



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Bell Canada SIP Trunking Service with Avaya Communication Server 1000 Release 7.5, Avaya Aura ® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 4.0.5 – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell Canada SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 Release 7.5, Avaya Aura ® Session Manager Release 6.3, Avaya Session Border Controller for Enterprise Release 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 Bell Canada networks as an alternative to traditional PSTN trunks such as analog or ISDN-PRI. 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 is conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

## Table of Contents

1. Introduction.....	4
2. General Test Approach and Test Results.....	5
2.1. Interoperability Compliance Testing .....	5
2.2. Test Results.....	6
2.3. Support.....	9
3. Reference Configuration.....	10
4. Equipment and Software Validated .....	12
5. Avaya Communication Server 1000 Configuration .....	13
5.1. Log into the CS1000.....	13
5.1.1. Log into Unified Communications Management (UCM) and Element Manager (EM).....	13
5.1.2. Log into Call Server Command Line Interface (CLI) .....	14
5.2. Administer Node IP Telephony .....	15
5.2.1. Obtain Node IP Address .....	15
5.2.2. Administer Quality of Service (QoS) .....	16
5.2.3. Synchronize the new configuration .....	16
5.3. Administer Voice Codec.....	16
5.3.1. Enable Voice Codec, Node IP Telephony .....	16
5.3.2. Administer Voice Codec on Media Gateways.....	17
5.4. Administer Zones and Bandwidth .....	18
5.4.1. Create Zone for VGW and IP phones .....	19
5.4.2. Create Zone for virtual SIP Trunk .....	19
5.5. Administer SIP Trunk Gateway.....	19
5.5.1. Integrated Services Digital Network (ISDN).....	20
5.5.2. Administer SIP Trunk Gateway to the Avaya SBCE .....	20
5.5.3. Administer Virtual D-Channel.....	22
5.5.4. Administer Virtual Super-Loop .....	24
5.5.5. Enable Music for Customer Data Block .....	24
5.5.6. Administer Virtual SIP Route.....	24
5.5.7. Administer Virtual SIP Trunks .....	27
5.5.8. Administer Calling Line Identification Entry .....	28
5.5.9. Enable External Trunk to Trunk Transferring .....	29
5.6. Administer Dialing Plans.....	30
5.6.1. Define ESN Access Codes and Parameters (ESN).....	30
5.6.2. Associate NPA and SPN calls to ESN Access Code 1 .....	31
5.6.3. Administer Digit Manipulation Block (DMI).....	32
5.6.4. Administer Route List Block (RLB).....	32
5.6.5. Administer Incoming Digit Translation (IDC) .....	33
5.6.6. Administer Outbound Call - Special Number.....	34
5.6.7. Administer Outbound Call - Numbering Plan Area (NPA).....	35
6. Configure Avaya Aura® Session Manager .....	37
6.1. System Manager Login and Navigation .....	37
6.2. Specify SIP Domain.....	39
6.3. Add Location .....	39
6.4. Add SIP Entities.....	40

6.5. Add Entity Links.....	43
6.6. Add Routing Policies .....	45
6.7. Add Dial Patterns .....	46
6.8. Add/View Avaya Aura ® Session Manager.....	48
7. Configure Avaya Session Border Controller for Enterprise .....	50
7.1. Log into the Avaya Session Border Controller for Enterprise.....	51
7.2. Global Profiles .....	53
7.2.1. Uniform Resource Identifier (URI) Groups.....	53
7.2.2. Routing Profiles .....	54
7.2.3. Topology Hiding.....	56
7.2.4. Server Interworking .....	57
7.2.5. Signaling Manipulation.....	62
7.2.6. Server Configuration.....	65
7.3. Domain Policies .....	69
7.3.1. Application Rules.....	70
7.3.2. Media Rules .....	71
7.3.3. Signaling Rules .....	73
7.3.4. Endpoint Policy Groups.....	78
7.3.5. Session Policy .....	79
7.4. Device Specific Settings .....	81
7.4.1. Network Management.....	81
7.4.2. Media Interface .....	82
7.4.3. Signaling Interface.....	83
7.4.4. End Point Flows - Server Flow .....	84
7.4.5. Session Flows.....	86
8. Bell Canada SIP Trunking Service Configuration.....	88
9. Verification and Troubleshooting .....	89
9.1. Verification Steps.....	89
9.2. Protocol Traces .....	89
9.3. Troubleshooting .....	90
9.3.1. The Avaya SBCE.....	90
9.3.2. The CS1000 Verification Steps .....	94
10. Conclusion .....	97
11. References.....	98

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell Canada SIP Trunking Service (Bell Canada) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 (CS1000) Release 7.5, Avaya Aura® Session Manager (Session Manager) Release 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 4.0.5 and various Avaya endpoints.

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 using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog or ISDN-PRI.

Bell Canada applies Digest Authentication for outgoing calls from the enterprise. It uses challenge-response authentication with a “401 Unauthorized” responding to each initial outgoing INVITE to Bell Canada. The subsequent INVITE from the enterprise provides the “Authorization” header with a configured user name and password. This credential is provided by Bell Canada and configured on the Avaya SBCE. This call authentication scheme as specified in RFC 3261 provides authentication for the SIP signaling.



## 2. General Test Approach and Test Results

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

Bell Canada is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to Bell Canada via the public Internet and exercise the features and functionalities listed in **Section 2.1**.

### 2.1. Interoperability Compliance Testing

To verify Bell Canada SIP Trunking interoperability, the following features and functionalities were covered during the compliance testing:

- Incoming PSTN calls to various phone types including UNISTim, SIP, digital, and analog telephones at the enterprise. All incoming calls from PSTN are routed to the enterprise across the SIP Trunk from the service provider.
- Outgoing PSTN calls from various phone types including UNISTim, SIP, digital, and analog telephones at the enterprise. All outgoing calls to PSTN are routed from the enterprise across the SIP Trunk to the service provider.
- Incoming and outgoing PSTN calls to/from 2050PC softphones.
- Incoming and outgoing PSTN calls to/from Avaya One-X® Communicator (SIP) softphones for the CS1000.
- Dialing plans including local, long distance, international, outgoing toll-free, operator assisted calls, local directory assistance (411) calls, etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Proper codec negotiation with G.711MU codec.
- Proper early media transmission using G.711MU codec.
- Proper media transmission using G.711MU codec.
- Incoming and outgoing fax calls using G.711MU codec.
- DTMF tone transmission as out-of-band RTP events as per RFC 2833.
- Voicemail navigation for incoming and outgoing calls.
- Call Pilot voicemail hosted on the CS1000.
- Telephony features such as Hold and Resume, Call Waiting, Call Park, Call Transfer, Call Forward, and Conferencing.
- Music on Hold.
- Off-net call transfer using subsequent INVITE method.
- Off-net call forward using Diversion method.
- Mobility Extension (MobX) twining incoming call to cellular phones.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.

- SIP Digest Authentication.
- Session Timers implementation.

Items that are not supported by Bell Canada in the test environment or not tested as part of the compliance testing, are listed as following:

- Inbound toll-free and outgoing emergency calls (E911) are supported but were not tested as part of the compliance testing because Bell Canada has not provided the necessary configuration.
- G.729 codec is not supported.
- T.38 fax is not supported.
- Off-net call transfers using the REFER method are not supported.
- Off-net call forwarding using the History-Info method is not supported.

## 2.2. Test Results

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

### 1. Incoming call to retrieve voicemail on Call Pilot is corrected and working properly.

An incoming call to Call Pilot was unexpectedly disconnected by Bell Canada with a BYE message responding to the 200OK without Session Description Protocol (SDP) from the CS1000. According to RFC 3262, this 200OK is valid because the signaling from Bell Canada contains “Supported:100rel” to indicate that the Reliability of Provisional Responses is supported. A workaround has been implemented to disable the Reliability of Provisional Responses on the SIP Trunk by provisioning a Signaling Manipulation (SigMa) script on the SBCE to delete the “Supported:100rel” signaling on both inbound and outbound traffics. By removing the “100rel”, it forces the CS1000 to send a SDP along with 200OK. This allows the call to establish successfully. For the detailed configuration, refer to **Section 7.2.5**.

### 2. For off-net blind transfer call, the calling PSTN does not hear ringback when the called PSTN is ringing.

This limitation was encountered due to the workaround from the above observation (observation #1). Without the “100rel” signaling which is for the Reliability of Provisional Responses (RFC3262) support, the UPDATE/SDP from the CS1000 to complete an off-net call transfer was rejected by Bell Canada with a “500 Internal Server Error”. The call failed to transfer. To correct this scenario, the patch MPLR30224 needs to be installed on the CS1000 SIP Gateway. With the patch in-service, the CS1000 uses the subsequent INVITE method to complete the transferred call instead of using the UPDATE/SDP. The call successfully transferred, however, it was being observed that the calling PSTN did not hear ringback when the called PSTN was ringing. This is a known limitation of the patch with no resolution available at this time.

### 3. Calling Party Name and Number are not updated if the CS1000 off-net redirects (by transferring or forwarding) an incoming or outgoing PSTN call to internal station.

Before (or after) completing the local redirection to internal station, the CS1000 did not

send UPDATE or re-INVITE signaling to update the true connected Calling Party Name and Number to PSTN party. It results the PSTN party still display Calling Party Name and Number of the CS1000 extension. This is a known issue of the CS1000 when it interoperates with Bell Canada where the proprietary signaling of the CS1000 is not supported. This issue has low user impact, it is listed here simply as an observation.

4. **Calling Party Name and Number are not updated if the CS1000 redirects (by transferring or forwarding) an incoming or outgoing call back to PSTN.** Before (and after) completing the off-net redirection, the CS1000 did not send UPDATE or re-INVITE signaling to update the true connected Calling Party Name and Number to PSTN parties. It results both PSTN parties still display Calling Party Name and Number of the CS1000 extension. This is a known issue of the CS1000 when it interoperates with Bell Canada where the proprietary signaling of the CS1000 is not supported. This issue has low user impact, it is listed here simply as an observation.
5. **CS1000 SIP phone fails to transfer off-net to PSTN if “Music On Hold” is enabled.** When “Music On Hold” is enabled, the CS1000 SIP phone fails to transfer off-net an incoming or outgoing call between the CS1000 SIP phone and PSTN\_1 to PSTN\_2. PSTN\_1 continues to hear ringback after the call has already been answered by PSTN\_2. The same call scenario is successful when the SIP phone is replaced by the other endpoints, e.g. UNISTim or digital phones. A product defect has been reported to Avaya team for investigation. This issue, however, is listed here as a limitation.
6. **CS1000 UNISTim phone places an external call on hold then retrieves the held call, it causes Calling Party Number to change.** After retrieving a held external call, Calling Party Number previously displayed on the CS1000 UNISTim phone is replaced by “Route ACOD” – “Trunk Channel ID”. This is a known behavior of the CS1000 with no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
7. **CS1000 UNISTim phone calls to an internal SIP phone which Call Forward All Call to PSTN, the UNISTim phone does not display Calling Party Name and Number of the PSTN party.** After the call was successfully forwarded to PSTN, the PSTN party properly displayed Calling Party Name and Number of the UNISTim. However, the UNISTim phone still displayed local extension of the SIP phone which is not expected. It should display Calling Party Name and Number of the PSTN which is the true connected party. This is a known behavior of the CS1000 with no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
8. **CS1000 UNISTim phone calls to PSTN then blind transfers to an internal SIP phone, the SIP phone does not display places Calling Party Name and Number of the PSTN party.** After the call was successfully transferred, the SIP phone displayed Calling Party Name and Number of the UNISTim which is not expected. It should display Calling Party Name and Number of the PSTN which is the true connected party. This is a known behavior of the CS1000 with no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.

- 9. CS1000 SIP phone dials a local UNISTim phone then blind transfers to PSTN, it causes Calling Party Number to change.** The call was successfully transferred, however, the CS1000 UNISTim phone displays “Route ACOD” – “Trunk Channel ID” instead of displaying Calling Party Name and Calling Party Number of the PSTN party. This is a known behavior of the CS1000 with no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
- 10. Calling Party Name and Number of outgoing calls to Mobility Extension (MobX) is corrected and working properly.** When an incoming call to a local deskphone was twined to MobX, it did not contain the “Diversion” header with an assigned DID number. Thus it failed to be authenticated by Bell Canada. This issue has been corrected by a SigMa script implemented on the Avaya SBCE (see **Section 7.2.5**) to check if the “From” and “P-Asserted-Identity” header do not contain the DID number then it constructs the proper “Diversion” header for call authentication purpose. This is a known behavior of the CS1000 with no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
- 11. Cellular Voice Mail Avoidance function of the Mobility Extension (MobX) feature is corrected and working properly.** When an incoming call being answered by the cellular voice mail, the **Mobile extension timer** (MBXT) setting on the SIP Trunk as described in **Section 5.5.6**, cannot ignore the answering as expected. The call then is unexpectedly connected to cellular voice mailbox instead of connecting to enterprise voice mailbox (hosted by Call Pilot). This issue has been corrected by patch MPLR32246. With the patch in-service, the answering by cellular voice mail before MBXT will be ignored, it allows incoming calls to route to Call Pilot.
- 12. MobX does not hear ringback when calling to PSTN using Mobility System Access (MSA).** After making a call to MSA configured on the CS1000, MobX received the dial tone to make and an outgoing call to PSTN by entering the desired dial number of PSTN party. It was observed that there was no ringback heard on MobX when PSTN party was ringing. However, the call was successfully answered with good audio paths. This is a known behavior of the CS1000 with no resolution available at this time. It is listed here as a limitation.
- 13. The off-net call forward unconditional or busy fails if the forwarded PSTN party takes longer than 8 seconds to respond.** The issue has been seen on cellular PSTN phone. The CS1000 relies on the respond time of the cellular PSTN phone on the 2<sup>nd</sup> leg to transmit ringback to the original calling PSTN party on the 1<sup>st</sup> leg. If the respond time exceeds 8 seconds, Bell Canada terminates the call with a CANCEL request on the 1st call leg. This failed the scenarios. The issue does not happen if the cellular PSTN phone in good wireless coverage that can significantly reduce the respond time under 8 second limit. The same call scenarios are successful on the regular PSTN phone (instead of the cellular PSTN party). Bell Canada is recommended to increase the Session Provisioning Timer to correct the issue. This is acknowledged as a known behavior of Bell Canada SIP Trunking Service with no resolution available at this time. It is listed here as a limitation.

**14. For off-net call forward unconditional or call forward busy scenarios, a general reason code unknown is set to the Diversion header.** As a limitation of the Avaya SBCE, a typical reason code **unknown** was set to the “Diversion” header for all call forward scenarios instead of the particular reason code of **unconditional**, **no-answer**, or **user-busy** appropriately for call forward all call, no answer, or busy call scenarios. In the compliance testing, with the reason code was set to **unknown**, all off-net call forward scenarios were successful. For detailed configuration, see **Section 7.2.5**.

**15. Performing an “Application Restart” on the Avaya SBCE may cause the SigmaScript or Authentication to stop working.** If the SigMa script or Authentication do not work after an “Application Restart”, contact Avaya for support on the Avaya SBCE by telephone numbers +1-866-861-3113 (toll free) or +1-214-269-2424. **Note:** The password for Authentication should not contain special character, e.g. “!”. A product defect has been reported to Avaya team for investigation but there is no resolution available at this time. This issue is listed here as a limitation.

## **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 Service, please contact Bell Canada at [http://www.bell.ca/enterprise/EntPrd\\_SIP\\_Trunking.page](http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page).

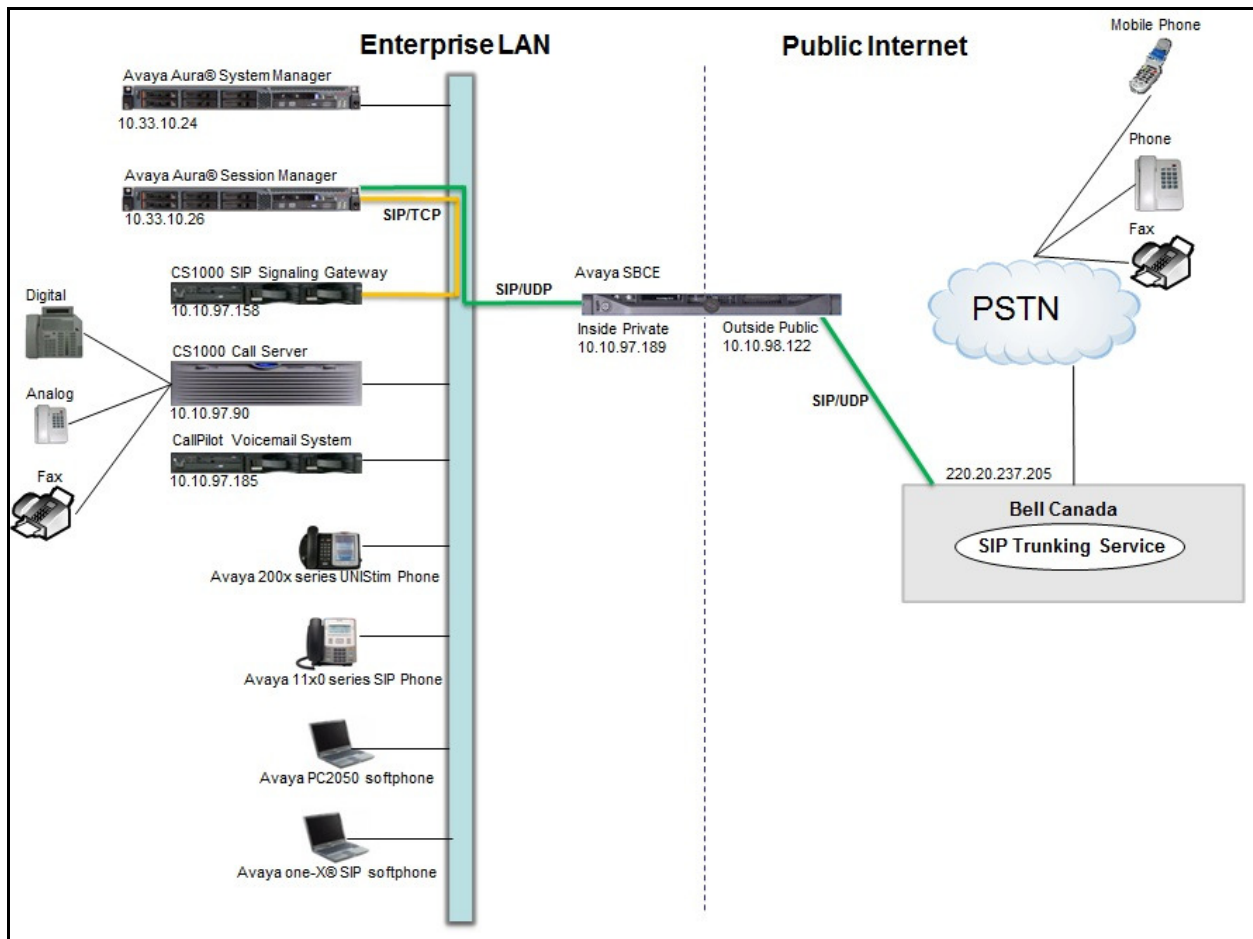
### 3. Reference Configuration

**Figure 1** illustrates the sample Avaya SIP-enabled enterprise solution connected to Bell Canada SIP Trunking Service (Vendor Validation Circuit) through the Internet.

For confidentiality and privacy purposes, the actual public IP addresses and PSTN routable phone numbers used in the certification testing have been replaced with fictitious parameters throughout the Application Notes.

The Avaya SBCE is located at the edge of the enterprise network. The Avaya SBCE has two connection points, a public side connecting to Bell Canada via the Internet and a private side connecting to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flow through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. The Avaya SBCE provides Network Address Translation (NAT) at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Bell Canada across the public network is UDP, the transport protocol between the Avaya SBCE and Session Manager across the enterprise network is also UDP.

In the compliance testing, Bell Canada provided the service provider public SIP domain as **sipxxxxxxx.bell.ca** and the enterprise public SIP domain as **cust6xxxx.xxxx.bell.ca**. These public SIP domains will be used for the public SIP traffic between the Avaya SBCE and Bell Canada. The Avaya lab was configured with a SIP domain **avaya.com** for the enterprise, the Topology-Hiding feature of the Avaya SBCE (see **Section 7.2.3.1**) was used to adapt the enterprise SIP domain to the service provider SIP domains known to Bell Canada. **Figure 1** below illustrates the network diagram for the enterprise.



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

## 4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya CS1000 7.5 (CPPM)	<ul style="list-style-type: none"> <li>• Call Server: 7.50 Q GA plus latest DEPLIST Issue: 01 Release: 2013-03-19 16:44:12 (est) and patch MPLR32246</li> <li>• SSG and SLG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20130308.ntl and patch MPLR30224</li> </ul>
Avaya Aura® Session Manager running on Avaya S8800 Server	6.3 (6.3.1.0.631004)
Avaya Aura® System Manager running on Avaya S8800 Server	6.3 (6.3.1.9.1212)
Avaya Call Pilot	05.00.41.141
Avaya IP Telephone	<ul style="list-style-type: none"> <li>• 2002 p2: 0604DCJ (UNISim)</li> <li>• 2004 p2: 0604DCJ (UNISim)</li> <li>• 1140: 0625C6O (UNISim)</li> <li>• 1120: 0624C6O (UNISim)</li> <li>• 2007: 0621C6M (UNISim)</li> <li>• 1220: 062AC6O (UNISim)</li> <li>• SIP 1120, 1140: SIP11x0e04.03.12.00</li> <li>• SIP 1220,1240: SIP12x0e04.03.12.00</li> </ul>
Avaya 2050PC softphone	3.4
Avaya One-X® Communicator (SIP) softphone for the CS1000	CS6.1.0.25-GA-33661
Avaya Digital Telephone	n/a
Avaya Analog Telephone	n/a
Avaya Session Border Controller for Enterprise (running on Dell R210 platform)	4.0.5 Q09
Bell Canada SIP Trunking Service Components	
Equipment/Software	Release/Version
Bell Canada SIP Trunking Service	Version 1.3

**Table 1: Equipment and Software Tested**



## 5. Avaya Communication Server 1000 Configuration

This section describes the procedure for configuring the CS1000 for inter-operating with the Bell Canada.

A two-way SIP Trunk was created between the CS1000 and Session Manager to carry traffic to and from the service provider respectively. Incoming calls flow from the Bell Canada networks to the Avaya SBCE to the CS1000 via Session Manager. Incoming calls into the CS1000 may undergo call treatments such as incoming digit translations and class of service restrictions. Outgoing calls to PSTN are first processed by the CS1000 for call treatments such as route selection and class of service. Once the CS1000 selects the proper SIP Trunk, the call is routed to the Avaya SBCE via Session Manager for egress to the Bell Canada network.

For the compliance testing, Bell Canada applied Digest Authentication for outgoing calls from the enterprise, using challenge-response authentication based on a configured user name and password (provided by Bell Canada and configured on the Avaya SBCE). This call authentication scheme, as specified in SIP RFC3261, provides authentication for the SIP signaling.

These Application Notes assume the basic configuration has already been administered and it is not discussed here. For further information on the CS1000, see **References** in **Section 11**.

### 5.1. Log into the CS1000

#### 5.1.1. Log into Unified Communications Management (UCM) and Element Manager (EM)

Open the web browser and connect to the UCM GUI <https://<UCM IP address>> as shown in the screenshot below then log in using an appropriate username and password.

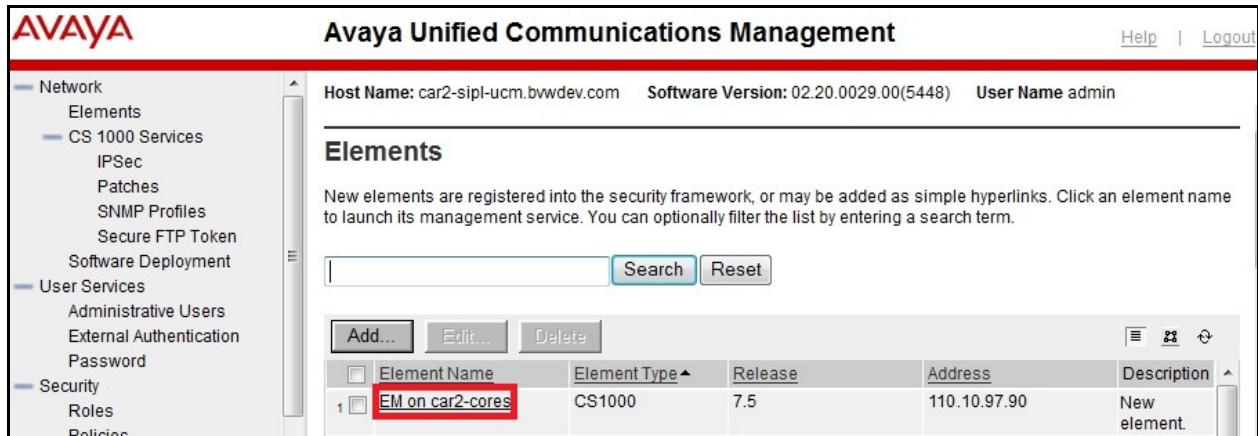
This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.

User ID:

Password:

Copyright © 2002-2010 Avaya Inc. All rights reserved.

The **Avaya Unified Communications Management** is shown in the following screenshot. Click the **Element Name** of the CS1000 Element as highlighted in the red box.



The following screenshot shows the CS1000 Element Manager **System Overview** page.



### 5.1.2. Log into Call Server Command Line Interface (CLI)

Using Putty, SSH to the IP address of the SIP Signaling Gateway (SSG) Server with the *admin* account then run the command *cslogin* and login with the appropriate admin account name and password. The following screenshot shows the logs.

```
login as: admin

Avaya Inc. Linux Base 7.50
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.

admin@10.10.97.158's password:
Last login: Wed Apr 3 10:41:08 2013 from 10.10.98.86
[admin@car2-ssg2 ~]$ cslogin
```

```
SEC054 A device has connected to, or disconnected from, a pseudo tty without
authenticating
```

```
TTY 10 SCH MTC TRF BUG OSN    10:43
OVL111 IDLE    0
>
```

## 5.2. Administer Node IP Telephony

This section describes how to configure an IP Telephony Node on the CS1000.

### 5.2.1. Obtain Node IP Address

These Application Notes assume the basic configuration has already been administered and that a Node has already been created. This section describes configuration steps for Node ID 2003.

To create an IP Node, select **System** → **IP Network** → **Nodes: Servers, Media Cards**. In the **IP Telephony Nodes** page as shown in the screenshot below, click the Node ID of the CS1000.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
2003	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.10.97.158		Synchronized

The **Node Details** page is shown in the screenshot below with the IP address of Node ID 2003. The SIP Signaling Gateway uses the **Node IP Address** to connect to the Avaya SBCE for the SIP Trunk to Bell Canada.

**Node Details (ID: 2003 - SIP Line, LTPS, Gateway (SIPGw))**

**Embedded LAN (ELAN)**  
Gateway IP address: 10.10.97.65 \*  
Subnet mask: 255.255.255.192 \*

**Telephony LAN (TLAN)**  
Node IPv4 address: 10.10.97.158 \*  
Subnet mask: 255.255.255.192 \*  
Node IPv6 address:

**IP Telephony Node Properties**

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN

**Applications (click to edit configuration)**

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)

### 5.2.2. Administer Quality of Service (QoS)

To configure the QoS, click **Quality of Service (QoS)** link in Node Details page shown in **Section 5.2.1**. Verify that the default Diffserv values were used as shown in the screenshot below, then click **Save** button (not shown).

### 5.2.3. Synchronize the new configuration

In order for the changes to take effect, the Node Details page needs to be saved and synchronized by following the steps below.

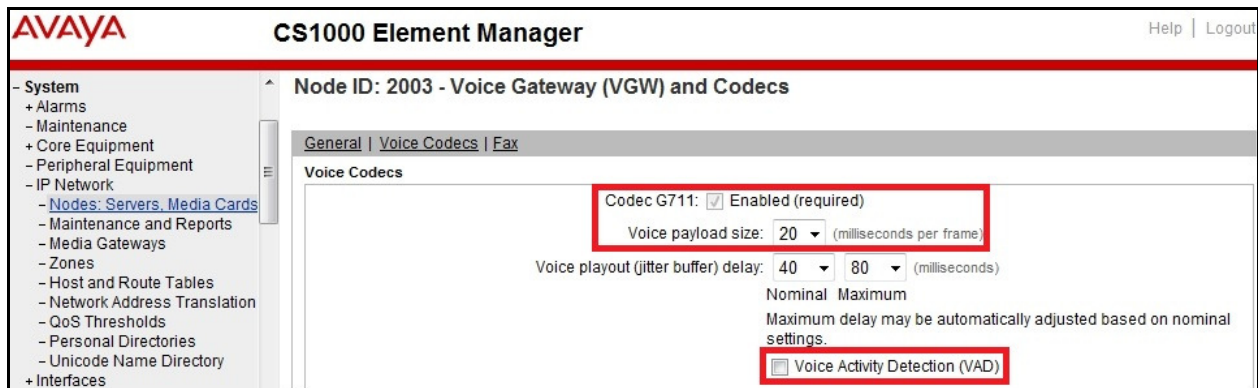
- Return to the **Node Details** page shown in **Section 5.2.1** and click the **Save** button (not shown).
- The **Node Saved** screen is displayed. Click the **Transfer Now** button (not shown).
- The **Synchronize Configuration Files** screen is displayed. Check the **Signaling Server** checkbox and click **Start Sync** button (not shown).
- When the synchronization completes, check the **Signaling Server** check box and click the **Restart Applications** button (not shown).

## 5.3. Administer Voice Codec

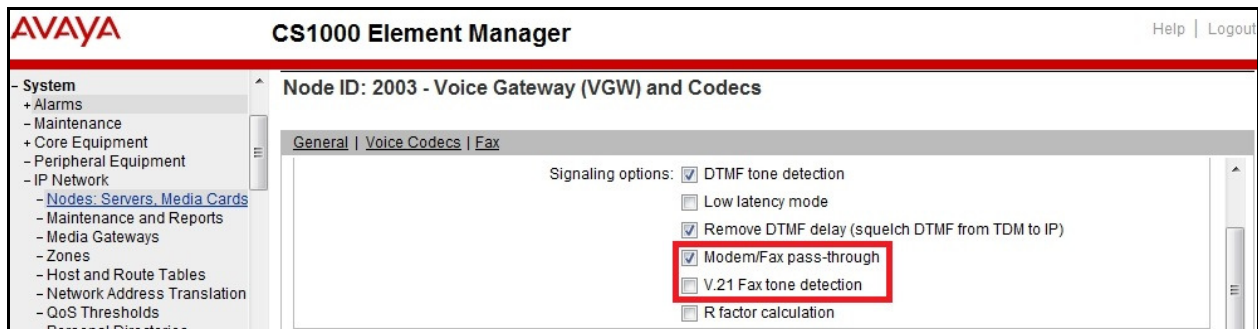
### 5.3.1. Enable Voice Codec, Node IP Telephony

To configure the Voice Codec, select **IP Network** → **Nodes: Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as described in **Section 5.2.1**.

On the **Node Details** page (not shown), click on **Voice Gateway (VGW) and Codec**. Bell Canada supports voice codec G.711, payload size 20 ms, with VAD disabled. The following screenshot shows appropriated voice codec profile configured on the CS1000.



For Fax over IP, Bell Canada supports G.711MU codec as default and does not support T.38. The following screenshot shows **Modem Pass Through** is selected for Node 2003, this enables G.711MU codec to be used for fax calls between the CS1000 and Bell Canada. **Note:** The **V.21 Fax tone detection** should be unchecked to disable T.38 fax capability on the SIP Trunk.



Click **Save** (not shown) then synchronize the new configuration (see **Section 5.2.3**).

### 5.3.2. Administer Voice Codec on Media Gateways

The CS1000 uses Media Gateways to support traditional analog and digital phones for voice calls over the SIP Trunk. Media Gateways are also needed to support analog terminals to send fax over IP.

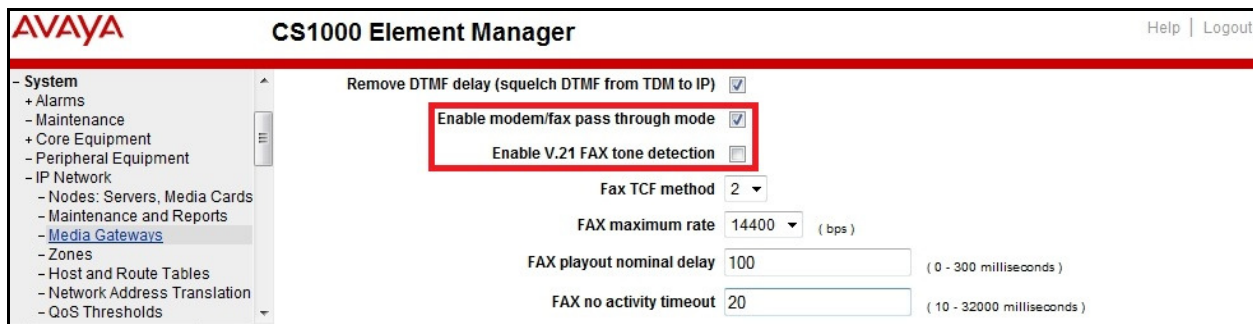
To configure the Voice Codec on Media Gateways, from the left menu of the Element Manager page (not shown), select the **IP Network → Media Gateways** menu item. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page (not shown).

Bell Canada supports voice codec G.711MU, payload size 20 ms, with VAD disabled. The screenshot below shows appropriated codec profile configured for Media Gateways.





For Fax over IP, Bell Canada supports G.711MU codec as default and does not support T.38. The following screenshot shows **Modem Pass Through** is selected for Media Gateways, this enables G.711MU codec to be used for fax calls between the CS1000 and Bell Canada. **Note:** The **V.21 Fax tone detection** should be unchecked to disable T.38 fax capability on the Media Gateway.



## 5.4. Administer Zones and Bandwidth

This section describes the steps to create 2 zones: zone **10** for VGW and IP phones, and zone **255** for the SIP Trunk. The CS1000 uses zone configuration for bandwidth management purposes.

Bell Canada supports only the G.711MU codec in the test environment. In the sample configuration as shown in the screenshots below, the **MO** zone **10** and **VTRK** zone **255** were configured with **Strategy Best Quality (BQ)** to allow the CS1000 to prioritize the G.711MU codec for both voice and fax calls. **Note:** In the fax call scenario, the call has to be established with the G.711MU codec otherwise it will fail because the CS1000 cannot switch the codec over to G.711MU.

In general, a bandwidth zone is configured with parameters described as the following:

- **INTRA\_STGY:** Bandwidth configuration for local calls.
- **INTER\_STGY:** Bandwidth configuration for calls over the SIP Trunk.
- **BQ:** G.711 is first choice and G.729 is second choice.
- **BB:** G.729 is first choice and G.711 is second choice.
- **MO:** The zone type which is used for IP phones and Voice Gateway (VGW).
- **VTRK:** The zone type which is used for the SIP Trunk.

### 5.4.1. Create Zone for VGW and IP phones

To create a MO zone **10** for VGW and IP phones, select **IP Network** → **Zones** from the left pane and then configure as follows:

- Click **Bandwidth Zones** link (not shown).
- In **Bandwidth Zones** screen, click **Add** button (not shown).
- In the **Add Bandwidth Zone** screen, click on **Zone Basic Property and Bandwidth Management**, select the values as shown (in red box) in the screenshot below and click on the **Submit** button (not shown).

Input Description	Input Value
Zone Number (ZONE):	10 ( 1 - 8000 )
Intrazone Bandwidth (INTRA_BW):	100000 ( 0 - 10000000 )
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	100000 ( 0 - 10000000 )
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

### 5.4.2. Create Zone for virtual SIP Trunk

Follow **Section 5.4.1** to create a VTRK zone **255** for the virtual trunk. The difference is in the **Zone Intent (ZBRN)** field, select **VTRK** for virtual trunk as shown in the screenshot below and then click the **Submit** button (not shown).

Input Description	Input Value
Zone Number (ZONE):	255 ( 1 - 8000 )
Intrazone Bandwidth (INTRA_BW):	100000 ( 0 - 10000000 )
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	100000 ( 0 - 10000000 )
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	

## 5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP Trunk between the CS1000 SSG and the Avaya SBCE.

### 5.5.1. Integrated Services Digital Network (ISDN)

To configure ISDN, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case it is **03**. The system can support more than one customer with different network settings and options. The **Customer 03 Edit** page will appear (not shown). Select the **Feature Packages** option from this page (not shown).

The screen is populated with a list of **Feature Packages**. Select **Integrated Services Digital Network** to edit its parameters. The screen is populated with **Integrated Services Digital Network** parameters as follows.

- Virtual private network identifier: Enter a valid value, e.g. **3**.
- Private network identifier: Enter a valid value, e.g. **3**.
- Node DN: Enter the Node DN, e.g. **2003**.

AVAYA CS1000 Element Manager Help | Logout

- Engineered Values  
+ Emergency Services  
+ Geographic Redundancy  
+ Software  
- **Customers**  
- Routes and Trunks  
- Routes and Trunks  
- D-Channels  
- Digital Trunk Interface  
- Dialing and Numbering Plans  
- Electronic Switched Network

- Integrated Services Digital Network Package: 145  
+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

- Virtual private network identifier: 3 (1 - 16383)  
- Private network identifier: 3 (1 - 16383)  
- Node DN: 2003

Multi-location business group: 0 (0 - 65535)

Retain the default values for all remaining fields. Scroll down to the bottom of the screen and click the **Save** button (not shown).

### 5.5.2. Administer SIP Trunk Gateway to the Avaya SBCE

To configure the SIP Trunk Gateway, select **IP Network → Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID 2003**. The **Node Details** screen is displayed as shown in Section 5.2.1.

On the **Node Details** screen, select **Gateway (SIPGw)** (not shown). Under **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values which are highlighted in red boxes as shown in screenshot below.

- **Vtrk gateway application:** Select **SIP Gateway (SIPGw)**.
- **SIP domain name:** An enterprise SIP Domain name, .e.g. **avaya.com**.
- **Local SIP port:** A port open to receive SIP traffic, .e.g. **5060**.
- **Gateway endpoint name:** A descriptive name for SIP Gateway, .e.g. **car2-ssg2**.
- **Application node ID:** An available node ID, .e.g. **2003**.



Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the IP address of Session Manager and the values highlighted in the red box as shown in the screenshot below. Retain the default values for the remaining fields.

On the same page, scroll down to the **SIP URI Map** section as shown in the screenshot below. The URI Map settings were set to blank to disable the “phone-context” from being sent because it is not required by Bell Canada.

Under the **Public E.164 Domain Names**:

- **National:** Set the field to blank.
- **Subscriber:** Set the field to blank.
- **Special Number:** Set the field to blank.
- **Unknown:** Set the field to blank.

Under the **Public E.164 Domain Names**:

- **UDP:** Set the field to blank.
- **CDP:** Set the field to blank.
- **Special Number:** Set the field to blank.

- **Vacant number:** Set the field to blank.
- **Unknown:** Set the field to blank.

**AVAYA CS1000 Element Manager** Help | Logout

**Node ID: 2003 - Virtual Trunk Gateway Configuration Details**

General | SIP Gateway Settings | SIP Gateway Services

**SIP URI Map:**

Public E.164 domain names		Private domain names	
National:	<input type="text"/>	UDP:	<input type="text"/>
Subscriber:	<input type="text"/>	CDP:	<input type="text"/>
Special number:	<input type="text"/>	Special number:	<input type="text"/>
Unknown:	<input type="text"/>	Vacant number:	<input type="text"/>
		Unknown:	<input type="text"/>

Then click the **Save** button (not shown) and synchronize the new configuration (see **Section 5.2.3**).

### 5.5.3. Administer Virtual D-Channel

To create a D-Channel, select **Routes and Trunks → D-Channels** from the left pane to display the **D-Channels** screen (not shown). In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list (not shown). Click on the **to Add** button (not shown).

The **D-Channels Property Configuration** of DCH **103** is shown in the screenshot below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D channel Card Type (CTYP):** D-Channel is over IP (**DCIP**).
- **Designator (DES):** A descriptive name.
- **Interface type for D-channel (IFC):** Meridian Meridian1 (**SL1**).
- **Meridian 1 node type:** Slave to the controller (**USR**).
- **Release ID of the switch at the far end (RLS):** **25**.

**AVAYA** CS1000 Element Manager Help | Logout

---

- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Geographic Redundancy
  - + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - **D-Channels**
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools
  - + Backup and Restore
  - Date and Time

### D-Channels 103 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	BellCanada
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> <span style="float: right;">more PRI</span>
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)

Click on **Basic Options** then click on the **Edit** button at the **Remote Capabilities (RCAP)** attribute (not shown). The **Remote Capabilities Configuration** page will appear. Check on the **ND2** and **MWI** checkboxes as shown in the screenshot below.

**AVAYA** CS1000 Element Manager Help | Logout

---

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Geographic Redundancy
  - + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - **D-Channels**
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools
  - + Backup and Restore

Remote D-channel is on a MSDSL card (MSL) ☐

Message waiting interworking with DMS-100 (MWI) ☒

Network access data (NAC) ☐

Network call trace supported (NCT) ☐

Network name display method 1 (ND1) ☐

Network name display method 2 (ND2) ☒

Network name display method 3 (ND3) ☐

Name display - integer ID coding (NDI) ☐

Name display - object ID coding (NDO) ☐

Path replacement uses integer values (PRI) ☐

Path replacement uses object identifier (PRO) ☐

Release Link Trunks over IP (RLTI) ☐

Remote virtual queuing (RVQ) ☐

Trunk anti-tromboning operation (TAT) ☐

User to user service 1 (UUS1) ☐

NI-2 name display option. (NDS) ☐

Message waiting indication using integer values (QMWI) ☐

Message waiting indication using object identifier (QMWO) ☐

User to user signalling (UUI) ☐

Return - Remote Capabilities

Cancel

Click the **Return – Remote Capabilities** button and then click the **Submit** button (not shown).

#### 5.5.4. Administer Virtual Super-Loop

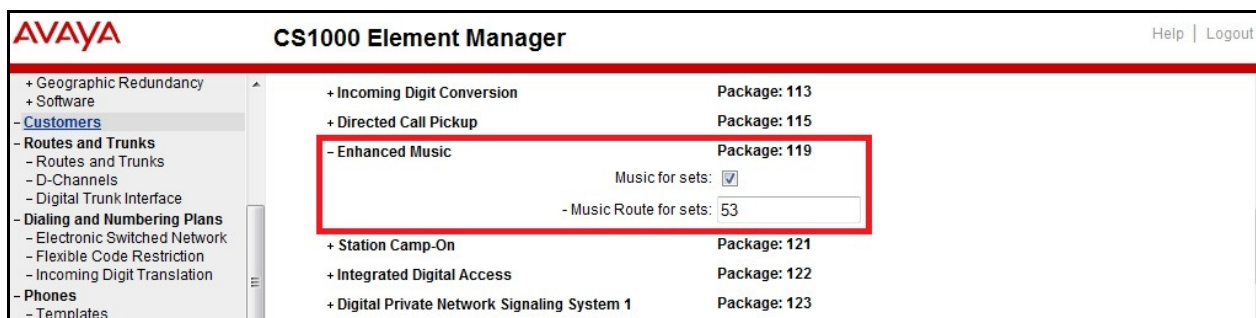
To add a virtual loop, select **System** → **Core Equipments** → **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click the **Add** button to create a new one as shown in the screenshot below. In this example, Superloop **100** was added.



#### 5.5.5. Enable Music for Customer Data Block

To enable music for a customer, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case it is **03**. The **Customer 03 Edit** page will appear (not shown). Select the **Feature Packages** option from this page (not shown).

The screen is populated with a list of **Feature Packages**. Select **Enhanced Music** to edit its parameters. Check **Music for sets** to enable music for Customer **03**, define music route **53** as shown in the red box of screenshot below. The CS1000 has been pre-configured with music route **53**.

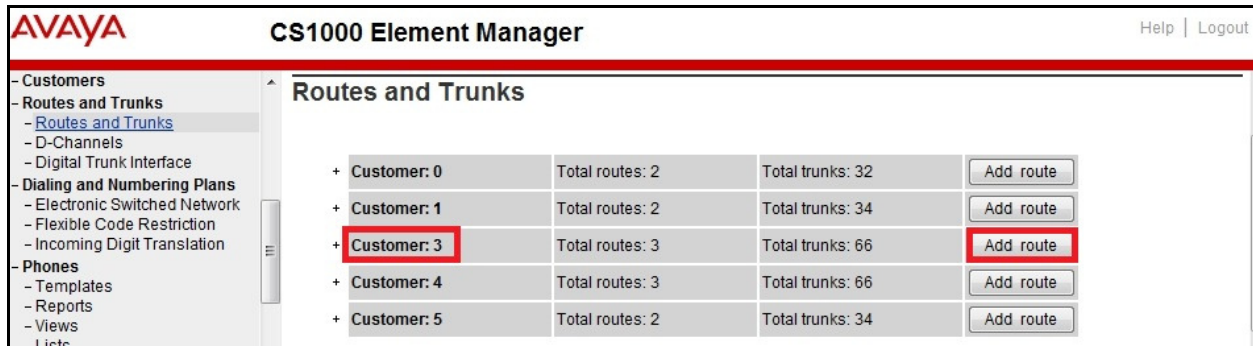


Scroll down to the bottom of the screen and click the **Save** button (not shown).

#### 5.5.6. Administer Virtual SIP Route

To create a SIP Route, select **Routes and Trunks** → **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 03** was added. Click the **Add route** button as shown in the screenshot below.





The **Customer 3**, New **Route Configuration** screen is displayed (not shown). Scroll down until the **Basic Configuration** section is displayed and enter the following values for the specified fields. Retain the default values for the remaining fields as shown in the screenshot below.

- **Route Number (ROUT):** Select an available route number.
- **Designator field for trunk (DES):** A descriptive text.
- **Trunk Type (TKTP):** TIE trunk data block (TIE).
- **Incoming and Outgoing trunk (ICOG):** Incoming and Outgoing (IAO).
- **Access Code for the trunk route (ACOD):** An available access code.
- Check the field **The route is for a virtual trunk route (VTRK)**, to enable additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter zone **255** (created in Section 5.4.2).
- For the **Node ID of signalling server of this route (NODE)** field, enter the node number **2003** (created in Section 5.2.1).
- Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields.
  - **Mode of operation (MODE):** Route uses ISDN Signalling Link (ISLD).
  - **D channel number (DCH):** D-Channel number **103** (created in Section 5.5.3).
  - **Network calling name allowed (NCNA):** Checked.
  - **Network call redirection (NCRD):** Checked.
  - **Insert ESN access code (INAC):** Checked.
  - **Mobile extension outgoing type (MBXOT):** Select **National number (NPA)**.
  - **Mobile extension timer (MBXT):** Define an appropriate value to meet the certain deployment at enterprise network. For this compliance test, a value of 1000ms is used to determine if the outgoing call to MobX is answered by cellular voice mail within 1000ms then the answering will be ignored. The caller will be connected to Call Pilot to leave a voice message to enterprise mail box of the desk phone user. For more information, please refer to **Section 2.2**, observation **#11**.  
**Note:** Patch MPLR32246 is required to make Cellular Voice Mail Avoidance function properly.
  - **Calling number dialling plan (CNDP):** National (NATL).

**AVAYA** CS1000 Element Manager Help | Logout

---

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
  - + Alarms
  - + Maintenance
  - + Core Equipment
  - + Peripheral Equipment
  - + IP Network
  - + Interfaces
  - + Engineered Values
  - + Emergency Services
  - + Geographic Redundancy
  - + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools
  - + Backup and Restore
  - + Date and Time
  - + Logs and reports
- Security
  - + Passwords
  - + Policies
  - + Login Options

### Customer 3, Route 103 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE):   
 Customer number (CUST):   
 Route number (ROUT):   
 Designator field for trunk (DES):   
 Trunk type (TKTP):   
 Incoming and outgoing trunk (ICOG):   
 Access code for the trunk route (ACOD):   
 Trunk type M911P (M911P): ☐  
 The route is for a virtual trunk route (VTRK): ☒  
 - Zone for codec selection and bandwidth management (ZONE):  (0 - 8000)  
 - Node ID of signaling server of this route (NODE):  (0 - 9999)  
 - Protocol ID for the route (PCID):   
 - Print correlation ID in CDR for the route (CRID): ☐

Integrated services digital network option (ISDN): ☒  
 - Mode of operation (MODE):   
 - D channel number (DCH):  (0 - 254)  
 - Interface type for route (IFC):   
 - Private network identifier (PNI):  (0 - 32700)  
 - Network calling name allowed (NCNA): ☒  
 - Network call redirection (NCRD): ☒  
 - Trunk route optimization (TRO): ☐  
 - Recognition of DTI2 ABCD FALT signal for ISL (FALT): ☐  
 - Channel type (CHTY):   
 - Call type for outgoing direct dialed TIE route (CTYP):   
 - Insert ESN access code (INAC): ☒

- Integrated service access route (ISAR): ☐  
 - Display of access prefix on CLID (DAPC): ☐  
 - Mobile extension route (MBXR): ☐  
 - Mobile extension outgoing type (MBXOT):   
 - Mobile extension timer (MBXT):  (0 - 8000 milliseconds)  
 Calling number dialing plan (CNDP):

Click on **Basic Route Options**, check **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)** and input **DCNO 0** for both Day IDC Tree Number and Night IDC Tree Number as shown in screenshot below. The IDC is discussed in **Section 5.6.5**.

**AVAYA** CS1000 Element Manager Help | Logout

---

- Customers
- Routes and Trunks
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists

- - Number of digits printed (NDP):

North American toll scheme (NATL): ☒

Controls or timers (CNTL): ☐

Conventional (Tie trunk only) (CNVT): ☐

Incoming DID digit conversion on this route (IDC): ☒  
 - Day IDC tree number (DCNO):  (0 - 254)  
 - Night IDC tree number (NDNO):  (0 - 254)

- Display external dialed digits (DEXT): ☐

Click on **Advance Configurations**; check **Music-on-hold (MUS)** to enable music on hold for the route. Input **Music route number (MRT) 53** in the box as shown in the screenshot below. The CS1000 has been pre-configured with route **53** as a music route.

AVAYA CS1000 Element Manager

Help | Logout

- Routes and Trunks

- Routes and Trunks
- D-Channels
- Digital Trunk Interface

- Dialing and Numbering Plans

- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation

- Phones

- Templates
- Reports
- Views
- Lists
- Properties

Manual outgoing trunk route (MANO): ☐

Manual route (MNL): ☐

Music on-hold (MUS): ☒

- Music route number (MRT): 53 (0 - 511)

Outgoing identifier send (OGIS): ☒

Off-hook timer delay (OHTD): ☐

Outpulsing route (OPR): ☐

Pseudo answer (PANS): ☒

Periodic clearing signal (PECL): ☐

Click the **Submit** button (not shown).

### 5.5.7. Administer Virtual SIP Trunks

To configure the virtual SIP Trunks, select **Route 103** that was added in **Section 5.6.6** and then click the **Add trunk** button next to the newly added **Route 103** as shown in the screenshot below.

AVAYA CS1000 Element Manager

Help | Logout

- Routes and Trunks

- Routes and Trunks
- D-Channels
- Digital Trunk Interface

- Dialing and Numbering Plans

- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation

- Phones

- Templates
- Reports
- Views
- Lists
- Properties

Routes and Trunks

Customer	Total routes	Total trunks	Add route
+ Customer: 0	Total routes: 2	Total trunks: 32	Add route
+ Customer: 1	Total routes: 2	Total trunks: 34	Add route
- Customer: 3	Total routes: 3	Total trunks: 66	Add route

Route	Type	Description	Edit	Add trunk
+ Route: 53	Type: MUS	Description: MUSIC	Edit	Add trunk
Route: 103	Type: TIE	Description: BELLCANADA	Edit	Add trunk
	Type: TIE	Description: BELLCANADA	Edit	Add trunk

The **Customer 3, Route 103, Trunk 1 Property Configuration** is shown in the screenshot below. Enter the **Multiple trunk input number (MTINPUT)** field to add multiple trunks in a single operation, or repeat the operation for each trunk. In the certification testing, 32 trunks were created (not shown). The following values were entered for specified fields and retain the default values for the remaining fields.

- **Trunk data block: IP Trunk (IPTI).**
- **Terminal Number:** Available terminal number (created in **Section 5.5.4**).
- **Designator field for trunk:** A descriptive text.
- **Extended Trunk:** Virtual trunk (**VTRK**).
- **Member number:** Current route number and starting member.
- **Start arrangement Incoming: Immediate (IMM).**
- **Start arrangement Outgoing: Immediate (IMM).**
- **Trunk Group Access Restriction:** Desired trunk group access restriction level, e.g. **1**.
- **Channel ID for this trunk:** An available starting channel ID, e.g. **1**.

**AVAYA** CS1000 Element Manager Help | Logout

**Customer 3, Route 103, Trunk 1 Property Configuration**

**- Basic Configuration**

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service: **Edit**

The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service** (CLS) at the bottom of the basic trunk configuration page. Click the **Edit** button to configure (not shown). For **Media Security**, select **Media Security Never (MSNV)**. Select **Restriction level** as **Unrestricted (UNR)**. The remaining values are kept as default as shown in the screenshot below. Scroll down to the bottom of the screen and click **Return Class of Service** and then click the **Save** button (not shown).

**AVAYA** CS1000 Element Manager Help | Logout

**Customer 3, Route 103, Trunk 1 Property Configuration**

**- Manual Incoming:**

**-Media Security:**

**-Network Hook Flash Over M911P:**

**- Polarity:**

**- Priority:**

**- Restriction level:**

**- Reversed Ear Piece:**

**- Short or long line:**

**- Transmission Class of Service:**

**- Warning Tone:**

**- Reversed Ear Piece:**

**- ARF Supervised COT:**

**Return Class of Service**

### 5.5.8. Administer Calling Line Identification Entry

To create Calling Line Identification Entry, select **Customers > 03 > ISDN and ESN Networking**. Click the **Calling Line Identification Entries** link at the bottom of the page (not shown).



On the Calling Line Identification Entries page (not shown), click **Add**. Add entry **0** as shown in the screenshot below.

- **National Code:** Leave as blank.
- **Local Code:** Input a prefix what was assigned by the service provider, in this case it is 6 digits, **416XXX**. This **Local Code** is used for call display purposes of the outgoing call configuration in **Section 5.6.6** where the Special Number is associated with Call Type = NONE.
- **Home Location Code:** Input a prefix that was assigned by the service provider, in this case it is 6 digits, **416XXX**. This **Home Location Code** is used for call display purposes of the outgoing call configuration in **Section 5.6.6** where the Special Number is associated with Call Type = National (NPA).
- **Local Steering Code:** Input a prefix that was assigned by the service provider, in this case it is 6 digits, **416XXX**. This **Local Steering Code** is used for call display purposes of the outgoing call configuration in **Section 5.6.6** where the Special Number is associated with Call Type = National (NXX).
- **Use DN as DID:** Select **YES**.
- **Calling Party Name Display:** Uncheck the **Roman characters** field.
- Click the **Save** button (not shown).

**AVAYA CS1000 Element Manager** Help | Logout

**Edit Calling Line Identification 0**

**General Properties**

National Code:  (0 - 999999)  
Code for national home number

Local Code:  416 (1-12 digits)  
Code for home local number or listed DN

Home Location Code:  416 (1-7 digits)

Local Steering Code:  416 (1-7 digits)

Use DN as DID: ☒ YES

**Emergency Services Access**

Emergency Local Code:  (1-12 digits)  
Code for home local number during Emergency calls

Emergency Options: ☐ Home national number for emergency services access calls  
☒ Append the originating directory number for emergency services access calls

**Calling Party Name Display**

Roman characters: ☐

CPND Name:   
first name, last name

Expected Length:

Display Format:  First name, Last name

### 5.5.9. Enable External Trunk to Trunk Transferring

This section shows how to enable the **External Trunk to Trunk Transferring** feature which is a mandatory configuration to make call transfers and conferencing work properly over the SIP Trunk.

- Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail).
- Allow **External Trunk To Trunk Transferring** for **Customer Data Block** by using **LD 15**.
- Set **TRNX** to **YES**.
- Set **EXTT** to **YES**.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600176      USED U P: 8325631 954062      TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 3
OPT
...
TRNX YES
EXTT YES
...
```

## 5.6. Administer Dialing Plans

### 5.6.1. Define ESN Access Codes and Parameters (ESN)

To configure ESN parameters, select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **ESN Access Code and Parameters (ESN)** as shown in the screenshot below.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left pane contains a navigation tree with the following structure:

- UCM Network Services
  - Home
  - Links
    - Virtual Terminals
  - System
    - + Alarms
    - Maintenance
    - + Core Equipment
    - Peripheral Equipment
    - + IP Network
    - + Interfaces
    - Engineered Values
    - + Emergency Services
    - + Geographic Redundancy
    - + Software
  - Customers
  - Routes and Trunks
    - Routes and Trunks
    - D-Channels
    - Digital Trunk Interface
  - Dialing and Numbering Plans
    - **Electronic Switched Network** (highlighted)
    - Flexible Code Restriction
    - Incoming Digit Translation
  - Phones
    - Templates
    - Reports
    - Views
    - Lists
    - Properties
    - Migration
  - Tools

The main pane displays the **Electronic Switched Network (ESN)** configuration screen. It shows a tree of parameters for three customers: Customer 00, Customer 01, and Customer 03. Under Customer 03, the following parameters are listed:

- Network Control & Services
  - Network Control Parameters (NCTI)
  - **ESN Access Codes and Parameters (ESN)** (highlighted)
  - Digit Manipulation Block (DGT)
  - Home Area Code (HNPA)
  - Flexible CLID Manipulation Block (CMDB)
  - Free Calling Area Screening (FCAS)
  - Free Special Number Screening (FSNS)
  - **Route List Block (RLB)** (highlighted)
  - Incoming Trunk Group Exclusion (ITGE)
  - Network Attendant Services (NAS)
- Coordinated Dialing Plan (CDP)
  - Local Steering Code (LSC)
  - Distant Steering Code (DSC)
  - Trunk Steering Code (TSC)
- Numbering Plan (NET)
  - Access Code 1
    - Home Location Code (HLOC)
    - Location Code (LOC)
    - **Numbering Plan Area Code (NPA)** (highlighted)
    - **Special Number (SPN)** (highlighted)
    - Network Speed Call Access Code (NSCL)
  - Access Code 2

In the **ESN Access Codes and Basic Parameters** page, define **NARS/ BARS Access Code 1** and disable **Check for Trunk Group Access Restrictions** as shown in the screenshot below.

Click the **Submit** button (not shown).

### 5.6.2. Associate NPA and SPN calls to ESN Access Code 1

This section shows the configuration to associate the NPA and SPN to ESN Access Code 1.

- Login to the Call Server CLI (refer to **Section 5.1.2** for more detail).
- In **LD 15**, change Customer Net\_Data block by disabling NPA and SPN to be associated to Access Code 2. It means Access Code 1 will be used for NPA and SPN calls.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600086      USED U P: 8325631 954152      TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 3
OPT
AC2 xNPA xSPN
FNP
CLID
...
```

Verify Customer Net\_Data block by using **LD 21**.

```
>ld 21
PT1000

REQ: prt
TYPE: net
```

```

TYPE NET_DATA
CUST 3

TYPE NET_DATA
CUST 01
OPT RTA
AC1 INTL NPA SPN NXX LOC
AC2
FNP YES
...

```

### 5.6.3. Administer Digit Manipulation Block (DMI)

To create a DMI entry, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Then select **Digit Manipulation Block (DGT)** (not shown).

In the **Choose a DMI Number** field, select an available DMI from the drop-down list and click to **Add** (not shown). The screenshot below shows **DMI 1** is created with the following values.

- **Number of leading digits to be Deleted (Del): 0.**
- **Call Type to be used by the manipulated digits (CTYP): NPA (NPA).**
- Click the **Submit** button

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with the following items: Customers, Routes and Trunks (with sub-items: Routes and Trunks, D-Channels, Digital Trunk Interface), Dialing and Numbering Plans (with sub-items: Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation), Phones (with sub-items: Templates, Reports, Views, Lists, Properties, Migration), and Migration. The main area is titled 'Digit Manipulation Block'. It contains several input fields: 'Digit Manipulation Index numbers' with the value '1', 'Number of leading digits to be deleted' with the value '0' and a range '( 0 - 19 )', an 'Insert' field, and 'IP Special Number' with a checkbox. A dropdown menu for 'Call Type to be used by the manipulated digits' is set to 'NPA (NPA)'. At the bottom right, there are four buttons: 'Submit', 'Refresh', 'Delete', and 'Cancel'. The 'Submit' button is highlighted with a red box.

### 5.6.4. Administer Route List Block (RLB)

This section shows how to add a RLB associated with the **DMI 1** created in **Section 5.6.3**.

To create **RLB 103** for the certification testing, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen then select **Route List Block (RLB)** as shown in **Section 5.6.1**.

Select an available value, e.g. **103** in the textbox for the **route list index** and click on the **to Add** button (not shown). Enter the following values for the specified fields as shown in the screenshot below, and retain the default values for the remaining fields.

- **Route number (ROUT): 103** (created in **Section 5.5.6**).

- **Digit Manipulation Index (DMI): 1** (created in Section 5.6.3).

**AVAYA CS1000 Element Manager** Help | Logout

**Route List Block**

**General Properties**

Number of Alternate Routing Attempts: 5 (1 - 10)

Initial Set: 0 (0 - 64)

Set Minimum Facility Restriction Level:

Overlap Length: 0 (0 - 24)

Extended Local Calls: ☐

**Route List Index: 103**

Entry Number for the Route List: 0 (0 - 63)

**Indexes**

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

**Digit Manipulation Index: 1**

ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1999)

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: ☐

Incoming CLID Table: 0 (0 - 256)

**Options**

Local Termination entry: ☐

**Route Number: 103**

Skip Conventional Signaling: ☐

On the same page, scroll down to the bottom of the screen and click the **Submit** button (not shown).

### 5.6.5. Administer Incoming Digit Translation (IDC)

This section describes the steps for receiving calls from the PSTN via the Bell Canada network.

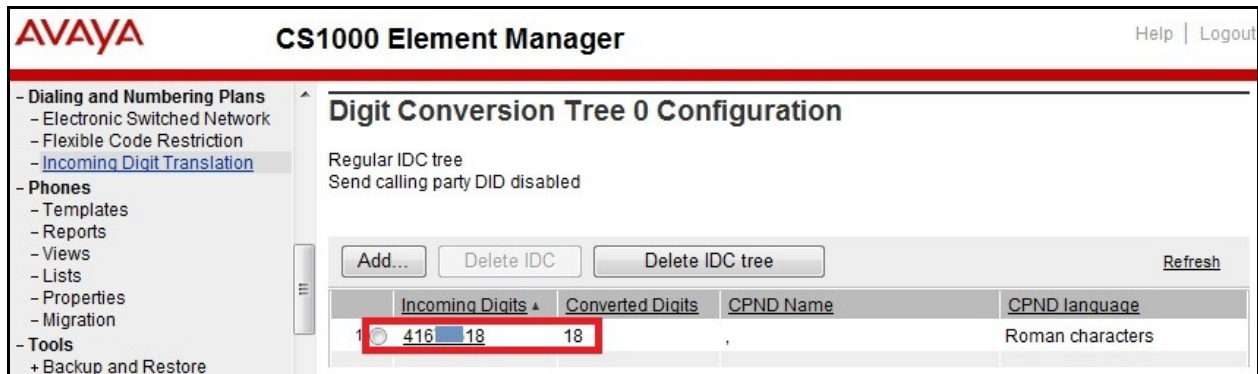
To create an IDC, select **Dialing and Numbering Plans** → **Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen then click on the **Edit IDC** button (not shown).

Click on **New DCNO** to create a digit translation entry. In this example, **Digit Conversion Tree Number (DCN0) 0** was created. Detailed configuration of the **DCNO** is shown in screenshot below. The **Incoming Digits** can be added to map to the **Converted Digits** which



would be the CS1000 DN. This **DCN0** has been assigned to Route **103** as shown in **Section 5.5.6**.

In the following configuration, incoming calls from the PSTN with prefix **416XXX18XX** will be translated to CS1K DN **18XX**, including the DID **416XX1883** which is translated to **1883** for Call Pilot voice mail access purpose.



### 5.6.6. Administer Outbound Call - Special Number

Special Number is configured to be used for this testing. For example, **0** to reach service provider operator, **0+10** digits to reach service provider operator assistant, **011** prefix for international calls, **1** for national long distance calls, **411** for directory assistant and so on.

To create a Special Number, select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Then select **Special Number (SPN)** (not shown).

Enter the SPN value and then click on the **to Add** button (not shown). The screenshot below shows all the Special Numbers used for this testing.

Special Number: **0**

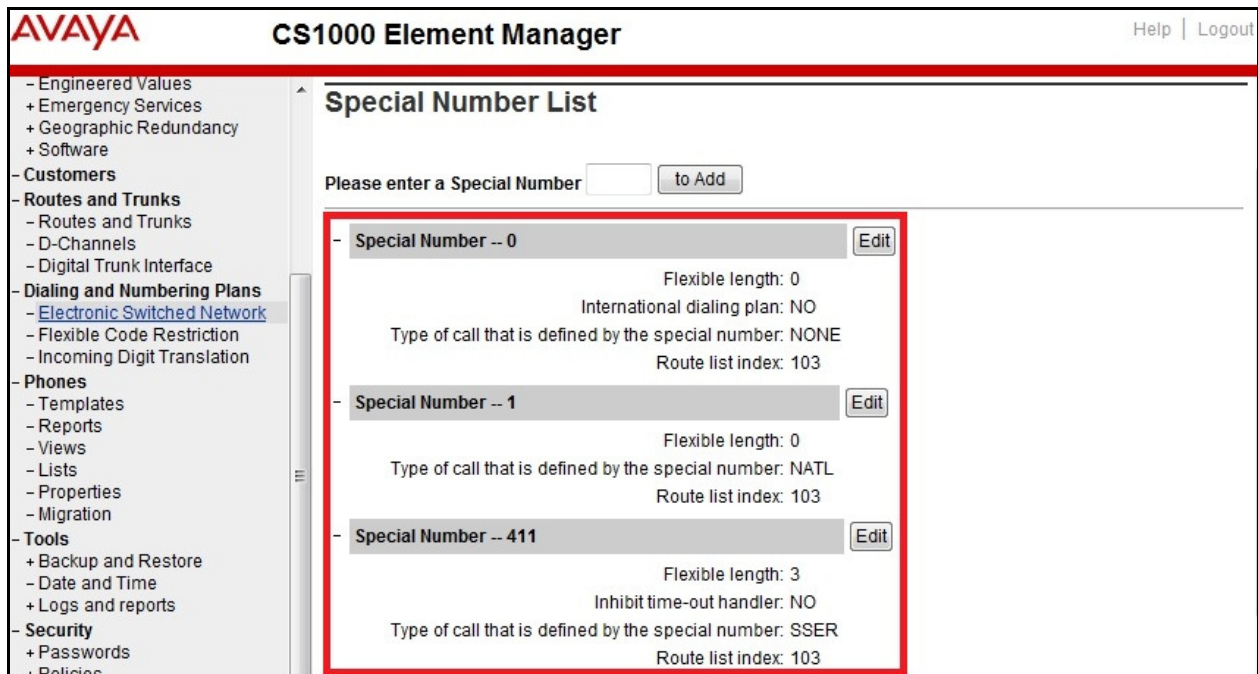
- **Flexible length: 0** (flexible, unlimited and accept the character # to ending dial number).
- **Call Type: NONE.**
- **Route list index: 103**, created in **Section 5.6.4**.

Special Number: **1**

- **Flexible length: 0** (flexible, unlimited and accept the character # to ending dial number).
- **Call Type: NATL.**
- **Route list index: 103**, created in **Section 5.6.4**.

Special Number: **411**

- **Flexible length: 3.**
- **CallType: SSER.**
- **Route list index: 103**, created in **Section 5.6.4**.



### 5.6.7. Administer Outbound Call - Numbering Plan Area (NPA)

This section describes the creation of NPA numbers used in this testing configuration.

To create an NPA number, select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Select **Numbering Plan Area Code (NPA)** (not shown).

Enter the area code(s) desired in the textbox and click the **to Add** button (not shown). The screenshot below shows NPA numbers **416**, **647** and **905** that were configured for this testing. These NPA numbers are associated to the SIP Trunk for 10-digit outgoing local calls.

- Engineered Values
- + Emergency Services
- + Geographic Redundancy
- + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - [Electronic Switched Network](#)
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration

## Numbering Plan Area Code List

Please enter an area code

- **Numbering Plan Area Code -- 416** 
  - Route List Index: 103
  - Incoming Trunk group Exclusion Index: NONE
- **Numbering Plan Area Code -- 647** 
  - Route List Index: 103
  - Incoming Trunk group Exclusion Index: NONE
- **Numbering Plan Area Code -- 905** 
  - Route List Index: 103
  - Incoming Trunk group Exclusion Index: NONE



## 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.
- SIP Entities corresponding to the CS1000, Session Manager and the 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, Location(s), 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.

Avaya Aura® System Manager 6.3

Last Logged on at April 3, 2013 10:20 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Home](#)

**Users**

**Administrators**  
Manage Administrative Users

**Directory Synchronization**  
Synchronize users with the enterprise directory

**Groups & Roles**  
Manage groups, roles and assign roles to users

**User Management**  
Manage users, shared user resources and provision users

**Elements**

**B5800 Branch Gateway**  
Manage B5800 Branch Gateway 6.2 elements

**Communication Manager**  
Manage Communication Manager 5.0 and higher elements

**Communication Server 1000**  
Manage Communication Server 1000 elements

**Conferencing**  
Manage Conferencing Multimedia Server objects

**Inventory**  
Manage, discover, and navigate to elements, update element software

**Meeting Exchange**  
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

**Messaging**  
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

**Presence**  
Presence

**Routing**  
Session Manager Routing Administration

**Session Manager**  
Session Manager Administration, Status, Maintenance and Performance Management

**Services**

**Backup and Restore**  
Backup and restore System Manager database

**Bulk Import and Export**  
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

**Configurations**  
Manage system wide configurations

**Events**  
Manage alarms, view and harvest logs

**Geographic Redundancy**  
Manage Geographic Redundancy

**Licenses**  
View and configure licenses

**Replication**  
Track data replication nodes, repair replication nodes

**Scheduler**  
Schedule, track, cancel, update and delete jobs

**Security**  
Manage Security Certificates

**Shutdown**  
Shutdown System Manager Gracefully

**Templates**  
Manage Templates for Messaging System objects

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen. The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

Avaya Aura® System Manager 6.3

Last Logged on at April 3, 2013 10:20 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing

**Introduction to Network Routing Policy**

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.  
  
The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:  
  
Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).  
Step 2: Create "Locations"  
Step 3: Create "Adaptations"  
Step 4: Create "SIP Entities"  
  
- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"

## 6.2. Specify SIP Domain

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

The following screen shows the list of configured SIP domains. The domain **avaya.com** is an enterprise private SIP domain that was defined to route incoming calls to the CS1000. Incoming calls were received with the service provider public SIP domain **cust6xxxx.xxxx.bell.ca** which will be translated by the Avaya SBCE to **avaya.com** to route to Session Manager. For outgoing calls, Bell Canada requires the value of the trunk group (tgrp) to be **vsxx-416XXX1880-01a** as presented in the “Contact” header. The “tgrp” was added by the Avaya SBCE (see **Section 7.2.5**). The enterprise SIP domain **avaya.com** will be translated by the Avaya SBCE to **sipxxxxxxxx.bell.ca** to route to the Bell Canada network.



## 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, 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 screenshots for the location **Belleville** which includes all equipment on the **10.10.97.\***, **10.10.98.\*** and **10.33.10.\*** subnets including the CS1000, Session Manager, the Avaya SBCE and IP phones. Click **Commit** to save.

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at April 3, 2013 10:20 AM

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

Routing

Home

Home / Elements / Routing / Locations

Help ?

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Location Details

Commit

Cancel

General

\* Name:

Belleville

Notes:

GSSCP Belleville

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

10000000

Multimedia Bandwidth:

10000000

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

10000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

10000

Kbit/Sec

\* Minimum Multimedia Bandwidth:

64

Kbit/Sec

\* Default Audio Bandwidth:

80

Kbit/sec

Location Pattern

Add

Remove

3 Items

Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.10.*	
<input type="checkbox"/>	* 10.10.97.*	
<input type="checkbox"/>	* 10.10.98.*	

Select : All, None

## 6.4. Add SIP Entities

A **SIP Entity** must be added for Session Manager and for each SIP telephony system connected to Session Manager, which includes the CS1000 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, and **Other** for the CS1000 and the Avaya SBCE.
- **Location:** Select the Location defined previously.
- **Time Zone:** Select the time zone for the Location above.

The following screen shows the addition of the SIP Entity for Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**. The **SIP Link Monitoring** is kept as default **Use Session Manager Configuration**.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'SIP Entities' option selected under the 'Routing' category. The main content area is titled 'SIP Entity Details' and includes a 'Commit' button. The 'General' tab is active, showing the following configuration details:

- Name:** SPSM63
- FQDN or IP Address:** 10.33.10.26
- Type:** Session Manager
- Notes:** GSSCP SM63
- Location:** Belleville
- Outbound Proxy:** (empty field)
- Time Zone:** America/Toronto
- Credential name:** (empty field)

Below the 'General' section, the 'SIP Link Monitoring' section shows 'Use Session Manager Configuration' selected from a dropdown menu.

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 Session Manager will 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 testing used **Port** entry **TCP/5060** connecting to the CS1000 for internal enterprise calls. The **Port** entry **UDP/5060** is for connecting to the Avaya SBCE for external PSTN calls.

**Port**

TCP Failover port:

TLS Failover port:

---

5 Items | [Refresh](#) Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avayalab.com	
<input type="checkbox"/>	5060	UDP	avayalab.com	

The following section shows the addition of the SIP Entity **CS1K** for the CS1000. The **FQDN or IP Address** field is set to the IP address of the CS1000 as **10.10.97.158**. Select **Type** as **Other**. In the compliance testing, a single SIP Entity was created for both incoming and outgoing calls in association with the SIP Trunk created on the CS1000 in **Section 5.5**. The **SIP Link Monitoring** was set to **Use Session Manager Configuration**, which is the default. This setting allows Session Manager to periodically send OPTIONS heartbeats to check the status of the SIP Trunk.

**AVAYA** Avaya Aura® System Manager 6.3 Last Logged on at April 4, 2013 1:47 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

---

Home / Elements / Routing / SIP Entities [Help ?](#)

**SIP Entity Details**

**General**

\* Name: CS1K

\* FQDN or IP Address: 10.10.97.158

Type: Other

Notes: CS1K for Bell cust6

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS ☐

SRV:

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

The following screens show the addition of the SIP Entity **SBCE** for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the private network interfaces for the Avaya SBCE as **10.10.97.189**. The **SIP Link Monitoring** was set to **Link Monitoring Enabled**



where the **Proactive Monitoring Interval** and **Reactive Monitoring Interval** were set to 60 seconds. This setting allows Session Manager to send OPTIONS heartbeats to check the status of the SIP Trunk, every 60 seconds.

**AVAYA** Avaya Aura® System Manager 6.3

Last Logged on at April 4, 2013 1:47 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

**Routing** \* **Home**

**Home / Elements / Routing / SIP Entities**

**SIP Entity Details** **Commit** **Cancel**

**General**

\* **Name:** SBCE

\* **FQDN or IP Address:** 10.10.97.189

**Type:** Other

**Notes:** SBCE for Bell cust6

**Adaptation:**

**Location:** Belleville

**Time Zone:** America/Toronto

**Override Port & Transport with DNS**

**SRV:**

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

**Credential name:**

**Call Detail Recording:** none

**CommProfile Type Preference:**

**SIP Link Monitoring**

**SIP Link Monitoring:** Link Monitoring Enabled

\* **Proactive Monitoring Interval (in seconds):** 60

\* **Reactive Monitoring Interval (in seconds):** 60

\* **Number of Retries:** 5

## 6.5. Add Entity Links

A SIP Trunk between Session Manager and a telephony system is described by an **Entity Link**. From Session Manager to the CS1000, one Entity Link was created for internal enterprise traffic. Session Manager will also have one Entity Link to the Avaya SBCE for external service provider traffic.

To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the CS1000, this must match the SIP Trunk configuration in **Section 5.5**.

- **SIP Entity 2:** Select the name of the other system. For the CS1000, select the SIP Entity **CS1K** defined in **Section 6.4**. For the Avaya SBCE, select the SIP Entity **SBCE** defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For the CS1000, this must match the SIP Trunk configuration in **Section 5.5**.
- **Connection Policy:** Select **Trusted**. **Note:** If **Trusted** is not selected, all calls from the associated SIP Entity specified in **Section 6.4** will be challenged for authentication.

Click **Commit** to save (not shown).

The following screenshots illustrate the Entity Links from Session Manager to the CS1000 and the Avaya SBCE.

Entity Links between Session Manager and the CS1000 for enterprise calls on **Port** entry **TCP/5060**:

The screenshot shows the 'Entity Links' configuration interface. At the top, there are 'Add' and 'Remove' buttons. Below them, it says '1 Item | Refresh' and 'Filter: Enable'. The main table has the following columns: SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. A single row is highlighted with a red border, showing the configuration for the link between SPSM63 and CS1K using TCP on port 5060 with a Trusted connection policy. The 'Deny New Service' checkbox is unchecked. At the bottom, there is a 'Select : All, None' option.

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	SPSM63	TCP	* 5060	CS1K	* 5060	Trusted	<input type="checkbox"/>

Select : All, None

Entity Links between Session Manager and the Avaya SBCE for service provider calls on **Port** entry **UDP/5060**:

The screenshot shows the 'Entity Links' configuration interface. At the top, there are 'Add' and 'Remove' buttons. Below them, it says '1 Item | Refresh' and 'Filter: Enable'. The main table has the following columns: SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. A single row is highlighted with a red border, showing the configuration for the link between SPSM63 and SBCE using UDP on port 5060 with a Trusted connection policy. The 'Deny New Service' checkbox is unchecked. At the bottom, there is a 'Select : All, None' option.

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	SPSM63	UDP	* 5060	SBCE	* 5060	Trusted	<input type="checkbox"/>

Select : All, None



## 6.6. Add Routing Policies

**Routing Policies** describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. A separate Routing Policy was added to route both incoming calls to the CS1000 and outgoing calls to 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). Fill in the following values on the new screen that is displayed:

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 used in the compliance testing.

Routing Policy **Inbound\_Bell\_cust6** for incoming calls to the CS1000:

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane has 'Routing Policies' highlighted. The main area displays the 'Routing Policy Details' for 'Inbound\_Bell\_cust6'. The 'General' section includes fields for Name, Disabled, Retries, and Notes. The 'SIP Entity as Destination' section has a 'Select' button and a table showing the selected entity 'CS1K' with FQDN '10.10.97.158' and Type 'Other'. The 'Commit' and 'Cancel' buttons are at the top right.

Name	FQDN or IP Address	Type	Notes
CS1K	10.10.97.158	Other	CS1K for Bell cust6

Routing Policy **Outbound\_Bell\_cust6** for outgoing calls to the Avaya SBCE:

Avaya Aura® System Manager 6.3

Last Logged on at April 4, 2013 1:47 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

Home / Elements / Routing / Routing Policies

Routing Policy Details

**General**

\* Name: Outbound\_Bell\_cust6

Disabled: ☐

\* Retries: 0

Notes: Outbound to Bell cust6

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
SBCE	10.10.97.189	Other	SBCE for Bell cust6

**Commit** **Cancel**

## 6.7. Add Dial Patterns

**Dial Patterns** are needed to route specific calls through Session Manager. For the compliance testing, Dial Patterns were needed to route calls from the CS1000 to Bell Canada and vice versa. Dial Patterns define which Routing 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 testing are shown below, one for outgoing calls from the enterprise to the PSTN and one for incoming calls from the PSTN to the enterprise. Other outgoing dial patterns e.g. **011** international calls, **411** directory assistance calls, etc., were similarly defined.

The first example shows a Dial Pattern for incoming calls that contain 10-digit DID numbers that start with **416XXX** to SIP domain **avaya.com** (after being translated by the Avaya SBCE from the service provider public SIP domain **cust6xxxx.xxxx.bell.ca**). The Dial Pattern uses the Route Policy **Inbound\_Bell\_cust6** as defined in **Section 6.6**. These DID numbers are assigned to the enterprise by Bell Canada.

**AVAYA** Avaya Aura® System Manager 6.3

Last Logged on at April 4, 2013 1:47 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details** [Commit](#) [Cancel](#) [Help ?](#)

**General**

\* **Pattern:** 416  
 \* **Min:** 10  
 \* **Max:** 10

**Emergency Call:** ☐  
**Emergency Priority:** 1  
**Emergency Type:**  
**SIP Domain:** avaya.com  
**Notes:** Inbound from Bell cust6

**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 checked="" type="checkbox"/>	Belleville	GSSCP Belleville	Inbound_Bell_cust6	0	<input type="checkbox"/>	CS1K	Inbound from Bell cust6

Select : All, None

The second example shows the Dial Pattern for outgoing calls that contain 11-digit dialed numbers that begin with the digit **1**. The Dial Pattern uses Routing Policy **Outbound\_Bell\_cust6** as defined in **Section 6.6** to route outgoing calls to the Avaya SBCE.

**AVAYA** Avaya Aura® System Manager 6.3 Last Logged on at April 4, 2013 1:47 PM  
Help | About | Change Password | **Log off**  
admin

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

**Routing** ▾ [Home / Elements / Routing / Dial Patterns](#) [Help ?](#)

**Dial Pattern Details** **Commit**

**General**

\* **Pattern:** 1

\* **Min:** 11

\* **Max:** 11

**Emergency Call:** ☐

**Emergency Priority:** 1

**Emergency Type:**

**SIP Domain:** avaya.com

**Notes:** Outbound to Bell cust6

**Originating Locations and Routing Policies**

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	GSSCP Belleville	Outbound_Bell_cust6	0	<input type="checkbox"/>	SBCE	Outbound to Bell cust6

Select : All, None

## 6.8. Add/View Avaya Aura® 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.

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.

In the **Monitoring** section, verify **Enable Monitoring** is checked.

Use default values for the remaining fields and then click **Save** (not shown).

The screenshots below show the Session Manager values.



AVAYA Avaya Aura® System Manager 6.3

Last Logged on at April 4, 2013 1:47 PM  
Help | About | Change Password | Log off admin

Session Manager x Home

Home / Elements / Session Manager / Session Manager Administration

Help ?

**View Session Manager** Return

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |  
Expand All | Collapse All

General

SIP Entity Name SPSM63  
Description GSSCP SM63  
Management Access Point Host Name/IP 10.33.10.25  
Direct Routing to Endpoints Enable



Security Module

SIP Entity IP Address 10.33.10.26  
Network Mask 255.255.255.0  
Default Gateway 10.33.10.1  
Call Control PHB 46  
QOS Priority 6  
Speed & Duplex Auto  
VLAN ID



Monitoring

Enable Monitoring ☒

Proactive cycle time (secs) 900  
Reactive cycle time (secs) 120  
Number of Retries 1

## 7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see **References [15]** and **[16]**.

The compliance testing comprised the configuration for two major components, Trunk Server for the service provider and Call Server for the 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 the service provider Bell Canada:

- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Signaling Manipulation
  - 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

Call Server configuration elements for the 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. Log into the Avaya Session Border Controller for Enterprise

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

Enter the appropriate credentials then click *Sign In*.

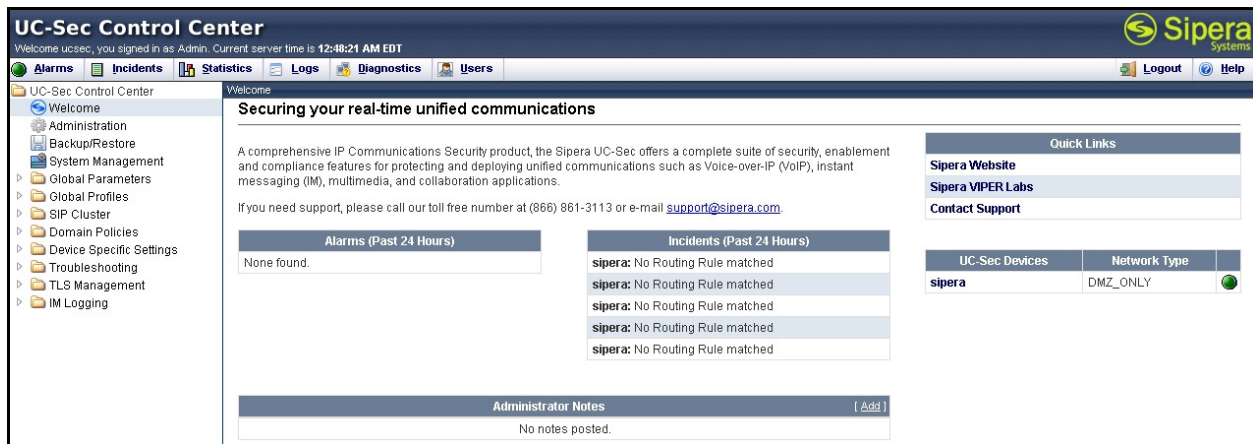


The UC-Sec™ family of products from Siper Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

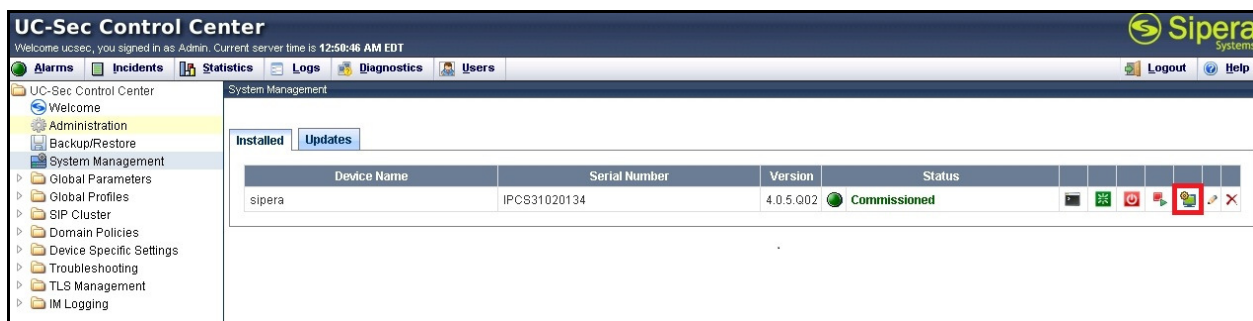
[Visit the Siper Systems website to learn more.](#)

**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 as shown below.



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



The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. Under **General Settings**, the **Box Type** is set to **SIP** and the **Deployment Mode** is set to **Proxy**. Default values are 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
10.10.97.189	10.10.97.189	255.255.255.192	10.10.97.129	A1
10.10.98.112	10.10.98.112	255.255.255.224	10.10.98.97	B1
10.10.98.108	10.10.98.108	255.255.255.224	10.10.98.97	B1
10.10.98.122	10.10.98.122	255.255.255.224	10.10.98.97	B1

DNS Configuration

Primary DNS	10.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.10.97.189

Management IP(s)

IP	10.10.98.85
----	-------------

## 7.2. Global Profiles

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

### 7.2.1. Uniform Resource Identifier (URI) Groups

The **URI Group** feature allows a 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 used for a given call flow.

To add a URI Group, select **UC-Sec Control Center → Global Profiles → URI Groups** and click on the **Add Group** button (not shown).

In the compliance testing, a URI Group named **CS1K\_Bell\_cust6** was added with URI type **Regular Expression** and consists of enterprise SIP domains “**.\*avaya\.com**” for regular call and “**.\*nonymous\.invalid**” for private call; service provider SIP domains “**.\*cust6xxxx\.xxxx\.bell\.ca**”, “**.\*sipxxxxxxxxx\.bell\.ca**” and “**.\*UNKNOWNCALLDER\.invalid**”; IP addresses of URI-Host in OPTIONS heartbeat originated by Session Manager “**.\*10\.33\.10\.26**” and “**.\*10\.10\.97\.189**”; IP address and value

TD; Reviewed:  
SPOC 8/12/2013

Solution & Interoperability Test Lab Application Notes  
©2013 Avaya Inc. All Rights Reserved.

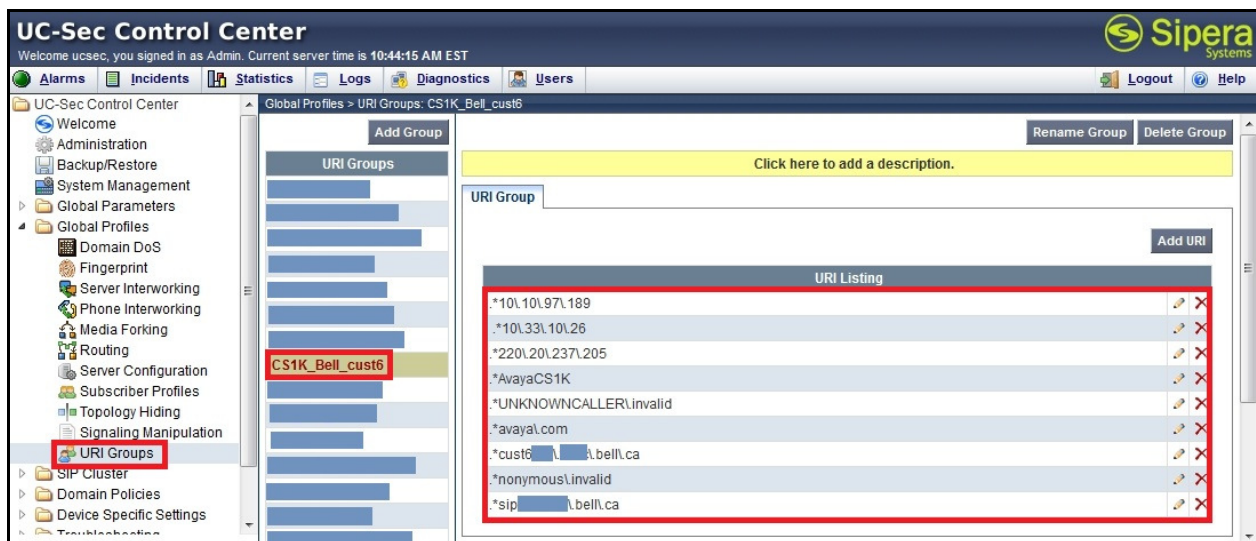
53 of 99  
BCCS1KSM63SBCE

of URI-Host in OPTIONS heartbeat originated by the service provider “.\*220\20\237\205” and “.\*AvayaCS1K”.

SIP domain “.\***nonymous\invalid**” was defined for outgoing private calls from the CS1000 in which the URI-Host is masked as **anonymous.invalid**. SIP domain “.\***UNKNOWNCALLER\invalid**” was defined for incoming private calls from Bell Canada in which the URI-Host is masked as **UNKNOWNCALLER.invalid**. The enterprise SIP domain “.\***avaya\com**” was defined as per description in **Section 5.5.2** for the enterprise traffic originated from the CS1000. For the public SIP Trunk between the Avaya SBCE and Bell Canada, the URI-Host in the “From”, “PAI”, and “Diversion” headers includes SIP domain “.\***cust6xxxx.xxxx.vsac.bell.ca**” while the URI-Host in the “Request-URI” and “To” headers will have SIP domain “.\***sipxxxxxxxxx.bell.ca**”. These domains are assigned by Bell Canada. The IP addresses and value of URI-Host in OPTIONS heartbeats were defined to route incoming and outgoing OPTIONS between the CS1000 and Bell Canada.

This URI-Group is used to match the “From” and “To” headers in a SIP call dialog received from both the CS1000 and Bell Canada. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see **Section 7.2.2**) and Server Flow (see **Section 7.4.4**) to route incoming and outgoing calls to the right destination.

The screenshot below illustrates the URI listing for URI Group **CS1K\_Bell\_cust6**.



## 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.

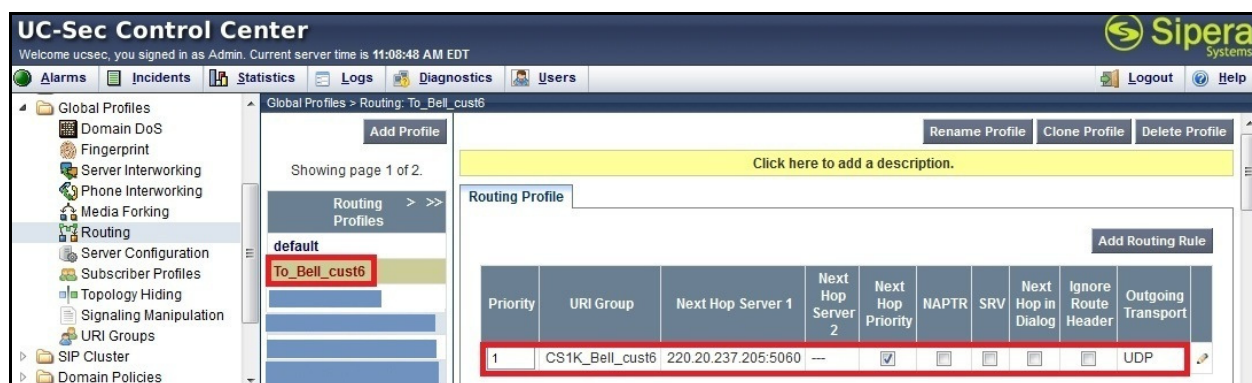
To create a Routing profile, select **UC-Sec Control Center** → **Global Profiles** → **Routing** then click on the **Add Profile** button (not shown).

In the compliance testing, a Routing profile **To\_Bell\_cust6** was created to be used in conjunction with the Server Flow (see **Section 7.4.4**) defined for the CS1000. This entry is to route outgoing calls from the enterprise to Bell Canada.

In the opposite direction, a Routing profile **To\_SM63\_Bell\_cust6** was created to be used in conjunction with the Server Flow (see **Section 7.4.4**) defined for Bell Canada. This entry is to route incoming calls from Bell Canada to the enterprise.

### 7.2.2.1 Routing Profile for Bell Canada

The screenshot below illustrate the **UC-Sec Control Center** → **Global Profiles** → **Routing**: **To\_Bell\_cust6**. If there is a match between the SIP domain in the “To” header with the URI Group **CS1K\_Bell\_cust6** defined in **Section 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of the Bell Canada Trunk Server on port **5060**. As shown in **Figure 1**, Bell Canada SIP Trunking Service is connected with transport protocol **UDP**.



### 7.2.2.2 Routing Profile for Avaya Aura® Session Manager

The Routing Profile **To\_SM63\_Bell\_cust6** in the screenshot below was defined to route calls where the SIP domain in the “To” header matches the URI-Group **CS1K\_Bell\_cust6** defined in **Section 7.2.1**, to **Next Hop Server 1** which is the IP address of Session Manager on port **5060**. As shown in **Figure 1**, the SIP Trunk between Session Manager and the Avaya SBCE is connected with transport protocol **UDP**.





### 7.2.3. Topology Hiding

**Topology Hiding** is a security feature of the Avaya SBCE 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** and then click on **Add Profile** (not shown).

In the compliance testing, two Topology Hiding profiles were created: **To\_Bell\_cust6** and **To\_CS1K\_cust6**.

#### 7.2.3.1 Topology Hiding Profile for Bell Canada

Topology Hiding profile **To\_Bell\_cust6** was defined for outgoing calls to Bell Canada to:

- Mask URI-Host of the “Request-URI” and “To” headers with service provider SIP domain **sipxxxxxxx.bell.ca** to meet the requirements of Bell Canada.
- Mask URI-Host of the “From” header to service provider SIP domain **cust6xxxx.xxxx.bell.ca**.
- Change the “Record-Route”, “Via” headers and SDP added by the CS1000 with the external IP address known to Bell Canada.

This implementation is to secure the enterprise network topology and also to meet the SIP requirements from the service provider.

The screenshots below illustrate the Topology Hiding profile **To\_Bell\_cust6**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration categories, with 'Topology Hiding' selected. The main panel displays the configuration for the 'To\_Bell\_cust6' profile. A table titled 'Topology Hiding' lists the headers, criteria, replace actions, and overwrite values for this profile.

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	cust6xxxx.bell.ca
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	sipxxxx.bell.ca
To	IP/Domain	Overwrite	sipxxxx.bell.ca
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---

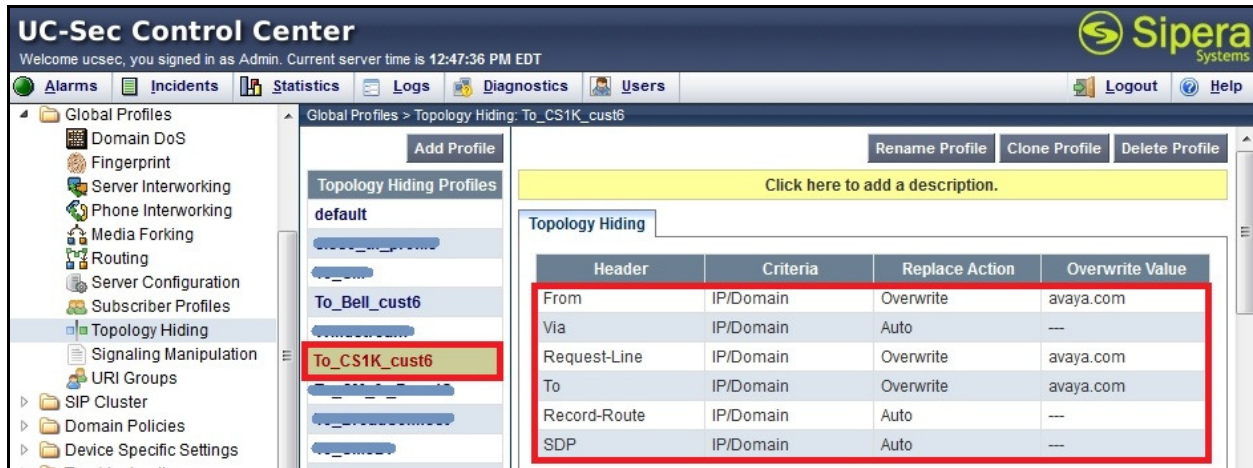
#### 7.2.3.2 Topology Hiding Profile for the CS1000

Topology Hiding profile **To\_CS1K\_cust6** was defined for incoming calls to the CS1000 to:

- Mask URI-Host of the “Request-URI”, “To”, and “From” headers with the enterprise SIP domain **avaya.com**.
- Change the “Record-Route”, “Via” headers and SDP added by Bell Canada with the internal IP address known to the CS1000.



The screenshots below illustrate the Topology Hiding profile **To\_CS1K\_cust6**.



#### Notes:

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

### 7.2.4. Server Interworking

The **Server Interworking** profile features are configured differently for the Call Server and Trunk Server.

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

In the compliance testing, two Server Interworking profiles, **Bell\_cust6** and **CS1K\_cust6**, were created for Bell Canada (Trunk Server) and the CS1000 (Call Server).

#### 7.2.4.1 Server Interworking Profile for Bell Canada

Server Interworking profile **Bell\_cust6** was defined to match the specification of Bell Canada. The **General** and **Advanced** tabs were configured with the following parameters while the other tabs; **Timers**, **URI Manipulation** and **Header Manipulation**, were kept as default.

General settings:

- **Hold Support** = **None**. The Avaya SBCE will not handle Hold/ Resume signaling, it keeps the Hold/ Resume signaling unchanged to send to the destination server.
- **18X Handling** = **None**. The Avaya SBCE will not handle 18X, it keeps the incoming 18X responds unchanged to send to the destination server.
- **Refer Handling** = **Unchecked**. The Avaya SBCE will not handle Refer, it keeps REFER unchanged to send to the destination server.

- **T.38 Support = Unchecked.** Bell Canada does not support the T.38 codec for fax over IP in the compliance testing.
- **Privacy Enabled = Unchecked.** The Avaya SBCE will not mask the “From” header with **anonymous** to the destination server. It depends on the far end to enable/ disable the “Privacy” on individual call basis.
- **DTMF Support = None.** The Avaya SBCE will not modify the DTMF transmission method. It keeps the DTMF unchanged to send to the destination server.

Advanced settings:

- **Record Routes = Both Sides.** The Avaya SBCE will send the “Record-Route” header to both the CS1000 and Bell Canada.
- **Topology-Hiding: Change Call-ID = Checked.** The Avaya SBCE will mask the “Call-ID” header for the calls to the destination server.
- **Change Max-Forwards = Checked.** The Avaya SBCE will reduce the counter of the “Max-Forwards” header by 1 for the calls to the destination server.
- **Has Remote SBC = Checked.** The Avaya SBCE will flexibly handle the changes to the SDP when the call is active.

The screenshots below illustrate the Server Interworking profile **Bell\_cust6**.

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\_cust6

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

Editing Profile: Bell\_cust6

Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLiC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Finish

#### 7.2.4.2 Server Interworking Profile for the CS1000

Server Interworking profile **CS1K\_cust6** was similarly defined to match the specification of the CS1000 with the exception of **Hold Support** which was set to **RFC2354** which is the standard that CS1K follows.

The screenshots below illustrate the Server Interworking profile **CS1K\_cust6**.

Editing Profile: CS1K\_cust6

General	
Hold Support	<input type="radio"/> None <input checked="" 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: CS1K\_cust6

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

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

Back Finish

Editing Profile: CS1K\_cust6

Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLiC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

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 manipulations done by the Avaya SBCE. Using this language, a script can be written and tied to a given Server Configuration (see **Section 7.2.6**) through the UC-Sec Web interface. 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.



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

In the compliance testing, a SigMa script named **Bell\_cust6** was created for the Server Configuration for Bell Canada and is described in detail in the following:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("416XXX188")) then
    {
      %var="this does nothing, match for DID number passed";
    }
    else
    {
      if (%HEADERS["History-Info"][1].regex_match("reason")) then
      {
        %var="this does nothing, match for DID number passed";
      }
      else
      {
        %HEADERS["History-Info"][1].URI.USER="416XXX1883";
      }
      %HEADERS["Diversion"][1] = "<sip:dummy@dummy.com>";
      %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-Info"][1].URI.SCHEME;
      %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-Info"][1].URI.USER;
      %HEADERS["Diversion"][1].URI.HOST = "cust6xxx.xxxx.bell.ca";
      %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-Info"][1].URI.PORT;
      append(%HEADERS["Diversion"][1], "reason=\"unknown\"");
    }
    remove(%HEADERS["History-Info"][2]);
    remove(%HEADERS["History-Info"][1]);
    %HEADERS["P-Asserted-Identity"][1].URI.HOST="cust6xxxx.xxxx.bell.ca";
    remove(%HEADERS["Supported"][1]);
    append(%HEADERS["Contact"][1].URI.USER, ";tgrp=VSXX_416XXX1880_01A;trunk-
context=sipxxxxxxxx.bell.ca");
  }
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    %HEADERS["From"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["Contact"][1].URI.USER.regex_replace("(\\+)", "");
    remove(%HEADERS["Supported"][1]);
    remove(%HEADERS["Require"][1]);
  }
}
```

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 outgoing calls to Bell Canada and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

A set of rules as shown in the screenshot below are added in an “if” statement to check the “P-Asserted-Identity” header if a DID number does not exist in the URI-User to match the scenario of either call forward off-net or MobX calls. In case of call forward off-net, the URI-User of the “History-Info” header will present a DID number known to Bell Canada for call authentication.

Then the followed rules will apply to construct the “Diversion” header based on the information of “History-Info” header. However, in case of MobX calls, URI-User of “History-Info” header presents original PSTN number which is not known to Bell Canada. Therefore, before constructing the “Diversion” header, the URI-User of “History-Info” needs to be re-defined as a DID number (also known as a pilot number) known to Bell Canada. Without the pilot number, outgoing calls to MobX will fail to be authenticated by Bell Canada, it will result a call drop. For more information, see observation #14 in Section 2.2.

As a limitation of the Avaya SBCE, a typical reason code **unknown** was set to the “Diversion” header for all call forward scenarios instead of the particular reason code of **unconditional, no-answer, or user-busy** appropriately for call forward all call, no answer, or busy scenarios. In the compliance testing, with the reason code was set to **unknown**, the off-net call forward calls were successful. For more information, see observation #14 in Section 2.2.

```
if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("416XXX188")) then
{
    %var="this does nothing, match for DID number passed";
}
else
{
    if (%HEADERS["History-Info"][1].regex_match("reason")) then
    {
        %var="this does nothing, match for DID number passed";
    }
    else
    {
        %HEADERS["History-Info"][1].URI.USER="416XXX1883";
    }
    %HEADERS["Diversion"][1] = "<sip:dummy@dummy.com>";
    %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-Info"][1].URI.SCHEME;
    %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-Info"][1].URI.USER;
    %HEADERS["Diversion"][1].URI.HOST = "cust6xxxx.xxxx.bell.ca";
    %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-Info"][1].URI.PORT;
    append(%HEADERS["Diversion"][1],";reason=\"unknown\"");
}
```

After the “Diversion” has been created, two rules are also added as shown in the screenshot below to delete the index 1 and 2 of the “History-Info” header because they are not required by Bell Canada. **Note:** The indexes need to be deleted in the right order from higher to lower.

```
remove(%HEADERS["History-Info"][2]);
remove(%HEADERS["History-Info"][1]);
```

The Topology-Hiding profile **Bell\_cust6** could mask the URI-Host of the “P-Asserted-Identity” header successfully in “request” SIP messages. However, as a limitation, the “P-Asserted-Identity” headers in “response” SIP messages still contain the private enterprise SIP domain. Therefore, a SigMa rules was added to correct the URI-Host of the “P-Asserted-Identity” header as shown in the screenshot below.

```
%HEADERS["P-Asserted-Identity"][1].URI.HOST="cust6xxxx.xxxx.bell.ca";
```

As described in **Section 2.2**, observation #1 the “Supported” header needs to be deleted to disable support of “100rel” signaling on the outbound traffic. The rule for it is described in the screenshot below.

```
remove(%HEADERS["Supported"][1]);
```

Bell Canada also requires the “Contact” header must include a pre-defined Trunk Group Identification (tgrp), this value is obtained through Bell Canada and it is assigned per individual SIP Trunk basis. In the certification testing, the “tgrp” was inserted in “Contact” header as shown in the following rule.

```
append(%HEADERS["Contact"][1].URI.USER, ";tgrp=VSXX_416XXX1880_01A;trunk-  
context=sipxxxxxxxx.bell.ca");
```

The statement **act on message where %DIRECTION="INBOUND" and %ENTRY\_POINT="AFTER\_NETWORK"** is to specify the script will take effect on all types of SIP messages for incoming calls from Bell Canada and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement.

In the compliance testing, Bell Canada sent the “+” sign in the URI-User of the “From” and “Contact” headers. Two rules as shown in the screenshot below are added to remove the “+” sign to format the dialing plan to be compliant to North America numbering plan.

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

As described in **Section 2.2**, observation #1 the “Supported” and “Require” headers need to be removed to disable support of “100rel” signaling on the inbound traffic. The rules for it are described in the screenshot below.

```
remove(%HEADERS["Supported"][1]);  
remove(%HEADERS["Require"][1]);
```

**Note:** The SigMa script for Server Configuration of Session Manager is not necessary as all signaling manipulations have been done on the Server Configuration for Bell Canada, it will apply to both inbound and outbound traffic.

## 7.2.6. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to 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**, then click on the **Add Profile** button (not shown).

In the compliance testing, two separate Server Configurations were created; server entry **Bell\_cust6** for Bell Canada and server entry **SM63** for Session Manager.

### 7.2.6.1 Server Configuration for Bell Canada

The Server Configuration **Bell\_cust6** was added for Bell Canada, it is discussed in detail below. The **General**, **Authentication** and **Advanced** tabs were provisioned. The **Heartbeat** tab, however, was disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat originated from the CS1000 to Bell Canada to query for the status of the SIP Trunk. Two tabs of **Dos Whitelist** and **Dos Protection** are added by checking on the option to **Enable DoS Protection** in the **Advanced** tab which will be discussed later. These tabs are kept unchanged to use the default configurations.



In the **General** tab, specify the **Server Type** for Bell Canada as a **Trunk Server**. The IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, Bell Canada supported transport protocol **UDP** and listens on port **5060**.

Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	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 implements Digest Authentication on the SIP Trunk which requires the enterprise to provide proper information in the Authorization header for authentication purposes. In the compliance testing, the Avaya SBCE was configured to support Digest Authentication for the trunk server under the **Authentication** tab as shown in the screenshot below. It is set with information of **User Name**, **Realm** and **Password** which are obtained through Bell Canada.

Enable Authentication		<input checked="" type="checkbox"/>
User Name	416...1880	
Realm	sip...bell.ca	
Password (Leave blank to keep existing password)	.....	
Confirm Password	.....	
Finish		

Under the **Advanced** tab, check **Enable DoS Protection**. For **Interworking Profile** drop down list, select **Bell\_cust6** as defined in **Section 7.2.4.1** and for **Signaling Manipulation Script** drop down list, select **Bell\_cust6** as defined in **Section 7.2.5**. These configurations are applied to the specific SIP profile and SigMa rules for the traffic from and to Bell Canada. The other settings are kept as default.

Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Bell_cust6
Signaling Manipulation Script	Bell_cust6
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Finish

### 7.2.6.2 Server Configuration for Avaya Aura ® Session Manager

The **Server Configuration SM63** was added for Session Manager, it is discussed in detail below. Only the **General** and **Advanced** tabs required provisioning. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Bell Canada to Session Manager to query for the status of the SIP Trunk.

General	
Server Type	Call Server
IP Addresses / FQDNs	10.33.10.26
Supported Transports	UDP
UDP Port	5060

Edit

In the **General** tab, specify the **Server Type** as **Call Server**. The IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, Session Manager was configured with transport protocol **UDP** and listens on port **5060**. For details of the configuration, refer to **Section 6.5**.



Edit Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.33.10.26
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
<input type="button" value="Finish"/>	

Under the **Advanced** tab, for **Interworking Profile** drop down list, select **CS1K\_cust6** as defined in **Section 7.2.4.2** and for **Signaling Manipulation Script** drop down list select **None**. The other settings are kept as default.

Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	CS1K_cust6
Signaling Manipulation Script	None
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 various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at 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 for use, or a custom domain policy can be created.

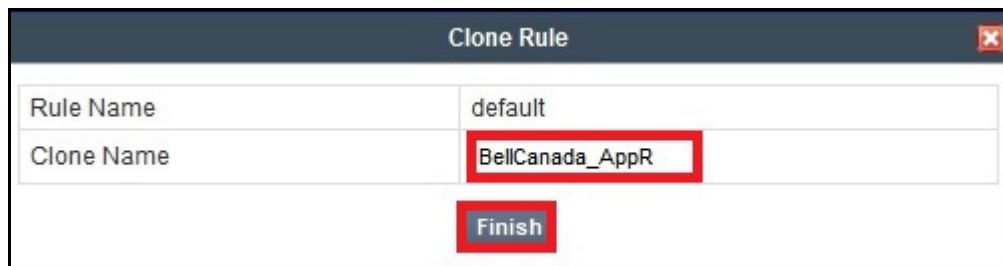
### 7.3.1. Application Rules

The **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 configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

An Application Rule was created to set the number of concurrent voice traffic calls. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint**.

To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**, select the default rule then click on the **Clone Rule** button (not shown).

Enter a descriptive name e.g. **BellCanada\_AppR** for the new rule, then click on the **Finish** button.



Clone Rule	
Rule Name	default
Clone Name	BellCanada_AppR
<b>Finish</b>	

Click the **Edit** button (not shown) to modify the rule. Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** each set to **1000**. In the compliance testing, the CS1000 was programmed to control the concurrent sessions by setting the number of Virtual Trunks (see **Section 5.5.7**) to the allotted number. Therefore, the values in the Application Rule **BellCanada\_AppR** are set high enough to be considered non-blocking.

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

**Miscellaneous**

CDR Support

☒ None
☐ CDR w/ RTP
☐ CDR w/o RTP

IM Logging
☐

RTCP Keep-Alive
☐

Finish

### 7.3.2. Media Rules

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

A custom Media Rule was created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration shows Media Rule **BellCanada\_MediaR** which was used for both the enterprise and Bell Canada networks.

To create a **Media Rule**, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**, select the **default-low-med** rule, then click on the **Clone Rule** button (not shown).

Enter a descriptive name e.g. **BellCanada\_MediaR** for the new rule then click **Finish** button.

**Clone Rule**

Rule Name
default-low-med

Clone Name
BellCanada\_MediaR

Finish

When the RTP changes during a call in progress, the Avaya SBCE interprets this as an anomaly and an alert will be created in the **Incidents Log**. Disabling **Media Anomaly Detection** could

prevent the **RTP Injection Attack** alerts from being created in the log when the audio attributes change.

To modify Media Anomaly, select the **Media Anomaly** tab and click on the **Edit** button (not shown). Then uncheck **Media Anomaly Detection** and click on the **Finish** button.



The screenshot shows a window titled "Media Anomaly" with a close button in the top right corner. Inside the window, there is a sub-header "Media Anomaly". Below this, there is a row with the label "Media Anomaly Detection" and a checkbox that is currently unchecked. At the bottom of the window, there is a "Finish" button. Red boxes highlight the checkbox and the "Finish" button.

On the Avaya SBCE, the **Media Silencing** feature detects the silence when the call is in progress. If the silence is detected and exceeds the allowed duration, the Avaya SBCE generates alert in the **Incidents Log**. In the compliance testing, the Media Silencing detection was disabled to prevent the call from unexpectedly disconnecting due to a RTP packet lost on the public Internet.

To modify Media Silencing, select the **Media Silencing** tab and click on the **Edit** button (not shown). Then uncheck **Media Silencing** and click on the **Finish** button.



The screenshot shows a window titled "Media Silencing" with a close button in the top right corner. Inside the window, there is a sub-header "Media Silencing". Below this, there is a row with the label "Media Silencing" and a checkbox that is currently unchecked. Below that, there is a row with the label "Timeout (seconds)" and a text input field. At the bottom of the window, there is a "Finish" button. Red boxes highlight the checkbox and the "Finish" button.

Under the **Media QoS** tab, click on the **Edit** button (not shown) to configure the Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for the compliance testing.

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	Minimize Delay	1000
	Video Precedence	Routine	000
	Video ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP			
	Audio	EF	101110
	Video	EF	101110

Finish

### 7.3.3. Signaling Rules

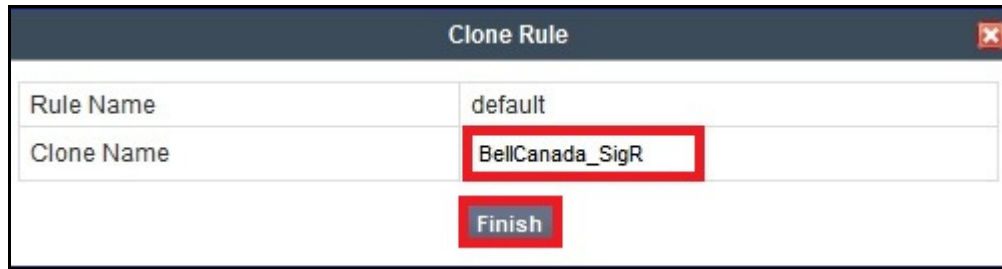
**Signaling Rules** define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and “pattern-matched” against the particular signaling criteria defined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

To clone a Signaling Rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**, select the **default** rule, then click on the **Clone Rule** button (not shown).

In the compliance testing, two **Signaling Rules** were created for Bell Canada and the CS1000.

#### 7.3.3.1 Signaling Rule for Bell Canada

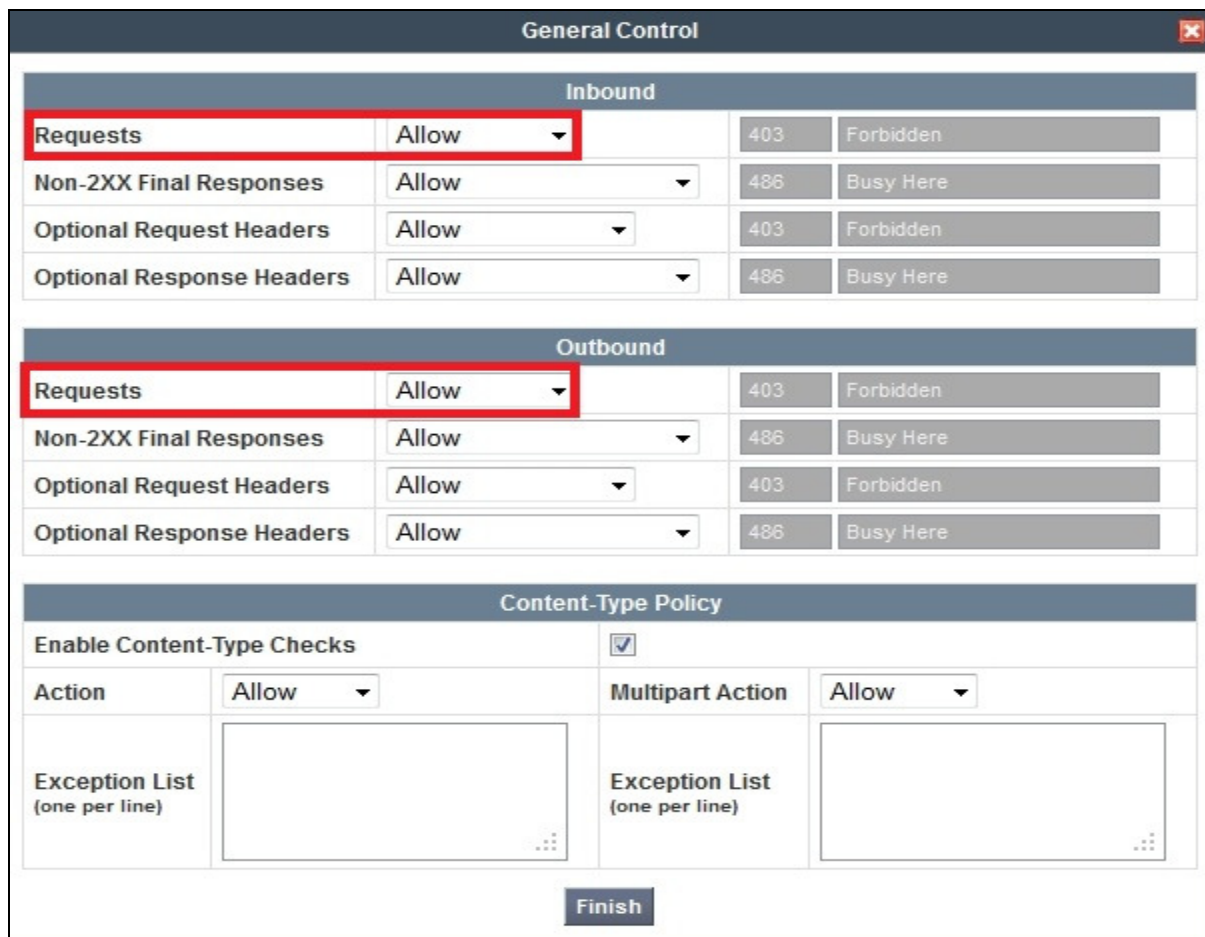
Clone a Signaling Rule with a descriptive name e.g. **BellCanada\_SigR** and click on the **Finish** button.



The 'Clone Rule' dialog box is shown. It has a title bar 'Clone Rule' with a close button. Inside, there are two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'BellCanada\_SigR'. The 'Clone Name' field is highlighted with a red rectangle. Below the fields is a 'Finish' button, also highlighted with a red rectangle.

The **BellCanada\_SigR** was configured to allow the Avaya SBCE to accept inbound and outbound call requests from Bell Canada. It also blocks “Alert-Info”, “x-nt-e164-clid” and “x-nt-ocn-id” headers from the CS1000 because these headers are not required by Bell Canada.

Cloning the Signaling Rule default, the **BellCanada\_SigR** will block all requests with a “403 Forbidden”. To start accepting calls, go to **General** tab, click on the **Edit** button (not shown) then change **Inbound** and **Outbound Requests** to **Allow** as shown in the following screenshot.



The 'General Control' dialog box is shown. It has a title bar 'General Control' with a close button. The dialog is divided into three main sections: 'Inbound', 'Outbound', and 'Content-Type Policy'.  
 In the 'Inbound' section, there is a table with four rows: 'Requests', 'Non-2XX Final Responses', 'Optional Request Headers', and 'Optional Response Headers'. The 'Requests' row is highlighted with a red rectangle, and its 'Allow' dropdown is selected. The other rows have 'Allow' selected for the first dropdown and 'Forbidden' or 'Busy Here' for the second dropdown.  
 In the 'Outbound' section, there is a similar table. The 'Requests' row is also highlighted with a red rectangle, and its 'Allow' dropdown is selected. The other rows have 'Allow' selected for the first dropdown and 'Forbidden' or 'Busy Here' for the second dropdown.  
 In the 'Content-Type Policy' section, there is a checkbox 'Enable Content-Type Checks' which is checked. Below it, there are two columns: 'Action' and 'Multipart Action', both with 'Allow' selected in their dropdowns. At the bottom, there are two 'Exception List' fields, each with a text area and a 'Finish' button at the bottom center.

The **Request Headers** setting is to allow or block a header in a particular direction for a certain request method. The buttons “**Add In Header Control**” and “**Add Out Header Control**” are used to define the inbound and outbound **Request Headers** rules. The signaling rule



**BellCanada\_SigR** will be assigned to the Server Configuration for Bell Canada as shown in **Section 7.2.6.1**.

The following screenshot shows three rules added to block the “Alert-Info”, “nt-e164-clid” and “x-nt-ocn-id” headers.

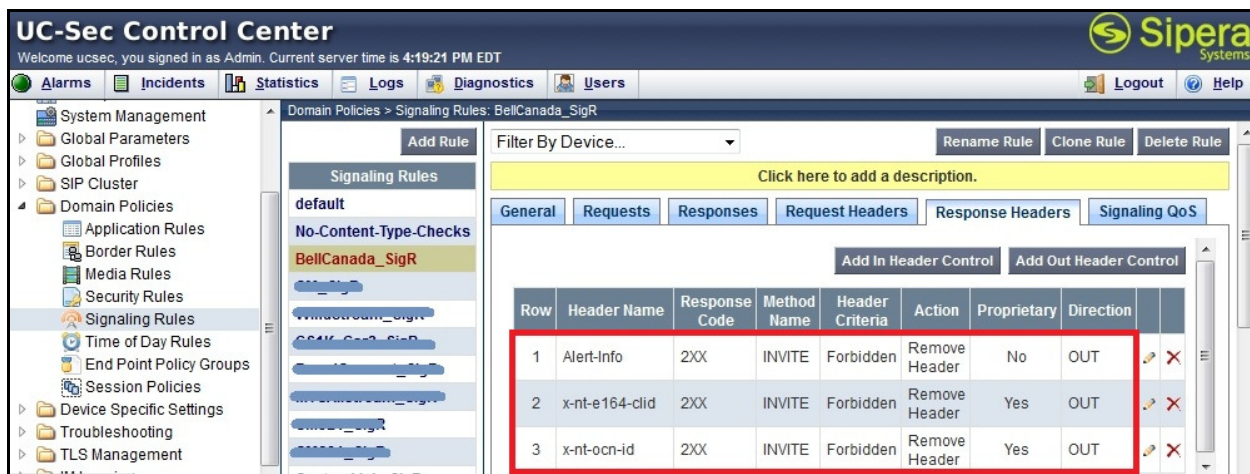
- **Header Name:** Select the header to be manipulated.
- **Method Name:** Select **INVITE** in an outbound call request.
- **Header Criteria:** Click on **Forbidden** to block the header.
- **Action:** Select **Remove header** to delete the header.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	Alert-Info	INVITE	Forbidden	Remove Header	No	OUT
2	x-nt-e164-clid	INVITE	Forbidden	Remove Header	Yes	OUT
3	x-nt-ocn-id	INVITE	Forbidden	Remove Header	Yes	OUT

The **Response Headers** setting allows or blocks a header in a particular direction for a certain response method. The buttons “**Add In Header Control**” and “**Add Out Header Control**” are used to define inbound and outbound **Response Headers** rules. The Signaling Rule **BellCanada\_SigR** will be assigned to the Server Configuration for Bell Canada as shown in **Section 7.2.6.1**.

The following screenshots show three rules added to block the “Alert-Info”, “nt-e164-clid” and “x-nt-ocn-id” headers:

- **Header Name:** Select the header to be manipulated.
- **Method Name:** Select **INVITE** for an inbound call request.
- **Header Criteria:** Click on **Forbidden** to block the header.
- **Action:** Select **Remove header** to delete the header.



**Note:** The pre-defined list does not have the “nt-e164-clid” and “x-nt-ocn-id” headers, but the Avaya SBCE provides an option to define these proprietary headers.

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

**Signaling QoS**

Enabled ☒

☐ ToS

Precedence: Routine (000)

ToS: Minimize Delay (1000)

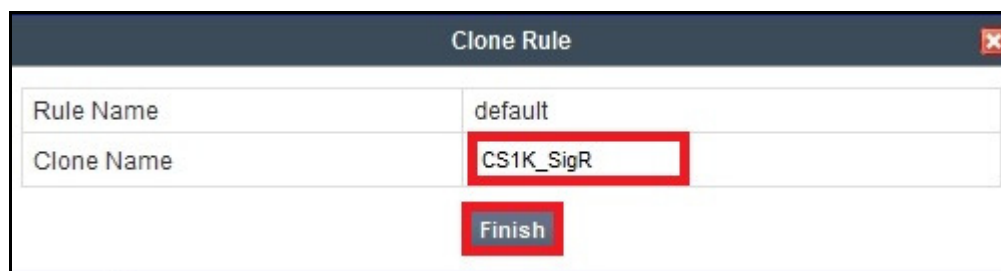
☒ **DSCP**

Value: EF (101110)

**Finish**

### 7.3.3.2 Signaling Rule for the CS1000

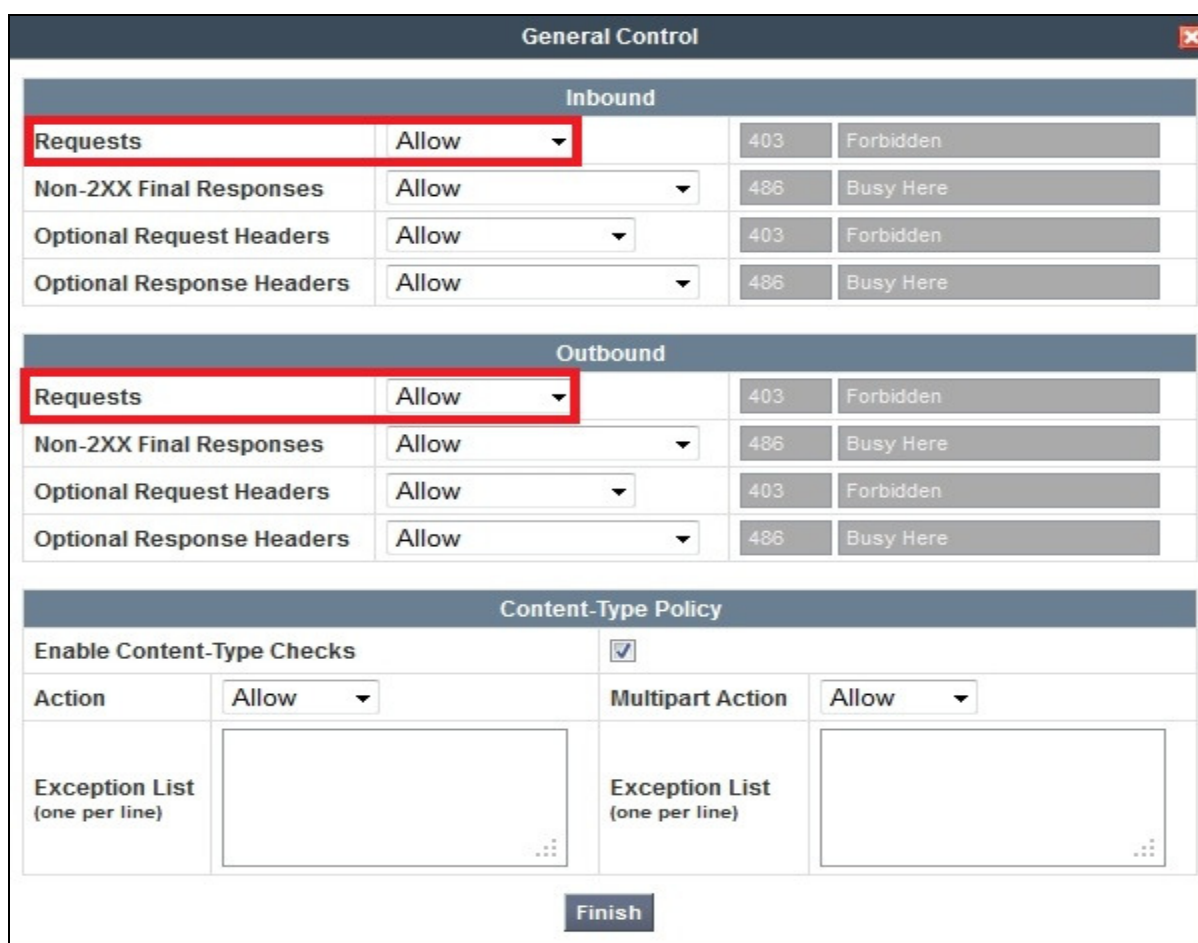
Clone a Signaling Rule with a descriptive name e.g. **CS1K\_SigR** for the CS1000 and click on the **Finish** button.



The 'Clone Rule' dialog box is shown. It has a title bar 'Clone Rule' with a close button. Inside, there are two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'CS1K\_SigR'. The 'Clone Name' field is highlighted with a red rectangle. Below these fields is a 'Finish' button, also highlighted with a red rectangle.

Rule Name	default
Clone Name	CS1K_SigR
<div>Finish</div>	

The **CS1K\_SigR** is configured to allow the Avaya SBCE to accept inbound and outbound call requests from the CS1000. Cloning the Signaling Rule **default**, the **CS1K\_SigR** will block all requests with a “403 Forbidden”. To start accepting calls, select **CS1K\_SigR** then go to **General** tab, click on the **Edit** button (not shown), then change **Inbound-Requests** and **Outbound-Requests** to **Allow** as shown in following screenshot.



The 'General Control' window is shown. It has a title bar 'General Control' with a close button. The window is divided into three main sections: 'Inbound', 'Outbound', and 'Content-Type Policy'. In the 'Inbound' section, the 'Requests' dropdown is set to 'Allow' and is highlighted with a red rectangle. In the 'Outbound' section, the 'Requests' dropdown is also set to 'Allow' and is highlighted with a red rectangle. The 'Content-Type Policy' section has a checkbox 'Enable Content-Type Checks' which is checked. Below this, there are two columns: 'Action' and 'Multipart Action', both with dropdowns set to 'Allow'. At the bottom of each column is an 'Exception List' text area. A 'Finish' button is at the bottom center of the window.

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

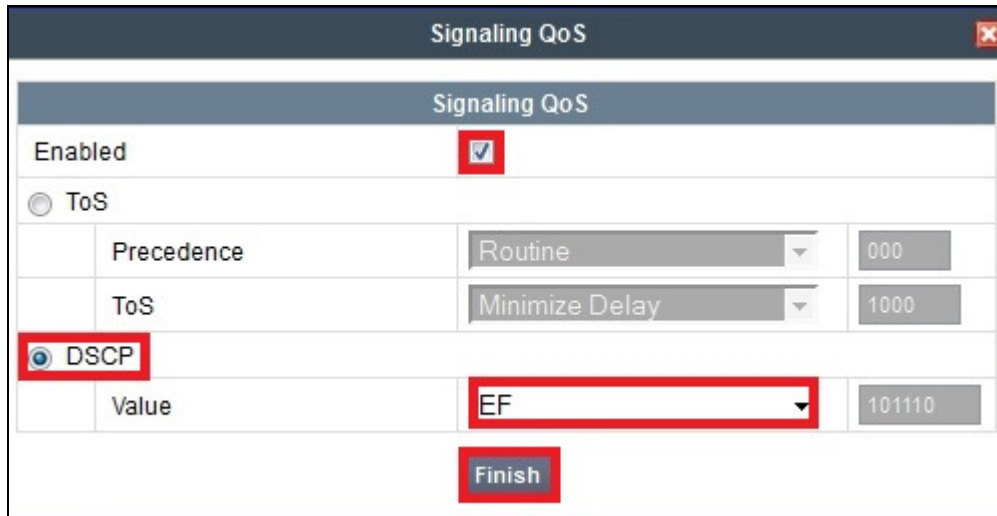
Outbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

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

Finish

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



The image shows a 'Signaling QoS' configuration window. It has a title bar with a close button. Inside, there's a section titled 'Signaling QoS'. Below this, there's a checkbox for 'Enabled' which is checked. There are two radio buttons: 'ToS' and 'DSCP'. 'DSCP' is selected. Under 'DSCP', there's a 'Value' dropdown menu set to 'EF' and a text box showing '101110'. At the bottom, there's a 'Finish' button. Above the 'DSCP' section, there are settings for 'Precedence' (set to 'Routine') and 'ToS' (set to 'Minimize Delay').

### 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.

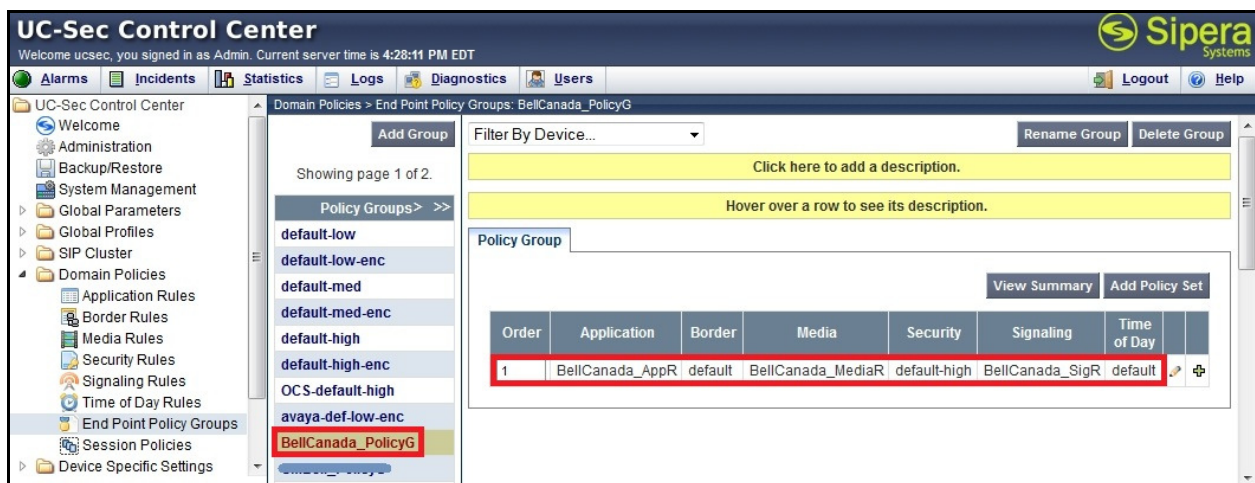
Endpoint Policy Groups were separately created for Bell Canada and the CS1000.

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

#### 7.3.4.1 Endpoint Policy Group for Bell Canada

The following screen shows **BellCanada\_PolicyG** created for Bell Canada.

- Set **Application** to **BellCanada\_AppR** which was created in **Section 7.3.1**.
- Set **Media** to **BellCanada\_MediaR** which was created in **Section 7.3.2**.
- Set **Signaling** to **BellCanada\_SigR** which was created in **Section 7.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** to **default-high**.



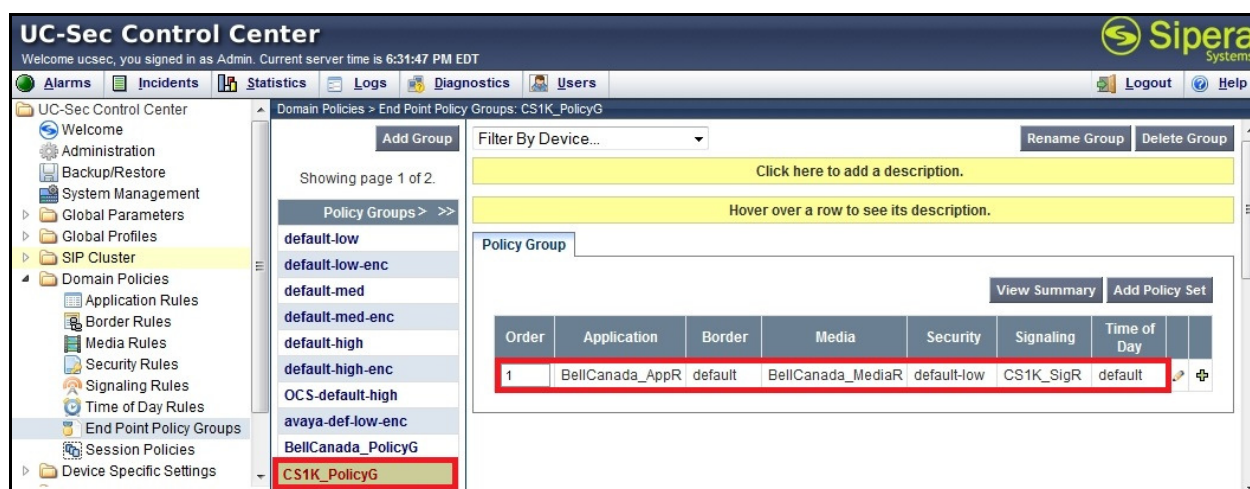
The screenshot shows the UC-Sec Control Center interface. The left sidebar has a tree view with 'Domain Policies' expanded, and 'End Point Policy Groups' selected. The main area shows a list of policy groups. 'BellCanada\_PolicyG' is highlighted. The details for this group are shown on the right, including a table with columns: Order, Application, Border, Media, Security, Signaling, Time of Day. The table has one row with values: 1, BellCanada\_AppR, default, BellCanada\_MediaR, default-high, BellCanada\_SigR, default.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	BellCanada_AppR	default	BellCanada_MediaR	default-high	BellCanada_SigR	default

### 7.3.4.2 Endpoint Policy Group for the CS1000

The following screen shows policy group **CS1K\_PolicyG** created for the CS1000.

- Set **Application** to **BellCanada\_AppR** which was created in **Section 7.3.1**.
- Set **Media** to **BellCanada\_MeidaR** which was created in and **Section 7.3.2**.
- Set **Signaling** to **CS1K\_SigR** which was created in **Section 7.3.3.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** to **default-low**.



### 7.3.5. Session Policy

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

In the compliance testing, the Session Policy **Bell\_cust6** was created to match the codec configuration for Bell Canada. The policy also allows the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.

To clone a common Session Policy which applies to both Bell Canada and the CS1000, navigate to **UC-Sec Control Center → Domain Policies → Session Policies**, select the **default** rule then click on the **Clone Rule** button (not shown).

Enter a descriptive name, .e.g. **Bell\_cust6** for the new policy and click on the **Finish** button.

The screenshot shows a 'Clone Policy' dialog box. It has two input fields: 'Policy Name' with the value 'default' and 'Clone Name' with the value 'Bell\_cust6'. A red box highlights the 'Clone Name' field. Below the fields is a 'Finish' button, also highlighted with a red box.



Bell Canada supports voice codec G.711MU and payload **101** for RFC2833/ DTMF. To define **Codec Prioritization** for Audio Codec, select the profile **Bell\_cust6** created above, click on the **Edit** button (not shown). Select **Preferred Codec #1** as **PCMU (0)**, which is G.711MU, **Preferred Codec #2** as **Dynamic (101)** for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent unsupported codecs from being sent to both ends.

**Note:** This Session Policy prioritizes G.711MU voice codec to establish the voice call. It is mandatory for a G.711MU fax call to be successful because both Bell Canada and the CS1000 cannot switch the voice call using a different codec to G.711MU for fax.

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

**Finish**

Under the **Media** tab of the Session Policy **Bell\_cust6** created above, click on the **Edit** button (not shown) then check on **Media Anchoring** to allow the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.



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

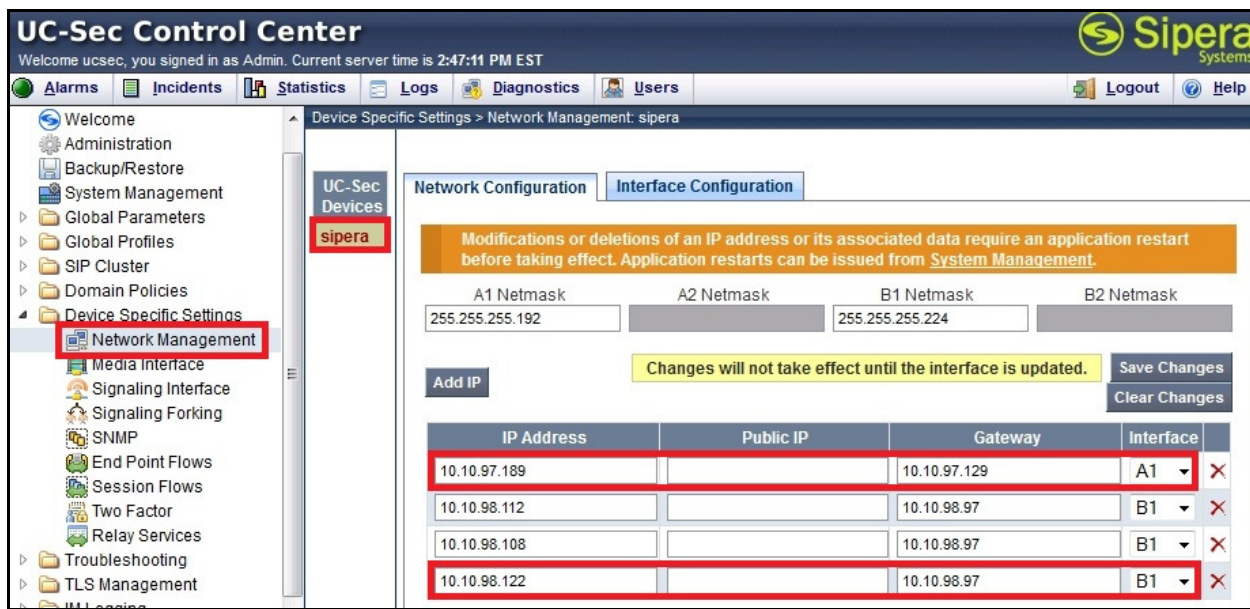
## 7.4. Device Specific Settings

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.

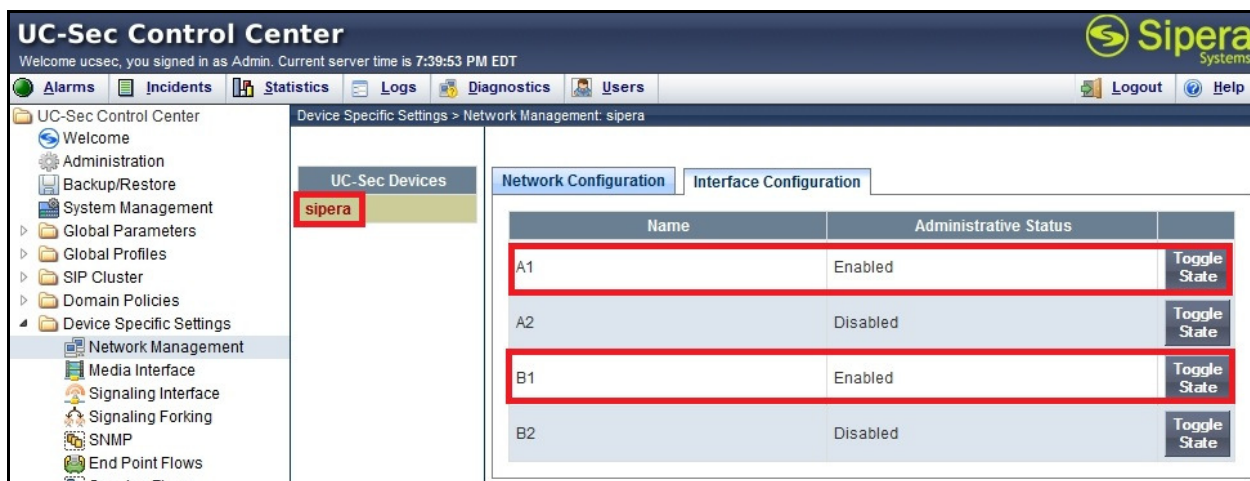
### 7.4.1. Network Management

The **Network Management** page is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP addresses, public IP addresses, subnet mask, gateway, etc. to interface the device to the network. This information populates the various Network Management tabs, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management**, Under the **Network Configuration** tab, 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 public interface is assigned to **B1**, appropriate to the parameters shown in **Figure 1**.



On the **Interface Configuration** tab, enable the interfaces connecting to the inside and outside networks. To enable an interface click it's **Toggle State** button. The following screen shows interface A1 and B1 were **Enabled**.



## 7.4.2. Media Interface

The **Media Interface** screen is where the media ports are defined. The Avaya SBCE will open connections for RTP traffic on the defined ports.

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

Two separate Media Interfaces are needed; one for the inside interface and one for the outside interface. The following screen shows the Media Interfaces **InsideMedia** and **OutsideMedia\_Bell\_cust6** that were created for the compliance testing.

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

The screenshot shows the UC-Sec Control Center interface. The left sidebar has a tree view with 'Media Interface' highlighted under 'Device Specific Settings'. The main panel is titled 'Device Specific Settings > Media Interface: sipera'. It contains a table of media interfaces. A warning message at the top states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below the table is an 'Add Media Interface' button.

Name	Media IP	Port Range		
InsideMedia	10.10.97.189	35000 - 40000		
OutsideMedia_Bell_cust6	10.10.98.122	35000 - 40000		

### 7.4.3. Signaling Interface

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

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

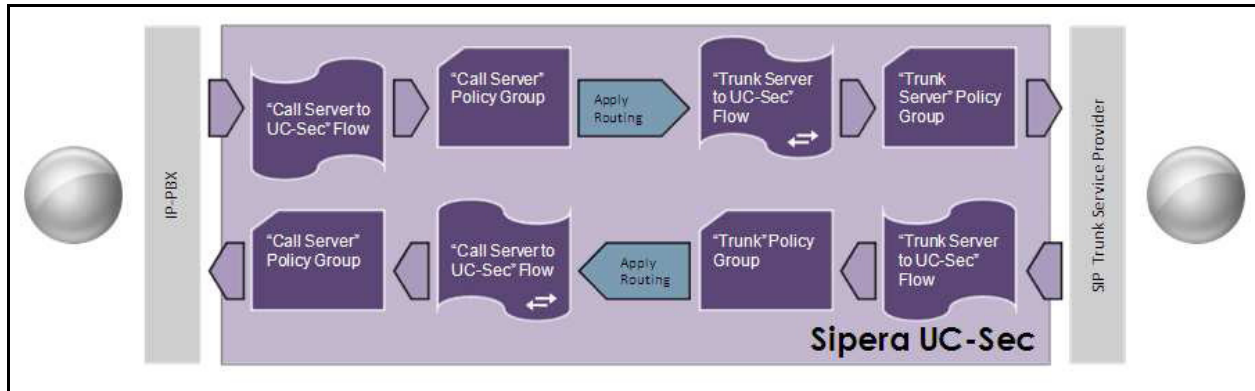
Two separate Signaling Interfaces are needed; one for the inside interface and one for the outside interface. The following screen shows the Signaling Interfaces **InsideSIP** and **OutsideSIP\_Bell\_cust6** that were created in the compliance testing with **UDP/5060** for both inside and outside interfaces.

The screenshot shows the UC-Sec Control Center interface. The left sidebar has a tree view with 'Signaling Interface' highlighted under 'Device Specific Settings'. The main panel is titled 'Device Specific Settings > Signaling Interface: sipera'. It contains a table of signaling interfaces. An 'Add Signaling Interface' button is visible at the top right.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
InsideSIP	10.10.97.189	---	5060	---	None		
OutsideSIP_Bell_cust6	10.10.98.122	---	5060	---	None		

#### 7.4.4. End Point Flows - Server Flow

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

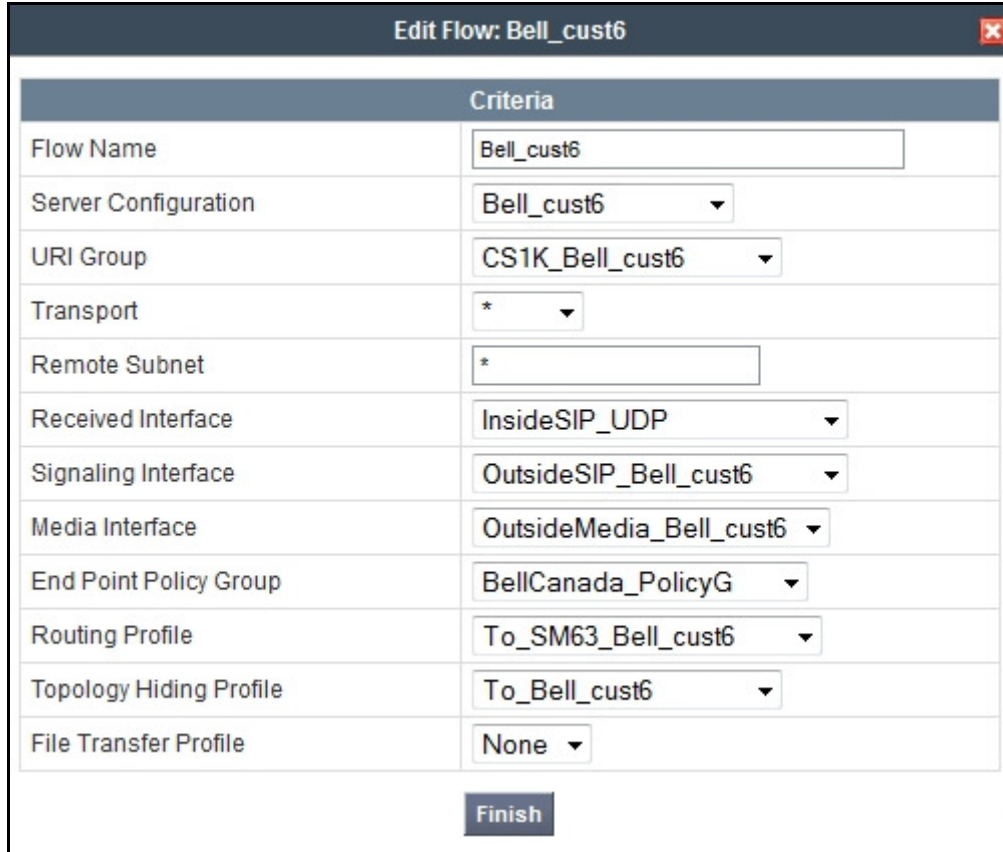


In the compliance testing, two separate **Server Flows** were created for Bell Canada and Session Manager.

To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the other fields are kept as default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.6** which the Server Flow associates to.
- **URI Group:** Select the URI Group **CS1K\_Bell\_cust6** created in **Section 7.2.1**.
- **Received Interface:** Select the Signaling Interface created in **Section 7.4.3** which is the Server Configuration designed to receive SIP signaling from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.4.3** which is the Server Configuration designed to send the SIP signaling to.
- **Media Interface:** Select the Media Interface created in **Section 7.4.2** which is the Server Configuration designed to send the RTP to.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 7.3.4**.
- **Routing Profile:** Select the Routing Profile created in **Section 7.2.2** which is the Server Configuration designed to route the calls to.
- **Topology Hiding Profile:** Select the Topology Hiding profile created in **Section 7.2.3** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows the Server Flow named **Bell\_cust6** for Bell Canada.



Criteria	
Flow Name	Bell_cust6
Server Configuration	Bell_cust6
URI Group	CS1K_Bell_cust6
Transport	*
Remote Subnet	*
Received Interface	InsideSIP_UDP
Signaling Interface	OutsideSIP_Bell_cust6
Media Interface	OutsideMedia_Bell_cust6
End Point Policy Group	BellCanada_PolicyG
Routing Profile	To_SM63_Bell_cust6
Topology Hiding Profile	To_Bell_cust6
File Transfer Profile	None

Finish

The following screen shows the Server Flow named **SM63\_Bell\_cust6** for Session Manager.



Criteria	
Flow Name	SM63_Bell_cust6
Server Configuration	SM63
URI Group	CS1K_Bell_cust6
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP_Bell_cust6
Signaling Interface	InsideSIP_UDP
Media Interface	InsideMedia
End Point Policy Group	CS1K_PolicyG
Routing Profile	To_Bell_cust6
Topology Hiding Profile	To_CS1K_cust6
File Transfer Profile	None
<input type="button" value="Finish"/>	

### 7.4.5. Session Flows

The **Session Flows** feature allows defining certain parameters that pertain to the media portions of a call, whether it originates from the enterprise or outside the enterprise. This feature provides 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.

A common Session Flow **Bell\_cust6** was created for both the Bell Canada and the CS1000.

To create a session flow, navigate to **UC-Sec Control Center → Device Specific Settings → Session Flows** then click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the remaining fields are kept as default.

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



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

The following screen shows the Session Flow named **Bell\_cust6**.

Criteria		
Flow Name	Bell_cust6	
URI Group #1	CS1K_Bell_cust6	
URI Group #2	CS1K_Bell_cust6	
Subnet #1	*	Ex: 192.168.0.1/24
Subnet #2	*	Ex: 192.168.0.1/24
Session Policy	Bell_cust6	

Finish

## 8. Bell Canada SIP Trunking Service Configuration

Bell Canada is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the public IP address of the Avaya SBCE at the enterprise. Bell Canada will provide the customer with the necessary information to configure the SIP Trunk connection from the enterprise to Bell Canada.

The information provided by Bell Canada includes:

- IP address of the Bell Canada SIP proxy.
- Service provider public SIP domains.
- CPE SIP domains.
- Credentials for Digest Authentication.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.
- A customer specific SIP signaling reference.

The sample configuration between Bell Canada and the enterprise for the compliance testing is a static configuration. There is no registration on the SIP Trunk implemented for either Bell Canada or the enterprise.

## 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 commands that can be used to troubleshoot the solution.

### 9.1. Verification Steps

The following items were verified for each test scenario.

- Calls are checked for the correct call progress tones and cadences.
- During the ringing state, the ring back tone and destination ringing are checked.
- Calls are checked in both hands-free and handset mode due to internal Avaya requirements.
- Calls are checked for speech path in both directions using spoken words to ensure clarity of speech.
- The display(s) of the handsets/clients involved are checked for consistent and expected calling party name and number and redirection information both prior to answer and after call establishment.
- The speech path and messaging system are observed for timely and quality end to end tone audio path generation and application responses.
- The call server maintenance terminal window is used for the monitoring of BUG(s), ERR and AUD messages.
- Speech path and display are checked before and after calls are put on/off hold from each end.
- Applicable files are screened on an hourly basis during the testing for messages that may indicate technical issues. This refers to Avaya PBX files.
- Calls are checked to ensure that all resources such as Virtual trunks, TDM trunks, handsets and VGWs are released when a call scenario ends.

### 9.2. Protocol Traces

The following SIP message headers are inspected using sniffer traces:

- Request-URI: Verify the request number and SIP domain.
- From: Verify the display name and display number.
- To: Verify the display name and display number.
- P-Asserted-Identity: Verify the display name and display number.
- Privacy: Verify privacy masking with “user, id”.
- Diversion: Verify DID number.
- Authorization: Verify Digest Authentication implementation.

The following attributes in SIP message bodies are inspected using sniffer traces:

- Connection Information (c line): Verify IP addresses of near and far endpoints.
- Time Description (t line): Verify session timeout value of near and far endpoints.
- Media Description (m line): Verify audio port, codec, DTMF event description.

- Media Attribute (a line): Verify specific audio port, codec,ptime, send/ receive abilities, DTMF event and fax attributes.

## 9.3. Troubleshooting

### 9.3.1. The Avaya SBCE

Use a network sniffing tool, e.g. Wireshark to monitor the SIP signaling between Bell Canada and the enterprise. The sniffer traces are captured at the public interface of the Avaya SBCE.

The following is an example inbound call from Bell Canada to the enterprise.

- Inbound INVITE request from Bell Canada.

```
INVITE sip:4167751881@cust6-tor.vsaac.bell.ca;transport=udp SIP/2.0
Via: SIP/2.0/UDP 207.236.237.205:5060;branch=z9hG4bKgoejjo00eoulvjoug2s0.1
From: <sip:+16139675258@siptrunking.bell.ca;user=phone>;tag=SDjsina01-840008108-1365100810217-
To: "Bell Demo12345"<sip:4167751881@cust6-tor.vsaac.bell.ca>
Call-ID: SDjsina01-fd8380e51eef732cb76588d779766207-a0n8330
CSeq: 724346869 INVITE
Contact: <sip:+16139675258@207.236.237.205:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 18
Content-Type: application/sdp
Content-Length: 208

v=0
o=BroadWorks 16033937 1 IN IP4 207.236.237.205
s=-
c=IN IP4 207.236.237.205
t=0 0
m=audio 20032 RTP/AVP 0 18 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=fmtp:18 annexb=no
```

- 200OK/SDP response from the enterprise.

```
SIP/2.0 200 OK
From: <sip:16139675258@siptrunking.bell.ca;user=phone>;tag=SDjsina01-840008108-1365100810217-
To: "Bell Demo12345" <sip:4167751881@cust6-tor.vsaac.bell.ca>;tag=6a1e078-9e610a87-13c4-55013-361275-28ebd2c-361275
CSeq: 724346869 INVITE
Call-ID: SDjsina01-fd8380e51eef732cb76588d779766207-a0n8330
Contact: <sip:4167751881;tgrp=VSAC_4167751880_01A;trunk-context=siptrunking.bell.ca@135.10.98.122:5060;transport=udp;user=phone;gsid=2c8bc810-9d57-11e2-b5dd-e41f13b32ca8>
Record-Route: <sip:135.10.98.122:5060;ipcs-line=331376;lr;transport=udp>
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, UPDATE
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
Via: SIP/2.0/UDP 207.236.237.205:5060;branch=z9hG4bKgoejjo00eoulvjoug2s0.1
Server: AVAYA-SM-6.3.1.0.631004
```

```

Privacy: none
P-Asserted-Identity: "BellCA i1140" <sip:4167751881@cust6-
tor.vvac.bell.ca;user=phone>
Content-Type: application/sdp
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Bellevil
le";termlocname="Belleville";termsiglocname="Belleville";termmedialocname="Bellevi
lle";smaccounting="true"
P-AV-Message-Id: 1_2
Av-Global-Session-ID: 2c8bc810-9d57-11e2-b5dd-e41f13b32ca8
Content-Length: 253

v=0
o=- 207 1 IN IP4 135.10.98.122
s=-
c=IN IP4 135.10.98.122
t=0 0
m=audio 35028 RTP/AVP 0 101 111
c=IN IP4 135.10.98.122
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=maxptime:20
a=sendrecv

```

The following is an example outbound call from the enterprise to Bell Canada.

- Outbound INVITE request from the enterprise.

```

INVITE sip:16139675258@siptrunking.bell.ca;user=phone SIP/2.0
From: "BellCA i1140" <sip:4167751881@cust6-
tor.vvac.bell.ca;user=phone>;tag=6a1f8f8-9e610a87-13c4-55013-3615f8-6c1bfd12-
3615f8
To: <sip:16139675258@siptrunking.bell.ca;user=phone>
CSeq: 1 INVITE
Call-ID: de24e859e6e7c05d0d32a174b71fc37a
Contact: <sip:4167751881;tgrp=VSAC_4167751880_01A;trunk-
context=siptrunking.bell.ca@135.10.98.122:5060;transport=udp;user=phone;gsid=448ce
230-9d59-11e2-b5dd-e41f13b32ca8>
Record-Route: <sip:135.10.98.122:5060;ipcs-line=331622;lr;transport=udp>
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO,
SUBSCRIBE, UPDATE
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17 AVAYA-SM-
6.3.1.0.631004
Max-Forwards: 65
Via: SIP/2.0/UDP 135.10.98.122:5060;branch=z9hG4bK-s1632-000665850530-1--s1632-
Privacy: none
P-Asserted-Identity: "BellCA i1140" <sip:4167751881@cust6-
tor.vvac.bell.ca;user=phone>
Content-Type: multipart/mixed;boundary=unique-boundary-1
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Bellevil
le";termlocname="Belleville";termsiglocname="Belleville";smaccounting="true"
P-AV-Message-Id: 1_1
P-Charging-Vector: icid-value="448ce230-9d59-11e2-b5dd-e41f13b32ca8"
Av-Global-Session-ID: 448ce230-9d59-11e2-b5dd-e41f13b32ca8
Content-Length: 898

--unique-boundary-1
Content-Type: application/sdp

```

```

v=0
o=- 208 1 IN IP4 135.10.98.122
s=-
c=IN IP4 135.10.98.122
t=0 0
m=audio 35030 RTP/AVP 0 101
c=IN IP4 135.10.98.122
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv

--unique-boundary-1
Content-Type: application/x-nt-mcdn-frag-hex;version=ssLinux-7.50.17;base=x2611
Content-Disposition: signal;handling=optional

0500a001
0107130081900000a200
09090f00e9a0830001002000
131e070011fd1800a1160201010201a1300e8102010582010184020000850104
1315070011fa0f00a10d02010102020100cc040000f08700
1e0403008183
460e01000a00010003000a0000000000
4a1c01001800010000000000000014765700000005000000000081180000

--unique-boundary-1
Content-Type: application/x-nt-epid-frag-hex;version=ssLinux-7.50.17;base=x2611
Content-Disposition: signal;handling=optional

011201
00:17:65:f9:fa:7a

--unique-boundary-1--

```

- 401 challenge from Bell Canada to request Digest Authentication.

```

SIP/2.0 401 Unauthorized
From: "BellCA i1140" <sip:4167751881@cust6-
tor.vzac.bell.ca;user=phone>;tag=6a1f8f8-9e610a87-13c4-55013-3615f8-6c1bfd12-3615f8
To: <sip:16139675258@siptrunking.bell.ca;user=phone>;tag=SDrsbq299-899298185-
1365101709583
CSeq: 1 INVITE
Call-ID: de24e859e6e7c05d0d32a174b71fc37a
Via: SIP/2.0/UDP 135.10.98.122:5060;branch=z9hG4bK-s1632-000665850530-1--s1632-
WWW-Authenticate: DIGEST
qop="auth", nonce="BroadWorksXhf4ab8cvTq3efmvBW", realm="siptrunking.bell.ca", algorit
hm=MD5
Content-Length: 0

```

- Subsequent INVITE from the enterprise with Authorization header response to Digest Authentication.

```

INVITE sip:16139675258@siptrunking.bell.ca;user=phone SIP/2.0
From: "BellCA i1140" <sip:4167751881@cust6-
tor.vzac.bell.ca;user=phone>;tag=6a1f8f8-9e610a87-13c4-55013-3615f8-6c1bfd12-
3615f8
To: <sip:16139675258@siptrunking.bell.ca;user=phone>
CSeq: 2 INVITE

```



```

Call-ID: de24e859e6e7c05d0d32a174b71fc37a
Contact: <sip:4167751881;tgrp=VSAC_4167751880_01A;trunk-
context=siptrunking.bell.ca@135.10.98.122:5060;transport=udp;user=phone;gsid=448ce
230-9d59-11e2-b5dd-e41f13b32ca8>
Record-Route: <sip:135.10.98.122:5060;ipcs-line=331622;lr;transport=udp>
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO,
SUBSCRIBE, UPDATE
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17 AVAYA-SM-
6.3.1.0.631004
Max-Forwards: 65
Via: SIP/2.0/UDP 135.10.98.122:5060;branch=z9hG4bK-s1632-000855131659-1--s1632-
Authorization: Digest username="avaya", realm="siptrunking.bell.ca",
nonce="BroadWorksXhf4ab8cvTq3efmvBW", uri="sip:avaya.com",
response="42d503f050ce42ba1367e14015830c1f", algorithm=MD5, cnonce="0a4f113b",
qop=auth, nc=00000001
Privacy: none
P-Asserted-Identity: "BellCA i1140" <sip:4167751881@cust6-
tor.vsaac.bell.ca;user=phone>
Content-Type: multipart/mixed;boundary=unique-boundary-1
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Bellevil
le";termlocname="Belleville";termsiglocname="Belleville";smaccounting="true"
P-AV-Message-Id: 1_1
P-Charging-Vector: icid-value="448ce230-9d59-11e2-b5dd-e41f13b32ca8"
Av-Global-Session-ID: 448ce230-9d59-11e2-b5dd-e41f13b32ca8
Content-Length: 898

--unique-boundary-1
Content-Type: application/sdp

v=0
o=- 208 1 IN IP4 135.10.98.122
s=-
c=IN IP4 135.10.98.122
t=0 0
m=audio 35030 RTP/AVP 0 101
c=IN IP4 135.10.98.122
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv

--unique-boundary-1
Content-Type: application/x-nt-mcdn-frag-hex;version=ssLinux-7.50.17;base=x2611
Content-Disposition: signal;handling=optional

0500a001
0107130081900000a200
09090f00e9a0830001002000
131e070011fd1800a1160201010201a1300e8102010582010184020000850104
1315070011fa0f00a10d02010102020100cc040000f08700
1e0403008183
460e01000a00010003000a0000000000
4a1c01001800010000000000000014765700000005000000000081180000

--unique-boundary-1
Content-Type: application/x-nt-epid-frag-hex;version=ssLinux-7.50.17;base=x2611
Content-Disposition: signal;handling=optional

011201
00:17:65:f9:fa:7a

```

--unique-boundary-1--

- 200OK/SDP response from Bell Canada.

```
SIP/2.0 200 OK
From: "BellCA i1140" <sip:4167751881@cust6-
tor.vsaac.bell.ca;user=phone>;tag=6alf8f8-9e610a87-13c4-55013-3615f8-6c1bfd12-
3615f8
To: <sip:16139675258@siptrunking.bell.ca;user=phone>;tag=SDrsbq299-1379110904-
1365101710788
CSeq: 2 INVITE
Call-ID: de24e859e6e7c05d0d32a174b71fc37a
Via: SIP/2.0/UDP 135.10.98.122:5060;branch=z9hG4bK-s1632-000855131659-1--s1632-
Record-Route: <sip:135.10.98.122:5060;ipcs-line=331622;lr;transport=udp>
Supported:
Contact: <sip:16139675258@207.236.237.205:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 184

v=0
o=BroadWorks 16057857 1 IN IP4 207.236.237.205
s=-
c=IN IP4 207.236.237.205
t=0 0
m=audio 20034 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

## 9.3.2. The CS1000 Verification Steps

### 9.3.2.1 Verify Patch Installation

Verify that the patches mentioned in **Section 4, Table 1** are properly installed on the CS1000.

The following screen shows output of the “dstat” command on the Call Server.

```
pdt> dstat
Call Server:
-----
DepList name: core
  Filename: /var/opt/nortel/cs/fs/u/patch/deplist/mcore_01.cpl
  Issue   : 01
  Release : x2107.50
  Created : 2013-03-19 16:44:12 (est)
  Number of patches: 340
  Patches Loaded: 340
  Patches In-service: 338
pdt>
```

**Note:** Activating patch MPLR32246 may require other patches to be deactivated. The activation of patch MPLR32246 is not shown in the screenshot above.

The following screen shows output of the “spstat” command on the SSG Server.

```
[admin@car2-ssg2 ~]$ spstat
There is no SP in loaded status.
The last applied SP: Service_Pack_Linux_7.50_17_20130308.nt1
It is a STANDARD SP.
Has been applied by user nortel on Fri Apr 5 11:24:58 2013.
spins command completed with no errors detected.
[admin@car2-ssg2 ~]$
```

### 9.3.2.2 Active Call Trace (LD 80)

The following is an example of one of the commands available on the CS1000 to trace the DN when the call is in progress. The call scenario involved the PSTN phone number 613XXX5258 calling 416XXX1881 on the CS1000.

- Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail).
- Login to the Overlay command prompt, issue the command **LD 80** then **trac 3 1881**.
- After the call is released, issue the command **trac 3 1881** again to see if the DN is released back to idle state.

Below is the actual output of the Call Server Command Line mode when the 1881 is in-call state:

```
>ld 80
TRA000
.trac 3 1881

ACTIVE VTN 108 0 00 17

ORIG VTN 100 1 00 00 VTRK IPTI RMBR 103 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 10.10.97.189
FAR-END MEDIA ENDPOINT IP: 10.10.97.189 PORT: 35664
FAR-END VendorID: AVAYA-SM-6.1.7.0.617012
TERM VTN 108 0 00 17 KEY 0 SCR CUST 3 DN 1881 TYPE 2002P2
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 10.10.98.132 PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 1881
MAIN_PM ESTD
TALKSLOT ORIG 84 TERM 57
QUEU NONE
CALL ID 0 34853

---- ISDN ISL CALL (ORIG) ----
CALL REF # = 385
BEARER CAP = VOICE
HLC =
CALL STATE = 10 ACTIVE
CALLING NO = 1613XXX5258 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
CALLED NO = 416XXX1881 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN

NON ACTIVE VTN 108 0 00 29

NON ACTIVE VTN 108 0 00 13 MARP
.
```

The following is an example after the call on 1881 is completed.

```
.trac 3 1881

IDLE VTN 108 0 00 17

IDLE VTN 108 0 00 29

IDLE VTN 108 0 00 13    MARP
```

### 9.3.2.3 SIP Trunk Monitoring (LD 32)

Place an incoming call from the PSTN (613XXX5258) to the CS1000 (416XXX1881). Then check the SIP Trunk status by using LD 32.

```
>ld 32
NPR000
.stat 100 1
063 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
.
```

The following is an example after the call is completed; the BUSY trunk changes its state to IDLE.

```
.stat 100 1
064 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
.
```

## 10. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.3 and the Avaya Session Border Controller for Enterprise Release 4.0.5 to Bell Canada SIP Trunking Service. Bell Canada SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Bell Canada SIP Trunking Service provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases have been executed. Despite the number of observations and limitations 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 Service is considered **compliant** with the Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.3 and the Avaya Session Border Controller for Enterprise Release 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] *Network Routing Service Fundamentals, Avaya Communication Server 1000*, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.
- [2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010.
- [3] *Communication Server 1000E Overview, Avaya Communication Server 1000*, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011.
- [4] *Communication Server 1000 Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000*, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011.
- [5] *Communication Server 1000 Dialing Plans Reference, Avaya Communication Server 1000*, Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010.
- [6] *Product Compatibility Reference, Avaya Communication Server 1000*, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011.
- [7] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.2, December 2012.
- [8] *Administering Avaya Aura® System Platform*, Release 6.2.1, July 2012.
- [9] *Implementing Avaya Aura® System Manager*, Release 6.3, Issue 1.0, December 2012.
- [10] *Administering Avaya Aura® System Manager*, Release 6.3, Issue 1.0, December 2012.
- [11] *Implementing Avaya Aura® Session Manager*, Release 6.3, March 2013.
- [12] *Administering Avaya Aura® Session Manager*, Release 6.3, December 2012.
- [13] *Administering Avaya one-X® Communicator*, April 2011.
- [14] *Using Avaya one-X® Communicator*, April 2011.
- [15] *UC-Sec Install Guide (102-5224-400v1.01)*.
- [16] *UC-Sec Administration Guide (010-5423-400v106)*.
- [17] *RFC3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [18] *RFC3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)* <http://www.ietf.org/>.
- [19] *RFC2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>.

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



---

**©2013 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](mailto:devconnect@avaya.com).