



Application Notes for Configuring Bell Canada SIP Trunking Service with Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 7.0 and Avaya Session Border Controller for Enterprise Release 7.0 – Issue 1.0

Abstract

These Application Notes describe the steps to configure a Session Initiation Protocol (SIP) trunk between Bell Canada SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager 7.0, Avaya Session Border Controller for Enterprise 7.0 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for Enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	6
2.3.	Support	8
3.	Reference Configuration.....	9
4.	Equipment and Software Validated	10
5.	Configure Avaya Communication Server 1000.....	12
5.1.	Log into Communication Server 1000 System	12
5.1.1.	Log into System Manager and Element Manager (EM)	12
5.1.2.	Log into Call Server by Using Overlay Command Line Interface (CLI)	14
5.2.	Administer IP Telephony Node	15
5.2.1.	Obtain Node IP address	15
5.2.2.	Administer Terminal Proxy Server (TPS)	17
5.2.3.	Administer Quality of Service (QoS)	18
5.2.4.	Synchronize New Configuration.....	18
5.3.	Administer Voice Codec	20
5.3.1.	Enable Voice Codec G.729A, G.711MU.....	20
5.3.2.	Enable Voice Codec on Media Gateways.....	21
5.4.	Zones and Bandwidth Management.....	22
5.4.1.	Create Zone for IP Phones (Zone 10)	22
5.4.2.	Create Zone for Virtual SIP Trunk (Zone 255)	23
5.5.	Administer SIP Trunk Gateway	24
5.5.1.	Integrated Services Digital Network (ISDN).....	24
5.5.2.	Administer Avaya Communication Server 1000 SIP Trunk Gateway	26
5.5.3.	Administer Virtual D-Channel.....	28
5.5.4.	Administer Virtual Super-Loop	32
5.5.5.	Administer Virtual SIP Routes	32
5.5.6.	Administer Virtual Trunks.....	34
5.5.7.	Administer Calling Line Identification Entries.....	37
5.5.8.	Enable External Trunk to Trunk Transfer.....	39
5.6.	Administer Dialing Plans	40
5.6.1.	Define ESN Access Codes and Parameters (ESN)	40
5.6.2.	Associate NPA and SPN Call to ESN Access Code 1	41
5.6.3.	Digit Manipulation Block Index (DMI).....	42
5.6.4.	Route List Block Index (RLI 14)	43
5.6.5.	Inbound Call – Incoming Digit Translation Configuration	45
5.6.6.	Outbound Call - Special Number Configuration	47
5.6.7.	Outbound Call - Numbering Plan Area (NPA).....	48
5.7.	Administer a Phone	49
5.7.1.	Phone creation.....	49
5.7.2.	Enable Privacy for the Phone.....	50
5.7.3.	Enable Call Forward for Phone.....	51

6.	Configure Avaya Aura® Session Manager	53
6.1.	Avaya Aura® System Manager Login and Navigation.....	54
6.2.	Specify SIP Domain	56
6.3.	Add Location.....	57
6.4.	Configure Adaptations	59
6.5.	Add SIP Entities	60
6.5.1.	Configure Session Manager SIP Entity	61
6.5.2.	Configure Communication Server 1000 SIP Entity.....	62
6.5.3.	Configure Avaya SBCE SIP Entity	63
6.6.	Add Entity Links	64
6.7.	Configure Time Ranges	65
6.8.	Add Routing Policies	65
6.9.	Add Dial Patterns	67
7.	Configure Avaya Session Border Controller for Enterprise	70
7.1.	Log in Avaya Session Border Controller for Enterprise	70
7.2.	Global Profiles.....	73
7.2.1.	Configure Server Interworking Profile - Avaya Session Manager	73
7.2.2.	Configure Server Interworking Profile – Bell Canada	75
7.2.3.	Configure Signaling Manipulation	78
7.2.4.	Configure Server – Avaya Session Manager	79
7.2.5.	Configure Server – Bell Canada	80
7.2.6.	Configure Routing – Avaya Session Manager.....	82
7.2.7.	Configure Routing – Bell Canada.....	83
7.2.8.	Configure Topology Hiding – Avaya Session Manager.....	84
7.2.9.	Configure Topology Hiding – Bell Canada	85
7.3.	Domain Policies	86
7.3.1.	Create Signaling Rules.....	86
7.3.2.	Create Endpoint Policy Groups	88
7.4.	Device Specific Settings.....	90
7.4.1.	Manage Network Settings.....	90
7.4.2.	Create Media Interfaces	93
7.4.3.	Create Signaling Interfaces	94
7.4.4.	Configuration Server Flows.....	95
8.	Bell Canada SIP Trunking Service Configuration.....	97
9.	Verification Steps.....	98
9.1.	General	98
9.2.	Verification of an Active Call on Communication Server 1000.....	98
9.3.	Protocol Trace	100
10.	Conclusion	101
11.	References.....	101
12.	Appendix A: Additional patch lineup for the CS1000 configuration.	102
13.	Appendix B: SigMa Script.....	104

1. Introduction

These Application Notes illustrate a sample configuration using an Avaya SIP-enabled enterprise solution which consists of an Avaya Communication Server 1000 (CS1000) Release 7.6, Avaya Aura® Session Manager Release 7.0 and Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 7.0 with Bell Canada SIP Trunking Service.

Customers using this Avaya SIP-enabled enterprise solution with Bell Canada are able to place and receive PSTN calls via a broadband Internet connection. This converged network solution is an alternative to a traditional PSTN trunk such as analog and/or ISDN-PRI.

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 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 Internet and exercise the features and functionalities listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- General call processing between CS1000 and Bell Canada SIP Trunking Service, including the following:
 - Codec/ptime: G.729A/20ms, G.711MU/20ms, no Voice Activity Detection (VAD).
 - Calling Line Identification Display (CLID) and Calling Party Name Display (CPND).
 - Ring-back tone.
 - Speech (audio) path.
 - SIP Transport: UDP, port: 5060.
 - RTP Port: 49152 – 49200.
- Incoming PSTN calls to various phone types including UNISim, SIP, digital, and analog phones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including UNISim, SIP, digital, and analog phones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya 2050 IP Softphone.
- Various call types including: local call, long distance call, international call, outbound toll-free, 411, and 911 Emergency services.

- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference). Call redirection was performed from both ends. Note: Bell Canada SIP Trunking Service supports Diversion Header for off-net call forward and SIP UPDATE for off-net call transfer.
- Response to SIP OPTIONS queries.
- Response to incomplete call attempts and trunk errors.
- Fax using G.711 pass-through mode.
- Outbound call with long-hold stability.
- Outbound call with long-duration stability.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF (RFC2833) in inbound and outbound calls.
- Voicemail navigation for inbound and outbound calls.
- CS1000 Mobile-X feature.
- Outbound call with authentication.
- Static and Dynamic Outgoing Name and Number Display (ONND). The ONND feature was configured on Bell Canada system. During this compliance testing, Bell Canada assisted to test this feature. However, Avaya is not responsible for supporting any related issues on this feature. Please contact Bell Canada for any concerns.

The following item was not supported:

- Inbound toll free - Bell Canada did not support this setup during this compliance testing.

During testing, the following activities were made to each tested scenario:

- Calls were checked for the correct call progress tones and cadences.
- During the ringing state, the ring back tone and destination ringing were checked.
- Calls were checked in both hands-free and handset mode in compliance with internal Avaya requirement.
- Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
- The display(s) of the sets/clients involved were checked for consistent and expected CLID and redirection information both prior to answer and after call establishment.
- The speech path and messaging system were observed for timely and quality End to End tone and audio path as well as application responses.
- The call server maintenance terminal window was open during the test execution for the monitoring of BUG(s), ERROR and AUD messages (see **Section 5.1.2**).
- Speech path was checked before and after calls were put on hold and resumed from each end.
- Calls were checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs (Voice Gateways) were released when calls were ended (see SIP Trunk monitoring in **Section 9.2**).

2.2. Test Results

The objectives outlined in **Section 2.1** were verified. All the applicable test cases were executed successfully. However, the following observations were noted during the compliance testing:

- **Outbound call with authentication could not complete and there was no speech path** - Bell Canada system authenticates every call coming from the Avaya system. With the authentication issue found in Avaya SBCE, calls from the Avaya system to the PSTN do not complete as there is no speech path on the outbound call. To resolve this issue, an authentication patch is applied on Avaya SBCE. The patch number is sbc700-p001-20151005-7.0.0-21.x86_64.rpm.
- **Bell Canada-sourced SIP OPTIONS included Max-Forward = 0, and Avaya responded with “483 Too Many Hops”** - The OPTIONS request is simply a keep-alive message. As long as Bell Canada received a legitimate reply, Bell Canada treated the connection to be alive. Of course the value of Max-Forward could be increased but since it did not cause any problem during compliance testing, Bell Canada would like to keep the existing configuration.
- **For outbound call and the call was terminated by PSTN phone, Avaya SBCE forwarded the BYE message to Session Manager without inserting the “maddr=10.10.97.178” parameter (CS1000 IP Address) in Request-URI header** - The call scenario was making an outbound call successfully with 2-way audio. When PSTN phone hangs up the call, PBX phone was still in an active state. The reason was when Avaya SBCE received BYE message from Bell Canada, it forwarded to Session Manager, but Avaya SBCE did not insert "maddr=10.10.97.178" parameter of CS1000 IP Address in Request-URI header. Therefore, Session Manager received BYE, but it did not forward to CS1000. There was a workaround to fix this issue by using Header Manipulation on Server Interworking to insert "maddr=10.10.97.178" in Request-URI header for BYE message (See **Section 7.2.1**). The JIRA ticket (Aurora-7198) was opened for Avaya SBCE team to support this issue.
- **Bell Canada sent empty Supported Header** - Avaya CS1000 did not respond to “183 Session in Progress” with PRACK message from an outbound call from CS1000 to PSTN causing the call failed with no speech path. The reason being was that Bell sent empty Supported header to Avaya system. When Avaya SBCE received empty Supported header, it inserted another “Supported: replace” header and passed it on to Session Manager. Session Manager received 2 Supported headers, Session Manager combined two Supported headers into one, “Supported: , replace”, and passes it on to CS1000. Upon receiving “erroneous” Supported header, CS1000 couldn’t parse this Supported header. Therefore, CS1000 did not respond to 183 messages from Bell system with the PRACK message. This intern causes the call failed with no speech path. Workaround: The solution was to use SIP Manipulation script at Avaya SBCE to remove this empty Supported header coming from Bell Canada (See **Section 0**).
- **For inbound call, Bell Canada offered G.729A as a primary codec and G.711 as a secondary codec** - This was a global codec policy which could not be changed during this compliance testing. The compliance testing was tested with G.729A and G.711MU codecs, in that order, for inbound calls.

- **If the CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed** - This is a known limitation on the CS1000.
- **Calling Line Identification Display (CLID) was not correctly displayed** - After call redirection, namely blind/consultative transfers, was completed with 2-way audio, however the CLID on the transferee's phone was not updated accordingly. This is a known CS1000 limitation.
- **There was no ring-back tone after Avaya 1140E SIP phone completed the off-net blind transfer** - For an inbound or outbound PSTN call to/from an Avaya 1140E SIP phone, the SIP phone performed blind transfer to another PSTN endpoint. The expected behavior of the SIP phone was after transferring, the original PSTN phone, should hear ring-back from another PSTN. However, when the user pressed the "Trnsfr" button and answered the question of "Consult with party ?", with "No", which implied a blind transfer, the transferee PSTN phone was ringing but the original PSTN phone could not hear ring-back while the call was being transferred. Until the transferee PSTN phone answered the call, the call transfer was completed with 2-way audio. In order to resolve the ring-back tone issue, there was a configuration on Signaling Rules on Avaya SBCE to translate the SIP 183 with SDP to SIP "180 Ringing" (See **Section 7.3.1**), so that the original PSTN phone could hear the local ring-back tones. However, this translation on the Avaya SBCE removed support for early media. Customers of the Bell Canada should be aware of this limitation before implementing this specific translation on the Avaya SBCE.
- **Blind Call Transfer to PSTN using Avaya 1140E SIP phone did not complete until transferee picked up the call** - Call scenario was when a PSTN phone called to an Avaya 1140E SIP phone, the SIP phone answered the call and performed a blind transfer to another PSTN endpoint. The expected behavior of the SIP phone was after transferring, the phone should display "Transfer successful". But in this case when the user pressed the "Trnsfr" button and answered the question of "Consult with party ?", with "No", which implied a blind transfer, the transferee PSTN phone was ringing and the SIP phone should be released and displayed "Transfer successful". Instead, the SIP phone was still displayed "Transferring" and not released until the transferee PSTN phone answered the call. This is very minor known limitation on CS1000 SIP phone. There was no user impact. Transfer was still completed with 2-way audio.
- **When the Avaya 1140E SIP phone hosted a conference call, but dropped out of the conference first, the entire conference call was terminated** - This is a known CS1000 SIP phone limitation.

- **For ONND testing on off-net call forward, Bell Canada expected to see the external number on Diversion header should be the same number on FROM header, however CS1000 always put the valid PBX DID number on Diversion header instead of the same number on FROM header.** This was a CS1000 design. In order to test with an external number for ONND, the Calling Line Identification Display (CLID) was temporarily changed to any invalid DID number rather than the valid DID numbers that Bell Canada provided for this compliance testing. This was a global setting on CS1000; therefore the CLID would be impacted for any outbound calls.
- When testing with ONND feature on off-net call forward, Bell Canada requested to manipulate the From and Contact headers for incoming calls to remove “+1” on user URI of From and Contact headers so that they contained only 10-digit number. By this way, when CS1000 did the off-net call forward, it sent the SIP re-Invite with From header contained only 10-digit number

2.3. Support

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

For technical support on the Bell Canada system, please use the support link at
http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page.

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance test between CS1000 and Bell Canada SIP Trunking Service. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked and replaced with fictitious IP addresses throughout the document.

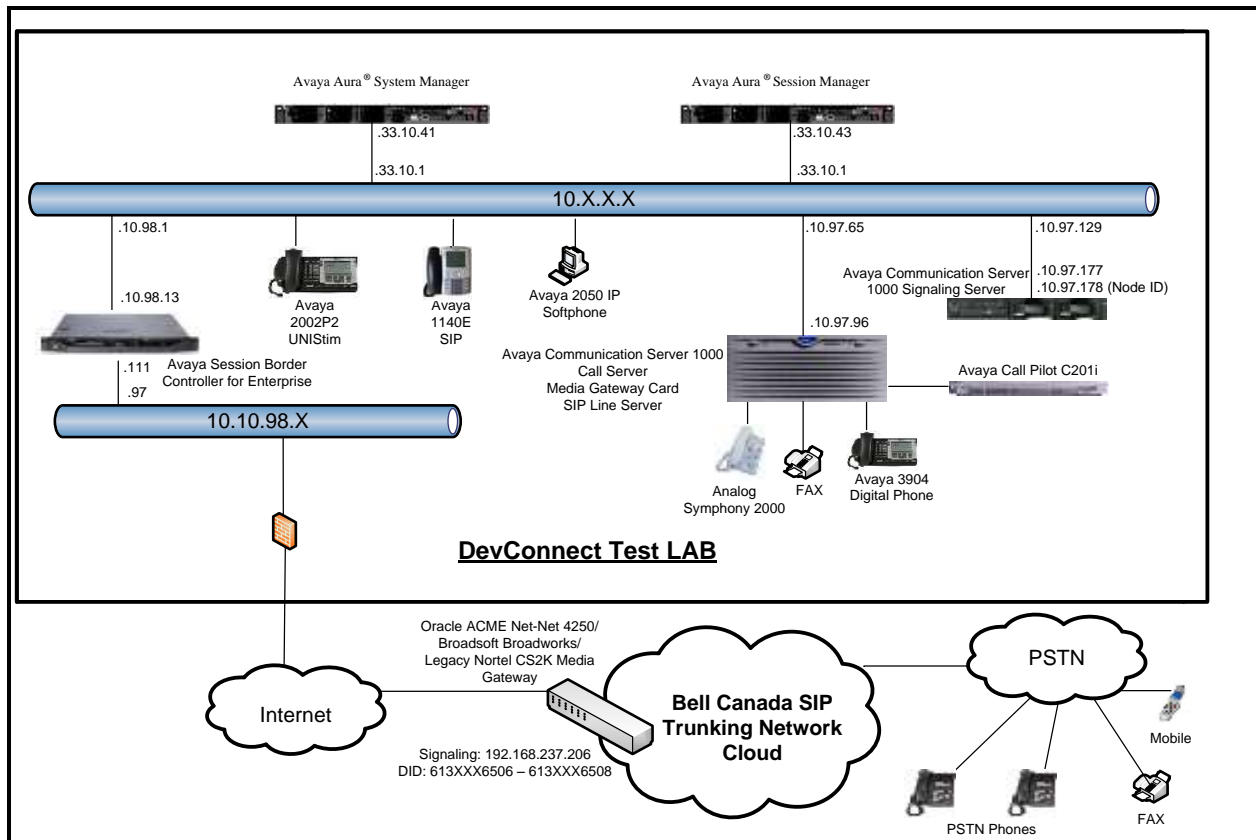


Figure 1 - Network diagram for Avaya and Bell Canada SIP Trunking Service

Note: From Release 7.0, Avaya uses the VMware®-based Avaya Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya appliance offer.

Avaya-appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7 (It was used for this compliance testing), and HP ProLiant DL360p G8
- S8300D and S8300E

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications such as Avaya Aura® System Manager, Avaya Aura® Session Manager on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware tools, such as vCenter

and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.

It is assumed the general installation of VMware®-based Avaya Appliance Virtualization Platform, Avaya Aura® System Manager, Avaya Aura® Session Manager has been previously completed and is not discussed in this document.

4. Equipment and Software Validated

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

Avaya systems:

Equipment/Software	Release/Version
Avaya Communication Server 1000 (CPPM)	Call Server: 765 P + Signaling Server: 7.65.16 GA SIP Line Server: 7.65.16 GA
Avaya Call Pilot C201i	Call Pilot Voice Mail Manager: 05.00.41.143
Avaya Aura® Session Manager running on VMware®-based Avaya appliance	7.0.0.0 Build No: 7.0.0.0.700001-7.0.0.0
Avaya Aura® System Manager running on VMware®-based Avaya appliance	7.0.0.0 Build No: 7.0.0.0.16266-7.0.9.912 Software Update Revision No: 7.0.0.0.3929
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	7.0.0-21-6602 (Patch: sbc700-p001-20151005-7.0.0-21.x86_64.rpm)
Avaya Phones: 2002 P2 (UNiStim) 1140E SIP	0604DCO 04.04.23.00
Avaya 3904 Digital Phone	Core: 2.4 – Flash: 9.4 PO L1.8
Avaya 2050 IP Softphone	4.04.0148 (4.4 SP4)
Analog Symphony 2000	N/A
HP Office jet 4500 Fax	N/A

Bell Canada SIP Trunking Service systems:

System	Software
Oracle ACME Packet Net-Net 4500	7.2.0 MR-5 Patch 3
BroadSoft Broadworks	20
Legacy Nortel CS2K Media Gateway	SN10 PVG/IW-SPM

The following assumptions were made for the compliance tested configuration:

- CS1000 R7.6 software with latest patches.
- Bell Canada SIP Trunking Service provides support to set up, configure and troubleshoot on the Bell Canada network side during test execution.

Additional patch lineup for the configuration is listed in **section 12 - Appendix A**.

5. Configure Avaya Communication Server 1000

The configuration of the CS1000 outlined in these Application Notes uses the Incoming Digit Translation feature to receive calls, the Numbering Plan Area Code (NPA), and the Special Number (SPN) features to route calls from the CS1000 to the PSTN via SIP trunks to the Bell Canada SIP Trunking Service network.

These Application Notes assume that the basic CS1000 configuration has already been administered. For further information on CS1000, please consult the references in **Section 11**.

The procedures below describe the configuration details for configuring the CS1000.

5.1. Log into Communication Server 1000 System

Changes to the CS1000 can be made using Element Manager, which is accessible from System Manager and offers the user a GUI like option for making changes. Changes to the CS1000 can also be made using the Command Line Interface (CLI) offered using PuTTY to make an SSH connection.

5.1.1. Log into System Manager and Element Manager (EM)

Open an instance of a web browser and connect to the System Manager using the following address: <https://<System Manager IP address>/SMGR/>. Log in using an appropriate User ID and Password (not shown). Select **Elements** → **Communication Server 1000**.

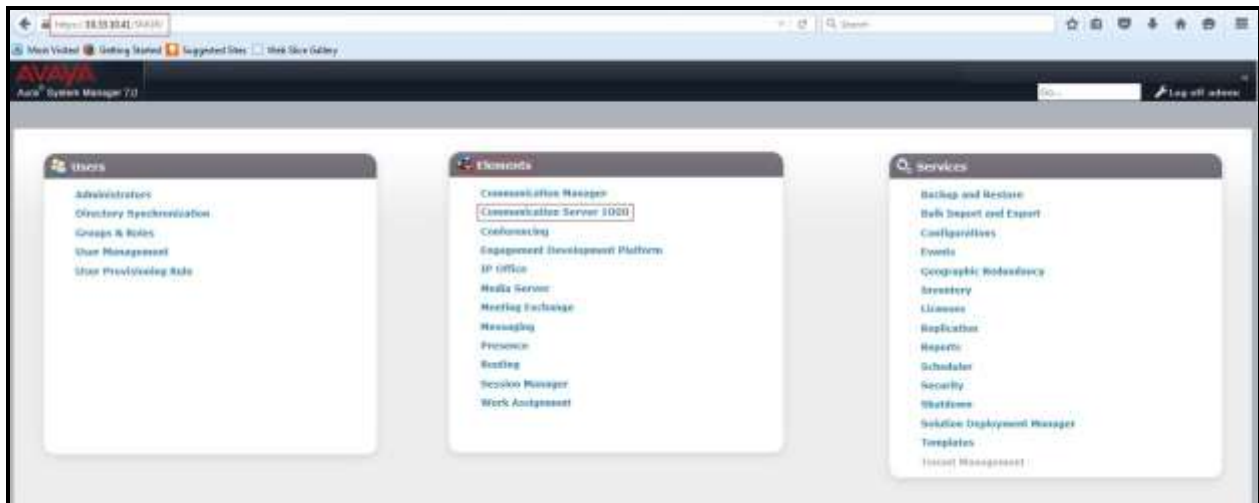


Figure 2 – System Manager Home Screen

The **Avaya Communication Server 1000 Management** screen is displayed. Click on the **Element Name** of the CS1000 Element as highlighted in red box below:

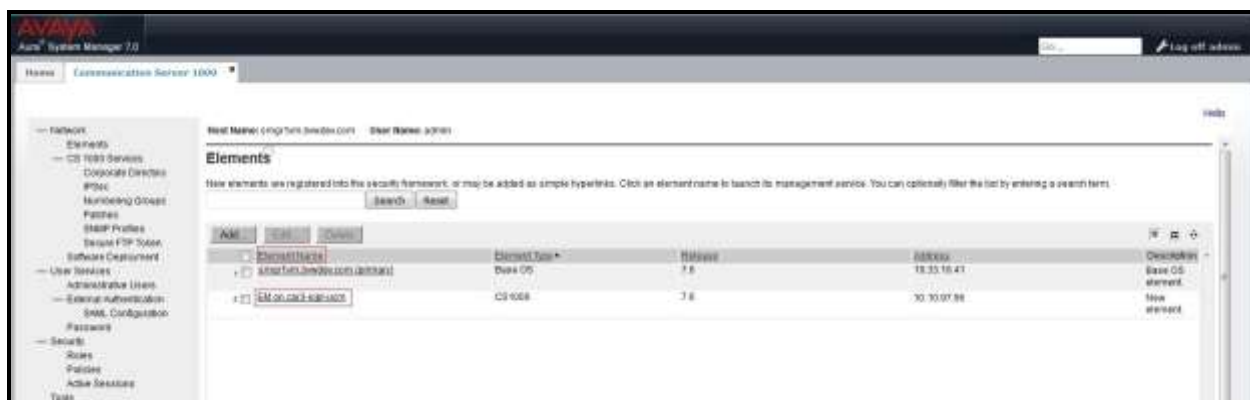


Figure 3 – Communication Server 1000 Management

Log into the CS1000 using an appropriate **User ID** and **Password**.



Figure 4 – Communication Server 1000 Log In Screen

The CS1000 Element Manager **System Overview** page is displayed as shown in **Figure 5**.

IP Address: 10.10.97.96

Type: Avaya Communication Server 1000E CPPM Linux

Version: 4121

Release: 765 P +



Figure 5 – Element Manager System Overview

5.1.2. Log into Call Server by Using Overlay Command Line Interface (CLI)

Using Putty, SSH to the IP address of the CS1000 Signaling Server using an account with administrator credentials.

Run the command **cslogin** and log in with the appropriate user account and password. Sample output is shown below.

login as: ← **Enter an account with administrator credentials**

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@10.10.97.178's password: ← **Enter the password**

Last login: Fri Oct 30 08:25:18 2015 from 10.10.98.78

[admin@car3-cores ~]\$ **cslogin**

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

USERID? ← **Enter the user account**

PASS? ← **Enter the password**

.

TTY #09 LOGGED IN ADMIN 09:05 30/10/2015

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 log out immediately. This system may be monitored for operational purposes at any time.

>

Note: This screen can be used for monitoring of BUG(s), ERROR and AUD messages.

5.2. Administer IP Telephony Node

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

5.2.1. Obtain Node IP address

These Application Notes assume that the basic CS1000 configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 3000) in CS1000 IP network to work with Bell Canada SIP Trunking Service. For further information on CS1000, please consult the references in **Section 11**.

Log in to Element Manager as per **Section 5.1.1**. Select **System → IP Network → Nodes: Servers, Media Cards** and then click on the **Node ID** as shown in **Figure 6**.

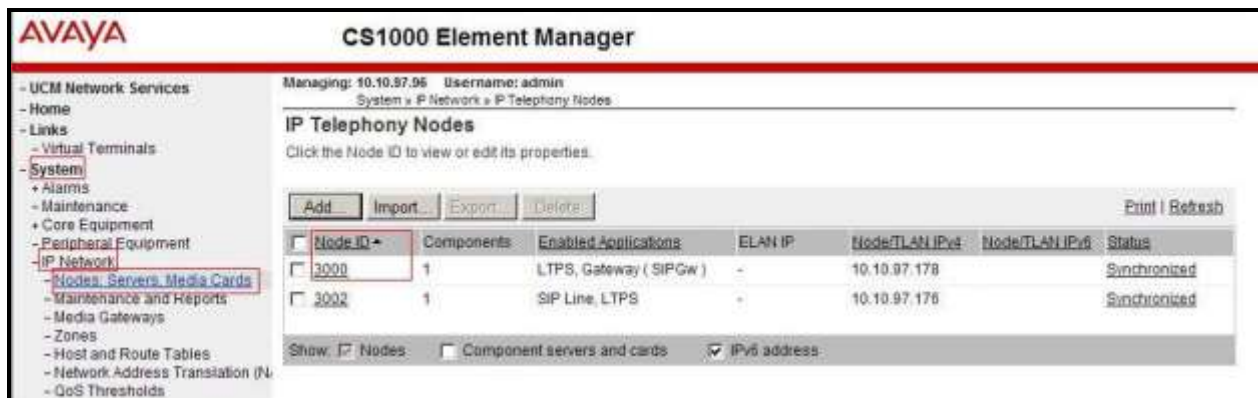


Figure 6 – IP Telephony Node

The **Node Details** screen is displayed in **Figure 7** with the IP address of the CS1000 node: **Call server IP address: 10.10.97.96**. The **Node IPv4 address 10.10.97.178** for **Telephony LAN (TLAN)** is a virtual address which corresponds to the **TLAN IPv4 address 10.10.97.177** of the Signaling Server/SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP address to communicate with other components to process SIP calls.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 3000 - LTPS, Gateway (SIPGw))

Node ID: 3000 * (0-9999)

Call server IP address: 10.10.97.96

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 10.10.97.65

Subnet mask: 255.255.255.192

Telephony LAN (TLAN)

Node IPv4 address: 10.10.97.178

Subnet mask: 255.255.255.192

Node IPv6 address:

* Required Value

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> car3-cores	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

Show ☐ IPVS applications

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

Figure 7 – Node Details 1

Scrolling down, the **Node Details** screen displays the **IP Telephony Node Properties** and **Applications** sections as shown in **Figure 8**.

Managing: 10.10.97.36 Username: admin
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 3000 - LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.192 * Subnet mask: 255.255.255.192 *
Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGV) and Coders
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCCN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value. [Save] [Cancel]

Associated Signaling Servers & Cards

[Select to add] [Add] [Remove] [Make Leader] [Print] [Refresh]

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
car3-cores	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

Show: ☐ IPv6 address

Figure 8 – Node Details 2

5.2.2. Administer Terminal Proxy Server (TPS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Terminal Proxy Server (TPS)** link as shown in **Figure 8**. Check the **UNISim Line Terminal Proxy Server** checkbox to enable proxy service on this node and then click the **Save** button as shown in **Figure 9**.

Managing: 10.10.97.36 Username: admin
System > IP Network > IP Telephony Nodes > Node Details > UNISim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 3000 - UNISim Line Terminal Proxy Server (LTPS) Configuration Details

UNISim Line Terminal Proxy Server ☒ Enable proxy service on this node

DTLS

DTLS policy: OFF

Options: ☐ Client authentication ☐ Periodic re-negotiation

Network Connect Server

* Required Value. [Save] [Cancel]

Note: Changes made on the page will NOT be transmitted until the node is saved.

Figure 9 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 8**. The default Diffserv values are shown in **Figure 10**. Click on the **Save** button.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with options like 'UCM Network Services', 'Home', 'Links', 'Virtual Terminals', 'System', 'Alarms', 'Maintenance', 'Core Equipment', 'Peripheral Equipment', 'IP Network', 'Nodes, Servers, Media Cards', 'Maintenance and Reports', 'Media Gateways', 'Zones', 'Host and Route Tables', 'Network Address Translation (NAT)', 'QoS Thresholds', 'Personal Directories', 'Unicode Name Directory', 'Interfaces', 'Engineered Values', 'Emergency Services', 'Geographic Redundancy', 'Software', 'Customers', 'Routes and Trunks', 'Routes and Trunks', 'D-Channels', 'Digital Trunk Interface', and 'Dialing and Numbering Plans'. The main content area is titled 'Node ID: 3000 - Quality of Service (QoS)'. It shows the 'Diffserv Codepoint (DSCP)' configuration. There are checkboxes for 'Enable Avaya automatic QoS', 'VLAN tagging', and '802.1Q support'. Below these are input fields for 'Control packets' (value 40), 'Voice packets' (value 40), and '802.1Q bits value (802.1P)' (value 0). A 'Save' button is highlighted at the bottom right.

Figure 10 – QoS Configuration Details

5.2.4. Synchronize New Configuration

Continuing from **Section 5.2.3**, return to the **Node Details** page (**Figure 7**) and click on the **Save** button. The **Node Saved** screen is displayed. Click on **Transfer Now**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar is the same as in Figure 10. The main content area is titled 'Node Saved'. It displays a message: 'Node ID: 3000 has been saved on the call server. The new configuration must also be transferred to associated servers and media cards.' Below this message are two buttons: 'Transfer Now' and 'Show Nodes'. The 'Transfer Now' button is highlighted.

Figure 11 – Node Saved Screen

The **Synchronize Configuration Files (Node ID <3000>)** screen is displayed. Check the **car3-cores** checkbox and click on **Start Sync**. When the synchronization completes, check the **car3-cores** checkbox and click on the **Restart Applications**.

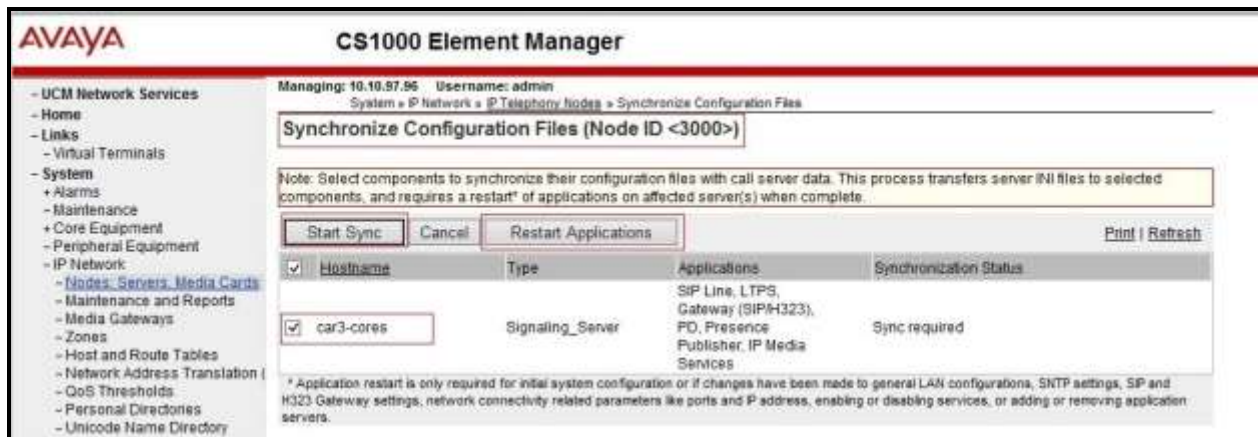


Figure 12 – Node Synchronized Screen

5.3. Administer Voice Codec

This section describes the steps to configure codecs for voice and media gateways.

5.3.1. Enable Voice Codec G.729A, G.711MU

Select **System** → **IP Network** → **Nodes: Servers, Media Cards** from the left pane and on the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed (see **Section 5.2.1** for more details). On the **Node Details** page shown in **Figure 8**, click on **Voice Gateway (VGW) and Codecs**.

Bell Canada SIP Trunking Service supports both G.729A, G.711MU during the compliance test. By default, Codec G711 was required on CS1000 configuration. Select **Voice payload size 20 milliseconds per frame** and uncheck **Voice Activity Detection (VAD)** checkbox for codec G711. Check **Codec G729** checkbox with **Voice payload size 20 milliseconds per frame**. Click on the **Save** button.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
System > IP Network > IP Telephony Nodes > Node Details > VGW and Codecs

Node ID: 3000 - Voice Gateway (VGW) and Codecs

General | Voice Codes | Fax

Codec G711: ☒ Enabled (required)
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 20 40 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Codec G722: ☐ Enabled
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

Codec G729: ☒ Enabled
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 20 40 (milliseconds)
Nominal Maximum

* Required Value

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Save Cancel

Figure 13 – Voice Gateway and Codec Configuration Details

Synchronize the new configuration (please refer to **Section 5.2.4**).

5.3.2. Enable Voice Codec on Media Gateways

From the left menu of the Element Manager page in **Figure 13**, select **System** → **IP Network** → **Media Gateways**. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page. In the following screen, scroll down to select the **Codec G711** (by default on CS1000) and **G.729A** with **Voice payload size 20 ms/frame** and uncheck **VAD** as shown in **Figure 14**. Scroll down to the bottom of the page and click on the **Save** button (not shown).

The screenshot displays the 'CS1000 Element Manager' interface. On the left is a navigation tree with categories like 'UCM Network Services', 'System', 'IP Network', 'Media Gateways', 'Zones', 'Host and Route Tables', 'Network Address Translation (NAT)', 'QoS Thresholds', 'Personal Directories', 'Unicode Name Directory', 'Interfaces', 'Engineered Values', 'Emergency Services', 'Geographic Redundancy', 'Software', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', 'Tools', and 'Security'. The 'Media Gateways' option is highlighted. The main content area is titled '- VGW and IP phone codec profile'. It contains various settings: 'Enable echo canceller' (checked), 'Echo canceller tail delay' (128 ms), 'Enable dynamic attenuation' (checked), 'Voice activity detection threshold' (1), 'Idle noise level' (0), 'R factor calculation' (unchecked), 'DTMF tone detection' (checked), 'Enable low latency mode' (unchecked), 'Remove DTMF delay (squelch DTMF from TDM to IP)' (checked), 'Enable modem/fax pass through mode' (checked), 'Enable V.21 FAX tone detection' (checked), 'Fax TCF method' (2), 'FAX maximum rate' (14400 bps), 'FAX playout nominal delay' (100 ms), 'FAX no activity timeout' (20 ms), and 'FAX packet size' (30). Below these are two sections for codec configuration. The first section, '- Codec G711', has 'Select' checked, 'Codec name G711', 'Voice payload size 20 (ms/frame)', and 'Voice playout (jitter buffer) nominal delay 20'. The second section, '- Codec G729A', has 'Select' checked, 'Codec name G729A', 'Voice payload size 20 (ms/frame)', and 'Voice playout (jitter buffer) nominal delay 20'. A 'VAD' checkbox is present and unchecked. Red text warnings state 'Modifications may cause changes to dependent settings'.

Figure 14 – Media Gateways Configuration Details

5.4. Zones and Bandwidth Management

This section describes the steps to create two zones: zone 10 for the VGW, IP phones; and zone 255 for the SIP Trunk.

5.4.1. Create Zone for IP Phones (Zone 10)

The following figures show how to configure a zone for VGW and IP phones for bandwidth management purposes. The bandwidth strategy can be adjusted to preference.

Select **System** → **IP Network** → **Zones** from the left pane (not shown), click on **Bandwidth Zones** as shown in **Figure 15**.

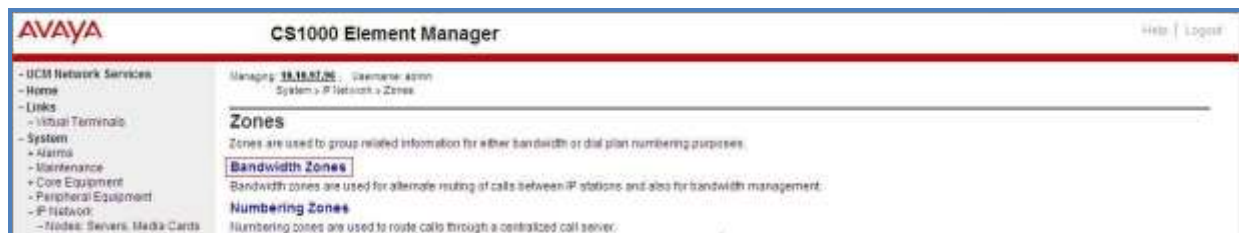


Figure 15 – Zones Page

The **Bandwidth Zones** screen is displayed as shown in **Figure 16**. Click **Add** to create a new zone for IP Phones.

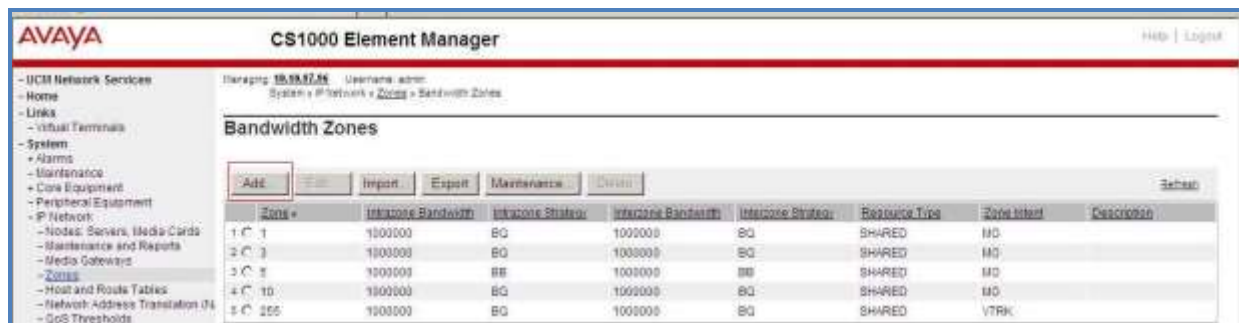


Figure 16 – Bandwidth Zones

Select and input the values as shown below (in the red boxes) in **Figure 17**, and click on the **Submit** button.

- **Intrazone Bandwidth (INTRA_BW): 1000000.**
- **Intrazone Strategy (INTRA_STGY):** Set codec for local calls. Select **Best Bandwidth (BB)** to use G.729 as the first priority codec for negotiation or select **Best Quality (BQ)** to use G.711 as the first priority codec for negotiation.
- **Interzone Bandwidth (INTER_BW): 1000000.**
- **Interzone Strategy (INTER_STGY):** Set codec for the calls over trunk. Select **Best Bandwidth (BB)** to use G.729 as the first priority codec for negotiation or select **Best Quality (BQ)** to use G.711 as the first priority codec for negotiation.
- **Zone Intent (ZBRN):** Select **MO (MO)** for IP phones, and VGW.

Input Description	Input Value
Zone Number (ZONE)	10
Intrazone Bandwidth (INTRA_BW)	1000000
Intrazone Strategy (INTRA_STGY)	Best Quality (BQ)
Interzone Bandwidth (INTER_BW)	1000000
Interzone Strategy (INTER_STGY)	Best Quality (BQ)
Resource Type (RES_TYPE)	Shared (SHARED)
Zone Intent (ZBRN)	MO (MO)
Description (ZDESC)	

Figure 17 – Bandwidth Management Configuration Details – IP phone

5.4.2. Create Zone for Virtual SIP Trunk (Zone 255)

Follow the steps described in **Section 5.4.1** to create a zone for the virtual SIP trunk. The difference is in the **Zone Intent (ZBRN)** field. Select **VTRK (VTRK)** for virtual trunk as shown in **Figure 18** and then click on the **Submit** button.

Input Description	Input Value
Zone Number (ZONE)	255
Intrazone Bandwidth (INTRA_BW)	1000000
Intrazone Strategy (INTRA_STGY)	Best Quality (BQ)
Interzone Bandwidth (INTER_BW)	1000000
Interzone Strategy (INTER_STGY)	Best Quality (BQ)
Resource Type (RES_TYPE)	Shared (SHARED)
Zone Intent (ZBRN)	VTRK (VTRK)
Description (ZDESC)	

Figure 18 – Bandwidth Management Configuration Details – Virtual SIP trunk

5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP connection between the SIP Signaling Gateway and Session Manager.

5.5.1. Integrated Services Digital Network (ISDN)

Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**.

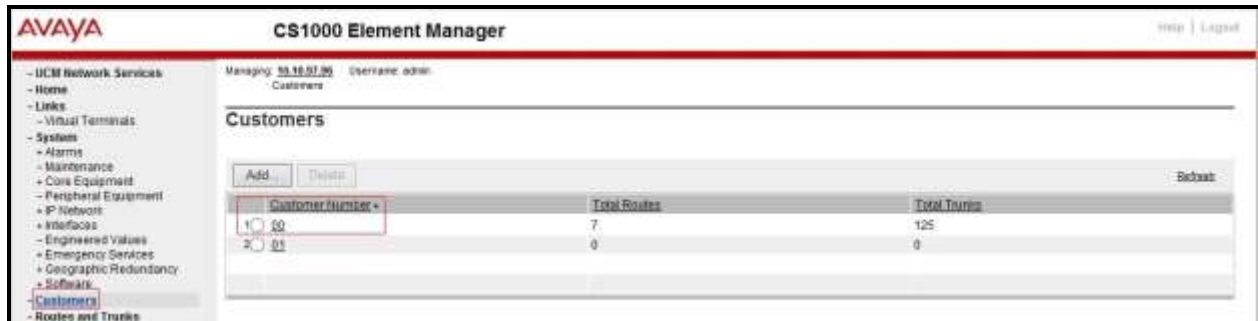


Figure 19 – Customer – ISDN Configuration 1

The system can support more than one customer with different network settings and options. The **Customer Details** page will appear. Select the **Feature Packages** option from **Customer Details** page.

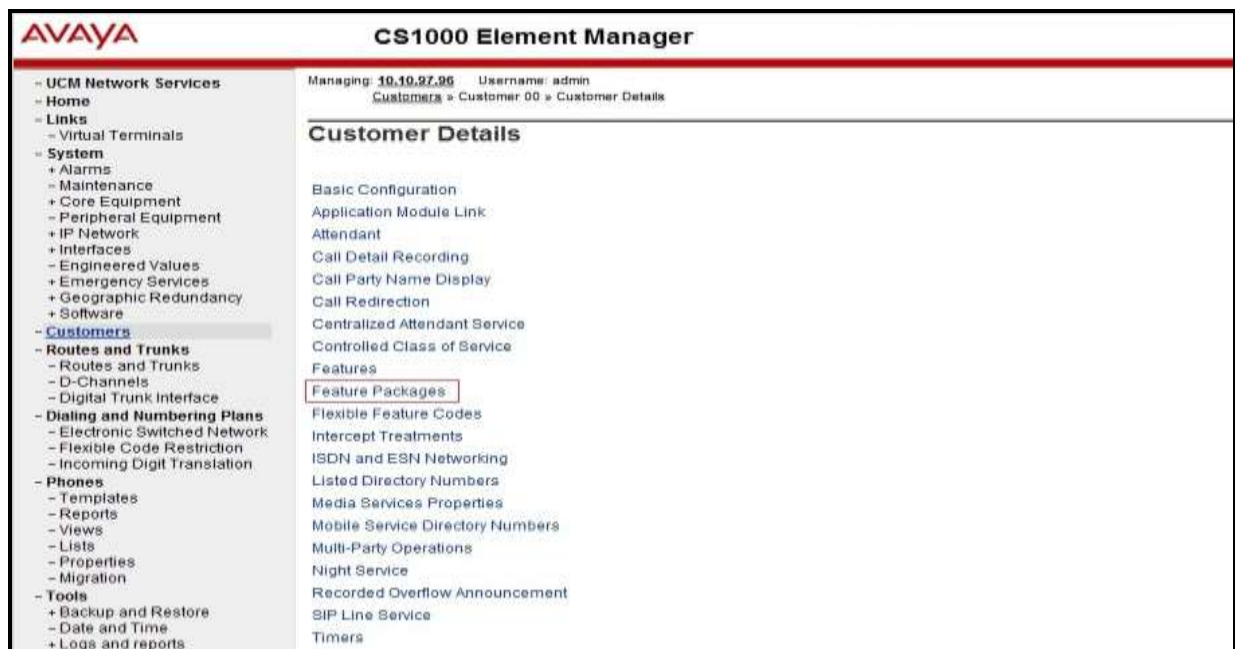


Figure 20 – Customer – ISDN Configuration 2

The screen is updated with a listing of available **Feature Packages** (not all features are shown in **Figure 21** below). Select **Integrated Services Digital Network** to edit the parameters shown below. Check the **Integrated Services Digital Network** option, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click on the **Save** button (not shown).

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
Customers » Customer 00 » Customer Details » Feature Packages

Feature Packages

+ Do Not Disturb Individual	Package: 9
+ End-to-End Signaling	Package: 10
+ Message Waiting Center	Package: 46
+ New Flexible Code Restriction	Package: 49
+ Set Relocation	Package: 53
+ Network Alternate Route Selection	Package: 58
+ Distinctive Ringing	Package: 74
+ Departmental Listed Directory Number	Package: 76
+ Command Status Link	Package: 77
+ Pretranslation	Package: 92
+ Dialed Number Identification System	Package: 98
+ Malicious Call Trace	Package: 107
+ Incoming Digit Conversion	Package: 113
+ Directed Call Pickup	Package: 115
+ Enhanced Music	Package: 119
+ Station Camp-On	Package: 121
+ Integrated Digital Access	Package: 122
+ Digital Private Network Signaling System 1	Package: 123
+ Flexible Tones and Cadences	Package: 125
+ Multifrequency Compelled Signaling	Package: 128
+ International Supplementary Features	Package: 131
+ Enhanced Night Service	Package: 133
- Integrated Services Digital Network	Package: 145

+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

- Virtual private network identifier: (1 - 16383)

- Private network identifier: (1 - 16383)

- Node DN:

Multi-location business group: (0 - 65535)

Business sub group consult-only: (0 - 65535)

Figure 21 – Customer – ISDN Configuration 3

5.5.2. Administer Avaya Communication Server 1000 SIP Trunk Gateway

Select **System** → **IP Network** → **Nodes: Servers, Media Cards** from the left pane. In the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as shown in **Figure 8, Section 5.2.1**.

On the **Node Details** screen, select **Gateway (SIPGw)**. Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 22**. The **SIP domain name** and **Local SIP port** should be matched in the configuration of Session Manager (in **Section 6.2**, and **6.6**).

The screenshot displays the AVAYA CS1000 Element Manager interface. The left navigation pane shows a tree structure with 'Nodes: Servers, Media Cards' selected. The main content area is titled 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details'. The 'General' tab is active, showing the 'Vtrk gateway application' set to 'SIP Gateway (SIPGw)'. Below this, several fields are highlighted with red boxes: 'SIP domain name' (jwdev.com), 'Local SIP port' (5060), 'Gateway endpoint name' (car3-ssg-carrier), 'Gateway password' (empty), and 'Application node ID' (3000). The 'Virtual Trunk Network Health Monitor' section on the right includes a checkbox for 'Monitor IP addresses' and a list of monitored IP addresses. The bottom of the screen shows a 'Save' button and a 'Cancel' button.

Figure 22 – Virtual Trunk Gateway Configuration Details

Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields and retain the default values for the remaining fields, as shown in **Figure 23**. Enter the IP address of Session Manager in the **Primary TLAN IP address** field. Enter **5060** for **Port** and select **UDP** for **Transport protocol**. This should be matched in the configuration of Session Manager (see in **Section 6.5.1**). Uncheck the **Support registration** checkbox.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes, Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory, 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, and Flexible Code Restriction. The main content area displays the 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details'. The 'SIP Gateway Settings' tab is selected. Under the 'Proxy or Redirect Server' section, the 'Primary TLAN IP address' is set to '10.33.10.43', the 'Port' is '5060', and the 'Transport protocol' is 'UDP'. The 'Support registration' checkbox is unchecked. The 'Secondary TLAN IP address' is set to '0.0.0.0', the 'Port' is '5060', and the 'Transport protocol' is 'TCP'. The 'Support registration' checkbox is also unchecked. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' There are 'Save' and 'Cancel' buttons at the bottom right.

Figure 23 – Virtual Trunk Gateway Configuration Details

On the same page as shown in **Figure 23**, scroll down to the **SIP URI Map** section. Under **Public E.164 domain names**, enter the following:

- **National:** leave this SIP URI field blank.
- **Subscriber:** leave this SIP URI field blank.
- **Special Number:** leave this SIP URI field blank.
- **Unknown:** leave this SIP URI field blank.

Under **Private domain names**, enter the following:

- **UDP:** leave this SIP URI field blank.
- **CDP:** leave this SIP URI field blank.
- **Special Number:** leave this SIP URI field blank.
- **Vacant number:** leave this SIP URI field blank.
- **Unknown:** leave this SIP URI field blank.

The remaining fields can be left at their default values as shown in **Figure 24**. Click on the **Save** button.

Figure 24 – Virtual Trunk Gateway Configuration Details

Synchronize the new configuration (please refer to **Section 5.2.4**).

5.5.3. Administer Virtual D-Channel

Select **Routes and Trunks** → **D-Channels** (not shown) from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list and type **DCH** as shown in **Figure 25**. Click on the **to Add** button.

Figure 25 – D-Channels

The **D-Channels 100 Property Configuration** screen is displayed next, as shown in **Figure 26**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D channel Card Type:** D-Channel is over IP (**DCIP**).
- **Designator:** A descriptive name.
- **User:** **Integrated Services Signaling Link Dedicated (ISLD)**.
- **Interface type for D-channel:** **Meridian Meridian1 (SL1)**.
- **Meridian 1 node type:** **Slave to the controller (USR)**.
- **Release ID of the switch at the far end:** **25**.

Click on **Advanced options (ADVOPT)**. Check on the **Network Attendant Service Allowed** checkbox under H323 Overlap Signaling Settings (H323) as shown in **Figure 26**. Other fields are left as default.

The screenshot displays the AVAYA CS1000 Element Manager interface for D-Channel Configuration. The left sidebar shows a navigation tree with categories like UCE Network Services, Links, System, and Customers. The main area is titled 'Basic Configuration' and contains a table with 'Input Description' and 'Input Value' columns. The 'Input Value' column shows the configured values for each field. The 'Advanced options (ADVOPT)' section is expanded, showing 'H323 Overlap Signaling Settings (H323)' with the 'Network Attendant Service Allowed' checkbox checked.

Input Description	Input Value
Action Device And Number (ADAN)	001
D channel Card Type	DCIP
Designator	VoIP
Recovery to Primary	<input type="checkbox"/>
PR1 loop number for Backup D-channel	
User	Integrated Services Signaling Link Dedicated (ISLD Co)
Interface type for D-channel	Meridian Meridian1 (SL1)
Country	ETS 300 102 basic protocol (ETSI)
D-Channel PRI loop number	
Primary Rate Interface	more PRI
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)
Integrated Services Signaling Link Maximum	4000 (Range: 1 - 4000)
Signaling server resource capacity	1800 (Range: 0 - 1700)
Layer 3 call control message count per 5 second time interval	300 (Range: 0 - 300)
Number of Status Enquiry Messages sent within 120 ms	1
Map channel number to time slots on a PRI2 loop	<input checked="" type="checkbox"/>
Overlap Receiving	<input type="checkbox"/>
Overlap Sending	<input type="checkbox"/>
Overlap Timer	
Multicast Business Group Allowed	<input type="checkbox"/>
Network Attendant Service Allowed	<input checked="" type="checkbox"/>

Figure 26 – D-Channel Configuration

Click on **Basic Options (BSCOPT)** and click on the **Edit** button on the **Remote Capabilities** field as shown in **Figures 27**.

AVAYA CS1000 Element Manager

Help | Logout

- UCM Network Services
 - Home
 - Links
 - Virtual Terminals
- System
 - Alarms
 - Maintenance
 - Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - Zones
 - Host and Route Tables
 - Network Address Translation (NAT)
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
- Interfaces
 - Engineered values
 - Emergency Services
 - Geographic Redundancy
 - Software
- Customers
- Routes and Trunks
 - Routes and Trunks
 - S-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

- Basic options (BSCOPT)

- Change protocol timer value (TMR)

- Advanced options (ADVOPT)

- Feature Packages

Action Device And Number (ADAN): DCH

D channel Card Type: DCP

Designator: VoIP

Recovery to Primary: ☐

PRF loop number for Backup D-channel:

User: Integrated Services Signaling Link Dedicated (IS-D)

Interface type for D-channel: Meridian (Meridian1 (SL1))

Country: ETS 300 =102 basic protocol (ETSI)

D-Channel PRF loop number:

Primary Rate Interface:

Secondary PRF loops:

Meridian 1 node type: Slave to the controller (UGR)

Release ID of the switch at the far end: 25

Central Office switch type: 100% compatible with Bellcore standard (STD)

Integrated Services Signaling Link Maximum: 4000 Range: 1 - 4000

Signalling server resource capacity: 1000 Range: 0 - 3700

Primary D-channel for a backup DCH: Range: 0 - 254

- PPS customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffer: 32

- D-channel transmission Rate: 56 kbps when LCMF is ALB (56K)

- Channel Negotiation option: No alternative acceptable, exclusive, (1)

- Remote Capabilities: Edit

- B channel Service messaging: ☐

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 27 – D-Channel Configuration

The **Remote Capabilities Configuration** page appears as shown in **Figures 28**. Check the **ND2** and the **MWI** checkboxes.

AVAYA CS1000 Element Manager

Managing: 18.16.37.26 username: admin
Route and Trunk > DCM0000 > DCM0000.100 Properties Configuration > Remote Capabilities Configuration

Remote Capabilities Configuration

Input Description	Input Value
Basic rate interface (BRI)	<input type="checkbox"/>
Call completion on busy using integer value (CCBI)	<input type="checkbox"/>
Call completion on busy using object identifier (CCBO)	<input type="checkbox"/>
Call completion on busy for GSK and EuroISDN BRI (CCBS)	<input type="checkbox"/>
Call completion on no response using integer value (CCNI)	<input type="checkbox"/>
Call completion on no response using object identifier (CCNO)	<input type="checkbox"/>
Call completion to no reply for GSK and EuroISDN BRI (CCNR)	<input type="checkbox"/>
Network call park (CPK)	<input type="checkbox"/>
Connected line identification presentation (COLP)	<input type="checkbox"/>
Call transfer integer (CTI)	<input type="checkbox"/>
Call transfer object (CTO)	<input type="checkbox"/>
Diversion info. is sent using integer value (DV1I)	<input type="checkbox"/>
Diversion info. is sent using object identifier (DV1O)	<input type="checkbox"/>
Rerouting requests processed using integer value (DV2I)	<input type="checkbox"/>
Rerouting requests processed using object identifier (DV2O)	<input type="checkbox"/>
Diversion info. sent. rerouting requests processed (DV3I)	<input type="checkbox"/>
EuroISDN -div. info sent. rerouting req. processed (DV3O)	<input type="checkbox"/>
Call transfer notification and invocation to EuroISDN (ECTO)	<input type="checkbox"/>
Multicous call identification (MCID)	<input type="checkbox"/>
ISDN QSIG conversion (ISQC)	<input type="checkbox"/>
Remote D-channel is on a MSOL card (MSL)	<input type="checkbox"/>
Message waiting interworking with DMS-100 (MWI)	<input checked="" type="checkbox"/>
Network access data (NAC)	<input type="checkbox"/>
Network call trace supported (NCT)	<input type="checkbox"/>
Network name display method 1 (ND1)	<input type="checkbox"/>
Network name display method 2 (ND2)	<input checked="" type="checkbox"/>
Network name display method 3 (ND3)	<input type="checkbox"/>
Name display - integer ID coding (NDI)	<input type="checkbox"/>
Name display - object ID coding (NDO)	<input type="checkbox"/>

Copyright © 2000-2011 Avaya Inc. All rights reserved.

Figure 28 – Remote Capabilities Configuration

Click on the **Return – Remote Capabilities** button (not shown).

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

5.5.4. Administer Virtual Super-Loop

Select **System** → **Core Equipment** → **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 **Figure 29**. In this example, Superloops 4, 96, 100, and 124 have been added and are being used.



Figure 29 – Administer Virtual Super-Loop Page

5.5.5. Administer Virtual SIP Routes

Select **Routes and Trunks** → **Routes and Trunks** (not shown) from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown in **Figure 30**.



Figure 30 – Add route

The **Customer 0, New Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed. Enter the following values for the specific fields, and retain the default values for the remaining fields. The screenshot of Basic Configuration section of existing route 100 is displayed to edit as shown in **Figure 31**.

- **Route data block (RDB) (TYPE):** RDB as default.
- **Customer number (CUST):** 0 as customer 0 is used.
- **Route number (ROUT):** Enter an available route number (example: route 100).
- **Designator field for trunk (DES):** A descriptive text (100).
- **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 (example: 8100).

- Check the **The route is for a virtual trunk route (VTRK)** field, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter **255** (created in Section 5.4.2). **Note:** The Zone value is filled out as 255, but after it is added, the screen is displayed with prefix 00.
- For the **Node ID of signaling server of this route (NODE)** field, enter the node number **3000** (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. Scrolling down to the bottom of the screen, enter the following values for the specified fields, and retain the default values for the remaining fields.
 - **Mode of operation (MODE):** Select **Route uses ISDN Signalling Link (ISLD)**.
 - **D channel number (DCH):** Enter **100** (created in Section 5.5.3).
 - **Interface type for route (IFC):** Select **Meridian M1 (SL1)**.
 - **Private network identifier (PNI):** Enter **1**. **Note:** The value is filled out as 1, but after it is added, the screen is displayed with prefix 0000.
 - **Network calling name allowed (NCNA):** Check this option to allow calling name display.
 - **Network call redirection (NCRD):** Check this option to allow call redirection.
 - **Insert ESN access code (INAC):** Check this option to insert ESN access code (refer to Section 0).

The screenshot shows the Avaya CS1000 Element Manager interface. The main window is titled 'Customer 0, Route 100 Property Configuration'. The 'Basic Configuration' tab is selected. The configuration fields are as follows:

- Route data block (RDB) (TYPE): [RDB]
- Customer number (CUST): [00]
- Route number (ROUT): [100]
- Designator field for trunk (DCE): [100]
- Trunk type (TRTP): [TR]
- Incoming and outgoing trunk (ICOG): [Incoming and outgoing (ICOG)]
- Access code for the trunk route (ACOG): [0100]
- Trunk type (ST1SP) (ST1SP): [ST1SP]
- The route is for a virtual trunk route (VTRK): [X]
- Zone for codec selection and bandwidth management (ZONE): [00255] (ID - 4000)
- Node ID of signaling server of this route (NODE): [3000] (ID - 9999)
- Protocol ID for the route (PCID): [SIP (SIP)]
- Print correlation ID in CDR for the route (ICDR): [X]
- Integrated services digital network option (ISDN): [X]
- Mode of operation (MODE): [Route uses ISDN Signalling Link (ISLD)]
- D channel number (DCH): [100] (ID - 254)
- Interface type for route (IFC): [Meridian M1 (SL1)]
- Private network identifier (PNI): [00001] (ID - 32700)
- Network calling name allowed (NCNA): [X]
- Network call redirection (NCRD): [X]
- Trunk route optimization (TRO): [X]
- Recognition of DTIS ABCD FALT signal for ISL (FALT): [X]
- Channel type (CHTY): [B-channel (BCH)]
- Call type for outgoing direct dialed TR route (CTRP): [Unicast Call type (UNCAST)]
- Insert ESN access code (INAC): [X]

Figure 31 – Route Configuration 1

Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)** checkboxes. Enter **1** for both **Day IDC tree number** and **Night IDC tree number** as shown in **Figure 32**. Click on the **Submit** button.

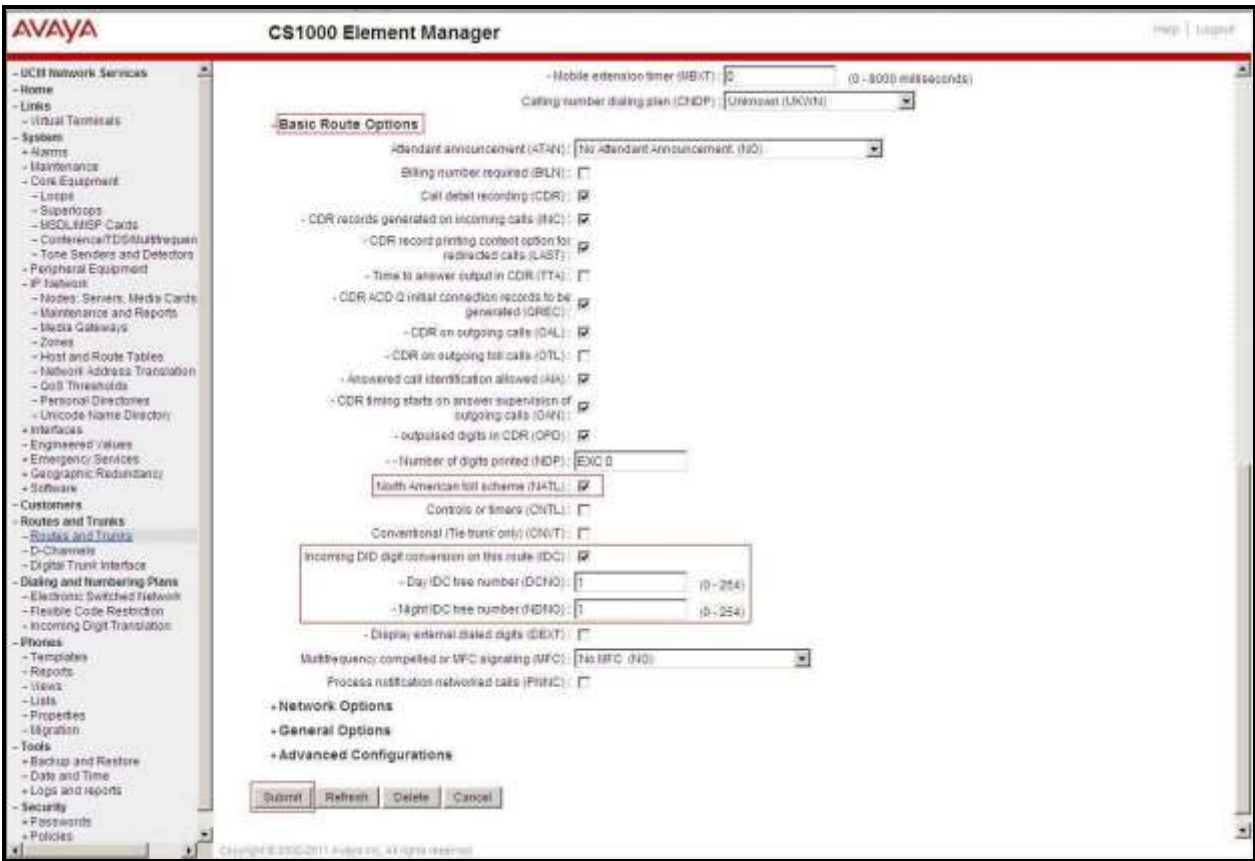


Figure 32 – Route Configuration 2

5.5.6. Administer Virtual Trunks

Select **Routes and Trunks** → **Route and Trunks** (not shown). The Route list is now updated with the newly added routes in **section 5.5.5**. In the example, Route 100 was being added. Click on the **Add trunk** button as shown in **Figure 33**.



Figure 33 – Routes and Trunks

The **Customer 0, Route 100, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service** (CLS) at the bottom of the basic trunk configuration page. Click on the **Edit** button as shown in **Figure 34**.

Note: The Multiple trunk input number (MTINPUT) field (not shown) may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created.

- **Trunk data block:** IP Trunk (**IPTI**).
- **Terminal Number:** Available terminal number (Superloop 100 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.
- **Card Density:** 8D.
- **Start arrangement Incoming:** Select **Immediate (IMM)**.
- **Start arrangement Outgoing:** Select **Immediate (IMM)**.
- **Trunk group access restriction:** Desired trunk group access restriction level.
- **Channel ID for this trunk:** An available starting channel ID.

Figure 34 – New Trunk Configuration

For **Media Security**, select **Media Security Never (MSNV)**. Enter the values for the specified fields as shown in **Figure 35**. Scroll down to the bottom of the screen and click **Return Class of Service** and click on the **Save** button (shown in **Figure 34**).

Input Description	Input Value
- ACD Priority	ACD Priority not required (APN)
- Analog Semi-Permanent Connections	Analog Semi-Permanent Connections Denied (SPCD)
- ARF Supervised COT	
- Barring	
- Battery Supervised COT	
- Bus/Tone Supervised COT	
- Calling Line Identification	
- Calling party	Calling party Denied (CND)
- Central Office Ringback	
- Centre Switchhook Flash	Centres Switchhook Flash Denied (THFD)
- Dial Pulse	Digitone (DTN)
- DTR PAD value	
- Echo Cancelling	Echo Cancelling Denied (ECD)
- Hong Kong DTI	
- Loop Break Supervised COT	
- Make-break rate for dial pulse	10 pulses per second (P10)
- Manual Incoming	Manual Incoming Denied (MID)
- Media Security	Media Security Never (MSNV)
- Network Hook Flash Over (NH1P)	
- Potency	
- Priority	Low Priority (LPR)
- Restriction level	Unrestricted (LPR)
- Reversed Ear Piece	Reversed Ear Piece denied (REP)
- Short or long line	
- Transmission Class of Service	Non-Transmission Compensated (NTC)
- Warning Tone	Warning Tone Allowed (WTA)
- Reversed Ear Piece	Reversed Ear Piece denied (REP)
- ARF Supervised COT	

Return Class of Service Cancel

Figure 35 – Class of Service Configuration

5.5.7. Administer Calling Line Identification Entries

Select **Customers** on the left pane, and then select **00 → ISDN and ESN Networking** (not shown). Click on **Calling Line Identification Entries** as shown in Figure 36.

AVAYA CS1000 Element Manager

Managing: 10.09.07.04 Username: admin
Customer 00 → Customer Details → ISDN and ESN Networking

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option:

Flexible orbiting prevention time:

Country code: (1 - 9999)

Core for processing the called number

National access code:

International access code:

Options: ☒ Transfer on ringing of supervised external trunks
☒ Connection of supervised external trunks

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan:

Private dialing plan for non-QD users: ☐ Coordinated dialing plan
☐ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls:

Stor: (1 - 4095)

Country code: (1 - 9999)

Core displayed as part of calling number

Calling Line Identification Entries

Save Cancel

Figure 36 – ISDN and ESN Networking

Click **Add** as shown in Figure 37.

AVAYA CS1000 Element Manager

Managing: 10.09.07.04 Username: admin
Customer 00 → Customer Details → ISDN and ESN Networking → Calling Line Identification Entries

Calling Line Identification Entries

Search for CLID

Start range:

End range:

Search

Calling Line Identification Entries

Add Cancel

Refresh

Figure 37 – Calling Line Identification Entries

The add entry **0** screen is displayed. Enter or select the following values for the specified fields and retain the default values for the remaining fields. The **Edit Calling Line Identification** screen of the existing entry 0 is displayed as shown in **Figure 38**.

- **National Code:** Leave it blank.
- **Local Code:** Input prefix digits assigned by Bell Canada SIP Trunking Service, in this case 6 digits – **613XXX**. This **Local Code** will be used for call display purpose for Call Type = Unknown.
- **Home Location Code:** Input the prefix digits assigned by Bell Canada SIP Trunking Service, in this case 6 digits – **613XXX**. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code:** Input prefix digits assigned by Bell Canada SIP Trunking Service, in this case 6 digits – **613XXX**. This **Local Steering Code** will be used for call display purpose for Call Type = Local Subscriber (NXX).
- **Use DN as DID:** YES.
- **Calling Party Name Display:** Uncheck **Roman characters**.

Note: For confidentiality and privacy purposes, actual 3 middle digits used for DID numbers in this testing have been masked and replaced with fictitious XXX throughout the document.

Click on the **Save** button as shown in **Figure 38**.

Figure 38 – Edit Calling Line Identification 0

5.5.8. Enable External Trunk to Trunk Transfer

This section shows how to enable the External Trunk to Trunk Transfer feature, which is a mandatory configuration to make call transfer and conference work properly over a SIP trunk.

Log in to Call Server Overlay CLI (please refer to **Section 5.1.2** for more details).
Allow External Trunk to Trunk Transfer for Customer Data Block by using **ld 15**.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 33600126  USED U P: 8345621 954062  TOT: 45579868
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 0
OPT
...
TRNX YES ← Enable transfer feature
EXTT YES ← Enable external trunk to trunk Transfer
...
```

5.6. Administer Dialing Plans

This section describes the steps to configure dialing plans for outbound and inbound calls.

5.6.1. Define ESN Access Codes and Parameters (ESN)

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 39**.

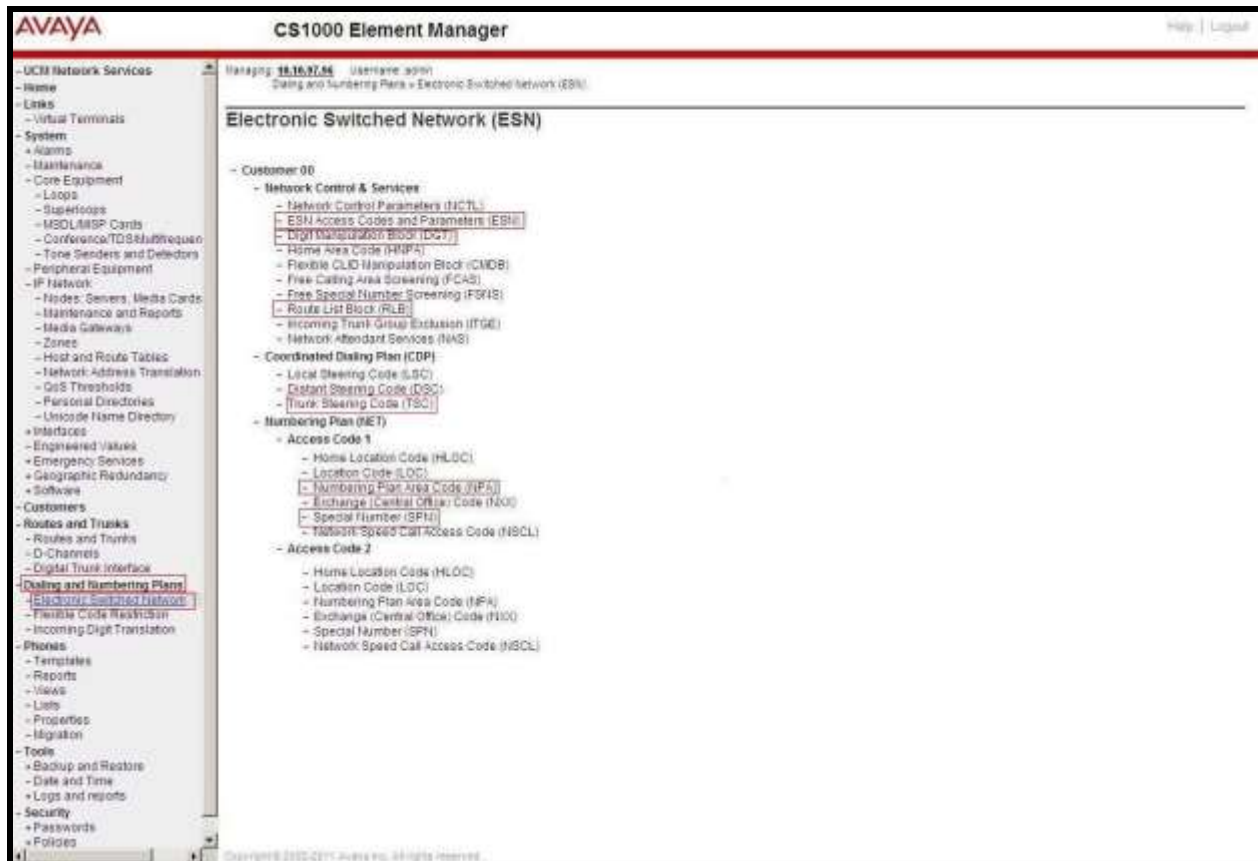


Figure 39 – ESN Configuration

On **Electronic Switched Network (ESN)** screen, select **ESN Access Codes and Parameters** to define **NARS/BARS Access Code 1** as shown in **Figure 40**.

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

Figure 40 – ESN Access Codes and Parameters

5.6.2. Associate NPA and SPN Call to ESN Access Code 1

Log in to Call Server CLI (please refer to **Section 5.1.2** for more details), change Customer Net Data block by using **ld 15**.

```
>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 0
OPT
AC2 xNPA xSPN ← Set NPA, SPN not to associate to ESN Access Code 2.
                  (With this setting, NPA and SPN are automatically associated to ESN Access Code 1)
FNP
CLID
...
```

Verify Customer Net Data block by using **ld 21**.

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

TYPE NET_DATA
CUST 00
OPT RTA
AC1 INTL NPA SPN NXX LOC ← NPA, SPN are associated to ESN Access Code 1
AC2
FNP YES
...
```

5.6.3. Digit Manipulation Block Index (DMI)

The following steps show how to add DMI for the outbound call. There is an index, which was added to the Digit Manipulation Block Index (14).

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 39** in **section 5.6.1**. Select **Digit Manipulation Block (DGT)**. The **Digit Manipulation Block List** is displayed as shown in **Figure 41**. In the **Please choose the** field, select an available **Digit Manipulation Block Index** from the drop-down list, and click on the **to Add** button.



Figure 41 – Add a DMI

The DMI 14 screen will open. In this testing, no leading digits are to be deleted, therefore, enter **0** for **Number of leading digits to be deleted** and select **NPA (NPA)** for **Call Type to be used by the manipulated digits** and then click on the **Submit** button as shown in **Figure 42**.

Figure 42 – DMI 14 Configuration

5.6.4. Route List Block Index (RLI 14)

This session shows how to add a RLI associated with the DMI created in **Section 5.6.3**. Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 39** in **section 5.6.1**. Select **Route List Block**.

Enter an available value in the textbox for the **Please enter a route list index** (in this case **14**) and click on the **to Add** button as shown in **Figure 43**. The screen shown in **Figure 44** will open.

Figure 43 – Add a Route List Block

Enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figure 44**. Scroll down to the bottom of the screen, and click on the **Submit** button (not shown).

- **Digit Manipulation Index: 14** (created in **Section 5.6.3**).
- **Incoming CLID Table: 0** (created in **Section 5.5.7**).
- **Route number: 100** (created in **Section 5.5.5**).

The screenshot displays the AVAYA CS1000 Element Manager web interface. The main title is 'CS1000 Element Manager'. The breadcrumb trail indicates the path: 'Managing: 10.10.10.10' > 'Username: admin' > 'Billing and Numbering Plans' > 'Electronic Switched Network (ESN)' > 'Customer CS' > 'Network Control & Services' > 'Route List Block' > 'Route List Block' > 'Data Entry of a Route List Block'.

The page is titled 'Data Entry of a Route List Block' and shows 'Route List Block Index: 14'.

General Properties

Entry Number for the Route List: 0

Indexes

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

Digit Manipulation Index: 14 (highlighted with a red box)

ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1000)

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: ☐

Incoming CLID Table: 0 (highlighted with a red box)

Options

Local Termination only: ☐

Route Number: 100 (highlighted with a red box)

Strip Conventional Signaling: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

Expensive Route: ☐

Strategy on Congestion: No Reroute (NRR)

CSG Alternate Routing Causes: CSG Alternate Routing Cause 1

Preferred Routing: Preferred Route 1

SDH Drop Back Back: Drop Back Disabled (DBD)

ISDN Off-Hook Queuing Option: ☐

Off-Hook Queuing Allowed: ☐

Figure 44 – RLI 14 Route List Block Configuration

5.6.5. Inbound Call – Incoming Digit Translation Configuration

This section describes the configuration steps required in order to receive calls from the PSTN via the Bell Canada SIP Trunking Service.

Select **Dialing and Numbering Plans** → **Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button as shown in **Figure 45**.

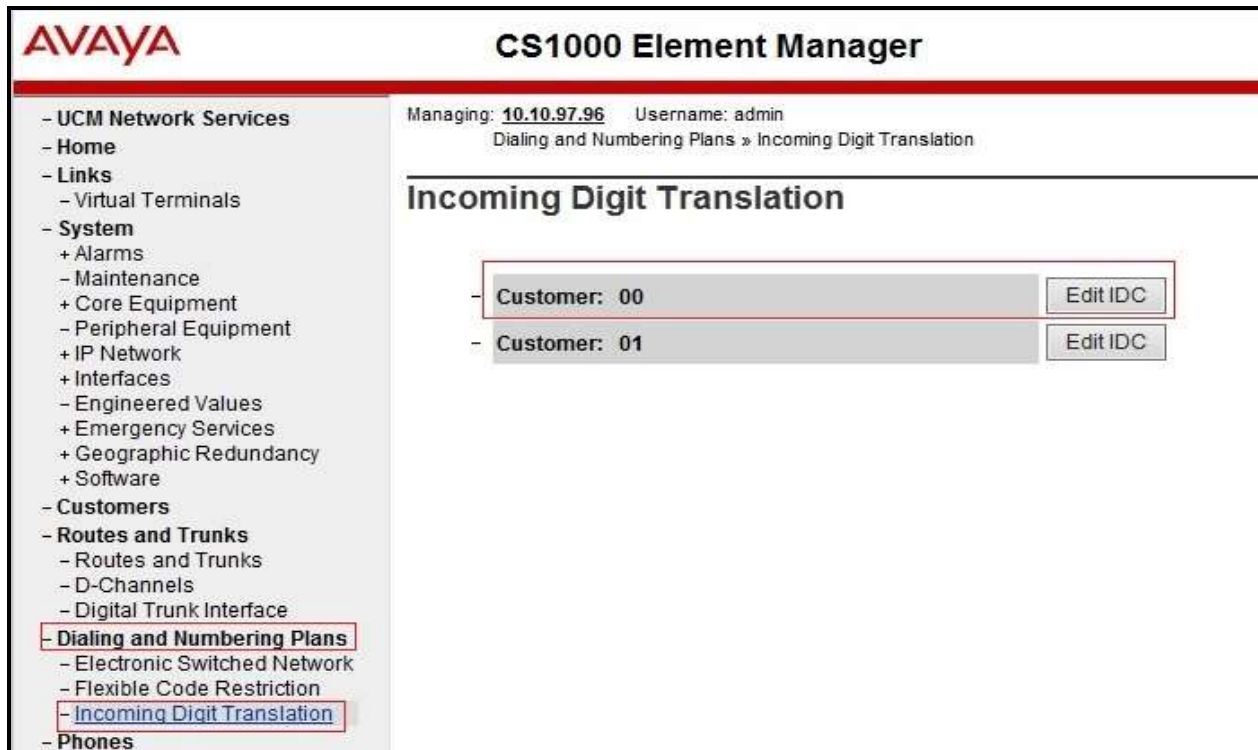


Figure 45 – Incoming Digit Translation

Click on the **New DCNO** to create the digit translation mapping. In this example, **Digit Conversion Tree Number 1** has been previously created and its **Edit DCNO** button is shown in **Figure 46**.



Figure 46 – Incoming Digit Conversion Property

Detailed configuration of the Digit Conversion Tree Configuration is shown in **Figure 47**. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the associated CS1000 system phone DN. This **DCNO** has been configured on route 100 as shown in **Figure 32** in **section 5.5.5**.

In the following configuration, the incoming call from the PSTN to DID with prefix **613XXX** will be translated to the associated DN with 4 digits. For testing purposes, DID number **613XXX6508** is translated to **1700** for voicemail testing.

Note: For confidentiality and privacy purposes, actual 3 middle digits used for DID numbers in this testing have been masked and replaced with fictitious XXX throughout the document.

Incoming Digits	Converted Digits	DCNO
613XXX6508	1700	Roman characters
613XXX6508	1700	Roman characters
613XXX6508	1700	Roman characters

Figure 47 – Digit Conversion Tree

5.6.6. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 0, 1800, 411, 4420, 911 and so on. These special numbers were associated to **Route list index 14** created in **Section 5.6.4**.

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as show in **Figure 39** in **section 5.6.1**. Select **Special Number (SPN)**. Enter a SPN number and then click on the **to Add** button. **Figure 48** shows all the special numbers used for this testing.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left-hand navigation pane shows a tree structure with 'Dialing and Numbering Plans' expanded, and 'Electronic Switched Network' selected. The main content area is titled 'Special Number List'. At the top, it says 'Managing: 10.10.97.96 Username: admin' and shows the breadcrumb path: 'Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 00 > Numbering Plan (NET) > Access Code 1 > Special Number List'. Below this, there is a 'Please enter a Special Number' input field and a 'to Add' button. The list contains five entries, each with a 'Special Number' label, an 'Edit' button, and configuration details: 'Flexible length', 'Inhibit time-out handler', 'Type of call that is defined by the special number', and 'Route list index'. All entries have a 'Route list index' of 14.

Special Number	Flexible length	Inhibit time-out handler	Type of call that is defined by the special number	Route list index
0	15	NO	NONE	14
1800	13	NO	NONE	14
411	4	NO	NONE	14
4420	14	NO	NONE	14
911	3	NO	NONE	14

Figure 48 – SPN numbers

5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

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)** as shown in **Figure 39** in section 5.6.1. Enter the area code desired in the textbox and click on the **to Add** button. The 1613, and 613 area codes were used in this configuration as shown in **Figure 49**. These area codes were associated to **Route List Index 14** created in **Section 5.6.4**.

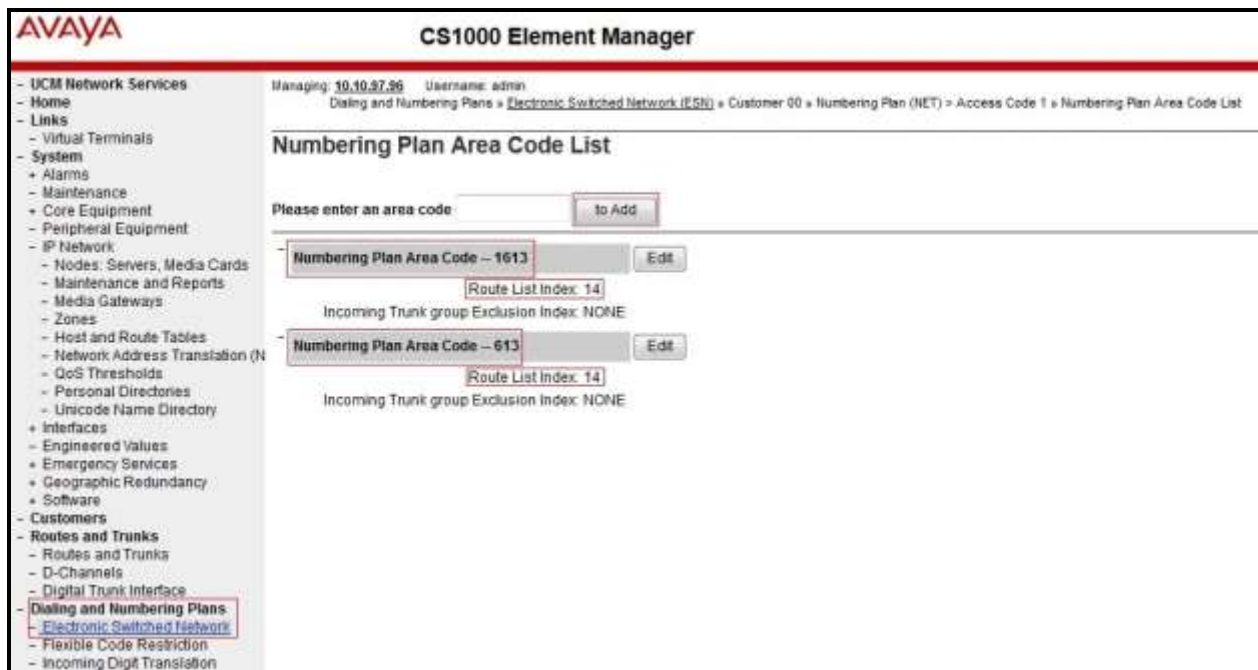


Figure 49 – Numbering Plan Area List

5.7. Administer a Phone

This section describes the creation of CS1000 clients used in this configuration.

5.7.1. Phone creation

Refer to **Section 5.5.4** to create a Virtual Superloop **96** used for IP phones. Refer to **Section 5.4.1** to create a bandwidth zone **10** for IP phones. Log in to the Call Server Command Line Interface (please refer to **Section 5.1.2** for more detail). Create an IP phone by using **ld 11** as shown below:

```
>ld 11
REQ: new
TYPE: 2002p2
TN 96 0 0 2
DATE
PAGE
DES
MODEL_NAME
EMULATED
DES 2002P2 ← Describe information for IP Phone
TN 96 0 00 02 VIRTUAL ← Set Terminal Number for IP Phone
TYPE 2002P2
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010 ← Set bandwidth zone for IP phone
CUR_ZONE 00010
MRT
ERL 12345
ECL 0
FDN
TGAR 0
LDN NO
NCOS 7
SGRP 0
RNPG 0
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBA WTA LPR MTD FNA HTA TDD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
```

```

UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0 USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3
MCBN FDSO NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
MSNV FRA PKCH MWTD DVLD CROD ELCD
CPND_LANG ENG
HUNT
PLEV 02
PUID
UPWD
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 6506 0   MARP ← Set the position of DN 6506 to display on key 0 of the phone
    CPND
        CPND_LANG ROMAN
            NAME Bell_01 ← Set name to display
            XPLN 13
            DISPLAY_FMT FIRST, LAST
    01
<Text removed for brevity>

```

5.7.2. Enable Privacy for the Phone

This section shows how to enable Privacy for a phone by changing its class of service (CLS). This feature cannot be enabled or disabled from the phone. By modifying the configuration of the phone created in **Section 5.7.1**, the display of the outbound call will be changed appropriately.

To hide the display number, set **CLS** (Class of Service) to **DDGD**. CS1000 will include “Privacy:id” in the SIP message header before sending it to Bell Canada SIP Trunking Service.

```

>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM CLS DDGD
...

```

To allow the display number, set **CLS** to **DDGA**. CS1000 will not send the Privacy header to Bell Canada SIP Trunking Service.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM CLS DDGA
...
```

5.7.3. Enable Call Forward for Phone

This section shows how to configure the Call Forward feature at the system and phone level.

Select **Customer** → **00** → **Call Redirection**. The Call Redirection page is shown in **Figure 50**.

- **Total redirection count limit: 0** (unlimited).
- **Call forward: Originating.**
- **Number of normal ringing cycles for CFNA: 3.**
- Click **Save** to save the configuration.

The screenshot displays the 'Call Redirection' configuration page in the AVAYA CS1000 Element Manager. The left sidebar shows a navigation tree with categories like 'UCM Network Services', 'System', 'IP Network', 'Interfaces', 'Customers', 'Dialing and Numbering Plans', 'Phones', 'Tools', and 'Security'. The main content area is titled 'Call Redirection' and includes the following settings:

- Call redirection by day:** Four input fields for days of the week (Option 0, 1, 2, 3).
- Redirection Holidays:** A checkbox for 'Do not disturb during'.
- Total redirection count limit:** A dropdown menu set to '0'.
- Options:** A group of checkboxes including 'Call forward reminder tone for 500/2500 sets', 'CFNA treatment for call waiting calls on a DN', 'DID call to second degree busy treatment', 'Message center' (checked), and 'Prevention of reciprocal call forward' (checked).
- Call forward:** Radio buttons for 'Originating' (selected) and 'Forwarding'.
- Number of normal ringing cycles for CFNA:** Three dropdown menus for Option 0, Option 1, and Option 2, all set to '3'.
- Number of distinctive ringing cycles for CFNA:** Three dropdown menus for Option 0, Option 1, and Option 2, all set to '3'.
- Calls routed to message center:** Three checkboxes for 'No answer DID calls', 'No answer non-DID calls', and 'DID calls to busy telephones'.

At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 50 – Call Redirection

To enable Call Forward All Call (CFAC) feature for a phone over SIP trunk, use **ld 11**. Change its **CLS** to **CFXA**, and **SFA**, then program the forward number on the phone set. The following is the configuration of a phone that has CFAC enabled with forwarding number **9613XXX5205**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2

ECHG yes
ITEM CLS CFXA SFA
ITEM key 19 CFW 16 9613XXX5205
```

To enable Call Forward Busy (CFB) feature for phone over SIP trunk, use **ld 11**. Change its **CLS** to **FBA**, **HTA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. The following is the configuration of a phone with CFB enabled to forwarding number **9613XXX5205**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2
ECHG yes
ITEM CLS FBA HTA SFA
ITEM HUNT 9613XXX5205
ITEM FDN 9613XXX5205
```

To enable Call Forward No Answer (CFNA) feature for a phone over SIP trunk, use **ld 11**. Change its **CLS** to **FNA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. The following is the configuration of a phone that has CFNA enabled with forwarding number **9613XXX5205**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2
ECHG yes
ITEM CLS FNA SFA
ITEM HUNT 9613XXX5205
ITEM FDN 9613XXX5205
```

6. Configure Avaya Aura® Session Manager

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

- SIP Domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to CS1000, Avaya SBCE and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which define route destinations and control call routing between the SIP Entities.
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call.

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

6.1. Avaya Aura® 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, enter an appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

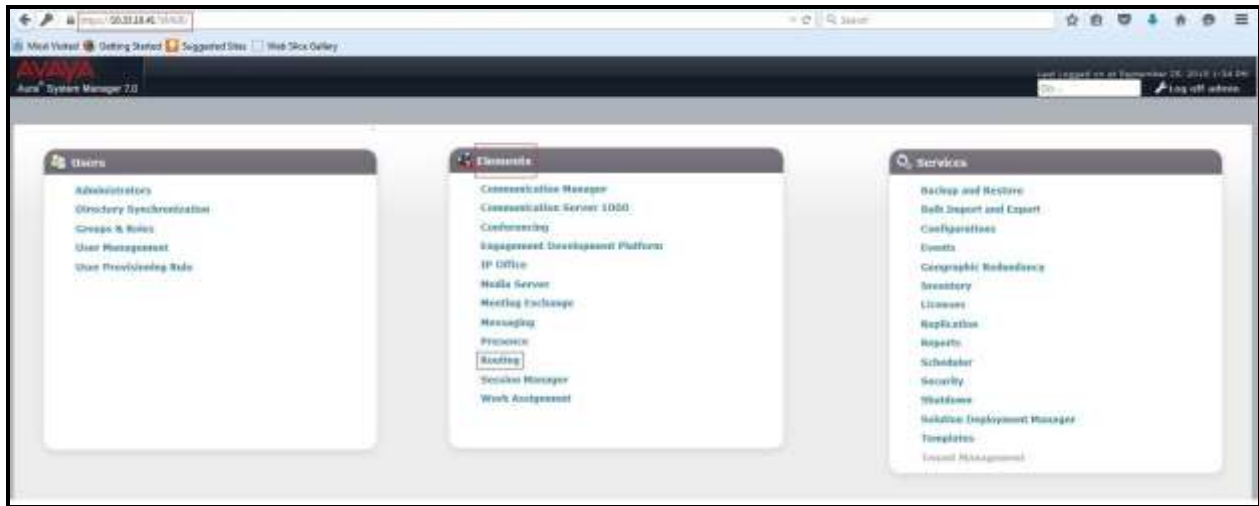


Figure 51 – System Manager Home Screen

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.

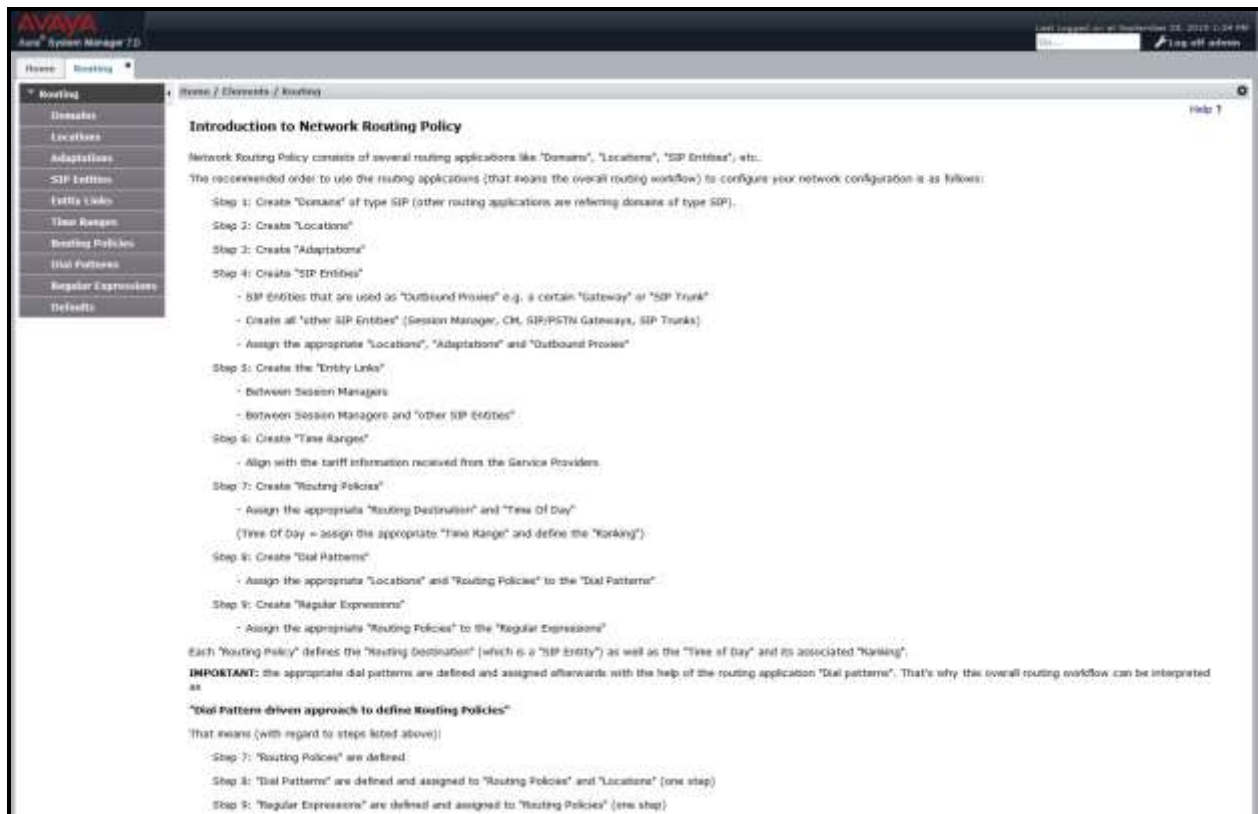


Figure 52 – Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bwvdev.com**.

Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), fill in the following:

- **Name:** Enter the domain name (refer to **Section 5.5.2**).
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

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

The screen below shows the configured entry for the enterprise domain.



Figure 53 – Domain Management

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. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville-GSSCP**, which includes all equipment in the enterprise including CS1000, Session Manager and Avaya SBCE.

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 new right pane that appears (shown below), fill in the following:

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

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

The screenshot shows the Avaya System Manager 7.0 interface. The left-hand navigation pane is open, showing the 'Routing' menu with sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The 'Locations' item is selected. The main content area is titled 'Location Details' and has a 'General' tab selected. The 'Name' field is filled with 'Belleville-GSSCP'. The 'Notes' field is empty. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox. The 'Overall Managed Bandwidth' section has fields for 'Managed Bandwidth Units' (Kb/sec), 'Total Bandwidth', and 'Multicast Bandwidth'. The 'Per-Call Bandwidth Parameters' section has fields for 'Maximum Multicast Bandwidth (Intra-Location)', 'Maximum Multicast Bandwidth (Inter-Location)', 'Minimum Multicast Bandwidth', and 'Default Audio Bandwidth'.

Figure 54 – Location Configuration

In the **Location Pattern** section, click **Add** to enter IP Address patterns. The following patterns were used in testing:

- **IP Address Pattern: 10.33.*, 10.10.97.*, 10.10.98.***

Click **Commit** to save.

Displayed below are the screenshots for location **Belleville-GSSCP**, which includes all equipment on the **10.33.***, **10.10.98.*** and **10.10.97.*** subnet including CS1000, Session Manager and Avaya SBCE.

The screenshot shows a web interface titled "Location Pattern". At the top left, there are "Add" and "Remove" buttons. Below them, it says "3 Items" and "Refresh". On the top right, there is a "Filter: Enable" link. The main area is a table with two columns: "IP Address Pattern" and "Notes". There are three rows in the table, each with a checkbox in the first column and a text input field in the second column. The first row has the pattern "10.33.*", the second row has "10.10.97.*", and the third row has "10.10.98.*". At the bottom left, there is a "Select: All, None" dropdown. At the bottom right, there are "Commit" and "Cancel" buttons.

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	10.33.*	
<input type="checkbox"/>	10.10.97.*	
<input type="checkbox"/>	10.10.98.*	

Figure 55 – IP Ranges Configuration

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

6.4. Configure Adaptations

An Adaptation is configured to format the History Info on CS1000 to be compatible with other Avaya products. To add a new adaptation, select **Routing** → **Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the adaptation. Select **CS1000Adapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click **Add** button to add **Name** as **fromto** and **Value** as **true**. Click the **Commit** button after changes are completed.



Figure 56 - CS1000 Adaptation

An adaptation is configured to convert the History Info to Diversion Header and to remove MIME. To add a new adaptation, select **Routing** → **Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the adaptation. Select **DiversionTypeAdapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click **Add** button to add **Name** as **MIME** and **Value** as **no**. Click the **Commit** button after changes are completed.

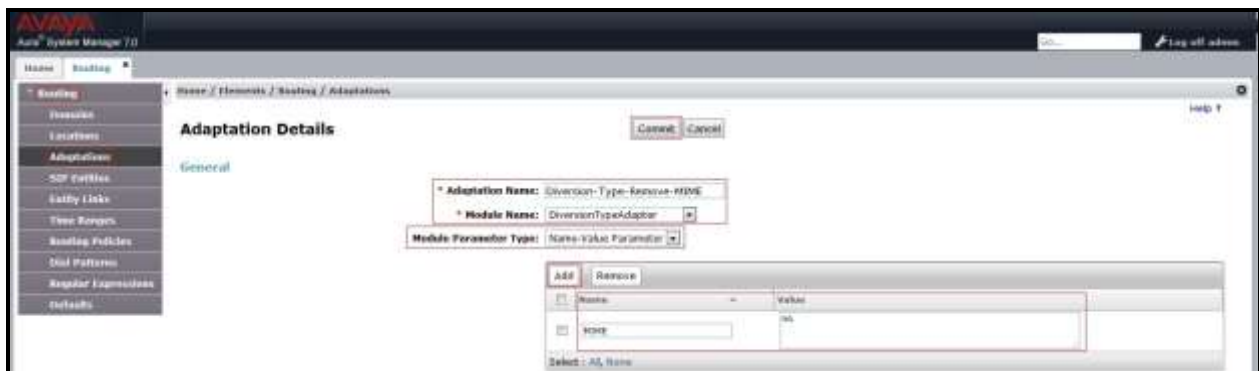


Figure 57 – Diversion Header Adaptation

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes CS1000 and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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, **Other** for CS1000 and Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate Adaptation module that will be applied to the SIP Entity being created.
- **Location:** Select the Location that applies to the SIP Entity being created defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

In this configuration, there are three SIP Entities:

- Session Manager SIP Entity.
- Communication Server 1000 SIP Entity.
- Avaya Session Border Controller for Enterprise SIP Entity.

6.5.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **bvwasm2**. The IP address of Session Manager's signaling interface **10.33.10.43** is entered for **FQDN or IP Address**. The user will need to select the specific values for the **Location** and **Time Zone**.

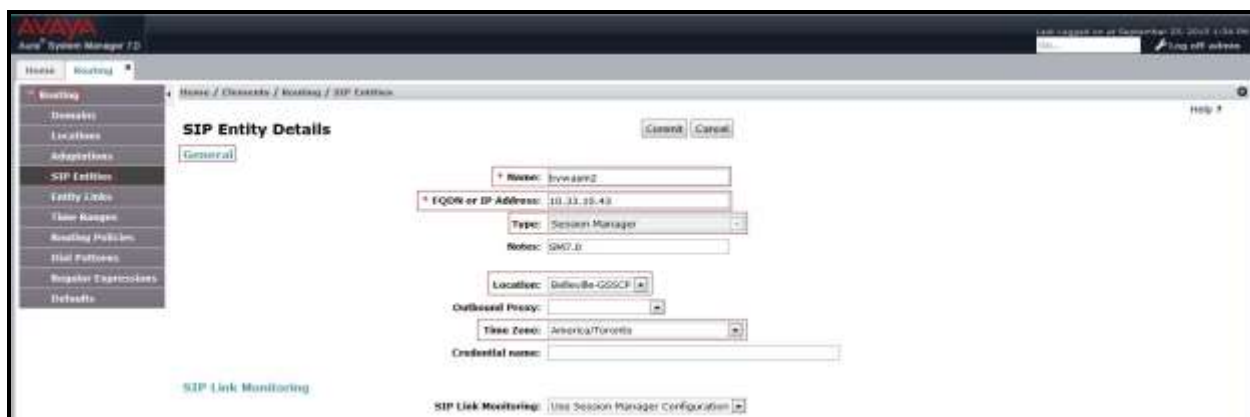


Figure 58 – Session Manager SIP Entity

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 listens for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

Defaults can be used for the remaining fields. Click the **Commit** button (not shown) to save. The compliance test used port **5060** with **UDP** for connecting to CS1000 and Avaya SBCE.



Port	Protocol	Default Domain	Notes
5060	UDP	bvwdev.com	

Figure 59 – Session Manager SIP Entity Port

6.5.2. Configure Communication Server 1000 SIP Entity

The following screen shows the addition of the CS1000 SIP Entity named **car3-ssg-carrier**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to CS1000, it is necessary to create a separate SIP Entity for CS1000, in addition to the one created at Session Manager, for use with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of CS1000 signaling Node **10.10.97.178**. Select **Type** as **Other**. Select **Adaptation** as **CS1K76_Adaptation** (created in **Section 6.4**). The user will need to select the specific values for the **Location** and **Time Zone**.

The screenshot displays the 'SIP Entity Details' configuration window in Avaya System Manager 7.0. The left sidebar shows a navigation menu with options like Domains, Locations, Adaptations, SIP Entities, and others. The main area is titled 'SIP Entity Details' and contains the following fields and settings:

- Name:** car3-ssg-carrier
- FQDN or IP Address:** 10.10.97.178
- Type:** Other
- Adaptation:** CS1K76_Adaptation
- Location:** Ballerina-COSCP
- Time Zone:** America/Toronto
- SIP Timer B/F (in seconds):** 5
- Credential name:** (empty field)
- Securable:** (checkbox, unchecked)
- Call Detail Recording:** none
- ConnProfile Type Preference:** (dropdown menu)
- Loop Detection:** (checkbox, unchecked)
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Link Monitoring Enabled
- Proactive Monitoring Interval (in seconds):** 300
- Reactive Monitoring Interval (in seconds):** 120
- Number of Retries:** 1

Figure 60 – Communication Server 1000 SIP Entity

6.5.3. Configure Avaya SBCE SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE named **SBCE**. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE's private network interface **10.10.98.13**. Select **Type** as **Other**. Select **Adaptation** as **Diversion-Type-Remove-MIME** (created in **Section 6.4**). The user will need to select the specific values for the **Location** and **Time Zone**.

The following screenshot shows the SIP Entity for Avaya SBCE.

The screenshot displays the Avaya System Manager 7.0 web interface. The left-hand navigation pane shows a tree structure with 'Routing' selected, and 'SIP Entities' highlighted under the 'Routing' folder. The main content area is titled 'SIP Entity Details' and shows the configuration for an entity named 'SBCE'. The 'FQDN or IP Address' field is set to '10.10.98.13', and the 'Type' is set to 'Other'. The 'Adaptation' is set to 'Diversion-Type-Remove-MIME'. The 'Location' is set to 'Belleville-OS55CP' and the 'Time Zone' is set to 'America/Toronto'. Other fields include 'SIP Timer B/F (in seconds)' set to 4, 'Credential name' (empty), 'Securable' (unchecked), 'Call Detail Recording' set to 'none', 'CrossProfile Type Preference' (empty), 'Loop Detection Mode' set to 'Off', 'SIP Link Monitoring' set to 'Link Monitoring Enabled', 'Proactive Monitoring Interval (in seconds)' set to 900, 'Reactive Monitoring Interval (in seconds)' set to 120, and 'Number of Retries' set to 1. The interface includes 'Go Back' and 'Cancel' buttons at the top right of the form area.

Figure 61 – Avaya SBCE SIP Entity

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an entity link. Two entity links were created: one to CS1000 and one to Avaya SBCE.

To add an entity link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager being used.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Connection Policy:** Select **trusted**. Note: If this box is not selected as trusted, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

Click **Commit** to save.

The following screen illustrates the Entity Link to the CS1000. The protocol and ports defined here must match the values used for the CS1000 signaling in **Section 5.5.2**.



Figure 62 – Communication Server 1000 Entity Link

The following screen illustrates the Entity Link to Avaya SBCE. The protocol and ports defined here must match the values used for Avaya SBCE mentioned in **Section 7.2.4**, later in this document.



Figure 63 – Avaya SBCE Entity Link

6.7. Configure Time Ranges

Time Ranges are configured for time-based routing. In order to add Time Ranges, select **Routing** → **Time Ranges** in the left-hand navigation pane and then click **New** button in the right pane. The Routing Policies shown subsequently will use the **24/7** range since time-based routing was not the focus of these Application Notes.



Figure 64 – Time Ranges

6.8. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added: one for the CS1000 and one for Avaya SBCE. To add a Routing Policy, navigate to **Routing** → **Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

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

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

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

The following screen shows the **Routing Policy Details** for the policy named **BellCanada_Inbound_To_CS1K** associated with incoming PSTN calls from the Bell Canada SIP Trunking Service to the CS1000. Observe the **SIP Entity as Destination** is the entity named **car3-ssg-carrier**.



Figure 65 – Routing to Communication Server 1000

The following screen shows the **Routing Policy Details** for the policy named **BellCanada_Outbound_To_SP4**. This is associated with outgoing calls from the CS1000 to the PSTN via the Bell Canada SIP Trunking Service, through Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.



Figure 66 – Routing to Avaya SBCE

6.9. Add Dial Patterns

Dial Patterns are used to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from the CS1000 to the Bell Canada SIP Trunking Service and vice versa. Dial Patterns define which Route Policy will be selected as route destination 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-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

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

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

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns (e.g., 1800, 411, etc.) were similarly defined.

The following screen shows that outbound dialed numbers with a maximum of 10 digits that begin with **6139** and have a destination SIP Domain of **bwvdev.com** use the Routing Policy Names **BellCanada_Outbound_To_SBCE** as defined in **Section 6.8**.

Dial Pattern Details

Pattern: 6139
Min: 10
Max: 10
Emergency Call: ☐
Emergency Priority:
Emergency Type:
SIP Domain: bwvdev.com
Refers: Bell Canada Outbound Calls

Originating Locations and Routing Policies

Originating Location Name	Originating Location Notes	Routing Policy Name	Route	Routing Policy (Shaded)	Routing Policy Destination	Routing Policy Notes
-ALL-		BellCanada_Outbound_To_SBCE			SBCE	

Figure 67 – Dial Pattern 6139

Note that with the above dial pattern, the Bell Canada did not restrict outbound calls to this specific Canada area code. In real deployments, appropriate restriction can be exercised per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed back to the PSTN.

The following screen shows that inbound 10-digit numbers that start with **6132** use Routing Policy Name **BellCanada_Inbound_To_CS1K** as defined in **Section 6.8**. This Dial Pattern matches the DID numbers assigned to the enterprise by Bell Canada SIP Trunking Service.

Dial Pattern Details

Pattern: 6132
 Min: 10
 Max: 10
 Emergency Call: ☐
 Emergency Priority: 1
 Emergency Type:
 SIP Domain: brodev.com
 Notes: Bell Canada Inbound Calls

Originating Location and Routing Policies

Originating Location Name	Originating Location Notes	Routing Policy Name	Route	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		BellCanada_Inbound_To_CS1K	1	<input type="checkbox"/>	car5-egw-camr	

Figure 68 – Dial Pattern 6132

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

Dial Patterns

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
6	1	15	<input type="checkbox"/>			brodev.com	Bell Canada Outbound Calls
1013	9	11	<input type="checkbox"/>			brodev.com	Bell Canada Outbound Calls
1800	9	11	<input type="checkbox"/>			brodev.com	Bell Canada Outbound Calls
411	3	3	<input type="checkbox"/>			brodev.com	Bell Canada Outbound Calls
4420	4	14	<input type="checkbox"/>			brodev.com	Bell Canada International Outbound Calls
6132	10	10	<input type="checkbox"/>			brodev.com	Bell Canada Inbound Calls
6135	10	10	<input type="checkbox"/>			brodev.com	Bell Canada Outbound Invalid Calls
6137	4	36	<input type="checkbox"/>			brodev.com	Bell Canada Outbound Calls
6138	10	10	<input type="checkbox"/>			brodev.com	Bell Canada Outbound Calls
811	3	3	<input type="checkbox"/>			brodev.com	Bell Canada Outbound Calls

Figure 69 – Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the Bell Canada system.

In this test configuration as shown in **Figure 1**, the Avaya elements reside on the Private side and the Bell Canada system resides on the Public side of the network.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, refer to the documentation listed in **Section 11** of these Application Notes.

7.1. Log in Avaya Session Border Controller for Enterprise

Access the web interface by typing “<https://x.x.x.x/sbc/>” (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the **Username** and **Password**.



Figure 70 - Avaya SBCE Login

The **Dashboard** main page will appear as shown below.

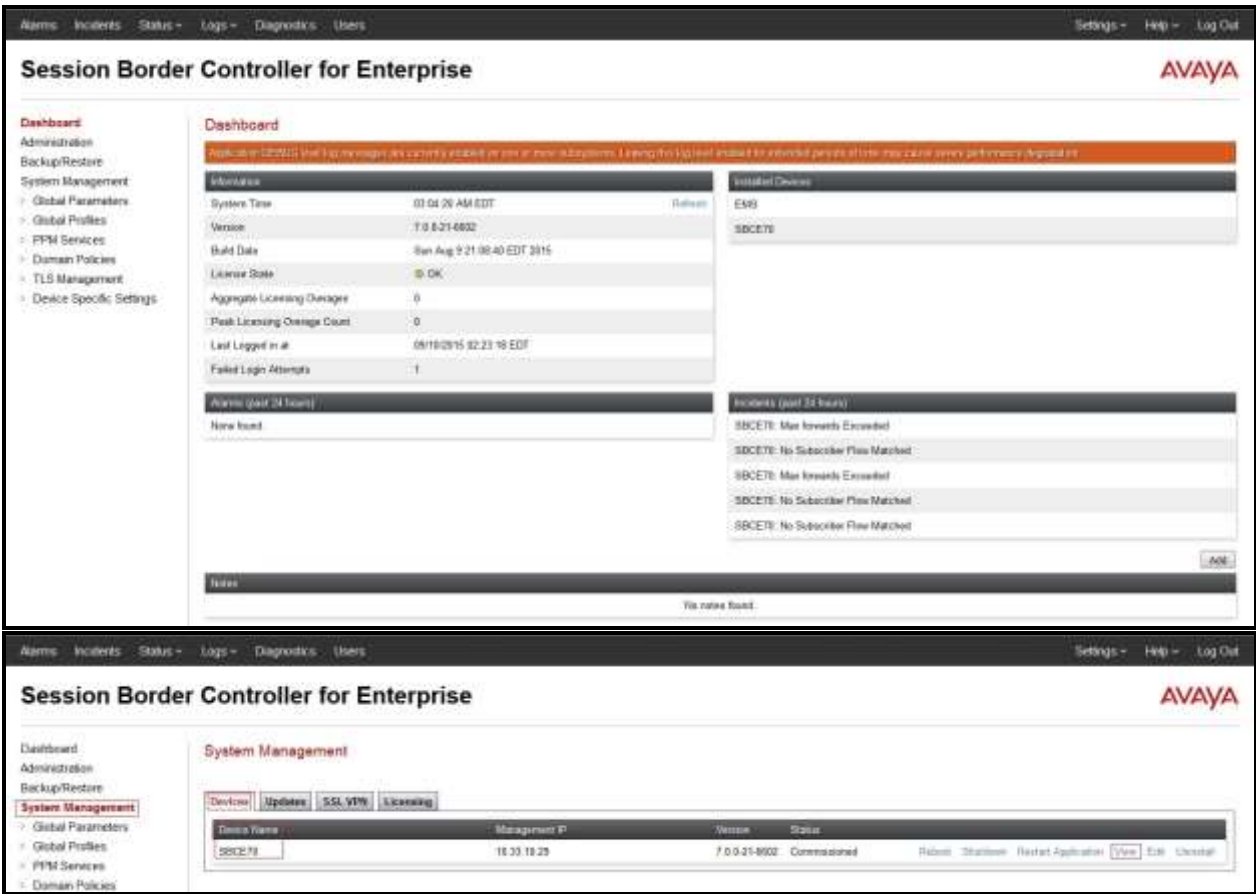


Figure 71 - Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance test, a single Device Name **SBCE70** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.



Figure 72 - Avaya SBCE System Management

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponded to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**.

System Information: SBCE70

General Configuration

Appliance Name SBCE70
Box Type SIP
Deployment Mode Proxy

Device Configuration

HA Mode No
Two Bypass Mode No

License Allocation

Standard Sessions 0
Requested: 0
Advanced Sessions 0
Requested: 0
Scopia Video Sessions 0
Requested: 0
CES Sessions 0
Requested: 0
Encryption ☒

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.98.13	10.10.98.13	255.255.255.192	10.10.98.1	A1
10.10.98.111	10.10.98.111	255.255.255.224	10.10.98.97	B1
10.10.98.99	10.10.98.99	255.255.255.224	10.10.98.97	B1
10.10.98.21	10.10.98.21	255.255.255.192	10.10.98.1	A1

DNS Configuration

Primary DNS 10.10.98.60
Secondary DNS
DNS Location DMZ
DNS Client IP 10.10.98.13

Management IP(s)

IP 10.33.10.29

Figure 73 - Avaya SBCE System Information

7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Configure Server Interworking Profile - Avaya Session Manager

Server Interworking profile allows administrator to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking**.

- Select **avaya-ru** in **Interworking Profiles**.
- Click **Clone**.
- Enter **Clone Name: SMVM** and click **Finish** (not shown).

The following screen shows that Session Manager server interworking profile (named: **SMVM**) was added.

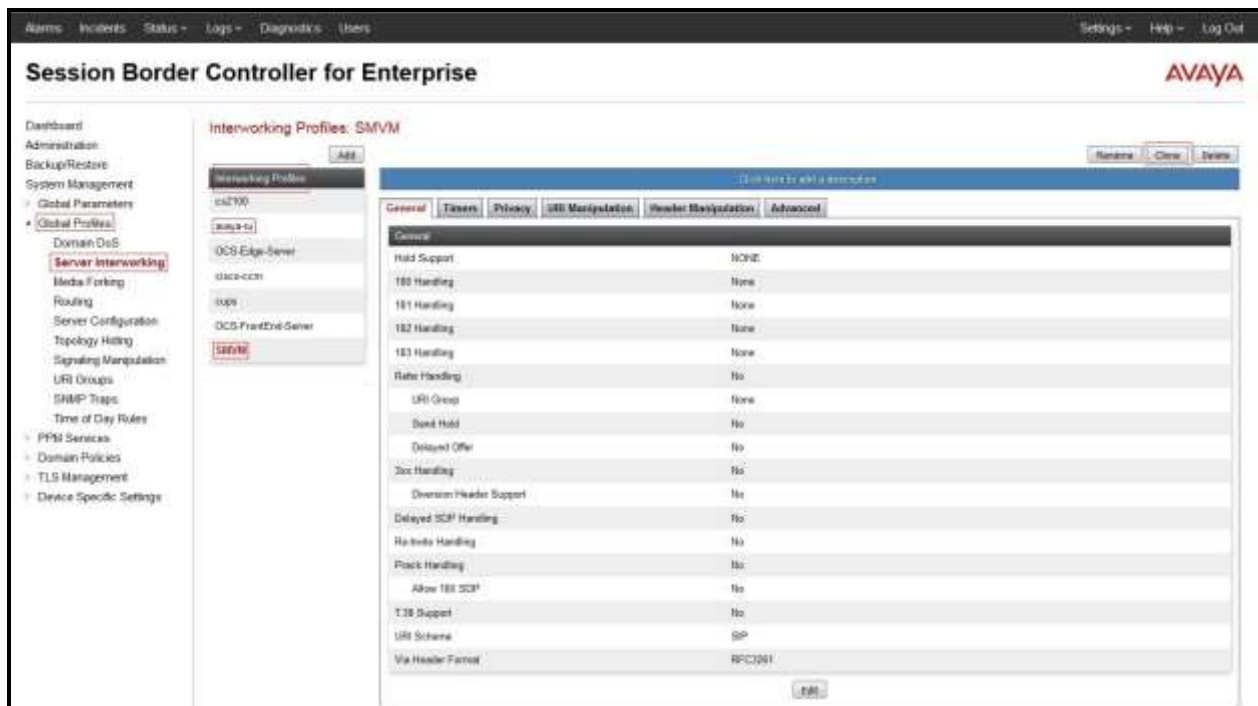


Figure 74 - Server Interworking – Avaya site

From the list of **Interworking Profiles**, click on **SMVM** to edit.

- On the **Header Manipulation** tab, click **Add** button to add a rule:
 - **Header: RequestURI.**
 - **Action: Add Parameter w/ [Value].**
 - **Parameter: maddr.**
 - **Value: 10.10.97.178** (This is CS1000 Node IP Address).
 - Click **Finish**.

Note: This configuration for a workaround to fix BYE issue mentioned in **Section 2.2**.

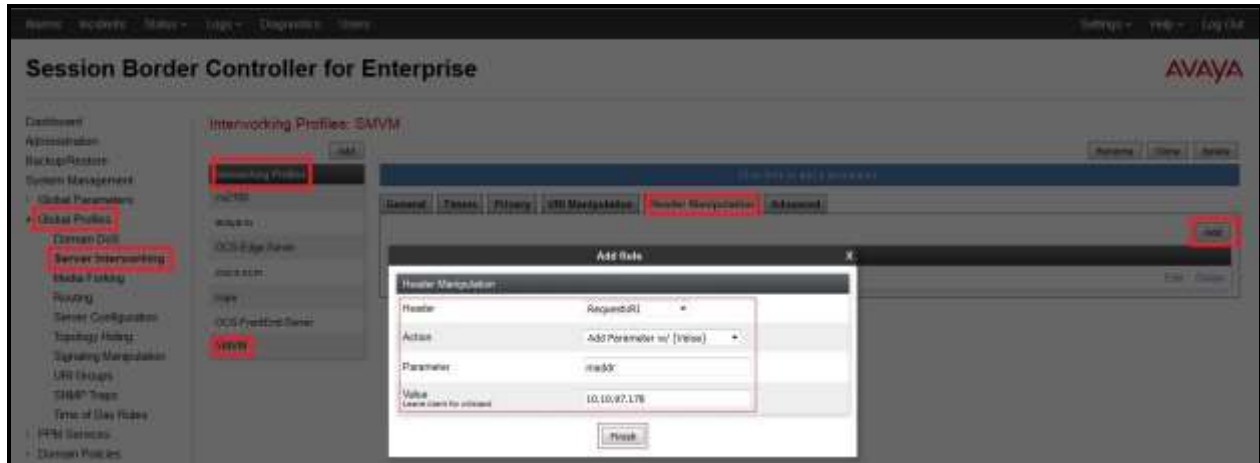


Figure 75 - Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – Bell Canada

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking** → **Add**.

- Enter **Profile Name: SP4** (not shown).
- Click **Next** button to leave all options at default. Click **Finish** (not shown).

The following screen shows that Bell Canada server interworking profile (named: **SP4**) was added.

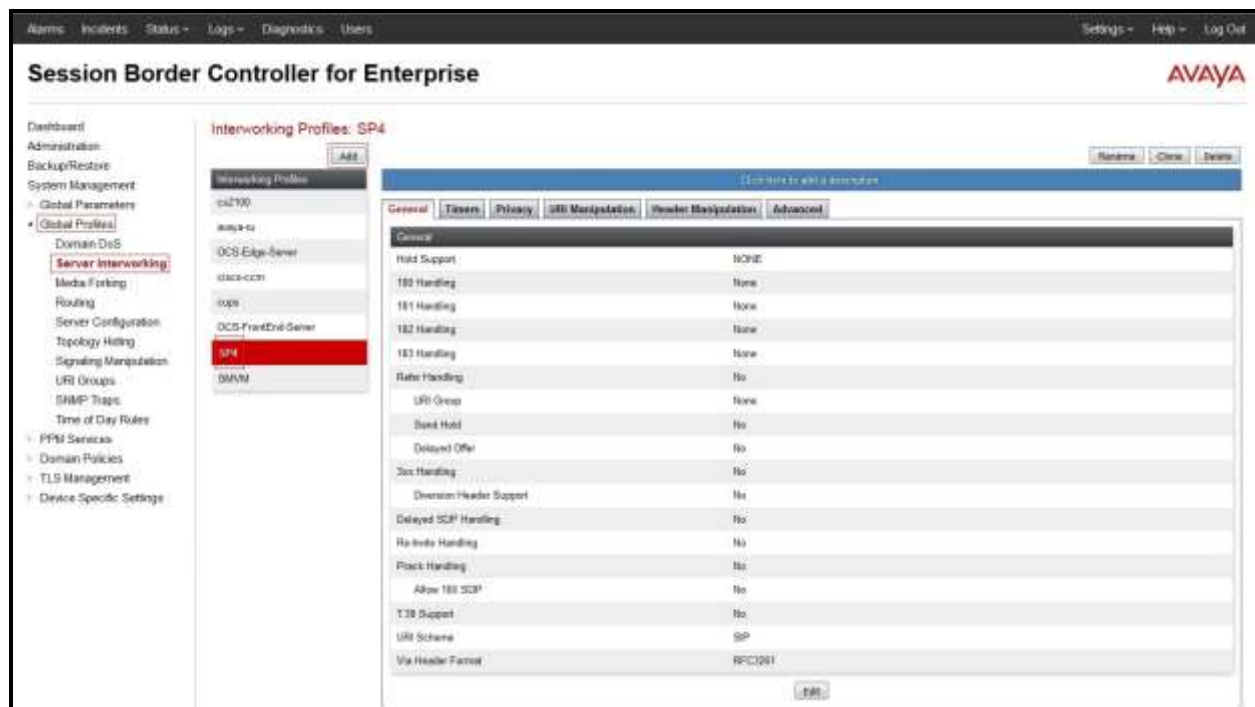


Figure 76- Server Interworking – Bell Canada site

From the list of **Interworking Profiles**, click on **SP4** to edit.

- On **Header Manipulation** tab, click **Add** button to manipulate the following headers for outbound calls:
 - Remove “user=phone” on From header (This is optional for ONND testing).
 - Add “trgp = trunk-group-id” and “trunk-context=siptrunking.bell.ca” on Contact header.
 - Add “otg=trunk-group-id” on From/P-Asserted-Identity/Diversion headers (This is optional for ONND testing).

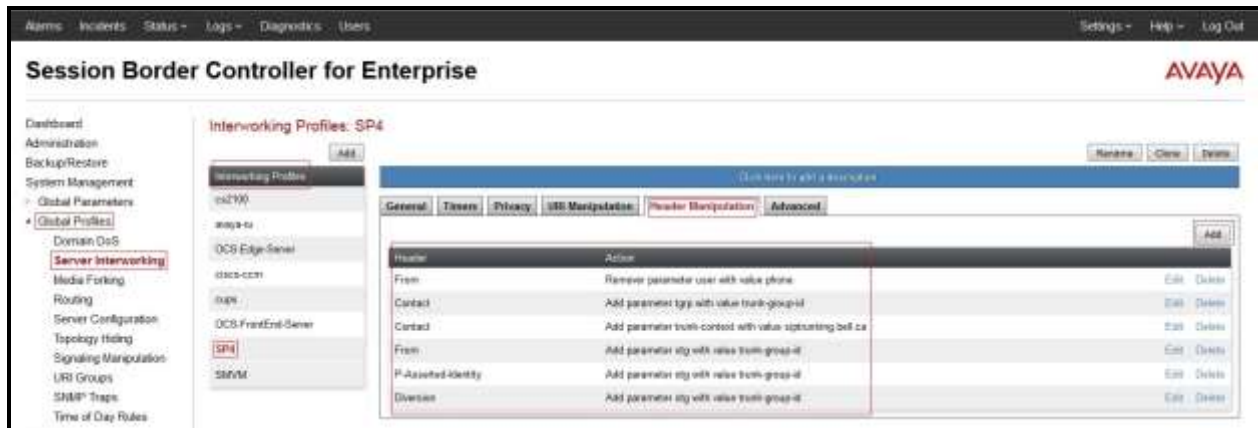


Figure 77 - Server Interworking – Bell Canada site - Header Manipulation

Note:

Bell Canada SIP Trunking Service uses the concept of trunk groups to model logical pipes that all calls, inbound or outbound, take to travel between the SIP Trunking infrastructure and the customer’s voice network. Trunk groups can be unidirectional or bidirectional. They each have specific inbound, outbound and total capacity thresholds. Some treatments can be applied when these thresholds are exceeded. Please contact Bell Canada for the Capacity Management for more details.

Bell Canada SIP Trunking Service supports RFC-4904. Trunk group labels are determined at service provisioning time. The following syntax must be followed:

Contact: <sip:[user-part];trgp=[trunk-group-id];trunk-context=siptrunking.bell.ca@[CPE/PBX-IP-address]>

Bell Canada supports the “otg” header parameter in the “From”, “P-Asserted-Identity” or “Diversion” header (OTG: Originating Trunk Group). Trunk group labels are determined at service provisioning time.

The following syntax must be followed, depending on the headers used:

From: <sip:[10-digit-caller-number]@[customer-domain];user=phone;otg=[trunk-group-id]>

P-Asserted-Identity: <sip:[10-digit-caller-number]@[customer-domain];otg=[trunk-group-id]>

Diversion: <sip:[10-digit-diverted-number]@[customer-domain];user=phone;otg=[trunk-group-id]>

If the outbound trunk group is not explicitly selected through one of the above methods, the trunk group that will implicitly be selected will be the one with which the originating number is associated. The originating number is specified either through the “From”, “P-Asserted-Identity” or “Diversion” header.

Bell Canada Static/Dynamic ONND (Outbound Calling Name and Number Display) and Trunk Group Selection features require header manipulation in Avaya SBCE (**Figure 77** in **section 7.2.2**). However, this is provided as reference configuration for this specific testing. Please contact Bell Canada for Bell Canada Static/Dynamic ONND features for more details.

For Static ONND in this compliance testing, CS1000 will always send P-Asserted-Identity (PAI) header to Bell Canada system. Therefore, the PAI and Diversion headers should always include parameter user=phone. And for Trunk Group Selection, it is optional that the PAI and Diversion headers include parameter otg=trunk-group-id. With the presence of a Trunk Group Selection the display will be as in the From header. The display will be as in the PAI with an implicit Trunk Group Selection (i.e. without a Trunk Group Selection). Even though, these user and otg parameters are not required in the From header, it is being included in here for completeness. When using a Trunk Group Selection, the otg tag must be present in the From, PAI and Diversion headers when applicable.

For Dynamic ONND in this compliance testing, the From and PAI headers will not require user=phone parameter. However, Diversion header should always be including parameter user=phone. And for Trunk Group Selection, the From, PAI and Diversion headers should always include parameter otg=trunk-group-id. For the domain name in URI of the From header, the general domain name is specified but not the specific vendor domain name. For example, if the vendor specific domain is vendor6.lab.internetvoice.ca, then the domain used should be lab.internetvoice.ca (general domain). **Section 7.2.9** shows an example of this specific domain setting.

For multi-trunk group and geographic redundant configuration, please refer to document [9] in section 11.

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

From the menu on the left-hand side, select **Global Profiles** → **Signaling Manipulation** → **Add**.

- Enter script **Title: SP4**. In the script editing window, enter the text exactly as shown in the screenshot below to perform the following:
 - Remove “+1” on user URI of From and Contact SIP headers for incoming calls (When testing with ONND feature on off-net call forward, Bell Canada requested to manipulate the From and Contact headers for incoming calls to remove “+1” on user URI of the From and Contact headers so that they contained only 10-digit number. By this way, when CS1000 did the off-net call forward, it sends the SIP re-Invite with From header contained only 10-digit number).
 - Remove the empty the Supported header sending from Bell Canada (This is a workaround to fix no-speech path issue mentioned in **Section 2.2**).
 - Remove unwanted SIP headers for outgoing calls (**Note:** This is optional to remove the P-Asserted-Identity header for ONND testing).
 - Modify user URI of the P-Asserted-Identity header for CS1000 Mobile-X feature and off-net call forward testing.
 - Click **Save** (not shown).

Note: See **Appendix B** in **Section 13** for the reference of this sigma script.

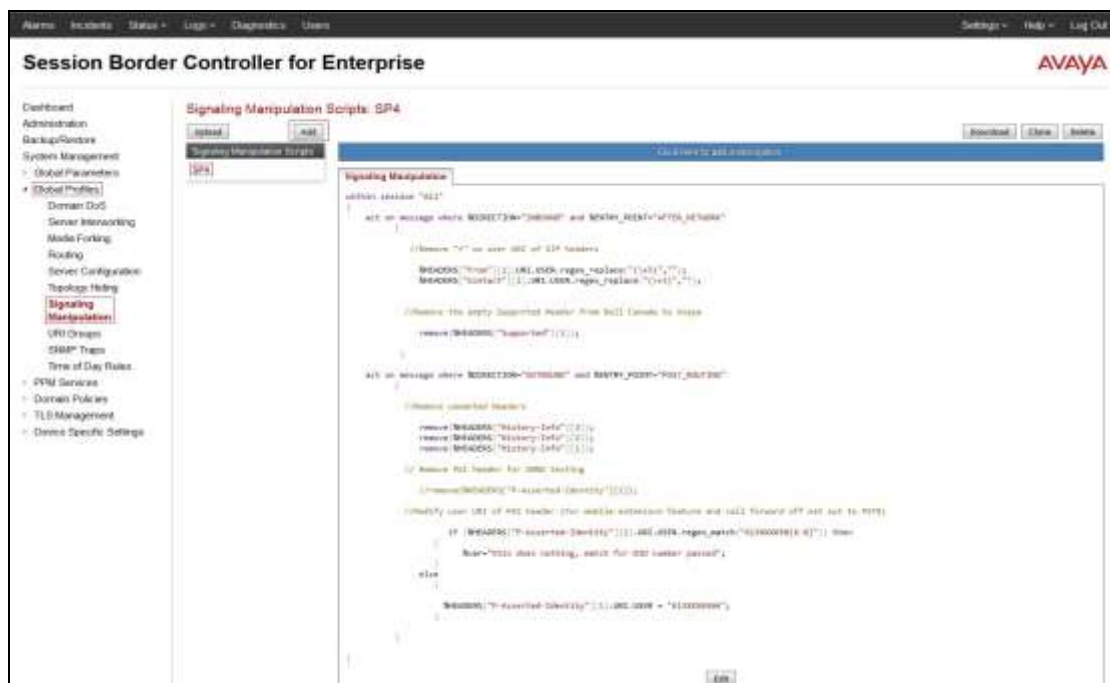


Figure 78 - Signaling Manipulation

7.2.4. Configure Server – Avaya Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server-specific parameters such as UDP port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** → **Add**.

Enter **Profile Name: SMVM**. On **General** tab, enter the following:

- **Server Type:** Select **Call Server**.
- **IP Address/FQDN:** **10.33.10.43** (Avaya Aura® Session Manager IP Address).
- **Port:** **5060**.
- **Transport:** **UDP**.
- Click **Finish** (not shown).



Figure 79 - Server Configuration – General - Avaya Session Manager

On the **Advanced** tab:

- Select **SMVM** for **Interworking Profile** (see Section 7.2.1).
- Click **Finish** (not shown).

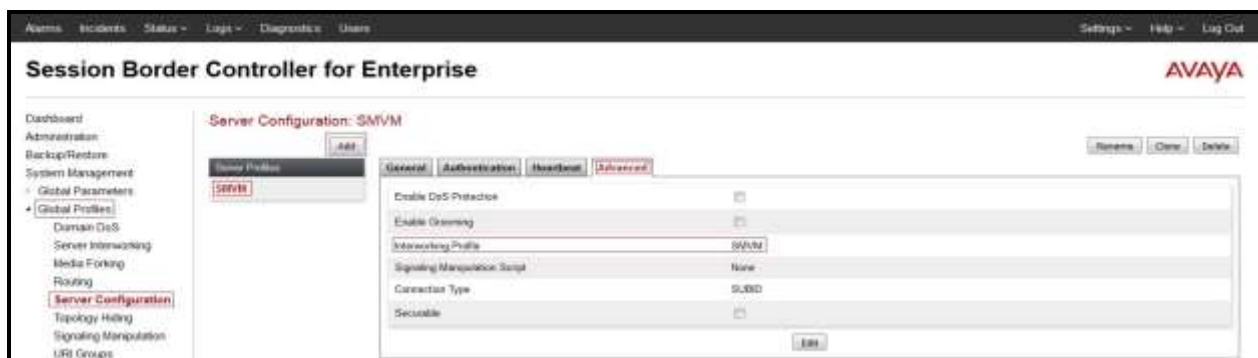


Figure 80 - Server Configuration – Advanced - Avaya site

7.2.5. Configure Server – Bell Canada

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**. Enter **Profile Name: SP4**.

On **General** tab, enter the following:

- **Server Type:** Select **Trunk Server**.
- **IP Address/FQDN:** **192.168.237.206** (Bell Canada Signaling Server IP Address).
- **Port:** **5060**.
- **Transport:** **UDP**.
- Click **Finish** (not shown).



Figure 81 - Server Configuration – General – Bell Canada site

On the **Authentication** tab, click **Edit** button and enter the following:

- Check **Enable Authentication** checkbox.
- **User Name:** ***** (Bell Canada provided this user name for authentication).
- **Password:** ***** (Bell Canada provided this password for authentication).
- **Confirm Password:** ***** (as above).
- Click **Finish**.

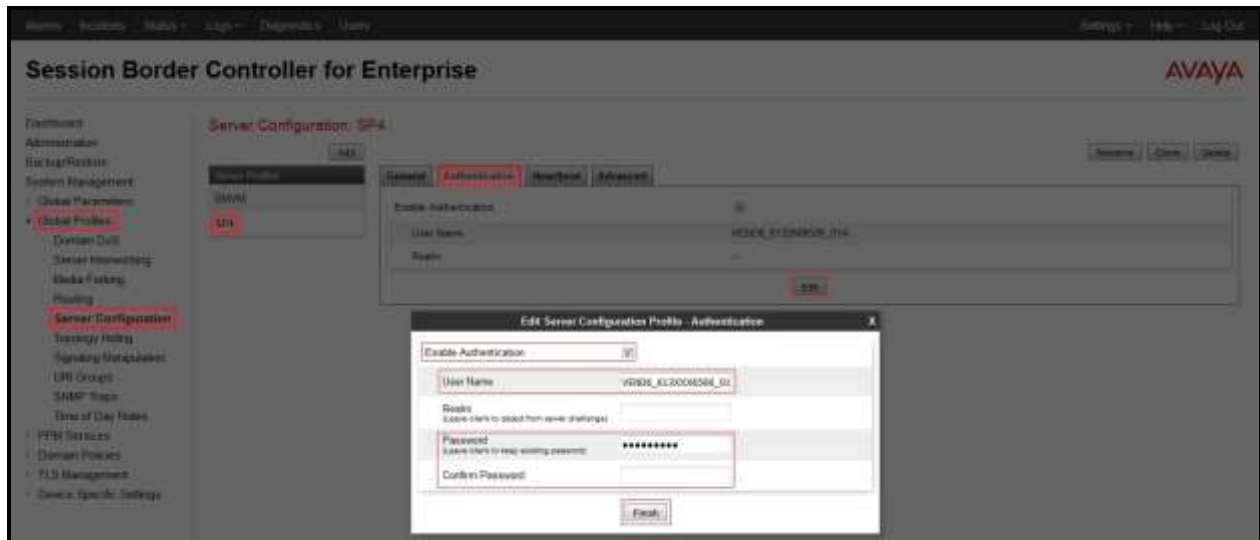


Figure 82 - Server Configuration – Authentication – Bell Canada site

On the **Advanced** tab, enter the following:

- **Interworking Profile:** select SP4 (see Section 7.2.2).
- **Signaling Manipulation Script:** select SP4 (see Section 0).
- Click **Finish** (not shown).

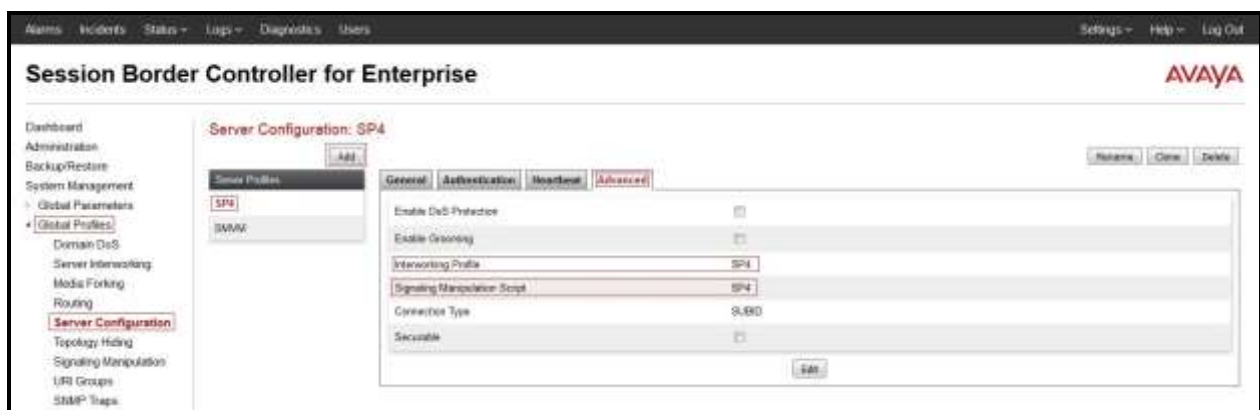


Figure 83 - Server Configuration – Advanced – Bell Canada site

7.2.6. Configure Routing – Avaya Session Manager

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.

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: SP4_To_SMVM** and click **Next** button (not shown).

- Select **Load Balancing: Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight: 1**.
- **Server Configuration: SMVM** (see **Section 7.2.4**). This selection will automatically populate the **Next Hop Address** field with **10.33.10.43:5060 (UDP)** (Avaya Aura® Session Manager IP Address).
- Click **Finish**.

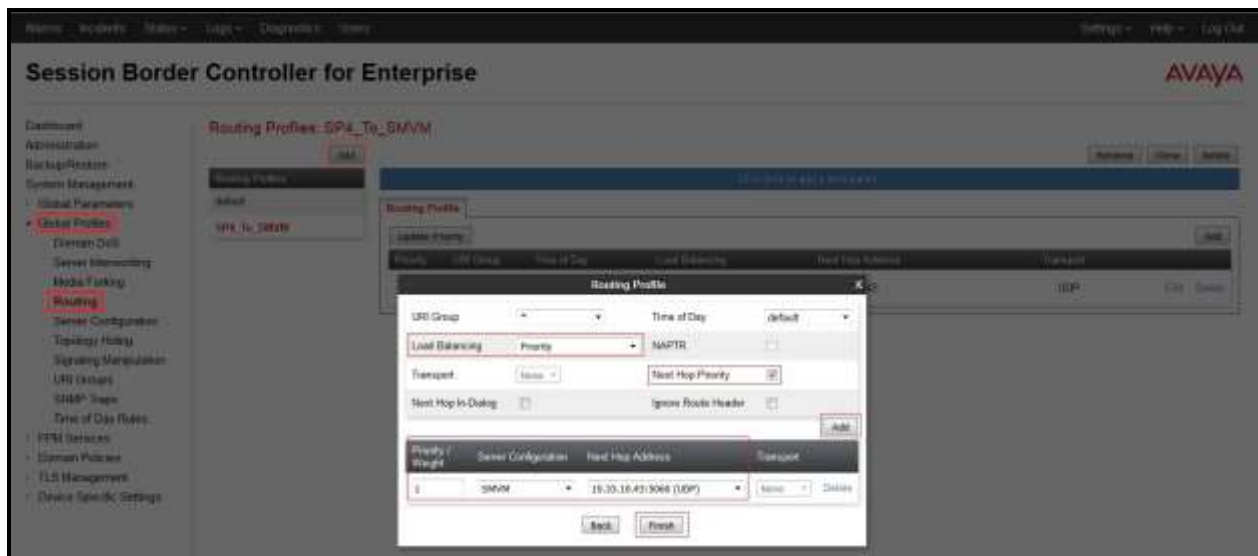


Figure 84 - Routing to Session Manager

7.2.7. Configure Routing – Bell Canada

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: SMVM_To_SP4** (not shown).

- **Load Balancing: Priority.**
- Check **Next Hop Priority.**
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight: 1.**
- **Server Configuration: SP4** (see Section 7.2.5). This selection will automatically populate the **Next Hop Address** field with **192.168.237.206:5060 (UDP)** (Bell Canada Signaling IP Address).
- Click **Finish**.

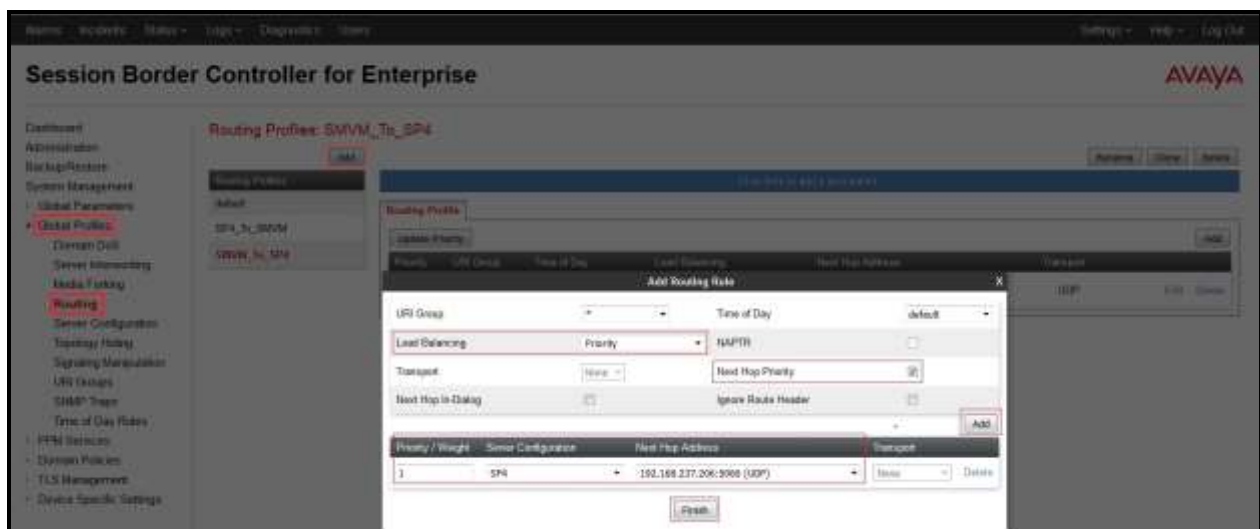


Figure 85 - Routing to Bell Canada

7.2.8. Configure Topology Hiding – Avaya Session Manager

The **Topology Hiding** screen allows administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**.

- Select **default** in **Topology Hiding Profiles**.
- Click **Clone**.
- Enter **Clone Name: SP4_To_SMVM** and click **Finish** (not shown).
- Select **SP4_To_SMVM** in **Topology Hiding Profiles** and click **Edit** button to modify as below:
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bvwddev.com**
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bvwddev.com**
- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bvwddev.com**

Click **Finish** (not shown).

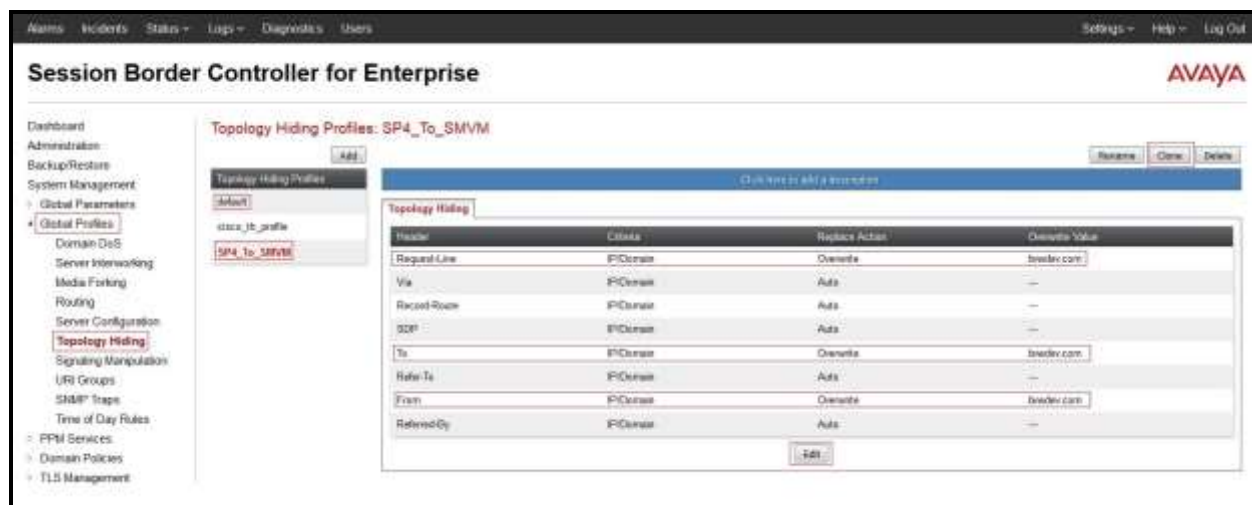


Figure 86 - Topology Hiding Session Manager

7.2.9. Configure Topology Hiding – Bell Canada

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

- Select **default** in **Topology Hiding Profiles**.
- Click **Clone**.
- Enter **Clone Name: SMVM_To_SP4** and click **Finish** (not shown).
- Select **SMVM_To_SP4** in **Topology Hiding Profiles** and click **Edit** button to modify as below:
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **siptrunking.bell.ca** (This was Bell Canada domain)
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **siptrunking.bell.ca** (This was Bell Canada domain)
- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **vendor6.lab.internetvoice.ca** (Bell Canada defined this as PBX domain)

Note: Mentioned in **Section 7.2.2** for Dynamic ONND, the specific domain shows in below capture in the **From** header, **vendor6.lab.internetvoice.ca**, should be changed to a general domain as **lab.internetvoice.ca**.

Click **Finish** (not shown).

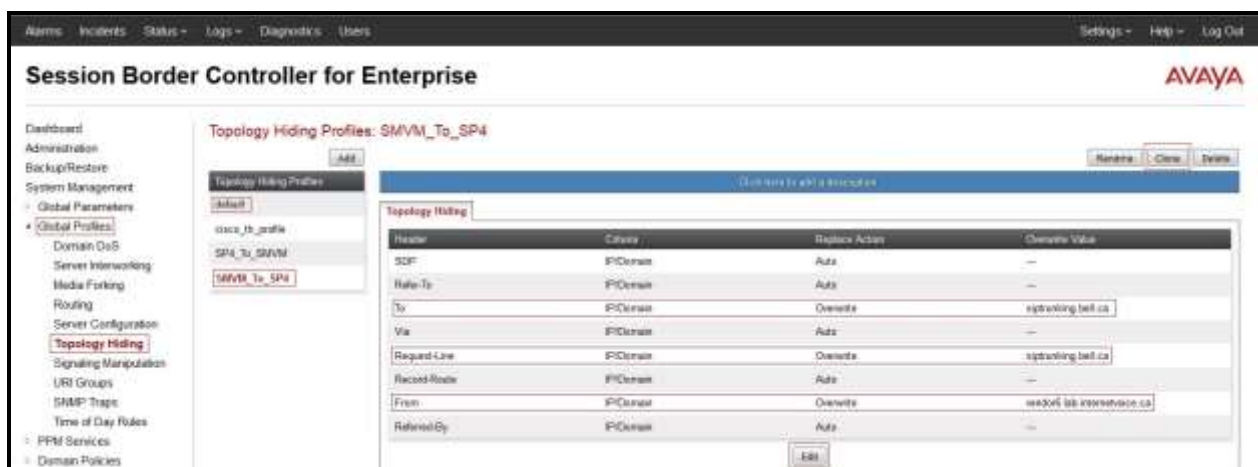


Figure 87 - Topology Hiding Bell Canada

7.3. Domain Policies

The Domain Policies feature allows one to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or one can create a custom domain policy.

7.3.1. Create Signaling Rules

Signaling Rules allow one to 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 Avaya SBCE, 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.

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Enter **Clone Name: SP4**.
 - Click **Finish** (not shown).

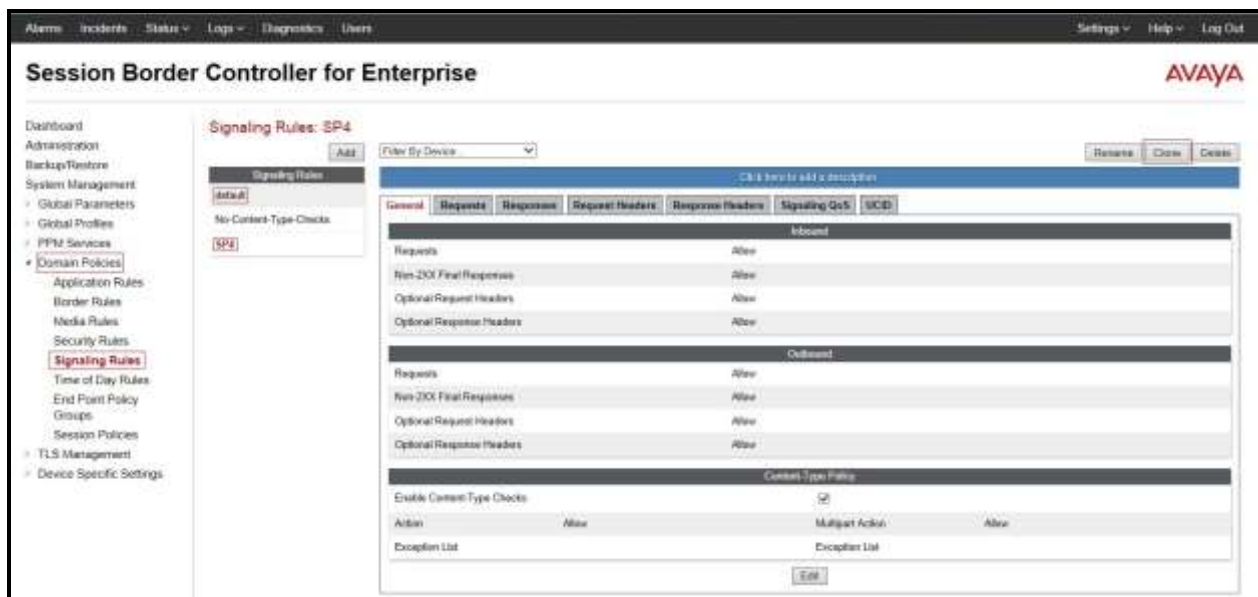


Figure 88 - Signaling Rule SP4

The following configuration on the SP4 Signaling Rule converts 183 with SDP to 180 Ringing. From the list of **Signaling Rules**, click on **SP4**.

- On the **Response Headers** tab, select **Add In Header Control**.
 - **Header Name:** Contact.
 - **Response Code:** 183.
 - **Method Name:** INVITE.
 - **Header Criteria:** Forbidden.
 - **Presence Action:** Change response to 180 Ringing.
- Click **Finish**.

Note: The above configuration for workaround to fix ring-back tone issue (See **Section 2.2**). However, this translation on the Avaya SBCE removed support for early media. Customers of the Bell Canada should be aware of this limitation before implementing this specific translation on the Avaya SBCE.

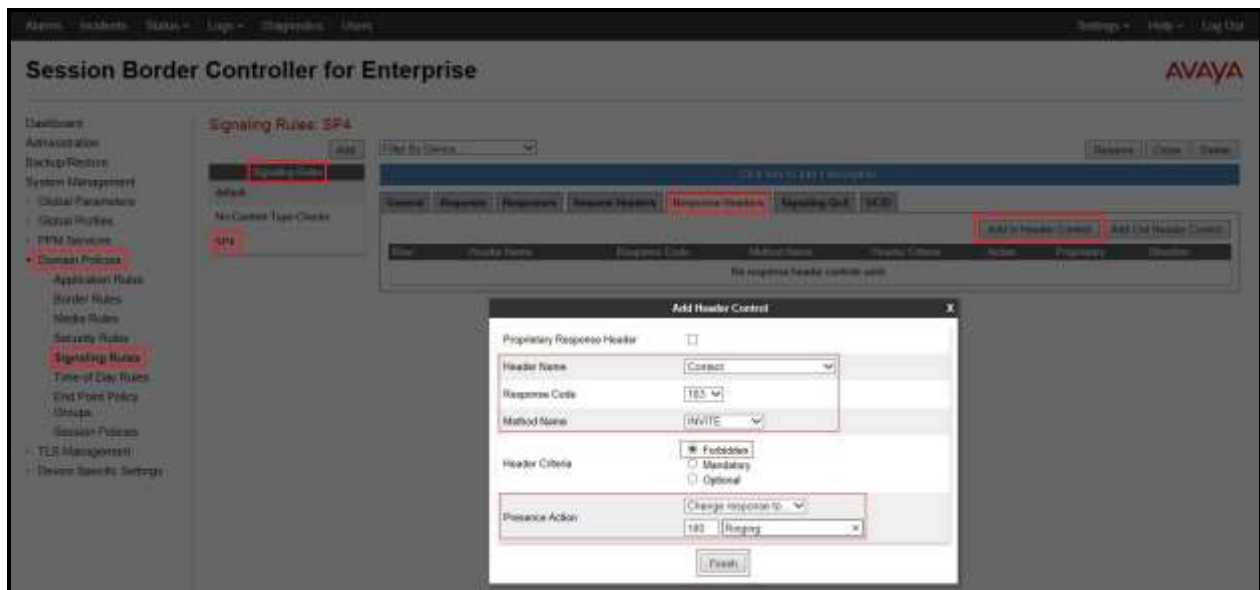


Figure 89 - Signaling Rule SP4 – Header Control

7.3.2. Create Endpoint Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD. In compliance test, a Policy Group is comprised of signaling rule created in the previous **section 7.3.1** and other default rule sets.. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: SMVM_SP4_PolicyG**.
 - **Application Rule: default.**
 - **Border Rule: default.**
 - **Media Rule: default-low-med.**
 - **Security Rule: default-med.**
 - **Signaling Rule: default.**
 - **Time of Day: default.**
- Select **Finish** (not shown).



Figure 90 - Endpoint Policy – Avaya site

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: SP4_PolicyG**.
 - **Application Rule: default.**
 - **Border Rule: default.**
 - **Media Rule: default-low-med.**
 - **Security Rule: default-med.**
 - **Signaling Rule: SP4** (see Section 7.3.1).
 - **Time of Day: default.**
- Select **Finish** (not shown).

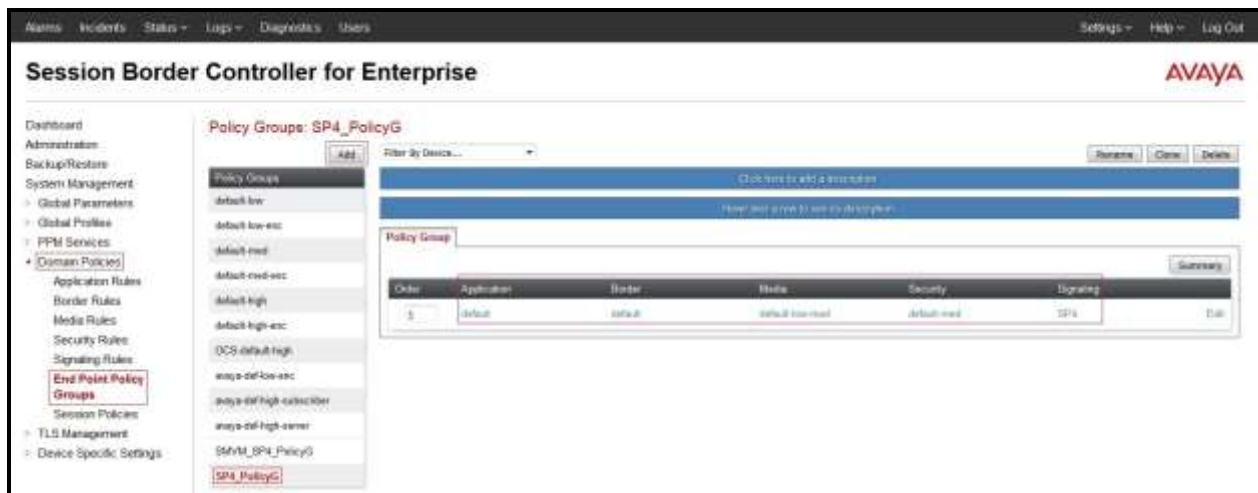


Figure 91 - Endpoint Policy – Bell Canada site

7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

7.4.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- Select **Networks** tab and click **Add** button to add a network of inside interface as follows:
 - **Name:** Network_A1.
 - **Default Gateway:** 10.10.98.1.
 - **Subnet Mask:** 255.255.255.192.
 - **Interface:** A1 (This is Avaya SBCE's inside interface).
 - Click **Add** button to add **IP Address** for inside interface: 10.10.98.13.
 - Click **Finish** button to save the changes.

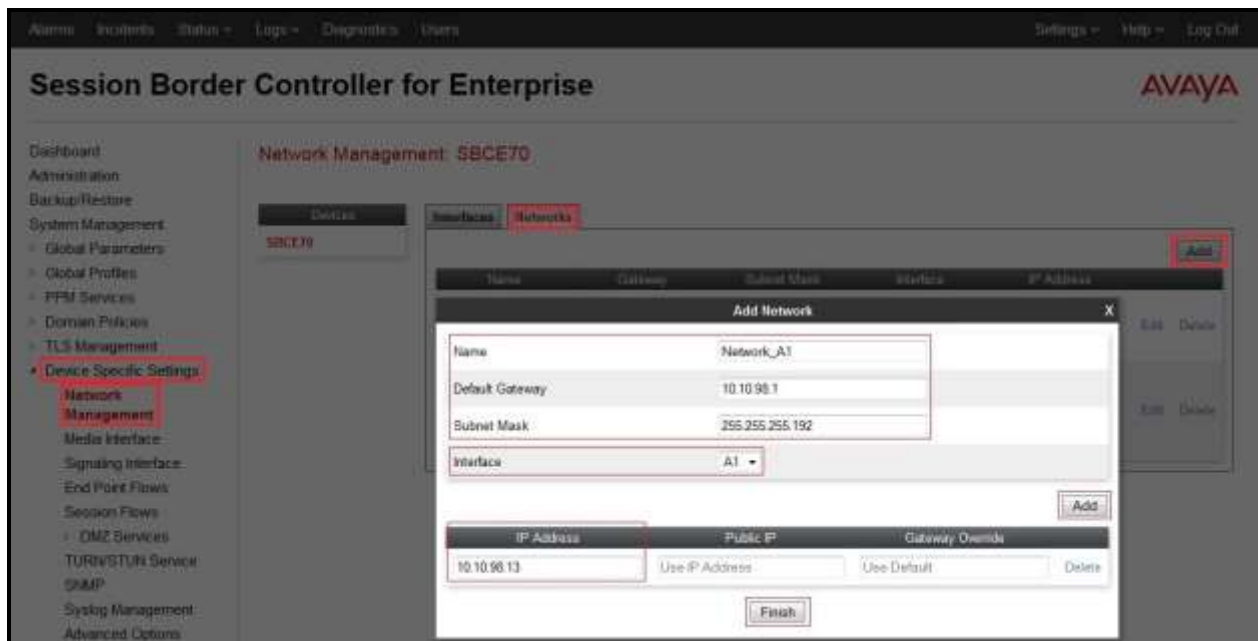


Figure 92 - Network Management – Inside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- Select **Networks** tab and click **Add** button to add a network of outside interface as followings:
 - **Name: Network_B1.**
 - **Default Gateway: 10.10.98.97.**
 - **Subnet Mask: 255.255.255.224.**
 - **Interface: B1** (This is Avaya SBCE outside interface).
 - Click **Add** button to add **IP Address** for outside interface: **10.10.98.111.**
 - Click **Finish** button to save the changes.

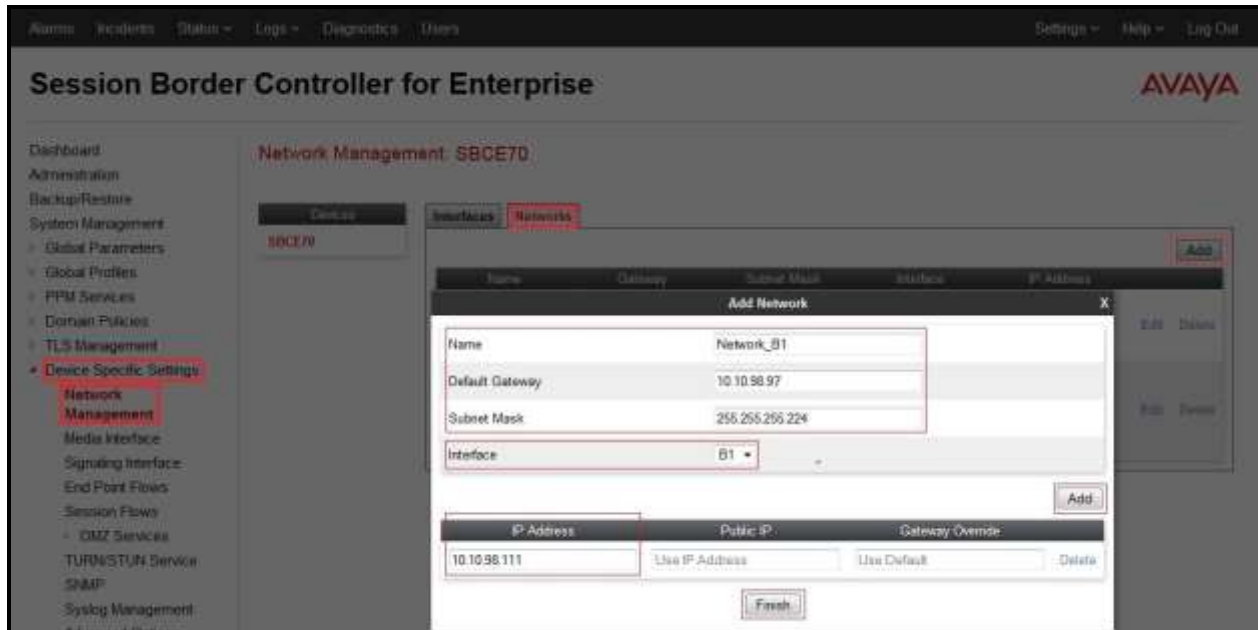


Figure 93 - Network Management – Outside Interface

From the menu on the left-hand side, select **Device Specific Settings** → **Network Management**.

- Select **Interfaces** tab.
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state.



Figure 94 - Network Management – Interface Status

7.4.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya can be used for both inside and outside ports.

From the menu on the left-hand side, **Device Specific Settings → Media Interface**.

- Select **Add** button and enter the following in the configuration window (not shown):
 - **Name:** **InsideMedia1**.
 - **IP Address:** Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Avaya Session Manager).
 - **Port Range:** **49152 – 49200** (Bell Canada supported this port range during the compliance testing).
 - Click **Finish** (not shown).
- Select **Add** button and enter the following in the configuration window (not shown):
 - **Name:** **OutsideMedia1**.
 - **IP Address:** Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward Bell Canada SIP Trunk).
 - **Port Range:** **49152 – 49200** (Bell Canada supported this port range during the compliance testing).
 - Click **Finish** (not shown).

The screen below shows the configured media interfaces:



Figure 95 - Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**.

- Select **Add** button and enter the following in the configuration window (not shown):
 - **Name:** **InsideUDP1**.
 - **IP Address:** Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Avaya Session Manager).
 - **UDP Port:** **5060**.
 - Click **Finish** (not shown).

From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**.

- Select **Add** button and enter the following in the configuration window (not shown):
 - **Name:** **OutsideUDP1**.
 - **IP Address:** Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward Bell Canada SIP trunk).
 - **UDP Port:** **5060**.
 - Click **Finish** (not shown).

Note: For the internal interface, the Avaya SBCE was configured to listen for UDP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 as same by Bell Canada.

The screen below shows the configured signaling interfaces:



Figure 96 - Signaling Interface

7.4.4. Configuration Server Flows

Server Flows allow an administrator to categorize signaling and apply various policies.

7.4.4.1 Create End Point Flows – Avaya Session Manager

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter
 - **Flow Name:** SMVM_Flow.
 - **Server Configuration:** SMVM (see Section 7.2.4).
 - **URI Group:** *.
 - **Transport:** *.
 - **Remote Subnet:** *.
 - **Received Interface:** OutsideUDP1 (see Section 7.4.3).
 - **Signaling Interface:** InsideUDP1 (see Section 7.4.3).
 - **Media Interface:** InsideMedia1 (see Section 7.4.2).
 - **End Point Policy Group:** SMVM_SP4_PolicyG (see Section 7.3.2).
 - **Routing Profile:** SMVM_To_SP4 (see Section 7.2.7).
 - **Topology Hiding Profile:** SP4_To_SMVM (see Section 7.2.8).
 - Click **Finish**.

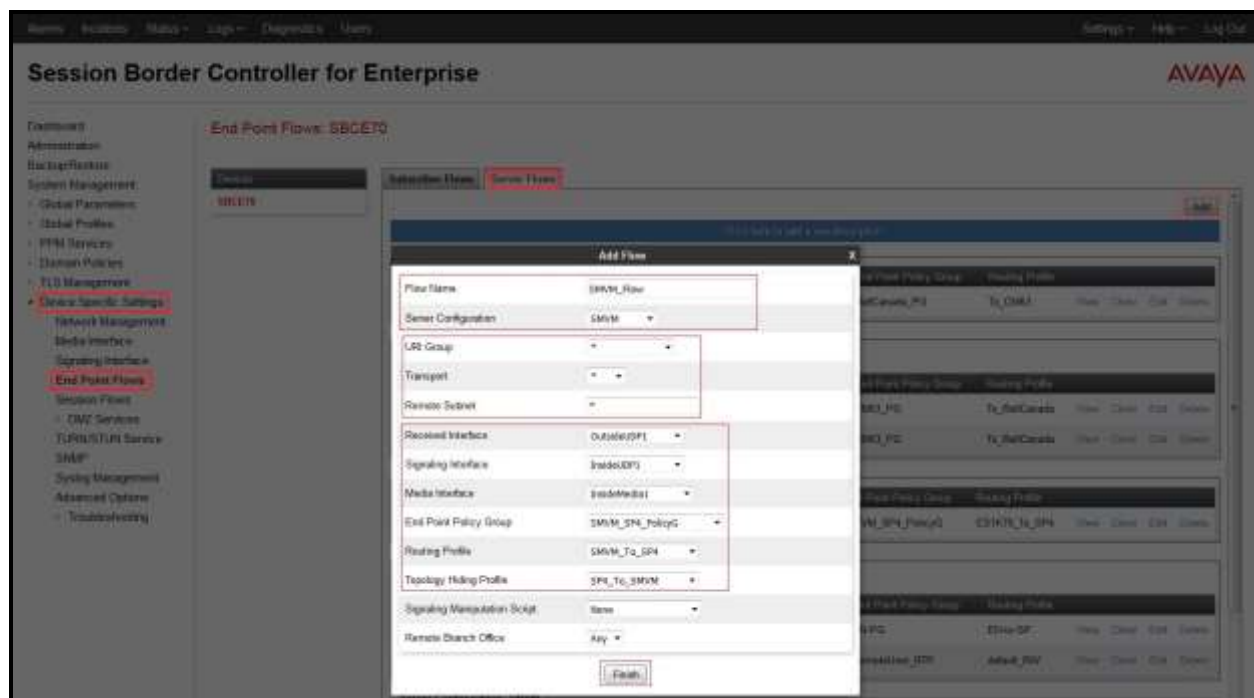


Figure 97 - End Point Flow to Bell Canada

7.4.4.2 Create End Point Flows – Bell Canada

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter
 - **Flow Name:** SP4_Flow.
 - **Server Configuration:** SP4 (see Section 7.2.5).
 - **URI Group:** *.
 - **Transport:** *.
 - **Remote Subnet:** *.
 - **Received Interface:** InsideUDP1 (see Section 7.4.3).
 - **Signaling Interface:** OutsideUDP1 (see Section 7.4.3).
 - **Media Interface:** OutsideMedia1 (see Section 7.4.2).
 - **End Point Policy Group:** SP4_PolicyG (see Section 7.3.2).
 - **Routing Profile:** SP4_To_SMVM (see Section 7.2.6).
 - **Topology Hiding Profile:** SMVM_To_SP4 (see Section 7.2.9).
 - Click **Finish**.

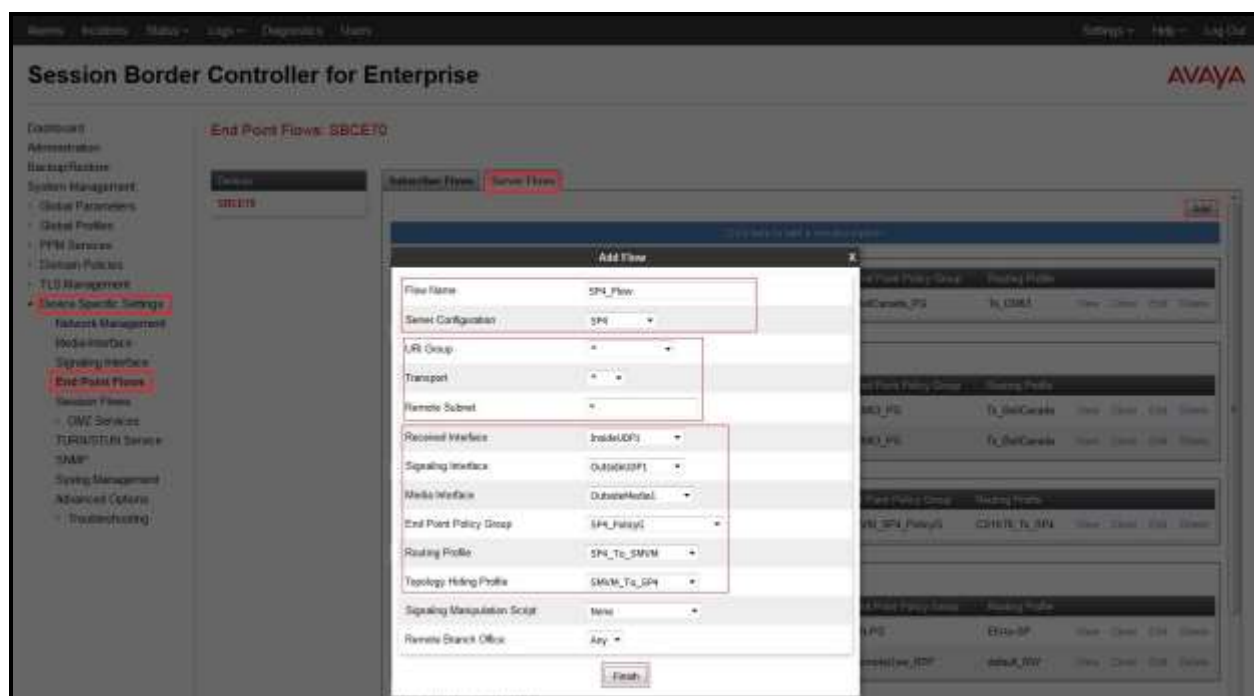


Figure 98 - End Point Flow from Bell Canada

8. Bell Canada SIP Trunking Service Configuration

Bell Canada is responsible for the network configuration of the Bell Canada SIP Trunking Service. Bell Canada will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. Bell Canada will provide the IP address and port number used for signaling through security devices, IP address and port number used for media through security devices and Direct Inward Dialed (DID) numbers assigned to the enterprise. Bell Canada also provides the Bell Canada SIP Trunking Service Interface Specification document for reference. This information is used to complete configurations for Avaya Communication Server 1000, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between Bell Canada and the enterprise is a static IP configuration. There is no registration on the SIP trunk implemented on either Bell Canada or enterprise side.

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

Place an inbound call from a PSTN phone to an internal Avaya phone, answer the call, and verify that two-way speech path exists. Verify that the call remains stable for several minutes and disconnects properly.

9.2. Verification of an Active Call on Communication Server 1000

Active Call Trace (Id 80)

The following is an example of one of the commands available on the CS1000 to trace the DN for which the call is in progress or idle (6506). The call scenario involved PSTN phone number 16139XX5206 calling 6132XX6506 (which is translated to extension 6506).

- Login into CS1000 Signaling Server 10.10.97.177 with admin account and password.
- Issue a command “cslogin” to login on to the CS1000 Call Server.
- Log in to the Overlay command prompt, issue the command **Id 80** and then **trace 0 6506**.
- After the call is released, issue command **trac 0 6506** again to see if the DN is released back to idle state.

Below is the actual output of the CS1000 Call Server Command Line mode when the **6506** is in call state:

```
>Id 80
TRA000
.trace 0 6506

TRA100

.trac 0 6506

ACTIVE VTN 096 0 00 02

ORIG VTN 100 0 01 00 VTRK IPTI RMBR 101 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 10.10.98.13
FAR-END MEDIA ENDPOINT IP: 10.10.98.13 PORT: 35590
FAR-END VendorID: AVAYA-SM-7.0.0.0.700007
TERM VTN 096 0 00 02 KEY 0 SCR MARP CUST 0 DN 6506 TYPE 2002P2
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 10.33.5.9 PORT: 5200
MEDIA PROFILE: CODEC G.729A NO-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 6506
MAIN_PM ESTD
TALKSLOT ORIG 30 TERM 5
EES_DATA:
NONE
QUEU NONE
CALL ID 501 16
```

```
---- ISDN ISL CALL (ORIG) ----  
CALL REF # = 385  
BEARER CAP = VOICE  
HLC =  
CALL STATE = 10  ACTIVE  
CALLING NO = 16139XX5206 NUM_PLAN:UNKNOWN  TON:UNKNOWN  ESN:UNKNOWN  
CALLED NO = 6132XX6506 NUM_PLAN:UNKNOWN  TON:UNKNOWN  ESN:UNKNOWN
```

And this is the example after the call to 6506 is finished.

```
>ld 80  
TRA000  
.trac 0 6506  
IDLE VTN 96 0 00 02  MARP
```

SIP Trunk monitoring (ld 32)

Place a call inbound from PSTN (16139XX5206) to an internal Avaya phone (6132XX6506). Then check the SIP trunk status by using ld 32, and verify one trunk is BUSY.

```
>ld 32  
NPR000  
.stat 100 0  
091 UNIT(S) IDLE  
001 UNIT(S) BUSY  
000 UNIT(S) DSBL  
000 UNIT(S) MBSY
```

After the call is released, check that SIP trunk status should change to the IDLE state.

```
>ld 32  
NPR000  
.stat 100 0  
092 UNIT(S) IDLE  
000 UNIT(S) BUSY  
000 UNIT(S) DSBL  
000 UNIT(S) MBSY
```

9.3. Protocol Trace

Below is a Wireshark trace of the same call scenario described in **Section 9.2**.

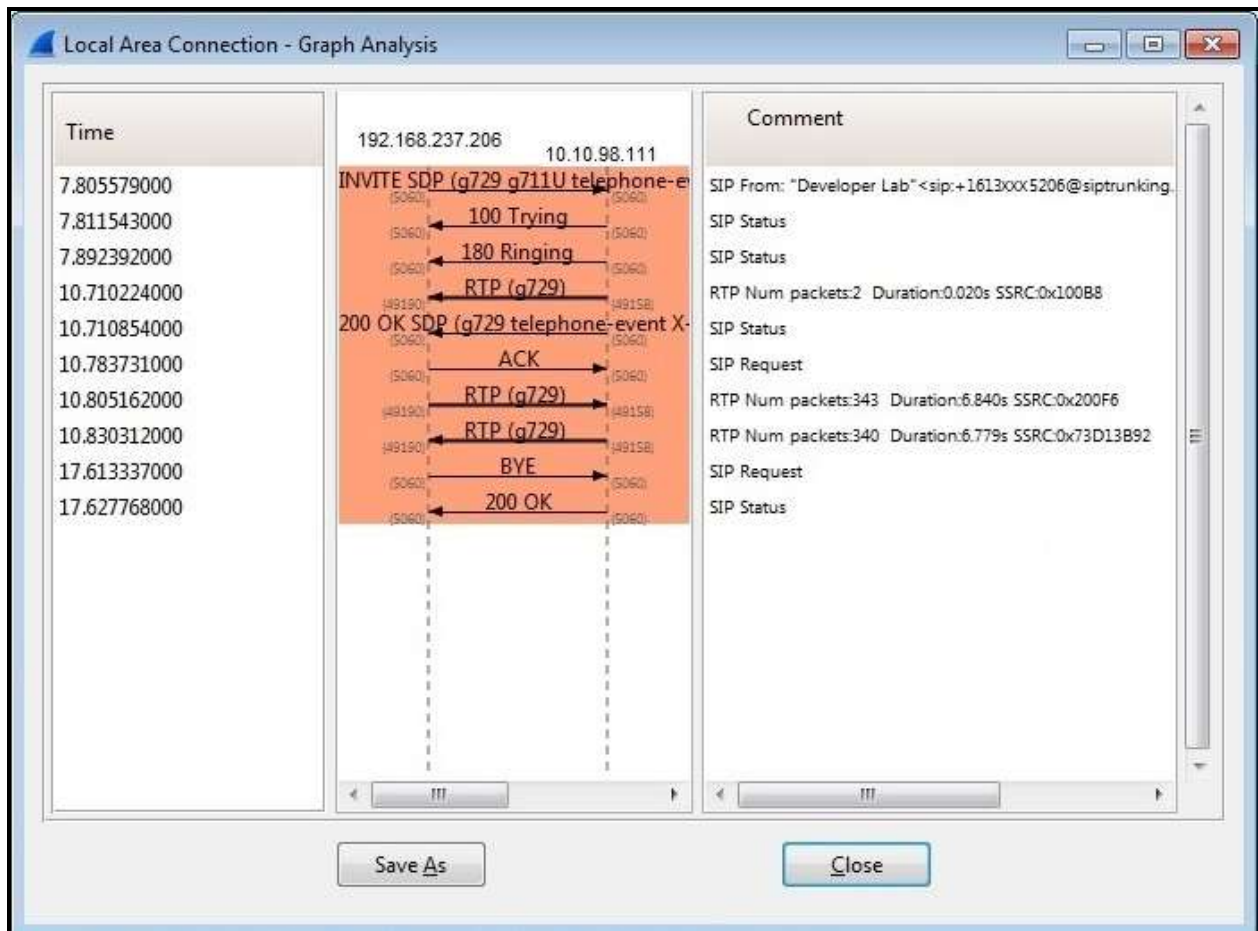


Figure 99 – SIP Call Trace

10. Conclusion

All of the test cases have been executed. Observations/limitations seen during the test was noted in **Section 2.2**. The test met the objectives outlined in **Section 2.1**. The Bell Canada SIP Trunking Service is considered **compliant** with Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 7.0 and Avaya Session Border Controller for Enterprise Release 7.0.

11. References

This section references documentation relevant to these Application Notes.

Product documentation for Avaya products, including the following, is available at <http://support.avaya.com/>

Avaya Communication Server 1000

- *Network Routing Service Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013
- *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013
- *Communication Server 1000E Overview, Avaya Communication Server 1000*, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013
- *Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013
- *Dialing Plans Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.
- *Product Compatibility Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013

Avaya Aura® Session Manager/System Manager

- *Administering Avaya Aura® Session Manager*, Release 7.0, Issue 1, August 2015
- *Administering Avaya Aura® System Manager*, Release 7.0, Issue 1, August 2015

Avaya Session Border Controller for Enterprise

- *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.0 Issue 1, August 2015
- *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015
- *Application Notes for Bell Canada SIP Trunking Service using Least Cost Routing with Avaya Aura® Communication Manager R6.0.1, Geographic Redundant Avaya Aura® Session Managers R6.1 and Avaya Session Border Controllers for Enterprise R4.0.5 –Issue 1.0*

12. Appendix A: Additional patch lineup for the CS1000 configuration.

Call Server: 7.65 P+ GA plus latest DEPLIST – CPL_7.6_7.zip (X2107.65P)

Signaling Server: 7.65.16 GA plus latest DEPLIST – SP_7.6_7.ntl (7.65.16.00)

CS1000 Signaling Server patch list:

[admin@car3-cores ~]\$ pstat

Product Release: 7.65.16.00

In system patches: 8

PATCH#	NAME	IN_SERVICE	DATE	SPECINS	TYPE	RPM
30	p33456_1	Yes	20/10/15	YES	FRU	cs1000-OS-1.00.00.00-00.noarch
32	p33493_1	Yes	20/10/15	NO	FRU	cs1000-OS-1.00.00.00-00.noarch
33	p33554_1	Yes	20/10/15	YES	FRU	cs1000-OS-1.00.00.00-00.noarch
35	p33557_1	Yes	20/10/15	YES	FRU	cs1000-OS-1.00.00.00-00.noarch
38	p31484_1	Yes	20/02/14	NO	FRU	cs1000-shared-general-7.65.16-00.i386
47	p33125_1	Yes	23/12/14	NO	FRU	cs1000-OS-1.00.00.00-00.noarch
48	p33274_1	Yes	23/12/14	YES	FRU	initscripts-8.45.25-1.el5.i386
50	p33384_1	Yes	23/12/14	NO	FRU	cs1000-OS-1.00.00.00-00.noarch

In System service updates: 35

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	Yes	20/10/15	NO	YES	cs1000-Jboss-Quantum-7.65.16.23-5.i386.000
1	Yes	20/10/15	YES	YES	cs1000-dmWeb-7.65.16.23-4.i386.000
2	Yes	23/12/14	YES	YES	cs1000-patchWeb-7.65.16.22-4.i386.000
3	Yes	20/10/15	YES	YES	cs1000-shared-pbx-7.65.16.23-1.i386.000
4	Yes	23/12/14	YES	YES	cs1000-csoneksvrMgr-7.65.16.22-5.i386.000
5	Yes	23/12/14	YES	YES	cs1000-baseWeb-7.65.16.22-4.i386.000
6	Yes	23/12/14	YES	YES	cs1000-oam-logging-7.65.16.22-4.i386.000
7	Yes	23/12/14	YES	YES	cs1000-csv-7.65.16.22-2.i386.000
8	Yes	23/12/14	YES	YES	cs1000-mscTone-7.65.16.22-2.i386.000
9	Yes	23/12/14	YES	YES	cs1000-mscMusc-7.65.16.22-4.i386.000
10	Yes	23/12/14	YES	YES	cs1000-mscConf-7.65.16.22-2.i386.000
11	Yes	23/12/14	YES	YES	cs1000-mscAnnc-7.65.16.22-2.i386.000
12	Yes	23/12/14	YES	YES	cs1000-mscAttn-7.65.16.22-2.i386.000
13	Yes	23/12/14	NO	YES	cs1000-gk-7.65.16.22-1.i386.000
15	Yes	20/02/14	NO	YES	cs1000-pd-7.65.16.21-00.i386.000
16	Yes	20/02/14	NO	YES	cs1000-shared-carIdtct-7.65.16.21-01.i386.000
17	Yes	20/02/14	NO	YES	cs1000-shared-tpselect-7.65.16.21-01.i386.000
18	Yes	20/02/14	NO	YES	cs1000-dbcom-7.65.16.21-00.i386.000
19	Yes	20/10/15	YES	YES	cs1000-linuxbase-7.65.16.23-19.i386.000
20	Yes	20/10/15	NO	YES	libxml2-2.6.26-2.1.25.el5_11.i386.000
21	Yes	20/10/15	NO	YES	libxml2-python-2.6.26-2.1.25.el5_11.i386.000
22	Yes	20/10/15	NO	YES	freetype-2.2.1-32.el5_9.1.i386.000

23	Yes	20/10/15	NO	YES	cs1000-cppmUtil-7.65.16.23-4.i686.000
24	Yes	20/10/15	NO	YES	tzdata-2015a-1.el5.i386.000
25	Yes	20/10/15	YES	YES	cs1000-tps-7.65.16.23-15.i386.000
26	Yes	20/02/14	NO	YES	cs1000-snmp-7.65.16.21-00.i686.000
27	Yes	20/10/15	YES	YES	kernel-2.6.18-406.el5.i686.000
28	Yes	20/10/15	YES	YES	jdk-1.6.0_101-fcs.i586.000
29	Yes	20/10/15	YES	YES	cs1000-vtrk-7.65.16.23-76.i386.000
31	Yes	20/02/14	NO	YES	cs1000-shared-omm-7.65.16.21-2.i386.000
34	Yes	20/02/14	YES	YES	cs1000-ipsec-7.65.16.22-1.i386.000
39	Yes	23/12/14	YES	YES	cs1000-shared-xmsg-7.65.16.22-1.i386.000
40	Yes	23/12/14	NO	YES	cs1000-sps-7.65.16.23-1.i386.000
42	Yes	23/12/14	YES	YES	cs1000-cs-7.65.P.100-03.i386.000
43	Yes	23/12/14	NO	YES	bash-3.2-33.el5_11.4.i386.000

13. Appendix B: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE in **Section 7.2.3**:

```
within session "All"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {

    //Remove "+" on user URI of SIP headers
    %HEADERS["From"][1].URI.USER.regex_replace("(\\+1)","");
    %HEADERS["Contact"][1].URI.USER.regex_replace("(\\+1)","");

    //Remove the empty Supported Header from Bell Canada to Avaya
    remove(%HEADERS["Supported"][1]);

  }

  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {

    //Remove unwanted Headers
    remove(%HEADERS["History-Info"][3]);
    remove(%HEADERS["History-Info"][2]);
    remove(%HEADERS["History-Info"][1]);

    //Remove PAI header for ONND testing
    //remove(%HEADERS["P-Asserted-Identity"][1]);

    //Modify user URI of PAI header (For mobile extension feature and call forward off net out to
    PSTN)
    if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("613XXX650[6-
8]")) then
    {
      %var="this does nothing, match for DID number passed";
    }
    else
    {
      %HEADERS["P-Asserted-Identity"][1].URI.USER = "613XXX6506";
    }
  }
}
```

©2015 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.