Avaya Solution & Interoperability Test Lab

# Application Notes for Configuring Bell Canada SIP Trunk Service with Avaya Communication Server 1000 Release 7.6, 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 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

These Application Notes illustrate a sample configuration using an Avaya SIP-enabled enterprise solution: Avaya Communication Server 1000 (CS1000) Release 7.6, 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 UNIStim, 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 UNIStim, 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 and P-Asserted-Identity 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). Note: 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 tested:

- Inbound toll free - Bell Canada did not support this setup during 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 due to 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 audio path generation and 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/off hold 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 8.2**).

## 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:

1. **Outbound call with authentication could not complete and there was no speech path** – Bell Canada system authenticates every call coming from Avaya system. With the authentication issue found in Avaya SBCE, calls from Avaya system to PSTN will not complete, and there will be 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.

2. **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.
3. **Outbound call and the call was terminated by PSTN phone, Avaya SBCE did not forward the BYE message to Avaya CS1000 -** The call scenario is 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 did not forward BYE to Avaya CS1000. Instead Avaya SBCE responded "500 Server Internal Error". The JIRA ticket (Aurora-7340) was opened for Avaya SBCE team to support this issue. Workaround: Enable "Next Hop In Dialog" on the routing profile towards CS1000 on Avaya SBCE (see **Section 6.2.6**) to fix this issue.
4. **For inbound call, Bell Canada offered G.729A as a primary codec and G.711MU as secondary**. This was a global codec policy which could not be changed during compliance testing. The compliance testing was tested with G.729A and G.711MU, in that order, for inbound calls.
5. **If the CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed**. This is a CS1000 known limitation.
6. **Calling Line Identification Display (CLID) was not correctly displayed in off-net call redirection -** After call redirection was completed with 2-way audio, namely blind/consultative transfers, the CLID on the transferee's phone was not updated accordingly. This is a CS1000 known limitation.
7. **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 is, after transferring, the original PSTN phone should hear ring-back tones from the other PSTN. However, when user pressed "Trnsfr" button, answered question of "Consult with party ?", and the answer was "No", which implied the blind transfer, the transferee PSTN phone was ringing, but the original PSTN phone could not hear ring-

back tones while the call was being transferred. After 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 (See **Section 6.3.1**) to translate the SIP 183 with SDP to SIP "180 Ringing", 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 Bell Canada should be aware of this limitation before implementing this specific translation on the Avaya SBCE.

8. **Blind Call Transfer to PSTN using Avaya 1140E SIP phone did not complete until transferee picked up the call** - Call scenario was when PSTN phone called to Avaya 1140E SIP phone, SIP phone answered the call and performed blind transfer the call to another PSTN endpoint. The expected behavior of the SIP phone was after transferring, the phone should display "Transfer successful". But in this case, user pressed "Trnsfr" button, answered question of "Consult with party ?", and the answer was "No", which implied the 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.

9. **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.

10. **Bell Canada sent the UPDATE every 10 minutes to ensure the media and the session were still established during the calls. However Avaya SBCE did not forward it to Avaya CS1000. Instead it responded "500 Server Internal Error"**- A JIRA ticket (Aurora-7342) was opened for Avaya SBCE team to investigate this issue. Workaround: Enable "Next Hop In Dialog" on the routing profile towards CS1000 on Avaya SBCE (see **Section 6.2.6**) to fix this issue.

11. **Off-net call forward failed during testing Static Outgoing Name and Number Display using Diversion Header (ONND) with user=phone (no PAI)** - By default, CS1000 always sends the SIP History-Info header with reason for off-net call forward. Avaya SBCE was configured to create a SIP Diversion header by collecting information within the History-Info header and converting them into a Diversion header. However, every parameters in the Diversion Header were translated and put in the < >. Bell rejected the call because the < > position was not correct in Diversion header syntax. In order to fix this issue, there was a signaling manipulation (SigMa) script (See **Section 6.2.3**) applied on Avaya SBCE to adjust the < > position on Diversion header so that Bell Canada system can process the parameters outside the < >.

12. **For ONND testing with off-net call forward, Bell Canada expected to see the external number in Diversion header should be the same number in FROM header, however CS1000 always put the valid PBX DID number in Diversion header instead of the same number in FROM header** - This was CS1000 design. In order to test with 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 compliance testing. This was a global setting on CS1000; therefore the CLID would be impacted for any outbound calls.

13. 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 processed the off-net call forward, it sends the SIP re-Invite with the From header contained only 10-digit number.

# 14.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 Trunk 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.

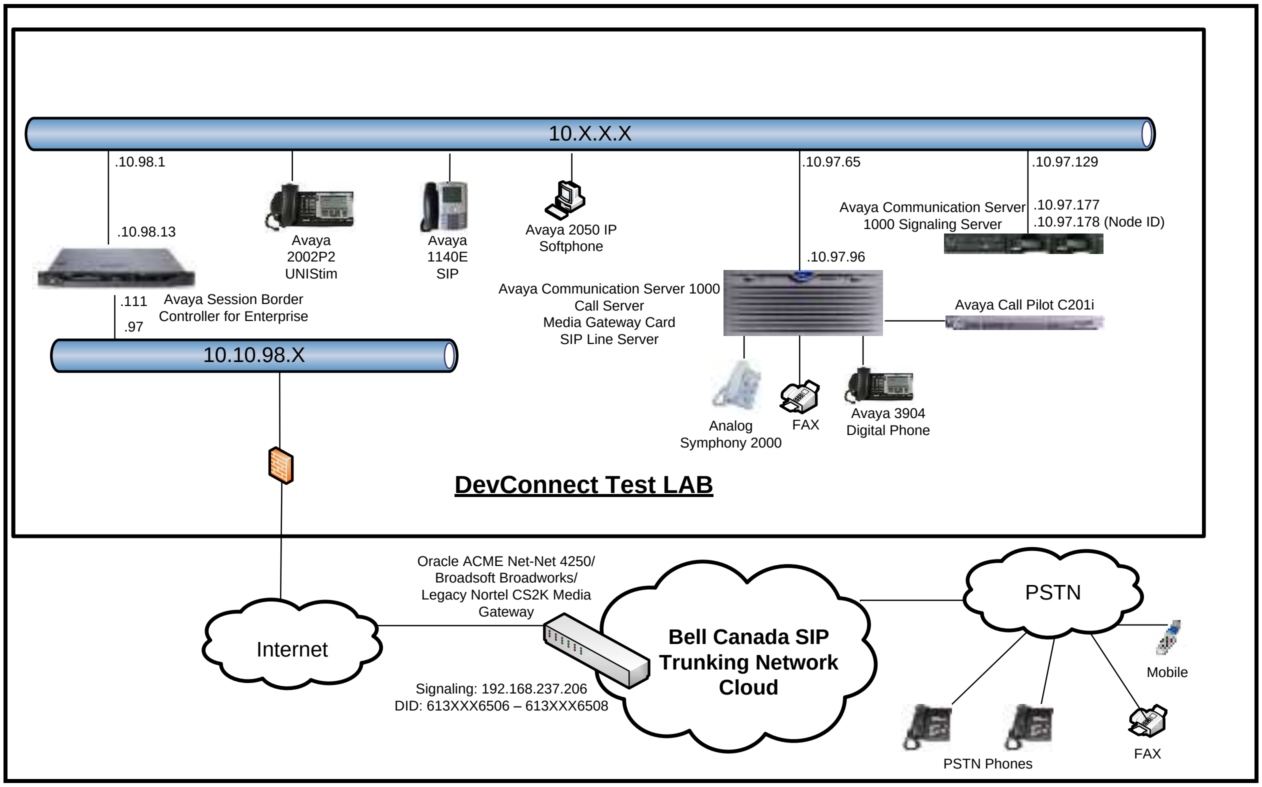

10.X.X.X
.10.98.1
.10.98.13
Avaya 2002P2 UNIStim
Avaya 1140E SIP
Avaya 2050 IP Softphone
.10.97.65
.10.97.129
Avaya Communication Server 1000 Signaling Server
.10.97.177
.10.97.178 (Node ID)
.10.97.96
.111
.97
Avaya Session Border Controller for Enterprise
Avaya Communication Server 1000 Call Server Media Gateway Card SIP Line Server
Avaya Call Pilot C201i
10.10.98.X
Analog Symphony 2000
FAX
Avaya 3904 Digital Phone
DevConnect Test LAB
Oracle ACME Net-Net 4250/ Broadsoft Broadworks/ Legacy Nortel CS2K Media Gateway
Internet
Bell Canada SIP Trunking Network Cloud
PSTN
Mobile
Signaling: 192.168.237.206
DID: 613XXX6506 – 613XXX6508
PSTN Phones
FAX

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

# 4. Equipment and Software Validated

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

**Avaya systems:**

| **Equipment/Software** | **Release/Version** |
|---|---|
| Avaya Communication Server 1000 (CPPM) | Call Server: 765 P +<br>Signaling Server: 7.65.16 GA<br>SIP Line Server: 7.65.16 GA |
| Avaya Call Pilot C201i | Call Pilot Voice Mail Manager: 05.00.41.143 |
| Avaya Session Border Controller for Enterprise<br>running on Dell R210 V2 Server | 7.0.0-21-6602<br>(Patch: sbc700-p001-20151005-7.0.0-21.x86_64.rpm) |
| Avaya Phones:<br>2002 P2 (UNIStim)<br>1140E SIP | <br>0604DCO<br>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 Trunk 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 as follows:

**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-carrdtct-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
```

# 5. Configure Avaya Communication Server 1000

These Application Notes use 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 Trunk 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 10**.

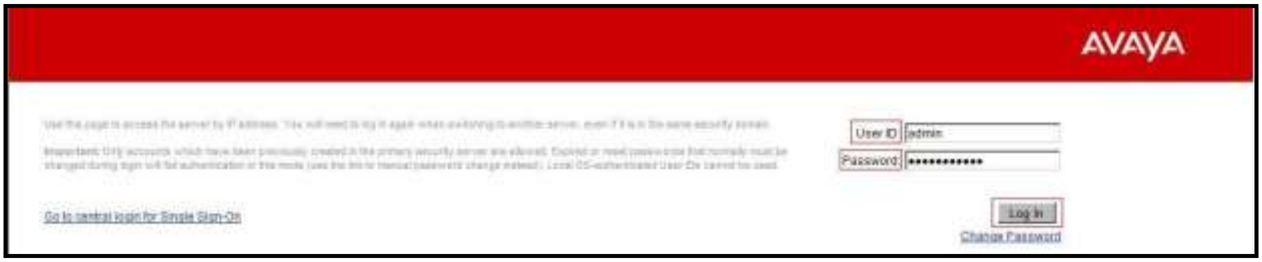
The procedures below describe the configuration details for configuring the CS1000.

## 5.1. Log into Communication Server 1000 System

### 5.1.1. Log into Communication Server 1000 Element Manager (EM)

Log in using the web based Avaya Unified Communications Management GUI. Avaya Unified Communications Management GUI may be launched directly via http://<ipaddress> where the relevant <ipaddress> is the TLAN IP address of the CS1000. Avaya Unified Communications Management can also be implemented on System Manager.

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



Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

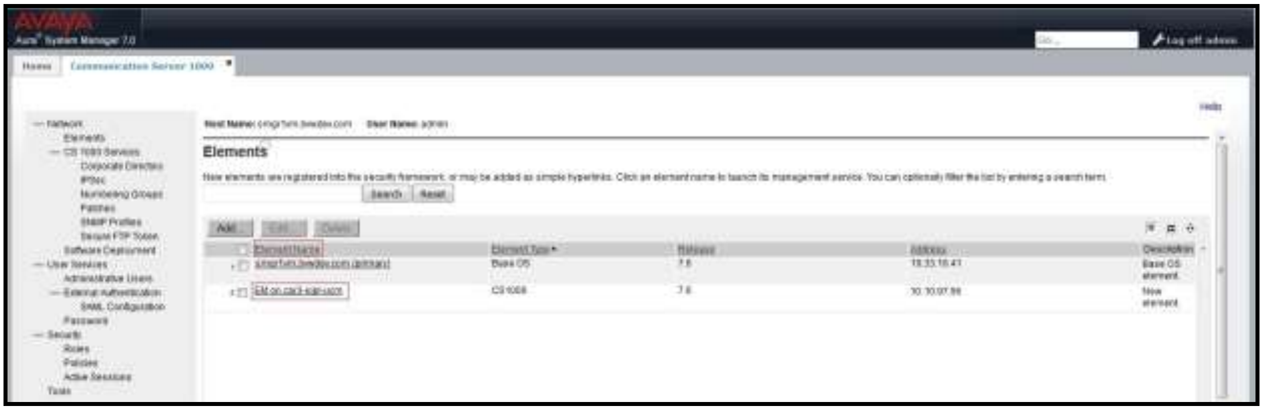
Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.

User ID: admin

Password: ••••••••••••

**Figure 2 – Communication Server 1000 Log In 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:



Host Name: smgr7vm.bvwdev.com User Name: admin

Elements

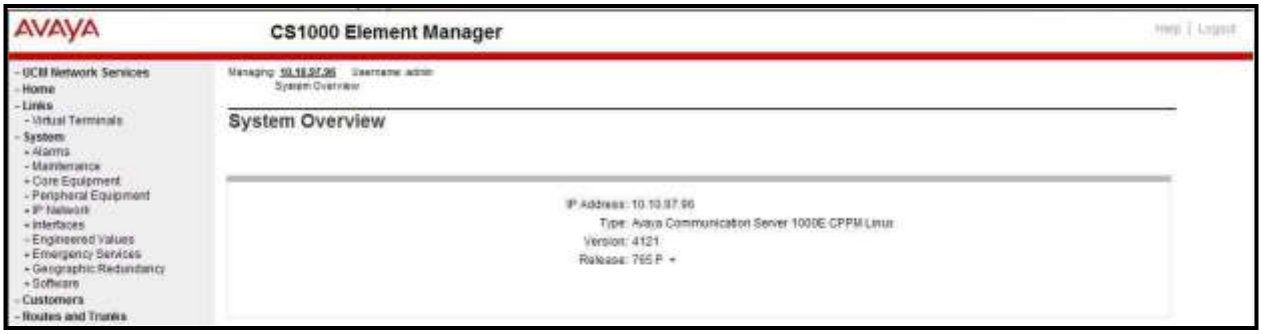
New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

| Element Name | Element Type | Release | Address | Description |
|---|---|---|---|---|
| smgr7vm.bvwdev.com (primary) | Base OS | 7.6 | 10.33.10.41 | Base OS element |
| EM on cppl-sipl-ucm | CS1000 | 7.6 | 10.10.97.98 | New element |

**Figure 3 – Communication Server 1000 Management**

The CS1000 Element Manager **System Overview** page is displayed as shown in **Figure 4**.

IP Address: 10.10.97.96
Type:  Avaya Communication Server 1000E CPPM Linux
Version: 4121
Release: 765 P +



Managing: 10.10.97.96 Username: admin
System Overview

System Overview

IP Address: 10.10.97.96
Type: Avaya Communication Server 1000E CPPM Linux
Version: 4121
Release: 765 P +

**Figure 4 – 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: Thu Nov 12 09:22:18 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 09:50 12/11/2015
```

```
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.

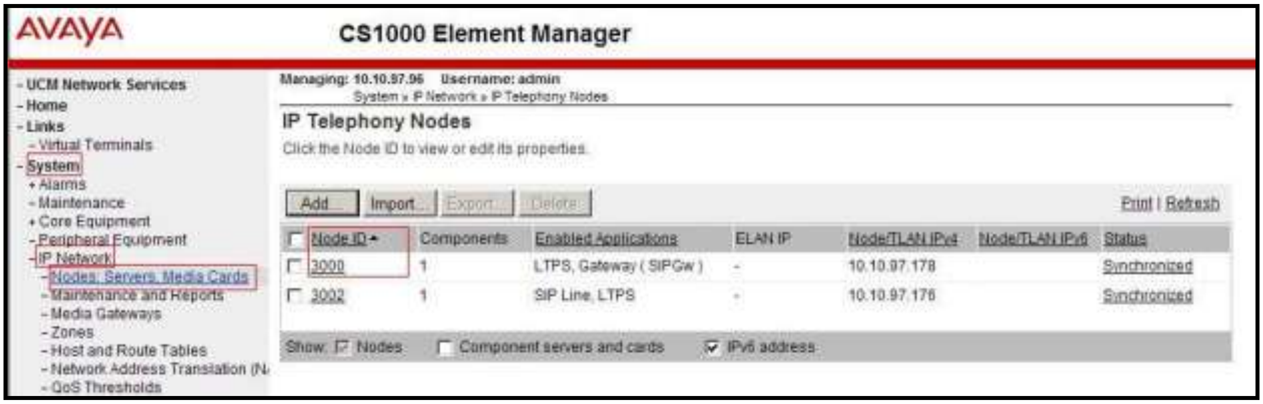
## 5.2. Administer IP Telephony Node

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 10**.

Select **System → IP Network → Nodes: Servers, Media Cards** and then click on the **Node ID** as shown in **Figure 5**.



Managing: 10.10.97.96 Username: admin

System » IP Network » IP Telephony Nodes

IP Telephony Nodes

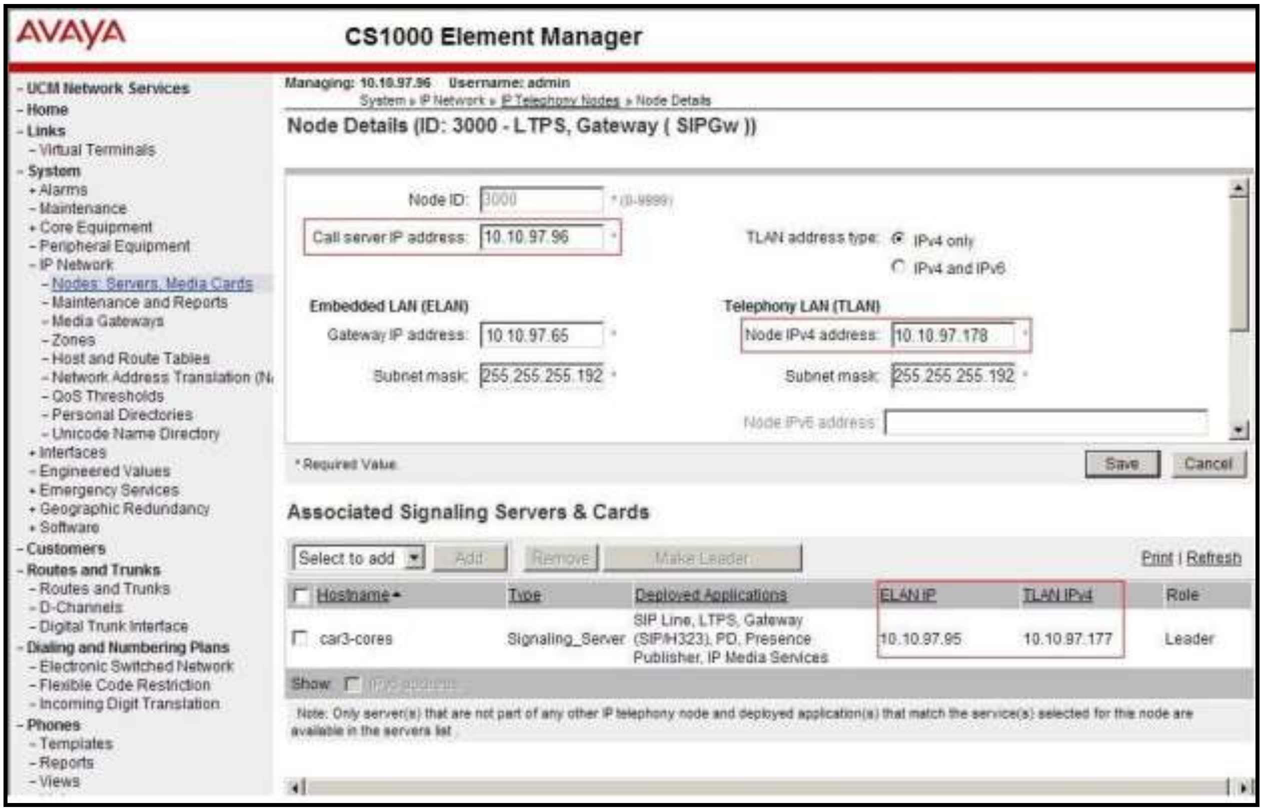
Click the Node ID to view or edit its properties.

| □ | Node ID ▴ | Components | Enabled Applications | ELAN IP | Node/TLAN IPv4 | Node/TLAN IPv6 | Status |
|---|---|---|---|---|---|---|---|
| □ | 3000 | 1 | LTPS, Gateway ( SIPGw ) | - | 10.10.97.178 |  | Synchronized |
| □ | 3002 | 1 | SIP Line, LTPS | - | 10.10.97.176 |  | Synchronized |

Show: ☑ Nodes □ Component servers and cards ☑ IPv6 address

**Figure 5 – IP Telephony Node**

The **Node Details** screen is displayed in **Figure 6** 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.



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

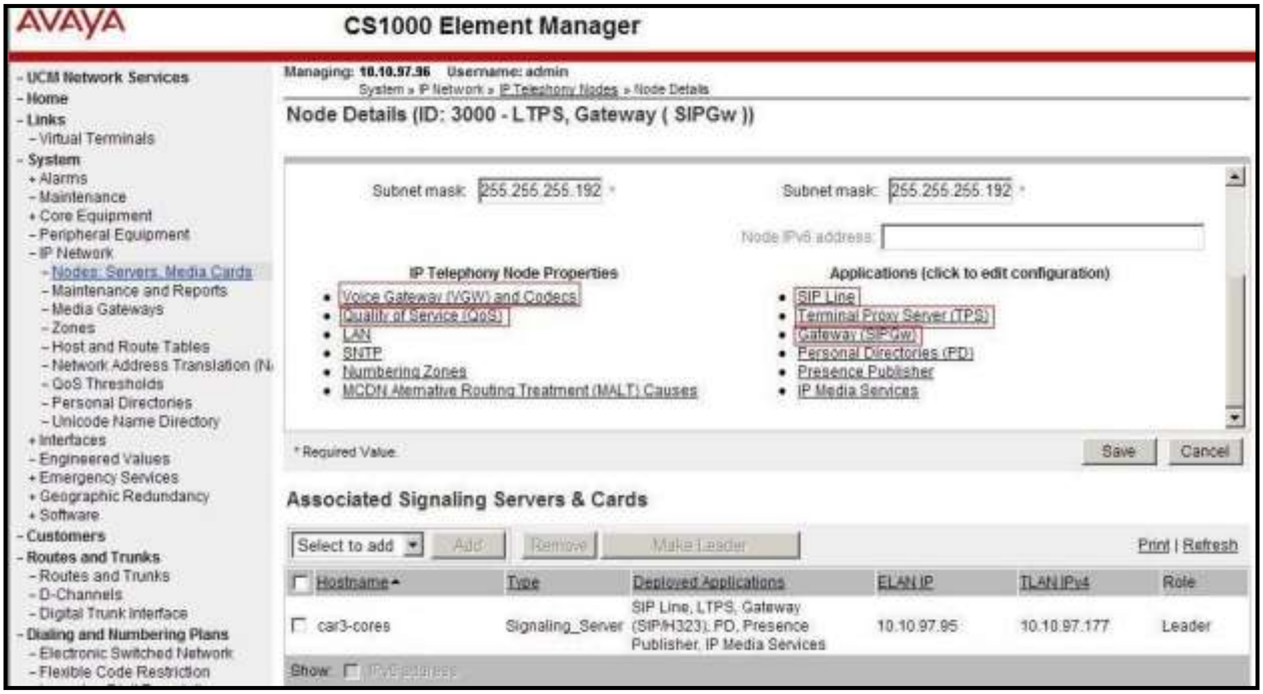
| □ Hostname | Type | Deployed Applications | ELAN IP | TLAN IPv4 | Role |
|---|---|---|---|---|---|
| □ car3-cores | Signaling_Server | SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services | 10.10.97.95 | 10.10.97.177 | Leader |

Show: □ IPv6 address

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 6 – Node Details 1**

Scrolling down, the **Node Details** screen displays the **IP Telephony Node Properties** and **Applications** sections as shown in **Figure 7**.



Managing: 10.10.97.96 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 (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN 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.

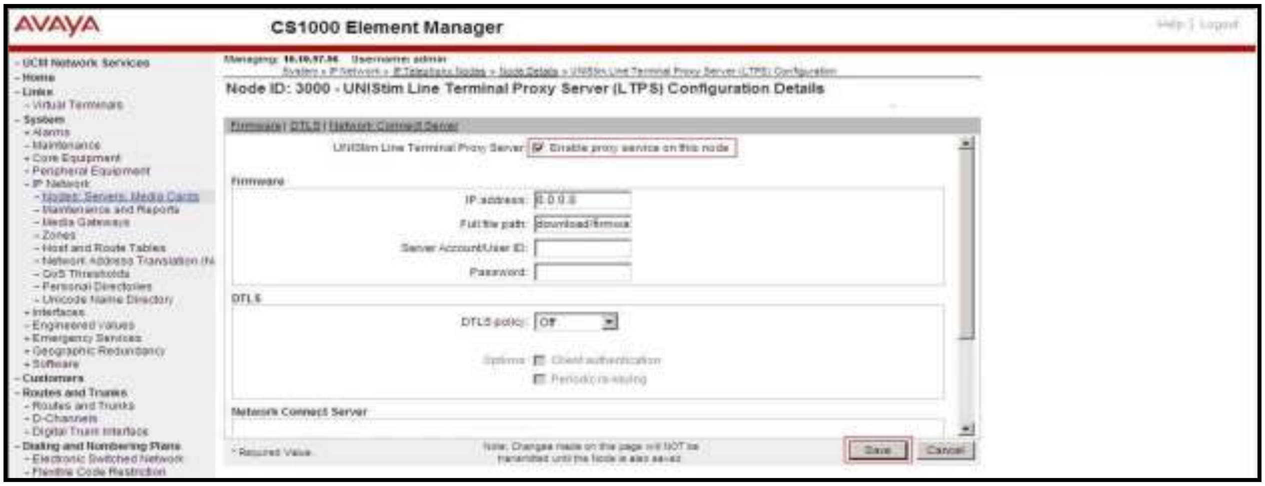
Associated Signaling Servers & Cards

| 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 |

**Figure 7 – 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 7**. Check the **UNIStim Line Terminal Proxy Server** checkbox to enable proxy service on this node and then click the **Save** button as shown in **Figure 8**.



Managing: 10.10.97.96 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » UNIStim Line Terminal Proxy Server (LTPS) Configuration

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

UNIStim Line Terminal Proxy Server: ☑ Enable proxy service on this node

Firmware

IP address: 0.0.0.0

Full file path: download/firmwa

Server Account/User ID:

Password:

DTLS

DTLS policy: Off

Options: ☐ Client authentication

☐ Periodic re-keying

Network Connect Server

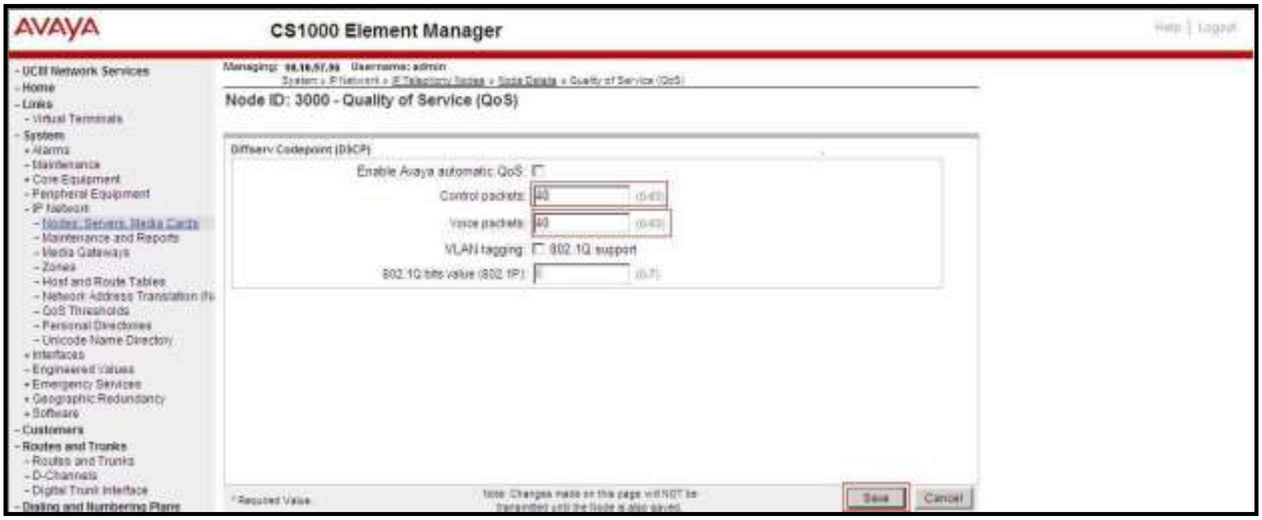
* Required Value.

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

**Figure 8 – 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 7**. The default Diffserv values are shown in **Figure 9**. Click on the **Save** button.



Managing: 10.10.97.96 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Quality of Service (QoS)

Node ID: 3000 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: □
Control packets: 40 (0-63)
Voice packets: 40 (0-63)
VLAN tagging: □ 802.1Q support
802.1Q bits value (802.1P): 6 (0-7)

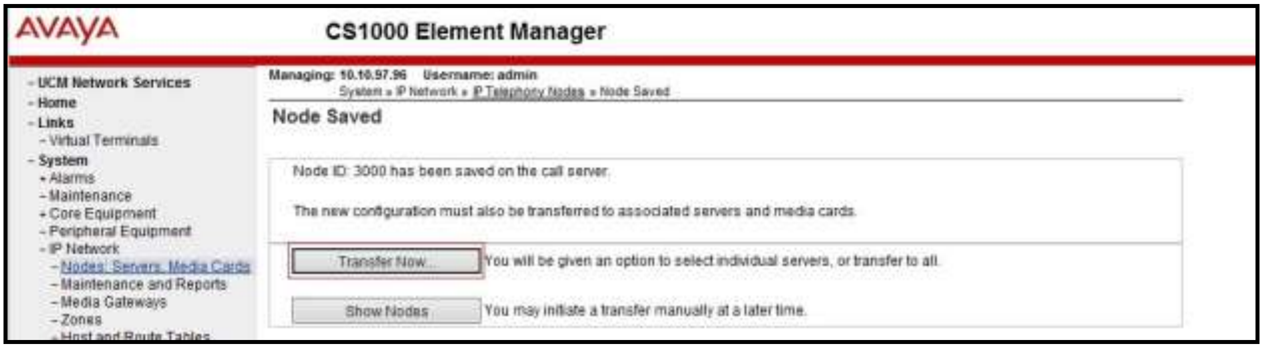
* Required Value

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

**Figure 9 – QoS Configuration Details**

### 5.2.4. Synchronize New Configuration

Continuing from **Section 5.2.3**, return to the **Node Details** page (**Figure 6**) and click on the **Save** button. The **Node Saved** screen is displayed. Click on **Transfer Now**.



Managing: 10.10.97.96 Username: admin
System » IP Network » IP Telephony Nodes » Node Saved

Node Saved

Node ID: 3000 has been saved on the call server.

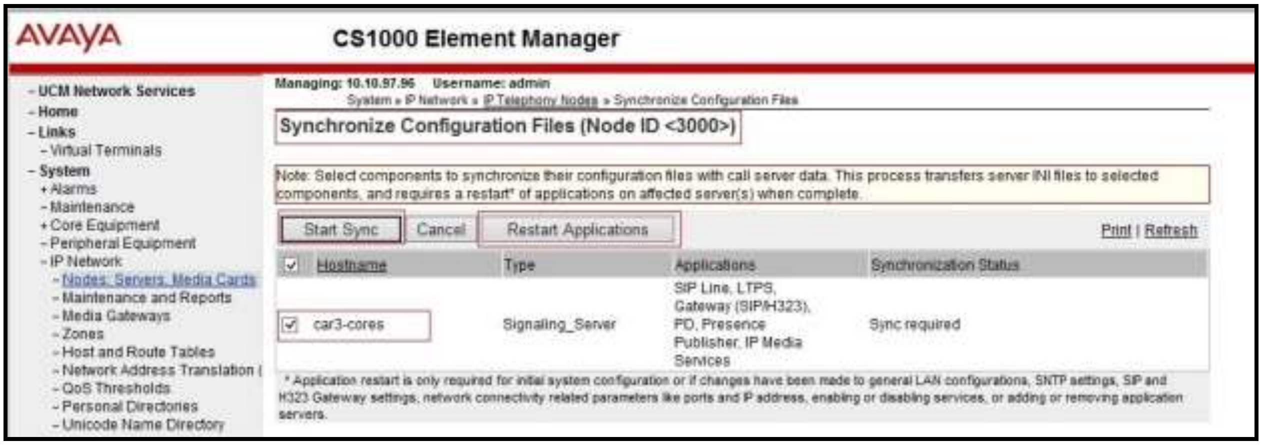
The new configuration must also be transferred to associated servers and media cards.

Transfer Now... You will be given an option to select individual servers, or transfer to all.

Show Nodes You may initiate a transfer manually at a later time.

**Figure 10 – 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**.



Managing: 10.10.97.96 Username: admin

System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <3000>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

| ☑ Hostname | Type | Applications | Synchronization Status |
|---|---|---|---|
| ☑ car3-cores | Signaling_Server | SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services | Sync required |

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

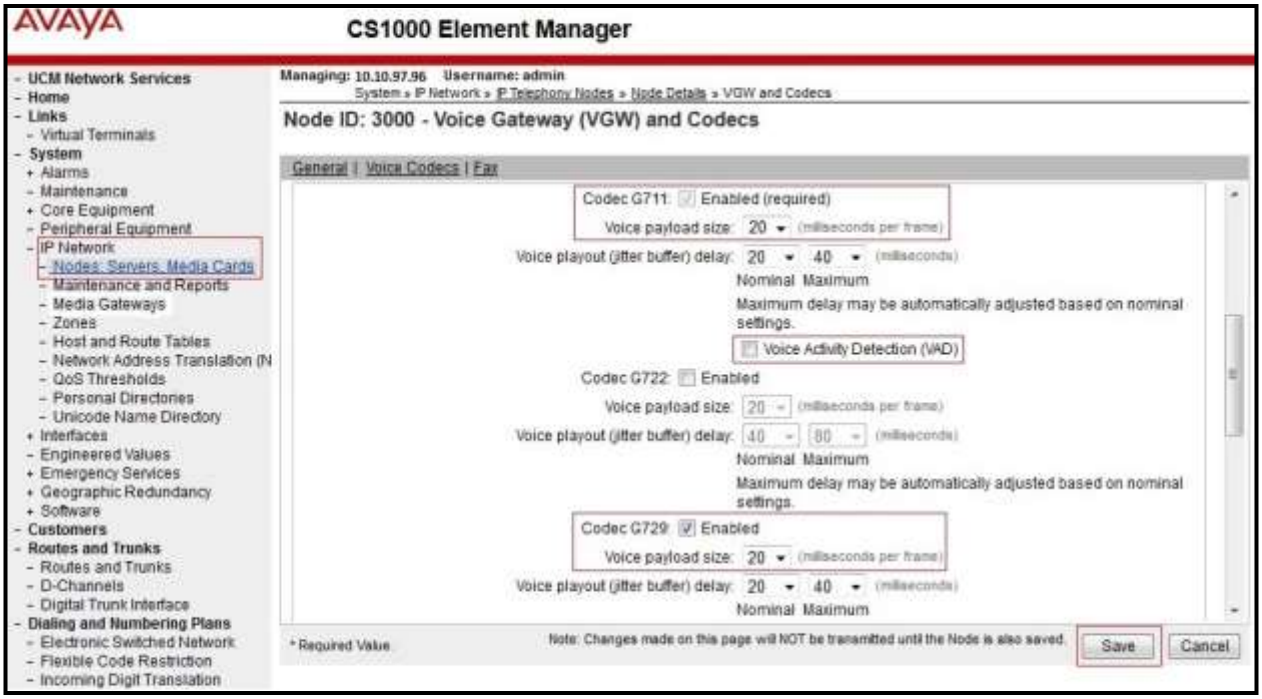
**Figure 11 – Node Synchronized Screen**

## 5.3. Administer Voice Codec

### 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 7**, 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.



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

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

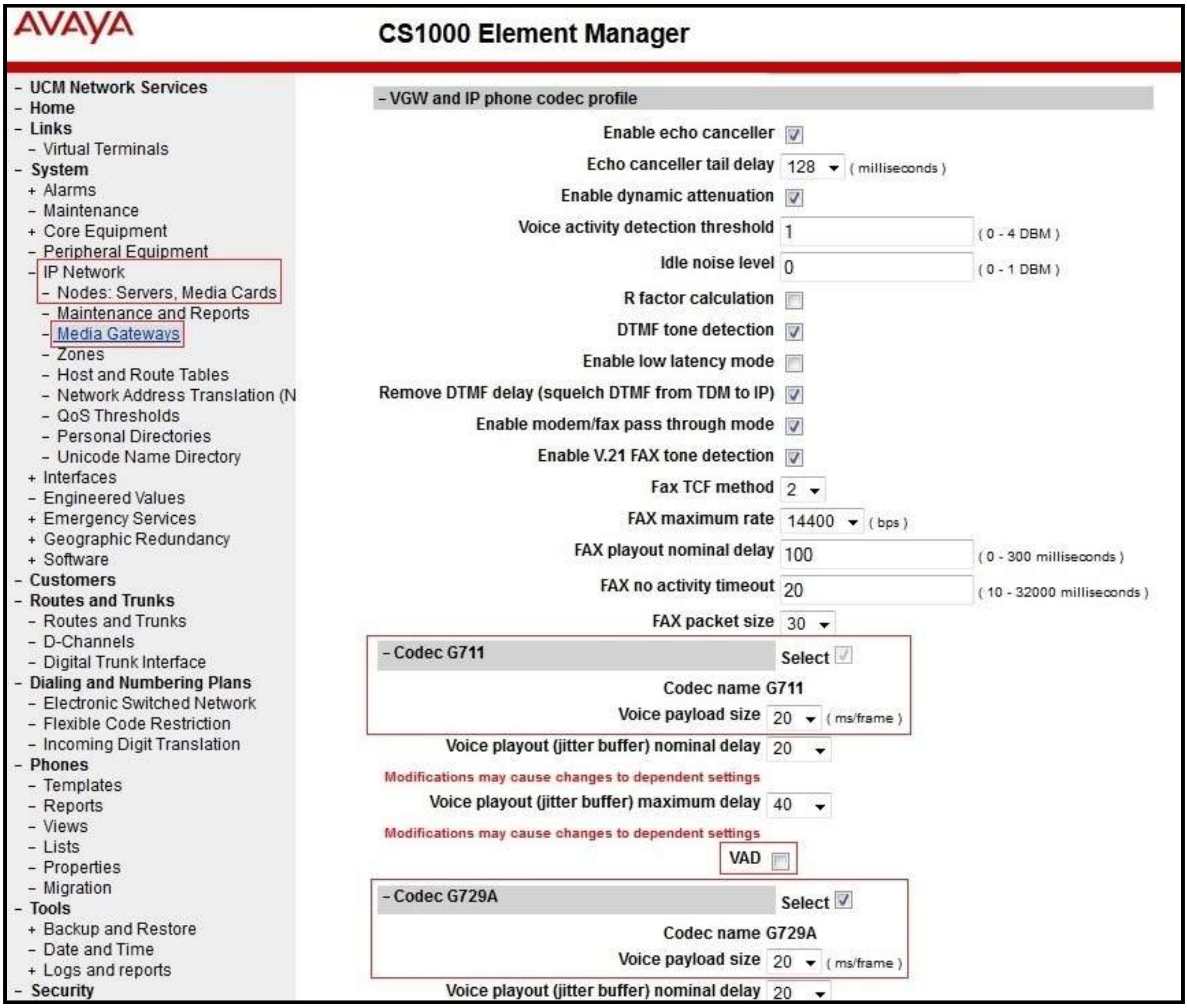
Note: Changes made on this page will NOT be transmitted until the Node is also saved.

**Figure 12 – 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 12**, 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 13**. Scroll down to the bottom of the page and click on the **Save** button (not shown).



- VGW and IP phone codec profile

Enable echo canceller ☑
Echo canceller tail delay 128 ( milliseconds )
Enable dynamic attenuation ☑
Voice activity detection threshold 1 ( 0 - 4 DBM )
Idle noise level 0 ( 0 - 1 DBM )
R factor calculation □
DTMF tone detection ☑
Enable low latency mode □
Remove DTMF delay (squelch DTMF from TDM to IP) ☑
Enable modem/fax pass through mode ☑
Enable V.21 FAX tone detection ☑
Fax TCF method 2
FAX maximum rate 14400 ( bps )
FAX playout nominal delay 100 ( 0 - 300 milliseconds )
FAX no activity timeout 20 ( 10 - 32000 milliseconds )
FAX packet size 30

- Codec G711 Select ☑
Codec name G711
Voice payload size 20 ( ms/frame )
Voice playout (jitter buffer) nominal delay 20
Modifications may cause changes to dependent settings
Voice playout (jitter buffer) maximum delay 40
Modifications may cause changes to dependent settings
VAD □

- Codec G729A Select ☑
Codec name G729A
Voice payload size 20 ( ms/frame )
Voice playout (jitter buffer) nominal delay 20

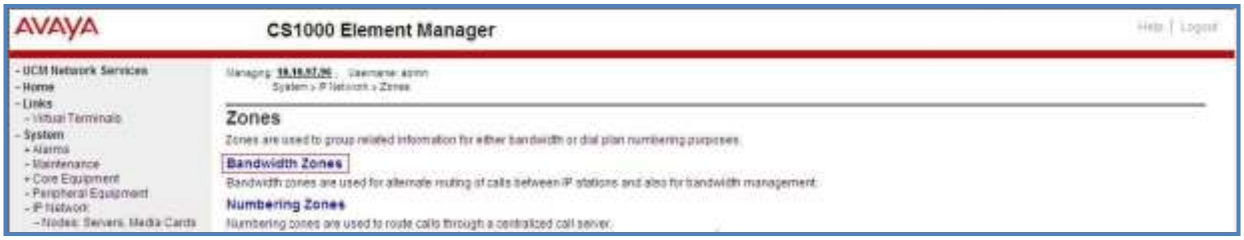
**Figure 13 – Media Gateways Configuration Details**

## 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 14**.



Managing: 10.10.97.96 Username: admin
System » IP Network » Zones

Zones

Zones are used to group related information for either bandwidth or dial plan numbering purposes.

Bandwidth Zones

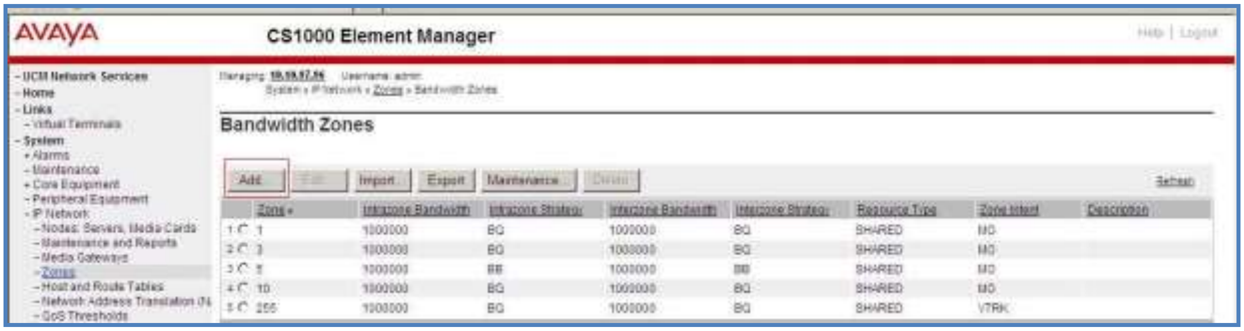
Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.

Numbering Zones

Numbering zones are used to route calls through a centralized call server.

**Figure 14 – Zones Page**

The **Bandwidth Zones** screen is displayed as shown in **Figure 15**. Click **Add** to create a new zone for IP Phones.



Managing: 10.10.97.96 Username: admin
System » IP Network » Zones » Bandwidth Zones

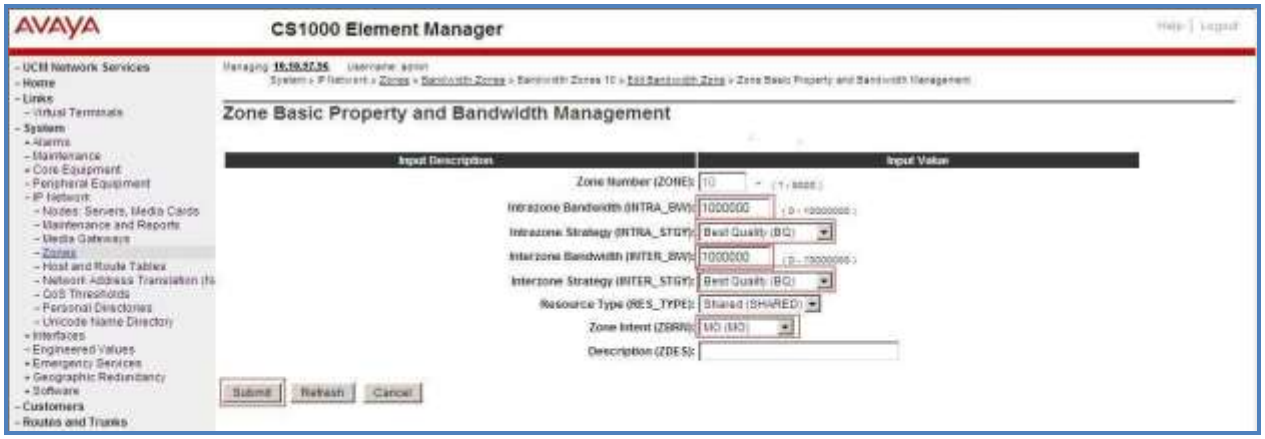
Bandwidth Zones

| | Zone ▴ | Intrazone Bandwidth | Intrazone Strategy | Interzone Bandwidth | Interzone Strategy | Resource Type | Zone Intent | Description |
|---|---|---|---|---|---|---|---|---|
| 1 ○ | 1 | 1000000 | BQ | 1000000 | BQ | SHARED | MO | |
| 2 ○ | 3 | 1000000 | BQ | 1000000 | BQ | SHARED | MO | |
| 3 ○ | 5 | 1000000 | BB | 1000000 | BB | SHARED | MO | |
| 4 ○ | 10 | 1000000 | BQ | 1000000 | BQ | SHARED | MO | |
| 5 ○ | 255 | 1000000 | BQ | 1000000 | BQ | SHARED | VTRK | |

**Figure 15 – Bandwidth Zones**

Select and input the values as shown below (in the red boxes) in **Figure 16**, 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.



Managing: 10.10.97.36 Username: admin

System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 10 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

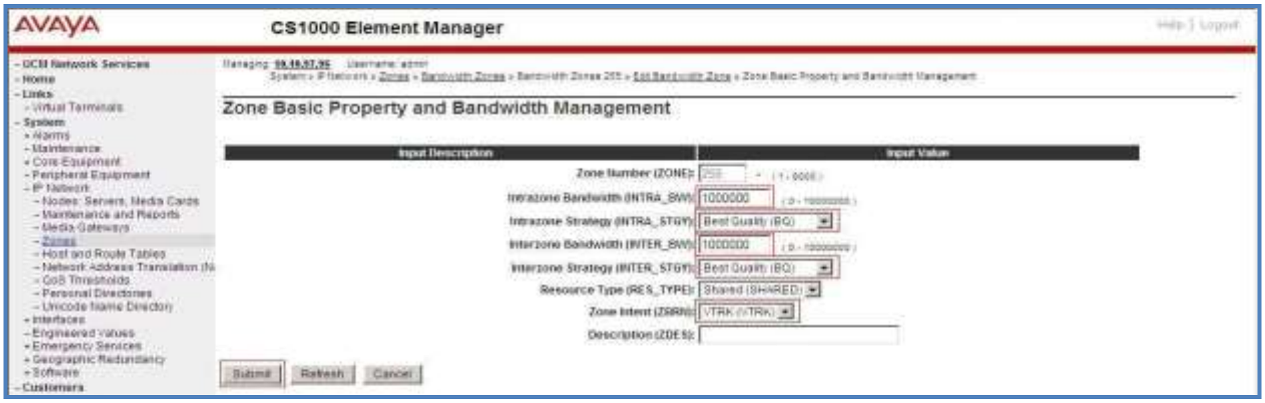
Zone Basic Property and Bandwidth Management

| Input Description | Input Value |
|---|---|
| Zone Number (ZONE): | 10 * ( 1 - 8000 ) |
| Intrazone Bandwidth (INTRA_BW): | 1000000 ( 0 - 10000000 ) |
| Intrazone Strategy (INTRA_STGY): | Best Quality (BQ) |
| Interzone Bandwidth (INTER_BW): | 1000000 ( 0 - 10000000 ) |
| Interzone Strategy (INTER_STGY): | Best Quality (BQ) |
| Resource Type (RES_TYPE): | Shared (SHARED) |
| Zone Intent (ZBRN): | MO (MO) |
| Description (ZDES): | |

**Figure 16 – 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 17** and then click on the **Submit** button.



Managing: 10.10.97.36 Username: admin

System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 255 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

| Input Description | Input Value |
|---|---|
| Zone Number (ZONE): | 255 * ( 1 - 8000 ) |
| Intrazone Bandwidth (INTRA_BW): | 1000000 ( 0 - 10000000 ) |
| Intrazone Strategy (INTRA_STGY): | Best Quality (BQ) |
| Interzone Bandwidth (INTER_BW): | 1000000 ( 0 - 10000000 ) |
| Interzone Strategy (INTER_STGY): | Best Quality (BQ) |
| Resource Type (RES_TYPE): | Shared (SHARED) |
| Zone Intent (ZBRN): | VTRK (VTRK) |
| Description (ZDES): | |

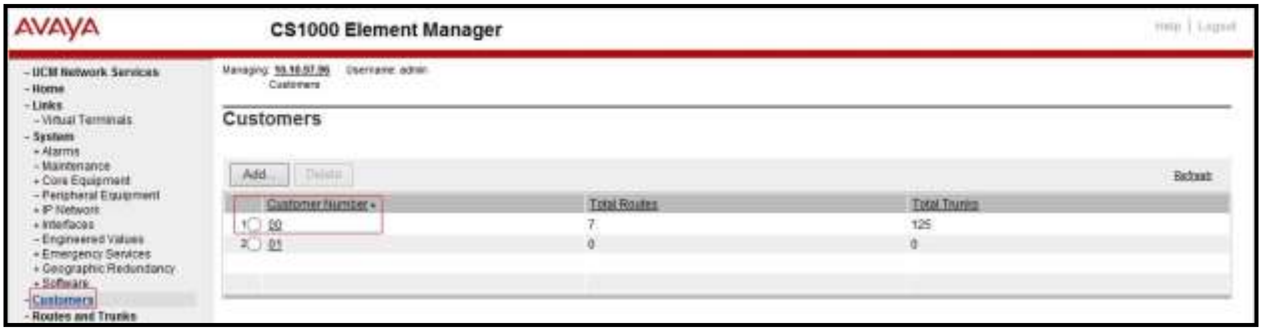
**Figure 17 – Bandwidth Management Configuration Details – Virtual SIP trunk**

## 5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP connection between the SIP Signaling Gateway and Avaya SBCE.

### 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**.



| | Customer Number ▴ | Total Routes | Total Trunks |
|---|---|---|---|
| 1 ○ | 00 | 7 | 125 |
| 2 ○ | 01 | 0 | 0 |

**Figure 18 – 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.

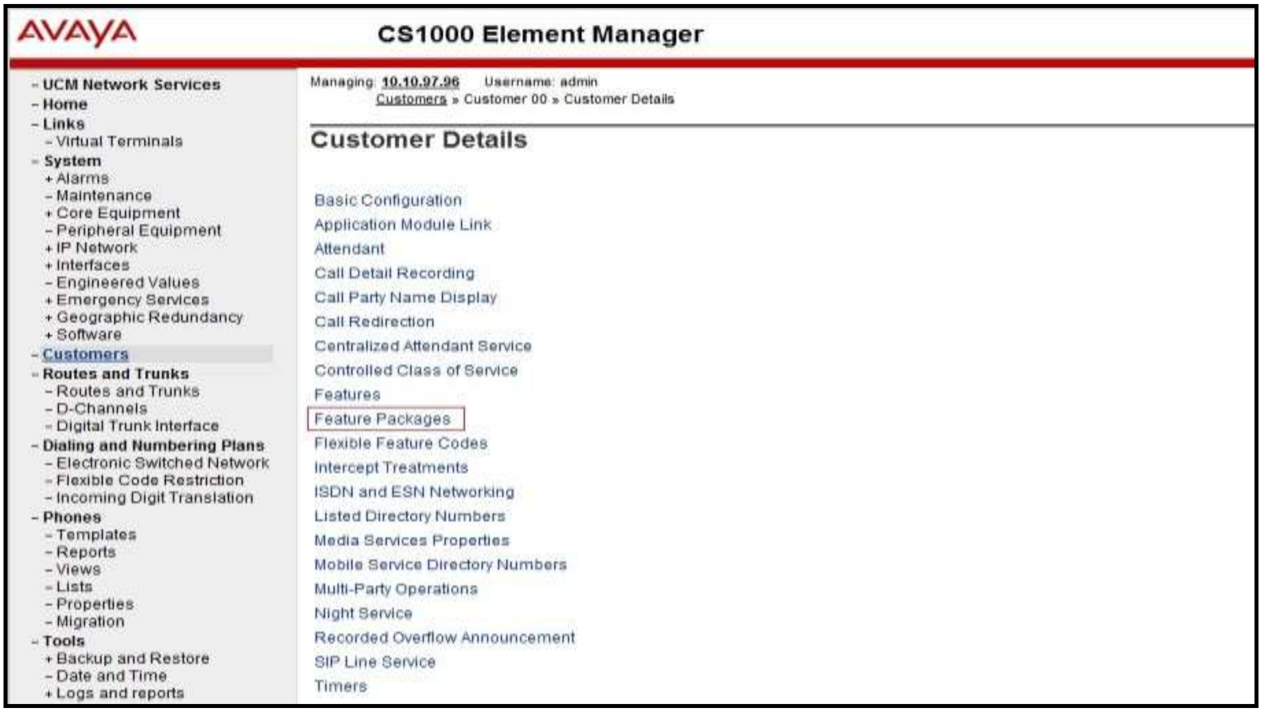
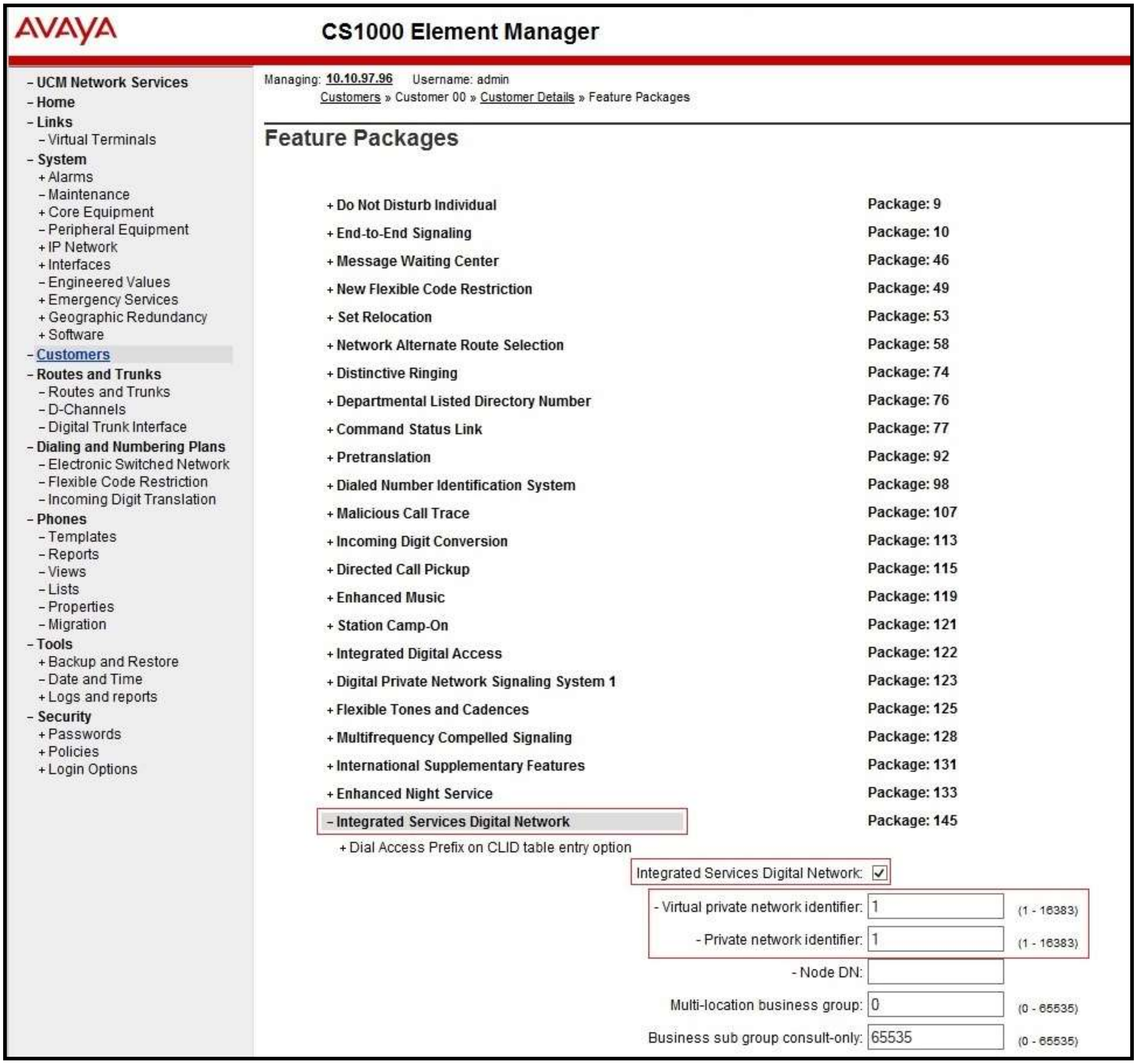


**Figure 19 – Customer – ISDN Configuration 2**

The screen is updated with a listing of available **Feature Packages** (not all features are shown in **Figure 20** 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).



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: ☑

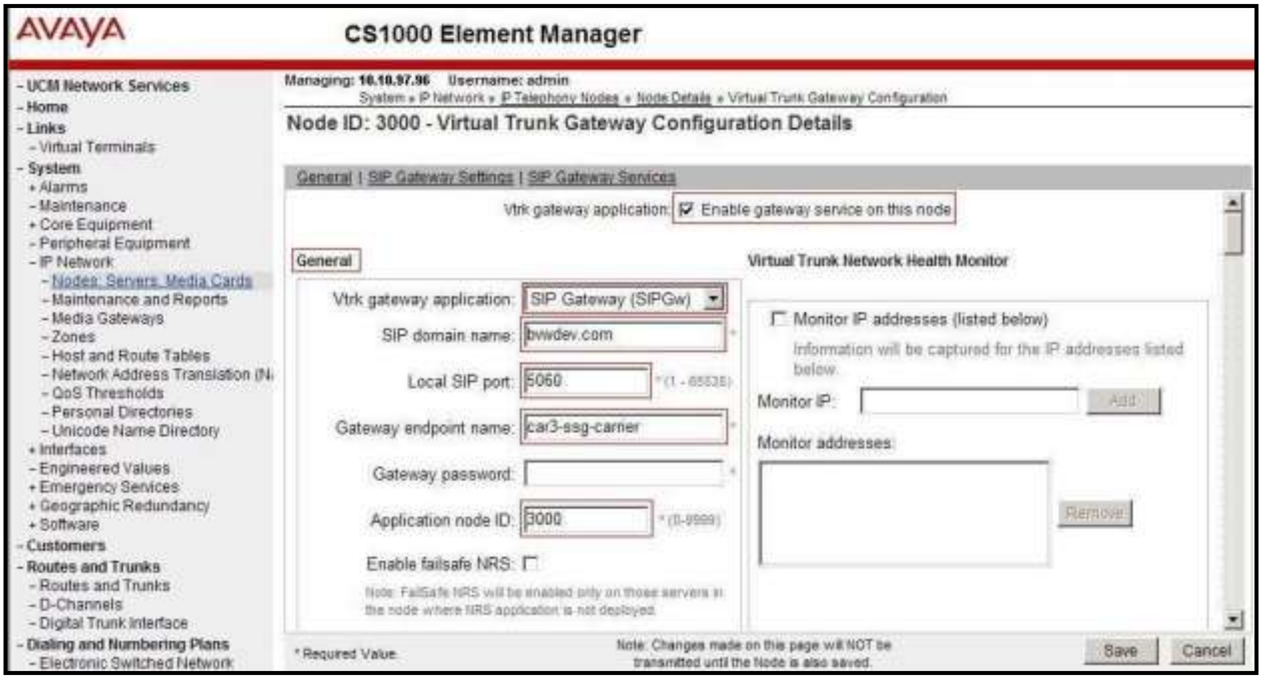
| | | |
|---|---|---|
| - Virtual private network identifier: | 1 | (1 - 16383) |
| - Private network identifier: | 1 | (1 - 16383) |
| - Node DN: | | |
| Multi-location business group: | 0 | (0 - 65535) |
| Business sub group consult-only: | 65535 | (0 - 65535) |

**Figure 20 – 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 7**, **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 21**. The **SIP domain name** and **Local SIP port** should be matched in the configuration of Avaya SBCE in **Section 6.2.4**, **6.2.6**, and **6.2.8**.



Managing: 10.10.97.96 Username: admin

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

Vtrk gateway application: ☑ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw)

SIP domain name: bwdev.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: car3-ssg-carrier *

Gateway password: *

Application node ID: 3000 * (0-9999)

Enable failsafe NRS: ☐

Note: FailSafe NRS will be enabled only on those servers in the node where NRS application is not deployed.

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

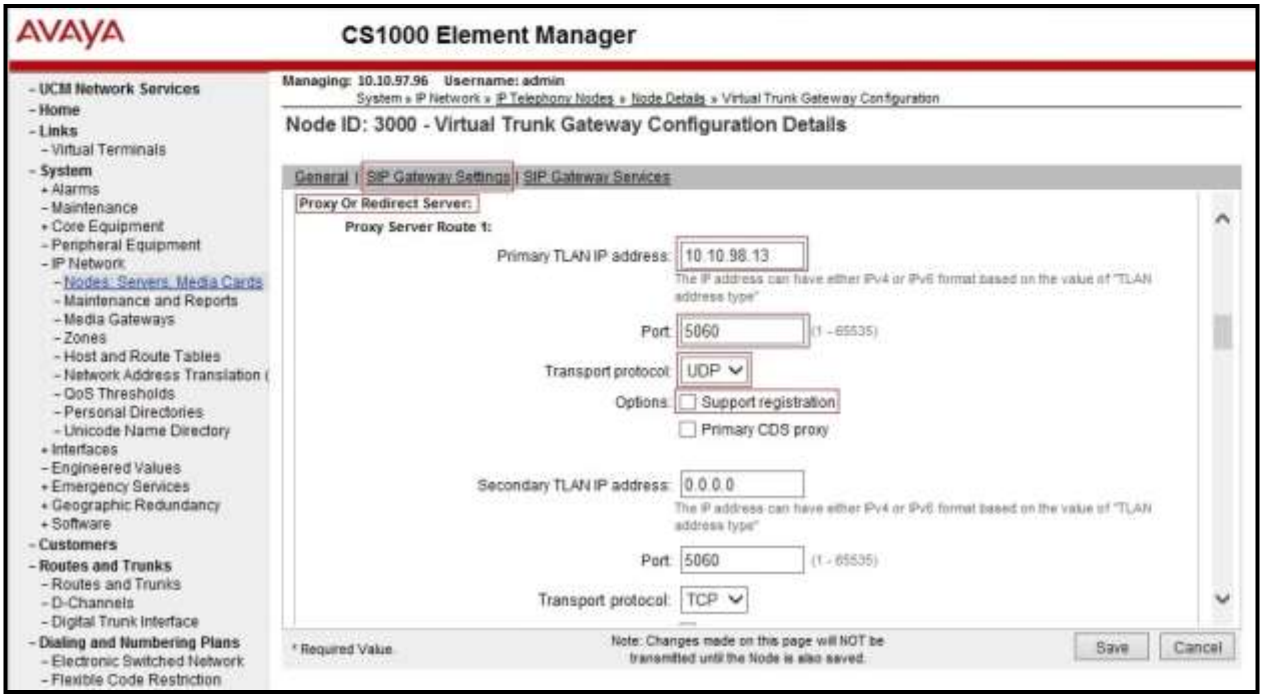
Monitor addresses:

* Required Value.

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

**Figure 21 – 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 22**. Enter the internal IP address of Avaya SBCE in the **Primary TLAN IP address** field. Enter **5060** for **Port** and select **UDP** for **Transport protocol**. Uncheck the **Support registration** checkbox.



CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.10.98.13
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: □ Support registration
□ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

* Required Value

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

**Figure 22 – Virtual Trunk Gateway Configuration Details**

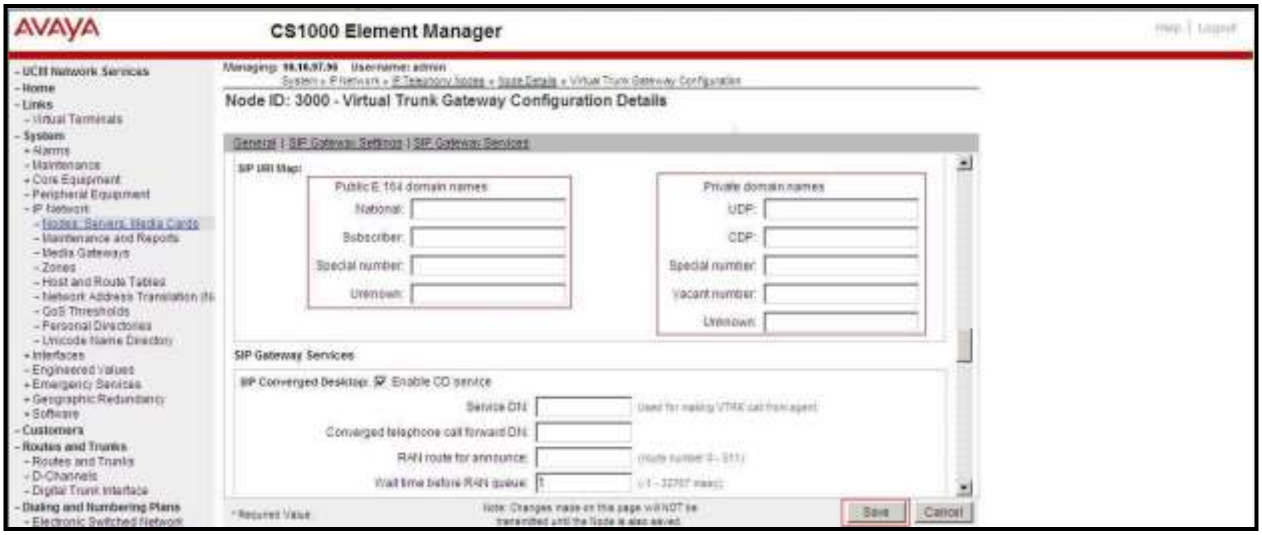
On the same page as shown in **Figure 22**, scroll down to the **SIP URI Map** section.
Under **Public E.164 domain names**, enter the following:

- **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 23**. Click on the **Save** button.



Managing: 10.10.97.96 Username: admin

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

SIP URI Map:

Public E.164 domain names
National:
Subscriber:
Special number:
Unknown:

Private domain names
UDP:
CDP:
Special number:
Vacant number:
Unknown:

SIP Gateway Services

SIP Converged Desktop: ☑ Enable CD service

Service DN: Used for making VTRK call from agent

Converged telephone call forward DN:

RAN route for announce: (route number 0 - 511)

Wait time before RAN queue: 1 (1 - 32767 msec)

* Required Value

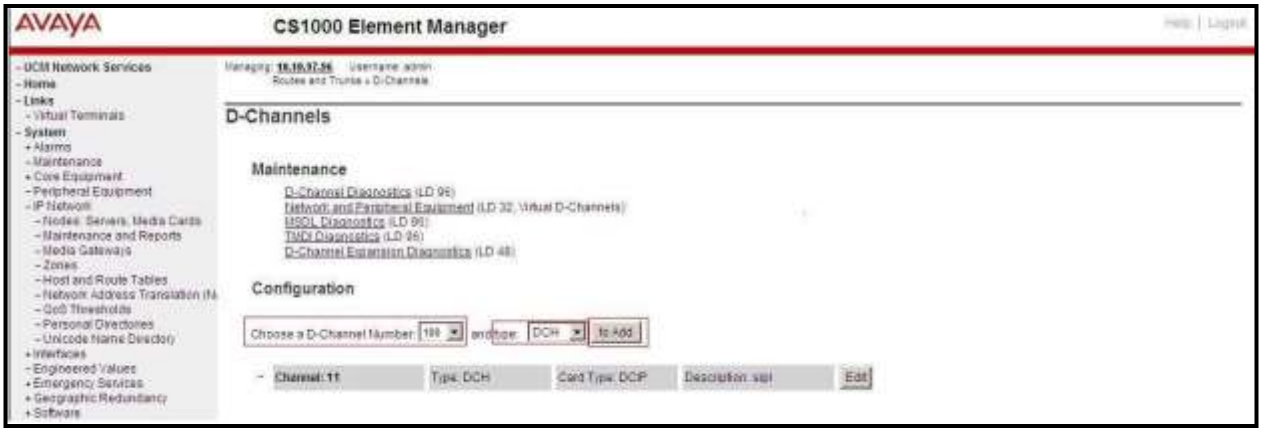
Note: Changes made on this page will NOT be transmitted until the Node is also saved.

**Figure 23 – 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 24**. Click on the **to Add** button.



Managing: 10.10.97.96 Username: admin

D-Channels

Maintenance

D-Channel Diagnostics (LD 96)
Network and Peripheral Equipment (LD 32, Virtual D-Channels)
MSDL Diagnostics (LD 96)
TMDI Diagnostics (LD 96)
D-Channel Expansion Diagnostics (LD 48)

Configuration

Choose a D-Channel Number: 199 and type: DCH

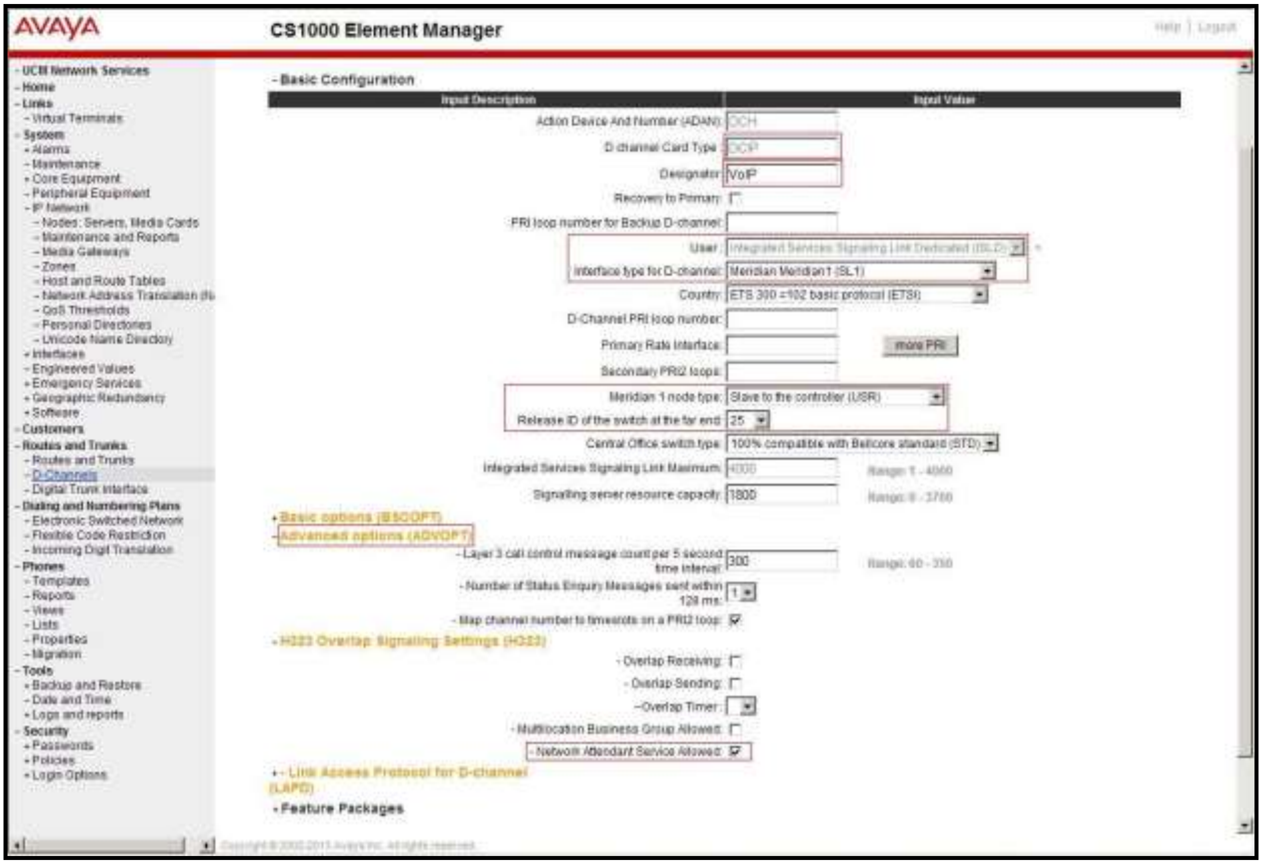
- Channel: 11 Type: DCH Card Type: DCIP Description: sipl

**Figure 24 – D-Channels**

The **D-Channels 100 Property Configuration** screen is displayed next, as shown in **Figure 25**. 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 25**. Other fields are left as default.



**CS1000 Element Manager**

- Basic Configuration

| Input Description | Input Value |
|---|---|
| Action Device And Number (ADAN): | DCH |
| D channel Card Type: | DCIP |
| Designator: | VoIP |
| Recovery to Primary: | □ |
| PRI loop number for Backup D-channel: | |
| User: | Integrated Services Signaling Link Dedicated (ISLD) * |
| Interface type for D-channel: | Meridian Meridian1 (SL1) |
| Country: | ETS 300 =102 basic protocol (ETSI) |
| D-Channel PRI loop number: | |
| Primary Rate Interface: | |
| 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 - 3700 |

+ Basic options (BSCOPT)

- Advanced options (ADVOPT)

| | |
|---|---|
| - Layer 3 call control message count per 5 second time interval: | 300 Range: 60 - 350 |
| - Number of Status Enquiry Messages sent within 128 ms: | 1 |
| - Map channel number to timeslots on a PRI2 loop: | ☑ |

- H323 Overlap Signaling Settings (H323)

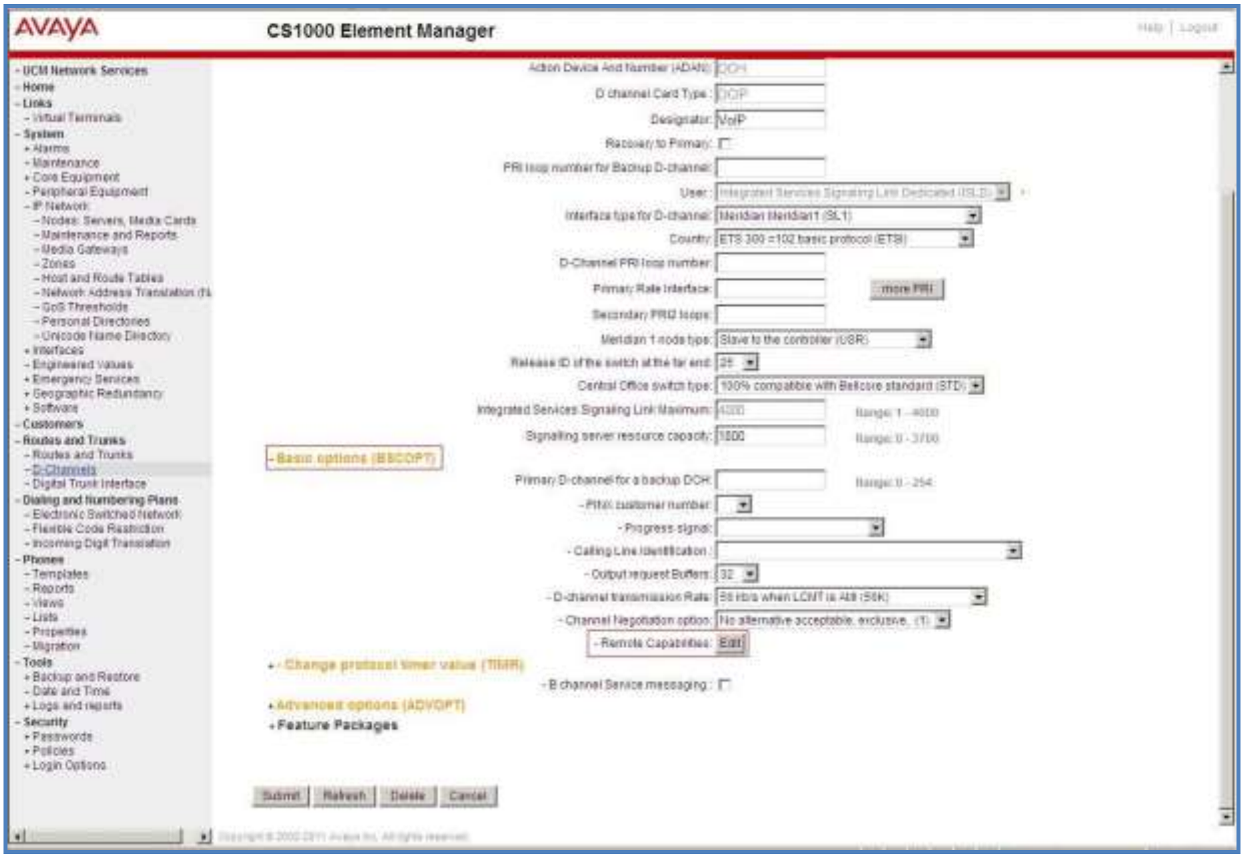
| | |
|---|---|
| - Overlap Receiving: | □ |
| - Overlap Sending: | □ |
| –Overlap Timer: | |
| - Multilocation Business Group Allowed: | □ |
| - Network Attendant Service Allowed: | ☑ |

+ - Link Access Protocol for D-channel (LAPD)

+ Feature Packages

**Figure 25 – D-Channel Configuration**

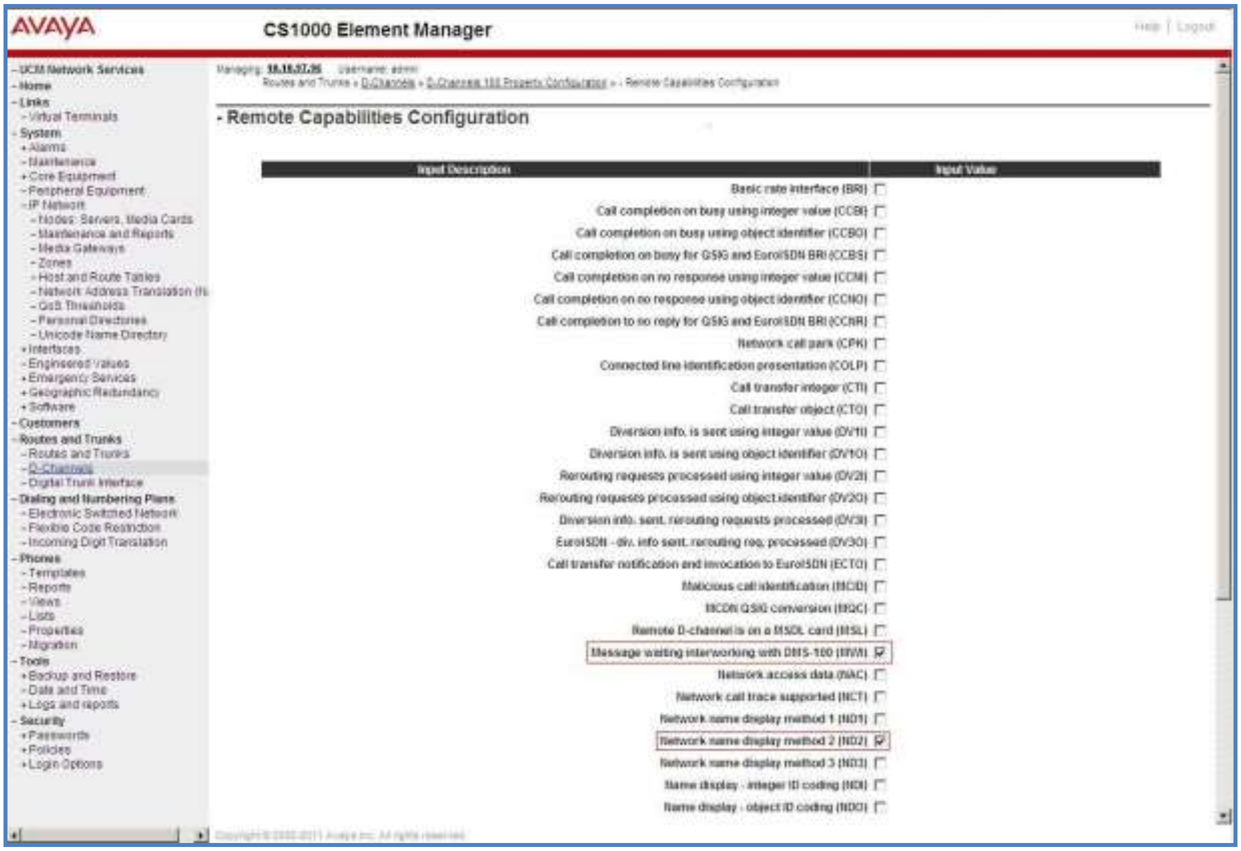
Click on **Basic Options (BSCOPT)** and click on the **Edit** button on the **Remote Capabilities** field as shown in **Figures 26**.



Action Device And Number (ADAN): DCH
D channel Card Type : DCIP
Designator: VoIP
Recovery to Primary: □
PRI loop number for Backup D-channel:
User : Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel: Meridian Meridian1 (SL1)
Country: ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:
Primary Rate Interface:
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 - 3700
Primary D-channel for a backup DCH: Range: 0 - 254
- PINX customer number:
- Progress signal:
- Calling Line Identification :
- Output request Buffers: 32
- D-channel transmission Rate: 56 kb/s when LCNT is A8 (56K)
- Channel Negotiation option: No alternative acceptable, exclusive. (1)
- Remote Capabilities: Edit
- B channel Service messaging : □

**Figure 26 – D-Channel Configuration**

The **Remote Capabilities Configuration** page appears as shown in **Figures 27**. Check the **ND2** and the **MWI** checkboxes.



Managing: 10.10.97.96 Username: admin
Routes and Trunks » D-Channels » D-Channels 100 Property Configuration » - Remote Capabilities Configuration

- Remote Capabilities Configuration

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

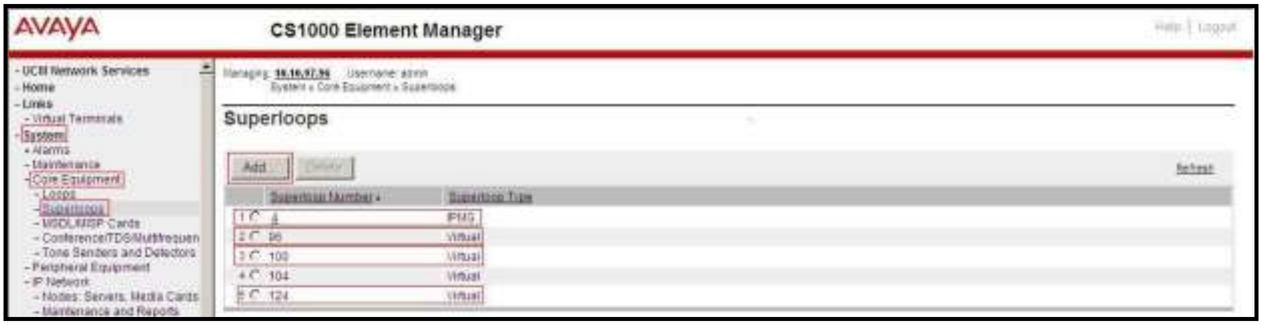
**Figure 27 – Remote Capabilities Configuration**

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 28**. In this example, Superloops 4, 96, 100, and 124 have been added and are being used.



Managing: 10.10.97.96 Username: admin
System » Core Equipment » Superloops

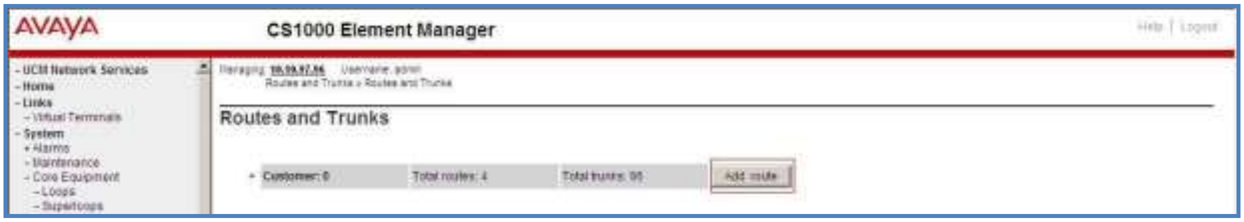
Superloops

| | Superloop Number | Superloop Type |
|---|---|---|
| 1 ○ | 4 | IPMG |
| 2 ○ | 96 | Virtual |
| 3 ○ | 100 | Virtual |
| 4 ○ | 104 | Virtual |
| 5 ○ | 124 | Virtual |

**Figure 28 – 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 29**.



Managing: 10.10.97.96 Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

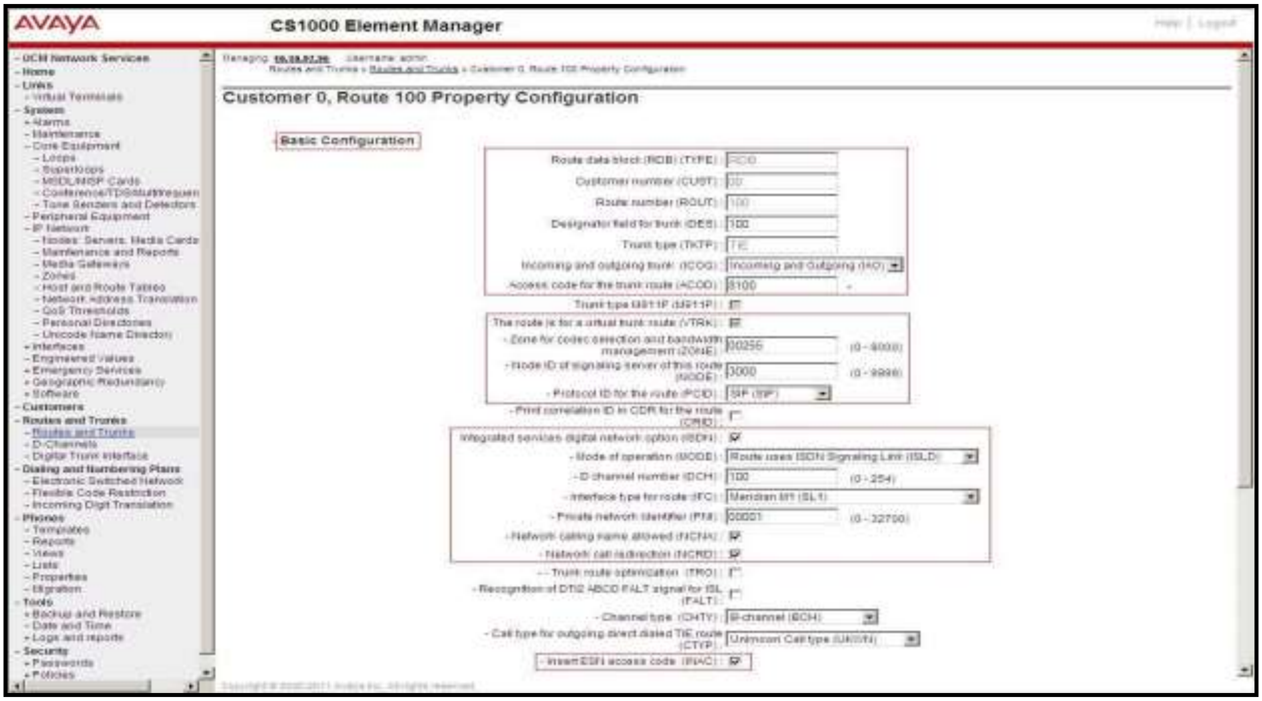
+ Customer: 0 Total routes: 4 Total trunks: 96

**Figure 29 – 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 30**.

- **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 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 5.6.1**).

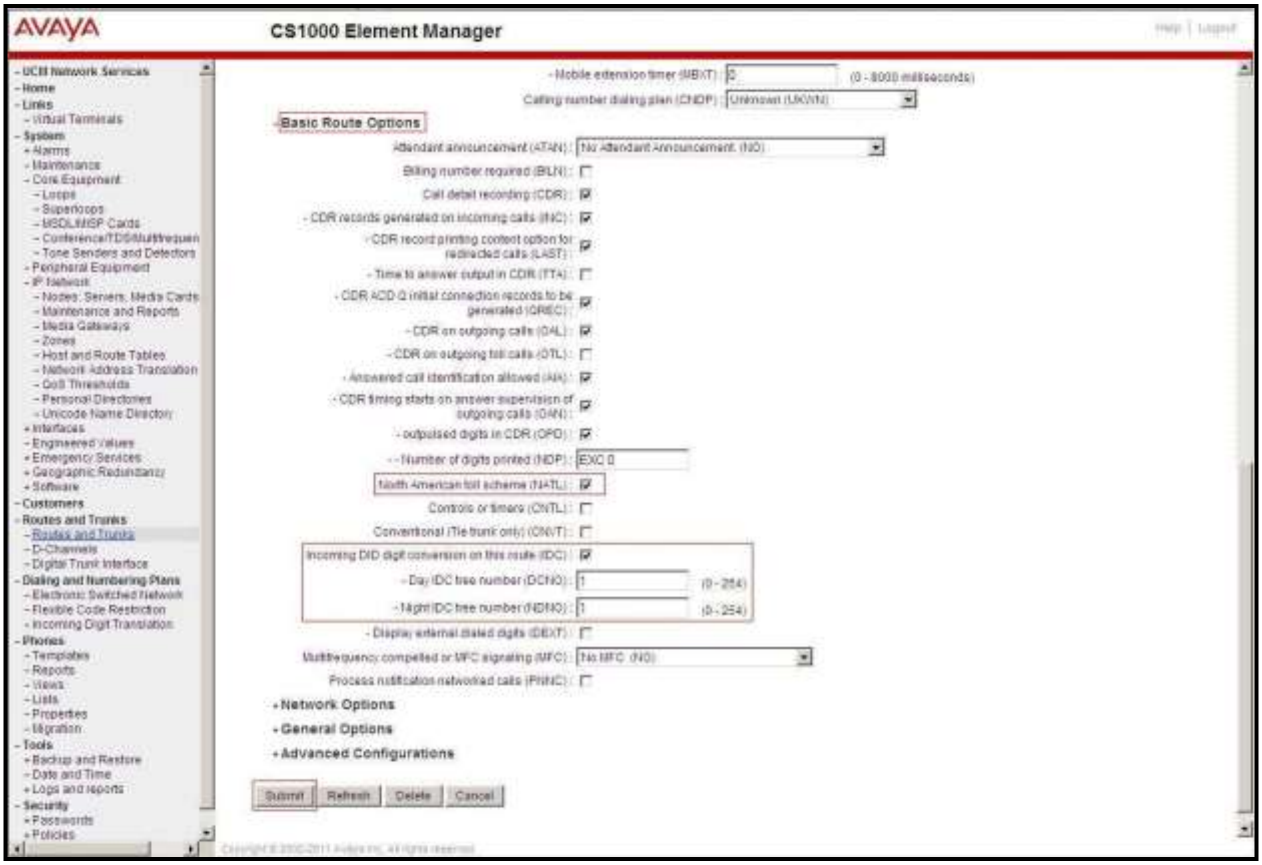


Customer 0, Route 100 Property Configuration

Route data block (RDB) (TYPE): RDB
Customer number (CUST): 00
Route number (ROUT): 100
Designator field for trunk (DES): 100
Trunk type (TKTP): TIE
Incoming and outgoing trunk (ICOG): Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD): 8100
Trunk type M911P (M911P): □
The route is for a virtual trunk route (VTRK): ☑
- Zone for codec selection and bandwidth management (ZONE): 00255 (0 - 8000)
- Node ID of signaling server of this route (NODE): 3000 (0 - 9999)
- Protocol ID for the route (PCID): SIP (SIP)
- Print correlation ID in CDR for the route (CRID): □
Integrated services digital network option (ISDN): ☑
- Mode of operation (MODE): Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH): 100 (0 - 254)
- Interface type for route (IFC): Meridian M1 (SL1)
- Private network identifier (PNI): 00001 (0 - 32700)
- Network calling name allowed (NCNA): ☑
- Network call redirection (NCRD): ☑
- - Trunk route optimization (TRO): □
- Recognition of DTI2 ABCD FALT signal for ISL (FALT): □
- Channel type (CHTY): B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP): Unknown Call type (UKWN)
- Insert ESN access code (INAC): ☑

**Figure 30 – 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 31**. Click on the **Submit** button.



- Mobile extension timer (MBXT) : 0 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP) : Unknown (UKWN)

- Basic Route Options

Attendant announcement (ATAN) : No Attendant Announcement. (NO)
Billing number required (BLN) : □
Call detail recording (CDR) : ☑
- CDR records generated on incoming calls (INC) : ☑
- CDR record printing content option for redirected calls (LAST) : ☑
- Time to answer output in CDR (TTA) : □
- CDR ACD-Q initial connection records to be generated (QREC) : ☑
- CDR on outgoing calls (OAL) : ☑
- CDR on outgoing toll calls (OTL) : □
- Answered call identification allowed (AIA) : ☑
- CDR timing starts on answer supervision of outgoing calls (OAN) : ☑
- outpulsed digits in CDR (OPD) : ☑
- - Number of digits printed (NDP) : EXC 0
North American toll scheme (NATL) : ☑
Controls or timers (CNTL) : □
Conventional (Tie trunk only) (CNVT) : □
Incoming DID digit conversion on this route (IDC) : ☑
- Day IDC tree number (DCNO) : 1 (0 - 254)
- Night IDC tree number (NDNO) : 1 (0 - 254)
- Display external dialed digits (DEXT) : □
Multifrequency compelled or MFC signaling (MFC) : No MFC (NO)
Process notification networked calls (PNNC) : □

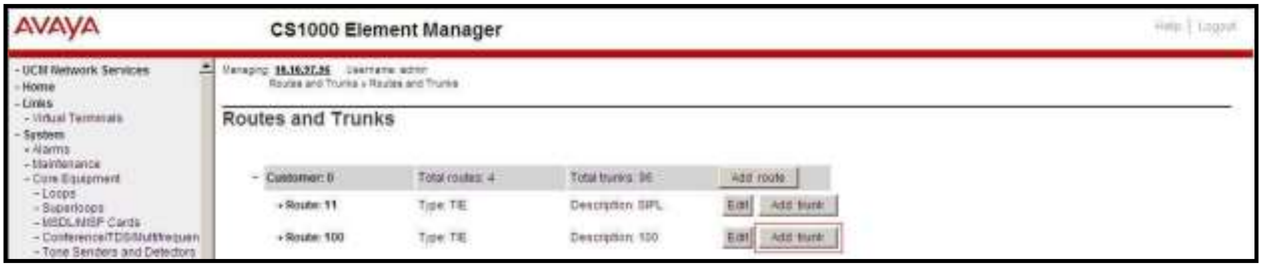
+ Network Options
+ General Options
+ Advanced Configurations

Submit | Refresh | Delete | Cancel

**Figure 31 – 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 32**.



Managing: 10.10.97.96 Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

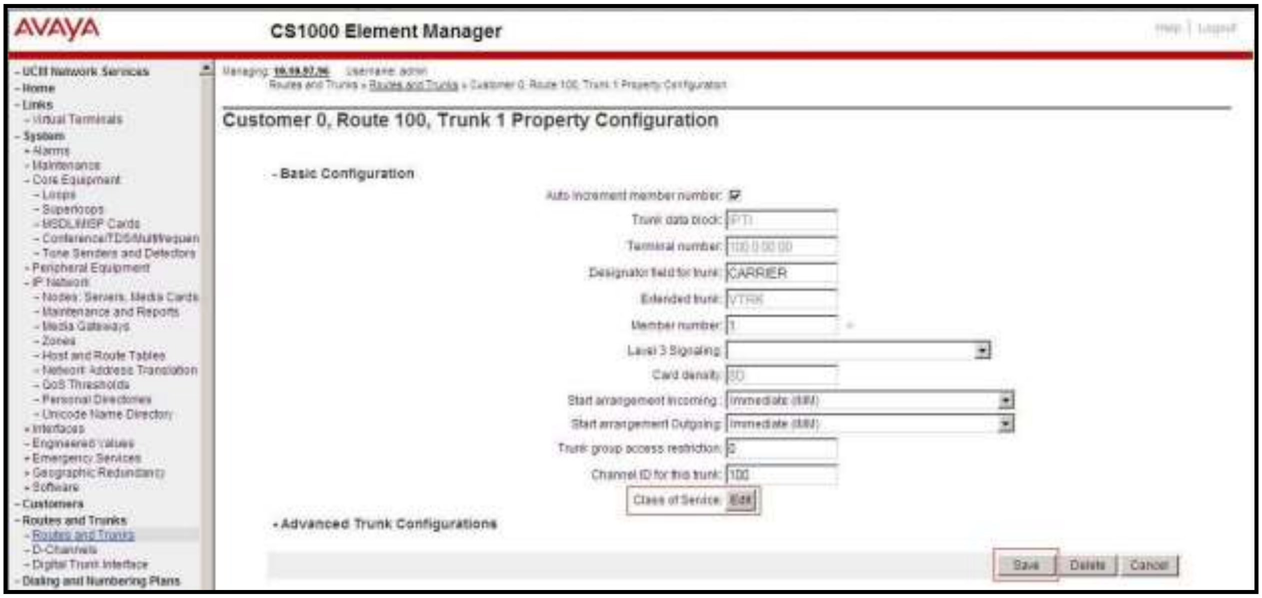
- Customer: 0 | Total routes: 4 | Total trunks: 96 | Add route
+ Route: 11 | Type: TIE | Description: SIPL | Edit | Add trunk
+ Route: 100 | Type: TIE | Description: 100 | Edit | Add trunk

**Figure 32 – 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 33**.

**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.



Customer 0, Route 100, Trunk 1 Property Configuration

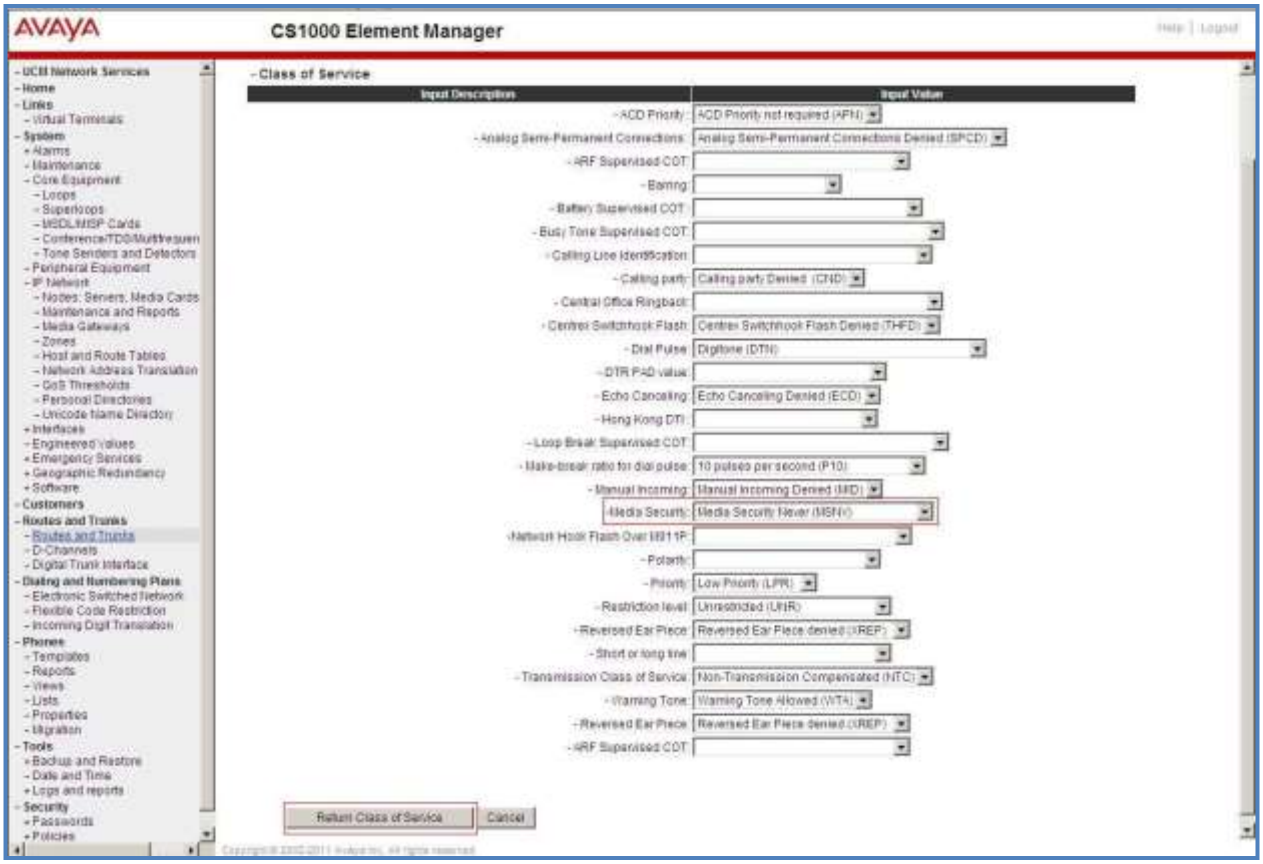
- Basic Configuration

Auto increment member number: ☑
Trunk data block: IPTI
Terminal number: 100 0 00 00
Designator field for trunk: CARRIER
Extended trunk: VTRK
Member number: 1
Level 3 Signaling:
Card density: 8D
Start arrangement Incoming: Immediate (IMM)
Start arrangement Outgoing: Immediate (IMM)
Trunk group access restriction: 2
Channel ID for this trunk: 100
Class of Service: Edit

+ Advanced Trunk Configurations

Figure 33 – New Trunk Configuration

For **Media Security**, select **Media Security Never** (**MSNV)**. Enter the values for the specified fields as shown in **Figure 34**. Scroll down to the bottom of the screen and click **Return Class of Service** and click on the **Save** button (shown in **Figure 33**).



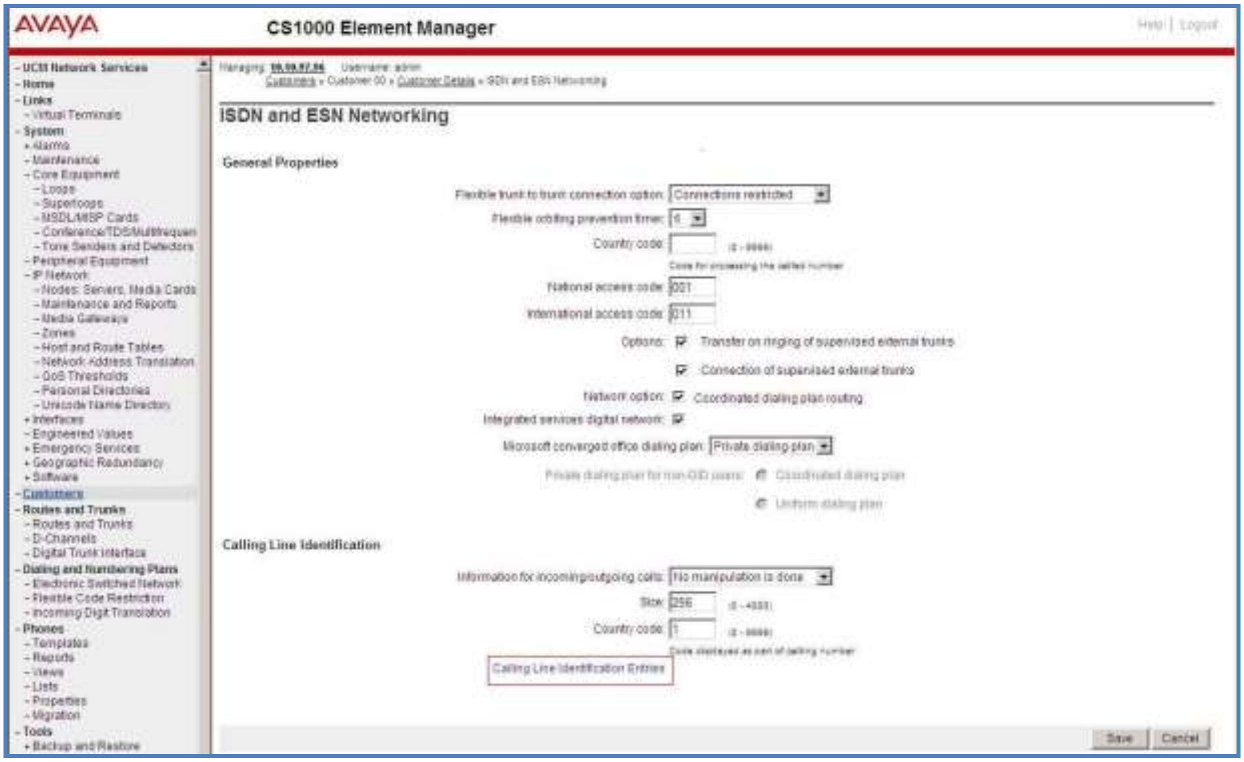
- Class of Service

| 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: | |
| - Busy Tone Supervised COT: | |
| - Calling Line Identification: | |
| - Calling party: | Calling party Denied (CND) |
| - Central Office Ringback: | |
| - Centrex Switchhook Flash: | Centrex Switchhook Flash Denied (THFD) |
| - Dial Pulse: | Digitone (DTN) |
| - DTR PAD value: | |
| - Echo Canceling: | Echo Canceling Denied (ECD) |
| - Hong Kong DTI: | |
| - Loop Break Supervised COT: | |
| - Make-break ratio for dial pulse: | 10 pulses per second (P10) |
| - Manual Incoming: | Manual Incoming Denied (MID) |
| - Media Security: | Media Security Never (MSNV) |
| - Network Hook Flash Over M911P: | |
| - Polarity: | |
| - Priority: | Low Priority (LPR) |
| - Restriction level: | Unrestricted (UNR) |
| - Reversed Ear Piece: | Reversed Ear Piece denied (XREP) |
| - 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 (XREP) |
| - ARF Supervised COT: | |

**Figure 34 – 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 35**.



ISDN and ESN Networking

General Properties

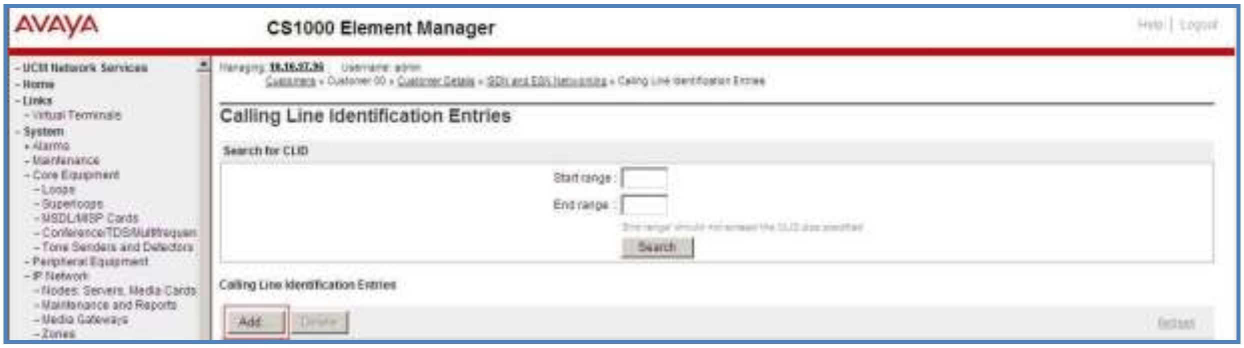
Flexible trunk to trunk connection option: Connections restricted
Flexible orbiting prevention timer: 6
Country code: (0 - 9999)
Code for processing the called number
National access code: 001
International access code: 011
Options: ☑ Transfer on ringing of supervised external trunks
☑ Connection of supervised external trunks
Network option: ☑ Coordinated dialing plan routing
Integrated services digital network: ☑
Microsoft converged office dialing plan: Private dialing plan
Private dialing plan for non-DID users: ● Coordinated dialing plan
● Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls: No manipulation is done
Size: 256 (0 - 4000)
Country code: 1 (0 - 9999)
Code displayed as part of calling number
Calling Line Identification Entries

**Figure 35 – ISDN and ESN Networking**

Click on **Add** as shown in **Figure 36**.


AVAYA
CS1000 Element Manager
Help | Logout
Managing: 10.10.97.96 Username: admin
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
- Core Equipment
- Loops
- Superloops
- MSDL/MISP Cards
- Conference/TDS/Multifrequen
- Tone Senders and Detectors
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
Search
Add
Delete
Refresh

Calling Line Identification Entries

Search for CLID

Start range :
End range :

Calling Line Identification Entries

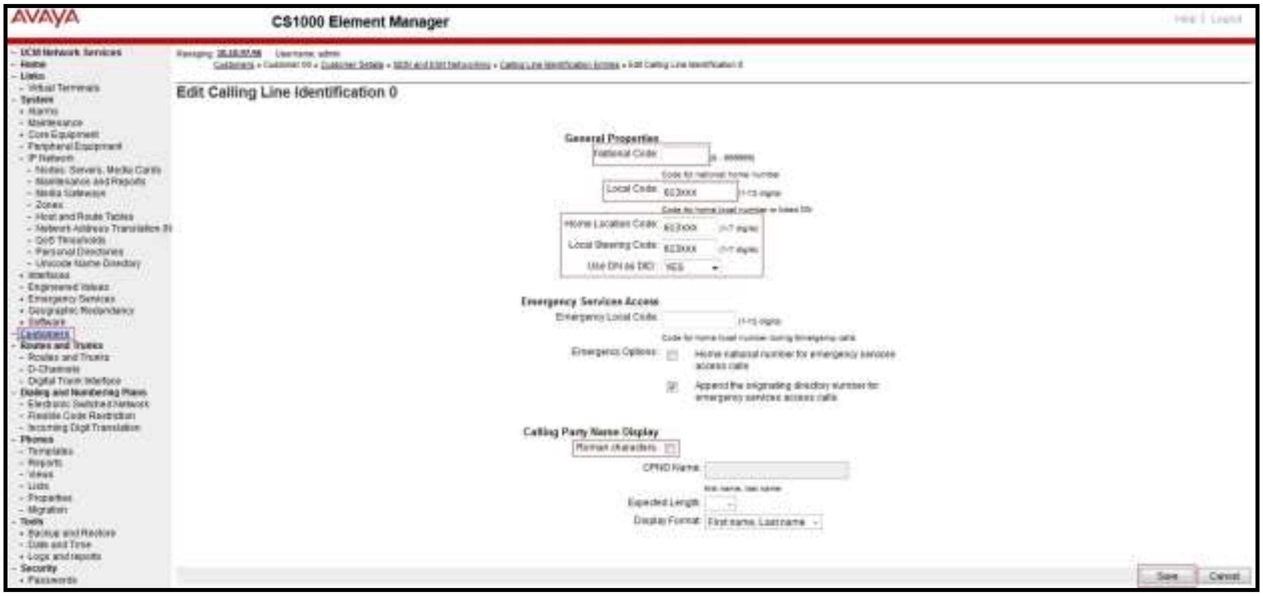
**Figure 36 – Calling Line Identification Entries**

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 37**.

- **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 37**.



Edit Calling Line Identification 0

General Properties

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

Local Code: 613XXX (1-12 digits)
Code for home local number or listed DN

Home Location Code: 613XXX (1-7 digits)
Local Steering Code: 613XXX (1-7 digits)
Use DN as DID: YES

Emergency Services Access

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

Emergency Options: □ Home national number for emergency services access calls
☑ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters □
CPND Name:
first name, last name
Expected Length:
Display Format: First name, Last name

**Figure 37 – 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

### 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 38**.

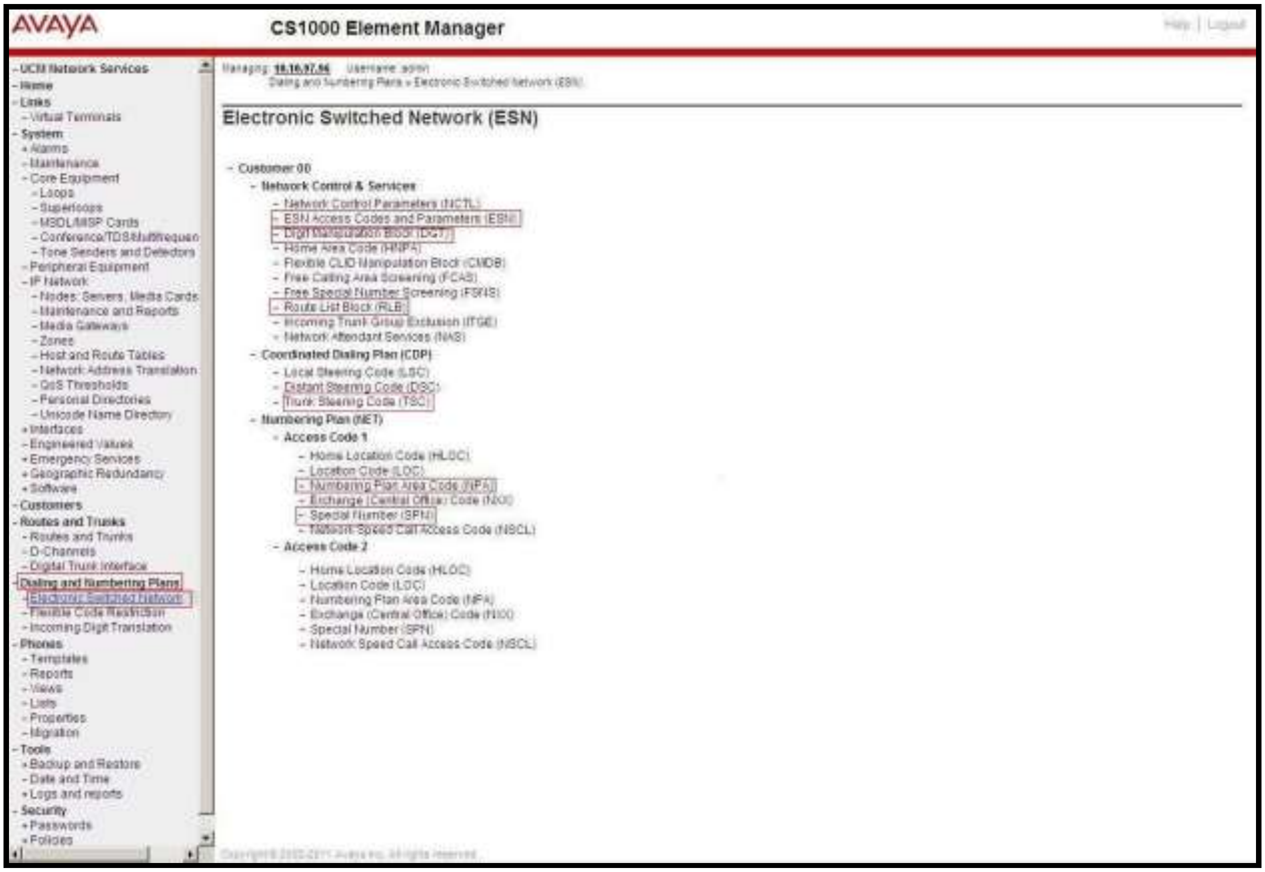
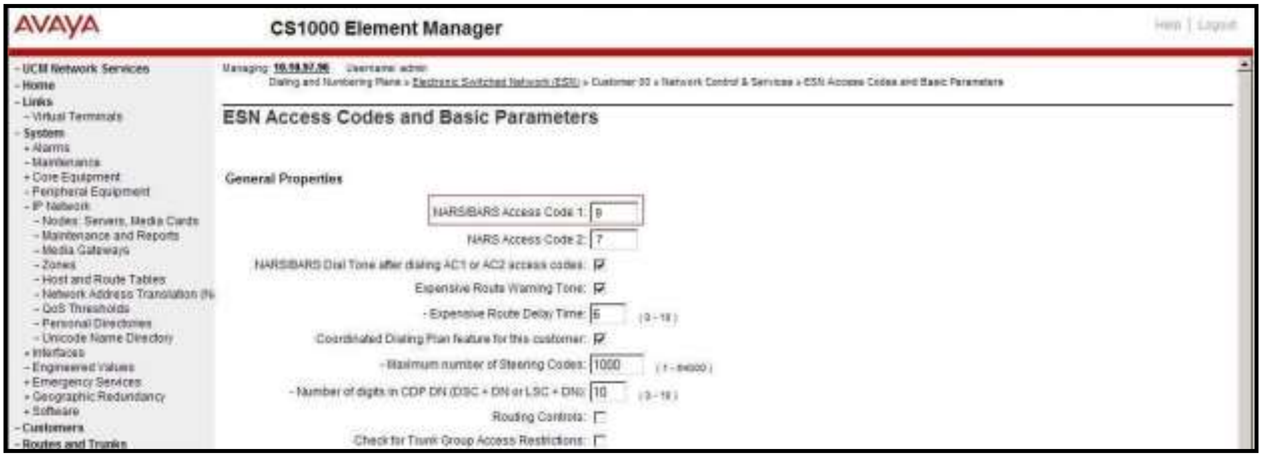

AVAYA
CS1000 Element Manager
Help | Logout
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
- Core Equipment
- Loops
- Superloops
- MSDL/MISP Cards
- Conference/TDS/Multifrequen
- Tone Senders and Detectors
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- 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
- 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
Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN)
Electronic Switched Network (ESN)
- Customer 00
- Network Control & Services
- Network Control Parameters (NCTL)
- ESN Access Codes and Parameters (ESN)
- Digit Manipulation Block (DGT)
- Home Area Code (HNPA)
- Flexible CLID Manipulation Block (CMDB)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)
- Coordinated Dialing Plan (CDP)
- Local Steering Code (LSC)
- Distant Steering Code (DSC)
- Trunk Steering Code (TSC)
- Numbering Plan (NET)
- Access Code 1
- Home Location Code (HLOC)
- Location Code (LOC)
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)
- Access Code 2
- Home Location Code (HLOC)
- Location Code (LOC)
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)
Copyright © 2002-2011 Avaya Inc. All rights reserved.

**Figure 38 – 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 39**.

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



Managing: 10.10.97.98 Username: admin

Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » ESN Access Codes and Basic Parameters

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1: 9
NARS Access Code 2: 7
NARS/BARS Dial Tone after dialing AC1 or AC2 access codes: ☑
Expensive Route Warning Tone: ☑
- Expensive Route Delay Time: 6 (0 - 10)
Coordinated Dialing Plan feature for this customer: ☑
- Maximum number of Steering Codes: 1000 (1 - 64000)
- Number of digits in CDP DN (DSC + DN or LSC + DN): 10 (3 - 10)
Routing Controls: □
Check for Trunk Group Access Restrictions: □

**Figure 39 – 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
…
```

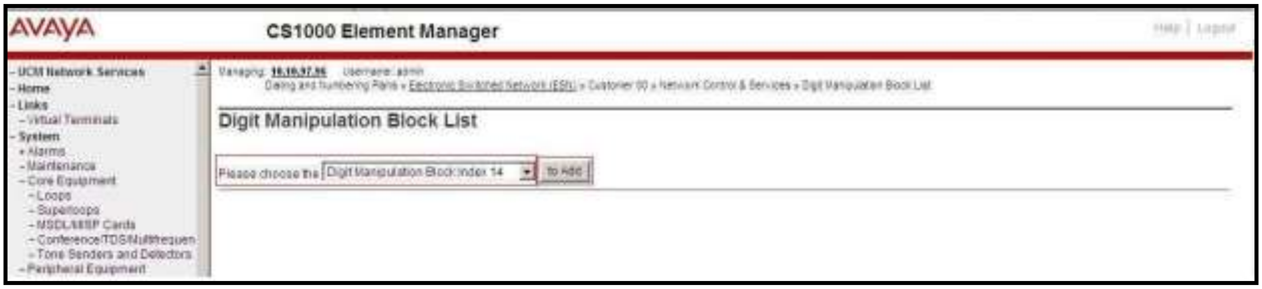
Verify Customer Net Data block by using **ld 21**.

```
>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 38 in Section 5.6.1**. Select **Digit Manipulation Block (DGT)**. The **Digit Manipulation Block List** is displayed as shown in **Figure 40**. 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.



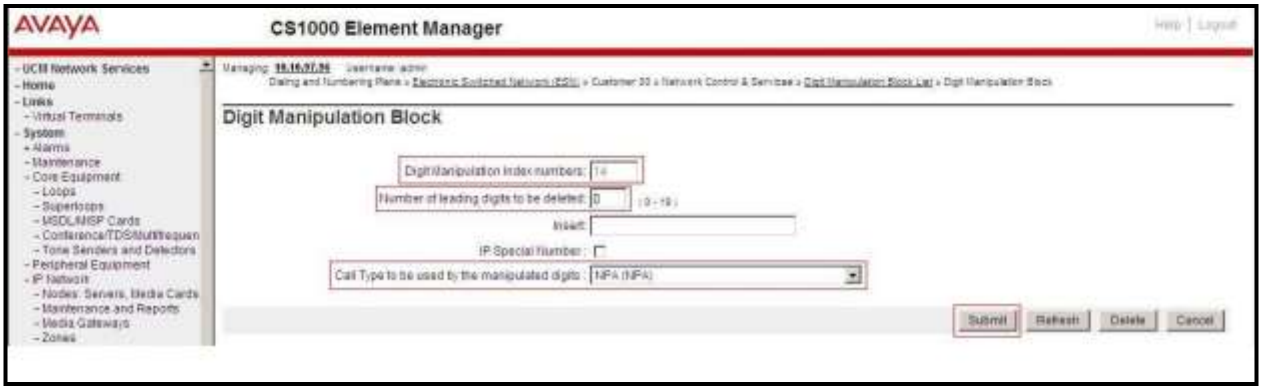
Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List

Digit Manipulation Block List

Please choose the Digit Manipulation Block Index 14 [to Add]

**Figure 40 – 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 41**.


AVAYA
CS1000 Element Manager
Help | Logout
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
- Core Equipment
- Loops
- Superloops
- MSDL/MISP Cards
- Conference/TDS/Multifrequen
- Tone Senders and Detectors
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block
Submit
Refresh
Delete
Cancel

Digit Manipulation Block

Digit Manipulation index numbers: 14

Number of leading digits to be deleted: 0 ( 0 - 19 )

Insert:

IP Special Number: □

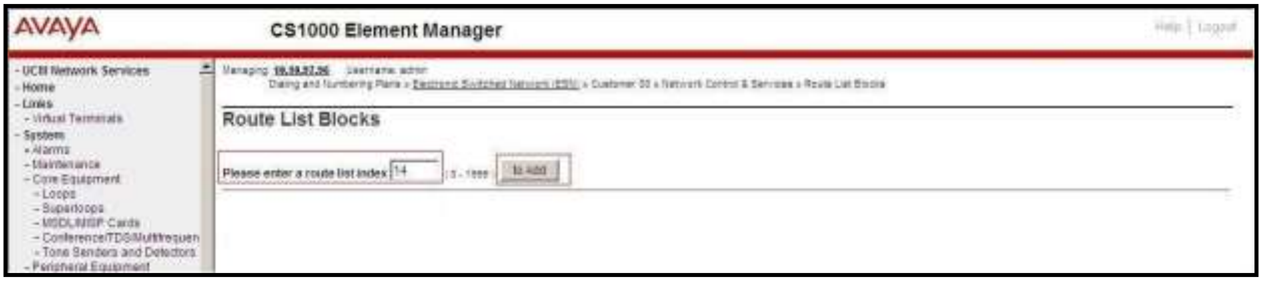
Call Type to be used by the manipulated digits: NPA (NPA)

**Figure 41 – DMI 14 Configuration**

### 5.6.4. Route List Block Index (RLI 14)

This session shows how to add an 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 38** 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 42**. The screen shown in **Figure 43** will open.


AVAYA
CS1000 Element Manager
Help | Logout
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
- Core Equipment
- Loops
- Superloops
- MSDL/MISP Cards
- Conference/TDS/Multifrequen
- Tone Senders and Detectors
- Peripheral Equipment
Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks
to Add

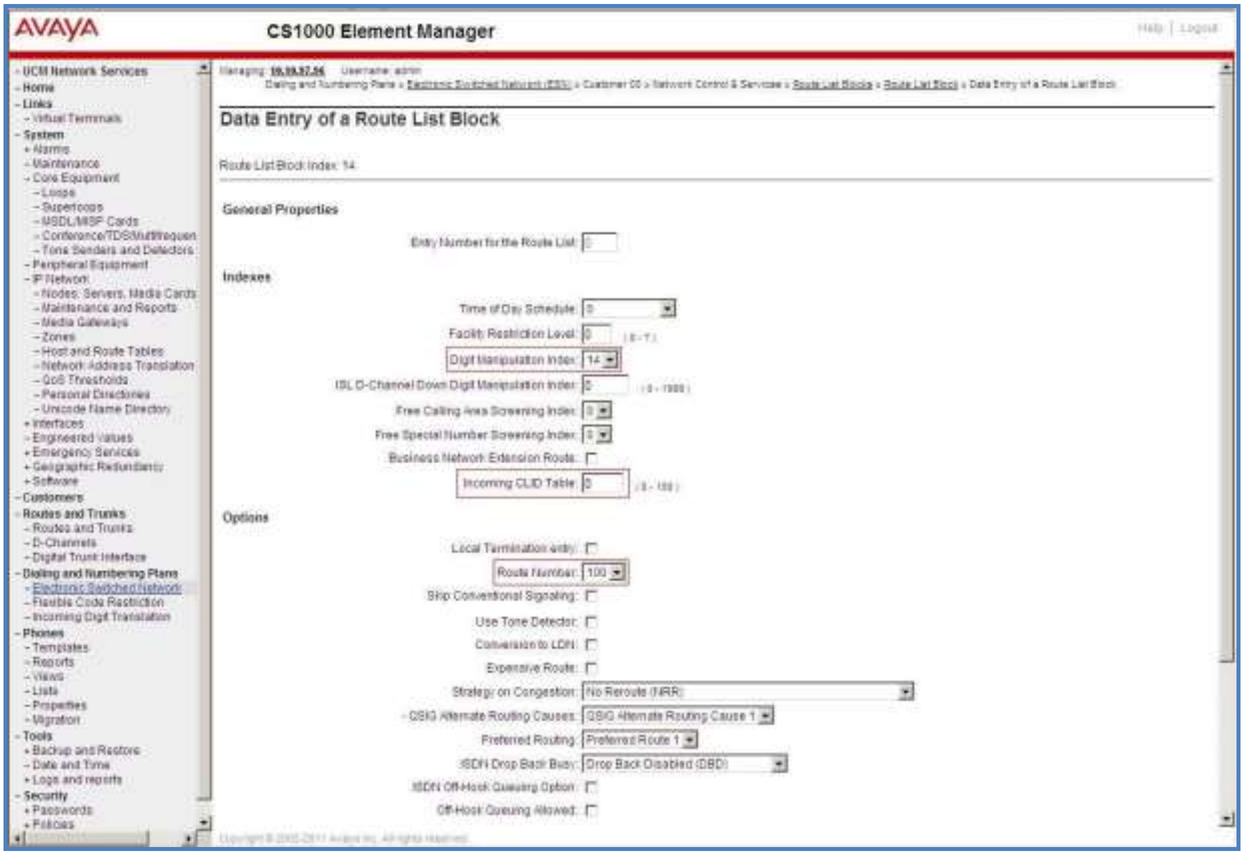
Route List Blocks

Please enter a route list index: 14 ( 0 - 1999 )

**Figure 42 – 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 43**. 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**).



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks » Route List Block » Data Entry of a Route List Block

Data Entry of a Route List Block

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
ISL D-Channel Down Digit Manipulation Index: 0 ( 0 - 1999 )
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: □
Incoming CLID Table: 0 ( 0 - 100 )

Options

Local Termination entry: □
Route Number: 100
Skip Conventional Signaling: □
Use Tone Detector: □
Conversion to LDN: □
Expensive Route: □
Strategy on Congestion: No Reroute (NRR)
- QSIG Alternate Routing Causes: QSIG Alternate Routing Cause 1
Preferred Routing: Preferred Route 1
ISDN Drop Back Busy: Drop Back Disabled (DBD)
ISDN Off-Hook Queuing Option: □
Off-Hook Queuing Allowed: □

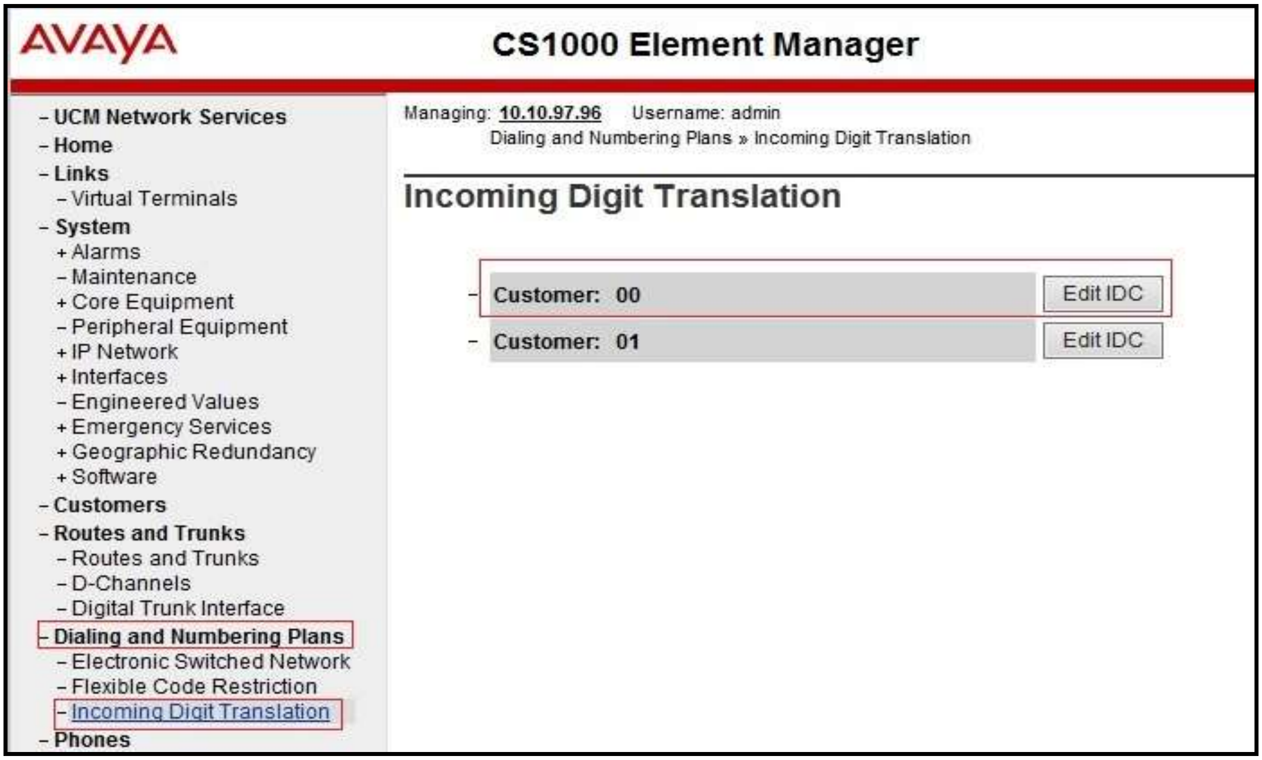
Copyright © 2002-2011 Avaya Inc. All rights reserved.

**Figure 43 – 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 44**.



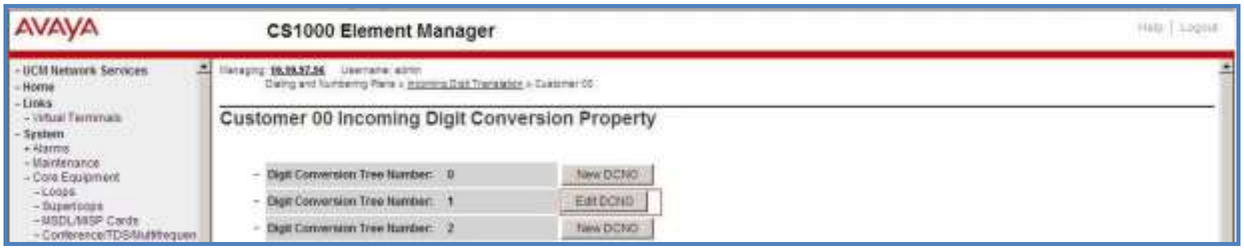
Managing: 10.10.97.96 Username: admin

Incoming Digit Translation

- Customer: 00
- Customer: 01

**Figure 44 – 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 45**.



Managing: 10.10.97.96 Username: admin

Customer 00 Incoming Digit Conversion Property

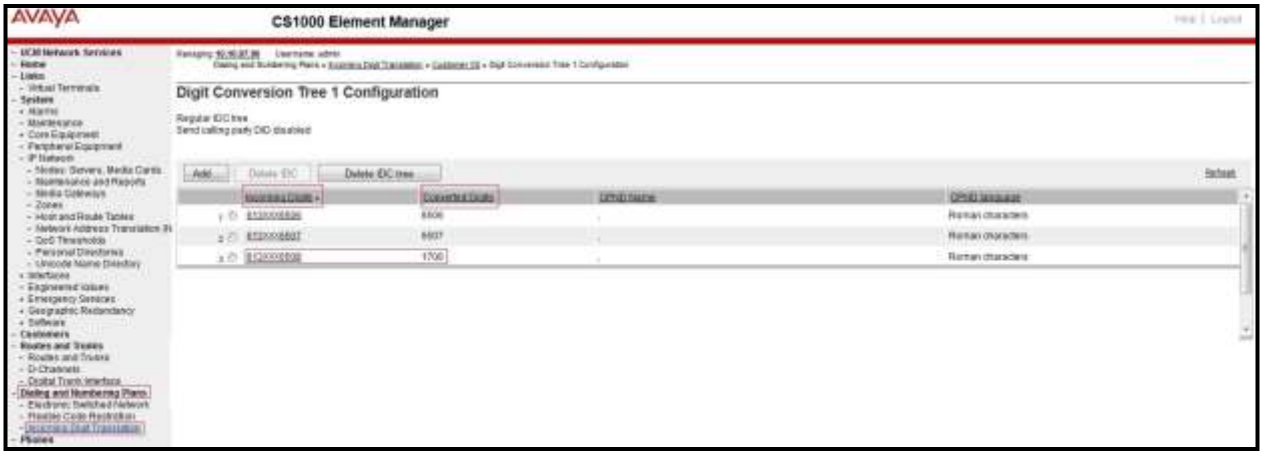
- Digit Conversion Tree Number: 0
- Digit Conversion Tree Number: 1
- Digit Conversion Tree Number: 2

**Figure 45 – Incoming Digit Conversion Property**

Detailed configuration of the Digit Conversion Tree Configuration is shown in **Figure 46**. 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 31** 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.



Managing: 10.10.97.98 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 1 Configuration

Digit Conversion Tree 1 Configuration

Regular IDC tree
Send calling party DID disabled

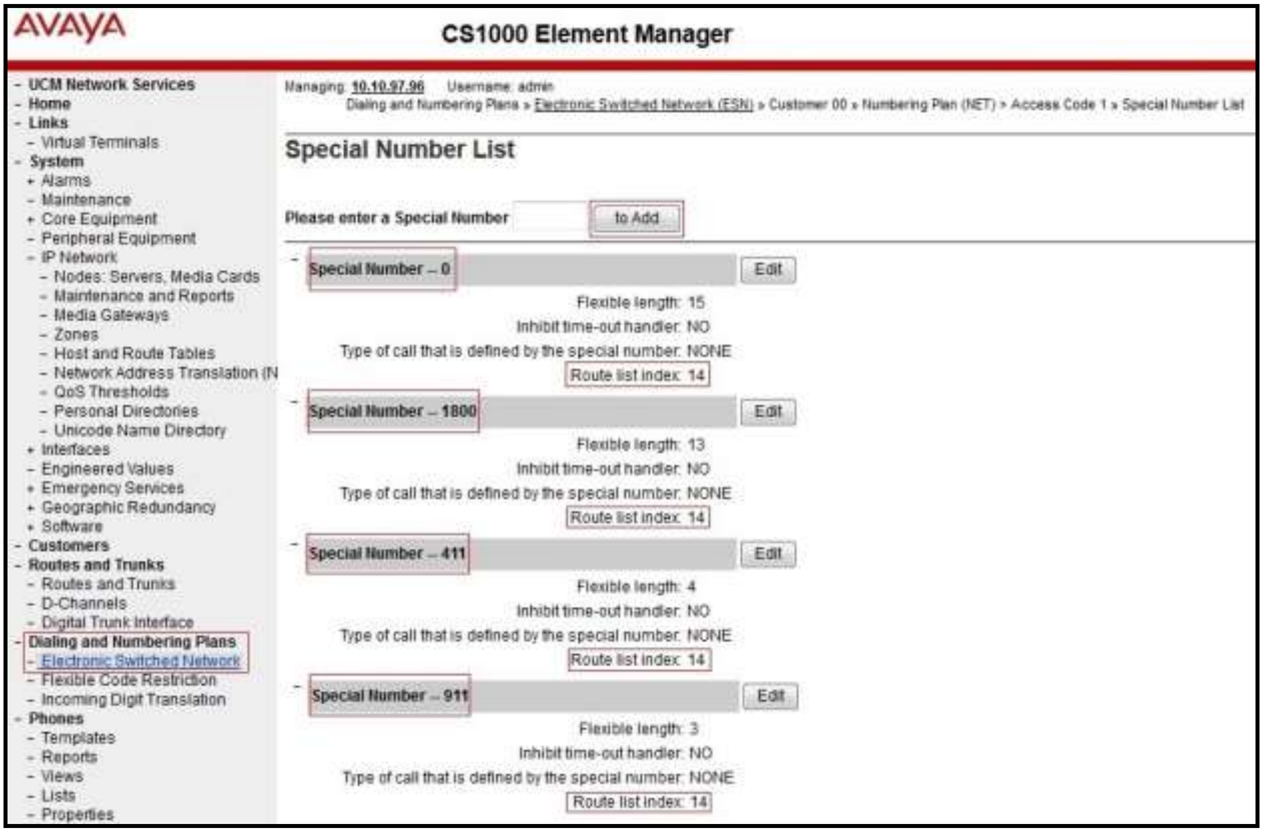
| | Incoming Digits | Converted Digits | CPND Name | CPND language |
|---|---|---|---|---|
| 1 ○ | 613XXX6506 | 6506 | | Roman characters |
| 2 ○ | 613XXX6507 | 6507 | | Roman characters |
| 3 ○ | 613XXX6508 | 1700 | | Roman characters |

**Figure 46 – 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, 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 38** in **Section 5.6.1**. Select **Special Number (SPN)**. Enter a SPN number and then click on the **to Add** button. **Figure 47** shows all the special numbers used for this testing.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Special Number List

Special Number List

Please enter a Special Number

- Special Number – 0
Flexible length: 15
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 14

- Special Number – 1800
Flexible length: 13
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 14

- Special Number – 411
Flexible length: 4
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 14

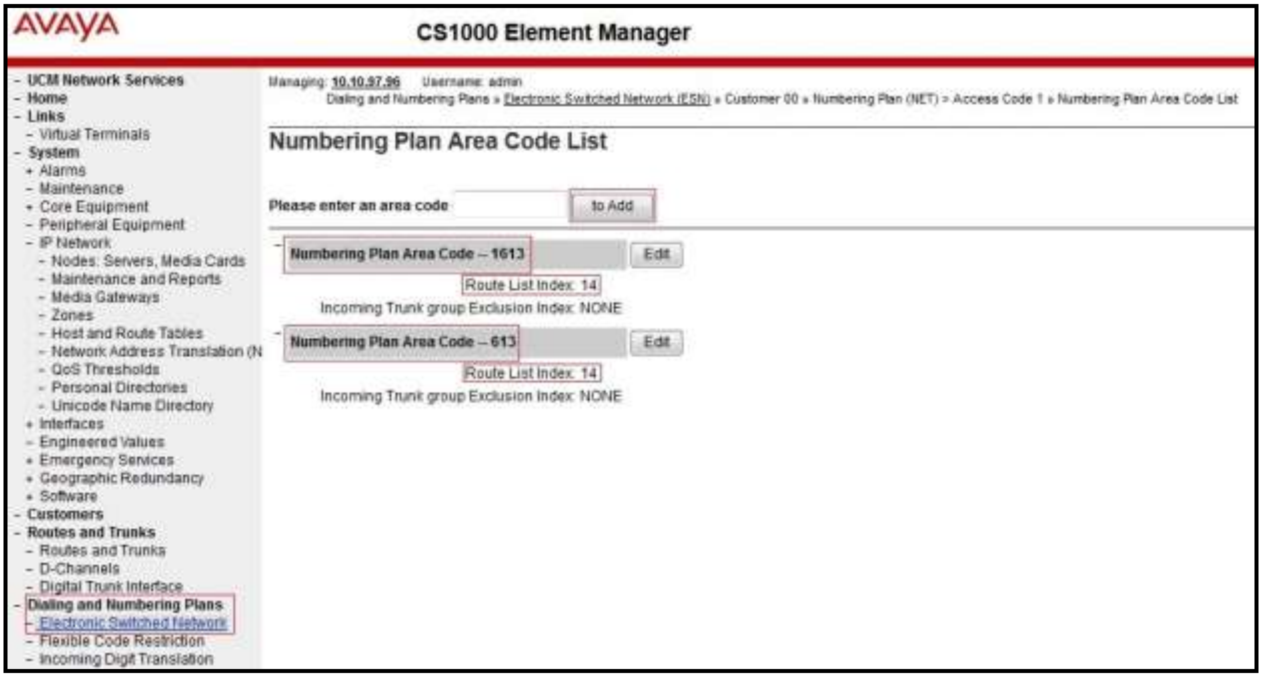
- Special Number – 911
Flexible length: 3
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 14

**Figure 47 – 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 38** 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 48**. These area codes were associated to **Route List Index 14** created in **Section 5.6.4**.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Numbering Plan Area Code List

Numbering Plan Area Code List

Please enter an area code

Numbering Plan Area Code – 1613
Route List Index: 14
Incoming Trunk group Exclusion Index: NONE

Numbering Plan Area Code – 613
Route List Index: 14
Incoming Trunk group Exclusion Index: NONE

**Figure 48 – 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 RCBD
    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 FDSD 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.

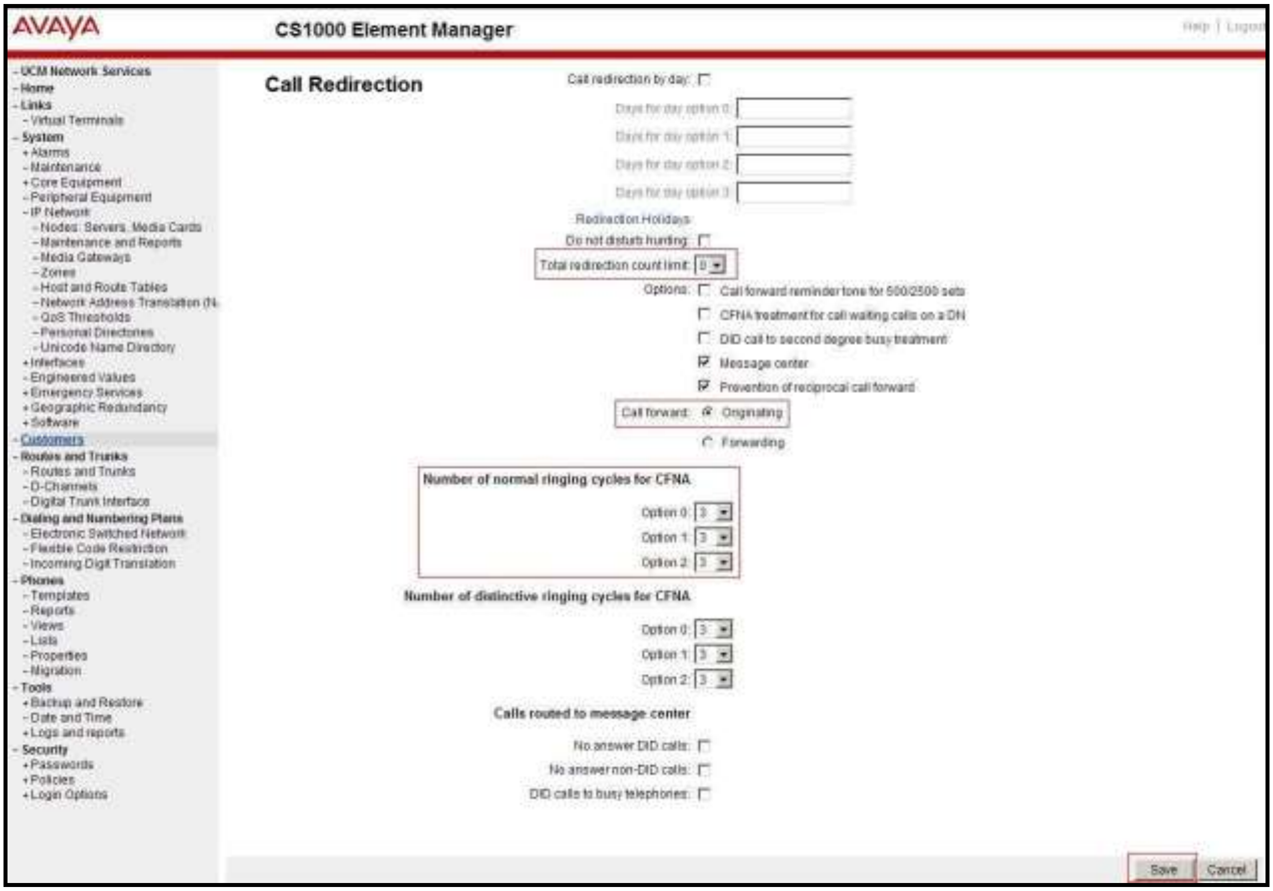
```
>ld 11
REQ: chg
TYPE: 2002p2
TN   96 0 0 2
ECHG yes
ITEM CLS DDGA
…
```

### 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 49**.

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



Call Redirection

Call redirection by day: □

Days for day option 0:

Days for day option 1:

Days for day option 2:

Days for day option 3:

Redirection Holidays

Do not disturb hunting: □

Total redirection count limit: 0

Options: □ 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

☑ Prevention of reciprocal call forward

Call forward: ● Originating

○ Forwarding

Number of normal ringing cycles for CFNA

Option 0: 3

Option 1: 3

Option 2: 3

Number of distinctive ringing cycles for CFNA

Option 0: 3

Option 1: 3

Option 2: 3

Calls routed to message center

No answer DID calls: □

No answer non-DID calls: □

DID calls to busy telephones: □

**Figure 49 – 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 Session Border Controller for Enterprise

This section describes the configuration of Avaya SBCE necessary for interoperability with the CS1000 and Bell Canada SIP Trunk Service.

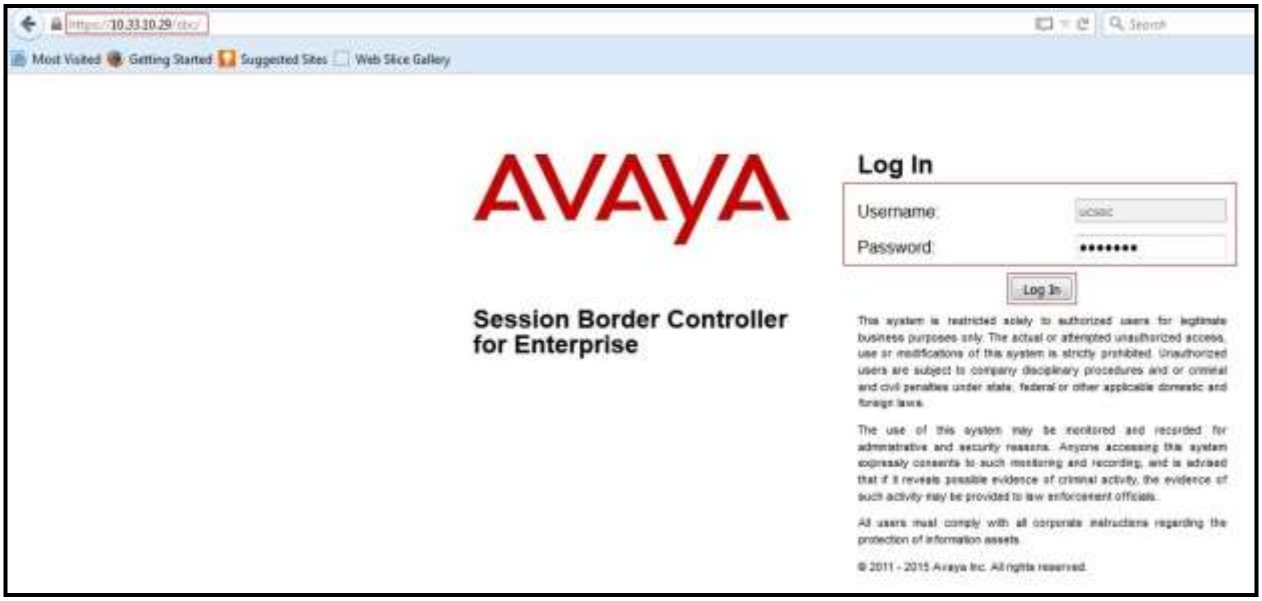
Avaya elements reside on the Private side and the Bell Canada SIP Trunk Service resides on the Public side of the network, as illustrated in **Figure 1**.

**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, see relevant product documentation references in **Section 10** of these Application Notes.

## 6.1. Log in to the SBCE

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**.



https://10.33.10.29/sbc/

Log In

Username: ucsec

Password: ••••••••

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

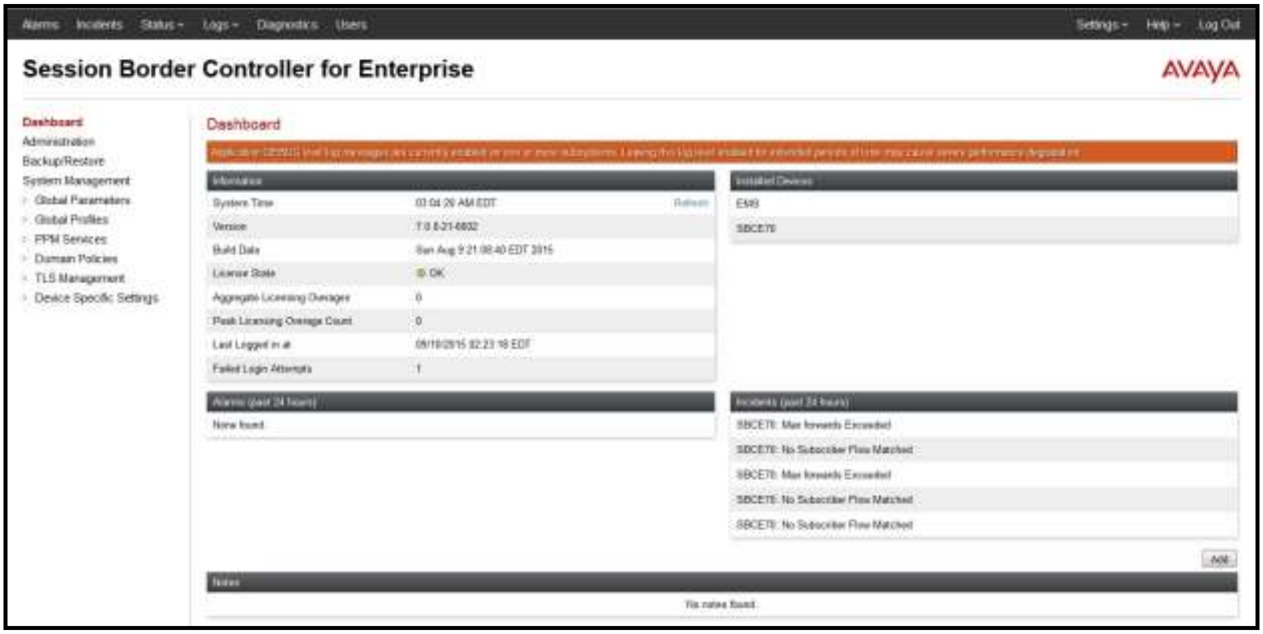
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2015 Avaya Inc. All rights reserved.

**Figure 50 – Avaya SBCE Login**

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



Dashboard

Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving the log level enabled for extended periods of time may cause severe performance degradation.

| Information | |
|---|---|
| System Time | 03:04:26 AM EDT |
| Version | 7.0.0-21-6602 |
| Build Date | Sun Aug 9 21:08:40 EDT 2015 |
| License State | ● OK |
| Aggregate Licensing Overages | 0 |
| Peak Licensing Overage Count | 0 |
| Last Logged in at | 08/10/2015 02:23:18 EDT |
| Failed Login Attempts | 1 |

| Installed Devices |
|---|
| EMS |
| SBCE70 |

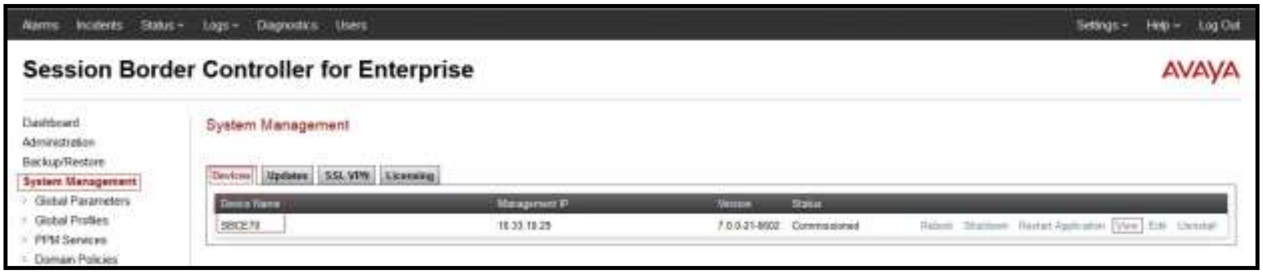
| Alarms (past 24 hours) |
|---|
| None found. |

| Incidents (past 24 hours) |
|---|
| SBCE70: Max forwards Exceeded |
| SBCE70: No Subscriber Flow Matched |
| SBCE70: Max forwards Exceeded |
| SBCE70: No Subscriber Flow Matched |
| SBCE70: No Subscriber Flow Matched |

| Notes |
|---|
| No notes found. |

**Figure 51 - 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.

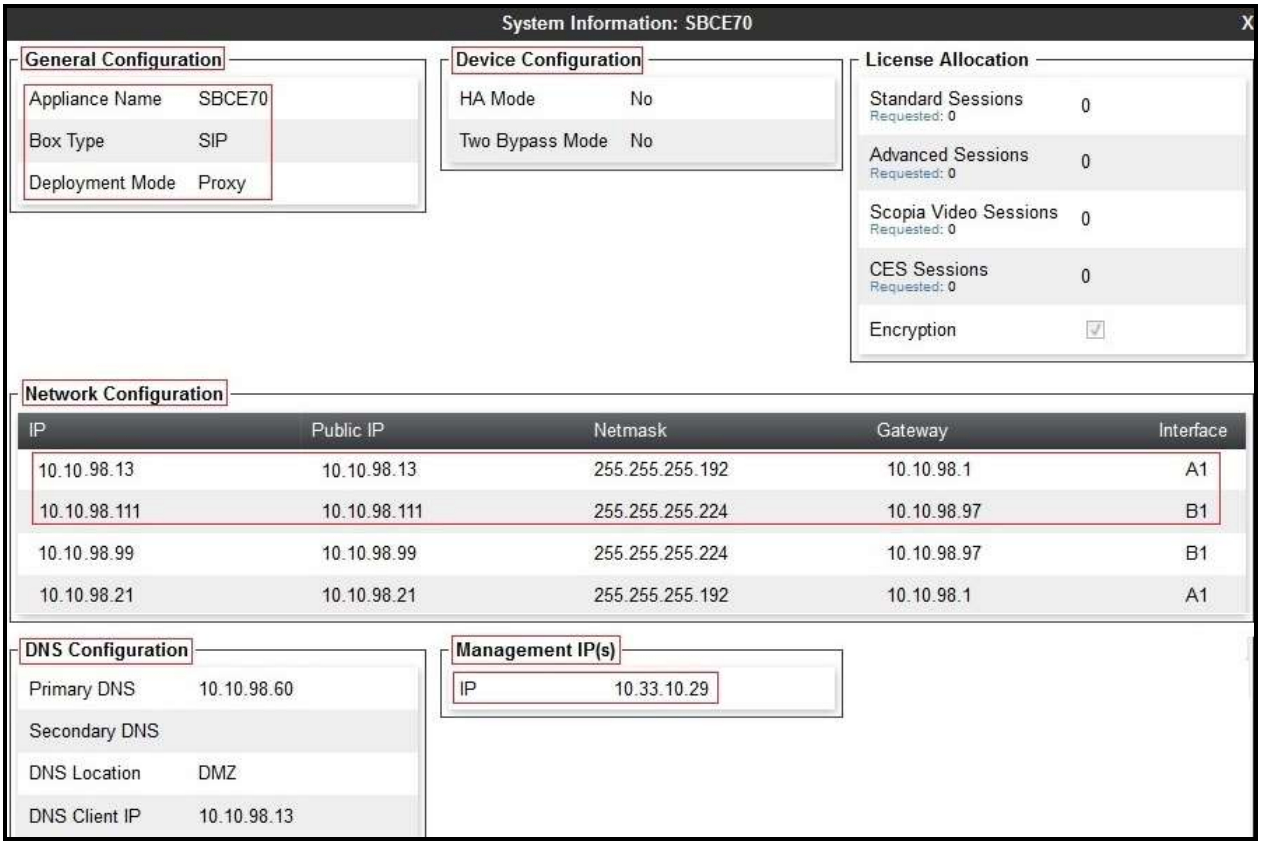


System Management

| Device Name | Management IP | Version | Status | |
|---|---|---|---|---|
| SBCE70 | 10.33.10.25 | 7.0.0-21-6602 | Commissioned | Reboot Shutdown Restart Application View Edit Uninstall |

**Figure 52 - 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 corresponds 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<br>Requested: 0 | 0 |
| Advanced Sessions<br>Requested: 0 | 0 |
| Scopia Video Sessions<br>Requested: 0 | 0 |
| CES Sessions<br>Requested: 0 | 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 53 - Avaya SBCE System Information**

## 6.2. Global Profiles

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

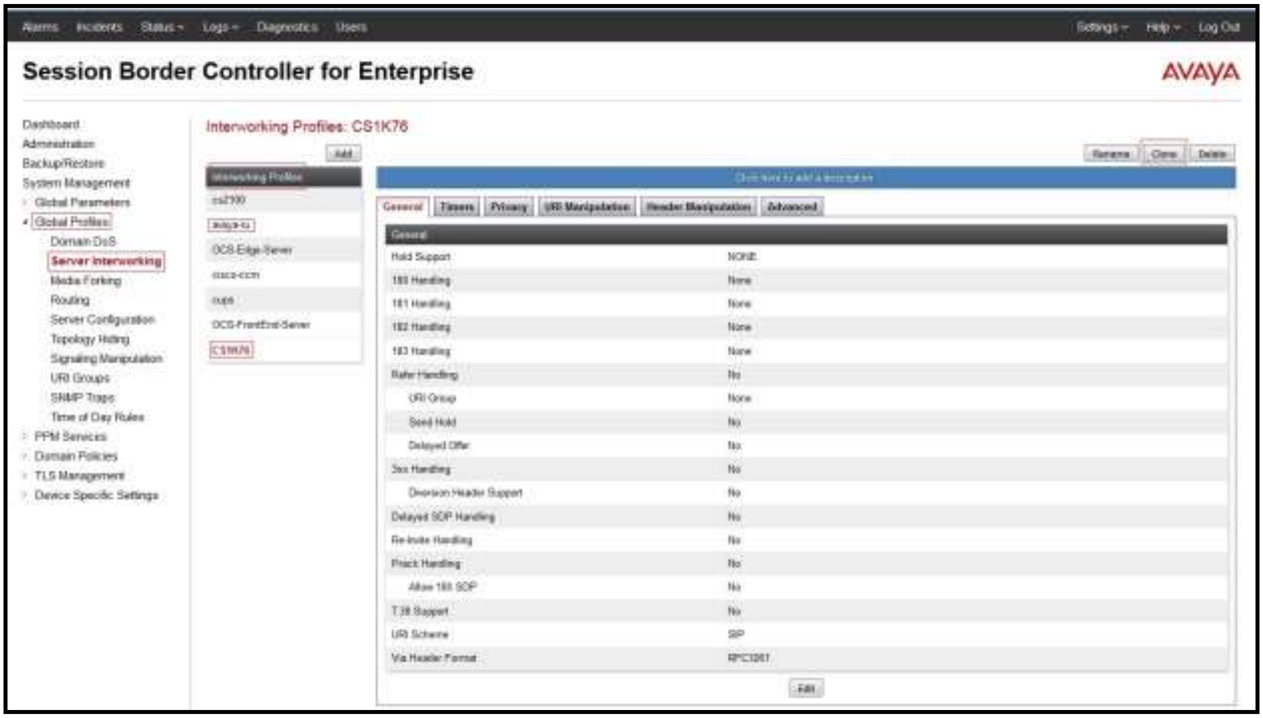
### 6.2.1. Configure Server Interworking Profile - CS1000

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**: **CS1K76** and click **Finish** (not shown).

The following screen shows that CS1000 server interworking profile (named: **CS1K76**) was added.



| General | |
|---|---|
| Hold Support | NONE |
| 180 Handling | None |
| 181 Handling | None |
| 182 Handling | None |
| 183 Handling | None |
| Refer Handling | No |
| URI Group | None |
| Send Hold | No |
| Delayed Offer | No |
| 3xx Handling | No |
| Diversion Header Support | No |
| Delayed SDP Handling | No |
| Re-Invite Handling | No |
| Prack Handling | No |
| Allow 18X SDP | No |
| T.38 Support | No |
| URI Scheme | SIP |
| Via Header Format | RFC3261 |

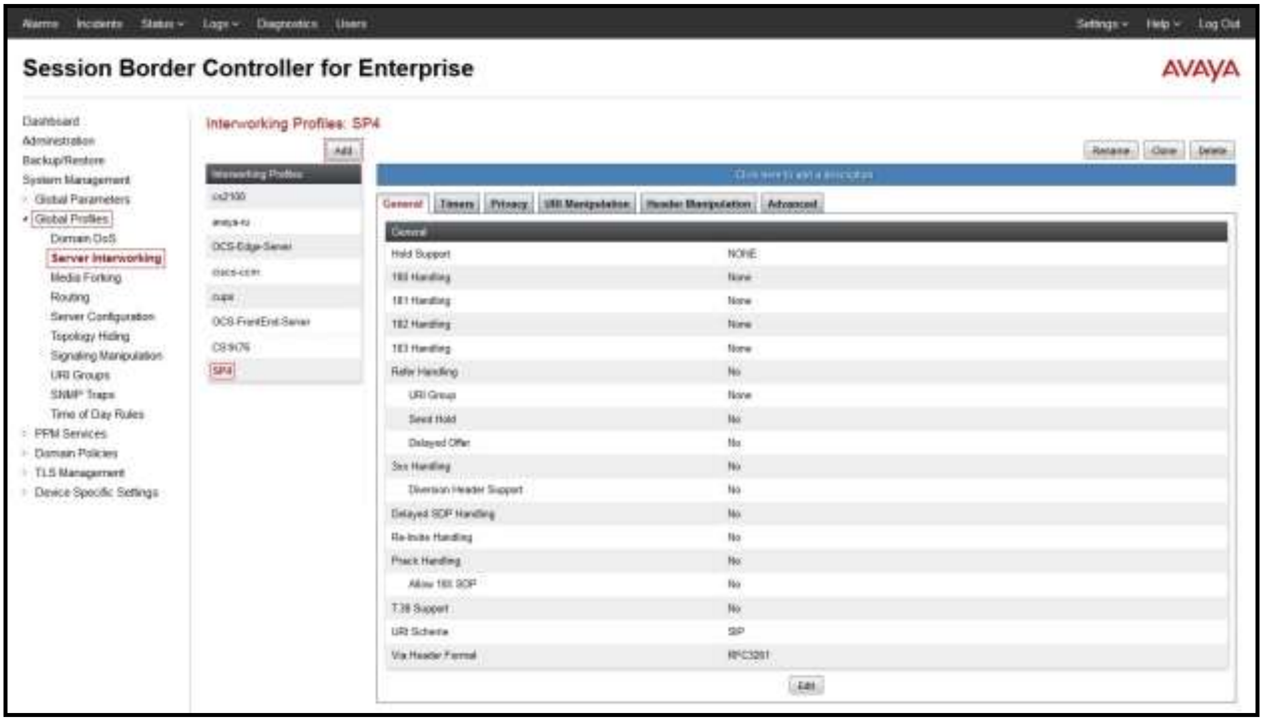
**Figure 54 - Server Interworking – Avaya**

### 6.2.2. 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.

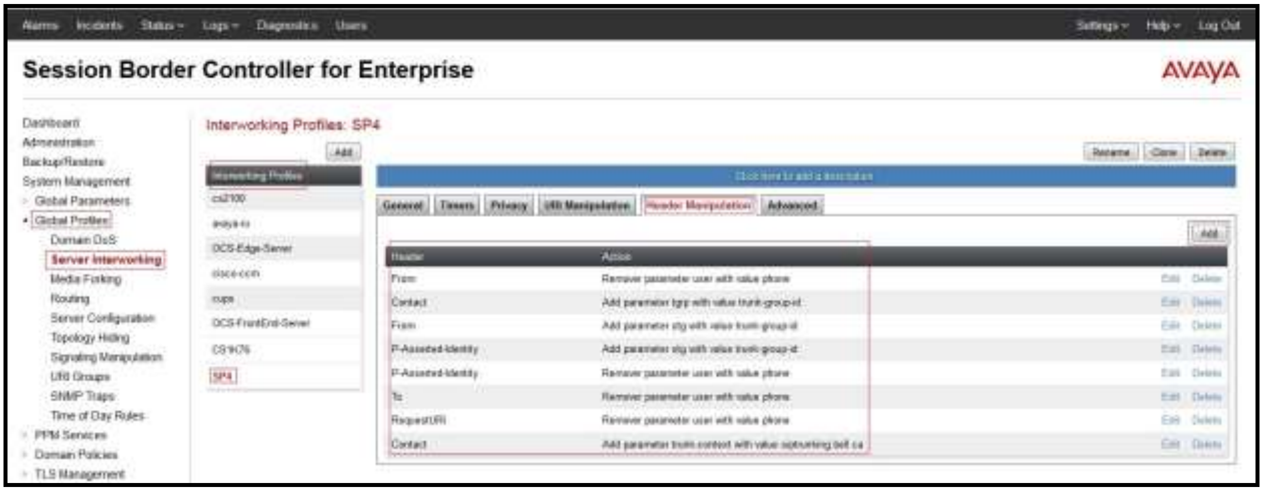


| General | |
|---|---|
| Hold Support | NONE |
| 180 Handling | None |
| 181 Handling | None |
| 182 Handling | None |
| 183 Handling | None |
| Refer Handling | No |
| URI Group | None |
| Send Hold | No |
| Delayed Offer | No |
| 3xx Handling | No |
| Diversion Header Support | No |
| Delayed SDP Handling | No |
| Re-Invite Handling | No |
| Prack Handling | No |
| Allow 18X SDP | No |
| T.38 Support | No |
| URI Scheme | SIP |
| Via Header Format | RFC3261 |

**Figure 55 - Server Interworking – Bell Canada**

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).
    - Remove “user=phone” on P-Asserted-Identity header (This is optional for ONND testing).
    - Remove “user=phone” on To and Request-URI headers.



| Header | Action | | |
|---|---|---|---|
| From | Remove parameter user with value phone | Edit | Delete |
| Contact | Add parameter tgrp with value trunk-group-id | Edit | Delete |
| From | Add parameter otg with value trunk-group-id | Edit | Delete |
| P-Asserted-Identity | Add parameter otg with value trunk-group-id | Edit | Delete |
| P-Asserted-Identity | Remove parameter user with value phone | Edit | Delete |
| To | Remove parameter user with value phone | Edit | Delete |
| Request-URI | Remove parameter user with value phone | Edit | Delete |
| Contact | Add parameter trunk-context with value siptrunking.bell.ca | Edit | Delete |

**Figure 56 - Server Interworking – Bell Canada - 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];tgrp=[trunk-group-id];trunk-context=siptrunking.bell.ca@[CPE/PBX-IP-address].

Bell Canada SIP Trunking Service supports the “otg” header parameter in the “From”, “P-Asserted-Identity” or “Diversion” header. 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 56** in **Section 6.2.2** and **Figure 57** in **Section 6.2.3**). 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 include 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 6.2.9** shows an example of this specific domain setting.

For multi-trunk group and geographic redundant configuration, please refer to document **[9]** in **Section 10**

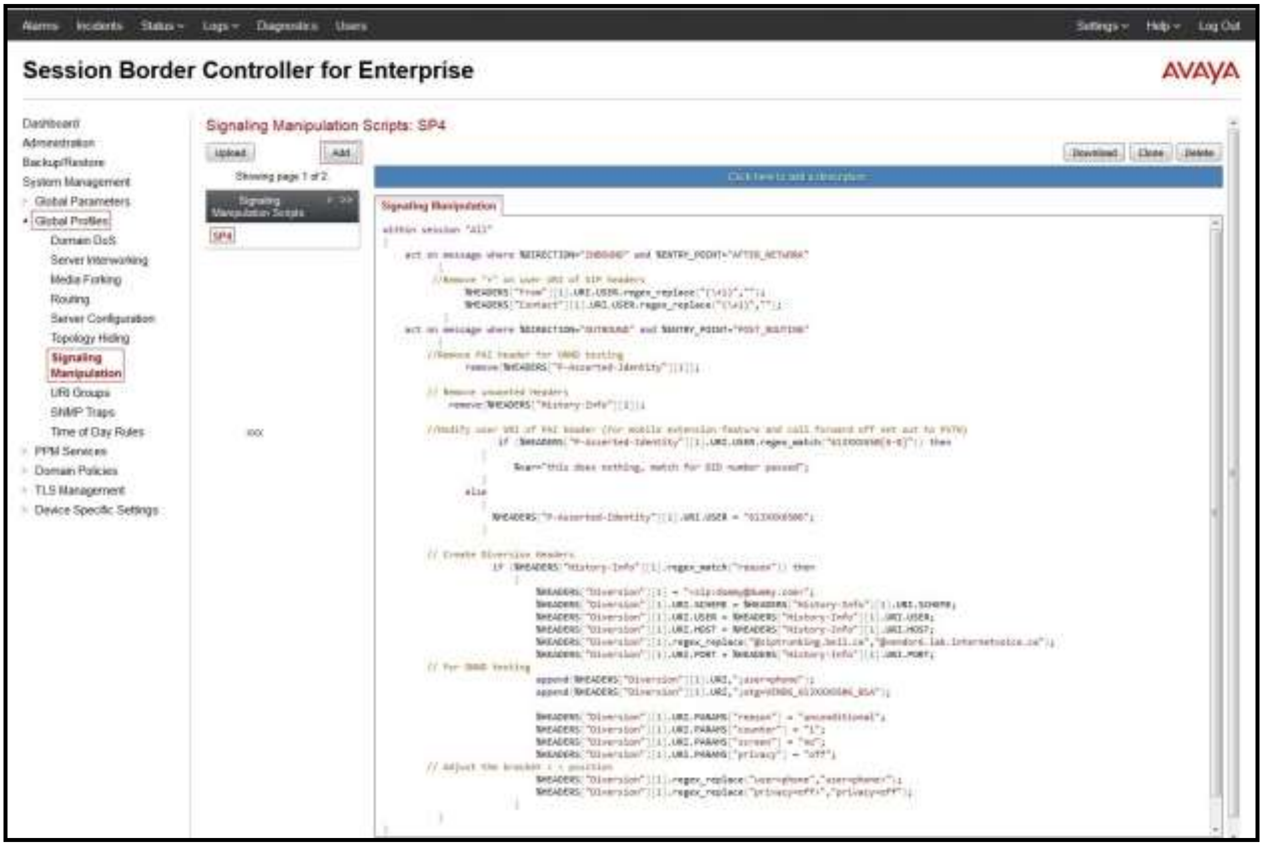
### 6.2.3. Configure Signaling Manipulation

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 on next page 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 processed the off-net call forward, it sends the SIP re-Invite with the From header contained only 10-digit number).
  - 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.
  - Replace History Info header with Diversion header for call forward off-net.
  - Add user=phone and otg on the Diversion header (**Note**: This is optional for ONND testing).
  - Adjust the bracket < > position on the Diversion header syntax.
  - Click **Save** (not shown).

**Note**: See **Appendix A** in **Section 11** for the reference of this signaling manipulation (SigMa) script.



```
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)","");
     }
   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
     {
     //Remove PAI header for VANO testing
           remove(%HEADERS["P-Asserted-Identity"][1]);

     // Remove unwanted Headers
        remove(%HEADERS["History-Info"][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("613XXX6500[0-9]")) then
                {
                   %var="this does nothing, match for DID number passed";
                }
           else
                {
               %HEADERS["P-Asserted-Identity"][1].URI.USER = "613XXX6500";
                }

     // Create Diversion Headers
               if (%HEADERS["History-Info"][1].regex_match("reason")) then
                  {
                      %HEADERS["Diversion"][1] = "<sip:dummy@dummy.com>";
                      %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-Info"][1].URI.SCHEME;
                      %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-Info"][1].URI.USER;
                      %HEADERS["Diversion"][1].URI.HOST = %HEADERS["History-Info"][1].URI.HOST;
                      %HEADERS["Diversion"][1].regex_replace("@siptrunking.bell.ca","@vendors.lab.internetvoice.ca");
                      %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-Info"][1].URI.PORT;
     // For VANO testing
                      append(%HEADERS["Diversion"][1].URI,";user=phone");
                      append(%HEADERS["Diversion"][1].URI,";otg=VENDG_613XXX6500_BSA");

                      %HEADERS["Diversion"][1].URI.PARAMS["reason"] = "unconditional";
                      %HEADERS["Diversion"][1].URI.PARAMS["counter"] = "1";
                      %HEADERS["Diversion"][1].URI.PARAMS["screen"] = "no";
                      %HEADERS["Diversion"][1].URI.PARAMS["privacy"] = "off";
     // Adjust the bracket < > position
                      %HEADERS["Diversion"][1].regex_replace("user=phone","user=phone>");
                      %HEADERS["Diversion"][1].regex_replace("privacy=off>","privacy=off");
                  }
     }
}
```

Figure 57 - Signaling Manipulation

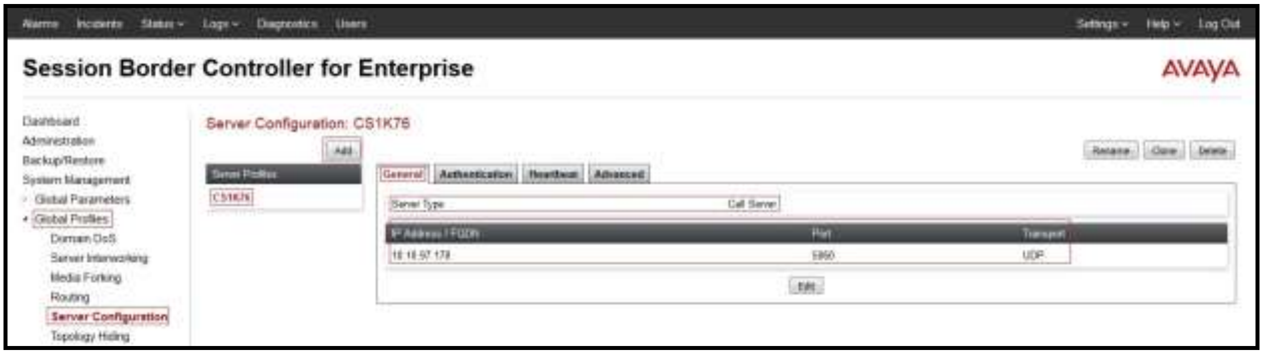
### 6.2.4. Configure Server – CS1000

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**: **CS1K76**.
On **General** tab, enter the following:

- **Server Type**: Select **Call Server**.
- **IP Address/FQDN**: **10.10.97.178** (Avaya CS1000 Node IP Address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).



Server Configuration: CS1K76

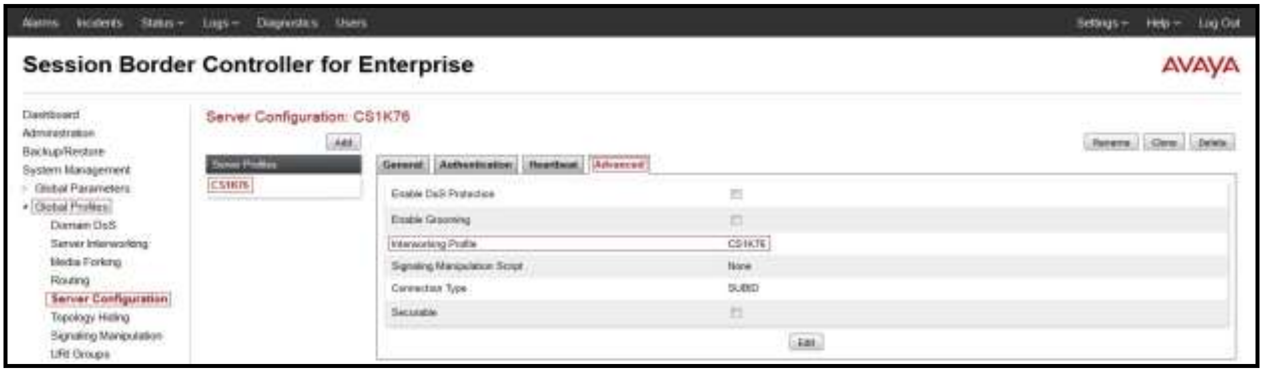
| | |
|---|---|
| Server Type | Call Server |

| IP Address / FQDN | Port | Transport |
|---|---|---|
| 10.10.97.178 | 5060 | UDP |

**Figure 58 - Server Configuration – General - CS1000**

On the **Advanced** tab:

- Select **CS1K76** for **Interworking Profile** (see **Section 6.2.1**).
- Click **Finish** (not shown).



Server Configuration: CS1K76

| | |
|---|---|
| Enable DoS Protection | □ |
| Enable Grooming | □ |
| Interworking Profile | CS1K76 |
| Signaling Manipulation Script | None |
| Connection Type | SUBID |
| Securable | □ |

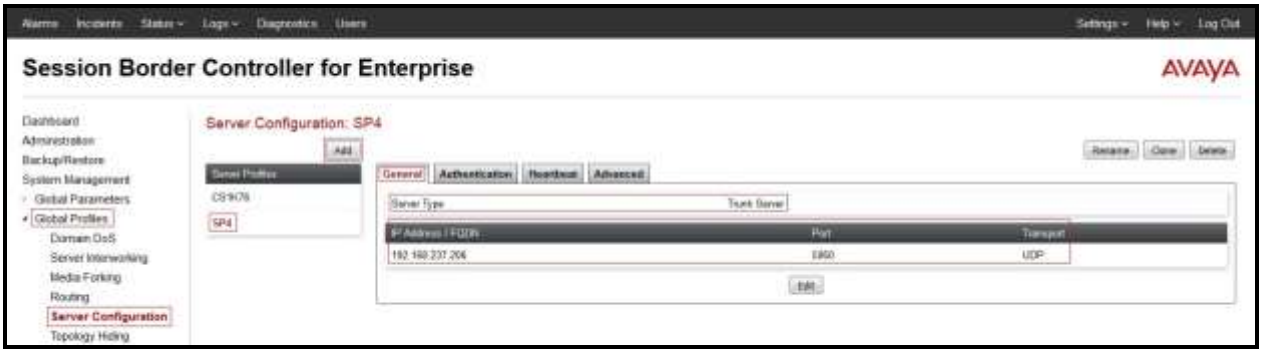
**Figure 59 - Server Configuration – Advanced - Avaya**

### 6.2.5. 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).



Server Configuration: SP4

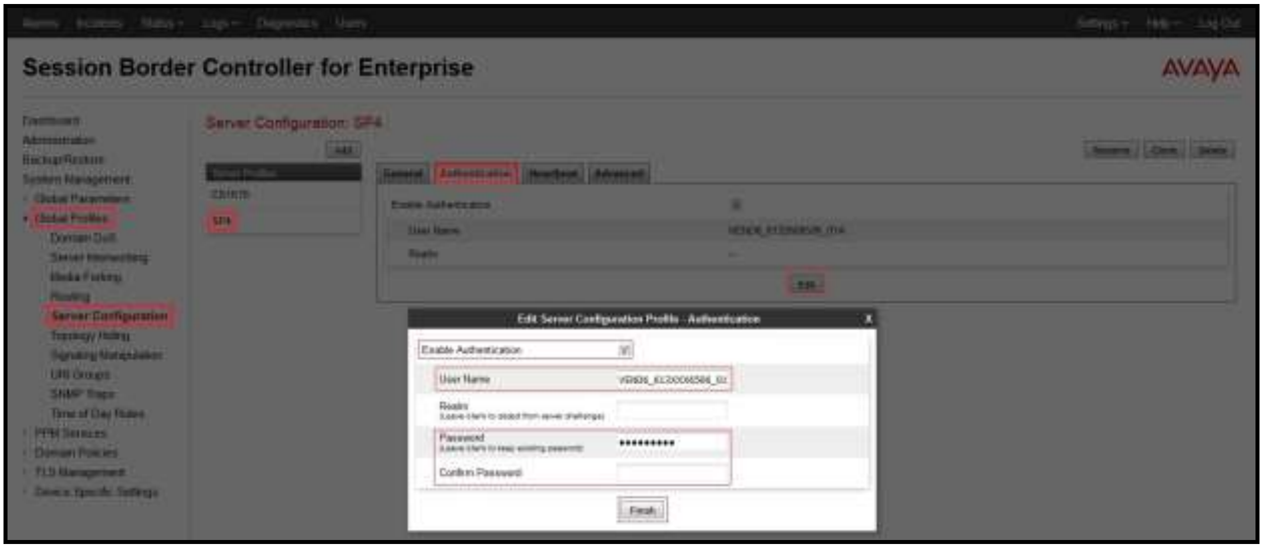
| | |
|---|---|
| Server Type | Trunk Server |

| IP Address / FQDN | Port | Transport |
|---|---|---|
| 192.168.237.206 | 5060 | UDP |

**Figure 60 - Server Configuration – General – Bell Canada**

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**.



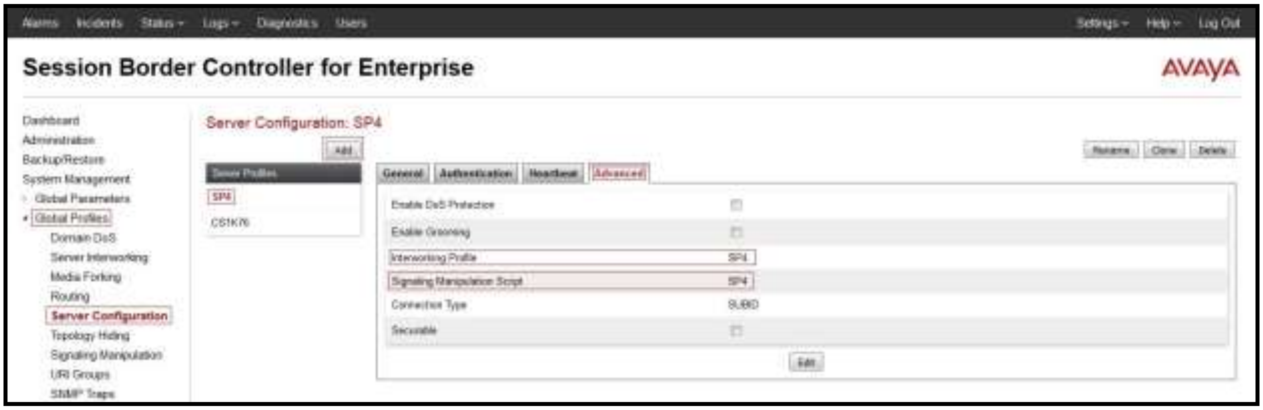
Edit Server Configuration Profile - Authentication

| | |
|---|---|
| Enable Authentication | ☑ |
| User Name | |
| Realm<br>(Leave blank to detect from server challenge) | |
| Password<br>(Leave blank to keep existing password) | •••••••••• |
| Confirm Password | |

**Figure 61 - Server Configuration – Authentication – Bell Canada**

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

- **Interworking Profile**: select **SP4** (see **Section 6.2.2**).
- **Signaling Manipulation Script**: select **SP4** (see **Section 6.2.3**).
- Click **Finish** (not shown).



| | |
|---|---|
| Enable DoS Protection | ☐ |
| Enable Grooming | ☐ |
| Interworking Profile | SP4 |
| Signaling Manipulation Script | SP4 |
| Connection Type | SUBID |
| Securable | ☐ |

**Figure 62 - Server Configuration – Advanced – Bell Canada**

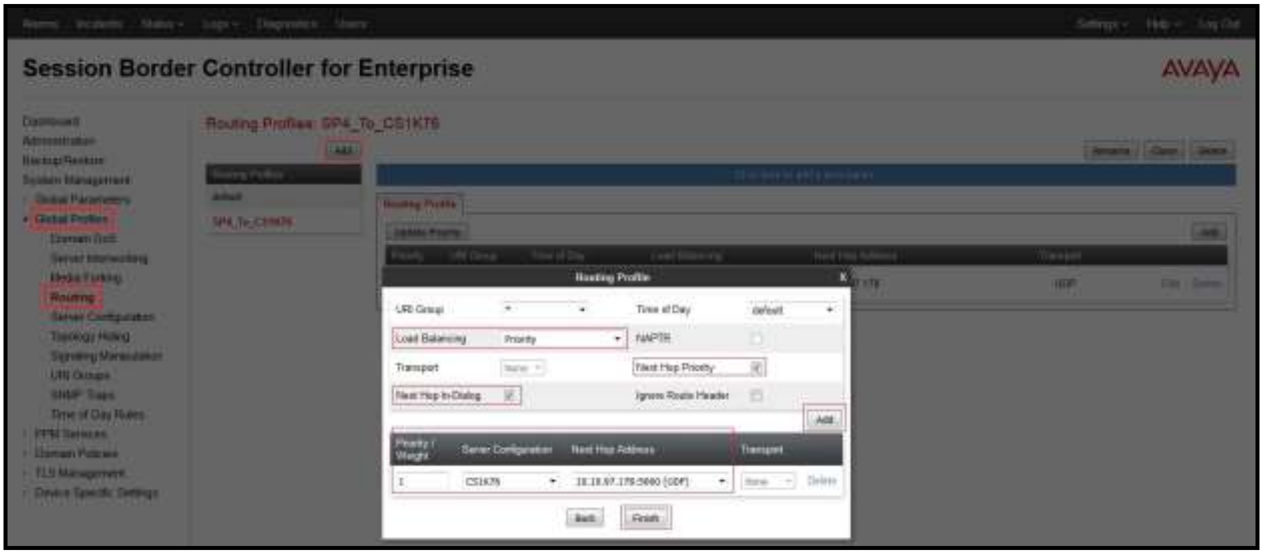
### 6.2.6. Configure Routing – CS1000

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_CS1K76** and click **Next** button (not shown).

- Select **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Check **Next Hop In-Dialog**. (This is the workaround to fix issues 3 and 10 mentioned in **Section 2.2**)
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight**: **1**.
- **Server Configuration**: **CS1K76** (see **Section 6.2.4**). This selection will automatically populate the **Next Hop Address** field with **10.10.97.178:5060 (UDP)** (Avaya CS1000 Node IP Address).
- Click **Finish**.



Session Border Controller for Enterprise
AVAYA
Global Profiles
Routing
Routing Profiles: SP4_To_CS1K76
Add
Routing Profile
Add
Back
Finish

URI Group: *
Time of Day: default
Load Balancing: Priority
NAPTR: □
Transport: None
Next Hop Priority: ☑
Next Hop In-Dialog: ☑
Ignore Route Header: □

| Priority / Weight | Server Configuration | Next Hop Address | Transport | |
|---|---|---|---|---|
| 1 | CS1K76 | 10.10.97.178:5060 (UDP) | None | Delete |

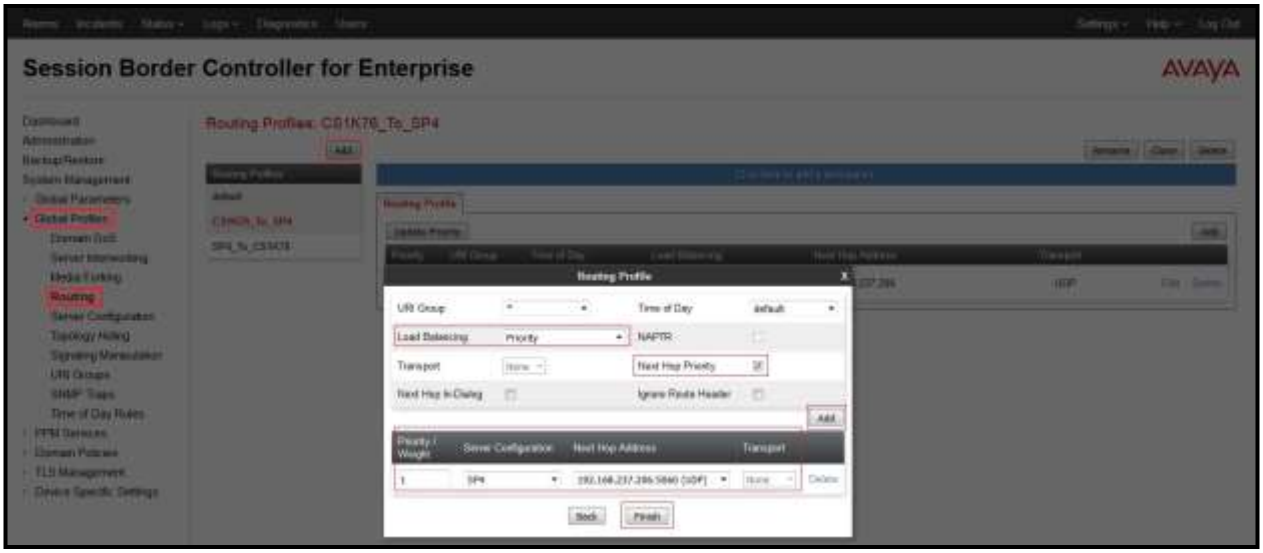
**Figure 63 - Routing to CS1000**

### 6.2.7. 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**: **CS1K76_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 6.2.5**). This selection will automatically populate the **Next Hop Address** field with **192.16.237.206:5060 (UDP)** (Bell Canada Signaling IP Address).
- Click **Finish**.



Session Border Controller for Enterprise
AVAYA
Routing Profiles: CS1K76_To_SP4
Add
Routing Profile
Back
Finish

Routing Profile

| | | | |
|---|---|---|---|
| URI Group | * | Time of Day | default |
| Load Balancing | Priority | NAPTR | □ |
| Transport | None | Next Hop Priority | ☑ |
| Next Hop In-Dialog | □ | Ignore Route Header | □ |

| Priority / Weight | Server Configuration | Next Hop Address | Transport | |
|---|---|---|---|---|
| 1 | SP4 | 192.168.237.206:5060 (UDP) | None | Delete |

**Figure 64 - Routing to Bell Canada**

### 6.2.8. Configure Topology Hiding – CS1000

The **Topology Hiding** screen allows an 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**.

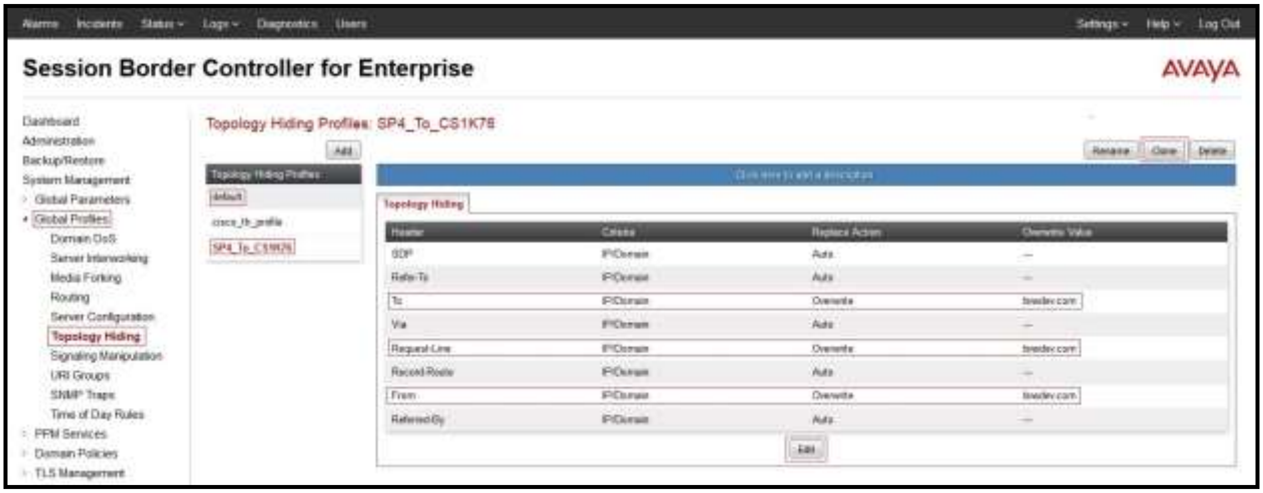
- Select **default** in **Topology Hiding Profiles**.
- Click **Clone**.
- Enter **Clone Name**: **SP4_To_CS1K76** and click **Finish** (not shown).
- Select **SP4_To_CS1K76** in **Topology Hiding Profiles** and click **Edit** button to modify as below:

  For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**

  For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**

  For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**

Click **Finish** (not shown).



Session Border Controller for Enterprise

Topology Hiding Profiles: SP4_To_CS1K76

| Header | Criteria | Replace Action | Overwrite Value |
|---|---|---|---|
| SDP | IP/Domain | Auto | --- |
| Refer-To | IP/Domain | Auto | --- |
| To | IP/Domain | Overwrite | bvwdev.com |
| Via | IP/Domain | Auto | --- |
| Request-Line | IP/Domain | Overwrite | bvwdev.com |
| Record-Route | IP/Domain | Auto | --- |
| From | IP/Domain | Overwrite | bvwdev.com |
| Referred-By | IP/Domain | Auto | --- |

**Figure 65 - Topology Hiding CS1000**

### 6.2.9. 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**: **CS1K76_To_SP4** and click **Finish** (not shown).
- Select **CS1K76_To_SP4** in **Topology Hiding Profiles** and click **Edit** button to modify as below:

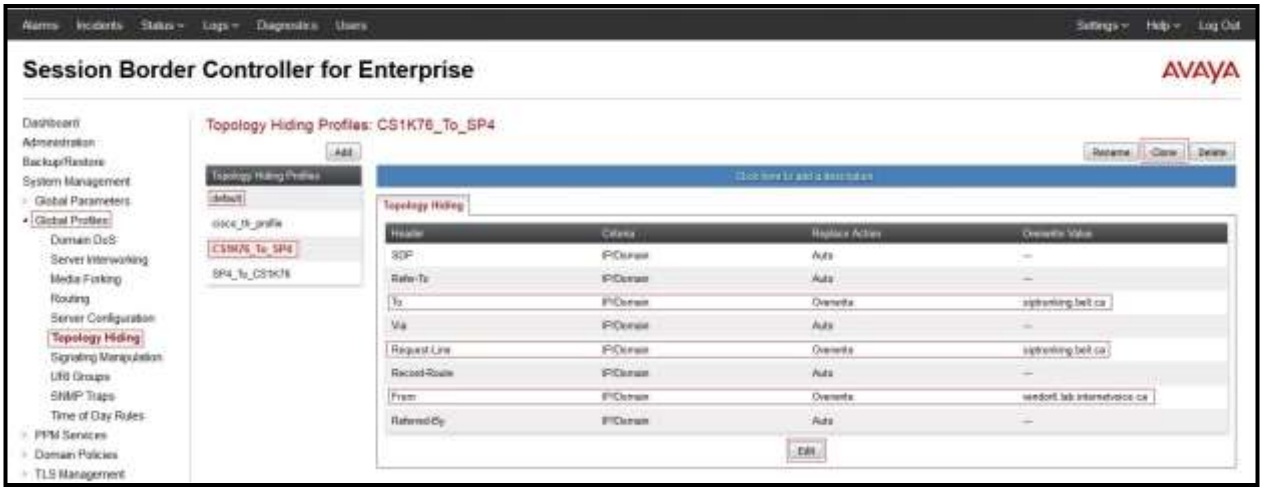
  For the Header **To,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **siptrunking.bell.ca** (This was Bell Canada domain).

  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 6.2.2** for Dynamic ONND, the specific domain shows in screenshot below in the **From** header, **vendor6.lab.internetvoice.ca**, should be changed to a general domain as **lab.internetvoice.ca**.

Click **Finish** (not shown).



Topology Hiding Profiles: CS1K76_To_SP4

| Header | Criteria | Replace Action | Overwrite Value |
|---|---|---|---|
| SDP | IP/Domain | Auto | --- |
| Refer-To | IP/Domain | Auto | --- |
| To | IP/Domain | Overwrite | siptrunking.bell.ca |
| Via | IP/Domain | Auto | --- |
| Request-Line | IP/Domain | Overwrite | siptrunking.bell.ca |
| Record-Route | IP/Domain | Auto | --- |
| From | IP/Domain | Overwrite | vendor6.lab.internetvoice.ca |
| Referred-By | IP/Domain | Auto | --- |

**Figure 66 - Topology Hiding Bell Canada**

## 6.3. Domain Policies

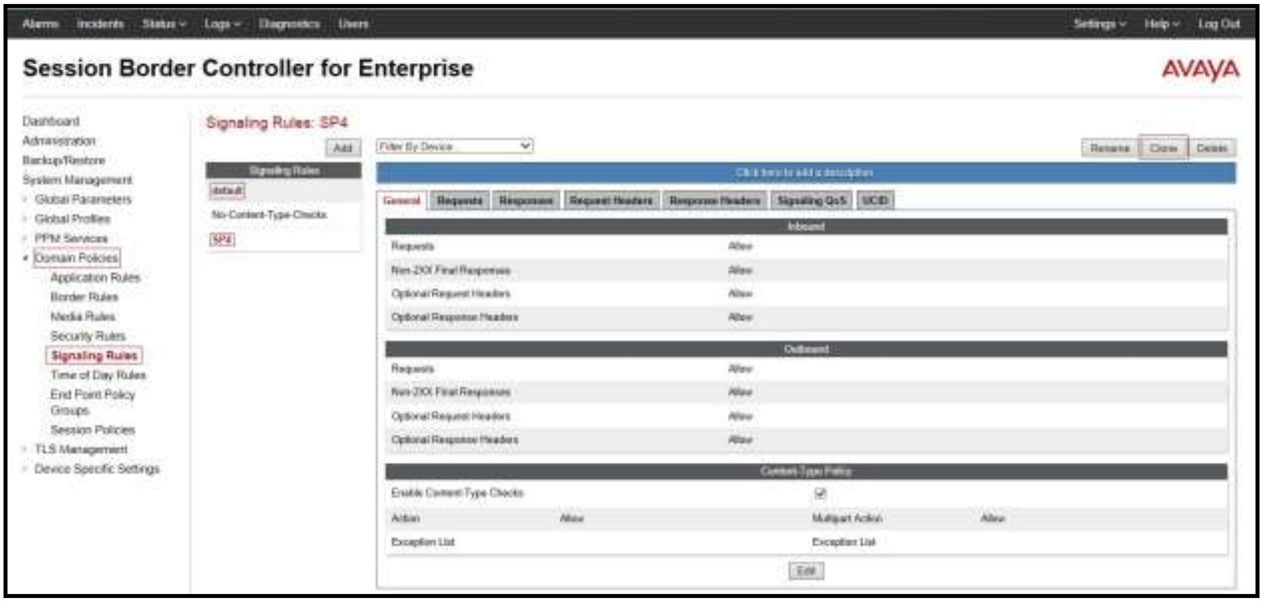
The Domain Policies feature allows one to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which 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.

### 6.3.1. 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).



Signaling Rules: SP4

| Inbound | |
|---|---|
| Requests | Allow |
| Non-2XX Final Responses | Allow |
| Optional Request Headers | Allow |
| Optional Response Headers | Allow |

| Outbound | |
|---|---|
| Requests | Allow |
| Non-2XX Final Responses | Allow |
| Optional Request Headers | Allow |
| Optional Response Headers | Allow |

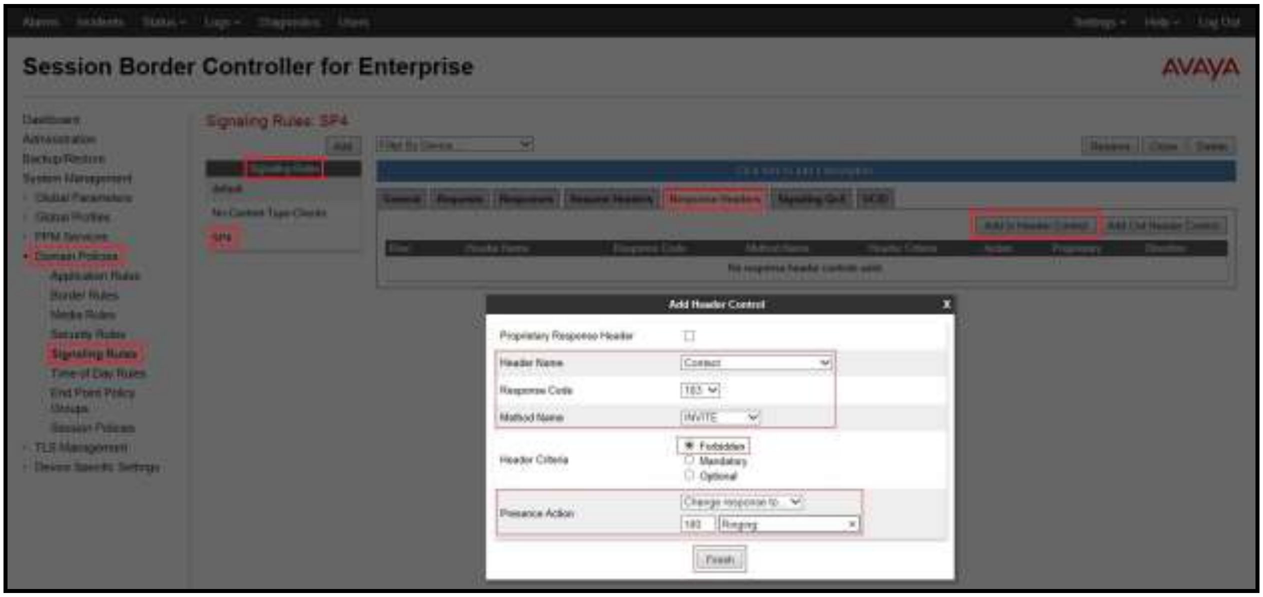
| Content-Type Policy | | | |
|---|---|---|---|
| Enable Content-Type Checks | | ☑ | |
| Action | Allow | Multipart Action | Allow |
| Exception List | | Exception List | |

**Figure 67 - 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 issue7 in **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.



Add Header Control

Proprietary Response Header ☐

Header Name: Contact

Response Code: 183

Method Name: INVITE

Header Criteria: ● Forbidden ○ Mandatory ○ Optional

Presence Action: Change response to 180 Ringing

Finish

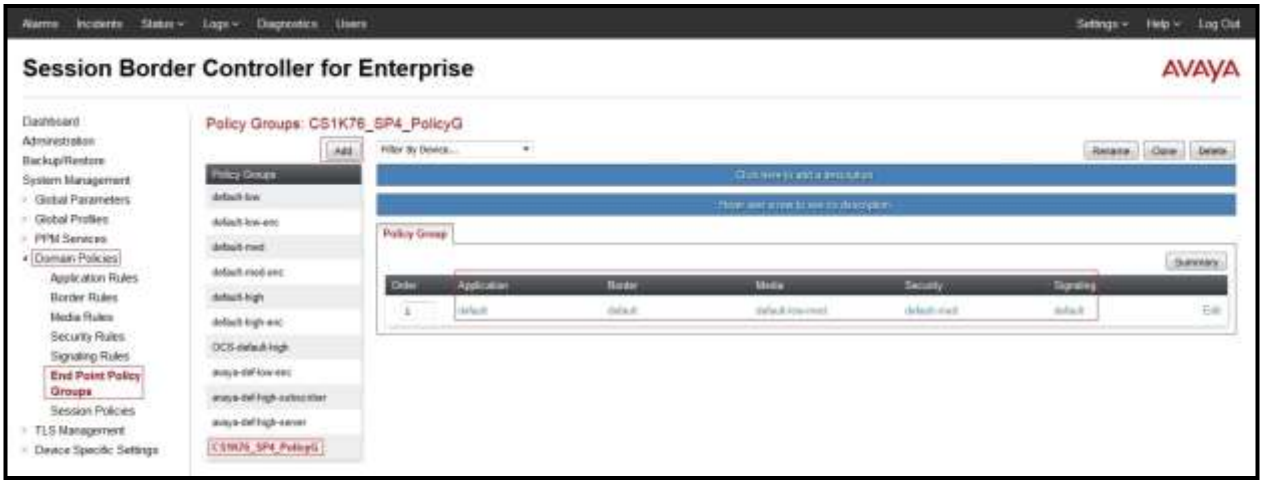
**Figure 68 - Signaling Rule SP4 – Header Control**

### 6.3.2. 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 6.3.1** 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**: **CS1K76_SP4_PolicyG**.
  - **Application Rule**: **default**.
  - **Border Rule**: **default**.
  - **Media Rule**: **default-low-med**.
  - **Security Rule**: **default-med**.
  - **Signaling Rule**: **default**.
  - **Time of Day**: **default**. Time of Day was selected by default; however, this selection did not appear in the screenshot below after the Endpoint Policy Group was created).
- Select **Finish** (not shown).



Session Border Controller for Enterprise

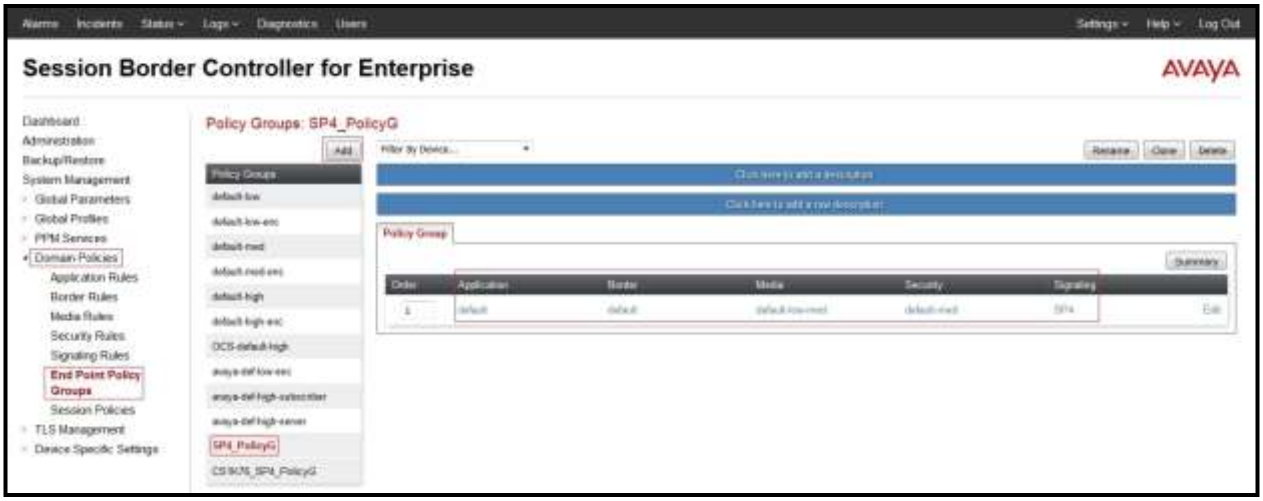
Policy Groups: CS1K76_SP4_PolicyG

| Order | Application | Border | Media | Security | Signaling |  |
|---|---|---|---|---|---|---|
| 1 | default | default | default-low-med | default-med | default | Edit |

**Figure 69 - Endpoint Policy – Avaya**

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 6.3.1** for optional choice, otherwise, select default rule).
    - **Time of Day**: **default**. Time of Day was selected by default; however, this selection did not appear in the screenshot below after the Endpoint Policy Group was created).
- Select **Finish** (not shown).



Session Border Controller for Enterprise

Policy Groups: SP4_PolicyG

| Policy Groups |
|---|
| default-low |
| default-low-enc |
| default-med |
| default-med-enc |
| default-high |
| default-high-enc |
| OCS-default-high |
| avaya-def-low-enc |
| avaya-def-high-subscriber |
| avaya-def-high-server |
| SP4_PolicyG |
| CS1K76_SP4_PolicyG |

| Order | Application | Border | Media | Security | Signaling | |
|---|---|---|---|---|---|---|
| 1 | default | default | default-low-med | default-med | SP4 | Edit |

**Figure 70 - Endpoint Policy – Bell Canada**

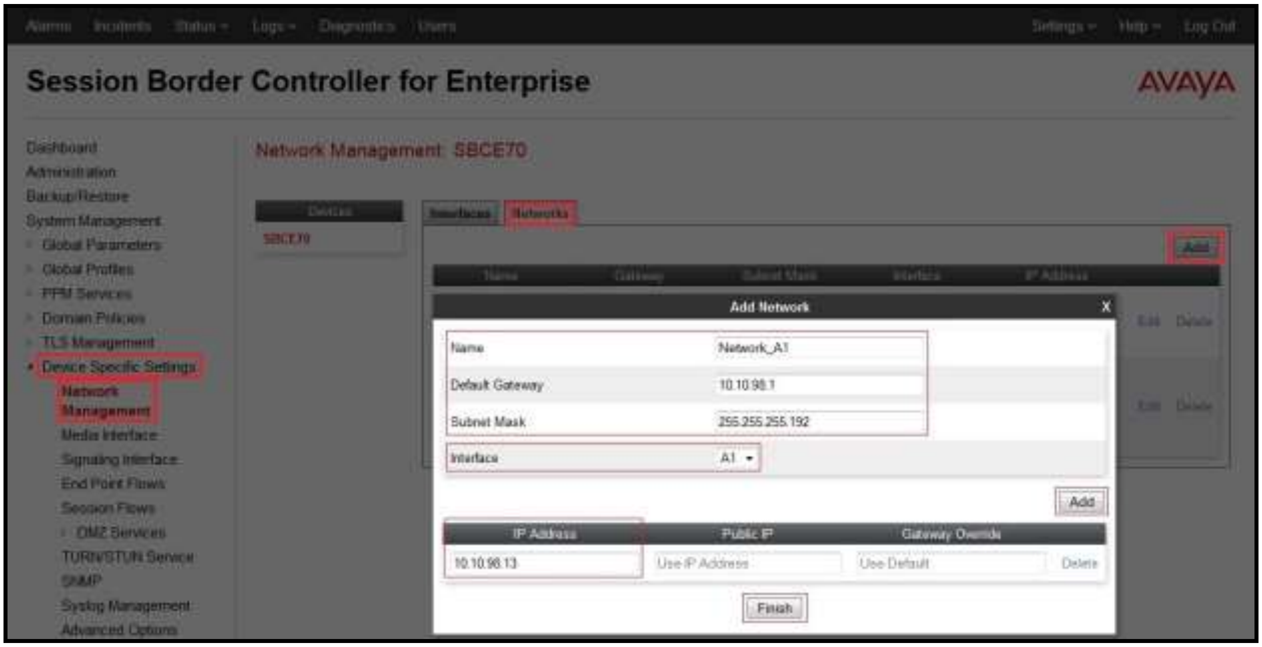
## 6.4. Device Specific Settings

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.

### 6.4.1. Manage Network Settings

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

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



Add Network

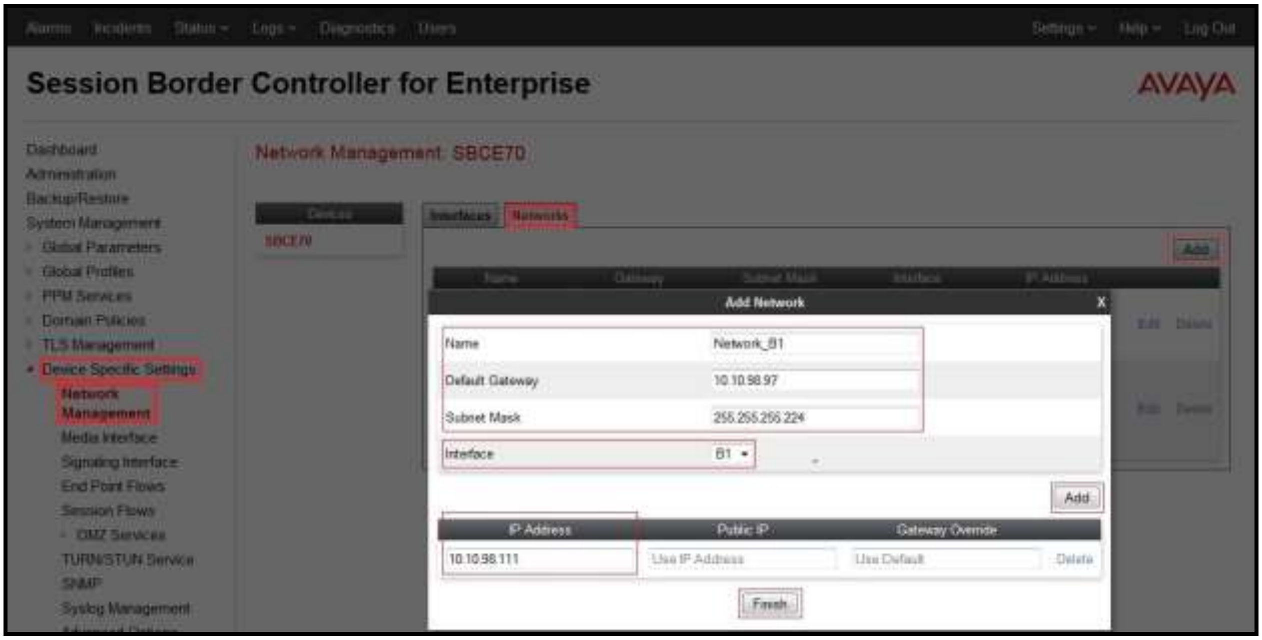
| | |
|---|---|
| Name | Network_A1 |
| Default Gateway | 10.10.98.1 |
| Subnet Mask | 255.255.255.192 |
| Interface | A1 |

| IP Address | Public IP | Gateway Override |
|---|---|---|
| 10.10.98.13 | Use IP Address | Use Default |

**Figure 71 - Network Management – Inside Interface**

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

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



Add Network

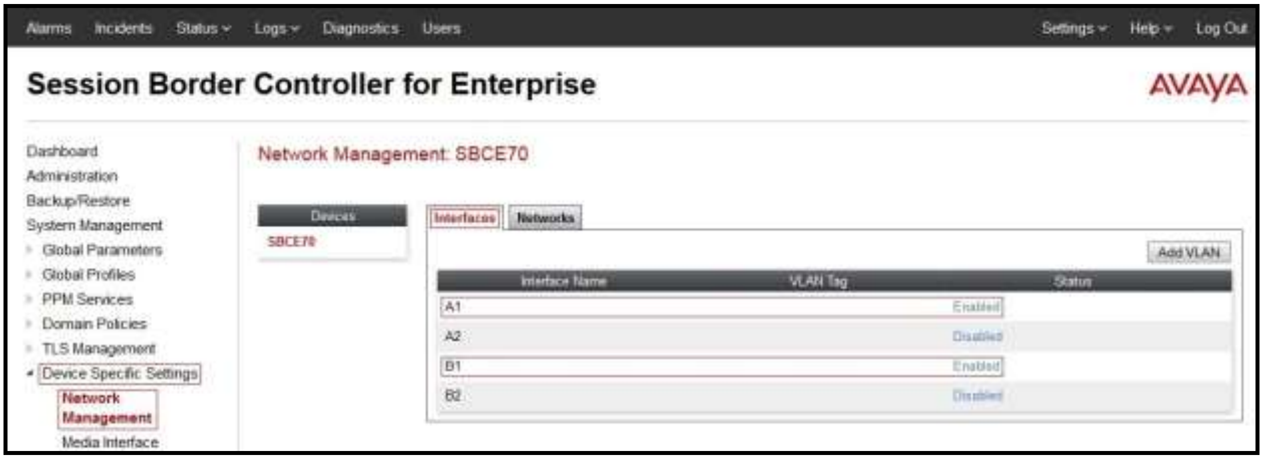
| | |
|---|---|
| Name | Network_B1 |
| Default Gateway | 10.10.98.97 |
| Subnet Mask | 255.255.255.224 |
| Interface | B1 |

| IP Address | Public IP | Gateway Override | |
|---|---|---|---|
| 10.10.98.111 | Use IP Address | Use Default | Delete |

**Figure 72 - Network Management – Outside Interface**

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

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



| Interface Name | VLAN Tag | Status |
|---|---|---|
| A1 | | Enabled |
| A2 | | Disabled |
| B1 | | Enabled |
| B2 | | Disabled |

**Figure 73 - Network Management – Interface Status**

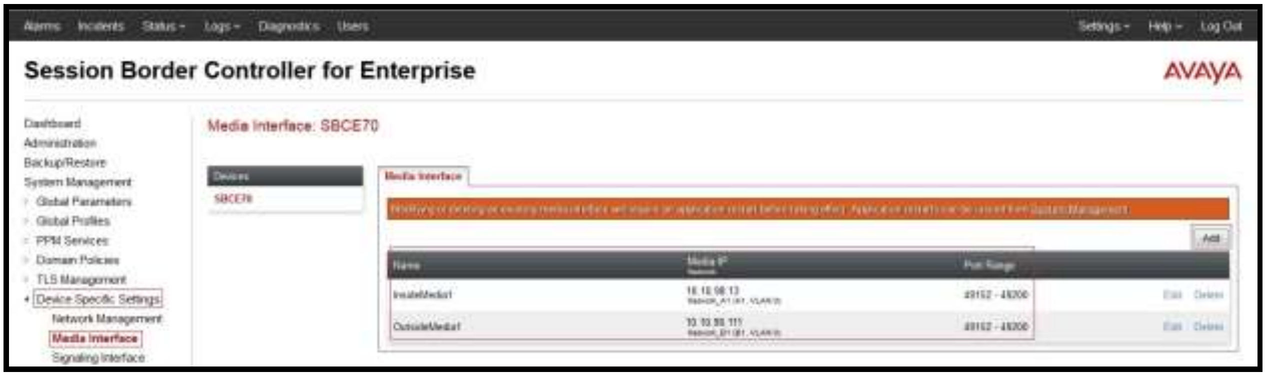
### 6.4.2. Create Media Interfaces

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

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

- Select the **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 CS1000).
  - **Port Range**: **49152 – 49200** (Bell Canada supported this port range during the compliance testing).
  - Click **Finish** (not shown).
- Select the **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:



Media Interface: SBCE70

| Name | Media IP<br>Network | Port Range |
|---|---|---|
| InsideMedia1 | 10.10.98.13<br>Network_A1 (A1, VLAN0) | 49152 - 49200 |
| OutsideMedia1 | 10.10.98.111<br>Network_B1 (B1, VLAN0) | 49152 - 49200 |

**Figure 74 - Media Interface**

### 6.4.3. 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**.

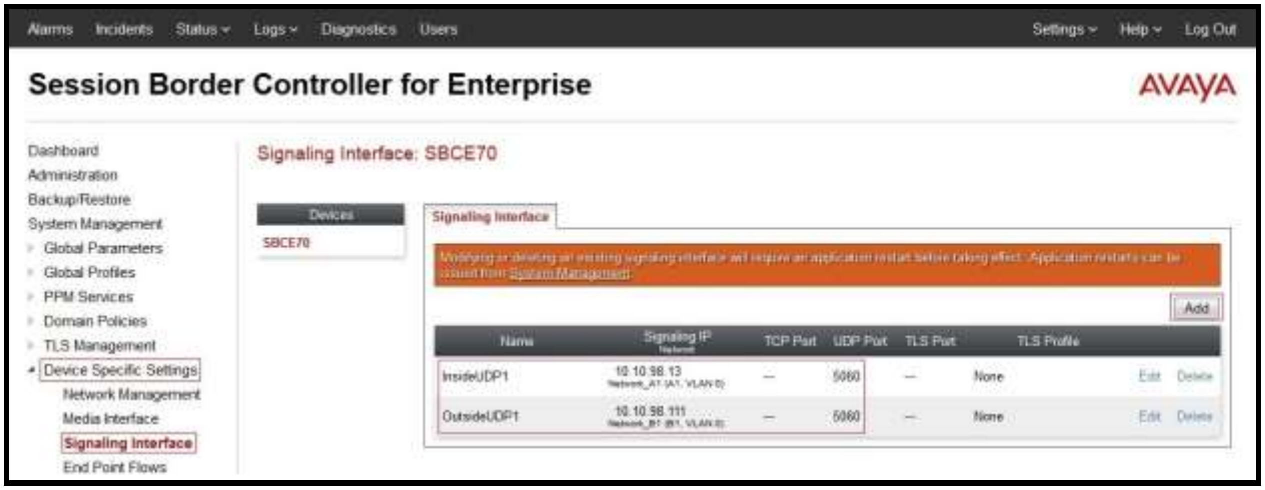
- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **InsideUDP1**.
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward CS1000).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).

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

- Select the **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:



Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

| Name | Signaling IP<br>Network | TCP Port | UDP Port | TLS Port | TLS Profile | | |
|---|---|---|---|---|---|---|---|
| InsideUDP1 | 10.10.98.13<br>Network_A1 (A1, VLAN 0) | — | 5060 | — | None | Edit | Delete |
| OutsideUDP1 | 10.10.98.111<br>Network_B1 (B1, VLAN 0) | — | 5060 | — | None | Edit | Delete |

**Figure 75 - Signaling Interface**

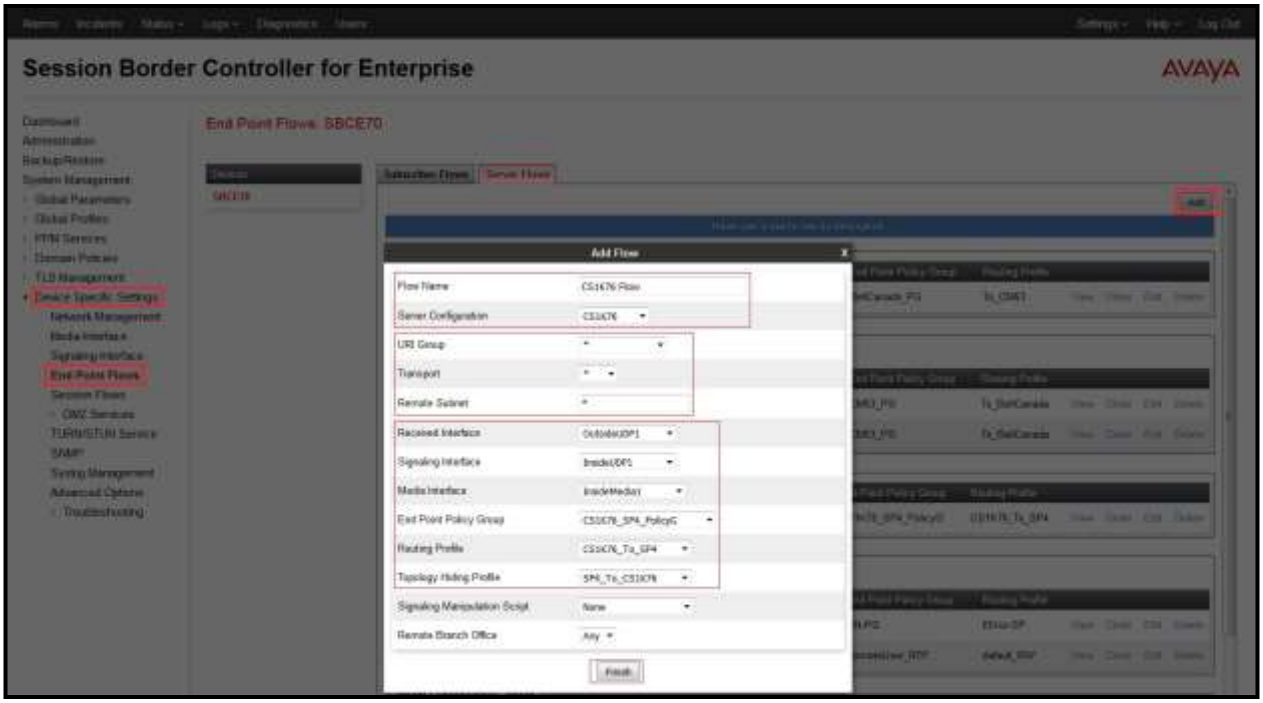
## 6.4.4. Configuration Server Flows

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

### 6.4.4.1 Create End Point Flows – CS1000

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**: **CS1K76 Flow**.
  - **Server Configuration**: **CS1K76** (see **Section 6.2.4**).
  - **URI Group**: *****.
  - **Transport**: *****.
  - **Remote Subnet**: *****.
  - **Received Interface**: **OutsideUDP1** (see **Section 6.4.3**).
  - **Signaling Interface**: **InsideUDP1** (see **Section 6.4.3**).
  - **Media Interface**: **InsideMedia1** (see **Section 6.4.2**).
  - **End Point Policy Group**: **CS1K76_SP4_PolicyG** (see **Section 6.3.2**).
  - **Routing Profile**: **CS1K76_To_SP4** (see **Section 6.2.7**).
  - **Topology Hiding Profile**: **SP4_To_CS1K76** (see **Section 6.2.8**).
  - Click **Finish**.



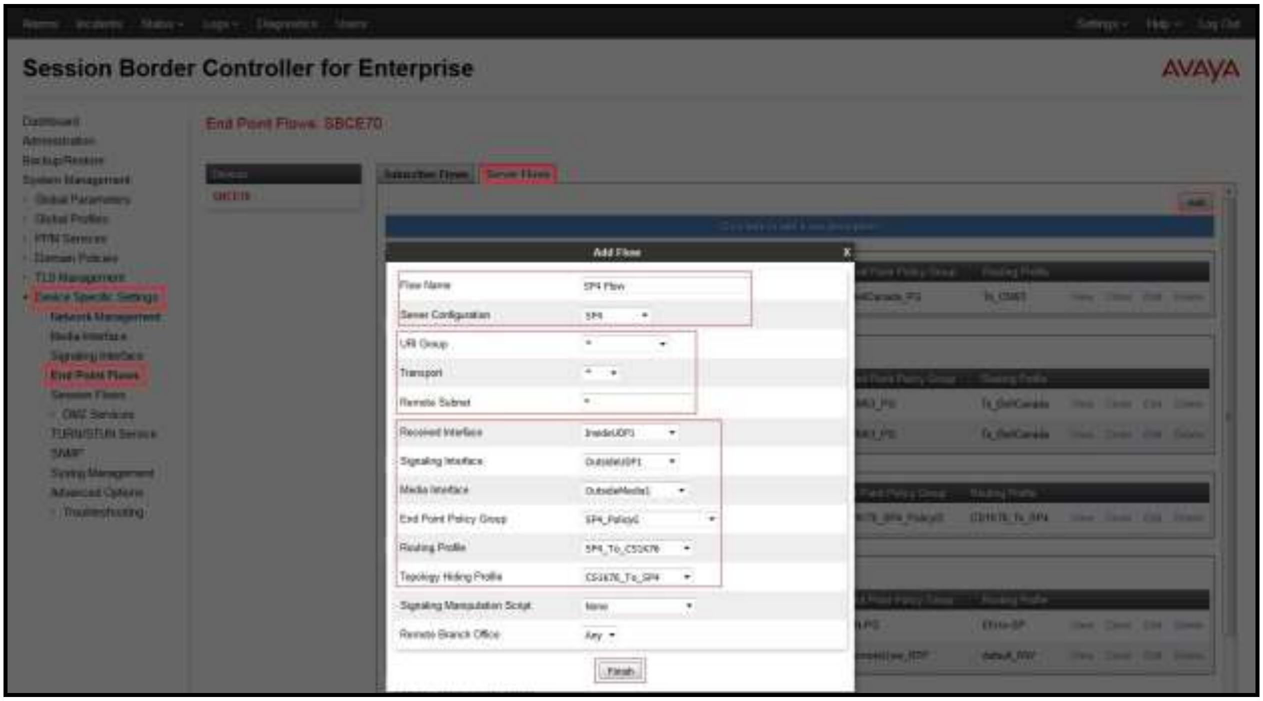
Flow Name: CS1K76 Flow
Server Configuration: CS1K76
URI Group: *
Transport: *
Remote Subnet: *
Received Interface: OutsideUDP1
Signaling Interface: InsideUDP1
Media Interface: InsideMedia1
End Point Policy Group: CS1K76_SP4_PolicyG
Routing Profile: CS1K76_To_SP4
Topology Hiding Profile: SP4_To_CS1K76
Signaling Manipulation Script: None
Remote Branch Office: Any

**Figure 76 - End Point Flow to Bell Canada**

### 6.4.4.2 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 6.2.5**).
  - **URI Group**: *****.
  - **Transport**: *****.
  - **Remote Subnet**: *****.
  - **Received Interface**: **InsideUDP1** (see **Section 6.4.3**).
  - **Signaling Interface**: **OutsideUDP1** (see **Section 6.4.3**).
  - **Media Interface**: **OutsideMedia1** (see **Section 6.4.2**).
  - **End Point Policy Group**: **SP4_PolicyG** (see **Section 6.3.2**).
  - **Routing Profile**: **SP4_To_CS1K76** (see **Section 6.2.6**).
  - **Topology Hiding Profile**: **CS1K76_To_SP4** (see **Section 6.2.9**).
  - Click **Finish**.



| | |
|---|---|
| Flow Name | SP4 Flow |
| Server Configuration | SP4 |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | InsideUDP1 |
| Signaling Interface | OutsideUDP1 |
| Media Interface | OutsideMedia1 |
| End Point Policy Group | SP4_PolicyG |
| Routing Profile | SP4_To_CS1K76 |
| Topology Hiding Profile | CS1K76_To_SP4 |
| Signaling Manipulation Script | None |
| Remote Branch Office | Any |

**Figure 77 - End Point Flow from Bell Canada**

## 7. 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, 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.

# 8. Verification Steps

The following steps may be used to verify the configuration.

## 8.1. 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.

## 8.2. Verification of an Active Call on Communication Server 1000

**Active Call Trace (ld 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 6139XX5206 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 **ld 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:

```
>ld 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: 49174
  FAR-END SIP SIGNALLING IP: 10.10.98.13
  FAR-END MEDIA ENDPOINT IP: 10.10.98.13  PORT: 49174
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  8   TERM  13
EES_DATA:
NONE
QUEU  NONE
CALL ID 501 87
```

```
----  ISDN ISL CALL (ORIG) ----
CALL REF # =  385
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  613XXX5206  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 (6139XX5206) to an internal Avaya phone (6132XX6506). Then check the SIP trunk status by using **ld 32**, and verify one trunk is BUSY.

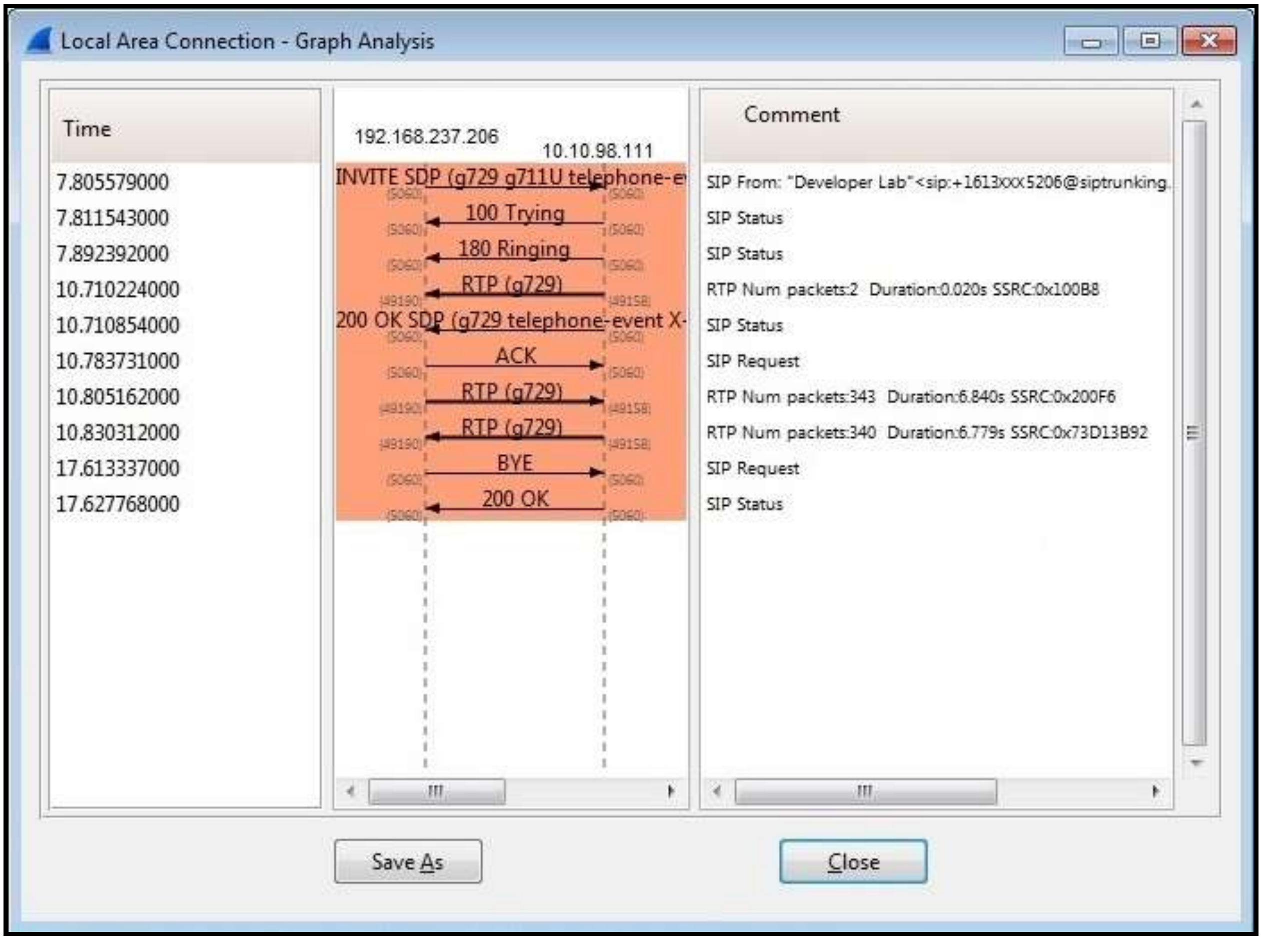
```
>ld 32
NPR000
.stat 100 0
091 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

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
```

## 8.3. Protocol Trace

Below is a wireshark trace of the same call scenario described in **Section 8.2**.



| Time | 192.168.237.206<br>10.10.98.111 | Comment |
|---|---|---|
| 7.805579000 | INVITE SDP (g729 g711U telephone-e | SIP From: "Developer Lab"<sip:+1613xxx5206@siptrunking. |
| 7.811543000 | 100 Trying | SIP Status |
| 7.892392000 | 180 Ringing | SIP Status |
| 10.710224000 | RTP (g729) | RTP Num packets:2 Duration:0.020s SSRC:0x100B8 |
| 10.710854000 | 200 OK SDP (g729 telephone-event X- | SIP Status |
| 10.783731000 | ACK | SIP Request |
| 10.805162000 | RTP (g729) | RTP Num packets:343 Duration:6.840s SSRC:0x200F6 |
| 10.830312000 | RTP (g729) | RTP Num packets:340 Duration:6.779s SSRC:0x73D13B92 |
| 17.613337000 | BYE | SIP Request |
| 17.627768000 | 200 OK | SIP Status |

**Figure 78 – SIP Call Trace**

# 9. Conclusion

All of the test cases have been executed. Despite observations seen during the testing, as noted in **Section 2.2**, the test met the objectives outlined in **Section 2.1**. The Bell Canada SIP Trunk Service is considered **compliant** with Avaya Communication Server 1000 Release 7.6 and Avaya Session Border Controller for Enterprise Release 7.0.

# 10. References

This section references the 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**

[1] *Network Routing Service Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013

[2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013

[3] *Communication Server 1000E Overview, Avaya Communication Server 1000*, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013

[4] *Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013

[5] *Dialing Plans Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.

[6] *Product Compatibility Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013

**Avaya Session Border Controller for Enterprise**

[7] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.0, Issue 1, August 2015

[8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0 Issue 1, August 2015

[9] *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*

# 11. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE in **Section 6.2.3**:

```
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)","");
         }
   act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
        {
      //Remove PAI header for ONND testing
            remove(%HEADERS["P-Asserted-Identity"][1]);

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

      //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";
              }

      // Create Diversion Headers
               if (%HEADERS["History-Info"][1].regex_match("reason")) then
                  {
                     %HEADERS["Diversion"][1] = "<sip:dummy@dummy.com>";
                     %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-
Info"][1].URI.SCHEME;
                     %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-
Info"][1].URI.USER;
```

```
                        %HEADERS["Diversion"][1].URI.HOST = %HEADERS["History-
Info"][1].URI.HOST;

%HEADERS["Diversion"][1].regex_replace("@siptrunking.bell.ca","@vendor6.lab.internetvoic
e.ca");
                        %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-
Info"][1].URI.PORT;
       // For ONND testing
                        append(%HEADERS["Diversion"][1].URI,";user=phone");

append(%HEADERS["Diversion"][1].URI,";otg=VEND6_613XXX6506_01A");

                        %HEADERS["Diversion"][1].URI.PARAMS["reason"] = "unconditional";
                        %HEADERS["Diversion"][1].URI.PARAMS["counter"] = "1";
                        %HEADERS["Diversion"][1].URI.PARAMS["screen"] = "no";
                        %HEADERS["Diversion"][1].URI.PARAMS["privacy"] = "off";
       // Adjust the bracket < > position
                        %HEADERS["Diversion"][1].regex_replace("user=phone","user=phone>");
                        %HEADERS["Diversion"][1].regex_replace("privacy=off>","privacy=off");
                     }
        }
}
```

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.