



Application Notes for Configuring Bell Canada SIP Trunking with Avaya Aura® Communication Manager Evolution Server Release 6.0.1, Avaya Aura® Session Manager Release 6.1, and Avaya Session Border Controller for Enterprise Release 4.0.5 – Issue 1.1

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, Avaya Session Border Controller For Enterprise 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager or Avaya Session Border Controller For Enterprise.

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

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

Table of Contents

1.	Introduction.....	4
2.	Test Scope and Results	5
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results	6
2.3.	Support.....	9
3.	Reference Configuration	10
4.	Equipment and Software Validated	13
5.	Configure Avaya Aura® Communication Manager	14
5.1.	Licensing and Capacity	14
5.2.	System Features	15
5.3.	IP Node Names	16
5.4.	Codecs.....	16
5.5.	IP Network Region	17
5.6.	Signaling Group	19
5.7.	Trunk Group.....	21
5.8.	Calling Party Information	25
5.9.	Outbound Routing.....	26
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	28
6.	Configure Avaya Aura® Session Manager	29
6.1.	System Manager Login and Navigation	30
6.2.	Specify SIP Domain.....	32
6.3.	Add Location	34
6.4.	Add Adaptation Module	35
6.5.	Add SIP Entities.....	38
6.6.	Add Entity Links.....	40
6.7.	Add Routing Policies	42
6.8.	Add Dial Patterns.....	43
6.9.	Add/View Session Manager	46
7.	Configure Avaya Session Border Controller for Enterprise	47
7.1.	Avaya Session Border Controller For Enterprise Login	48
7.2.	Global Profiles	50
7.2.1.	Uniform Resource Identifier (URI) Groups.....	51
7.2.2.	Routing Profiles	52
7.2.3.	Topology Hiding.....	54
7.2.4.	Server Interworking	56
7.2.5.	Signaling Manipulation.....	61
7.2.6.	Server Configuration.....	64
7.3.	Domain Policies	69
7.3.1.	Application Rules.....	69
7.3.2.	Media Rules	71
7.3.3.	Signaling Rules	73

7.3.4. Endpoint Policy Groups	76
7.3.5. Session Policy	77
7.4. Device Specific Settings	79
7.4.1. Network Management.....	80
7.4.2. Media Interface	81
7.4.3. Signaling Interface	82
7.4.4. End Point Flows - Server Flow	82
7.4.5. Session Flow	84
8. Bell Canada SIP Trunking Configuration.....	86
9. Verification and Troubleshooting	87
10. Conclusion	90
11. References	91

1. Introduction

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

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

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

2. Test Scope and Results

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

2.1. Interoperability Compliance Testing

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

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

- Incoming PSTN calls to various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phones.
- Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) were tested. 1XC also supports two signaling protocols (H.323 and SIP). Both protocols were tested.
- Various call types included: local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411), etc.
- G.729A Codec, G.711A and G.711MU Codec and proper codec negotiation.
- DTMF tone transmissions passed as out-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- Incoming and Outgoing fax over IP with codec G.711.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding with SIP Diversion method.
- EC500 mobility (extension to cellular).

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

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

- Inbound toll-free and outbound emergency calls (911) are supported but were not tested as part of the compliance testing.
- T.38 Faxing between the enterprise site and PSTN was not tested as part of the compliance test since Bell Canada currently does not support T.38 FoIP (Fax over IP) on its SIP Trunking Vendor Validation circuit.
- 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 was not tested with History-Info method. On Bell Canada SIP Trunk, it natively supports Diversion method; it also supports the History-Info header by converting it to Diversion header. Communication Manager has capability to support both methods but only Diversion was tested.

2.2. Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager, Session Manager and Avaya SBCE to connect to the Bell Canada SIP Trunking service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

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 have Avaya SBCE to normalize the calling number contained in the From header to remove the plus sign (see **Section 7.2.5**).

02. Off-net blind transfer by a SIP phone: Communication Manager SIP phone off-net blind transfers an inbound call back to PSTN. When Communication Manager sends REFER to complete the transferring after 200 OK received on the 2nd leg, the calling PSTN party does not hear the ringback tone. 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.

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

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

05. No matching codec: If the codec does not match any of the codec supported by Bell Canada in an outbound from enterprise to PSTN, Bell Canada responds with a “480 Temporary Unavailable”. The call is dropped as expected even when Bell Canada does not respond with a proper “488 Not Acceptable Here”. This is listed here just simply as an observation.

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

07. Calling CLID display for outbound call: In outbound call scenario, Communication Manager sends both calling CLID name and number to Bell Canada. In some cases, PSTN phone displays just calling CLID number and no calling CLID name. In some other cases, PSTN phone displays both calling CLID name and number. The calling CLID may be overridden by the intermediate service provider that routes the call through from Bell Canada to the endpoint.

08. Call display in inbound consultative call transfer to local extension: A Communication Manager SIP phone performs a consultative transfer of an inbound PSTN call to a local Communication Manager H.323 phone. The local H.323 phone displays the trunk-group name and TAC instead of the CLID of PSTN. This issue has very low user impact; it is listed here just simply as an observation.

09. Call display update in off-net call transfer scenario: Communication Manager off-net transfers an incoming call back to PSTN. After completing the transfer,

Communication Manager sends UPDATE with Remote-Party-Header to update the true connected CLID of PTSN parties. However, the CLID is not being updated. It depends on either Bell Canada or the intermediate service provider which routes the call from Bell Canada to the endpoint to support the display update.

10. The Call-ID for outbound call is not modified: In outbound call, Bell Canada expects the Call-ID sent from Communication Manager with “@cust6-tor.vsac.bell.ca” to be appended. With a SigMa script configured for the Call-ID modification, the outbound call works, but the inbound fails. Even though Bell Canada requires the Call-ID to be sent in specific format, but it should not be changed by Avaya SBCE. Changing the Call-ID is not recommended. It will cause the inbound call to fail. There is no resolution currently available at this time. The compliance test is conducted without Call-ID modification; the inbound and outbound calls appear to work properly.

11. Session Flow on Avaya SBCE does not apply to outbound call: The Session Flow is applied to the 1st INVITE from enterprise to Bell Canada. However, it does not apply to the reINVITE responding to 401 Digest Authentication from Bell Canada. As a result, the voice codec may be different than the definition in Session Policy profile configured in **Section 7.3.5**. There is no resolution currently available at this time.

12. Perform an “Application Restart” on Avaya SBCE causes SigmaScript and Authentication to stop working. There is no resolution currently available at this time. If the SigMa script and Authentication do not work after an “Application Restart”, please contact Avaya for support on Avaya SBCE by telephone numbers +1-866-861-3113 toll free or +1-214-269-2424. **Notes:** the password for Authentication should not contain special character e.g. “!”. It is a limitation on Avaya SBCE and there is currently no available resolution at this time.

13. Avaya SBCE does not forward BYE properly to Communication Manager in conference call scenario. A Communication Manager extension conferences an inbound call from PSTN to another local extension, then hangs up. The remaining call is kept on-going between PSTN and the 2nd extension. Then the PSTN hangs up. Avaya SBCE does not forward the BYE properly to Communication Manager to terminate the call. It forwards the BYE to another Server Configuration. Communication Manager keeps the 2nd extension active until the session timer expired, then it is able to terminate the call successfully. This issue is resolved by applying patch *ipcs-bin-mvista_debug_20120413150346-2.i386.rpm* to Avaya SBCE, To get the patch, please contact Avaya for support on Avaya SBCE by telephone numbers +1-866-861-3113 toll free or +1-214-269-2424. Notes: Avaya SBCE software version later than 4.0.5.Q02 will include this patch. For SIP Trunk configuration between Session Manager and Avaya SBCE with a custom port other than well-known 5060, the IP address of Communication Manager needs to be fined under **URI-Group**. Please refer to **Section 7.2.1** for **URI-Group** configuration.

2.3. Support

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

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

3. Reference Configuration

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

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

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

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

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

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

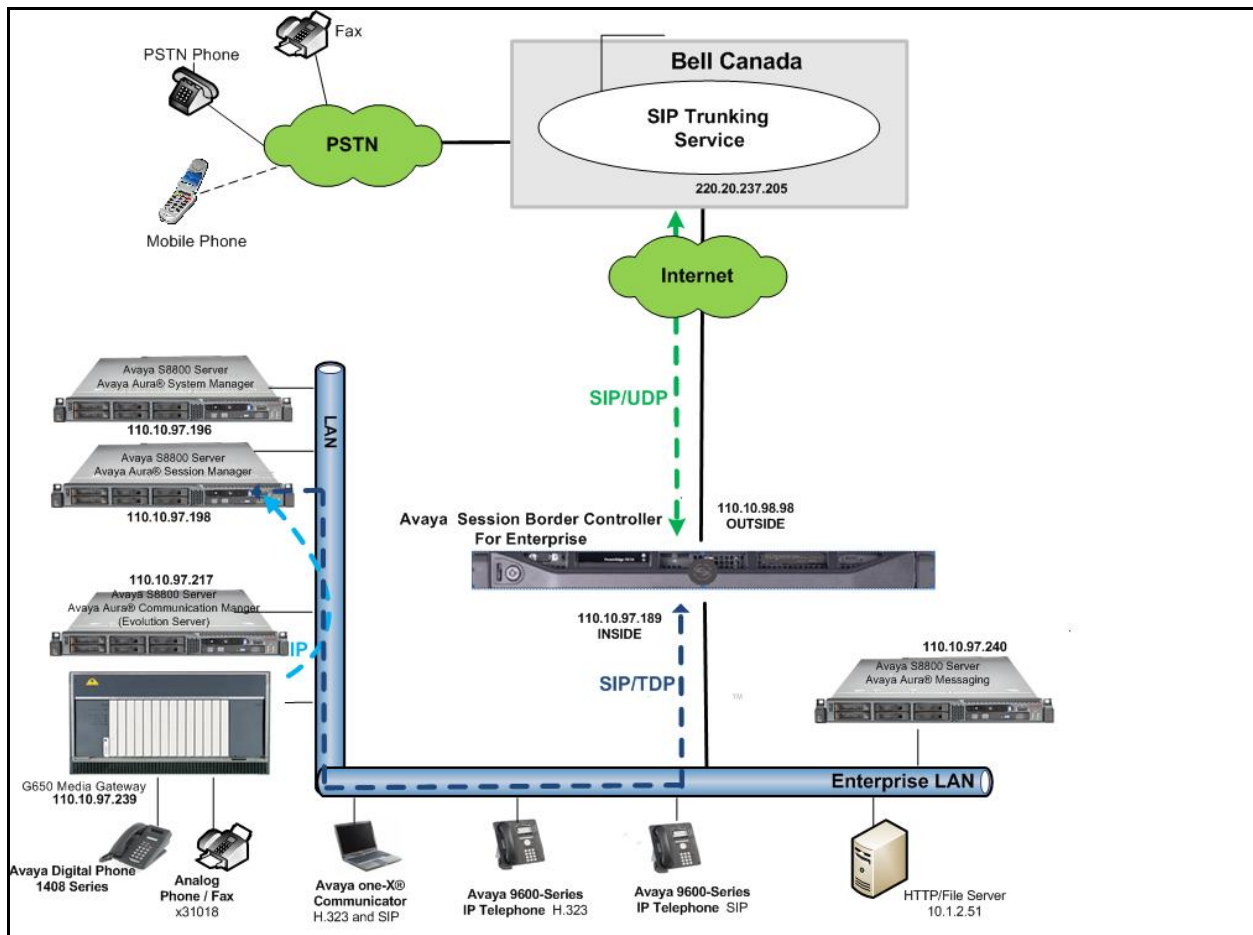


Figure 1: Avaya IP Telephony Network Connecting to Bell Canada SIP Trunking Service

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

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

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. The Session Manager once again used the configured dial patterns (or regular expressions) and

routing policies to determine the route to the Avaya SBCE for egress to the Bell Canada network.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on Avaya S8800 Server	6.0.1 (R016x.00.1.510.1-18621)
Avaya G650 Media Gateway IPSI TN2312BP Control-LAN TN799DP Digital Line TN2224 Analog Line TN746B	HW06 FW043 HW01 FW026 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 Session Border Controller For Enterprise	4.0.5 Q2
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
Bell Canada SIP Trunking Solution Components	
Component	Release
Acme Packet Net-Net 4250 SBC	Firmware SC6.2.0 MR-4 Patch 1 (Build 718)
Broadsoft SoftSwitch	Rel16
Legacy Nortel CS2K Media Gateway	SN10 PVG/IW-SPM

Table 1: Equipment and Software Tested

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

5. Configure 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 signaling traffic to the enterprise from Bell Canada (for inbound calls to the enterprise from the PSTN); similarly a separate SIP trunk is created for carrying signaling traffic to the network from the enterprise (for outbound calls to the PSTN from the enterprise).

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

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

5.1. Licensing and Capacity

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

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

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

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

5.2. System Features

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

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

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

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

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

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

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

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the 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	::	

Notes: 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 was configured to work with G450 Media Gateway.

5.4. Codecs

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

change ip-codec-set 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.711A	n	2 20
3: G.729	n	2 20
4:		
5:		

Bell Canada only supports G.711 faxing in this compliance test. The T.38 faxing is not currently supported. Communication Manager is not recommended for G.711 faxing. Communication Manager, however, will only support G.711 faxing in best effort, it treats the fax call like a regular voice call using codec G.711.

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 for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, **ip-network-region 3** was created for the service provider trunks. 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 shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region. Notes that Session Manager adaptation configuration (**Section 6.4**) is used to convert this shared domain name to the specific CPE domain as assigned by Bell Canada and expected by the Bell Canada network.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```

change ip-network-region 3
                                     IP NETWORK REGION
                                     Page 1 of 20

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
                   UDP Port Min: 2048      IP Audio Hairpinning? n
                   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5

```

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

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

For the compliance test, devices with IP addresses in the 110.10.97.0/24 subnet are assigned to network region 3. These include Communication Manager, Session Manager and Avaya SBCE that were set up for shared test environment. IP telephones used for the compliance test, including both the Avaya 9600 IP Telephones and the Avaya one-X® Communicator soft phones, are assigned to network region 3 with IP address in the 110.10.98.0/24 subnet. In production environments, different sites will typically be on different networks, and ranges of IP

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

change ip-network-map				Page 1 of 63	
IP ADDRESS MAPPING					
IP Address	Subnet Bits	Network Region	VLAN	Emergency Location Ext	
FROM: 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 2 signaling groups between Communication Manager and the Session Manager for use by inbound calls from the service provider network and outgoing calls from the enterprise. The signaling group used for inbound calls from the service provider is shown below. For the compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between Communication Manager and Session Manager. The transport method used between the Session Manager and Avaya SBCE is specified as TCP in **Section 6.6**. Lastly, the transport method between the Avaya SBCE and Bell Canada is UDP. This is defined in **Section 7.2.6.1** when the service provider name is selected.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so the Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5060** (the well-known port value for TCP is 5060).
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **Session Manager** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **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 **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **DTMF over IP** field to **rtp-payload**. This setting enables Communication Manager to send DTMF transmissions using RFC 2833.
- Verify that the **Initial IP-IP Direct Media** is set to the same value as the signaling group used for the enterprise site. The default setting for this field is **n**. See the **Media Format** bullet item in **Section 2.2** for more information about this setting.
- Change default setting of **6** for **Alternate Route Timer (sec)** to **12**. This allows more time for outbound PSTN calls to complete through the 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 the PSTN was similarly configured except that the **Far-end Domain** is set to “**siptrunking.bell.ca**”, this domain is known to the service provider network domain as provided by Bell Canada. For the compliance test, signaling group 4 was 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 2 signaling groups created in **Section 5.6**. For the compliance test, trunk group 3 was configured for incoming call and trunk group 4 was 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 the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```

add trunk-group 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 was 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** was set to **private** and the **Numbering Format** in the route pattern 4 was set to **unk-unk** (see **Section 5.9**).

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

add trunk-group 3		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
UI Treatment: service-provider		
Replace Restricted Numbers? y		
Replace Unavailable Numbers? y		
Show ANSWERED BY on Display? y		

On **Page 4**, set the **Network Call Redirection** field to **n**. This setting disables the use of the SIP REFER message to transfer an incoming call to a vector number back to PSTN as this method is not supported by Bell Canada. Notes: the outgoing trunk group 4 in the later discussion will also have **Network Call Redirection** set to **n**, this setting is to use reINVITE to off-net transfer an incoming call back to PSTN. For more information, please refer to **Section 2.2**, observation #03 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 of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

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

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

add trunk-group 3	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	

For trunk group 4 configuration, the screen below shows **Page 1**, the trunk group for outgoing calls from the enterprise. The **Direction** was set to “outgoing” and **Signaling Group** was set to 4.

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

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

Notes: When Network Call Redirection is set to “n”, Communication Manager will use reINVITE for off-net call transfer. This setting is to work around the issue “off-net blind transfer by a SIP phone” as specified in **Section 2.2**, observation #02 and #03.

```
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 was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. 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 188 will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 0                             Page 1 of 2
                                                    NUMBERING - PRIVATE FORMAT

Ext  Ext      Trk      Private      Total
Len  Code      Grp(s)   Prefix      Len
4   188       3-4       416775     10      Total Administered: 1
                                           Maximum Entries: 540
```

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

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp (s)	Prefix	CPN	
				Len	
4	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 via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1** as a feature access code (**fac**).

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
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 and route pattern 4 for vector call redirection which contains the SIP trunk to the service provider (as defined next).

```

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

    Dialed      Total      Route      Call      Node      ANI
    String      Min      Max      Pattern      Type      Num      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 parameters for the service provider trunk route pattern 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 was used.
- **FRL:** Set the Facility Restriction Level (FRL) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk: 1** The prefix mark (Pfx Mrk) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits

are sent to the service provider for the long distance North American Numbering Plan (NANP) numbers. All HNP 10 digit numbers are left unchanged.

- **Numbering Format: unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR: next**

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

5.10. Saving Communication Manager Configuration Changes

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

6. Configure Avaya Aura® Session Manager

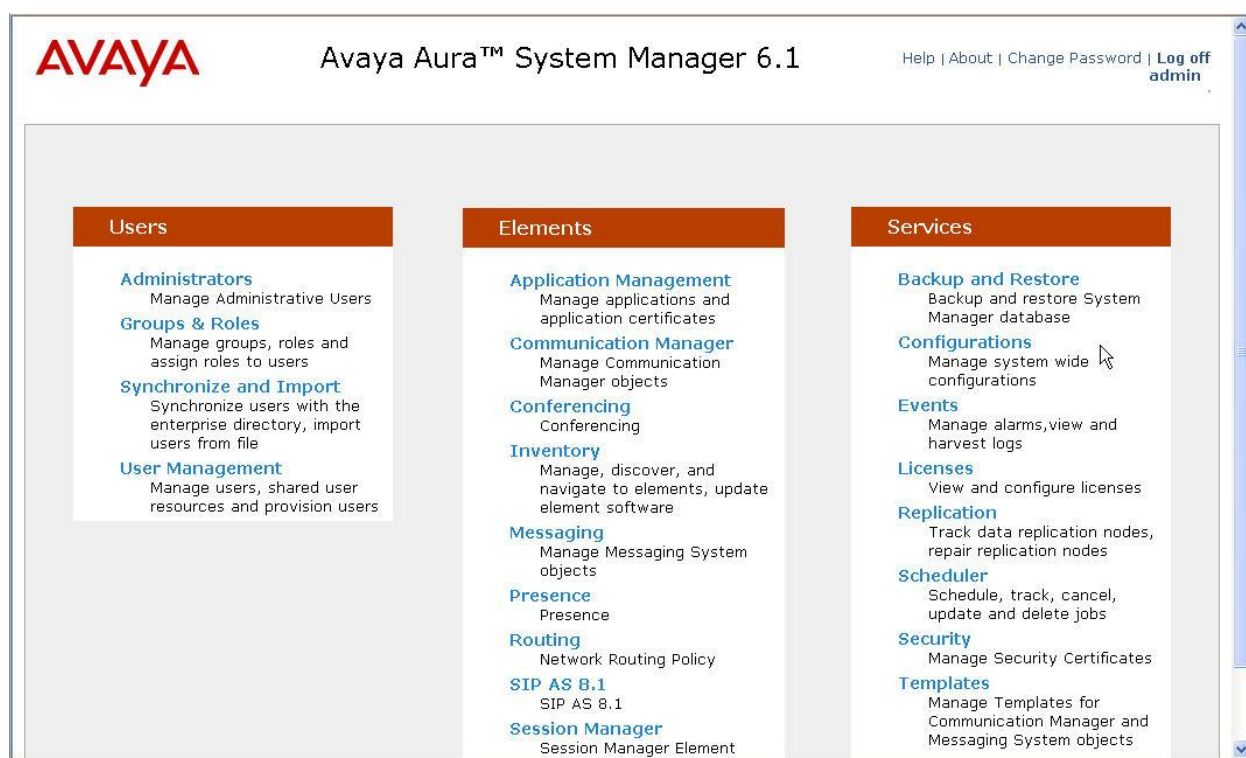
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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 Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

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

6.1. System Manager Login and Navigation

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



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

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

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

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

Routing x Home

Home /Elements / Routing- Introduction to Network Routing Policy

Introduction to Network Routing Policy Help ?

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

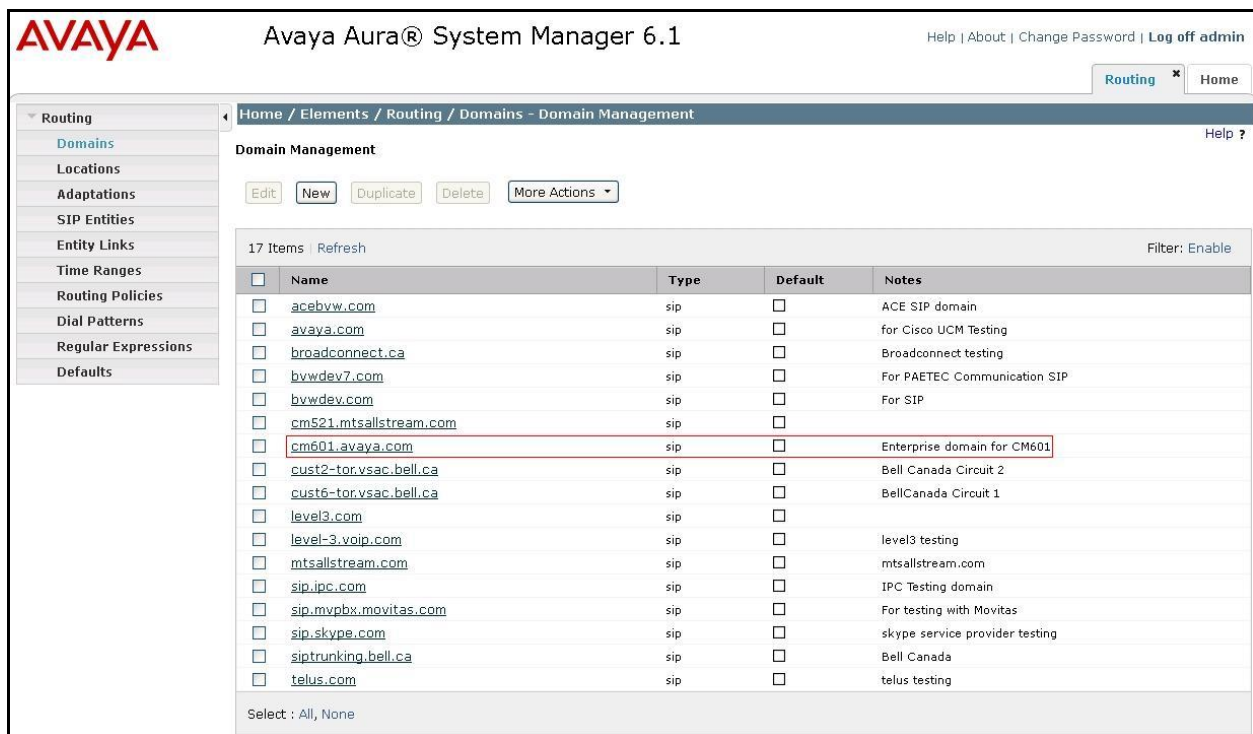
The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"

6.2. Specify SIP Domain

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

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



The screenshot shows the Avaya Aura® System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for Help, About, Change Password, and Log off admin. The main navigation menu on the left lists various configuration areas, with "Routing" expanded to show "Domains". The "Domain Management" page is displayed, showing a list of 17 SIP domains. The domain "cm601.avaya.com" is highlighted with a red border. The table below lists the domains:

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
bvwdev7.com	sip	<input type="checkbox"/>	For PAETEC Communication SIP
bvwdev.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-torvsac.bell.ca	sip	<input type="checkbox"/>	Bell Canada Circuit 2
cust6-torvsac.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

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 network, this domain can appear 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 x Home

Home / Elements / Routing / Domains - Domain Management

Domain Management

Edit New Duplicate Delete More Actions

17 Items Refresh Filter: Enable

Name	Type	Default	Notes
<input type="checkbox"/> acebyvw.com	sip	<input type="checkbox"/>	ACE SIP domain
<input type="checkbox"/> avaya.com	sip	<input type="checkbox"/>	for Cisco UCM Testing
<input type="checkbox"/> broadconnect.ca	sip	<input type="checkbox"/>	Broadconnect testing
<input type="checkbox"/> bywdev7.com	sip	<input type="checkbox"/>	For PAETEC Communication SIP
<input type="checkbox"/> bywdev.com	sip	<input type="checkbox"/>	For SIP
<input type="checkbox"/> cm521.mtsallstream.com	sip	<input type="checkbox"/>	
<input type="checkbox"/> cm601.avaya.com	sip	<input type="checkbox"/>	Enterprise domain for CM601
<input type="checkbox"/> cust2-tor.vtac.bell.ca	sip	<input type="checkbox"/>	Bell Canada Circuit 2
<input type="checkbox"/> cust6-tor.vtac.bell.ca	sip	<input type="checkbox"/>	BellCanada Circuit 1
<input type="checkbox"/> level3.com	sip	<input type="checkbox"/>	
<input type="checkbox"/> level-3.voip.com	sip	<input type="checkbox"/>	level3 testing
<input type="checkbox"/> mtsallstream.com	sip	<input type="checkbox"/>	mtsallstream.com
<input type="checkbox"/> sip.ipc.com	sip	<input type="checkbox"/>	IPC Testing domain
<input type="checkbox"/> sip.mvpx.movitas.com	sip	<input type="checkbox"/>	For testing with Movitas
<input type="checkbox"/> sip.skype.com	sip	<input type="checkbox"/>	skype service provider testing
<input type="checkbox"/> siptrunking.bell.ca	sip	<input type="checkbox"/>	Bell Canada
<input type="checkbox"/> 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 x Home

Home / Elements / Routing / Domains - Domain Management

Domain Management

Edit New Duplicate Delete More Actions

17 Items Refresh Filter: Enable

Name	Type	Default	Notes
<input type="checkbox"/> acebyvw.com	sip	<input type="checkbox"/>	ACE SIP domain
<input type="checkbox"/> avaya.com	sip	<input type="checkbox"/>	for Cisco UCM Testing
<input type="checkbox"/> broadconnect.ca	sip	<input type="checkbox"/>	Broadconnect testing
<input type="checkbox"/> bywdev7.com	sip	<input type="checkbox"/>	For PAETEC Communication SIP
<input type="checkbox"/> bywdev.com	sip	<input type="checkbox"/>	For SIP
<input type="checkbox"/> cm521.mtsallstream.com	sip	<input type="checkbox"/>	
<input type="checkbox"/> cm601.avaya.com	sip	<input type="checkbox"/>	Enterprise domain for CM601
<input type="checkbox"/> cust2-tor.vtac.bell.ca	sip	<input type="checkbox"/>	Bell Canada Circuit 2
<input type="checkbox"/> cust6-tor.vtac.bell.ca	sip	<input type="checkbox"/>	BellCanada Circuit 1
<input type="checkbox"/> level3.com	sip	<input type="checkbox"/>	
<input type="checkbox"/> level-3.voip.com	sip	<input type="checkbox"/>	level3 testing
<input type="checkbox"/> mtsallstream.com	sip	<input type="checkbox"/>	mtsallstream.com
<input type="checkbox"/> sip.ipc.com	sip	<input type="checkbox"/>	IPC Testing domain
<input type="checkbox"/> sip.mvpx.movitas.com	sip	<input type="checkbox"/>	For testing with Movitas
<input type="checkbox"/> sip.skype.com	sip	<input type="checkbox"/>	skype service provider testing
<input type="checkbox"/> siptrunking.bell.ca	sip	<input type="checkbox"/>	Bell Canada
<input type="checkbox"/> 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 2nd screen below), click **Add** and enter the following values:

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

Displayed below are the screenshot for **Belleville,Ont,Ca** location, which includes all equipment on the **110.10.x.x** subnet including Communication Manager, Session Manager and Avaya SBCE. 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'. It features a 'Location Details' section with a 'Commit' button and a 'Help ?' link. Below this is a 'General' section with fields for 'Name' (set to 'Belleville,Ont,Ca') and 'Notes' (set to '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 a 'Default Audio Bandwidth' of '80 Kbit/sec'. The 'Location Pattern' section includes an 'Add' button and a table with one entry: 'IP Address Pattern' with the value '110.10.*.*' and an empty 'Notes' field. The table has a 'Filter: Enable' option and a 'Select: All, None' dropdown. At the bottom, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

IP Address Pattern	Notes
* 110.10.*.*	

6.4. Add Adaptation Module

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

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

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

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left sidebar shows a navigation menu with 'Routing' selected. The main content area is titled 'Home / Elements / Routing / Adaptations - Adaptations'. Below the title, there are buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. A table lists 12 items, with columns for 'Name', 'Module name', 'Egress URI Parameters', and 'Notes'. The first two items, 'BC Avaya-SBCE' and 'BC CM-ES', are highlighted with red boxes. The table also includes a 'Filter: Enable' dropdown and a 'Select: All, None' option at the bottom.

Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/> BC Avaya-SBCE	DigitConversionAdapter osrcd=cust6-tor.vsac.bell.ca odstd=siptrunking.bell.ca fromto=true		
<input type="checkbox"/> BC CM-ES	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com fromto=true		
<input type="checkbox"/> ChangeDomainName	IPAdapter osrcd=sip.ipc.com odstd=sip.ipc.com		
<input type="checkbox"/> CS1K75Bottom	DigitConversionAdapter		
<input type="checkbox"/> CS1K Adaptation	CS1000Adapter		CS1000 Adapter
<input type="checkbox"/> Diversion for Level 3	DiversionTypeAdapter odstd=135.10.98.104 osrcd=4.55.35.85 MIME=no		Outbound Diversion for Level3
<input type="checkbox"/> Movitas	number_2_text		
<input type="checkbox"/> MSUM2010	DigitConversionAdapter 131.107.5.62		
<input type="checkbox"/> Paetec Diversion Header	DiversionTypeAdapter		
<input type="checkbox"/> skypeadap	osrcd=135.10.97.198 odstd=sip.skype.com		
<input type="checkbox"/> Star Telecom	DigitConversionAdapter osrcd=bvwddev7.com odstd=bvwddev7.com iosrcd=bvwddev7.com		
<input type="checkbox"/> StarTelecom2	DigitConversionAdapter iodstd=135.10.97.184		

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

The **BC Avaya SBCE** adaptation will later be assigned to the Avaya-SBCE SIP Entity. This adaptation uses the **DigitConversionAdapter** and specifies three parameters used to adapt the FQDN to the domains expected by the Bell Canada network 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 was used to adapt the domain **avaya.com** from Communication Manager to **cust6-tor.vsat.bell.ca** and **siptrunking.bell.ca** which are the domains known to Bell Canada.

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

The screenshot shows the Avaya Aura System Manager 6.1 web 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 'Adaptation Details' and shows the configuration for the 'BC Avaya-SBCE' adaptation. The 'General' tab is selected. The configuration fields are: 'Adaptation name' (BC Avaya-SBCE), 'Module name' (DigitConversionAdapter), and 'Module parameter' (osrcd=cust6-tor.vsat.bell.ca odstd). There are also empty fields for 'Egress URI Parameters' and 'Notes'. The interface includes a 'Commit' button and a 'Cancel' button.

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 to be overwritten with **avaya.com**. For example, for inbound PSTN calls from Bell Canada to Avaya CPE to Bell Canada, the PAI header will contain “avaya.com” as expected by Communication Manager.
- **odstd= avaya.com.** This configuration enables the outbound destination domain to be overwritten with **avaya.com**. For example, for inbound PSTN calls from Bell Canada to Avaya CPE, the Request-URI will contain **avaya.com** as expected by Communication Manager.
- **fromto=true.** With this configuration, for an outbound call to 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**.

Scrolling down, the following screen shows a portion of the **BC CM-ES** adaptation that can be used to convert digits between the extension numbers used on Communication Manager and the 10 digit DID numbers assigned by Bell Canada. Since this adaptation will be applied to the Communication Manager SIP Entity later on, the settings for **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. In general, digit conversion such as this, that converts a Communication Manager extension (e.g., 188X) to a corresponding LDN or DID number known to the PSTN (e.g., 416775188X), can be performed in Communication Manager

(e.g., using public unknown numbering and incoming call handling treatment for the Communication Manager trunk group) or in Session Manager as shown below.

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: bdstd=avaya.com osrcd=avaya.c

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. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. For an outbound call, if extension 31012 dials the PSTN, and if Communication Manager sends the extension 188X to Session Manager as the calling number, Session Manager would convert the calling number to 416777188X. Alternatively, the Communication Manager private-numbering form could have an entry to convert 31012 to 4167771111 before sending the call on the trunk group to Session Manager (as shown in **Section 5.7**).

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 Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **Communication Manager** for Communication Manager and **Other** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation** name created in **Section 6.4** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

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

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". A breadcrumb trail shows "Home / Elements / Routing / SIP Entities - SIP Entity Details". The left sidebar contains a navigation menu with "Routing" selected, and sub-items: "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 has a "General" tab selected. The form fields are as follows: "Name" (text box with "DevASM"), "FQDN or IP Address" (text box with "110.10.97.198"), "Type" (dropdown menu with "Session Manager" selected), "Notes" (text box with "For Session Manager"), "Location" (dropdown menu with "Belleville, Ont, Ca" selected), "Outbound Proxy" (dropdown menu), "Time Zone" (dropdown menu with "America/Toronto" selected), and "Credential name" (text box). At the bottom, there is a "SIP Link Monitoring" section with a dropdown menu set to "Use Session Manager Configuration". In the top right corner of the form area, there are "Commit" and "Cancel" buttons, and a "Help ?" link.

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 Avaya SBCE.

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

The screenshot shows the 'SIP Entity Details' page in the Avaya Aura® System Manager 6.1. The left navigation pane is expanded to 'Routing' > 'SIP Entities'. The main content area is titled 'SIP Entity Details' and 'General'. The configuration fields are as follows:

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

The following screen shows the addition of the Avaya SBCE SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). **Link Monitoring Enabled** was selected for **SIP Link Monitoring**. These time settings should be adjusted or left at their default values per customer needs and requirements.

The screenshot shows the 'SIP Entity Details' page in the Avaya Aura® System Manager 6.1. The left navigation pane is expanded to 'Routing' > 'SIP Entities'. The main content area is titled 'SIP Entity Details' and 'General'. The configuration fields are as follows:

- Name:** Avaya SBCE
- FQDN or IP Address:** 110.10.97.189
- Type:** Other
- Notes:** Avaya SBCE
- Adaptation:** BC Avaya SBCE
- Location:** Belleville,Ont,Ca
- Time Zone:** America/New_York
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none
- SIP Link Monitoring:** Link Monitoring Enabled

6.6. Add Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **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 Avaya SBCE, select the Avaya SBCE SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Trusted:** Check this box. Notes: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

Entity Link to Communication Manager:

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 (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Entity Links - Entity Links'. It features a 'Commit' button and a 'Cancel' button. Below this is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The table contains one row with the following data: Name: DevASM_DevCM217, SIP Entity 1: DevASM, Protocol: TCP, Port: 5060, SIP Entity 2: DevCM217, Port: 5060, Trusted: checked, Notes: . At the bottom of the table, there is a red asterisk and the text '* Input Required'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* DevASM_DevCM217	* DevASM	TCP	* 5060	* DevCM217	* 5060	<input checked="" type="checkbox"/>	

Entity Link to Avaya SBCE:

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 (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Entity Links - Entity Links'. It features a 'Commit' button and a 'Cancel' button. Below this is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The table contains one row with the following data: Name: DevASM_Avaya-SBC, SIP Entity 1: DevASM, Protocol: TCP, Port: 5060, SIP Entity 2: Avaya SBCE, Port: 5060, Trusted: checked, Notes: . At the bottom of the table, there is a red asterisk and the text '* Input Required'.

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

6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. 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.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is expanded to 'Routing', and the 'Routing Policies' link is selected. The main content area displays the 'Routing Policy Details' for a policy named 'BellCanada_To_CM601'. The 'General' section is active, showing the policy name, a disabled checkbox, and notes. The 'SIP Entity as Destination' section shows a table with one entry: 'DevCM217' with FQDN '110.10.97.217' and Type 'CM'.

Name	FQDN or IP Address	Type	Notes
DevCM217	110.10.97.217	CM	

The following screens show the Routing Policies **CM601_To_BellCanada** for Avaya SBCE.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is expanded to 'Routing', and the 'Routing Policies' link is selected. The main content area displays the 'Routing Policy Details' for a policy named 'CM601_To_BellCanada'. The 'General' section is active, showing the policy name, a disabled checkbox, and notes. The 'SIP Entity as Destination' section shows a table with one entry: 'Avaya SBCE' with FQDN '110.10.97.189' and Type 'Other'.

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	110.10.97.189	Other	Avaya SBCE

6.8. Add Dial Patterns

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

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

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

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

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

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

The first example shows that 11-digit dialed numbers that begin with **1** and have 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

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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

Dial Pattern Details

Commit

Cancel

General

* Pattern:

1

* Min:

11

* Max:

11

Emergency Call:

☐

SIP Domain:

siptrunking.bell.ca

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		CM601_To_BellCanada	0	<input type="checkbox"/>	Avaya SBCE	CM601_To_BellCanada

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

Refresh

Filter: Enable

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

* Input Required

Commit

Cancel

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 from Bell Canada.

Dial Pattern Details

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

General

* Pattern: #16

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: cust6-tor.vtac.bell.ca

Notes: BellCanada_To_CM601

Originating Locations and Routing Policies

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

1 Item [Refresh](#)

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	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 was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

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

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

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top header shows the Avaya logo and the title 'Avaya Aura® System Manager 6.1'. On the right, there are links for 'Help | About | Change Password | 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 '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 selected, showing the following fields: 'SIP Entity Name' (DevASM), 'Description' (empty), '*Management Access Point Host Name/IP' (110.10.97.197), and '*Direct Routing to Endpoints' (Enable).

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

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

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

The screenshot shows a configuration window titled "Security Module" with a dropdown arrow. It contains several input fields with the following values:

Field	Value
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 Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller For Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Reference [12]** and **[13]**.

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

Trunk server configuration elements for service provider Bell Canada:

- Global Profiles:
 - o URI Groups.
 - o Routing.
 - o Topology Hiding.
 - o Server Interworking.
 - o Signaling Manipulation.
 - o Server Configuration.
- Domain Policies
 - o Application Rules.

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


Call server configuration elements for enterprise Session Manager:

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

7.1. Avaya Session Border Controller For Enterprise Login

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

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

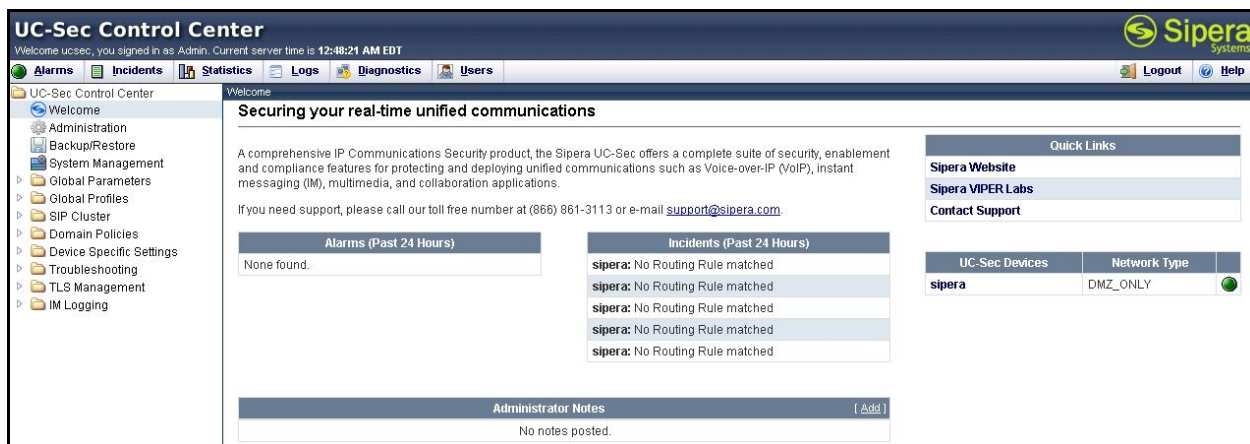


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

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

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

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



UC-Sec Devices	Network Type	Status
sipera	DMZ_ONLY	

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



The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

System Information: sipera

Network Configuration

General Settings

Appliance Name	sipera
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	NO
Secure Channel Mode	NONE
Two Bypass Mode	NO

Network Settings

IP	Public IP	Netmask	Gateway	Interface
110.10.97.189	110.10.97.189	255.255.255.192	110.10.97.129	A1
110.10.98.98	110.10.98.98	255.255.255.224	110.10.98.97	B1
110.10.98.112	110.10.98.112	255.255.255.224	110.10.98.97	B1

DNS Configuration

Primary DNS	110.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	110.10.97.189

Management IP(s)

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

7.2. Global Profiles

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

TD; Reviewed:
SPOC 11/26/2012

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

50 of 92
BCSipTrkCMSMSBC

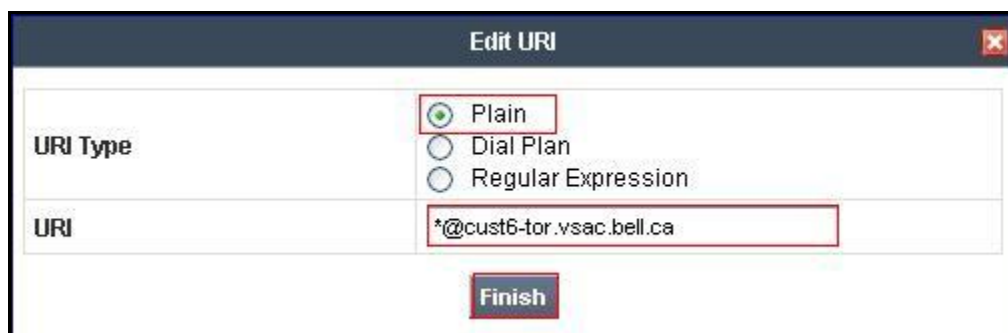
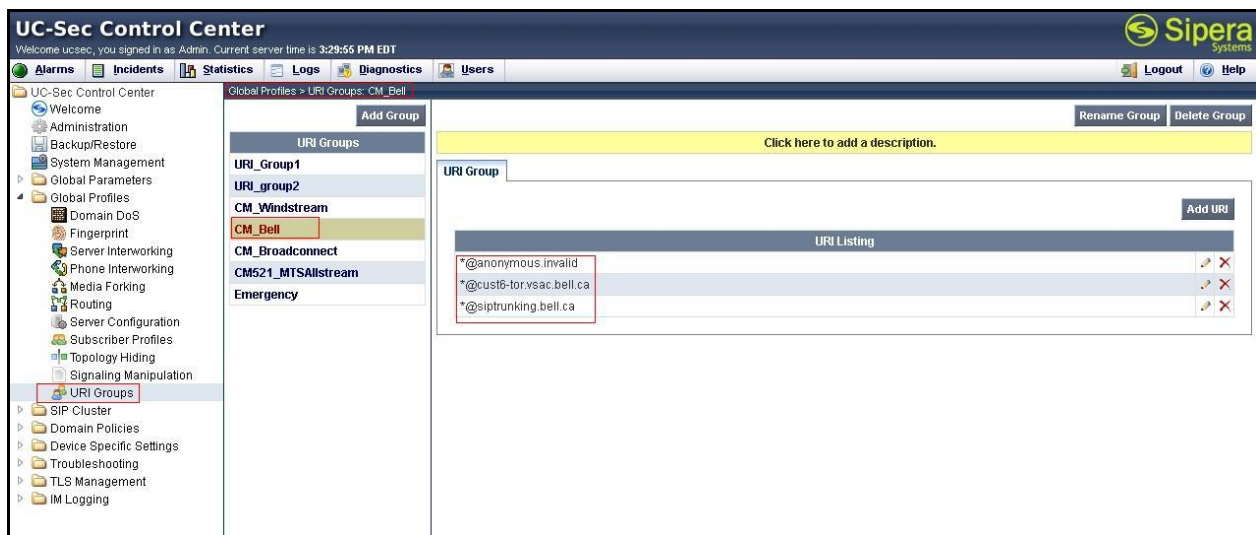
7.2.1. Uniform Resource Identifier (URI) Groups

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

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

In this compliance test, a **URI Group** named “CM_Bell” was added with plain URI type and consists of three domains [*@anonymous.invalid](#), [*@cust6-tor.vsac.bell.ca](#), and [*@siptrunking.bell.ca](#). This group was used to match the From and To headers in a SIP call dialogs received from Session Manager and Bell Canada SIP Trunk. If there is a match, then the Avaya SBCE applies the appropriate **Routing Profile** and **Server Flow** to route the inbound and outbound call to the right destinations. The **Routing Profile** and **Server Flow** are configured in next steps.

The screenshots below illustrate the **Global Profiles → URI Groups: CM_Bell**.



7.2.2. Routing Profiles

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

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

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

7.2.2.1 Routing Profile for Bell Canada

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

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows the navigation menu with 'Routing' highlighted. The main content area is titled 'Global Profiles > Routing: To_Bell'. It includes a list of routing profiles on the left, with 'To_Bell' selected. The right pane shows the configuration for 'To_Bell', including a description field and a table of routing rules. The table has columns for Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, and Outgoing Transport. A single rule is shown with Priority 1, URI Group CM_Bell, Next Hop Server 1 220.20.237.205, and Outgoing Transport UDP.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	CM_Bell	220.20.237.205	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

Edit Routing Rule
✕

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

Next Hop Routing

URI Group	CM_Bell	
Next Hop Server 1	220.20.237.205	IP, IP:Port, Domain, or Domain:Port
Next Hop Server 2		IP, IP:Port, Domain, or Domain:Port

☒ Routing Priority based on Next Hop Server
☐ Use Next Hop for In Dialog Messages
☐ Ignore Route Header for Messages Outside Dialog

☐ NAPTR ☐ SRV

Outgoing Transport
 ☐ TLS
 ☐ TCP
 ☒ UDP

Finish

7.2.2.2 Routing Profile for Session Manager

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

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 5:37:40 PM EDT

Alarms **Incidents** **Statistics** **Logs** **Diagnostics** **Users**

[Logout](#) [Help](#)

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- Domain DoS
- Fingerprint
- Server Interworking
- Phone Interworking
- Media Forking
- Routing
- Server Configuration
- Subscriber Profiles
- Topology Hiding
- Signaling Manipulation
- URI Groups
- SIP Cluster
- Domain Policies
- Device Specific Settings
- Troubleshooting
- TLS Management
- IM Logging

Global Profiles > Routing: To_CM

Add Profile

Routing Profiles
 default
To_Bell
To_CM
 SM_To_Windstream
 Windstream_To_SM
 CS1K_Car3_To_PAETEC
 PAETEC_To_CS1K_CAR3
 SM_To_PAETEC
 PAETEC_To_SM
 To_SM_fr_BroadConnect
 To_BroadConnect
 To_MTSAllstream
 To_CM521

[Rename Profile](#) [Clone Profile](#) [Delete Profile](#)

Click here to add a description.

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	CM_Bell	110.10.97.198	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

7.2.3. Topology Hiding

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

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

In this compliance test, two **Topology Hiding** profiles were created, named **To_Bell** and **To_CM**.

7.2.3.1 Topology Hiding Profile for Bell Canada

Profile **To_Bell** is defined to mask the enterprise SIP domain **cust6-tor.vsac.bell.ca** in Request-URI, From, To headers to **siptrunking.bell.ca** (the domain name defined here for Request-URI, From and To is to meet the SIP specification require by Bell Canada); delete Record-Route and Via entries added by Session Manager and replace internal IP addresses in SDP by external IP address known to Bell Canada. It secures the enterprise network topology and also meets the SIP requirement from service provider.

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

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 1:38:57 AM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Topology Hiding: To_Bell

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
 - Global Profiles
 - Domain DoS
 - Fingerprint
 - Server Interworking
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration
 - Subscriber Profiles
 - Topology Hiding**
 - Signaling Manipulation
 - URI Groups
 - SIP Cluster
 - Domain Policies
 - Device Specific Settings
 - Troubleshooting
 - TLS Management
 - IM Logging

Topology/Hiding Profiles

default

cisco_th_profile

To_CM

To_Bell

Windstream

CS1K_Car3

PAETEC

SM

To_SM_fr_BroadC

To_BroadConnect

To_CM521

To_MTSAllstream

Add Profile

Rename Profile Clone Profile Delete Profile

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	siptrunking.bell.ca
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	cust6-tor.vsac.bell.ca
To	IP/Domain	Overwrite	siptrunking.bell.ca
Via	IP/Domain	Auto	---

Edit

Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Overwrite	siptrunking.bell.ca	✗
SDP	IP/Domain	Auto		✗
Record-Route	IP/Domain	Auto		✗
From	IP/Domain	Overwrite	cust6-tor.vsac.bell.ca	✗
To	IP/Domain	Overwrite	siptrunking.bell.ca	✗
Via	IP/Domain	Auto		✗

Finish

7.2.3.2 Topology Hiding Profile for Session Manager

Profile **To_CM** is also needed to mask Bell Canada SIP domain **siptrunking.bell.ca** in Request-URI, From, To headers to **cust6-tor.vsac.bell.ca**, delete Record-Route and Via entries added by Bell Canada and replace external IP addresses in SDP by internal IP address known to Session Manager.

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

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 1:49:10 AM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
 - Domain DoS
 - Fingerprint
 - Server Interworking
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration
 - Subscriber Profiles
 - Topology Hiding**
 - Signaling Manipulation
 - URI Groups
 - SIP Cluster
 - Domain Policies
 - Device Specific Settings
 - Troubleshooting
 - TLS Management
 - IM Logging

Global Profiles > Topology Hiding: To_CM

Add Profile

Topology Hiding Profiles

- default
- cisco_th_profile
- To_CM**
- To_Bell
- Windstream
- CS1K_Car3
- PAETEC
- SM
- To_SM_fr_BroadC
- To_BroadConnect
- To_CM521
- To_MTSAllstream

Rename Profile Clone Profile Delete Profile

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	cust6-tor.vsac.bell.ca
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	cust6-tor.vsac.bell.ca
To	IP/Domain	Overwrite	cust6-tor.vsac.bell.ca
Via	IP/Domain	Auto	---

Edit

Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	cust6-tor.vsac.bell.ca
SDP	IP/Domain	Auto	
Record-Route	IP/Domain	Auto	
From	IP/Domain	Overwrite	cust6-tor.vsac.bell.ca
To	IP/Domain	Overwrite	cust6-tor.vsac.bell.ca
Via	IP/Domain	Auto	

Finish

Note:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in SIP URI-Host.
- The masking applied on From header also applies to Referred-By and P-Asserted-Identity headers.
- The masking applied on To header also applies to Refer-To header.

7.2.4. Server Interworking

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

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

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

7.2.4.1 Server Interworking profile for Bell Canada

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

General settings:

- **Hold Support** = **None**. Avaya SBCE will not modify the hold/ resume signaling from Communication Manager to send to Bell Canada.
- **18X Handling** = **None**. Avaya SBCE will not handle 180X, it will keep the 18X messages from Communication Manager unchanged to send to Bell Canada.
- **Refer Handling** = **unchecked**. Avaya SBCE will not handle Refer, it will keep the Refer messages from Communication Manager unchanged to send to Bell Canada.
- **T.38 Support** = **unchecked**. Bell Canada does not support T.38 fax in this compliance testing.
- **Privacy Enabled** = **unchecked**. Avaya SBCE will not mask the FROM header with anonymous for outbound call to Bell Canada. It depends on Communication Manager to enable/disable privacy on individual call basis.
- **DTMF Support** = **None**. Avaya SBCE will send original DTMF supported by Communication Manager to Bell Canada.

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

Editing Profile: Bell

General

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

Next

Editing Profile: Bell

Privacy

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

DTMF

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

Back

Finish

7.2.4.2 Server Interworking profile for Session Manager

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

General settings:

- **Hold Support** = **RFC3264**. Communication Manager supports hold/ resume as per RFC3264.
- **18X Handling** = **None**. Avaya SBCE will not handle 180X, it will keep the 18X messages from Bell Canada unchanged to send to Communication Manager via Session Manager.
- **Refer Handling** = **unchecked**. Avaya SBCE will not handle Refer, it will keep the Refer messages from Bell Canada unchanged to send to Communication Manager via Session Manager.
- **T.38 Support** = **unchecked**. Bell Canada does not support T.38 fax in this compliance testing.
- **Privacy Enabled** = **unchecked**. Avaya SBCE will not mask the From header with anonymous for inbound call from Bell Canada. It depends on Bell Canada to enable/ disable privacy on individual call basis.
- **DTMF Support** = **None**. Avaya SBCE will send original DTMF supported by Bell Canada to Communication Manager via Session Manager.

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

Editing Profile: SM

General

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

Next

Editing Profile: SM

Privacy

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

DTMF

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

Back

Finish

7.2.5. Signaling Manipulation

The **Signaling Manipulation** feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given **Server Configuration** which will be configured in the next steps through the UC-Sec GUI. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of the **Signaling Manipulation** but will show an example of a script created during compliance testing to aid in **Topology Hiding**. It is applied to Bell Canada. The script has two portions to normalize the outgoing and incoming call respectively.

In this compliance testing, a SigMa script named **Bell** is created to apply to Bell Canada Server Configuration. The script has two portions to normalize the outgoing and incoming call respectively.

Notes: the SigMa script for Session Manager is unnecessary since the signaling has already been normalized on the Bell Canada side.

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

The detail of SigMa script **Bell** is as following:

```

within session "ALL"
{

act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
append(%HEADERS["Contact"][1].URI.USER,";tgrp=VSAC_4167751880_01A;trunkcontext=sip
trunking.bell.ca");
%HEADERS["Contact"][1].regex_replace("(^\".*\\")", "");
remove(%HEADERS["P-Location"][1]);
remove(%HEADERS["P-Charging-Vector"][1]);
remove(%HEADERS["Accept-Language"][1]);
remove(%HEADERS["Alert-Info"][1]);
}

act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
{
%HEADERS["Request_Line"][1].regex_replace("AvayaCS1K","cust6-tor.v sac.bell.ca");
%HEADERS["To"][1].regex_replace("AvayaCS1K","cust6-tor.v sac.bell.ca");
%HEADERS["From"][1].regex_replace("207.236.237.205","siptrunking.bell.ca");
%HEADERS["From"][1].regex_replace("anonymous.invalid","siptrunking.bell.ca");
%HEADERS["From"][1].URI.USER.regex_replace("(\\+)", "");
%HEADERS["From"][1].URI.USER.regex_replace("^11","1");
%HEADERS["Contact"][1].URI.USER.regex_replace("(\\+)", "");
%HEADERS["Contact"][1].URI.USER.regex_replace("^11","1");
}

}

```

7.2.5.1 Signaling Manipulation rules for outbound call to Bell Canada

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

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

- SigMa rules to manipulate Contact header. The SigMa script would need two rules. The first rule is to append ";tgrp=VSAC_4167751880_01A;trunkcontext=siptrunking.bell.ca" after URI-USER. The second rule is to delete the display information.

```

append(%HEADERS["Contact"][1].URI.USER,";tgrp=VSAC_4167751880_01A;trunkcontext=siptr
unking.bell.ca");
%HEADERS["Contact"][1].regex_replace("(^\".*\\")", "");

```

For example: The original Contact header from Communication Manager:

Contact: "Bell H323 x1881" <sip:4167751881@110.10.97.217;transport=tcp>

The SigMa script will manipulate the Contact header to be expected by Bell Canada:

Contact:<sip:4167751881;tgrp=VSAC_4167751880_01A;trunkcontext=siptrunking.bell.ca@110.10.98.98:5060>

- **SigMa rules to delete unnecessary headers**, including P-Location, P-Charging-Vector, Accept-Language, and Alert-Info.

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

7.2.5.2 Signaling Manipulation rules for inbound call from Bell Canada

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

Bell Canada sends OPTIONS heartbeat toward Session Manager to maintain status of SIP Trunk service. Avaya SBCE dropped this OPTIONS by default because the OPTIONS contain different Request-Line, From and To headers than expected headers as being received in inbound INVITE. The **Topology Hiding** profile cannot be applied here, since the packet was dropped before routing while the **Topology Hiding** just only takes effect after routing. To solve this matter, SigMa rules are defined to normalize OPTIONS packet right after entering the enterprise network. Avaya SBCE needs to normalize the **OPTIONS** to meet the **Routing Profile** defined in **Section 7.2.2**.

- **SigMa rules to normalize OPTIONS heartbeat received from Bell Canada**. The rules are to replace URI-HOST of Request-Line and To header by **cust6-tor.vsaac.bell.ca** and URI-HOST of From header by **siptrunking.bell.ca** to match the URI Group defined in **Section 7.2.1** for routing purpose.

```
%HEADERS["Request_Line"][1].regex_replace("AvayaCS1K","cust6-tor.vsaac.bell.ca");  
%HEADERS["To"][1].regex_replace("AvayaCS1K","cust6-tor.vsaac.bell.ca");  
%HEADERS["From"][1].regex_replace("207.236.237.205","siptrunking.bell.ca");
```

- **SigMa rule to support receiving private call from PSTN**. Avaya SBCE also needs a SigMa rule defined to replace URI-HOST of Request-URI with “anonymous.invalid” to **cust6-tor.vsaac.bell.ca** to match the URI Group defined in **Section 7.2.1** for routing purpose.

```
%HEADERS["From"][1].regex_replace("anonymous.invalid","siptrunking.bell.ca");
```

- **SigMa rules to manipulate the calling number in From and Contact headers**. It is being observed that Bell Canada sends “+1” and 11 digits long distance number of the calling number in From and Contact header. This is not compliant to the North American Numbering Plan (NANP). The SigMa rules as shown below are to format the calling number to be 11 digit long distance number starting with digit “1”, it is compliant to NANP and makes possible for Communication Manager to implement off-net call forward and EC500 features.

```
%HEADERS["From"][1].URI.USER.regex_replace("(\\+)", "");
%HEADERS["From"][1].URI.USER.regex_replace("^11", "1");
%HEADERS["Contact"][1].URI.USER.regex_replace("(\\+)", "");
%HEADERS["Contact"][1].URI.USER.regex_replace("^11", "1");
```

7.2.6. Server Configuration

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

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

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

7.2.6.1 Server Configuration for Bell Canada

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

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'Server Configuration' highlighted. The main content area shows the 'Global Profiles > Server Configuration: Bell' page. A list of profiles is shown on the left, with 'Bell' selected. The 'General' tab is active, displaying the following configuration:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	220.20.237.205
Supported Transports	UDP
UDP Port	5060

Buttons for 'Rename Profile', 'Clone Profile', and 'Delete Profile' are visible at the top right. An 'Edit' button is located at the bottom right of the configuration table.

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

Edit Server Configuration Profile - General

Server Type	Trunk Server
IP Addresses / Supported FQDNs <small>Comma separated list</small>	220.20.237.205
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	

Finish

Bell Canada requests to have Digest Authentication supported on SIP Trunk. In this compliance testing, the authentication will be implemented by Avaya SBCE. In **Authentication** tab, click on the checkbox to **Enable Authentication**; provide the **Realm** as **siptrunking.bell.ca** and correct **User Name** and **Password** provided by Bell Canada.

Edit Server Configuration Profile - Authentication

Enable Authentication	<input checked="" type="checkbox"/>
User Name	4167751880
Realm	siptrunking.bell.ca
Password <small>(Leave blank to keep existing password)</small>
Confirm Password

Finish

In **Heartbeat** tab, **Enable Heartbeat** is checked to send OPTIONS in 60 seconds interval to check for the SIP trunk status, input From header as ping@cust6-tor.vsac.bell.ca and To header as ping@siptrunking.bell.ca as expected by Bell Canada. **TCP Probe** is kept unchecked as default.

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@cust6-tor.vsaac.bell.
To URI	ping@siptrunking.bell.ca
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds

Finish

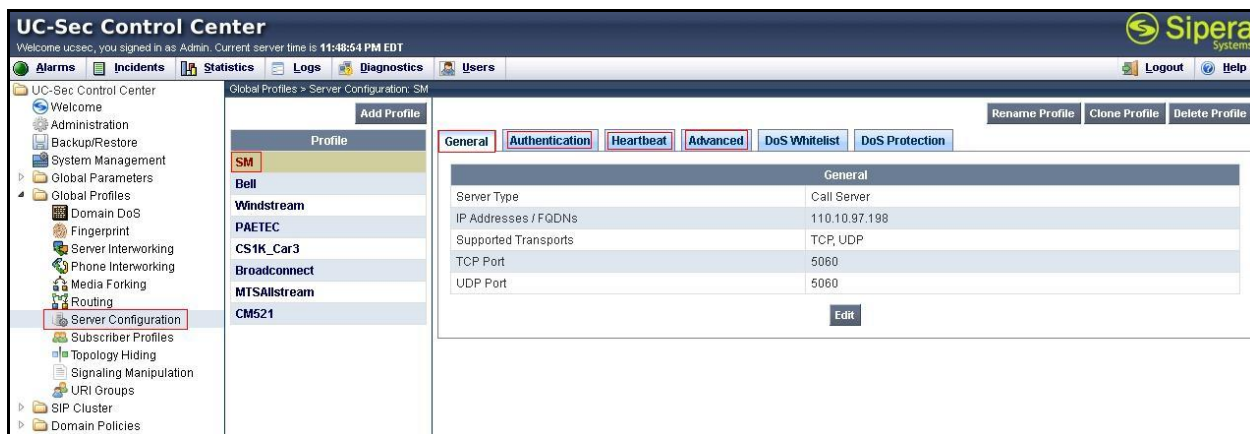
Under **Advanced** tab, in **Interworking Profile** drop down list select entry **Bell** as defined in **Section 7.2.4**, in **Signaling Manipulation Script** drop down list select entry **Bell** as defined in **Section 7.2.5**. This configuration is to apply the specific SIP profile and SigMa rules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

Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Bell
Signaling Manipulation Script	Bell
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Finish

7.2.6.2 Server Configuration for Session Manager

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



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

Edit Server Configuration Profile - General

Server Type	Call Server
IP Addresses / Supported FQDNs <small>Comma separated list</small>	110.10.97.198
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	
<div style="background-color: #4f81bd; color: white; padding: 5px 20px; display: inline-block;">Finish</div>	

In **Authentication** tab, uncheck the checkbox **Enable Authentication**. Session Manager was configured as a trusted link in **Section 6.6**, and does not require authentication.

Edit Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	
Realm	
Password	
Confirm Password	
<input type="button" value="Finish"/>	

In **Heartbeat** tab, **Enable Heartbeat** is checked to send OPTIONS in 60 seconds interval to check for the SIP trunk status, input From header as ping@cust6-tor.vtac.bell.ca and To header as ping@cust6-tor.vtac.bell.ca as expected by Session Manager. **TCP Probe** is kept unchecked as default.

Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@cust6-tor.vtac.bell.ca
To URI	ping@cust6-tor.vtac.bell.ca
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
<input type="button" value="Finish"/>	

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

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

7.3. Domain Policies

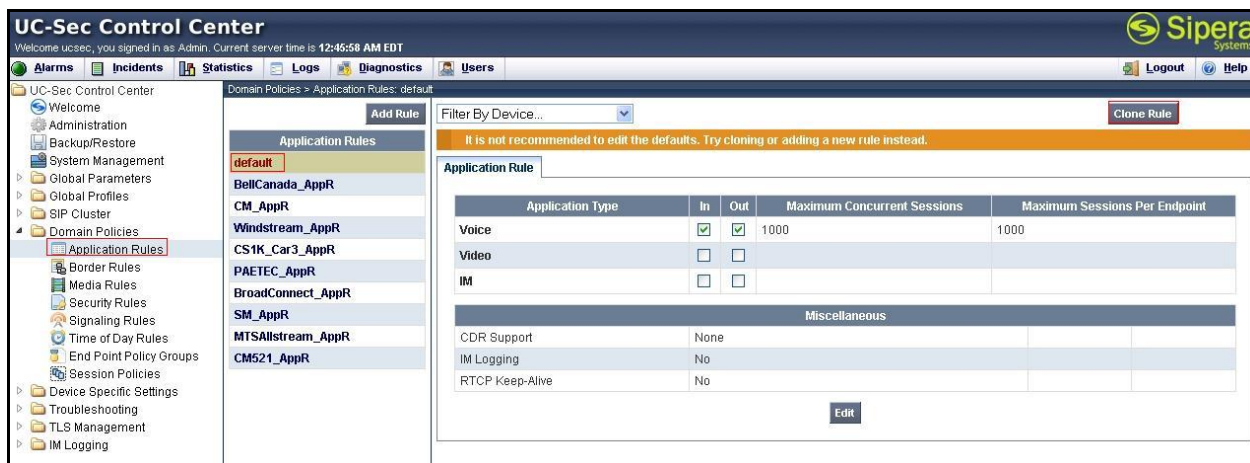
The **Domain Policies** feature configures, applies, and manages various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies which, in turn, activate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

7.3.1. Application Rules

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

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

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



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

Clone Rule
✕

Rule Name

default

Clone Name

BellCanada_AppR

Finish

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

Editing Rule: BellCanada_AppR

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

Miscellaneous

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

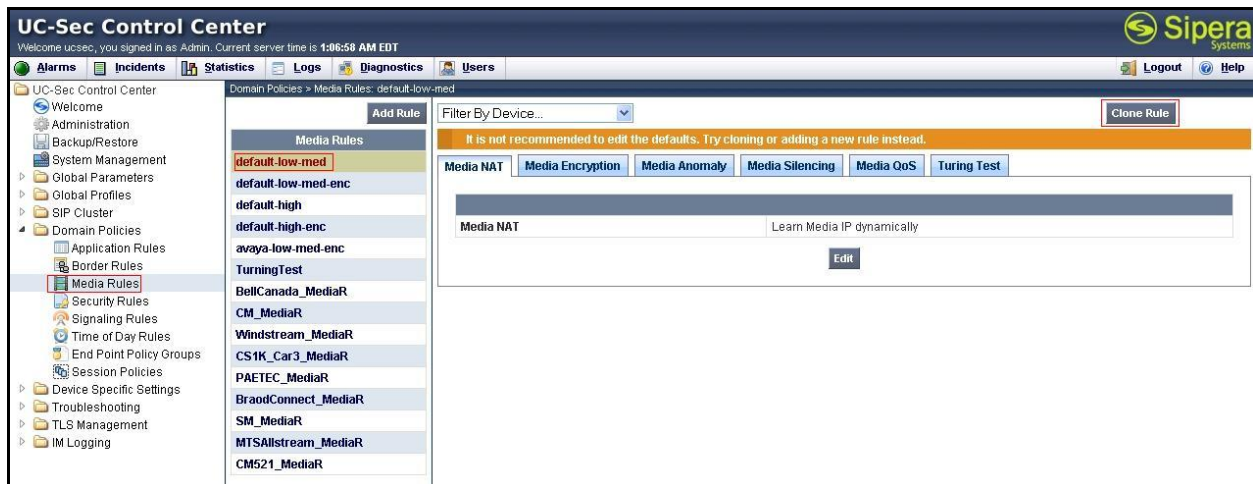
Finish

7.3.2. Media Rules

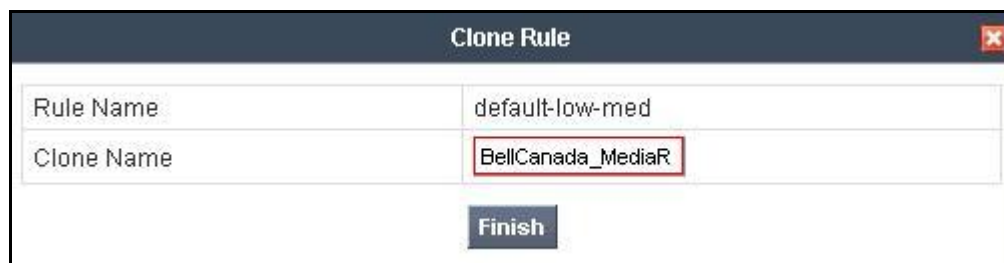
Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be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

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

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



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



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

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



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

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

Media Silencing	
Media Silencing	<input type="checkbox"/>
Timeout (seconds)	
Finish	

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

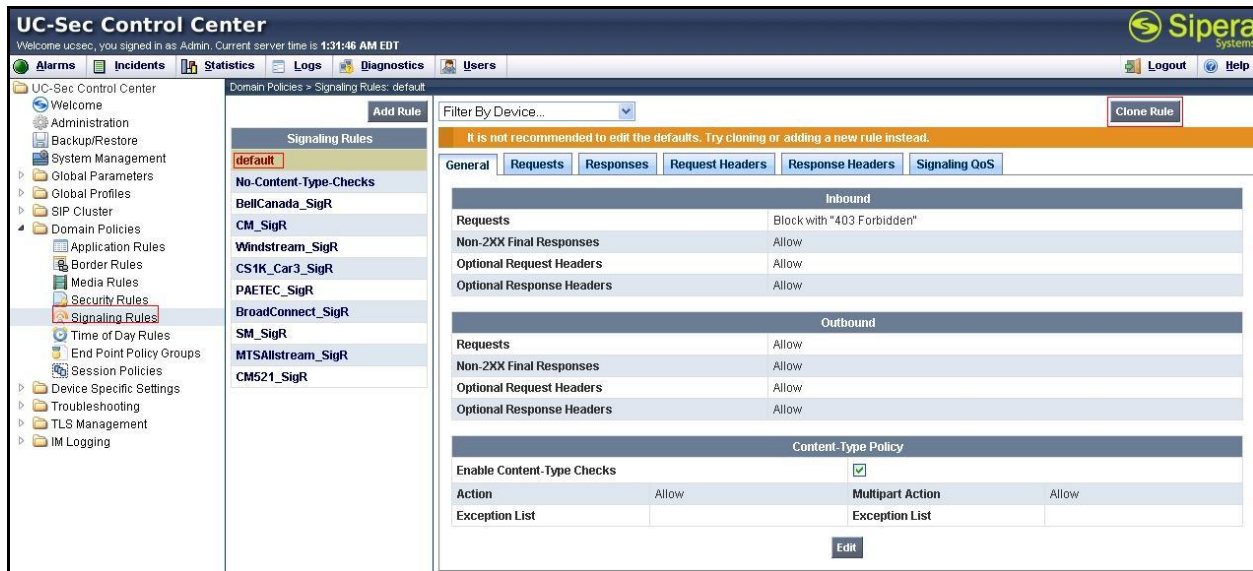
Media QoS			
Media QoS Reporting			
RTCP Enabled		<input type="checkbox"/>	
Media QoS Marking			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
Audio Precedence	Routine		000
Audio ToS	Normal Service		0000
Video Precedence	Routine		000
Video ToS	Normal Service		0000
<input checked="" type="radio"/> DSCP			
Audio	EF		101110
Video	EF		101110
Finish			

7.3.3. Signaling Rules

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

criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

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



The default **Signaling Rule** will block all request with 403 Forbidden. To accept new call, go to **General** tab, click on **Edit**. Change **Inbound** and **Outbound Request** to **Allow** as shown in following screenshot.

General Control ✕

Inbound

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

Outbound

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

Content-Type Policy

Enable Content-Type Checks

☒

Action	Allow ▼	Multipart Action	Allow ▼
Exception List <small>(one per line)</small>		Exception List <small>(one per line)</small>	

Finish

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

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

7.3.4. Endpoint Policy Groups

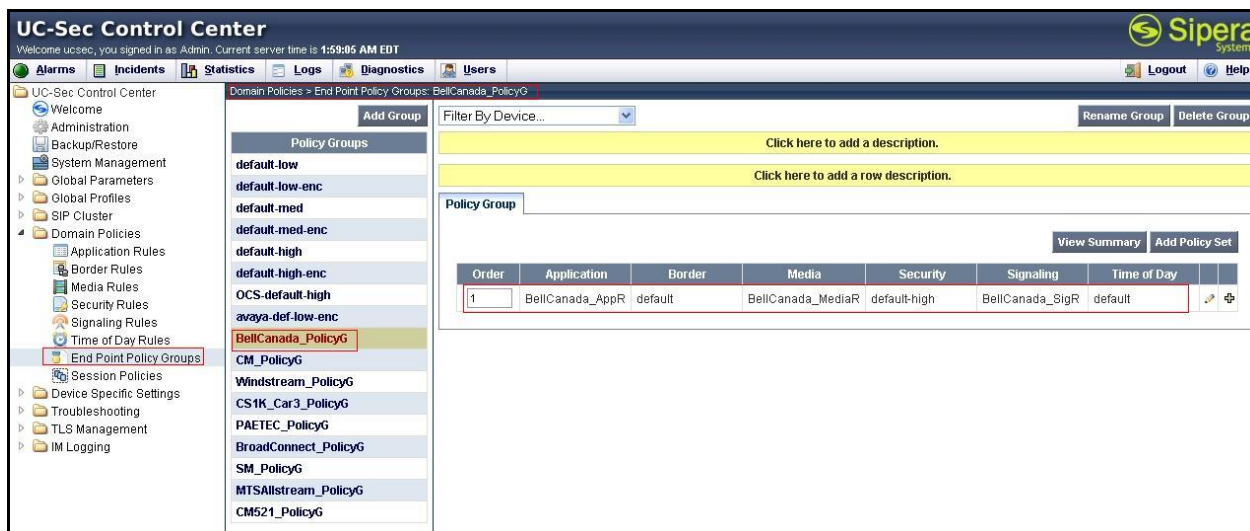
The rules created within the **Domain Policy** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section.

This sample configuration, create a separate **Endpoint Policy Group** for the enterprise and the Bell Canada SIP Trunking.

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

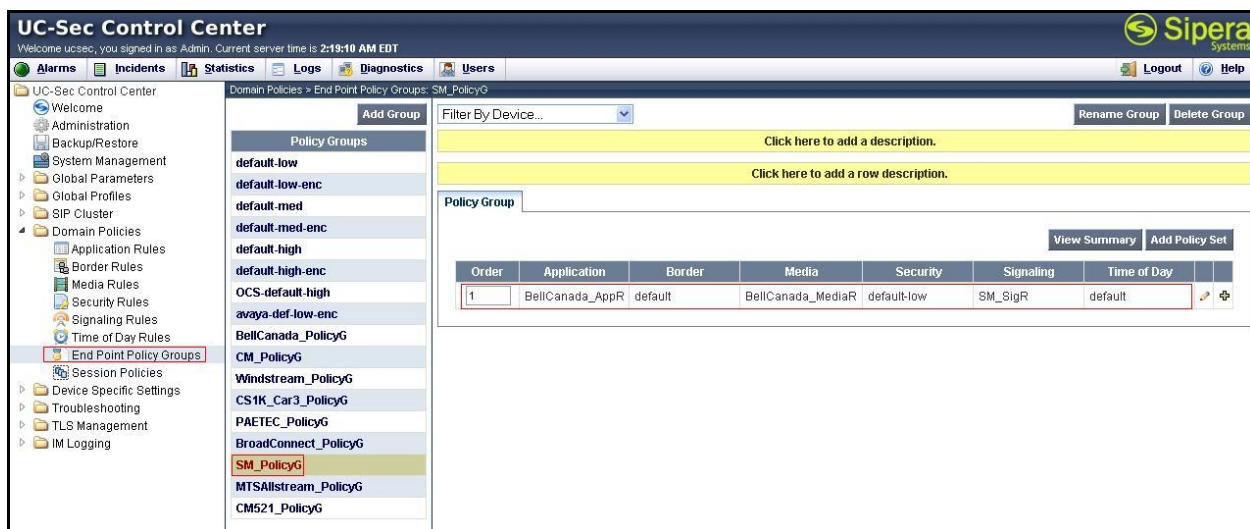
7.3.4.1 Endpoint Policy Group for Bell Canada

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



7.3.4.2 Endpoint Policy Group for Session Manager

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

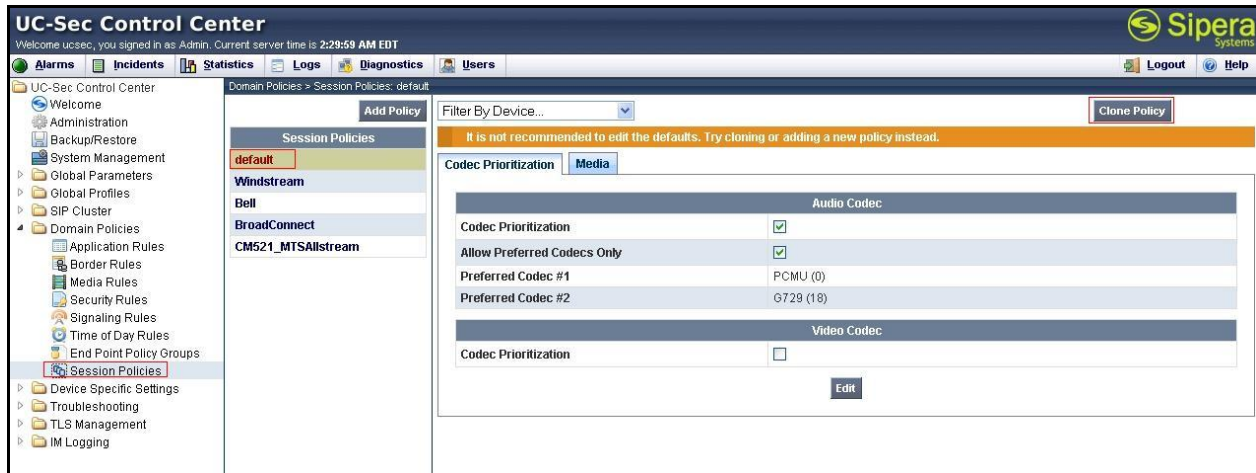


7.3.5. Session Policy

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

In this sample configuration, the Session Policy named **Bell** is created to match to codec configuration on Bell Canada SIP Trunking. The policy also allows Avaya SBCE to anchor media, it happens in off-net call transfer scenarios.

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



Enter a descriptive name **Bell** for the new policy and click **Finish** (not shown).

Bell Canada supports voice codec G.729, G.711MU in prioritized order with payload 101 for RFC2833/DTMF. To define **Codec Prioritization** for Audio Codec, select the profile **Bell**, click on **Edit**. Then check the **Codec Prioritization**, select **Preferred Codec #1** is **G.729 (18)**, **Preferred Codec #2** is **PCMU (0)**, **Preferred Codec #3** is **Dynamic (101)**. Check on the checkbox of **Allow Preferred Codecs Only** is to prevent the unsupported codec from being sent to both ends.

Notes: the T.38 fax is not yet supported by Canada SIP Trunk. This **Session Policy** prioritizes voice codec G.711 to establish the voice call. It is mandatory for a G.711 fax call to be successful because Communication Manager cannot switch the voice call using different codec to G.711 for fax.

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

To enable **Media Anchoring** on Avaya SBCE, select **Session Policy Bell** then select tab **Media**, click **Edit** (not shown). Check on **Media Anchoring**.

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

7.4. Device Specific Settings

The **Device Specific Settings** feature allows aggregate system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will

function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

7.4.1. Network Management

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

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

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 2:50:51 AM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

UC-Sec Devices

sipera

Network Configuration Interface Configuration

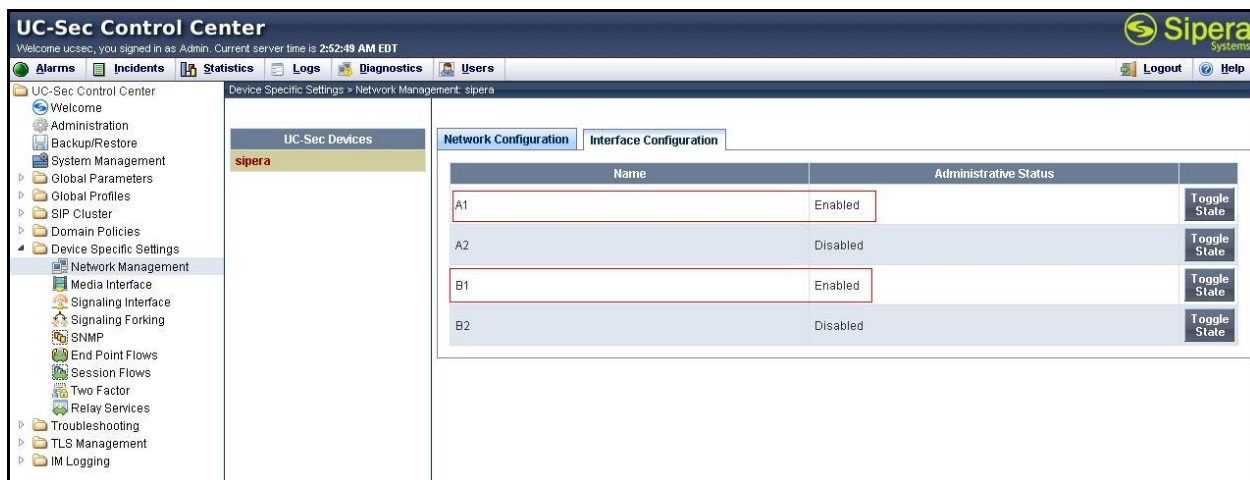
Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask 255.255.255.192 A2 Netmask B1 Netmask 255.255.255.224 B2 Netmask

Add IP Changes will not take effect until the interface is updated. Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface
110.10.97.189		110.10.97.129	A1
110.10.98.98		110.10.98.97	B1
110.10.98.112		110.10.98.97	B1

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



7.4.2. Media Interface

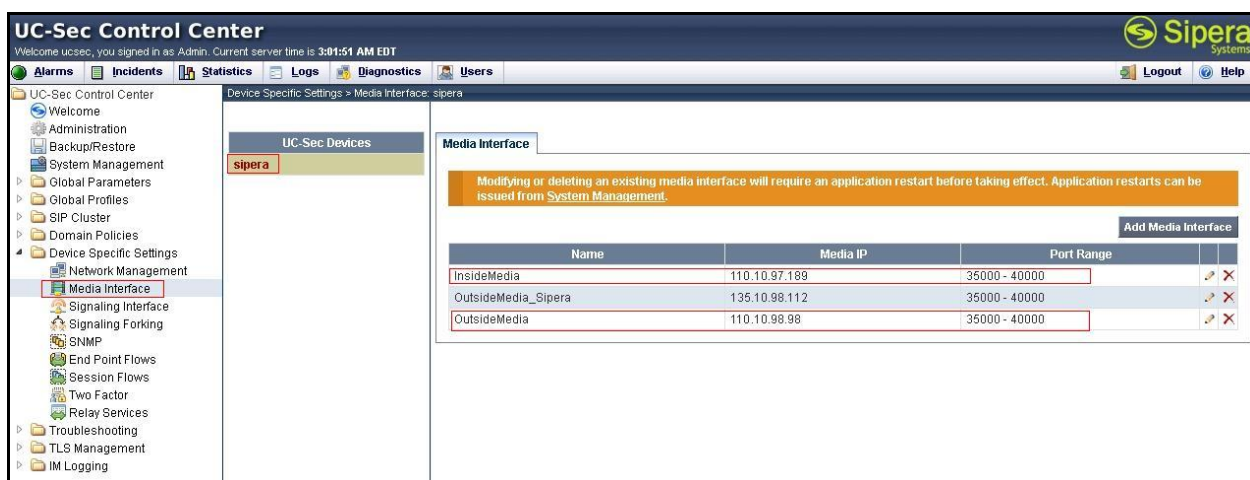
The **Media Interface** screen is where the media ports are defined. Avaya SBCE will listen for RTPs on the defined ports.

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

To create a new **Media Interface**, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface** (not shown).

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

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



7.4.3. Signaling Interface

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

Create a **Signaling Interface** for both the inside and outside IP interfaces. To create a new **Signaling Interface**, navigate to **UC-Sec Control Center** → **Device Specific** → **Settings** → **Signaling Interface** and click **Add Signaling Interface** (not shown).

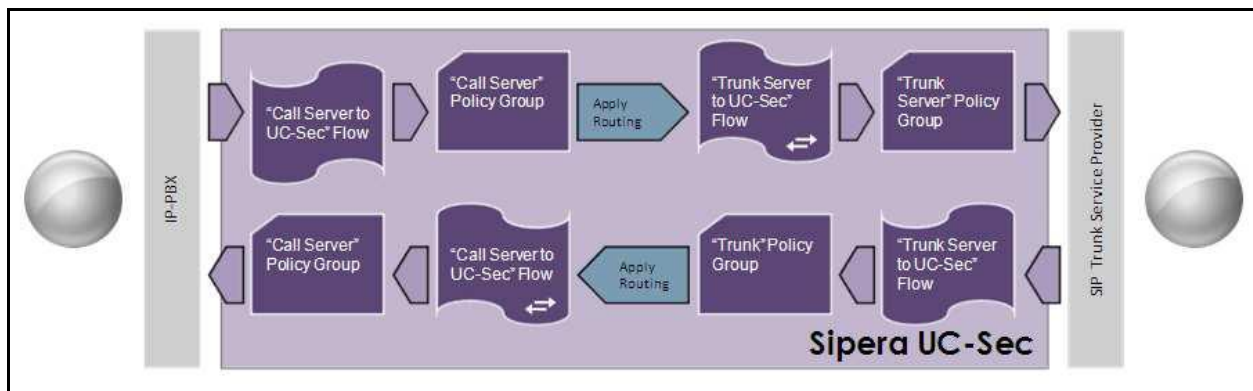
The following screen shows the signaling interfaces created in the sample configuration with TCP and UDP ports 5060 used for the inside and outside IP interfaces.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Signaling Interface' selected. The main area displays a table of configured signaling interfaces for the device 'sipera'.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	110.10.97.189	5060	5060	---	None	[Edit] [Delete]
OutsideSIP_Sipera	135.10.98.112	5060	5060	---	None	[Edit] [Delete]
OutsideSIP	110.10.98.98	5060	5060	---	None	[Edit] [Delete]

7.4.4. End Point Flows - Server Flow

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



Create a separate Server Flow for Session Manager and the Bell Canada SIP Trunking.

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

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

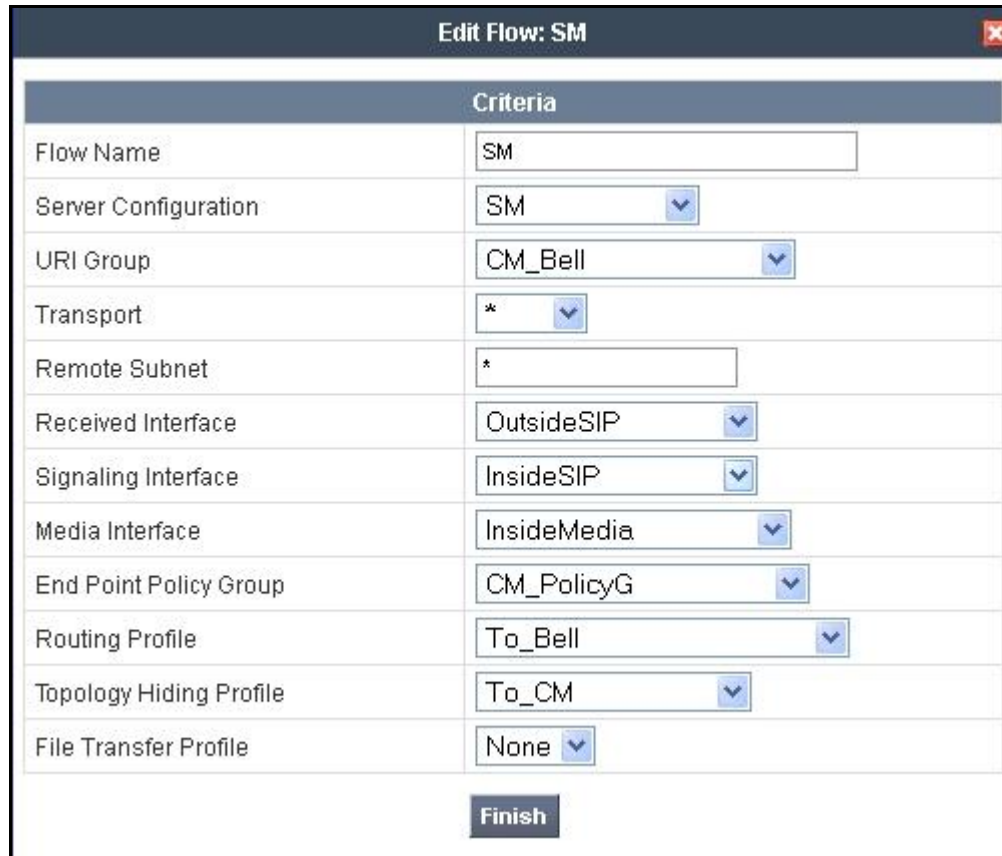
- **Flow Name:** Enter a descriptive name.
 - **Server Configuration:** Select a Server Configuration created in **Section 7.2.6** to assign to the Flow.
 - **URI Group:** Select the URI Group created in **Section 7.2.1** to assign to the Flow.
 - **Received Interface:** Select the Signaling Interface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

The following screen shows the **Sever Flow** named **Bell** for Bell Canada.

Criteria	
Flow Name	Bell
Server Configuration	Bell
URI Group	CM_Bell
Transport	*
Remote Subnet	*
Received Interface	InsideSIP
Signaling Interface	OutsideSIP
Media Interface	OutsideMedia
End Point Policy Group	BellCanada_PolicyG
Routing Profile	To_CM
Topology Hiding Profile	To_Bell
File Transfer Profile	None

Finish

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



The screenshot shows a window titled "Edit Flow: SM" with a close button in the top right corner. Below the title bar is a table with a header "Criteria". The table contains the following rows:

Criteria	
Flow Name	SM
Server Configuration	SM
URI Group	CM_Bell
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP
Signaling Interface	InsideSIP
Media Interface	InsideMedia
End Point Policy Group	CM_PolicyG
Routing Profile	To_Bell
Topology Hiding Profile	To_CM
File Transfer Profile	None

At the bottom of the window is a "Finish" button.

7.4.5. Session Flow

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

Create a common **Session Flow** for both enterprise and the Bell Canada SIP Trunking.

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

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

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

- **URI Group #2:** Select the URI Group created in **Section 7.2.1** to assign to the Flow as the destination **URI Group**.
- **Session Policy:** Select the Session Policy created in **Section 7.3.5** to assign to the Flow. Click **Finish** to save and exit.

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

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

Criteria	
Flow Name	Bell
URI Group #1	CM_Bell
URI Group #2	CM_Bell
Subnet #1	* Ex: 192.168.0.1/24
Subnet #2	* Ex: 192.168.0.1/24
Session Policy	Bell

Finish

8. Bell Canada SIP Trunking Configuration

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

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

- RequestURI: verify the request number and either SIP domain
- From: verify the display name and display number.
- To: verify the display name and display number.
- P-Assert-Identity: verify the display name and display number.
- Privacy: verify the "user, id" masking.

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

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

Troubleshooting:

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

Example of WWW-Authenticate Header:

```
WWW-Authenticate: DIGEST  
qop="auth", nonce="BroadWorksXgyvwpbfiTgxtru8BW", realm="siptrun  
king.bell.ca", algorithm=MD5
```

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

Example of Authorization Header:

```
Authorization: Digest username="4167751880",
realm="siptrunking.bell.ca",
nonce="BroadWorksXgyvwbfITgxtru8BW", uri="sip:cust6-
tor.vsac.bell.ca",
response="18bf8cc66d906b5da627362f0347ee65", algorithm=MD5,
cnonce="0a4f113b", qop=auth, nc=00000001
```

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

2. Communication Manager:

- **list trace station** <extension number> - 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**.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The left sidebar contains navigation links for Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, and System Tools. The main content area is titled 'Session Manager Dashboard' and includes a 'Session Manager Instances' table. The table has columns for Session Manager, Type, Alarms, Tests Pass, Security Module, Service State, Entity Monitoring, Active Call Count, Registrations, and Version. The first row shows 'DevASM' with a green checkmark in the 'Tests Pass' column and 'Accept New Service' in the 'Service State' column.

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

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

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller For Enterprise 4.0.5 to 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**. The Bell Canada SIP Trunking is considered **compliant** with Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Session Border Controller For Enterprise 4.0.5.

11. 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]*UC-Sec Install Guide (102-5224-400v1.01)*
- [13]*UC-Sec Administration Guide (010-5423-400v106)*
- [14]*RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [15]*RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [16]*RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [17]*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.