id** to **INSIDE**.

Note: the **in-manipulationid** and **out-manipulationid** are kept default which is blank. It means there is no signaling manipulation is performed on the SIP traffic toward Communication Manager. The manipulation is already applied to the Trunk Server side.

```

session-agent
  hostname                110.10.97.198
  ip-address              110.10.97.198
  port                    5060
  state                   enabled
  app-protocol            SIP
  app-type
  transport-method        DynamicTCP
  realm-id                INSIDE
  egress-realm-id
  description              BellCanada_To_CM
    <Text removed for brevity>

```

7.5. Digest Authentication Configuration

In the compliance test, Bell Canada requires Digest Authentication on trunk group connect to the enterprise. By nature, neither Session Manager nor Communication Manager supports this feature. Digest Authentication will be performed by the SBC. It is configured under Session

Agent defined for Call Server (as known as Session Manager). Note: Digest Authentication is not configured under Session Agent defined for Trunk Server (as known as Bell Canada)

The screen below shows the Digest Authentication in detail. The auth-attribute is configured with the values assigned by Bell Canada as following:

- Set the **auth-realm** to **siptrunking.bell.ca**.
- Set **username** to **4167751880**.
- Set **password** to the value assigned by Bell Canada.

```
session-agent
  hostname                110.10.97.198
  ip-address              110.10.97.198
  port                    5060
  state                   enabled
  app-protocol            SIP
  app-type
  transport-method        DynamicTCP
  realm-id                INSIDE
  egress-realm-id
  description              BellCanada_To_CM
  carriers
  allow-next-hop-lp       enabled
  constraints              disabled
  <Text removed for brevity>
  sip-profile
  sip-isup-profile
  auth-attribute
    auth-realm             siptrunking.bell.ca
    username               4167751880
    password                *****
    in-dialog-methods
```

7.6. SIP Configuration

The SIP configuration (*sip-config*) defines the global system-wide SIP parameters.

Configure the sip-config as follows:

- Set the **state** to **enabled** to allow SIP call to be processed by the SBC.
- Set **home-realm-id** to **INSIDE**.
- Set **egress-realm-id** to **OUTSIDE**.

```
sip-config
  state                   enabled
  operation-mode           dialog
  dialog-transparency      enabled
  home-realm-id            INSIDE
  egress-realm-id          OUTSIDE
  nat-mode                 None
  <Text removed for brevity>
```

7.7. SIP Interface

SIP interface (*sip-interface*) enables SIP application protocol on a particular network interface.

Two SIP interfaces are defined for this compliance test. The SIP interface as shown below is used by the SBC to listen to the enterprise SIP traffic from realm INSIDE. The SBC is configured to listen on network interface 110.10.97.184, transport protocol TCP and port 5060.

```
sip-interface
state                enabled
realm-id             INSIDE
description
sip-port
    address          110.10.97.184
    port             5060
    transport-protocol TCP
<Text removed for brevity>
```

The SIP interface below is used by the SBC to listen to SIP traffic from realm OUTSIDE which defined for Bell Canada. The SBC is configured to listen on network interface 110.10.98.98, transport protocol UDP and port 5060.

```
sip-interface
state                enabled
realm-id             OUTSIDE
description
sip-port
    address          110.10.98.98
    port             5060
    transport-protocol UDP
<Text removed for brevity>
```

7.8. SIP Manipulation

SIP Header Manipulation Rules (HMR) are used to modify the SIP messages (if necessary) for interoperability between Communication Manager and Bell Canada.

In the compliance test, Bell Canada requires the SIP signaling from enterprise has to meet its specification. For that purpose, the HMR **CM_To_BellCanada** is created for Session Agent which is defined for Bell Canada in **Section 7.4**. The HMR applied to SIP message from Communication Manager toward Bell Canada. It contains rules to perform the following:

- The header rule **modRURI** replaces the private enterprise SIP domain in URI-Host of Request-URI by **siptrunking.bell.ca** to send to Bell Canada.
- The header rule **modFrom** replaces the private enterprise SIP domain in URI-Host of From header to **cust6-tor.vsac.bell.ca** to sends to Bell Canada.
- The header rule **modTo** replaces the private enterprise SIP domain in URI-Host of To header to **siptrunking.bell.ca** to sends to Bell Canada.
- The header rule **checkCallID** is defined to search Call-ID header for a string of **cust6-tor.vsac.bell.ca**. The search result is stored as a logical value which will be used in combination by the header rule **modCallID**. If the **checkCallID** returns a negative result, it means the Call-ID header does not contain the expected string, and then the **modCallID** will delete the original URI-Host and replace it by the string of **cust6-tor.vsac.bell.ca** to the Call-ID header. This modification is to meet the requirement of Bell Canada SIP

Trunking Service. Note: The rules to modify the Call-ID only apply to the msg-type request. It should not apply to the msg-type response. It is dangerous to modify the Call-ID of the response, it can cause call dropped or fail to be successfully established.

- The header rule **modPAI** replaces the private enterprise SIP domain in URI-Host of P-Asserted-Identity header to **cust6-tor.v sac.bell.ca** to sends to Bell Canada.
- The header rule **storeContact** is defined to search for the URI-User in Contact header. If the URI-User is present, it will be stored and used in combination by modContact header rule. In case the Contact header does not contain an URI-User, the modContact header rule will replace the URI-Host with a value of “**tgrp=VSAC_4167751880_01A;trunk\ context=siptrunking.bell.ca@110.10.98.98:5060**”. In the other case where the Contact header has an URI-User, the modContact rule will keep construct new Contact header with URI-User is stored from the storeContact header rule and URI-Host as “**;tgrp=VSAC_4167751880_01A;trunk\ context=siptrunking.bell.ca@110.10.98.98:5060**”. This modification is to meet the requirement of Bell Canada SIP Trunking Service.
- The header rule **modDiversion** replaces the private enterprise SIP domain in URI-Host of Diversion header to **cust6-tor.v sac.bell.ca** to sends to Bell Canada. Note: If Diversion header contain URI-Host different than a pre-defined value assigned by Bell Canada, the call forward off-net and EC500 call from Communication Manager will fail.

```

sip-manipulation
  name                                CM_To_BellCanada
  description
  split-headers
  join-headers
  header-rule
    name                               modRURI
    header-name                        request-uri
    action                             manipulate
    comparison-type                    case-sensitive
    msg-type                           any
    methods
    match-value
    new-value
    element-rule
      name                             modURIHost
      parameter-name
      type                              uri-host
      action                            replace
      match-val-type                    any
      comparison-type                   case-sensitive
      match-value
      new-value                         "siptrunking.bell.ca"
  header-rule
    name                               modFrom
    header-name                        From
    action                             manipulate
    comparison-type                    case-sensitive
    msg-type                           any
    methods
    match-value
    new-value
    element-rule
      name                             modURIHost

```

	parameter-name	
	type	uri-host
	action	replace
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	"cust6-tor.vsac.bell.ca"
header-rule		
	name	modTo
	header-name	To
	action	manipulate
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	
	element-rule	
	name	modURIHost
	parameter-name	
	type	uri-host
	action	replace
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	"siptrunking.bell.ca"
header-rule		
	name	checkCallID
	header-name	Call-ID
	action	store
	comparison-type	pattern-rule
	msg-type	any
	methods	
	match-value	
	new-value	
	element-rule	
	name	checkCallID
	parameter-name	
	type	header-value
	action	store
	match-val-type	any
	comparison-type	pattern-rule
	match-value	(.*) (@cust6-
tor.vsac.bell.ca) (.*)	new-value	
header-rule		
	name	modCallID
	header-name	Call-ID
	action	manipulate
	comparison-type	case-sensitive
	msg-type	request
	methods	
	match-value	
	new-value	
	element-rule	
	name	delURIHost
	parameter-name	
	type	header-value
	action	find-replace-all
	match-val-type	any
	comparison-type	pattern-rule
	match-value	@.*
	new-value	

tor.vtac.bell.ca"	element-rule	
	name	addURIHost
	parameter-name	
	type	header-value
	action	add
	match-val-type	any
	comparison-type	boolean
	match-value	
	new-value	\$ORIGINAL+"@cust6-
	header-rule	
	name	modPAI
	header-name	P-Asserted-Identity
	action	manipulate
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	
	element-rule	
	name	modURIHost
	parameter-name	
	type	uri-host
	action	replace
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	"cust6-tor.vtac.bell.ca"
	header-rule	
	name	storeContact
	header-name	Contact
	action	store
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	
	element-rule	
	name	storeURIUser
	parameter-name	
	type	uri-user
	action	store
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	
	header-rule	
	name	modContact
	header-name	Contact
	action	manipulate
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	
	element-rule	
	name	withoutURIUser
	parameter-name	
	type	header-value
	action	replace
	match-val-type	any
	comparison-type	boolean

```

        match-value                !$storeContact.$storeURIUser
        new-value
<sip:tgrp=VSAC_4167751880_01A;trunk\~-context=siptrunking.bell.ca@110.10.98.98:5060>
    element-rule
        name                        withURIUser
        parameter-name
        type                        header-value
        action                      replace
        match-val-type             any
        comparison-type            boolean
        match-value                $storeContact.$storeURIUser
        new-value
<sip:+$storeContact.$storeURIUser.$0+;tgrp=VSAC_4167751880_01A;trunk\~-
context=siptrunking.bell.ca@110.10.98.98:5060>
    header-rule
        name                        modDiversion
        header-name                 Diversion
        action                      manipulate
        comparison-type             case-sensitive
        msg-type                    any
        methods
        match-value
        new-value
    element-rule
        name                        modURIHost
        parameter-name
        type                        uri-host
        action                      replace
        match-val-type             any
        comparison-type            case-sensitive
        match-value
        new-value                  "cust6-tor.vsac.bell.ca"

```

The HMR **BellCanada_To_CM** is created for Session Agent which is defined for Bell Canada in **Section 7.4**. The HMR applied to SIP message from Bell Canada toward Communication Manager. It contains rules to perform the following:

- The header rule **modRURI** replaces the public SIP domain in URI-Host of Request-URI by **cust6-tor.vsac.bell.ca** to send to Session Manager.
- The header rule **modFrom** replaces the public SIP domain in URI-Host of From header by **siptrunking.bell.ca** to send to Session Manager.
- The header rule **modFrom** replaces the public SIP domain in URI-Host of From header by **siptrunking.bell.ca** to send to Session Manager. The original URI-User of From header contains “+” sign which causes issue to call forward off-net and EC500, for more information please refer to **Section 2.2**, observation #01. Therefore an element rule to remove the “+” sign out of From header also need to be added.
- The header rule **modContact** removes the “+” sign out of URI-User of Contact header. Because the original URI-User of Contact header contains “+” sign which causes issue to call forward off-net and EC500, for more information please refer to **Section 2.2**, observation #01.

```

sip-manipulation
    name                        BellCanada_To_CM
    description                 BellCanada_To_CM
    split-headers
    join-headers

```

```

header-rule
    name
    header-name
    action
    comparison-type
    msg-type
    methods
    match-value
    new-value
    element-rule
        name
        parameter-name
        type
        action
        match-val-type
        comparison-type
        match-value
        new-value
header-rule
    name
    header-name
    action
    comparison-type
    msg-type
    methods
    match-value
    new-value
    element-rule
        name
        parameter-name
        type
        action
        match-val-type
        comparison-type
        match-value
        new-value
    element-rule
        name
        parameter-name
        type
        action
        match-val-type
        comparison-type
        match-value
        new-value
header-rule
    name
    header-name
    action
    comparison-type
    msg-type
    methods
    match-value
    new-value
    element-rule
        name
        parameter-name
        type
        action
        match-val-type
        comparison-type
        match-value

```

modRURI	
request-uri	
manipulate	
case-sensitive	
any	
modURIHost	
uri-host	
replace	
any	
case-sensitive	
"cust6-tor.vtac.bell.ca"	
modFrom	
From	
manipulate	
case-sensitive	
any	
modURIHost	
uri-host	
replace	
any	
case-sensitive	
siptrunking.bell.ca	
modURIUser	
uri-user	
replace	
any	
case-sensitive	
\$ORIGINAL-^"+	
modTo	
To	
manipulate	
case-sensitive	
any	
modURIHost	
uri-host	
replace	
any	
case-sensitive	
match-value	

	new-value	"cust6-tor.vtac.bell.ca"
header-rule		
name		modContact
header-name		Contact
action		manipulate
comparison-type		case-sensitive
msg-type		any
methods		
match-value		
new-value		
element-rule		
name		modURIUser
parameter-name		
type		uri-user
action		replace
match-val-type		any
comparison-type		case-sensitive
match-value		
new-value		\$ORIGINAL-^"+"

7.9. Steering Pools

Steering pools define the range of ports to be used for the RTP.

For the compliance test, separate steering pools are defined for each realm.

The key steering pool (*steering-pool*) fields are:

- **ip-address:** The network interface will be used to transmit or receive the RTP.
- **start-port:** An number that begins the port range for RTP.
- **end-port:** An number that ends the port range for RTP.
- **realm-id:** The realm to which steering pool is assigne.

The screen below is the steering pool for **OUTSIDE** realm:

steering-pool	
ip-address	110.10.98.98
start-port	20000
end-port	40000
realm-id	OUTSIDE
<Text removed for brevity>	

The screen below is the steering pool for **INSIDE** realm:

steering-pool	
ip-address	10.10.97.184
start-port	20000
end-port	40000
realm-id	INSIDE
<Text removed for brevity>	

7.10. Local Policy

The local policies below govern the routing call from the enterprise to the service provider and vice versa.

Two local policies are created for the compliance test.

For the inbound call, the local-policy allows all call from source realm **OUTSIDE** to the DID numbers (4167751880-4167751003) to pass through the SBC. To activate the local-policy, set the **state** to **enabled**.

The policy-attribute is defined as follow:

- Set the **next-hop** is the IP address of Session Manager.
- Set the **realm** to **INSIDE**.
- Set the **app-protocol** is **SIP**.
- Set the **state** to **enabled**.

```
local-policy
  from-address          *
  to-address            4167751880
                       4167751881
                       4167751882
                       4167751883
  source-realm          OUTSIDE
  description           BellCanada_To_CM
  activate-time         N/A
  deactivate-time       N/A
  state                 enabled
  policy-priority       none
  <Text removed for brevity>
  policy-attribute
    next-hop            110.10.97.198
    realm               INSIDE
    action              none
    terminate-recursion disabled
    carrier
    start-time          0000
    end-time            2400
    days-of-week        U-S
    cost                0
    app-protocol        SIP
    state               enabled
    methods
    media-profiles
    lookup              single
    next-key
    eloc-str-lkup       disabled
    eloc-str-match
```

For the outbound call, the local-policy allows all call from source realm **INSIDE** and domain **siptrunking.bell.ca** to the any PSTN destination to pass through the SBC. To activate the local-policy, set the **state** to **enabled**.

The policy-attribute is defined as follow:

- Set the **next-hop** is the IP address of Bell Canada SIP Trunking Service.

- Set the **realm** to **OUTSIDE**.
- Set the **app-protocol** is **SIP**.
- Set the **state** to **enabled**.

```

local-policy
  from-address          siptrunking.bell.ca
  to-address            *
  source-realm          INSIDE
  description           CM_To_CM
  activate-time         N/A
  deactivate-time       N/A
  state                 enabled
  policy-priority       none
  <Text removed for brevity>
  policy-attribute
    next-hop            220.20.237.205
    realm               OUTSIDE
    action              none
    terminate-recursion disabled
    carrier
    start-time          0000
    end-time            2400
    days-of-week        U-S
    cost                0
    app-protocol        SIP
    state               enabled
    methods
    media-profiles
    lookup              single
    next-key
    eloc-str-lkup       disabled
    eloc-str-match

```

8. Bell Canada SIP Trunking Configuration

Bell Canada is responsible for the configuration of Bell Canada SIP Trunking Service. The customer will need provide the IP address used to reach the Acme Packet SBC at the enterprise. Bell Canada will provide the customer with the necessary information to configure the SIP connection from the enterprise to the Bell Canada network.

The provided information from Bell Canada includes:

- IP address of the Bell Canada SIP Trunking Service.
- 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.
- Enable OPTIONS heartbeat on the SIP Trunk.
- A customized SIP signaling specification requirement for Call-ID, Contact headers.

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.

Protocol Traces:

The following SIP headers are inspected using Wireshark trace:

- RequestURI: verify the request number and SIP domain
- From: verify the display name and display number
- To: verify the display name and display number
- P-Asserted-Identity: verify the display name and display number
- Privacy: verify the “user, id” masking

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

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

Troubleshooting:

1. SBC
 - Using a network sniffing tool (e.g., Wireshark), monitor the SIP signaling messages between Bell Canada and SBC.

Following is an example inbound call from Bell Canada to Communication Manager.

- Inbound INVITE request from Bell Canada:

```
INVITE sip:4167751881@cust6-tor.vsac.bell.ca;transport=udp SIP/2.0
Via: SIP/2.0/UDP 220.20.237.205:5060;branch=z9hG4bK24tat3100gnhakg805k1.1
From: <sip:+16139675258@siptrunking.bell.ca;user=phone>;tag=SD14gbe01-1435897115-1336572922496-
To: "Bell Demo12345"<sip:4167751881@cust6-tor.vsac.bell.ca>
Call-ID: SD14gbe01-64b9997cb2c633fe01511abcf90a6d2b-a0n8330
CSeq: 419046721 INVITE
Contact: <sip:+16139675258@220.20.237.205:5060;transport=udp>
Supported: 100rel
```

Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: multipart/mixed,application/media_control+xml,application/sdp
Max-Forwards: 18
Content-Type: application/sdp
Content-Length: 205

v=0
o=BroadWorks 73956 1 IN IP4 220.20.237.205
s=-
c=IN IP4 220.20.237.205
t=0 0
m=audio 20018 RTP/AVP 0 18 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=fmtp:18 annexb=no

- 200OK/SDP response by Communication Manager:

SIP/2.0 200 OK
Via: SIP/2.0/UDP 220.20.237.205:5060;branch=z9hG4bK24tat3100gnhakg805k1.1
From: <sip:+16139675258@cust6-tor.v sac.bell.ca;user=phone>;tag=SD14gbe01-1435897115-1336572922496-
To: "Bell
Demol2345"<sip:4167751881@siptrunking.bell.ca>;tag=0b0b9d9e5a7e11fd114fc3681000
Call-ID: SD14gbe01-64b9997cb2c633fe01511abcf90a6d2b-a0n8330
CSeq: 419046721 INVITE
Supported: 100rel,join,replaces,sdp-anat,timer
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
Contact: <sip:4167751881;tgrp=VSAC_4167751880_01A;trunk-
context=siptrunking.bell.ca@110.10.98.98:5060>
Accept-Language: en
Server: Avaya CM/R016x.00.1.510.1 AVAYA-SM-6.1.1.0.611023
Session-Expires: 1200;refresher=uas
Content-Type: application/sdp
Content-Length: 173
P-Location: SM;origlocname="Belleville,Ont,Ca";termlocname="Belleville,Ont,Ca"
P-Asserted-Identity: "Bell H323 x1881" <sip:4167751881@cust6-tor.v sac.bell.ca>

v=0
o=- 1336573344 2 IN IP4 110.10.98.98
s=-
c=IN IP4 110.10.98.98
b=AS:64
t=0 0
m=audio 20176 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000

Following is an example outbound call from Communication Manager to Bell Canada.

- Outbound INVITE request from Communication Manager:

INVITE sip:16139675258@siptrunking.bell.ca SIP/2.0
Via: SIP/2.0/UDP 110.10.98.98:5060;branch=z9hG4bKfjd65g3030o1jhsb3311.1
To: <sip:16139675258@siptrunking.bell.ca>
Call-ID: 0cc8e7be9a7e1196124fc3681000@cust6-tor.v sac.bell.ca
CSeq: 1 INVITE
Supported: 100rel,join,replaces,sdp-anat,timer
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
User-Agent: Avaya CM/R016x.00.1.510.1 AVAYA-SM-6.1.1.0.611023

Contact: <sip:4167751881;tgrp=VSAC_4167751880_01A;trunk-context=siptrunking.bell.ca@110.10.98.98:5060>
Accept-Language: en
Alert-Info: <cid:internal@siptrunking.bell.ca>;avaya-cm-alert-type=internal
Min-SE: 1200
Session-Expires: 1200;refresher=uac
Content-Type: application/sdp
Content-Length: 255
P-Asserted-Identity: "Bell H323 x1881" <sip:4167751881@cust6-tor.vvac.bell.ca>
From: "Bell H323 x1881" <sip:4167751881@cust6-tor.vvac.bell.ca>;tag=0cc8e7be9a7e1195124fc3681000
P-Location: SM;origlocname="Belleville, Ont, Ca";termlocname="Belleville, Ont, Ca"
Max-Forwards: 66
Route: <sip:16139675258@220.20.237.205:5060;lr>

v=0
o=- 1336574904 1 IN IP4 110.10.98.98
s=-
c=IN IP4 110.10.98.98
b=AS:64
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 20184 RTP/AVP 0 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000

- 401 Unauthorized response by Bell Canada:

SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 110.10.98.98:5060;branch=z9hG4bKfjd65g3030o1jhsb3311.1
To: <sip:16139675258@siptrunking.bell.ca>;tag=SDs3m0e99-241879626-1336574482662
Call-ID: 0cc8e7be9a7e1196124fc3681000@cust6-tor.vvac.bell.ca
CSeq: 1 INVITE
From: "Bell H323 x1881" <sip:4167751881@cust6-tor.vvac.bell.ca>;tag=0cc8e7be9a7e1195124fc3681000
WWW-Authenticate: DIGEST
qop="auth",nonce="BroadWorksXh20hxr6uTeiowp0BW",realm="siptrunking.bell.ca",algorithm=MD5
Content-Length: 0

- reINVITE with Authorization header request from Communication Manager:

INVITE sip:16139675258@siptrunking.bell.ca SIP/2.0
Via: SIP/2.0/UDP 110.10.98.98:5060;branch=z9hG4bKf3k97p304gm1jh0ce0o0
To: <sip:16139675258@siptrunking.bell.ca>
Call-ID: 0cc8e7be9a7e1196124fc3681000@cust6-tor.vvac.bell.ca
CSeq: 2 INVITE
Supported: 100rel,join,replaces,sdp-anat,timer
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH
User-Agent: Avaya CM/R016x.00.1.510.1 AVAYA-SM-6.1.1.0.611023
Contact: <sip:4167751881;tgrp=VSAC_4167751880_01A;trunk-context=siptrunking.bell.ca;tgrp=VSAC_4167751880_01A;trunk-context=siptrunking.bell.ca@110.10.98.98:5060>
Accept-Language: en
Alert-Info: <cid:internal@siptrunking.bell.ca>;avaya-cm-alert-type=internal
Min-SE: 1200
Session-Expires: 1200;refresher=uac
Content-Type: application/sdp
Content-Length: 255

P-Asserted-Identity: "Bell H323 x1881" <sip:4167751881@cust6-tor.vvac.bell.ca>
From: "Bell H323 x1881" <sip:4167751881@cust6-tor.vvac.bell.ca>;tag=0cc8e7be9a7e1195124fc3681000
P-Location: SM;origlocname="Belleville,Ont,Ca";termlocname="Belleville,Ont,Ca"
Max-Forwards: 66
Route: <sip:16139675258@220.20.237.205:5060;lr>
Authorization: Digest username="4167751880", realm="siptrunking.bell.ca",
nonce="BroadWorksXh20hxr6uTeiowp0BW", uri="sip:16139675258@siptrunking.bell.ca",
response="dd878bdd5984c17d55e65aa95fbbe886", algorithm=MD5,
cnonce="5968c562e648071ca047aa4fd181b4e2", qop=auth, nc=00000001, auth-params=sha1-credential

v=0
o=- 1336574904 1 IN IP4 110.10.98.98
s=-
c=IN IP4 110.10.98.98
b=AS:64
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 20184 RTP/AVP 0 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000

- 200OK/SDP response by Bell Canada:

SIP/2.0 200 OK
Via: SIP/2.0/UDP 110.10.98.98:5060;branch=z9hG4bKf3k97p304gm1jh0ce0o0
To: <sip:16139675258@siptrunking.bell.ca>;tag=SDs3m0e99-777692209-1336574483829
Call-ID: 0cc8e7be9a7e1196124fc3681000@cust6-tor.vvac.bell.ca
CSeq: 2 INVITE
From: "Bell H323 x1881" <sip:4167751881@cust6-tor.vvac.bell.ca>;tag=0cc8e7be9a7e1195124fc3681000
Supported:
Contact: <sip:16139675258@220.20.237.205:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: multipart/mixed,application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 181

v=0
o=BroadWorks 74981 1 IN IP4 220.20.237.205
s=-
c=IN IP4 220.20.237.205
t=0 0
m=audio 20026 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20

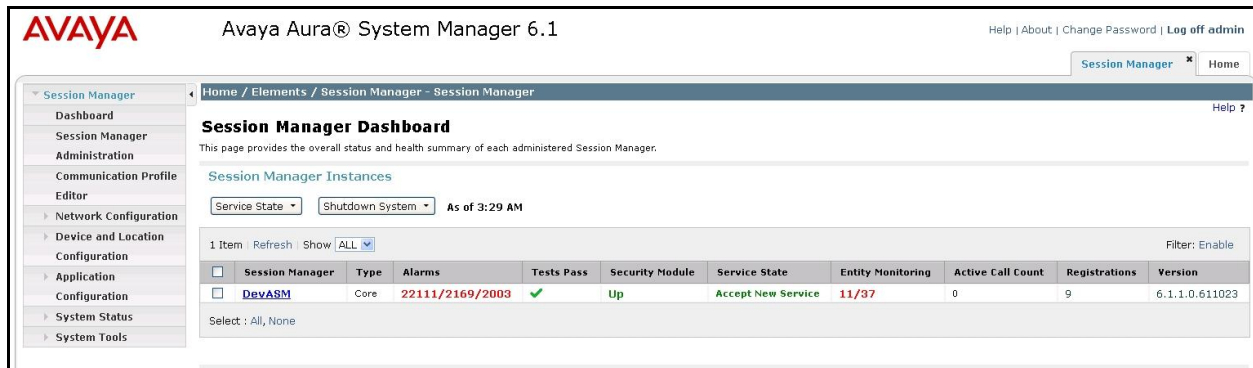
2. Communication Manager

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

- **status trunk** <trunk group number/channel number>. Displays signaling and media information for an active trunk channel

3. Session Manager

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



Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Home

Session Manager Dashboard

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

Session Manager Instances

Service State Shutdown System As of 3:29 AM

1 Item Refresh Show ALL Filter: Enable

	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/>	DevASM	Core	22111/2169/2003	✓	Up	Accept New Service	11/37	0	9	6.1.1.0.611023

Select : All, None

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Acme Packet Session Border Controller 6.2 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.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. Bell Canada SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Acme Packet Session Border Controller 6.2.

11. References

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

- [1]*Installing and Configuring Avaya Aura® System Platform*, Release 6.03, 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 one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.
- [9]*Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
- [10]*Administering Avaya one-X® Communicator*, April 2011.
- [11]*Using Avaya one-X® Communicator*, April 2011.
- [12]*Acme Packet Net-Net® EMS User Guide*, Release Version 4.1.
- [13]*RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [14]*RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [15]*RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [16]*RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

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

©2012 Avaya Inc. All Rights Reserved.

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

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