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 6.2.1 – Issue 1.0

Abstract

These Application Notes describe the procedure for configuration Bell Canada SIP Trunk Service with Avaya Communication Server 1000 Release 7.6, and Avaya Session Border Controller for Enterprise Release 6.2.1.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. Calls were placed to and from the PSTN with various Avaya endpoints.

Bell Canada SIP Trunk Service provides PSTN access via SIP trunks between enterprise and Bell Canada's network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 (CS1000) Release 7.6, Avaya Session Border Controller for Enterprise (SBCE) Release 6.2.1 with Bell Canada SIP Trunk Service. Bell Canada SIP Trunk Service provides PSTN access via SIP Trunks between the enterprise and Bell Canada's network as an alternative to legacy analog or digital trunks.

2. General Test Approach and Test Results

CS1000 was connected to SBCE via SIP Trunks. SBCE was connected to Bell Canada's network via SIP trunks. Various call types were made from CS1000 to Bell Canada and vice versa to verify interoperability.

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

2.1. Interoperability Compliance Testing

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

- General call processing between CS1000 and Bell Canada SIP Trunk Service, including the following:
  - Codec/ptime (G.711 u-law/20ms), no Voice Activity Detection (VAD).
  - Hold/Resume on both ends.
  - Calling Line Identification Display (CLID).
  - Ring-back tone.
  - Speech (audio) path.
  - Dialing plan support (local, long distance, international, outbound toll-free, assisted operator, 411, and 911).
  - Abandoned Call.
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends.
- Response to SIP OPTIONS queries.
- Registration and Authentication.
- Fax G.711 Pass Through.
- Inbound and outbound long hold time call stability.
- Caller number/ID presentation.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.

- DTMF (RFC2833) in both directions.
- SIP Transport UDP, port 5060.
- Voice Mail Server Call Pilot (hosted on CS1000 system).

The following assumptions were made for the compliance tested configuration:

1. CS1000 R7.6 software with latest patches.
2. Bell Canada SIP Trunk Service provides support to setup, configure and troubleshoot on carrier switch during testing execution.

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

1. Calls were checked for the correct call progress tones and cadences.
2. During the ringing state the ring back tone and destination ringing were checked.
3. Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
4. Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
5. 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.
6. The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
7. Speech path was checked before and after calls were put on/off hold from each end.

2.2. Test Results

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

1. **Calling Line ID is not available after hold/resume** – If the CS1000 phone holds/resumes an outbound call, the dialed digits are no longer displayed. This is a CS1000 known issue.
2. **SIP Telephone Conference** – During a conference call hosted by the SIP telephone, if the SIP telephone is hanged up/dropped out of the conference, the conference call is dropped. This is known CS1000 SIP telephone limitation.
3. **Calling Line ID (CLID) is not correctly displayed** – After call redirection, namely blind/consultative transfers, is completed with two way voice paths, the CLID on the transferee’s telephone is not updated accordingly. This is known CS1000 limitation.
4. **Blind Call Transfer to PSTN using SIP phone does not completed until transferee pick up the call** – Call scenario is when PSTN phone calls to enterprise SIP extension (CS1000 SIP phone), CS1000 answers the call and performs blind transfer the call to another PSTN endpoint. The expected behavior of the enterprise SIP phone is after transfer, the phone should display “transfer completed”. But in this case, user press “transfer” button, answer question of “Consultative transfer with party ?”, and the answer is “No”, which implies the blind transfer, as the transferee PSTN phone is ringing and the SIP phone should be released and displayed “transfer successfully”. Instead, the SIP phone is still displayed “transferring” and not released until the transferee PSTN phone answer the call. The work around is to hang up the SIP phone. This is very minor known limitation on CS1000 SIP phone. There is no user impact. Transfer is still completed with 2 way speech paths.

5. **Call from MobileX phone to internal phone number (other than the host) does not have audio path** – MobileX phone firstly dials MSA (Mobile Service Access) number, then dials any internal phone number. MobileX phone and internal phone do not have audio path after internal phone answers the call. But after host station joins the call, there is speech path on three end points. This is CS1000 limitation and this issue is under investigation.

2.3. Support

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

For technical support on the Bell Canada SIP Trunk Service, please contact customer service or visit 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.

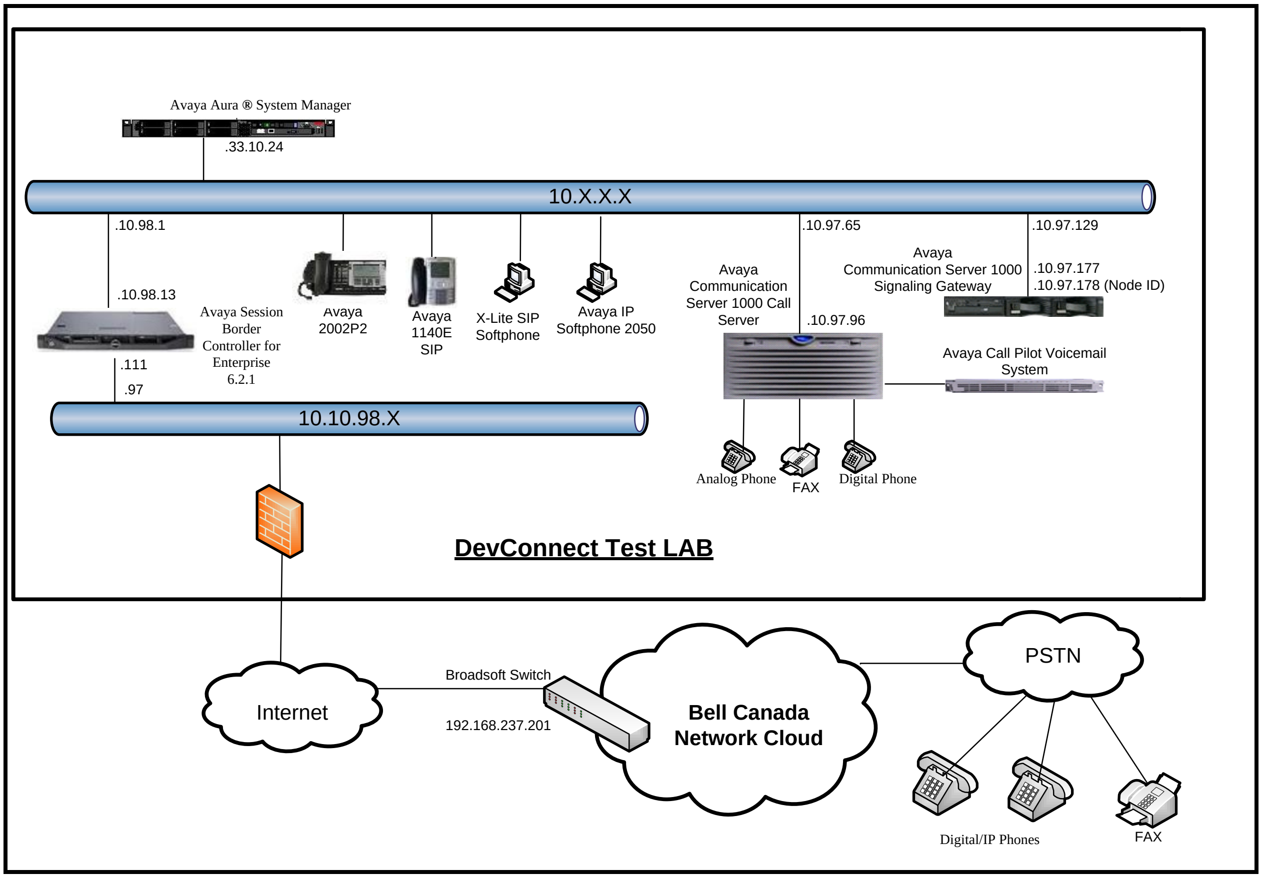

Figure 1- Network diagram for Avaya and Bell Canada SIP Trunk Service

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 + Signaling Server: 7.65.16 GA SIP Line Server: 7.65.16 GA
Avaya Call Pilot C201i	Call Pilot Voice Mail Manager: 05.00.41.143
Avaya Aura® System Manager running on an Avaya S8800 Server	6.3.4 (6.3.4.4.1830) (Build No. 6.3.0.8.5682-6.3.8.2631)
Avaya Session Border Controller for Enterprise	6.2.1 Q07
Avaya Phones: 2002 p2 (UNIStim) 1140E SIP	 0604DCO 04.03.12.00
Avaya 3904 Digital Phone	N/A
Avaya IP Softphone 2050	4.04.0067
X-Lite SIP Softphone	4.5.5 71236
Analog Symphony 2000	N/A
HP Office jet 4500 Fax	N/A

Bell Canada systems:

System	Software
Broadsoft SoftSwitch	Release 18
Acme Packet Net-Net 4250 SBC	Firmware SC6.2.0 MR-4 Patch 1 (Build 718)
Legacy Nortel CS2K Media Gateway	SN10 PVG/IW-SPM

Additional patch lineup for the configuration listed as follows:

Call Server: 7.65 P+ GA plus latest DEPLIST – CPL_7.6S4.zip (X2107.65P)
Signaling Server: 7.65.16 GA plus latest DEPLIST – SP_7.6_4.ntl (7.65.16.00)
CS1K Signaling Server patch list:

```
[admin@car3-ssg-carrier ~]$ pstat
Product Release: 7.65.16.00
In system patches: 1
PATCH#  NAME      IN_SERVICE   DATE      SPECINS  TYPE   RPM
37      p31484_1   Yes         20/02/14  NO       FRU    cs1000-shared-general-7.65.16-00.i386
In System service updates: 26
PATCH#  IN_SERVICE   DATE      SPECINS   REMOVABLE   NAME
9       Yes          20/02/14  YES       YES         cs1000-dmWeb-7.65.16.22-1.i386.000
12      Yes          19/02/14  NO        YES         cs1000-linuxbase-7.65.16.22-02.i386.000
13      Yes          20/02/14  NO        YES         cs1000-pd-7.65.16.21-00.i386.000
```

14	Yes	20/02/14	NO	YES	cs1000-Jboss-Quantum-7.65.16.22-3.i386.000
15	Yes	20/02/14	YES	YES	cs1000-patchWeb-7.65.16.22-1.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	20/02/14	NO	YES	cs1000-shared-xmsg-7.65.16.21-00.i386.000
20	Yes	20/02/14	NO	YES	cs1000-mscAnnc-7.65.16.21-02.i386.001
21	Yes	20/02/14	NO	YES	cs1000-mscAttn-7.65.16.21-04.i386.001
22	Yes	20/02/14	NO	YES	cs1000-mscConf-7.65.16.21-02.i386.001
23	Yes	20/02/14	NO	YES	cs1000-mscMusc-7.65.16.21-02.i386.001
24	Yes	20/02/14	NO	YES	cs1000-mscTone-7.65.16.21-03.i386.001
25	Yes	20/02/14	NO	YES	cs1000-gk-7.65.16.21-01.i386.000
26	Yes	20/02/14	NO	YES	cs1000-snmp-7.65.16.21-00.i686.000
27	Yes	20/02/14	YES	YES	tzdata-2013c-2.el5.i386.001
28	Yes	20/02/14	YES	YES	cs1000-tps-7.65.16.21-11.i386.000
29	Yes	20/02/14	NO	YES	cs1000-sps-7.65.16.21-8.i386.000
30	Yes	20/02/14	NO	YES	cs1000-shared-omm-7.65.16.21-2.i386.000
31	Yes	20/02/14	YES	YES	cs1000-baseWeb-7.65.16.22-1.i386.000
32	Yes	20/02/14	YES	YES	cs1000-csoneksvrmgr-7.65.16.22-1.i386.000
33	Yes	20/02/14	YES	YES	cs1000-ipsec-7.65.16.22-1.i386.000
34	Yes	20/02/14	YES	YES	cs1000-vtrk-7.65.16.22-4.i386.000
35	Yes	20/02/14	NO	YES	cs1000-cppmUtil-7.65.16.22-1.i686.000
36	Yes	20/02/14	YES	YES	cs1000-oam-logging-7.65.16.22-3.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 Special Number (SPN) features to route calls from the CS1000 to the PSTN, via SIP trunks to Bell Canada system.

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 System Manager and Element Manager (EM)

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

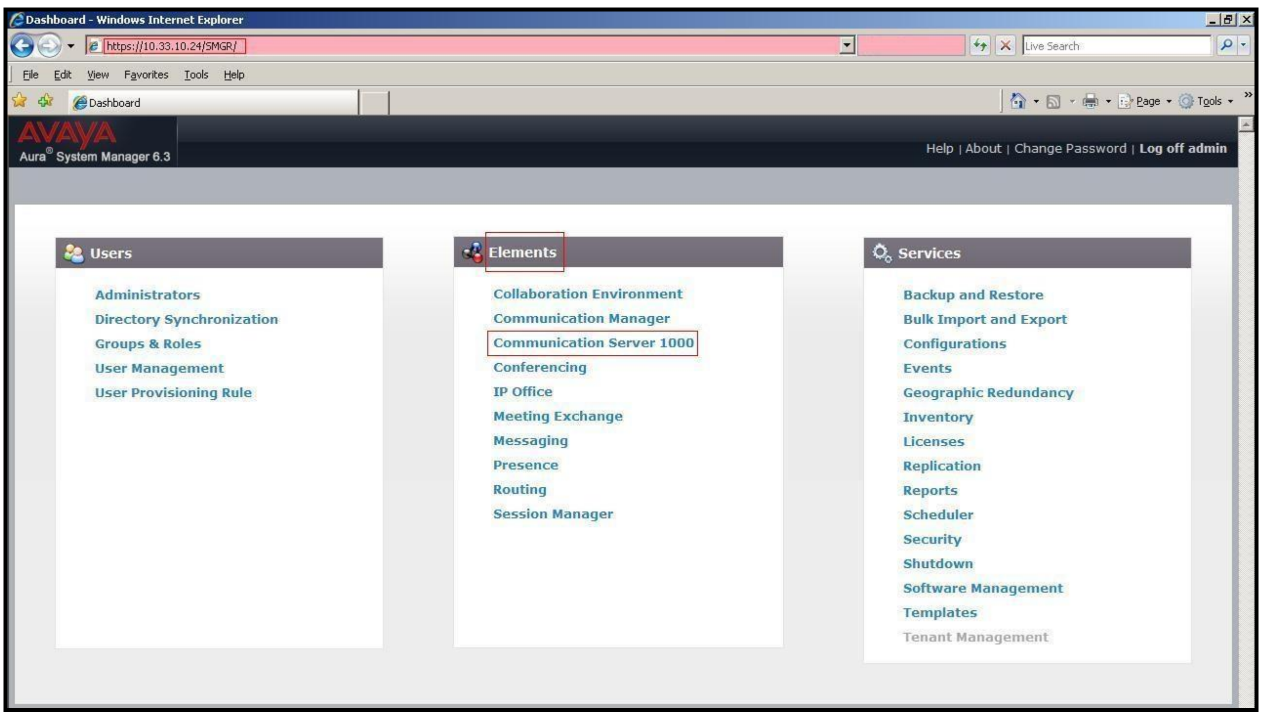

Figure 2 –System Manager Home Screen

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

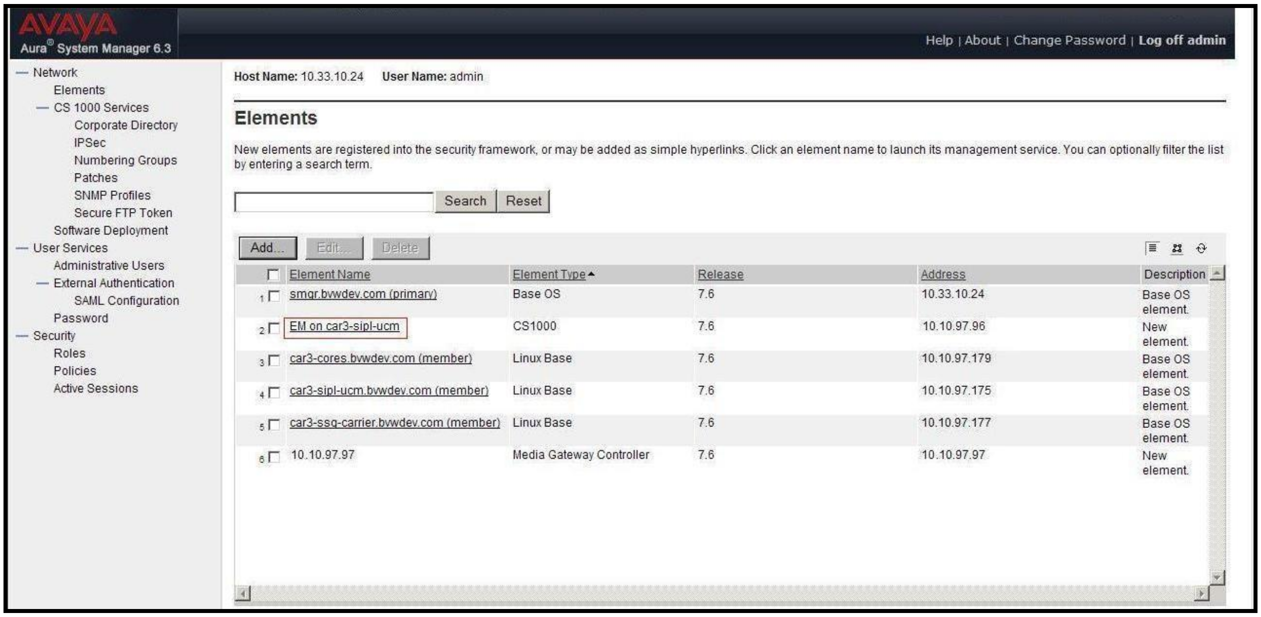

Figure 3 – Communication Server 1000 Management

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

Figure 4 – Communication Server 1000 Log In Screen

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

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

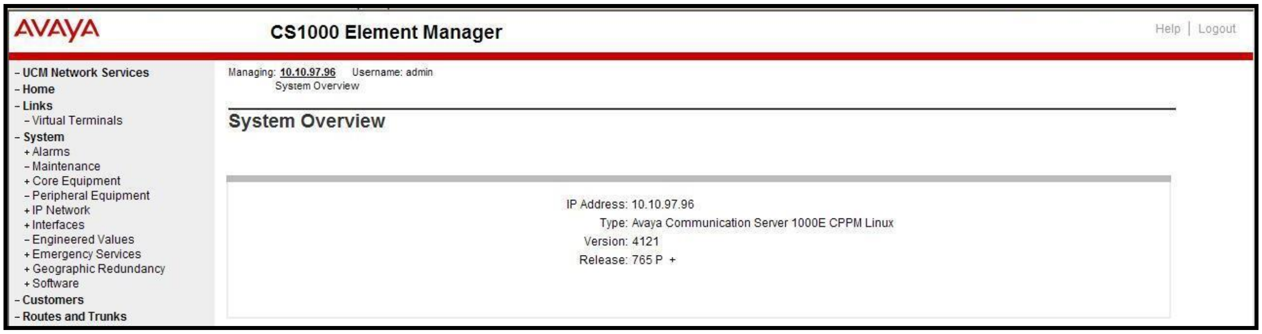

Figure 5 – Element Manager System Overview

5.1.2. Log into the Call Server by using the 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@10.10.97.177's password: **<----enter the password**
Last login: Fri Apr 18 07:20:18 2014 from 10.10.98.78
[admin@car3-ssg-carrier ~]$ **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 #08 LOGGED IN ADMIN 07:39 18/04/2014
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 an 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 Trunk 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 6**.

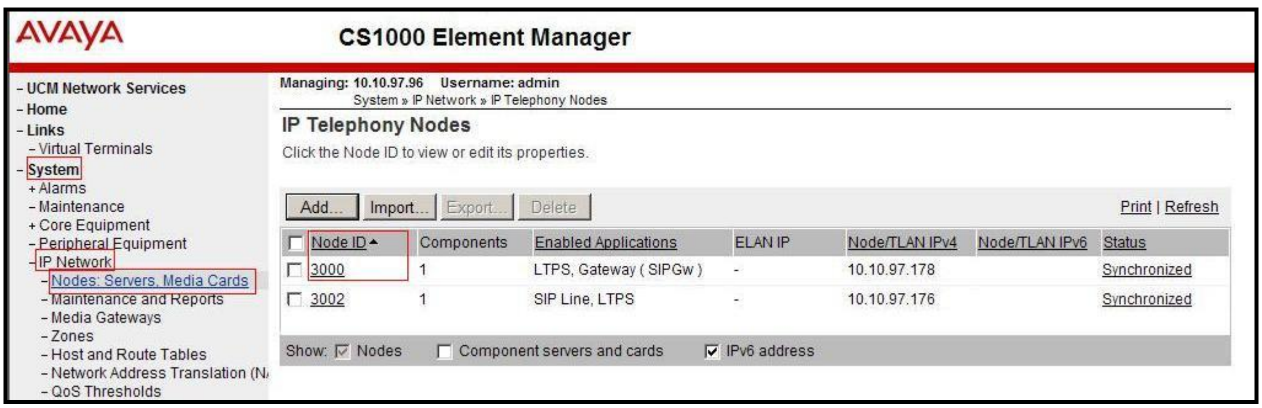

Figure 6 – IP Telephony Nodes

The **Node Details** screen is displayed in **Figure 7** with the IP address of the CS1000 node. **Call server IP address: 10.10.97.96**. The **Node IPv4 address 10.10.97.178** is a virtual address which corresponds to the **TLAN IP 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.

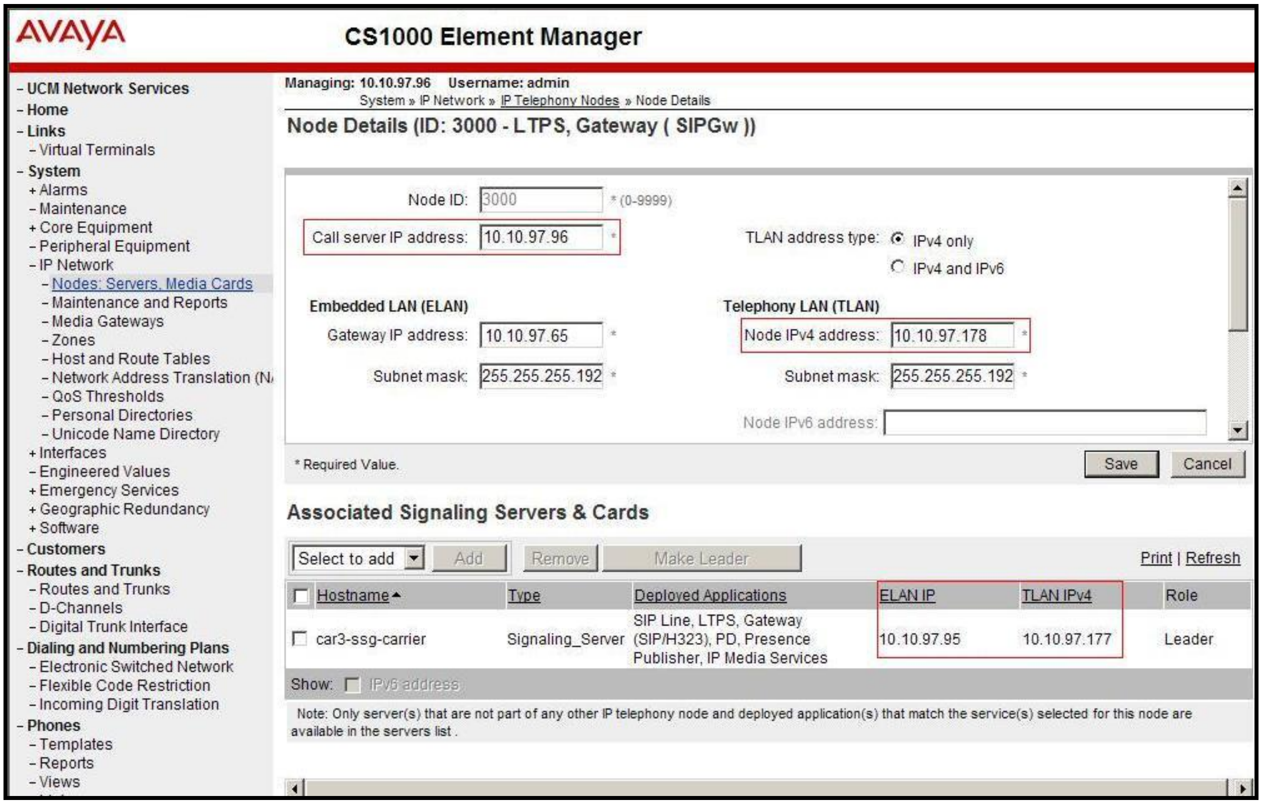

Figure 7 –Node Details 1

The **Node Details** screen is displayed in **Figure 8** with the IP Telephony Node Properties and Applications.

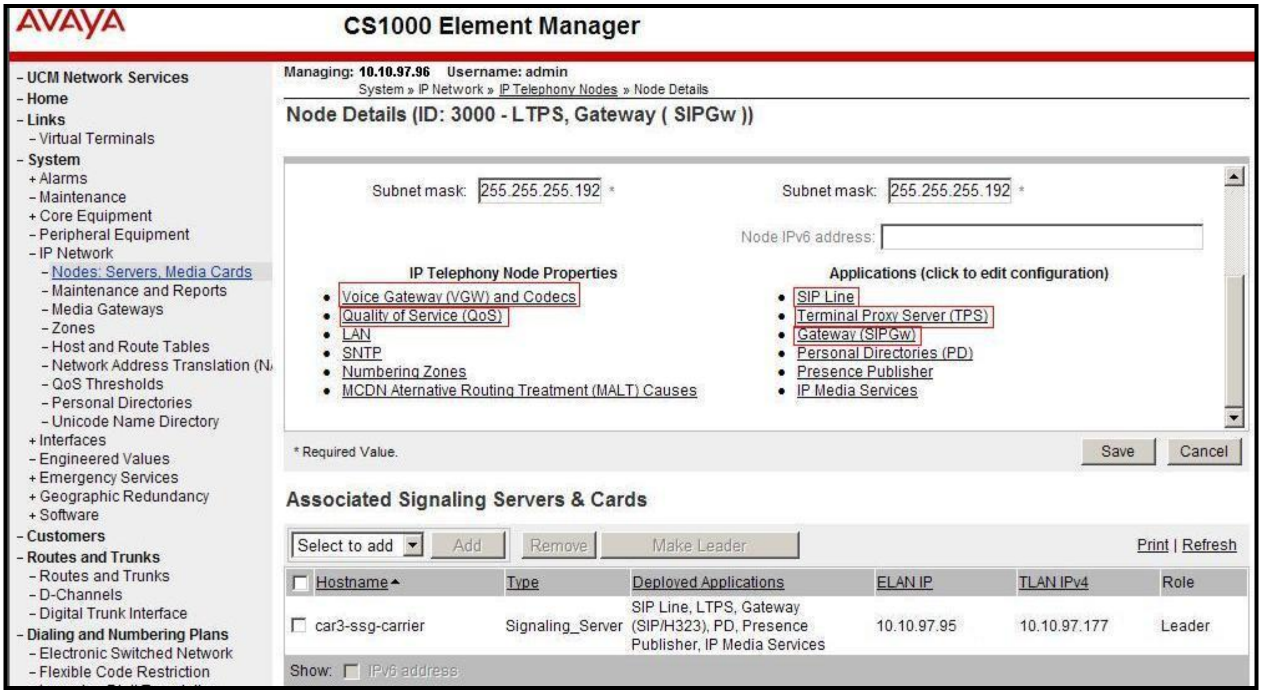

Figure 8 –Node Details 2

5.2.2. Administer Terminal Proxy Server (TPS)

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

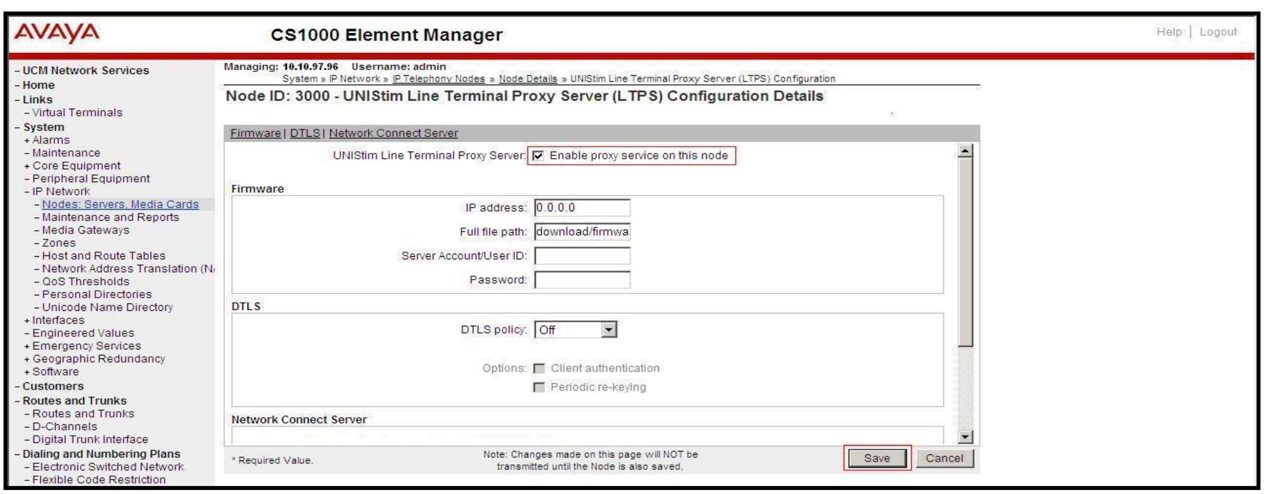

Figure 9 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

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

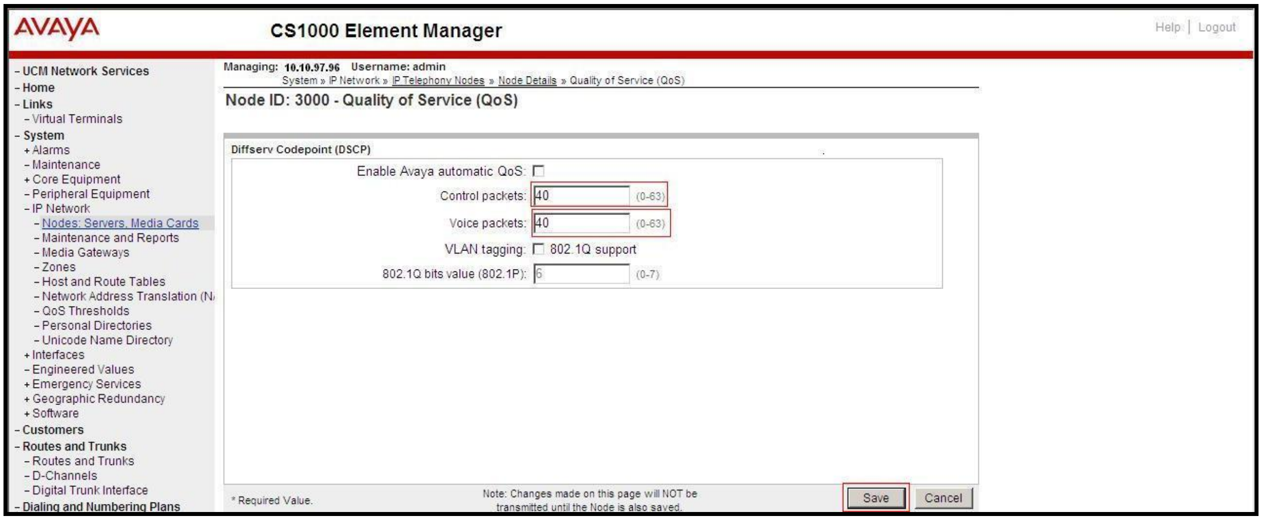

Figure 10 – QoS Configuration Details

5.2.4. Synchronize New Configuration

Continuing from **Section 5.2.3**, return to the **Node Details** page (**Figure 7**) and click on the **Save** button. The **Node Saved** screen is displayed. Click on **Transfer Now** (not shown). The **Synchronize Configuration Files (Node ID <3000>)** screen is displayed (not shown). Check the **Signaling Server** checkbox and click on **Start Sync** (not shown). When the synchronization completes, check the **Signaling Server** checkbox and click on the **Restart Applications** (not shown).

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec G.711

Select **IP Network → Nodes: Servers, Media Cards** from the left pane and on the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed, (see **Section 5.2.1** for more details). On the **Node Details** page shown in **Figure 8**, click on **Voice Gateway (VGW) and Codecs**.
Bell Canada supports **G.711/time 20ms** with **Voice Activity Detection (VAD)** checkbox unchecked. Click on the **Save** button.

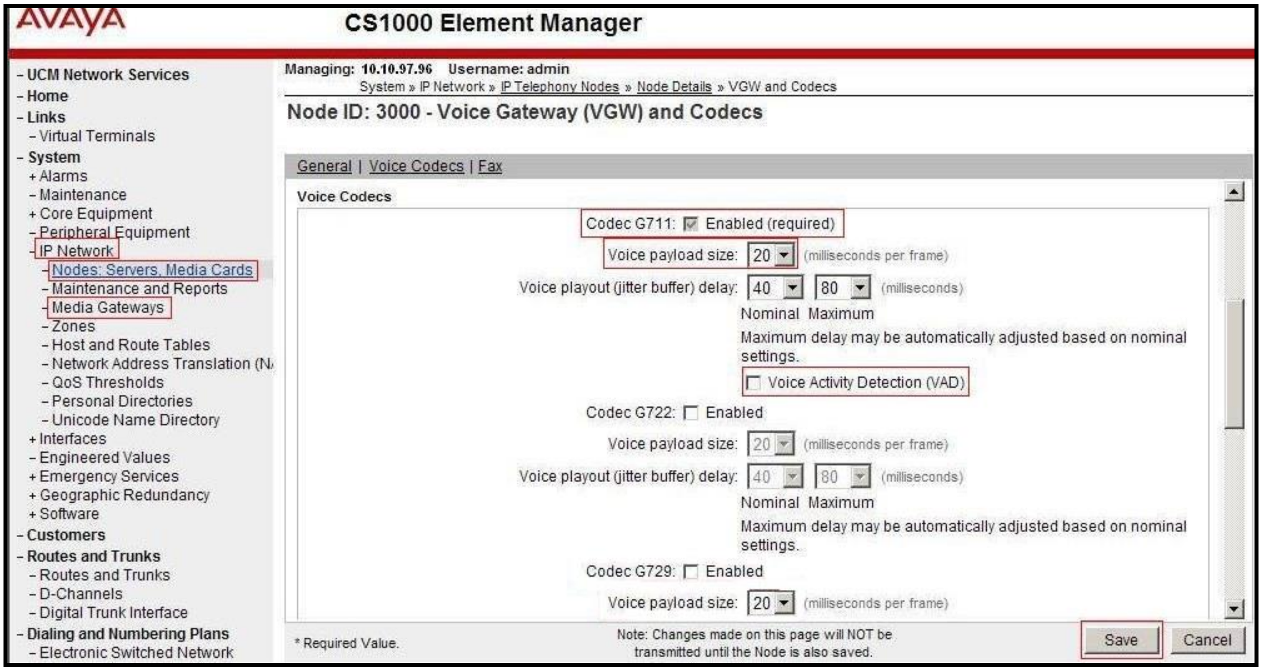

Figure 11 – Voice Gateway and Codec Configuration Details

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 11**, select **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 G.711** and uncheck **VAD** as shown in **Figure 12**. Scroll down to the bottom of the page and click on the **Save** button (not shown).

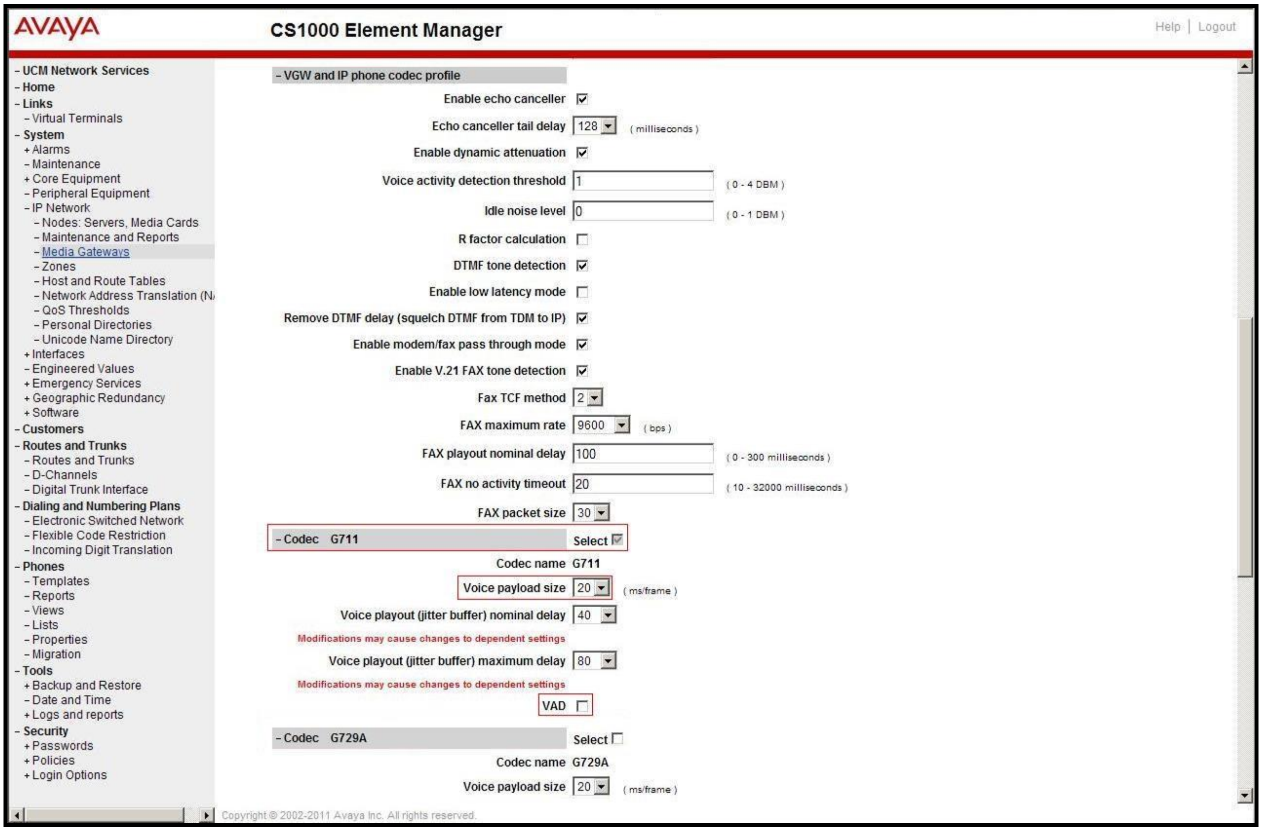

Figure 12 – Media Gateways Configuration Details

5.4. Zones and Bandwidth Management

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

5.4.1. Create a 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 **IP Network → Zones** from the left pane (not shown), click on **Bandwidth Zones** as shown in **Figure 13**.

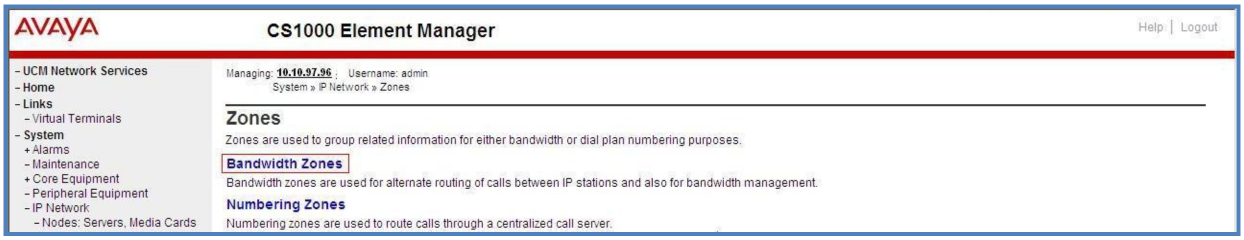

Figure 13 – Zones Page

The **Bandwidth Zones** screen is displayed as shown in **Figure 14**. Click **Add** to create a new zone for IP Phones.

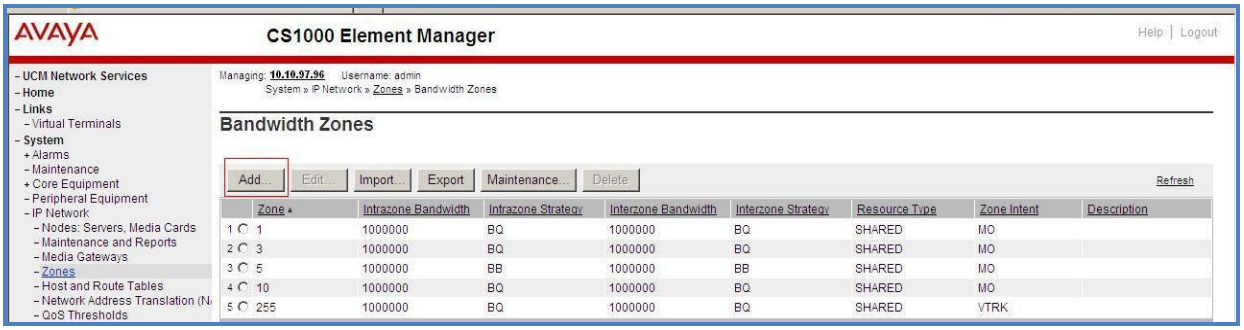

Figure 14 – Bandwidth Zones

Select and input the values as shown below (in the red boxes) in **Figure 15**, and click on the **Submit** button.

- **Intrazone Bandwidth (INTRA_BW): 1000000**
- **Intrazone Strategy (INTRA_STGY):** Set codec for local calls. 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 Quality (BQ)** to use G.711 as the first priority codec for negotiation.
- **Zone Intent (ZBRN):** Select **MO (MO)** for IP phones, and VGW.

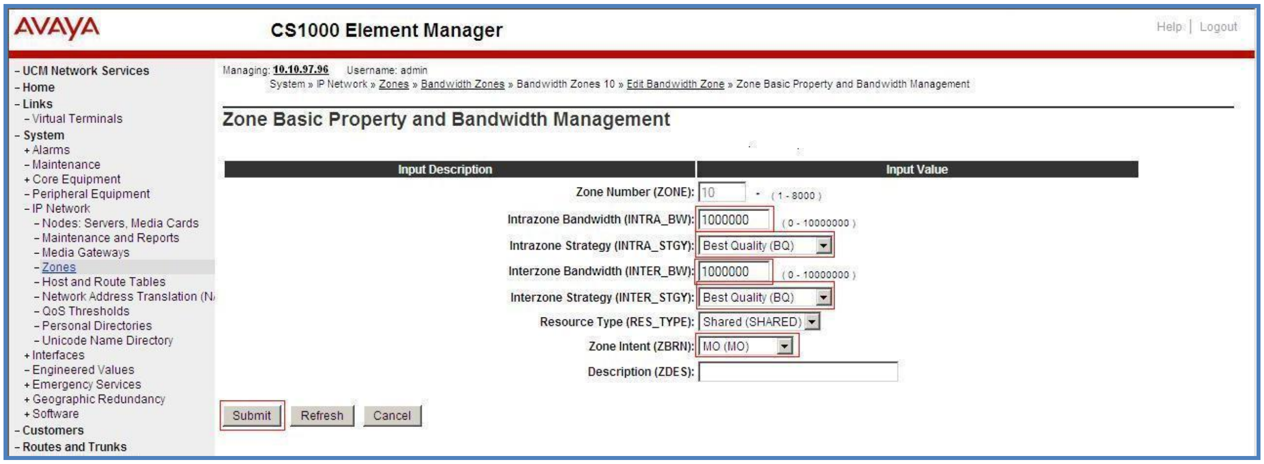

Figure 15 – Bandwidth Management Configuration Details – IP phone

5.4.2. Create a 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** for virtual trunk as shown in **Figure 16** and then click on the **Submit** button.

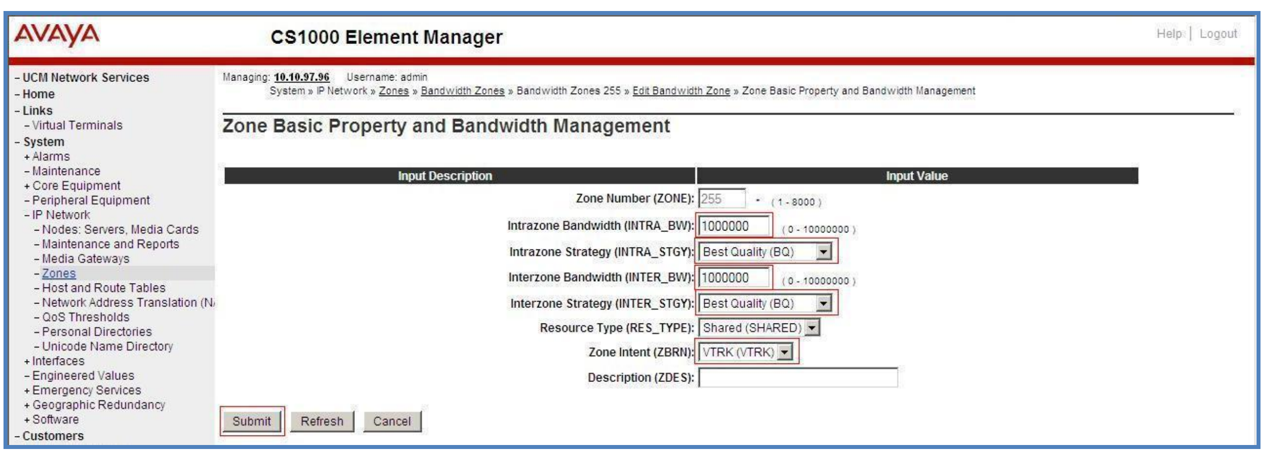

Figure 16 – Bandwidth Management Configuration Details – Virtual SIP trunk

5.5. Administer SIP Trunk Gateway

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

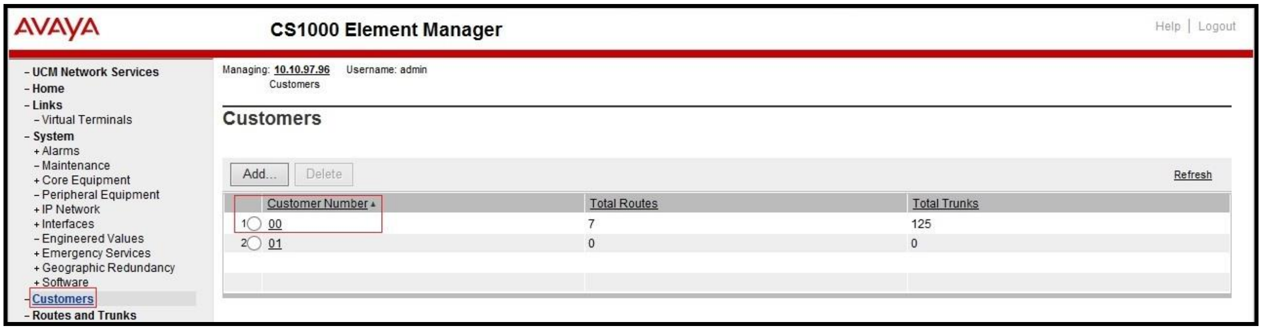

Figure 17 – Customer – ISDN Configuration 1

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.

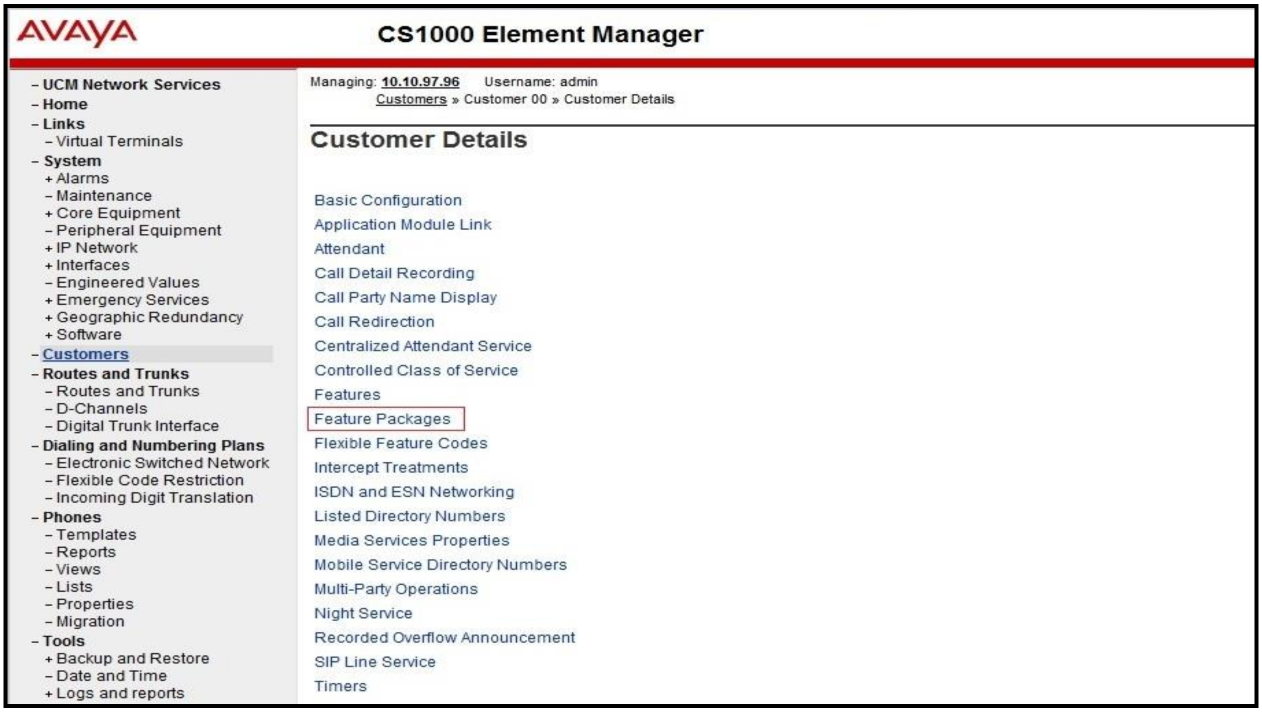

Figure 18 – Customer – ISDN Configuration 2

The screen is updated with a listing of available **Feature Packages** (not all features are shown in **Figure 19** 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).

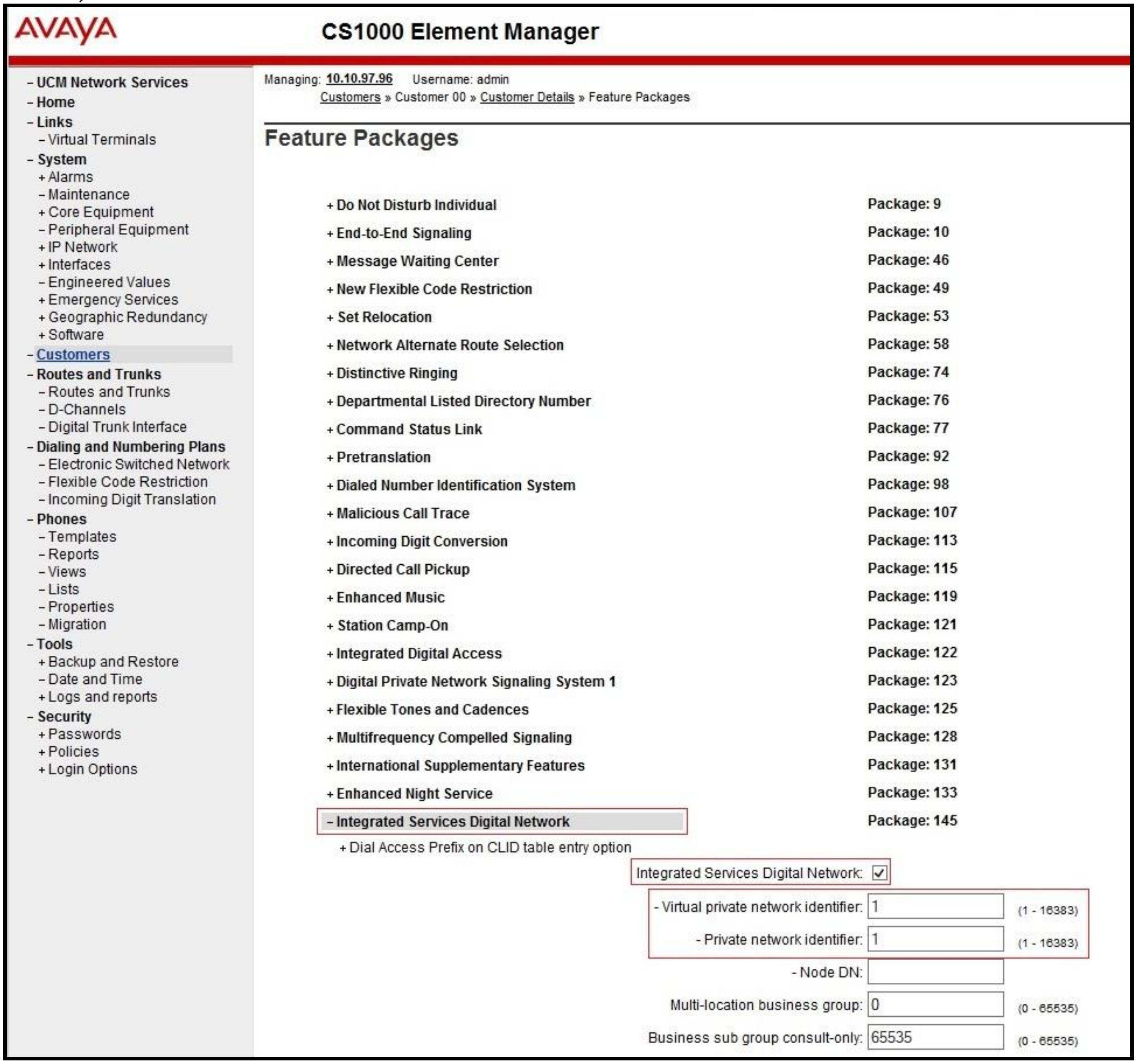

Figure 19 – Customer – ISDN Configuration 3

5.5.2. Administer SIP Trunk Gateway to Avaya Communication Server 1000

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

On the **Node Details** screen, select **Gateway (SIPGw)**. Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 20**. The **SIP domain name** and **Local SIP port** should be matched in the configuration of SBCE (in **Section 6.2.4**, **6.2.7**, and **6.2.9**).

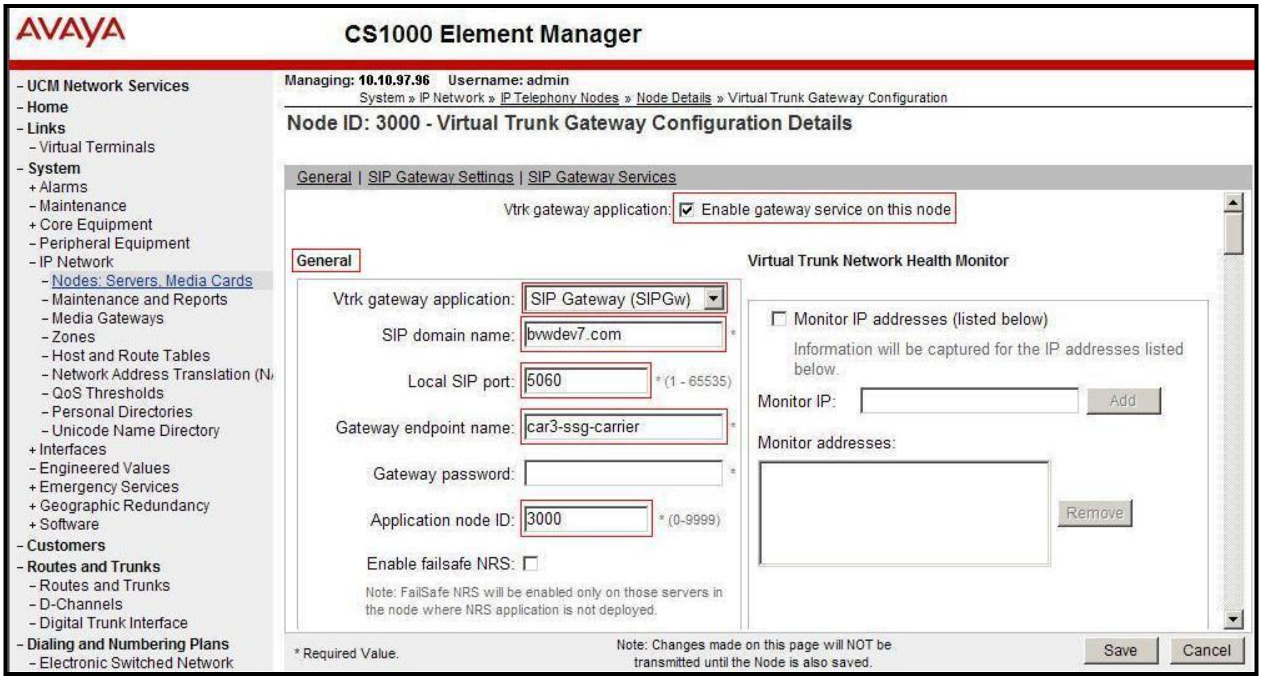

Figure 20 – Virtual Trunk Gateway Configuration Details

Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, and enter the following values (highlighted in red boxes) for the specified fields, retaining the default values for the remaining fields as shown in **Figure 21**. Enter the internal IP address of SBCE in the **Primary TLAN IP address** field. Enter **Port**: **5060** and **Transport protocol**: **UDP**. Uncheck **Support registration** checkbox.

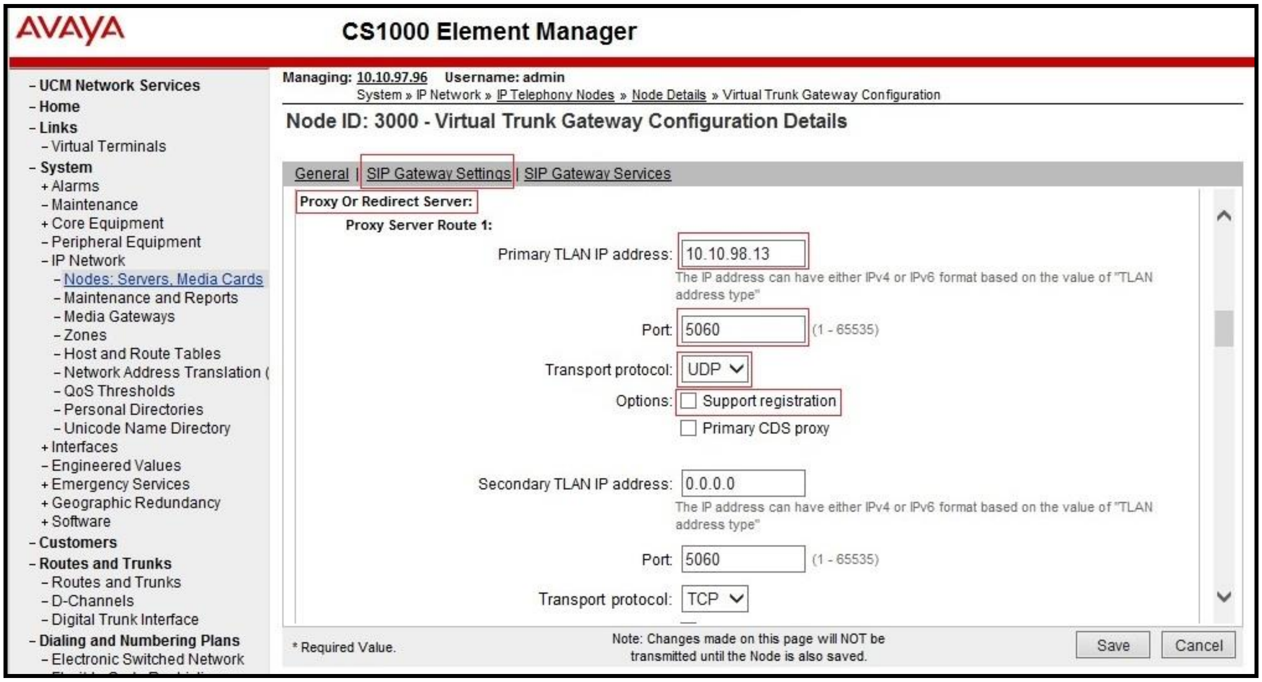

Figure 21 – Virtual Trunk Gateway Configuration Details

On the same page as shown in **Figure 21**, scroll down to the **SIP URI Map** section. Under the **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 the **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 22**. Then click on the **Save** button.

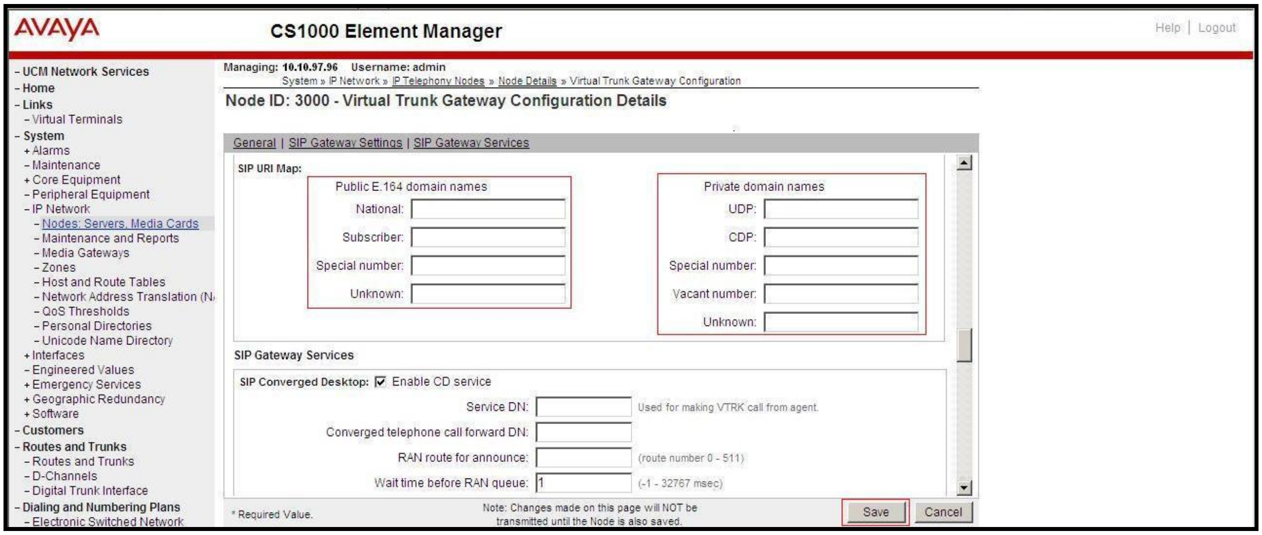

Figure 22 – Virtual Trunk Gateway Configuration Details

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 23**. Click on the **to Add** button.

Figure 23 – D-Channels

The **D-Channels 100 Property Configuration** screen is displayed next, as shown in **Figure 24**. 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 as shown in **Figure 24**. Other fields are left as default.

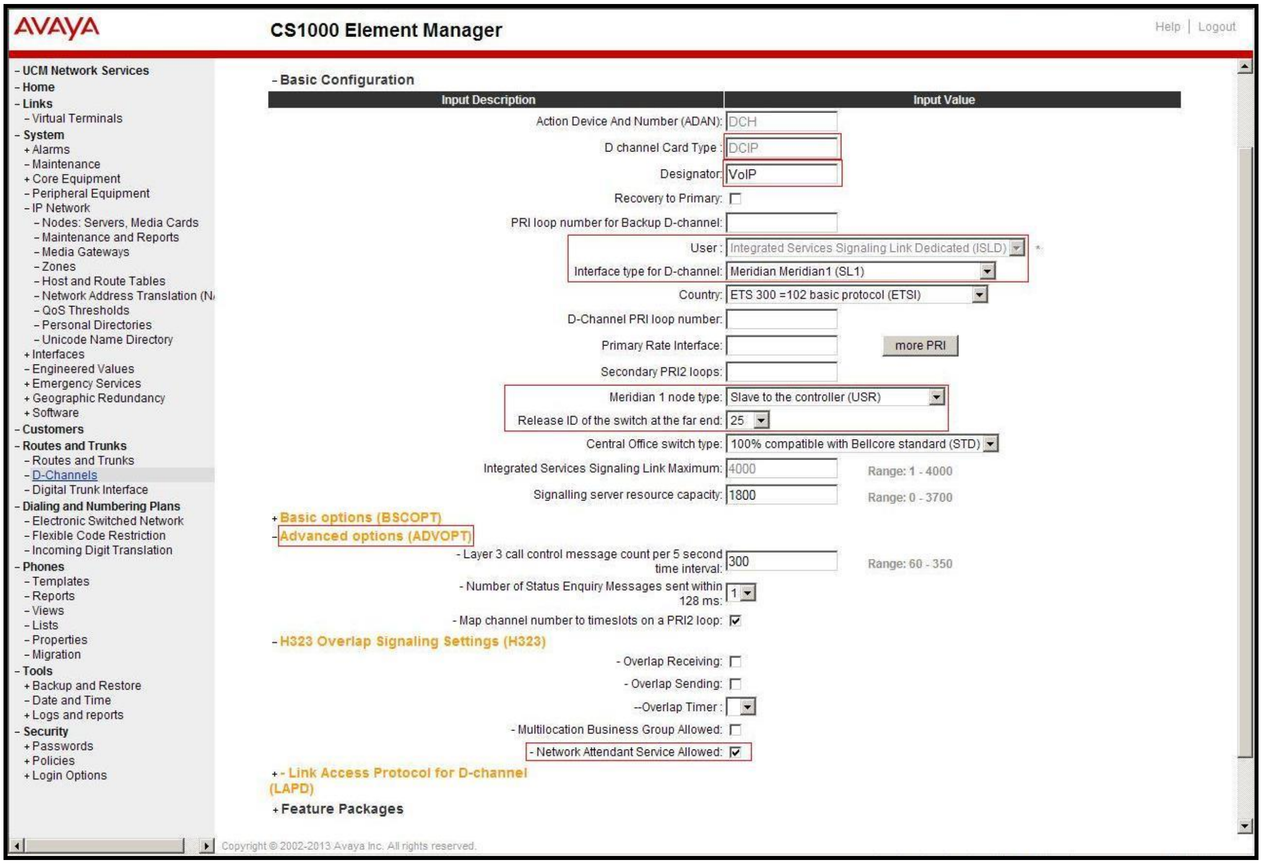

Figure 24 – D-Channel Configuration

Click on the **Basic Options (BSCOPT)** and click on the **Edit** button on the **Remote Capabilities** field as shown in **Figures 25**.

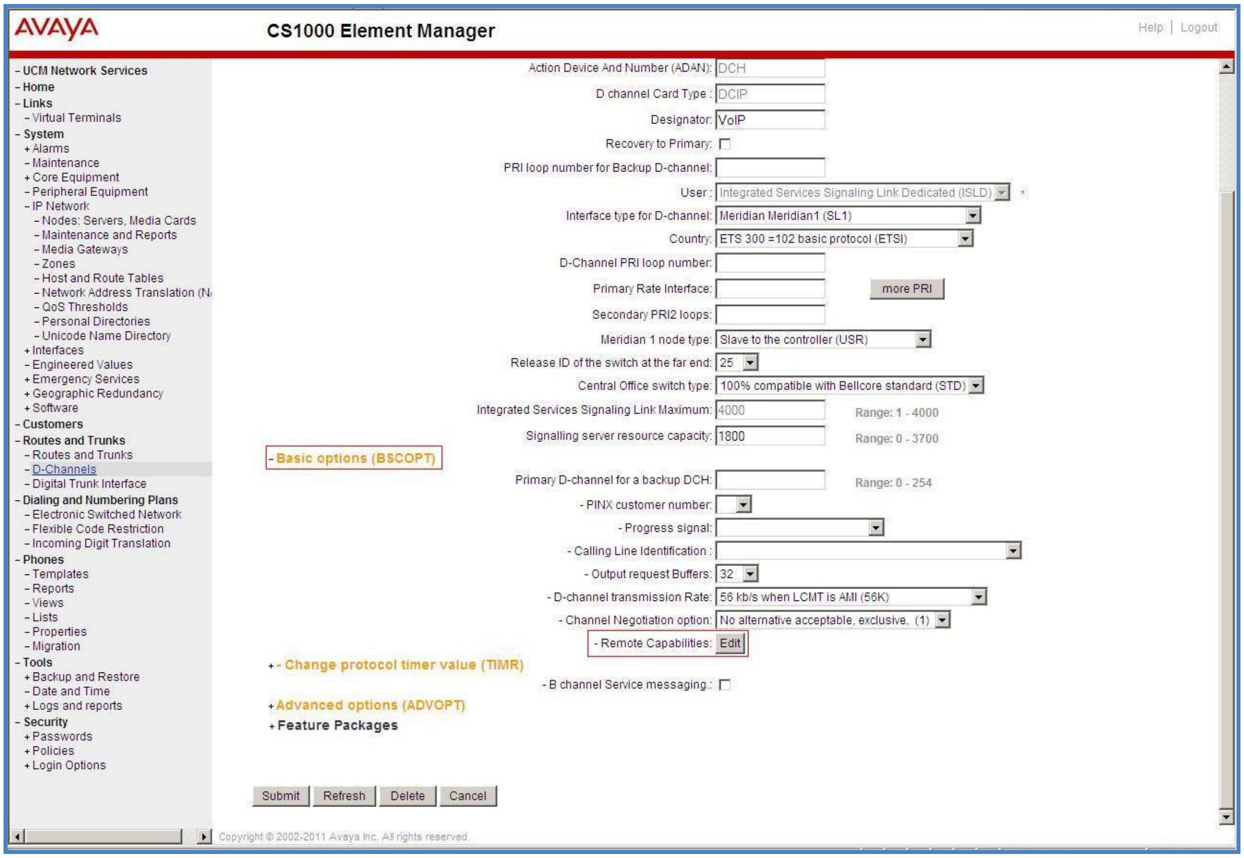

Figure 25 – D-Channel Configuration

The **Remote Capabilities Configuration** page appears as shown in **Figures 26**. Check on the **ND2** and the **MWI** checkboxes.

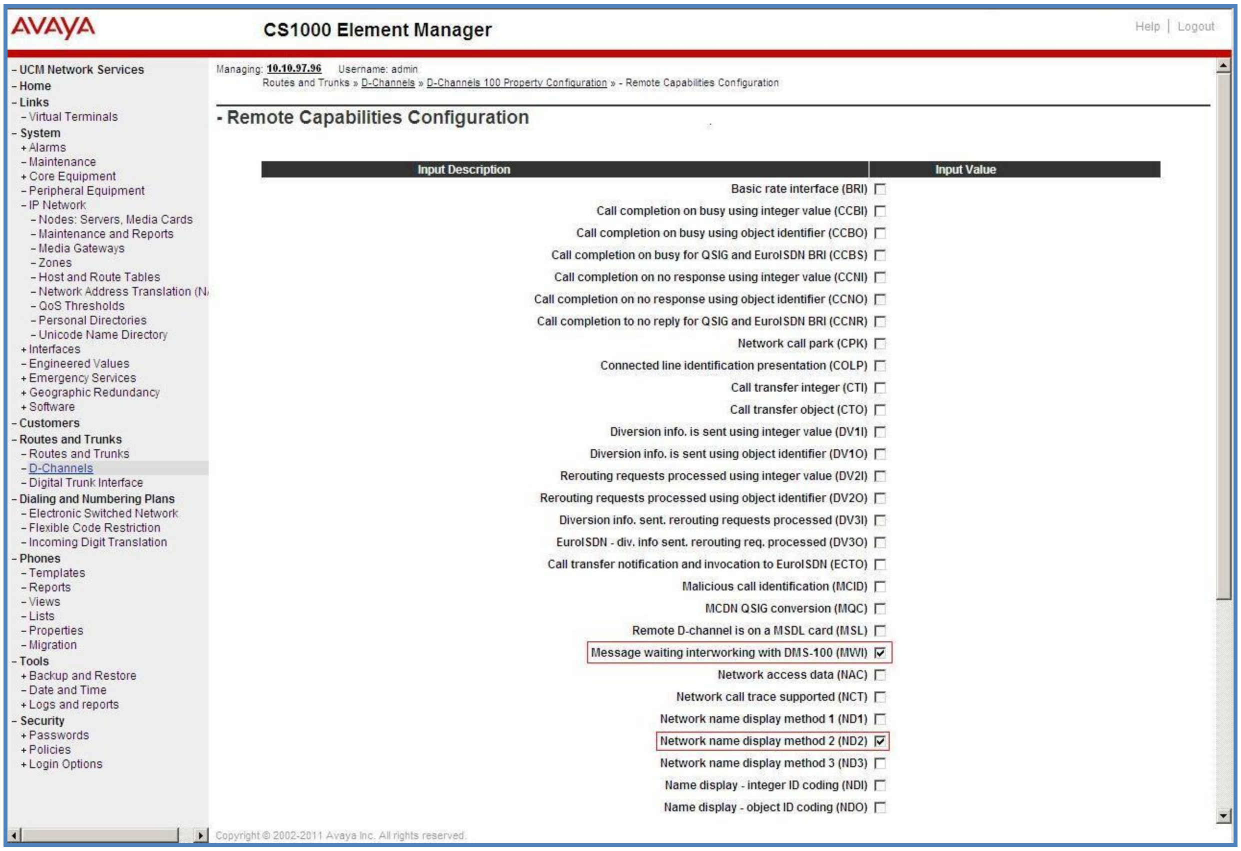

Figure 26 – Remote Capabilities Configuration

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

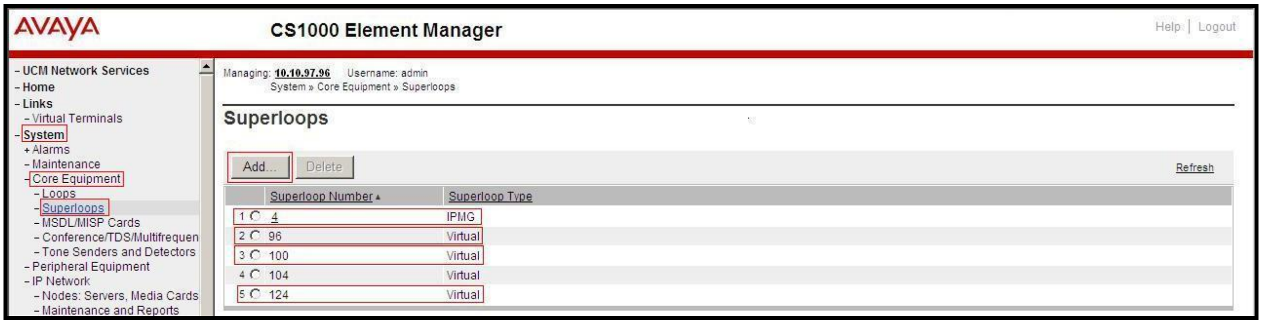

Figure 27 – Administer Virtual Super-Loop Page

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 28**.

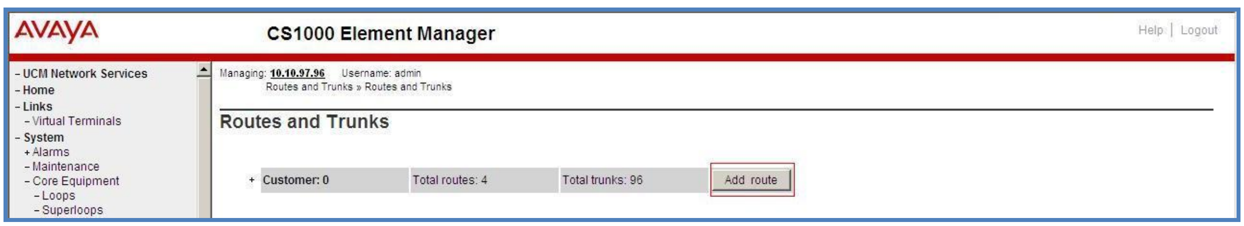

Figure 28 – Add route

The **Customer 0, New Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed to put 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 **Figures 29**.

- **Route data block (RDB)(TYPE)**: **RDB** as default.
- **Customer number (CUST)**: **0** as customer 0 is in used.
- **Route number (ROUT)**: Select an available route number (example: route **100**).
- **Designator field for trunk (DES)**: A descriptive text (**100**).
- **Trunk type (TKTP)**: TIE trunk data block (**TIE**)
- **Incoming and outgoing trunk (ICOG)**: **Incoming and Outgoing** (**IAO**)
- **Access code for the trunk route (ACOD)**: An available access code (example: **8100**).

- Check the **The route is for a virtual trunk route (VTRK)** field, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter **255** (created in **Section 5.4.2**). **Note:** The Zone value is filled out as 255, but after it is added, the screen is displayed with prefix 00.
- For the **Node ID of signaling server of this route (NODE)** field, enter the node number **3000** (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Scrolling down to the bottom of the screen, enter the following values for the specified fields, and retain the default values for the remaining fields.
  - **Mode of operation (MODE)**: Select **Route uses ISDN Signalling Link** (**ISLD**)
  - **D channel number (DCH)**: Enter **100** (created in **Section 5.5.3**).
  - **Interface type for route (IFC)**: Select **Meridian M1 (SL1)**.
  - **Private network identifier (PNI)**: Enter **1**. **Note:** The value is filled out as 1, but after it is added, the screen is displayed with prefix 0000.
  - **Network calling name allowed (NCNA)**: Check thisoption to allow calling name displayed.
  - **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**).

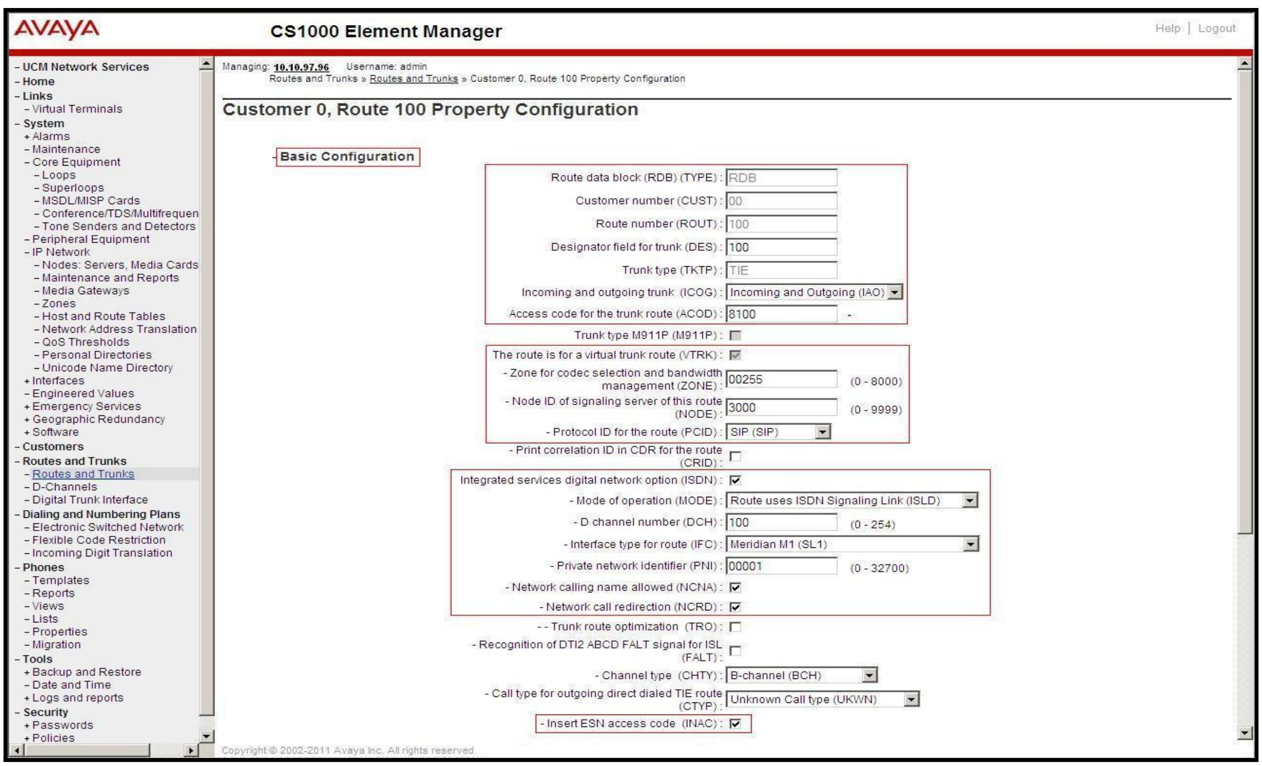

Figure 29 – Route Configuration 1

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 30**.
Click on the **Submit** button.

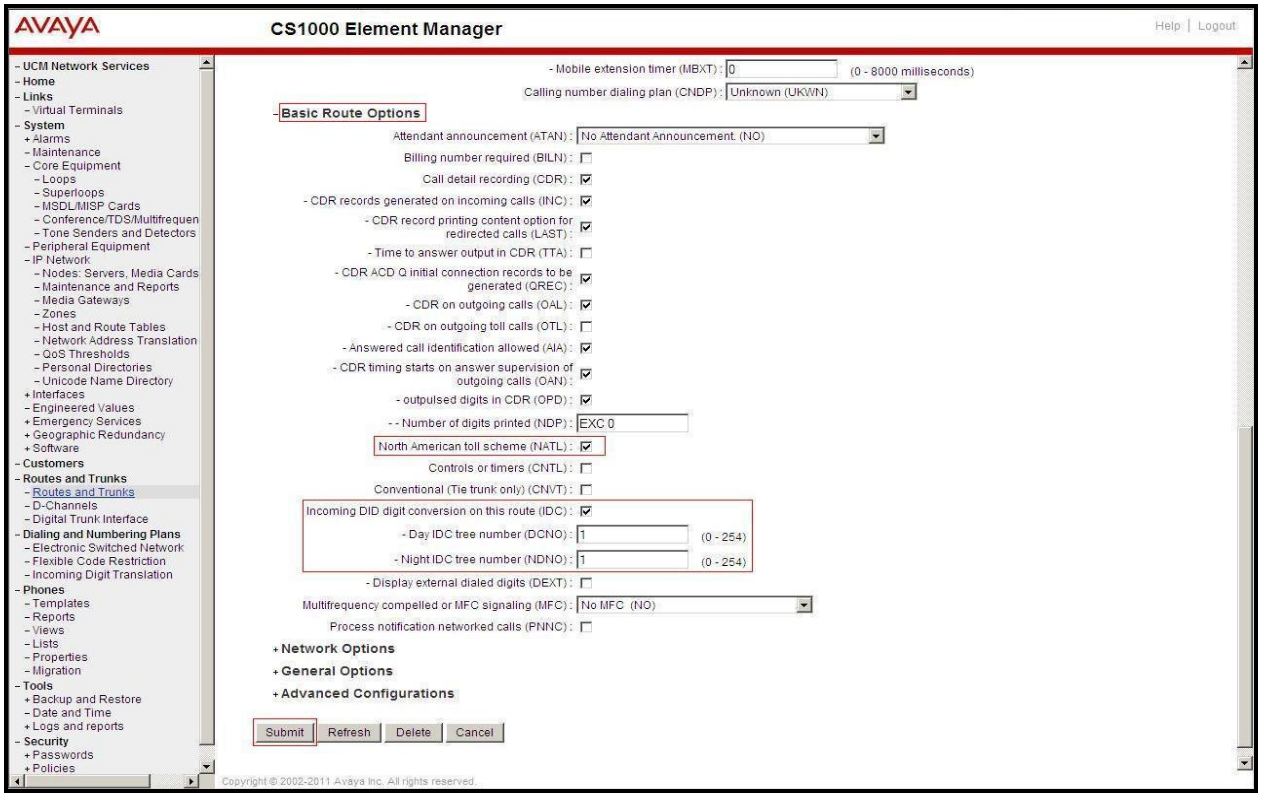

Figure 30 – Route Configuration 2

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 the example, the Route 100 was being added. Click on the **Add trunk** button as shown in **Figure 31**.

Figure 31 – 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. The 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 32**.

Note: The Multiple trunk input number (MTINPUT) field 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**: Immediate (**IMM**)
- **Start arrangement Outgoing**: Immediate (**IMM**)
- **Trunk group access restriction**: Desired trunk group access restriction level
- **Channel ID for this trunk**: An available starting channel ID

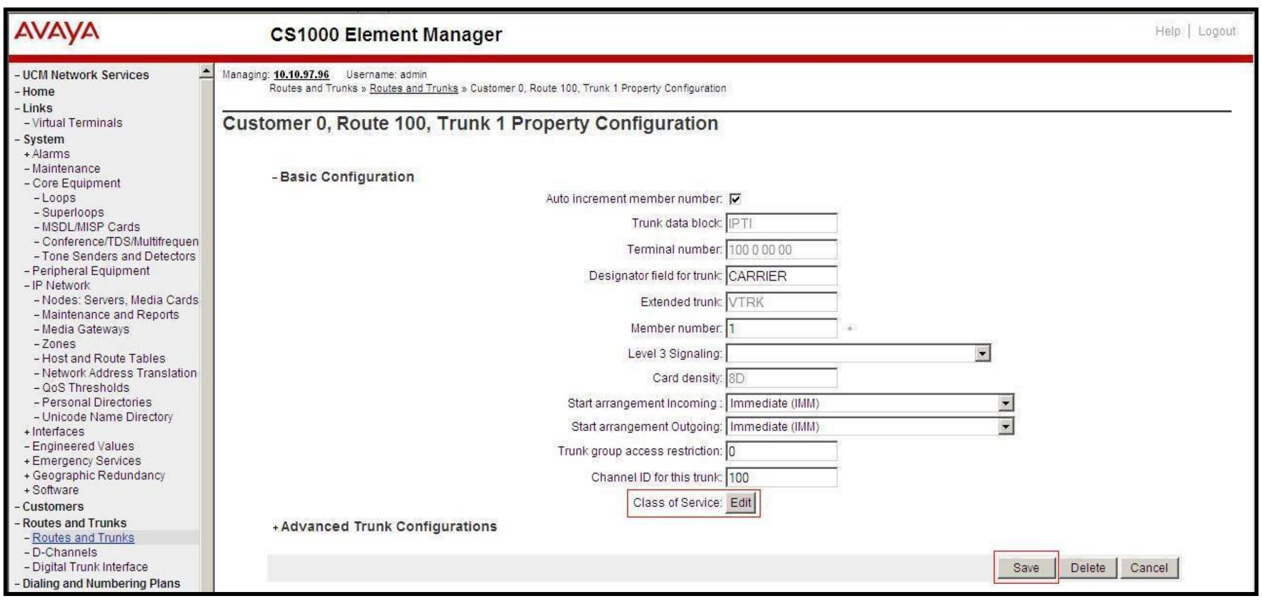

Figure 32 – New Trunk Configuration

For **Media Security**, select **Media Security Never** (**MSNV)**. Enter the values for the specified fields as shown in **Figure 33**. Scroll down to the bottom of the screen and click **Return Class of Service** and click on the **Save** button (shown in **Figure 32**).

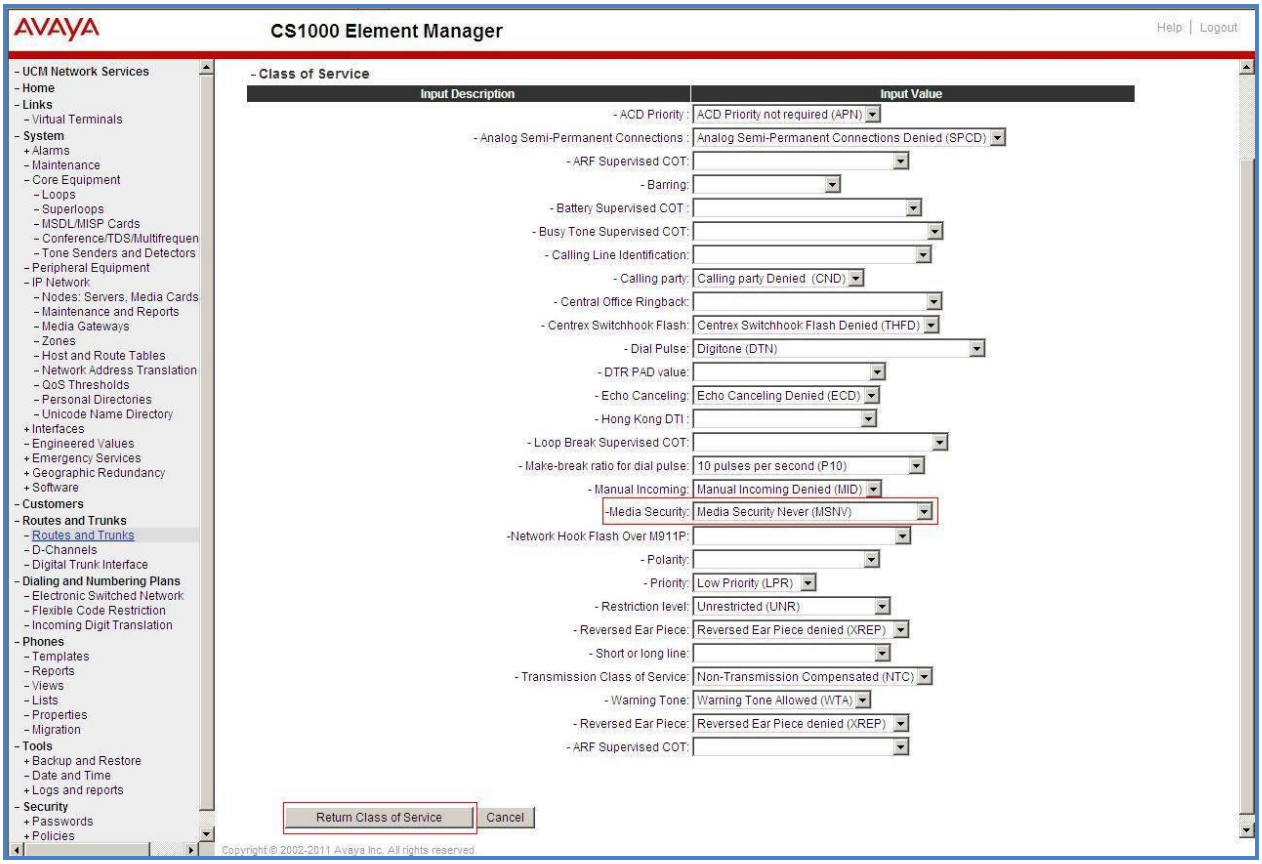

Figure 33 – Class of Service Configuration

5.5.7. Administer Calling Line Identification Entries

Select **Customers → 00 → ISDN and ESN Networking** on the left pane. Click on **Calling Line Identification Entries** as shown in **Figure 34**.

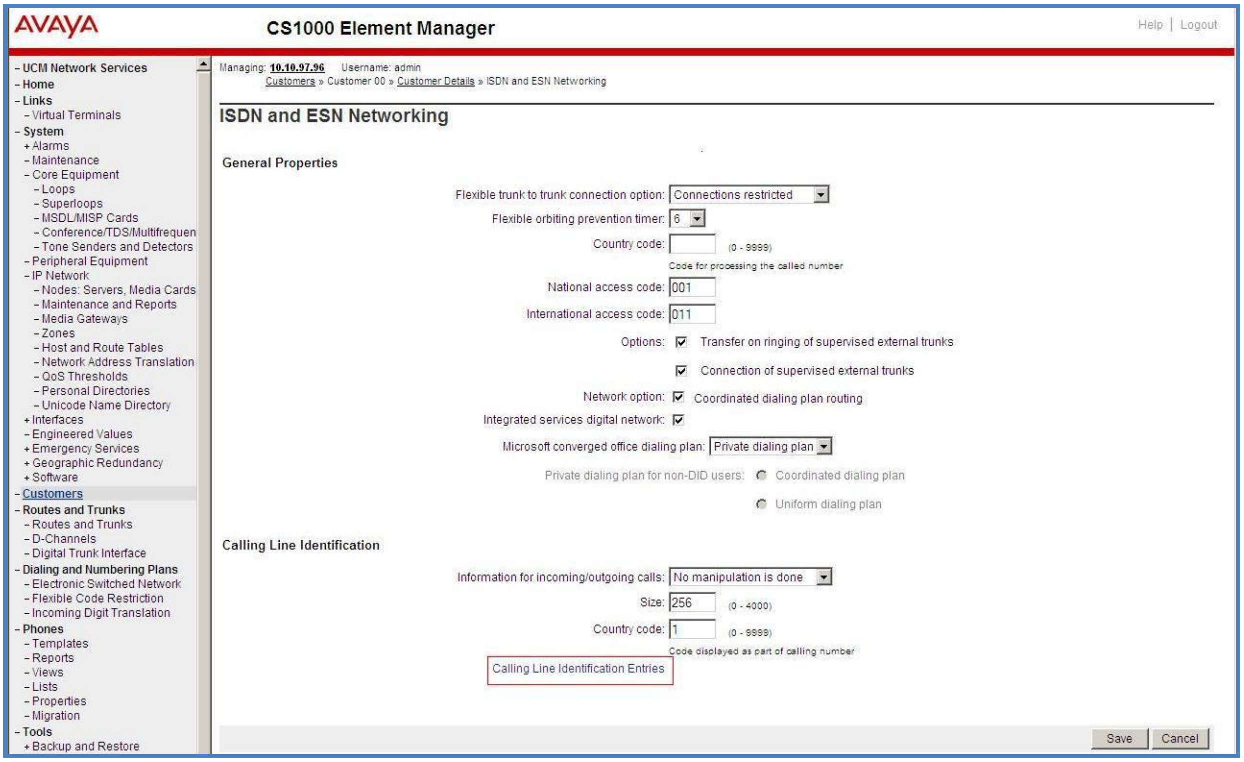

Figure 34 – ISDN and ESN Networking

Click on **Add** as shown in **Figure 35**.

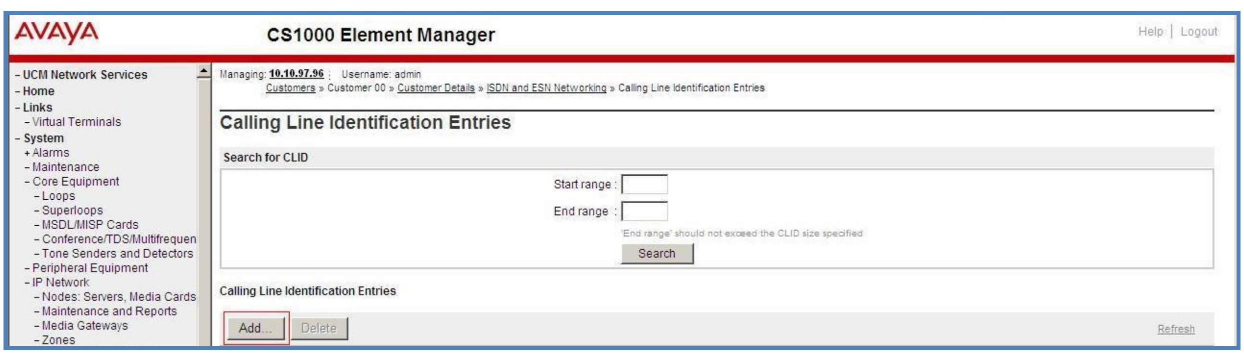

Figure 35 – Calling Line Identification Entries

The add entry **0** screen is displayed to put the following values for the specified fields and retain the default values for the remaining fields. The Edit Calling Line Identification of existing entry 0 is displayed as shown in **Figure 36**.

- **National Code**: leave it blank.
- **Local Code**: input prefix digits assigned by Bell Canada, in this case it is 6 digits – **416XXX**. 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, in this case it is 6 digits – **416XXX**. 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, in this case it is 6 digits – **416XXX**. 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**.

Click on the **Save** button as shown in **Figure 36**

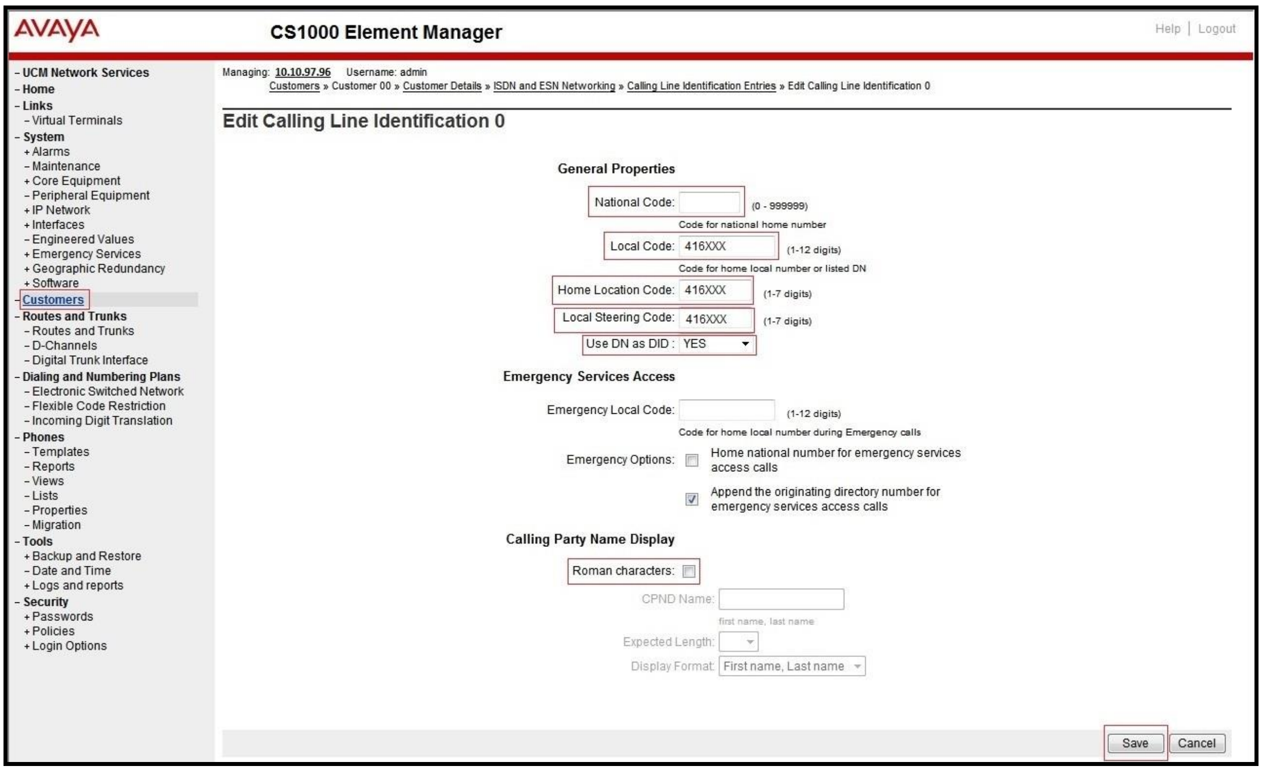

Figure 36 – Edit Calling Line Identification 0

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 37**.

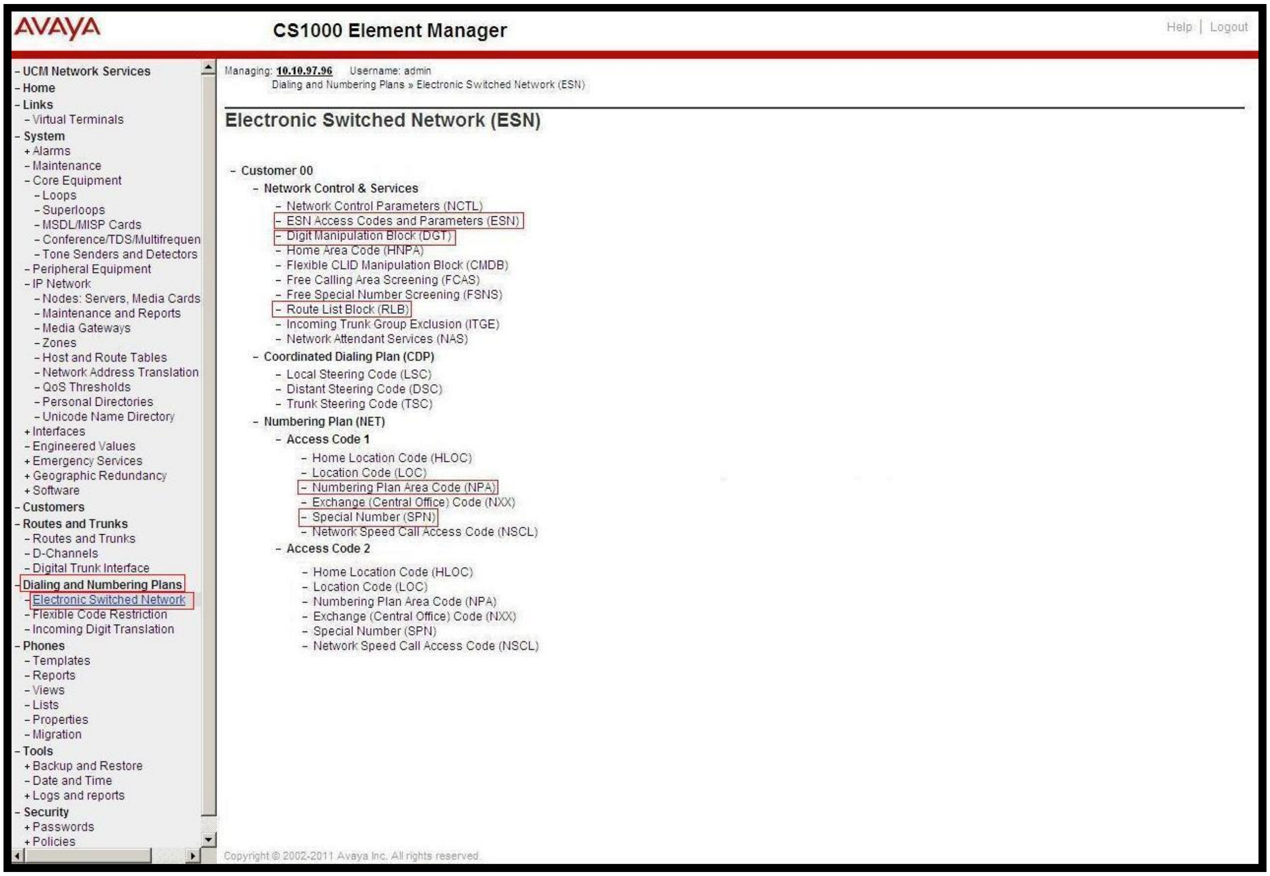

Figure 37 –ESN Configuration

On **Electronic Switched Network (ESN)** screen, select **ESN Access Codes and Basic Parameters** to define **NARS/BARS Access Code 1** as shown in **Figure 38**.

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

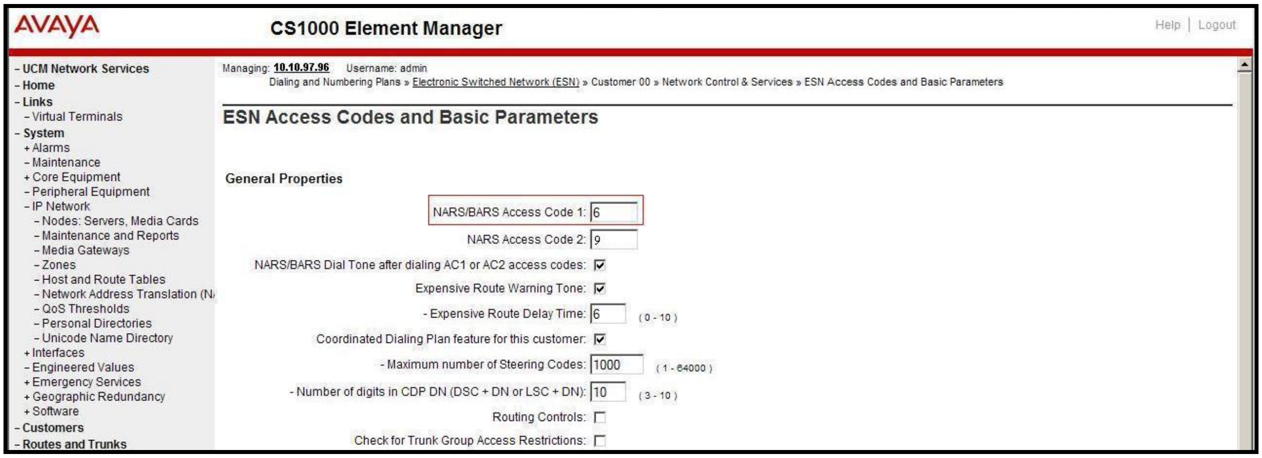

Figure 38 – ESN Access Codes and Basic Parameters

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)
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 List (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 37**. Select **Digit Manipulation Block (DGT)**. The **Digit Manipulation Block List** is displayed as shown in **Figure 39**. In the **Please choose the** field, select an available **Digit Manipulation Block Index** from the drop-down list, and click on the **to Add** button.

Figure 39 – Add a DMI

The DMI_14 screen will open. In this testing, no leading digits are to be deleted, therefore, enter **0** for the **Number of leading digits to be deleted** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits** and then click on **Submit** button as shown in **Figure 40**.

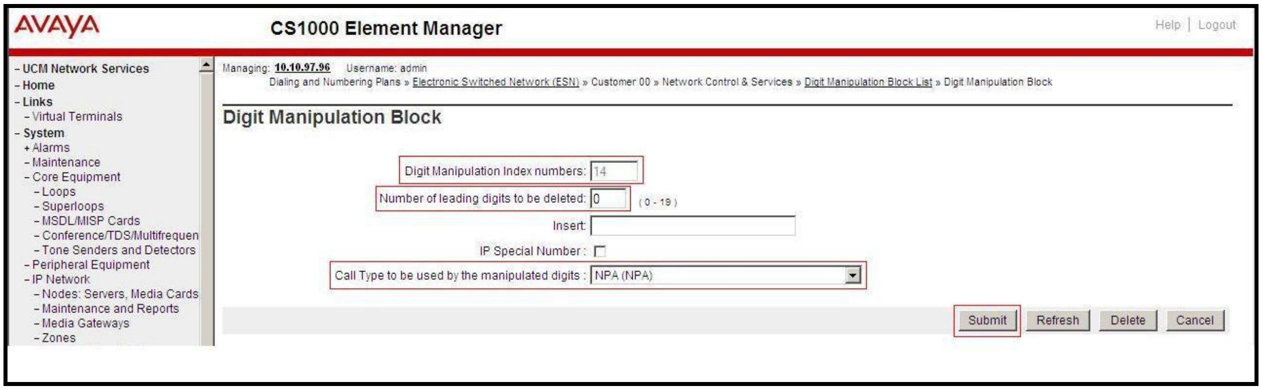

Figure 40 – DMI_14 Configuration

5.6.4. Route List Block (RLB) (RLB 14)

This session shows how to add a RLB 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 37**. Select **Route List Block (RLB)**.

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 41**. The screen shown in **Figure 42** will open.

Figure 41 – Add a Route List Block

Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 42**). 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**)

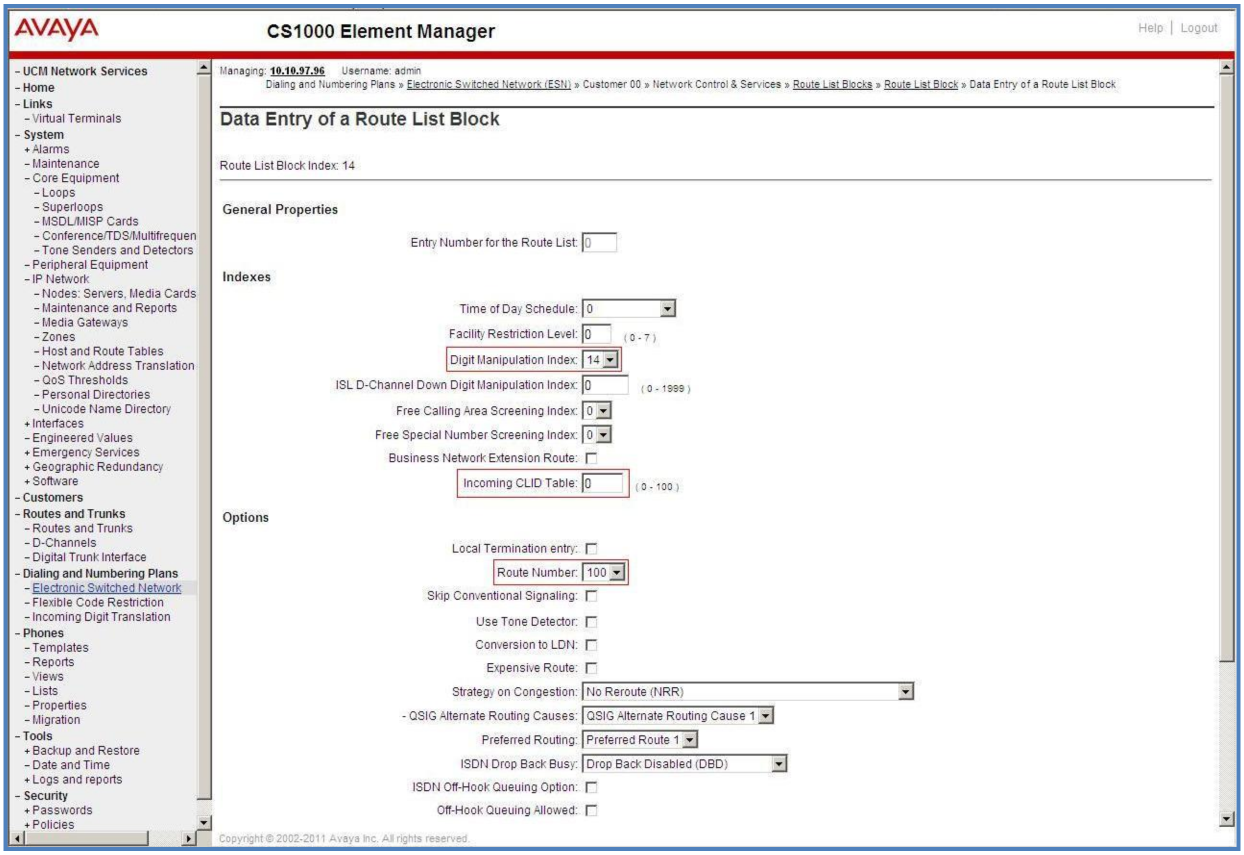

Figure 42 – RLB_14 Route List Block Configuration

5.6.5. Inbound Call – Incoming Digit Translation Configuration

This section describes the configuration steps required in order to receive calls from PSTN via the Bell Canada SIP Trunk 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 43**.

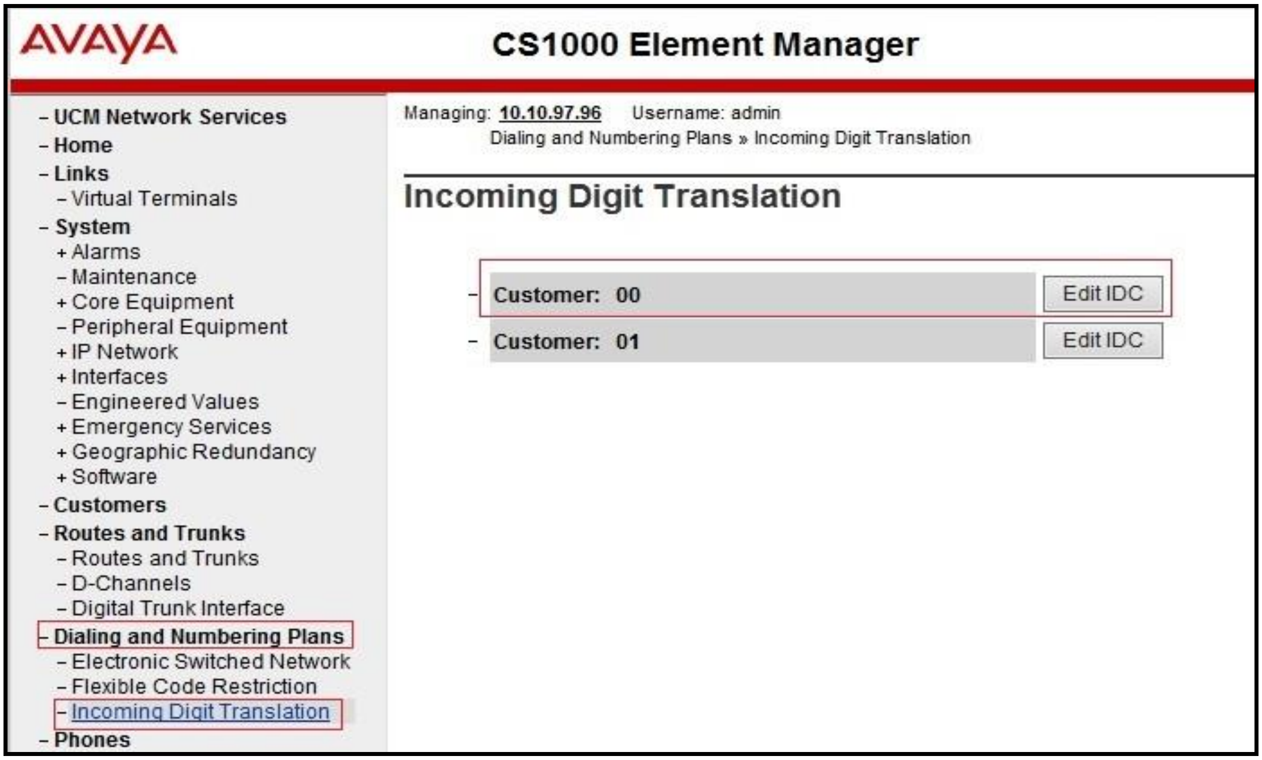

Figure 43 – Incoming Digit Translation

Click on the **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number 1** has been created as shown in **Figure 44**.

Figure 44 – Incoming Digit Conversion Property

Detail configuration of the Digit Conversion Tree Configuration is shown in **Figure 45**. 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 assigned to route 100 as shown in **Figure 30**.

In the following configuration, the incoming call from PSTN with DID with prefix 416XXX will be translated to the associated DN with 4 digits. DID number **416XXX1399** is translated to **1700** for voicemail testing purposes or to **1399** for Mobile Service Access DN number.

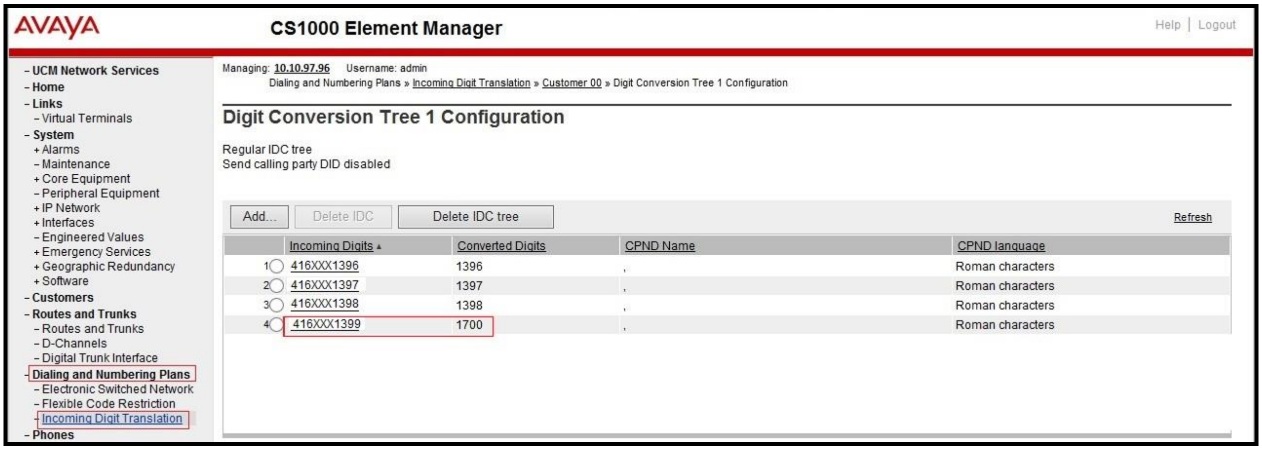

Figure 45 – Digit Conversion Tree

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.

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as show in **Figure 37**. Select **Special Number (SPN)**. Enter a SPN number and then click on **to Add** button. **Figure 46** shows all the special numbers used for this testing.

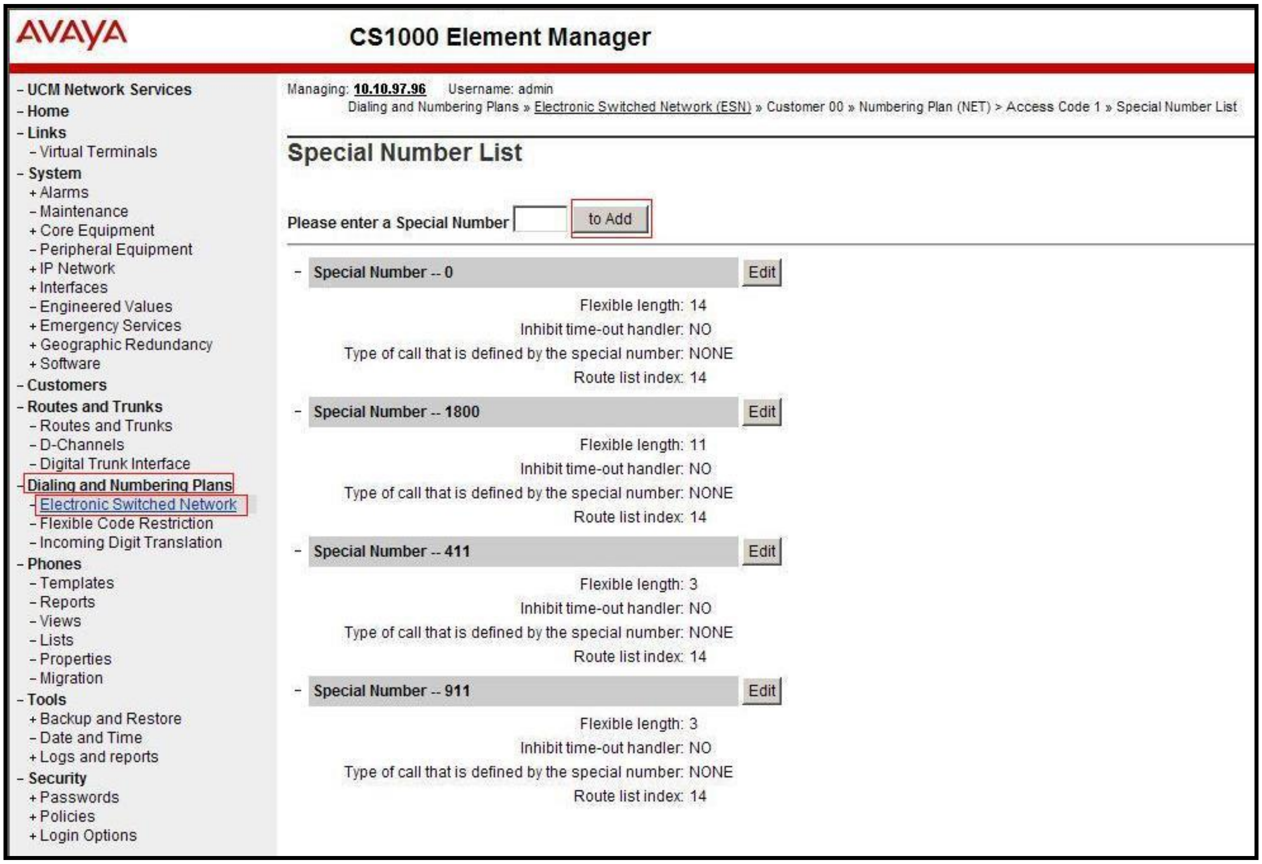

Figure 46 – Add a SPN

5.6.7. Outbound Call - Numbering Plan Area (NPA)

This section describes the creation of the 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 37**. Enter the area code desired in the textbox and click on the **to Add** button. The 1613, and 416 area codes were used in this configuration as shown in **Figure 47**.

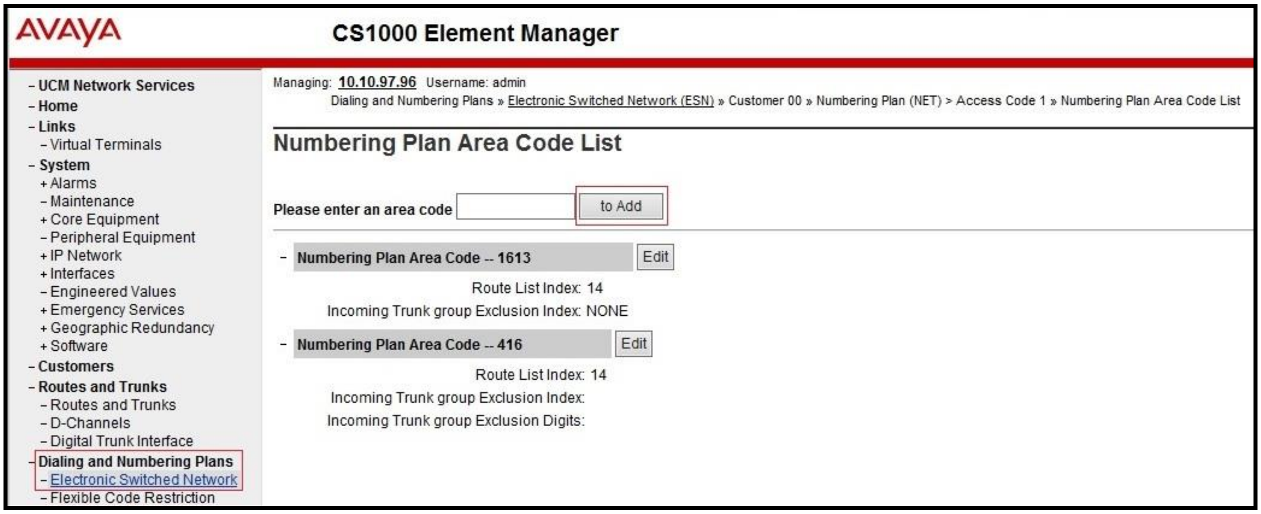

Figure 47 – Numbering Plan Area Code List

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 1397 0     MARP < --- Set the position of DN 1397 to display on key 0 of the phone
       CPND
         CPND_LANG ROMAN
           NAME Bell1 < --- 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) and 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.

```
>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.

```
>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 48**.

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

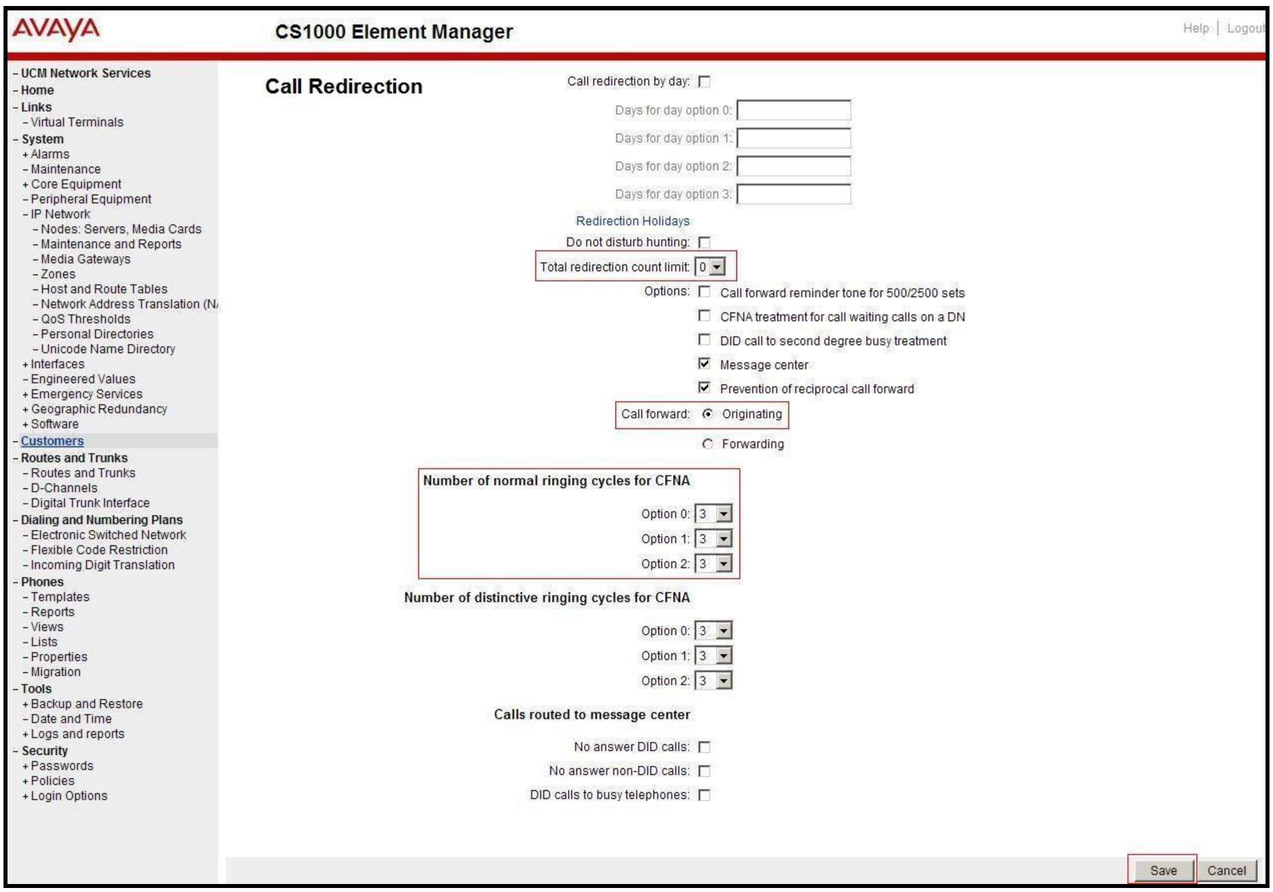

Figure 48 – Call Redirection

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 **61613XXX5205**.

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

ECHG yes
ITEM CLS CFXA SFA
ITEM key 19 CFW 16 61613XXX5205
```

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 has **CFB** enabled with forwarding number **61613XXX5205**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN   96 0 0 2
ECHG yes
ITEM CLS FBA HTA SFA
ITEM HUNT 61613XXX5205
ITEM FDN 61613XXX5205
```

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 **61613XXX5205**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN   96 0 0 2
ECHG yes
ITEM CLS FNA SFA
ITEM HUNT 61613XXX5205
ITEM FDN 61613XXX5205
```

6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the 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 SBCE has been installed and that network connectivity exists between the systems. For more information on SBCE, see **Section 10** of these Application Notes.

6.1. Log into 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 SBCE).

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

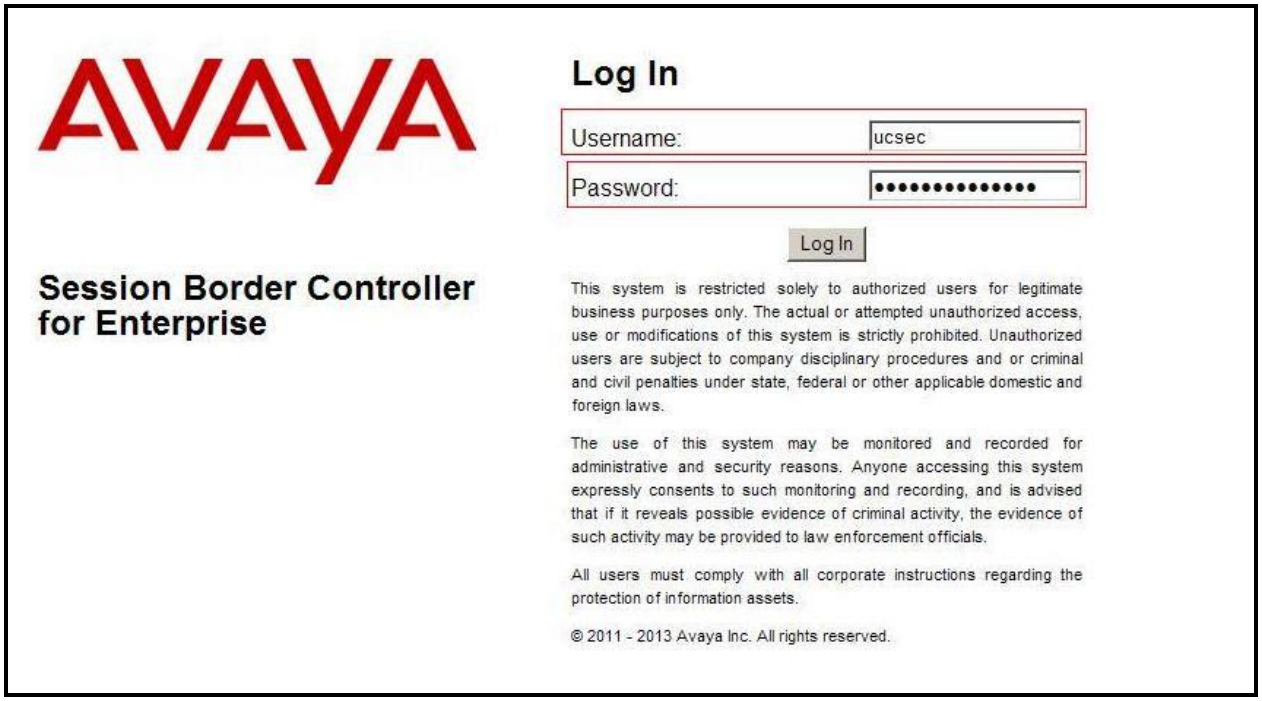

Figure 49 - SBCE Login

6.2. Global Profiles

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

6.2.1. Configure Server Interworking - Avaya site

Server Interworking allows one 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 → Add**

- Enter Profile name: **CS1K76**
- On the **General** tab, all options can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** tabs: All options can be left at default. Click **Finish** (not shown).

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

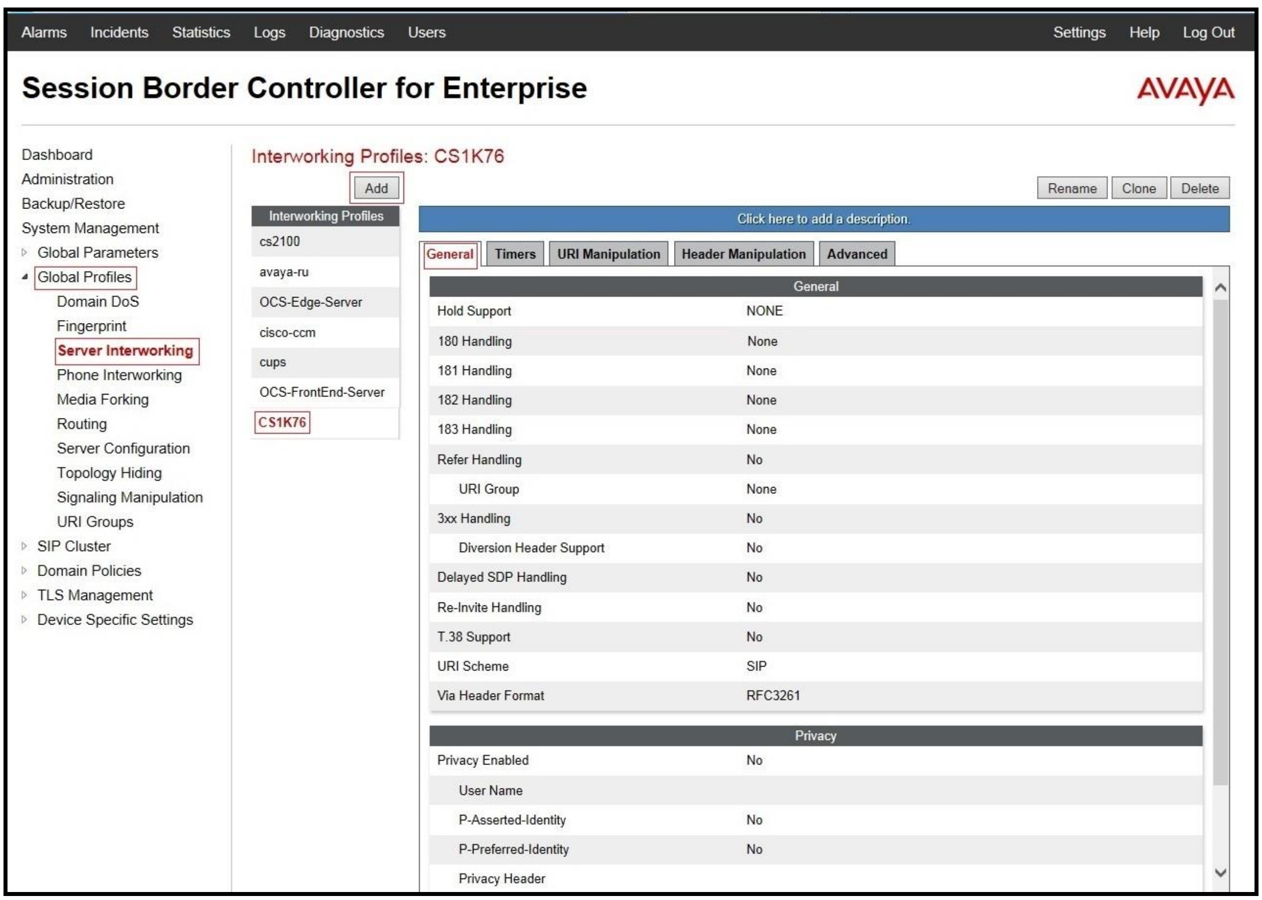

Figure 50 - Server Interworking – Avaya site

6.2.2. Configure Server Interworking – Bell Canada site

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

- Enter Profile name: **SP3**
- All options on the **General** tab can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** tabs: All options can be left at default. Click **Finish** (not shown).

The following screen is shown that Bell Canada server interworking (named: **SP3**) was added.

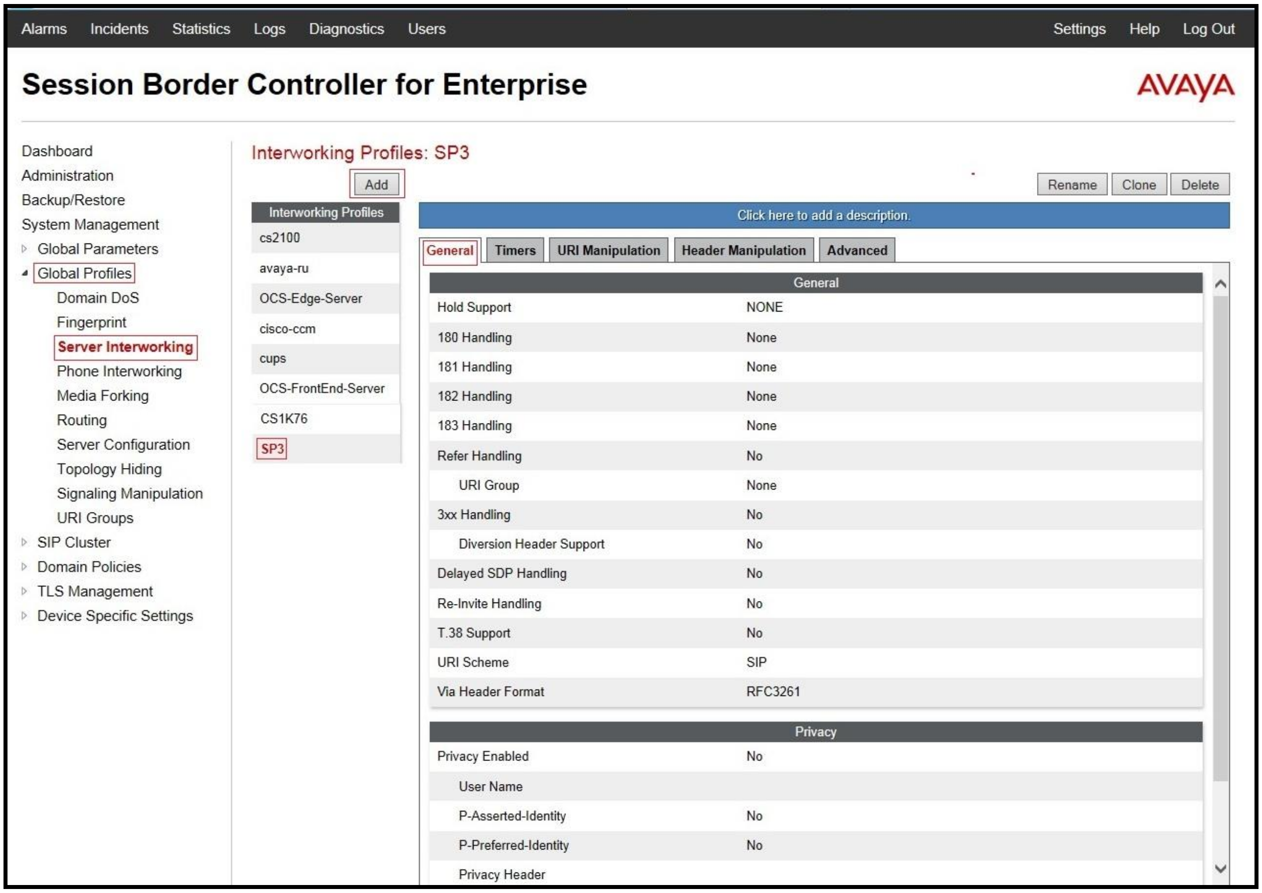

Figure 51 - Server Interworking – Bell Canada site

6.2.3. Configure URI Groups

The URI Group feature allows administrator to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group.

The following URI Group configuration is used for this specific testing in DevConnect Lab environment. The URI-Group named **SP3** was used to match the “From” and “To” headers in a SIP call dialog received from both Enterprise and Bell Canada SIP Trunk Service. If there is a match, the SBCE will apply the appropriate Routing profiles (see **Section 6.2.4, 6.2.5**), Server Flows (see **Section 6.4.4**), and Session Flow (see **Section 6.4.5**) to route incoming and outgoing calls to the right destinations. In production environment, there is not a requirement to define this URI.

From the menu on the left-hand side, select **Global Profiles → URI Groups**. Select **Add**.

- Enter Group Name: **SP3**.
- Edit the URI Type: **Regular Expression** (not shown).
- **Add** URI: **.*10\.10\.97\.178** (CS1000 Node IP address), **.*10\.10\.98\.111** (SBCE public interface IP address), .***10\.10\.98\.13** (SBCE internal interface IP address), **.*192\.168\.237\.201** (Bell Canada SIP Signaling server IP address**)**, **.*Avaya** (Receiving OPTIONS ping from Bell), .***anonymous\.invalid** (Anonymous URI**)**, **.*bvwdev7\.com** (Enterprise domain), **.*cust2-tor\.XXX\.bell\.ca** (Bell Canada domain), **.*sipXXX\.bell\.ca** (Bell Canada domain**)**.
- Click **Finish** (not shown).

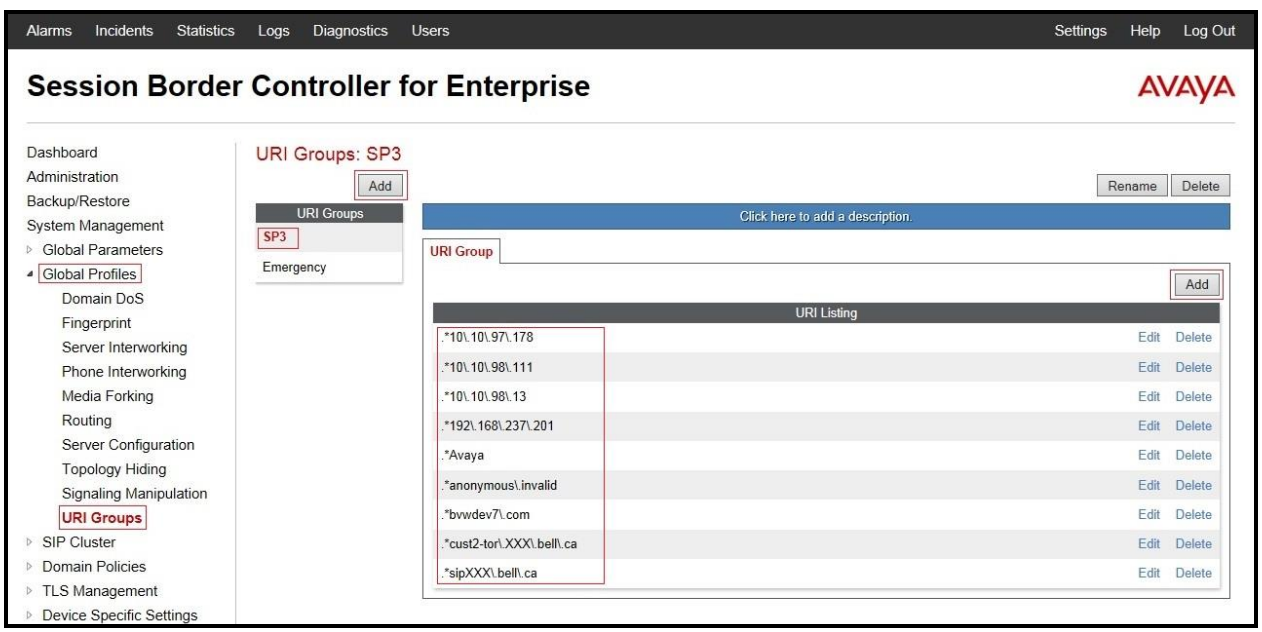

Figure 52 - URI Group

6.2.4. Configure Routing – Avaya site

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 → Add**
Enter Profile Name: **SP3_To_CS1K76**

- **URI Group**: **SP3** (Refer to **Section 6.2.3**).
- **Next Hop Server 1**: **10.10.97.178:5060** (CS1000 Node IP address)
- Check **Routing Priority based on Next Hop Server** (not shown)
- **Outgoing Transport**: **UDP** (not shown)
- Click **Finish** (not shown).

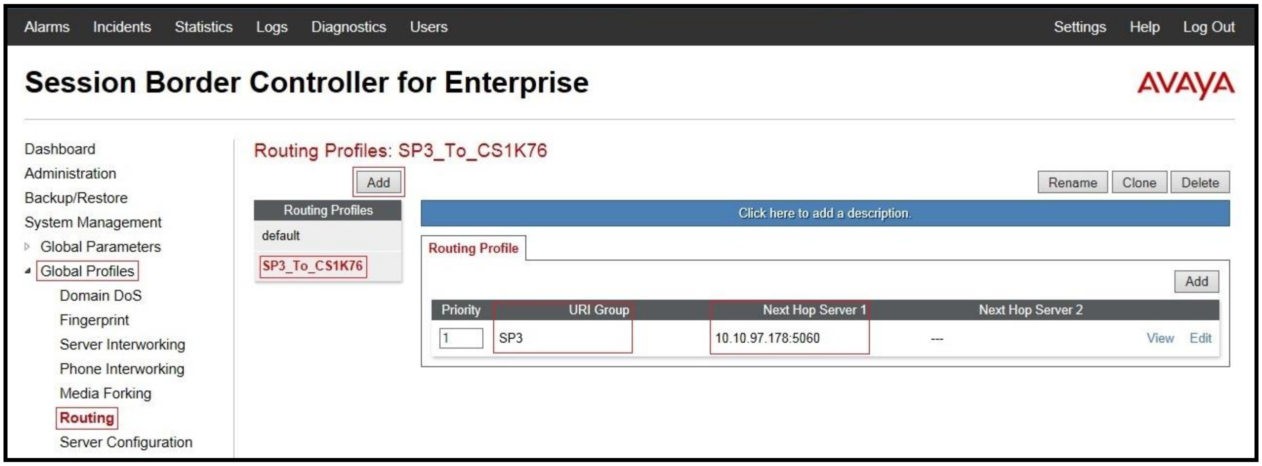

Figure 53 - Routing to Avaya

6.2.5. Configure Routing – Bell Canada site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select **Global Profiles → Routing →Add**
Enter Profile Name: **CS1K76_To_SP3**

- **URI Group**: **SP3** (Refer to **Section 6.2.3**).
- **Next Hop Server 1**: **192.168.237.201:5060** (Bell Canada SIP Signaling server IP address**)**
- Check **Routing Priority based on Next Hop Server** (not shown)
- **Outgoing Transport**: **UDP** (not shown)
- Click **Finish** (not shown).

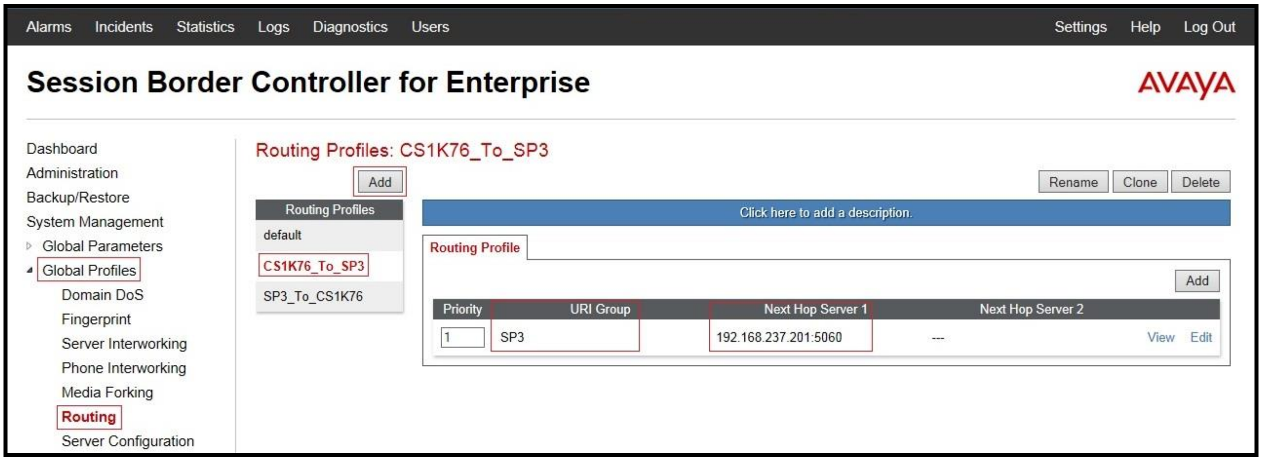

Figure 54 - Routing to Bell Canada

6.2.6. Configure Signaling Manipulation

The Avaya's SIP signaling header manipulation feature is used for the SBCE product. This feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Signaling Manipulation**
- Select **Add**. Enter script Title: **SP3**
    - Edit the script to remove + in From and Contact headers from incoming calls.
    - Edit the script to replace the P-Asserted-Identity number if it is not in the list of DID numbers that Bell Canada provided.
    - Edit the script to replace History Info by Diversion Header for call forward off-net.
    - Edit the script to replace MIME by SDP.
    - Edit the script to remove unwanted SIP headers.
    - Click **Save** (not shown).

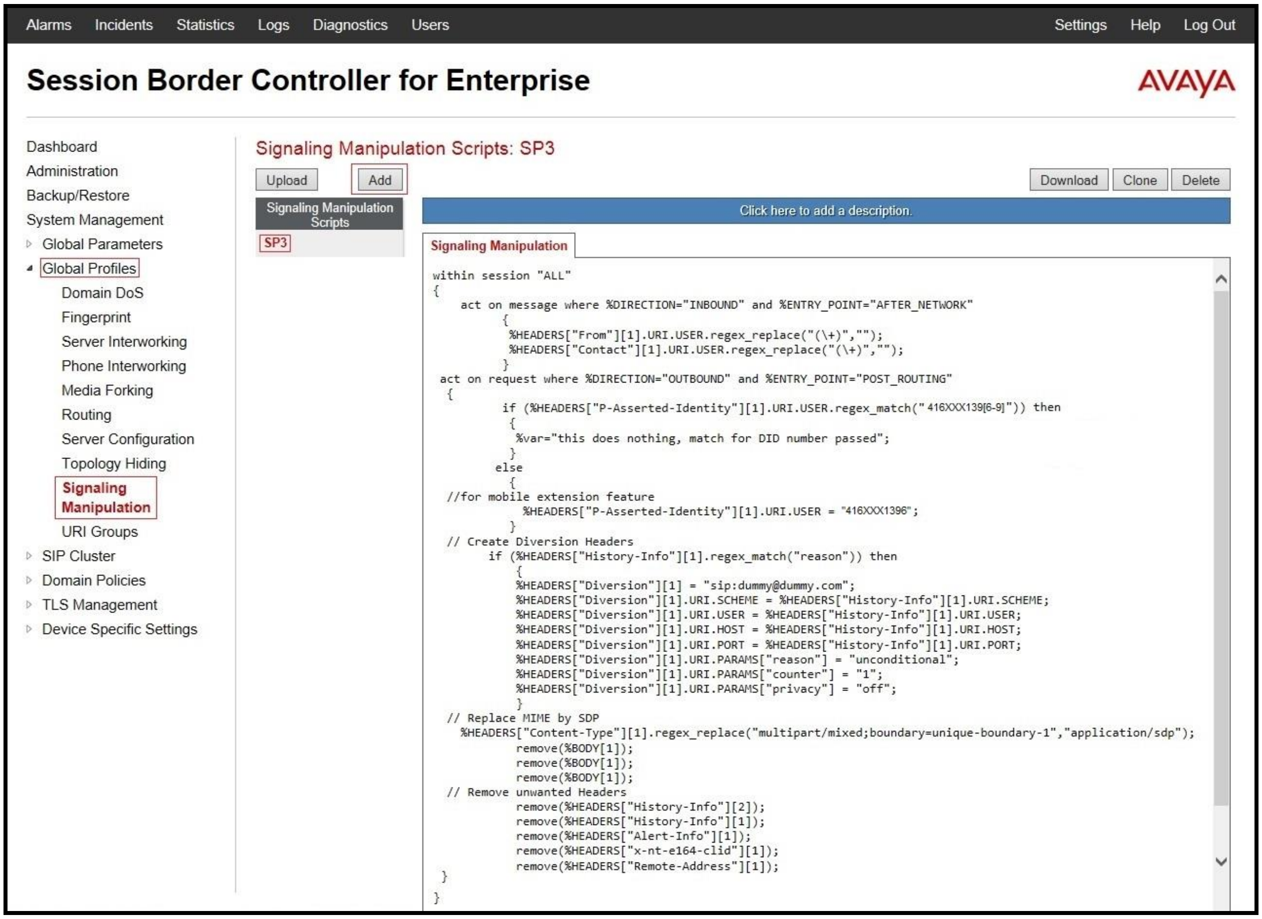

Figure 55 – Signaling Manipulation Bell Canada

6.2.7. 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/FQDNs**: **10.10.97.178** (CS1000 Node IP Address)
- **Supported Transports**: **UDP**
- **UDP Port**: **5060**

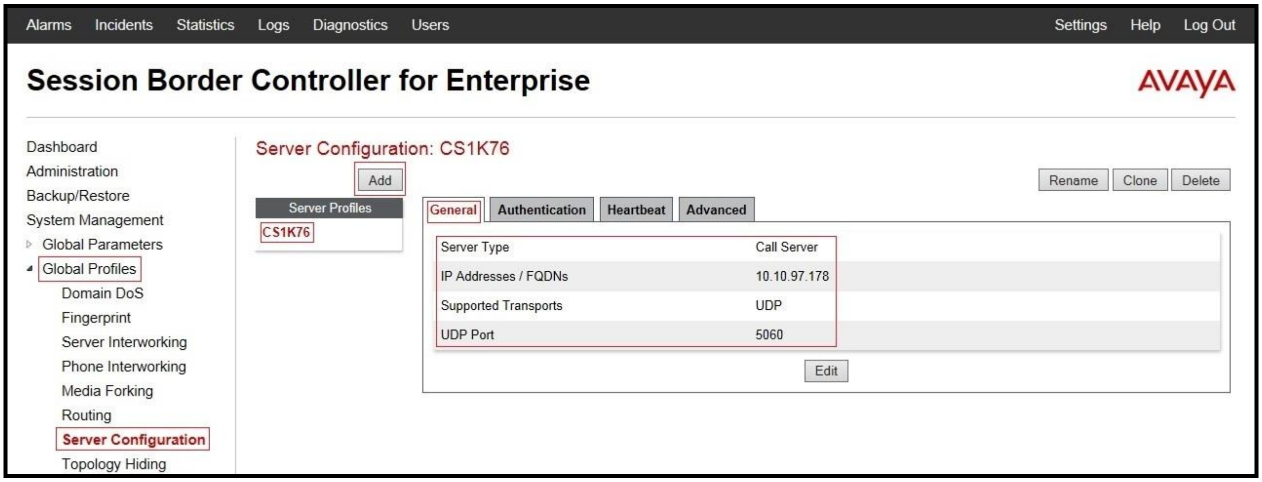

Figure 56 – CS1000 General Server Configuration

On the **Advanced** tab:

- Select **CS1K76** for **Interworking Profile**

Click **Finish** (not shown).

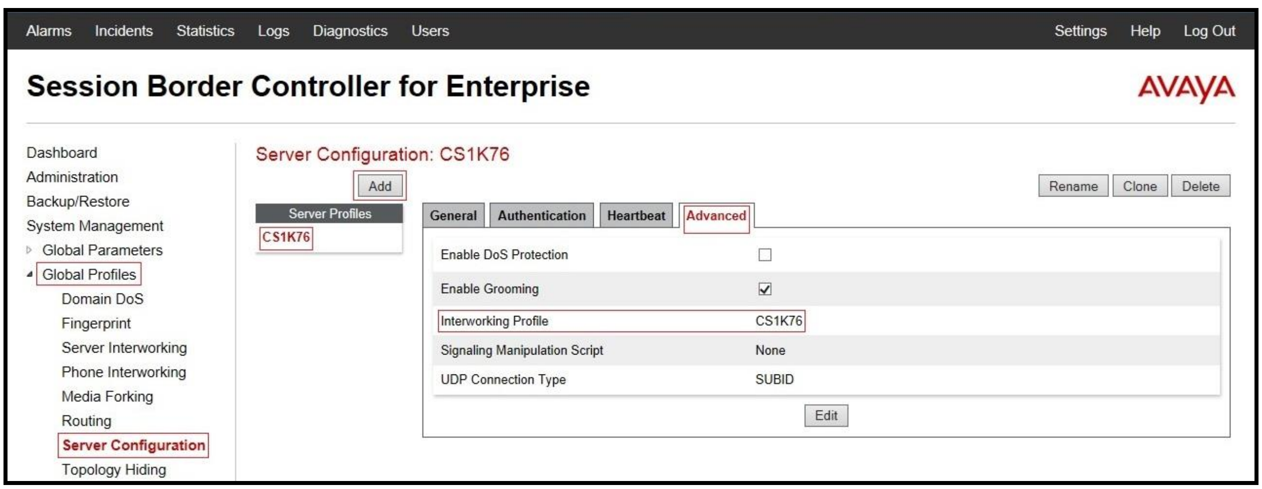

Figure 57 – Avaya Communication Server 1000 Advanced Server Configuration

6.2.8. Configure Server – Bell Canada

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

Enter profile name: **BellCanada**

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

- **Server Type:** Select **Trunk Server**
- **IP Address: 192.168.237.201** (Bell Canada Signaling server IP Address)

- **Supported Transports**: **UDP**
- **UDP Port: 5060**

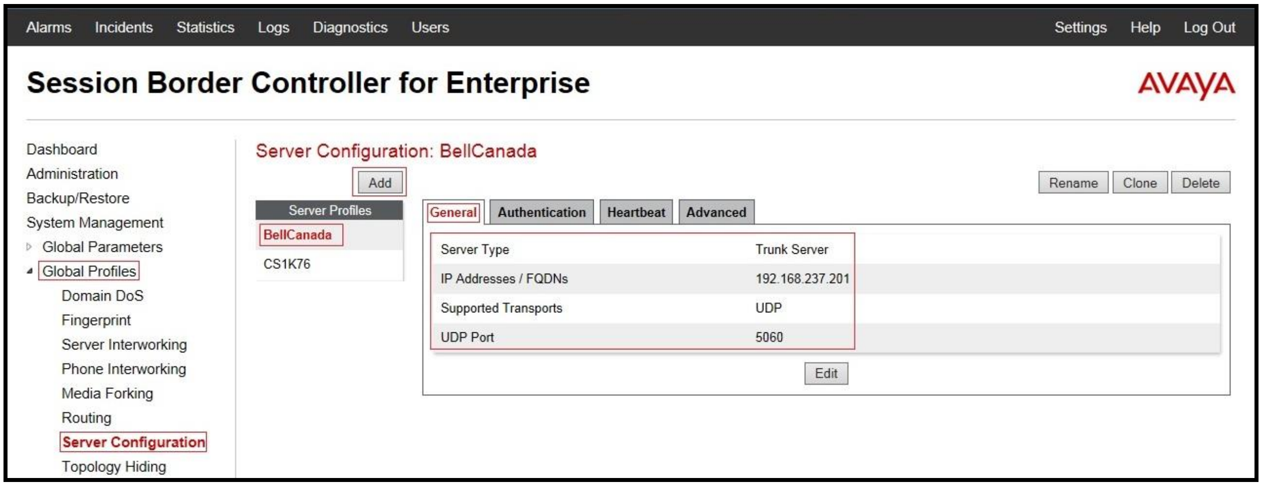

Figure 58 - Bell Canada General Server Configuration

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

- **Interworking Profile**: select **SP3** (Refer to **Section 6.2.2**).
- **Signaling Manipulation Script**: select **SP3** (Refer to **Section 6.2.6**).

Click **Finish** (not shown).

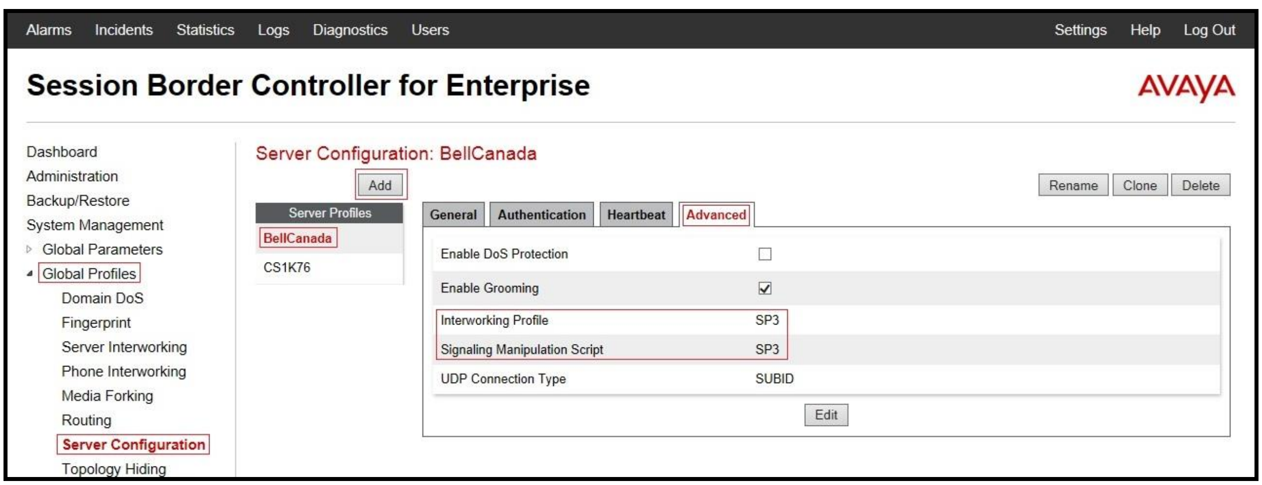

Figure 59 - Bell Canada Advanced Server Configuration

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

- Check **Enable Authentication**.
- Enter **User Name**: **416XXX1396** (Provided by Bell Canada).
- Enter **Password**: ******** (Provided by Bell Canada).

- Enter **Realm**: **sipXXX.bell.ca** (Provided by Bell Canada).

Click **Finish**.

Figure 60 - Bell Canada Authentication Server Configuration

On the **Heartbeat** tab, enter the following:
- Check **Enable Heartbeat**.
- Select **Method**: **OPTIONS**
- Enter **Frequency**: **60 seconds**
- Enter **From URI**: **416XXX1396@cust2-tor.XXX.bell.ca**
- Enter **To URI**: **416XXX1396@sipXXX.bell.ca**

Click **Finish** (not shown).

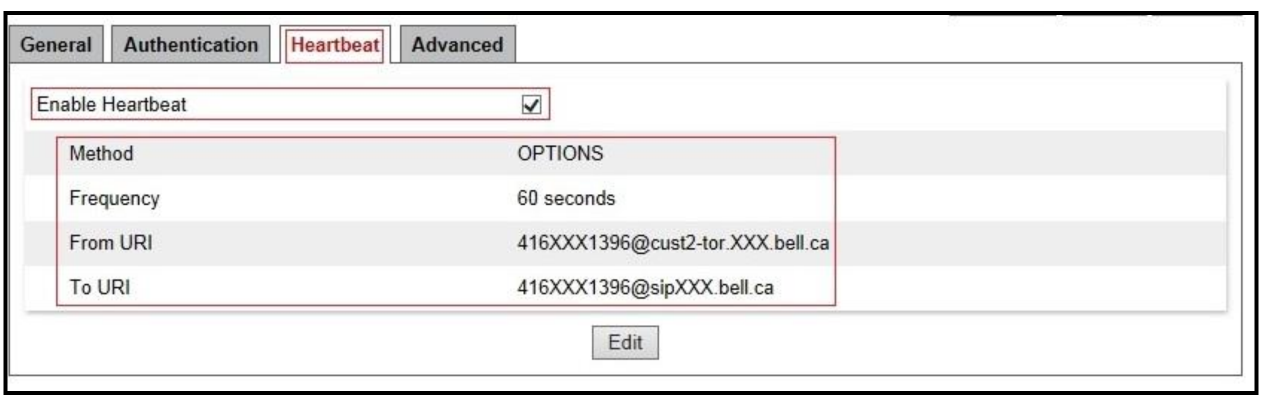

Figure 61 - Bell Canada HeartBeat Server Configuration

6.2.9. Configure Topology Hiding – Avaya site

The Topology Hiding screen allows one 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 **Add**, enter Profile Name: **SP3_To_CS1K76**.

- For the Header **To,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
    In the **Overwrite Value** column: **bvwdev7.**com (This is CS1000 domain configured in **Section 5.5.2**)
- For the Header **Request-Line,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
    In the **Overwrite Value** column: **bvwdev7.com** (This is CS1000 domain configured in **Section 5.5.2**)
  -
- For the Header **From,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
    In the **Overwrite Value** column: **bvwdev7.com** (This is CS1000 domain configured in **Section 5.5.2**)

Click **Finish** (not shown).

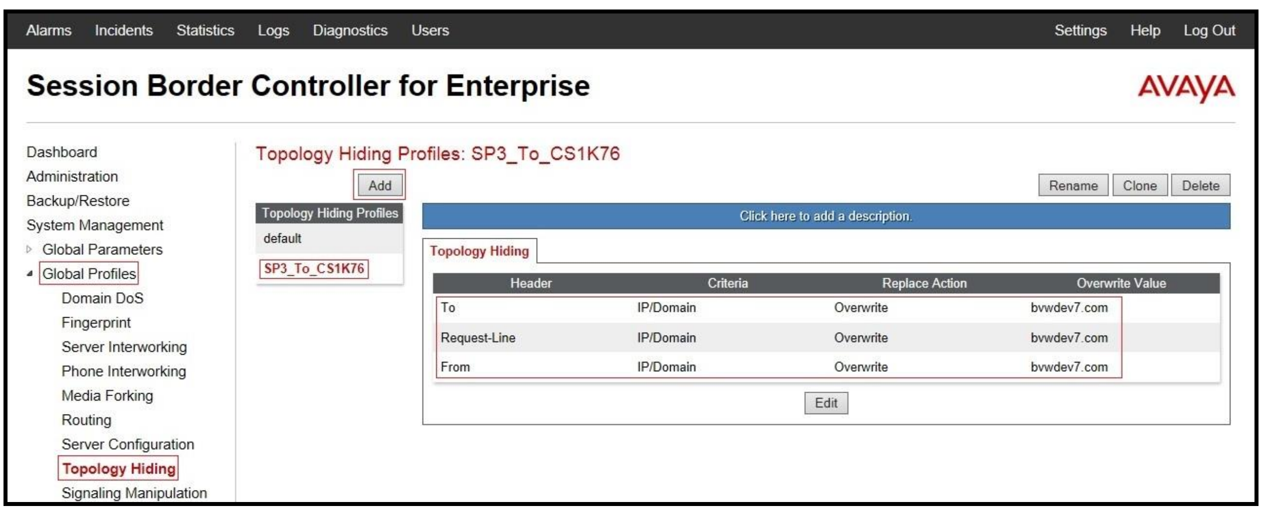

Figure 62 - Topology Hiding CS1000

6.2.10. Configure Topology Hiding – Bell Canada site

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

Select **Add Profile**, enter Profile Name: **CS1K76_To_SP3**.

- For the Header **To,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **sipXXX.bell.ca**
- For the Header **Request-Line,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **sipXXX.bell.ca**
- For the Header **From,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **cust2-tor.XXX.bell.ca**

Click **Finish** (not shown).

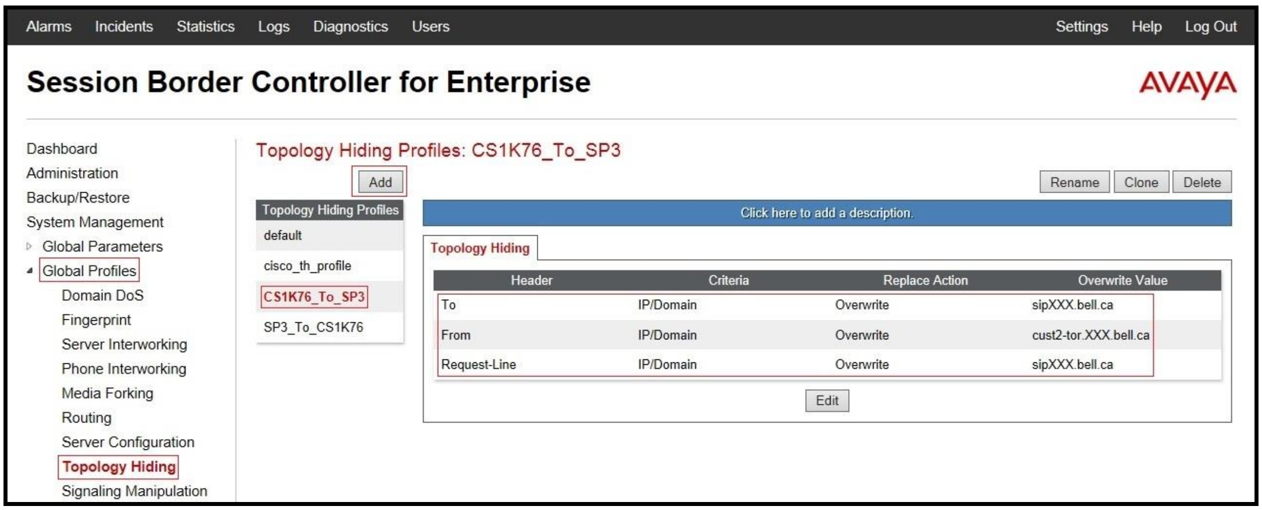

Figure 63 - Topology Hiding Bell Canada

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 Application Rules

Application Rules allow one to define which types of SIP-based Unified Communications (UC) applications the SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, one can determine the maximum number of concurrent voice and video sessions so that the network will process to prevent resource exhaustion.

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

- Select the **default** Rule
- Select **Clone** button
  - Name: **CS1K76_AppR**
  - Click **Finish** (not shown).

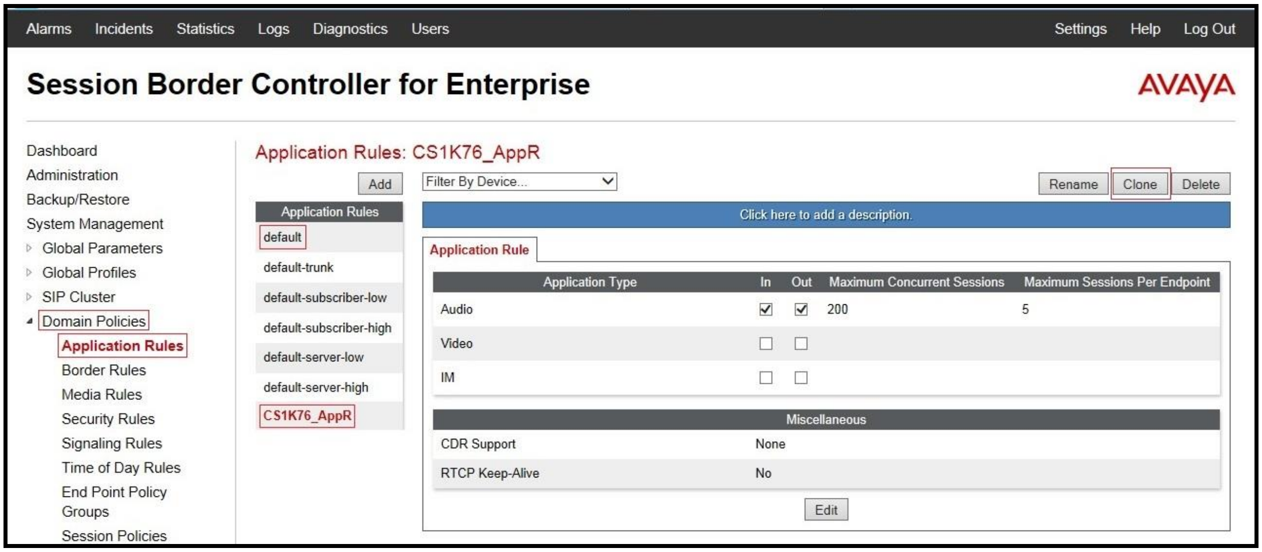

Figure 64 – CS1000 Application Rule

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

- Select the **default** Rule
- Select **Clone** button
  - Name: **SP3_AppR**
  - Click **Finish** (not shown).

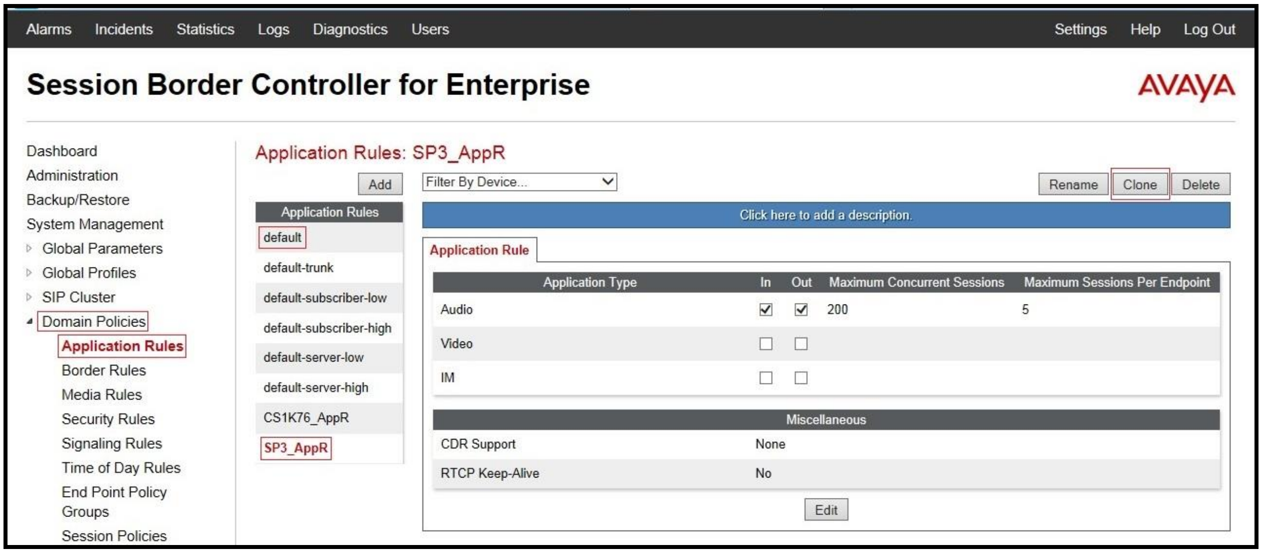

Figure 65 - Bell Canada Application Rule

6.3.2. Create Border Rules

Border Rules allow one to control NAT Traversal. The NAT Traversal feature allows one to determine whether or not call-flow through the DMZ needs to traverse a firewall and the manner in which pinholes will be kept open in the firewall to accommodate traffic.

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

- Select the **default** Rule
- Select **Clone** button
  - Enter Clone Name: **CS1K76_BorderR**
  - Click **Finish** (not shown).

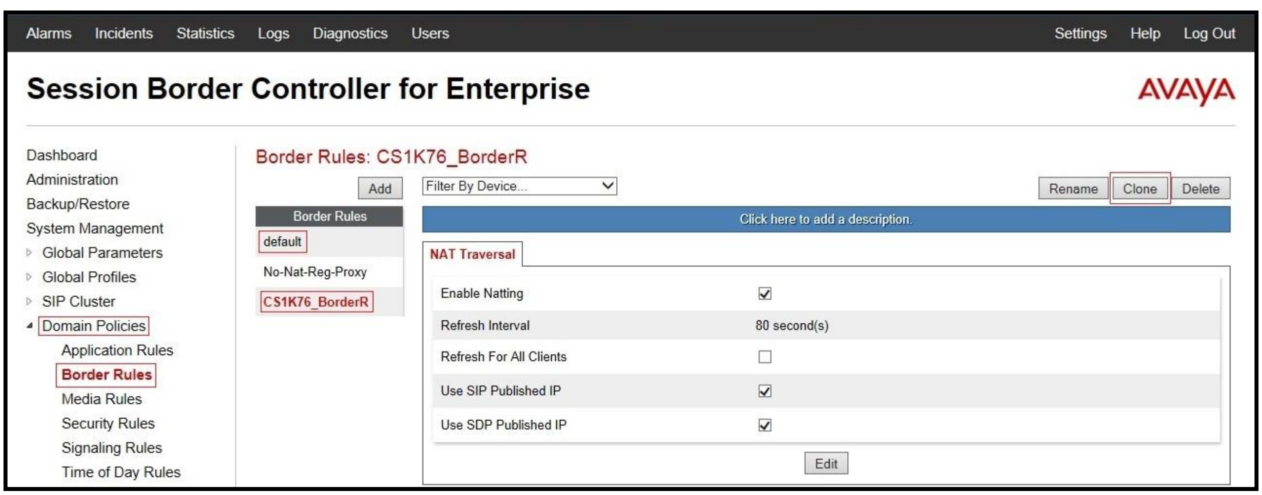

Figure 66 - CS1000 Border Rule

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

- Select the **default** Rule
- Select **Clone** button
  - Enter Clone Name: **SP3_BorderR**
  - Click **Finish** (not shown).

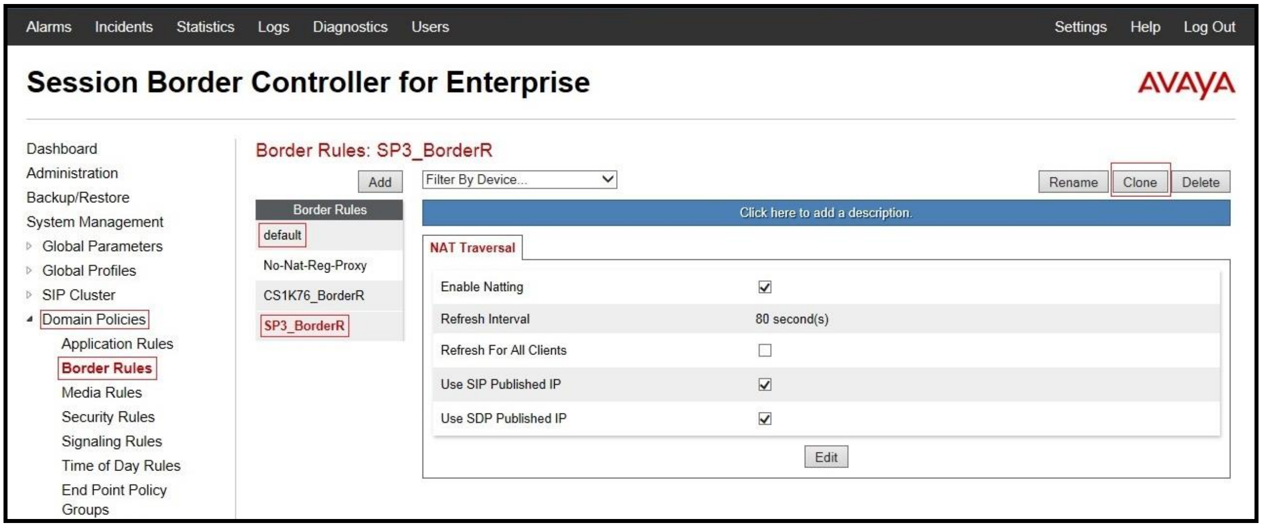

Figure 67 - Bell Canada Border Rule

6.3.3. Create Media Rules

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

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

- Select the **default-low-med** Rule
- Select **Clone** button
  - Enter Clone Name: **CS1K76_MediaR**
  - Click **Finish** (not shown).

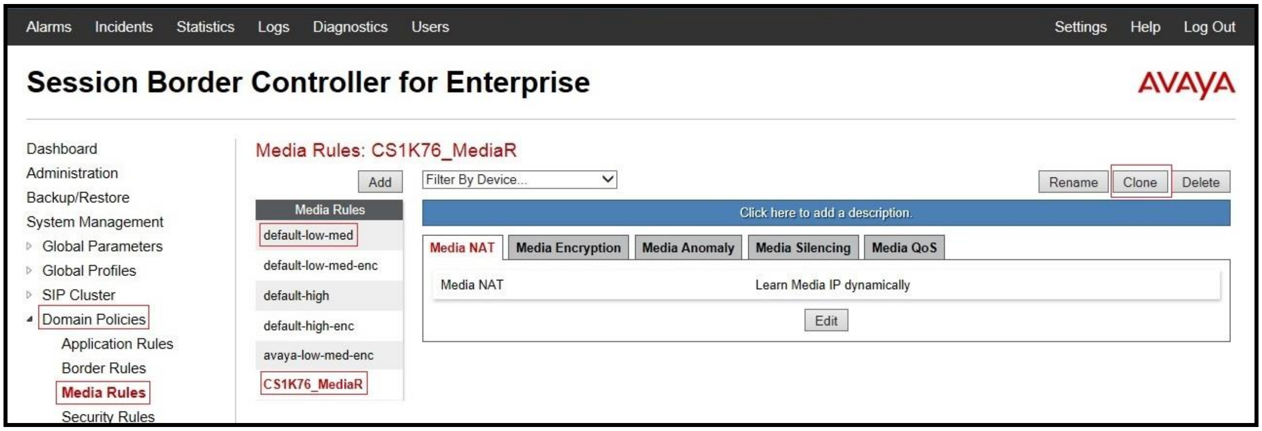

Figure 68 - CS1000 Media Rule

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

- Select the **default-low-med** Rule
- Select **Clone** button
  - Enter Clone Name: **SP3_MediaR**
  - Click **Finish** (not shown).

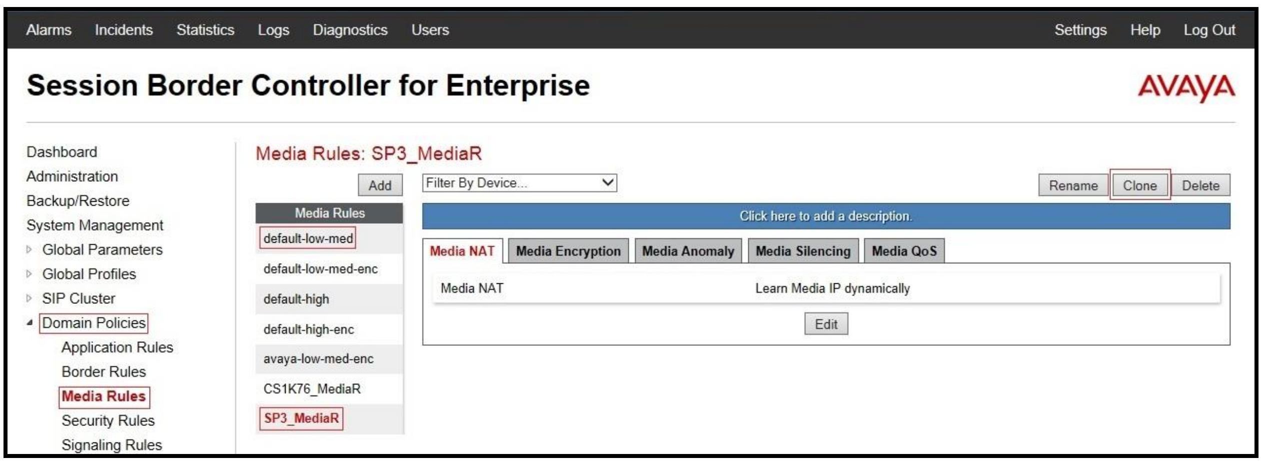

Figure 69 – Bell Canada Media Rule

6.3.4. Create Security Rules

Security Rules allow one to define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allows one to configure Authentication, Compliance, Fingerprinting, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, one can also define the security feature profile, so that the feature is applied in a specific manner to a specific situation. From the menu on the left-hand side, select **Domain Policies → Security Rules**.

- Select the **default-med** Rule
- Select **Clone** button

- Enter Clone Name: **CS1K76_SecR**
- Click **Finish** (not shown).

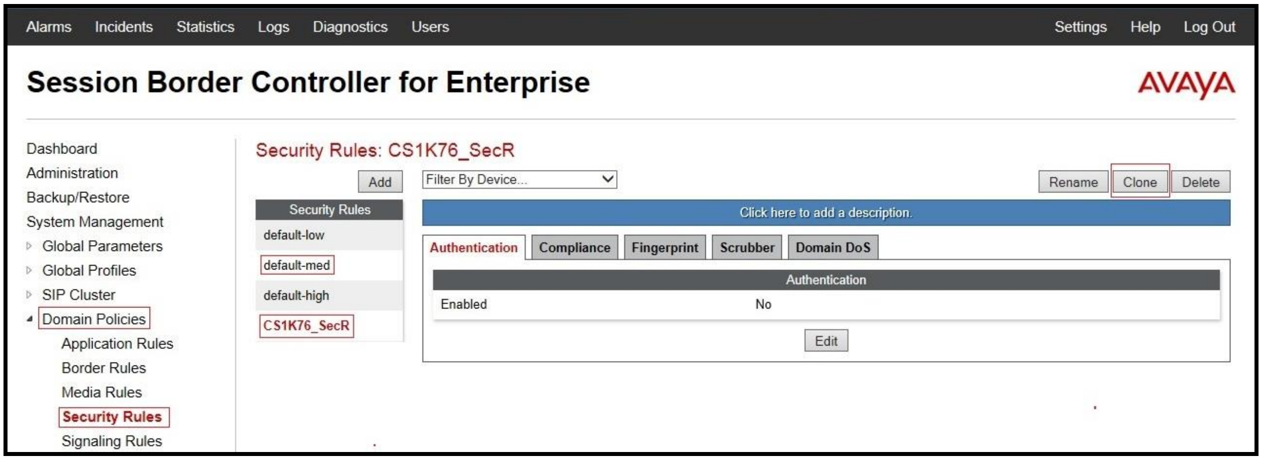

Figure 70 - CS1000 Security Rule

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

- Select the **default-med** Rule
- Select **Clone** button
  - Enter Clone Name: **SP3_SecR**
  - Click **Finish** (not shown).

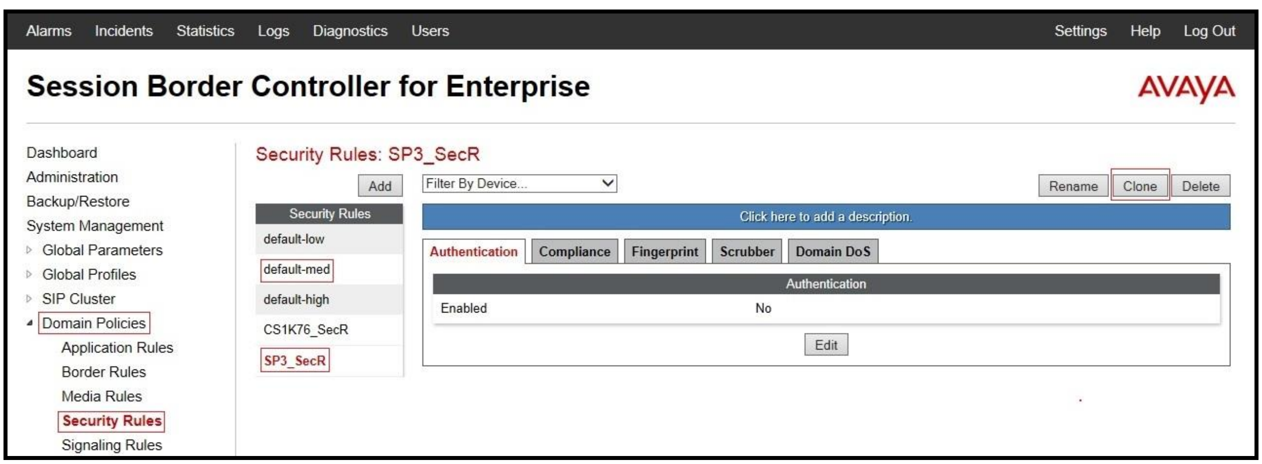

Figure 71 - Bell Canada Security Rule

6.3.5. 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 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: **CS1K76_SigR**
  - Click **Finish** (not shown).

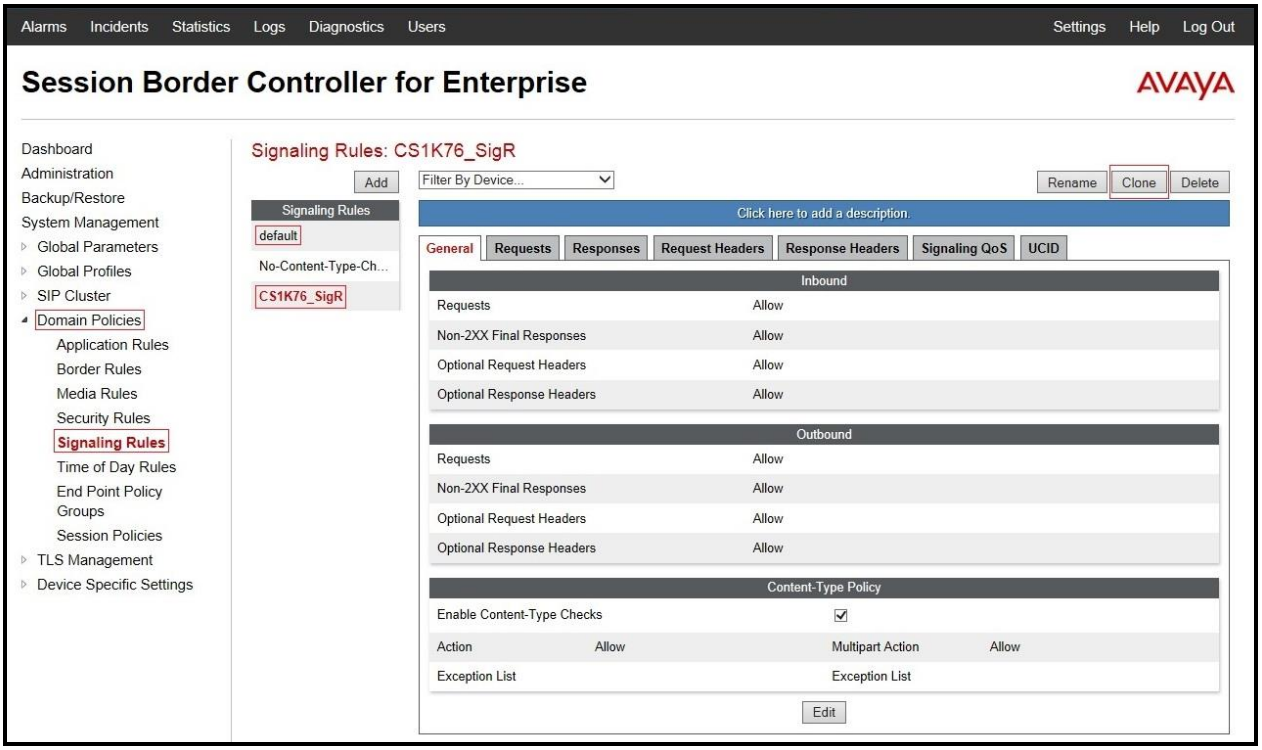

Figure 72 - CS1000 Signaling Rule

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

- Select the **default** Rule
- Select **Clone** button
  - Enter Clone Name: **SP3_SigR**
  - Click **Finish** (not shown).

On **Signaling QoS** tab,

- Check **Signaling QoS**
- Select **QoS Type**: **DSCP**
- Select **DSCP**: **EF**
- Select **Finish** (not shown).

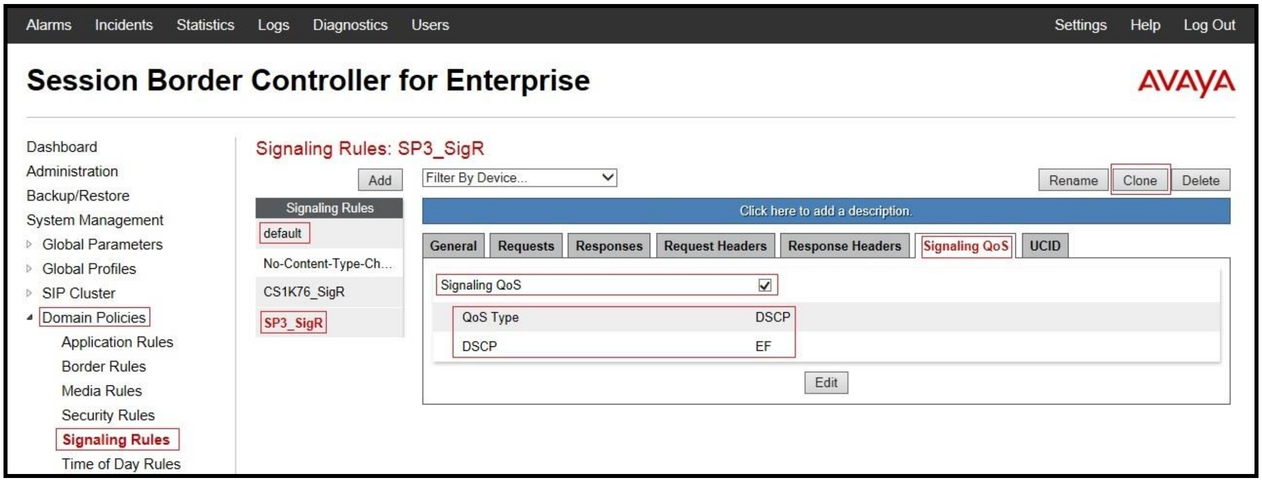

Figure 73 - Bell Canada Signaling Rule

6.3.6. Create Time of Day Rules

A Time-of-day (ToD) Rule allows one to determine when the domain policy which is assigned to will be in effect. ToD Rules provide complete flexibility to fully accommodate the enterprise by, not only determining when a particular domain policy will be in effect, but also to whom it will apply, and for how long it will remain in effect.

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

- Select the **default** Rule
- Select **Clone** button
  - Enter Clone Name: **CS1K76_ToDR**
  - Click **Finish** (not shown).

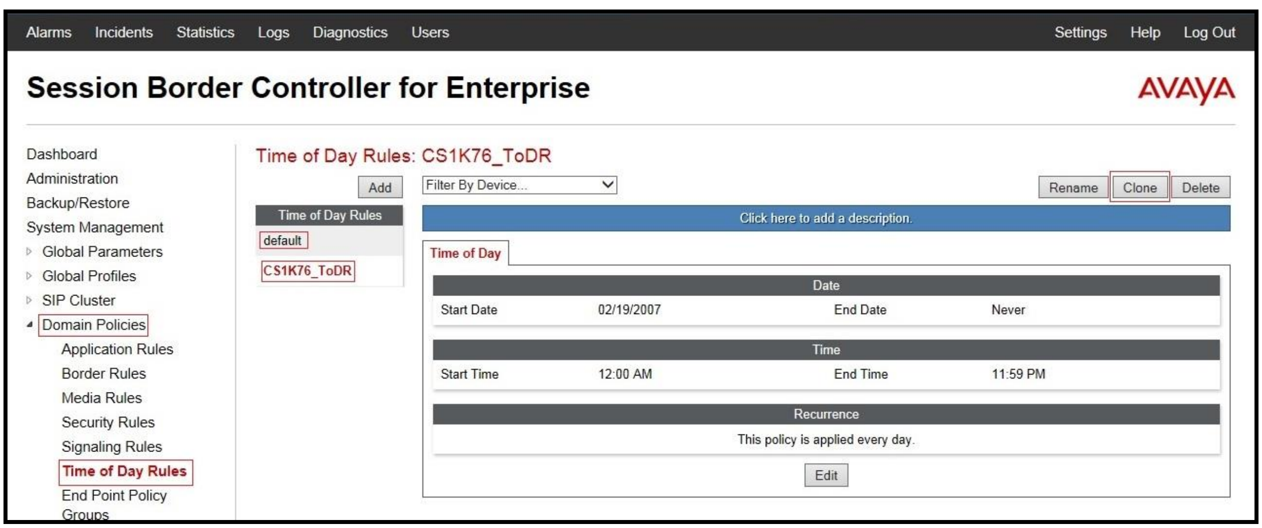

Figure 74 - CS1000 Time of Day Rule

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

- Select the **default** Rule
- Select **Clone** button
  - Enter Clone Name: **SP3_ToDR**
  - Click **Finish** (not shown).

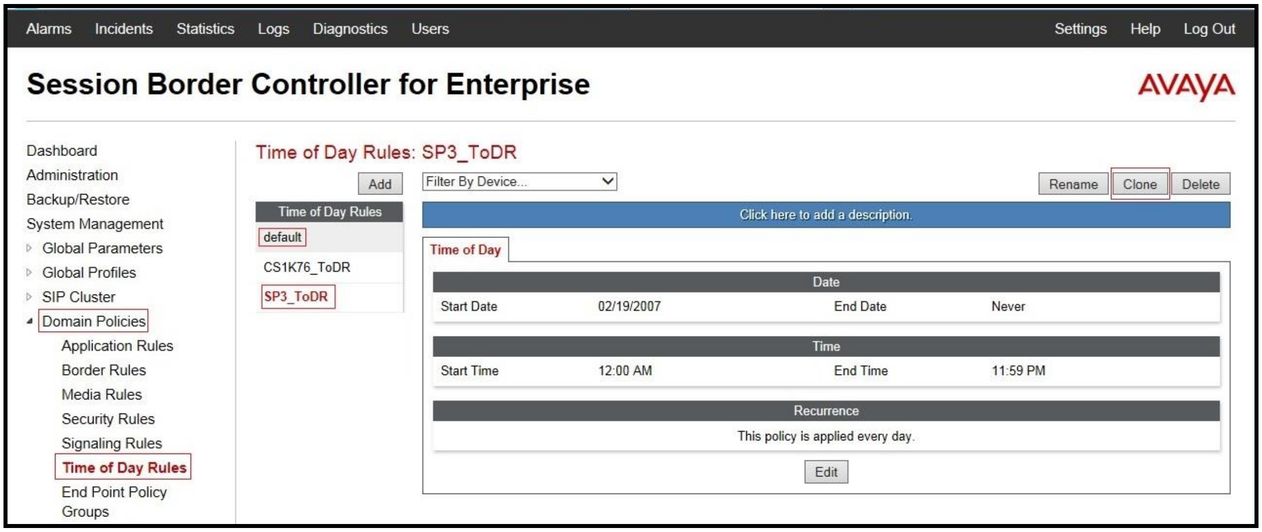

Figure 75 - Bell Canada Time of Day Rule

6.3.7. 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, each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of 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_PolicyG**
  - **Application Rule**: **CS1K76_AppR** (Refer to **Section 6.3.1**)
  - **Border Rule**: **CS1K76_BorderR** (Refer to **Section 6.3.2**)
  - **Media Rule**: **CS1K76_MediaR** (Refer to **Section 6.3.3**)
  - **Security Rule**: **CS1K76_SecR** (Refer to **Section 6.3.4**)
  - **Signaling Rule**: **CS1K76_SigR** (Refer to **Section 6.3.5**)
  - **Time of Day**: **CS1K76_ToDR** (Refer to **Section 6.3.6**)
- Select **Finish** (not shown).

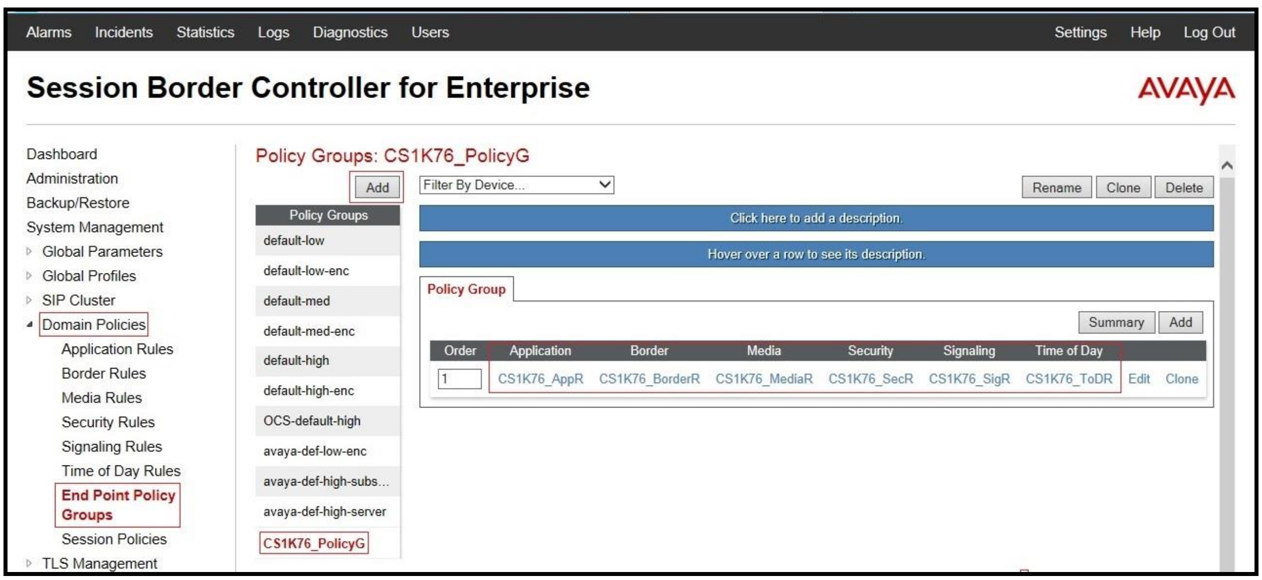

Figure 76 - CS1000 End Point Policy Group

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

- Select **Add**
- Enter **Group Name**: **SP3_PolicyG**
  - **Application Rule**: **SP3_AppR** (Refer to **Section 6.3.1**)
  - **Border Rule**: **SP3_BorderR** (Refer to **Section 6.3.2**)

- **Media Rule**: **SP3_MediaR** (Refer to **Section 6.3.3**)
- **Security Rule**: **SP3_SecR** (Refer to **Section 6.3.4**)
- **Signaling Rule**: **SP3_SigR** (Refer to **Section 6.3.5**)
- **Time of Day**: **SP3_ToDR** (Refer to **Section 6.3.6**)

• Select **Finish** (not shown).

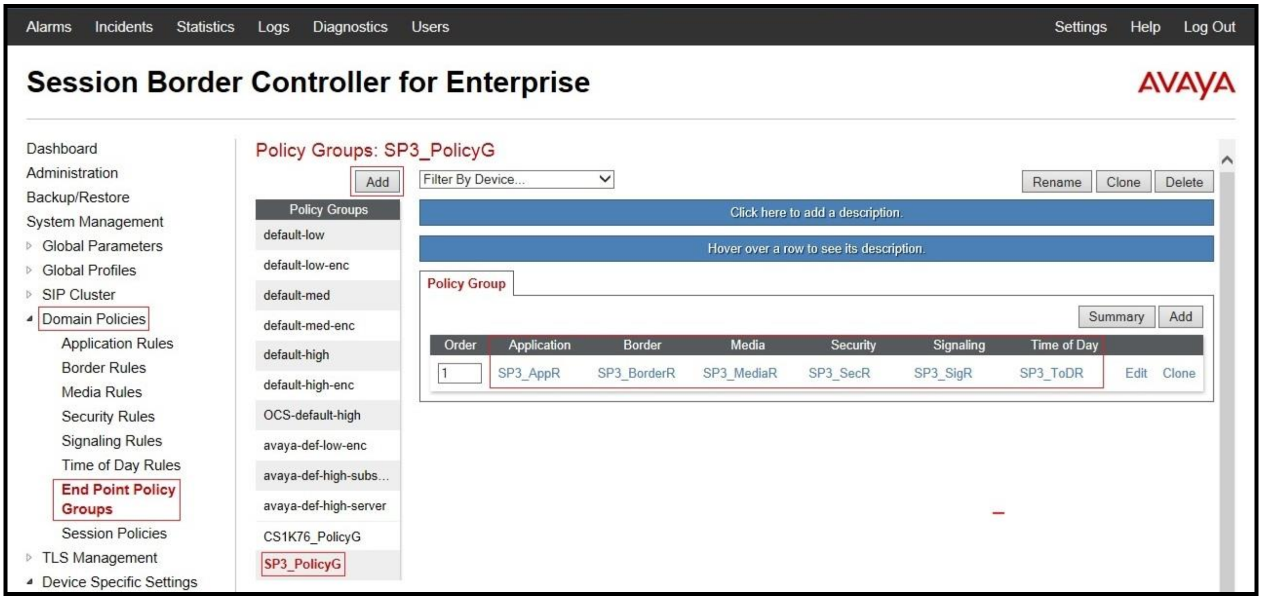

Figure 77 - Bell Canada End Point Policy Group

6.3.8. Create Session Policy

Session Policies allow users to define RTP media packet parameters such as codec types (both audio and video) and codec matching priority. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the SBCE security product.

- From the menu on the left-hand side, select **Domain Policies → Session Policies**.
- Select the **default** policy
- Select **Clone** button
  - Enter Clone Name: **SP3**
  - Click **Finish** (not shown).
- Click **Edit** button on **Media** tab
  - Check **Media Anchoring**
  - Select **Finish** (not shown).

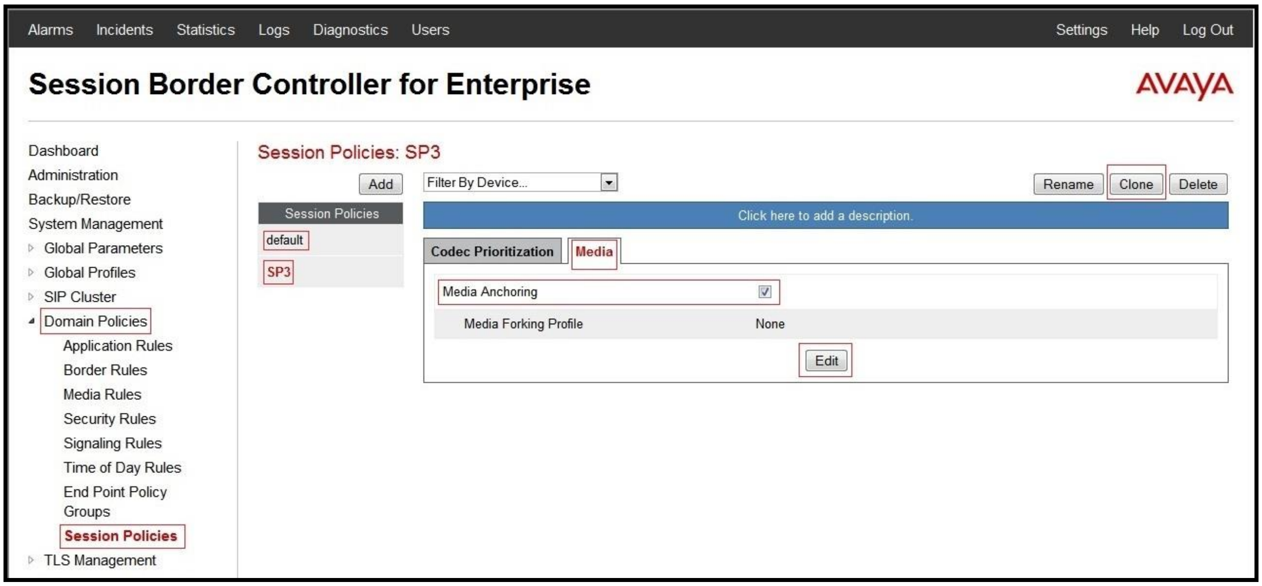

Figure 78 - Bell Canada Session Policy – Anchoring Media

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**.

- Enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:
  - **IP Address** for Inside interface: **10.10.98.13**; **Gateway**: **10.10.98.1**
  - **IP Address** for Outside interface: **10.10.98.111**; **Gateway**: **10.10.98.97**
- Select the physical interface used in the Interface column:
  - **Inside Interface**: **A1**
  - **Outside Interface**: **B1**

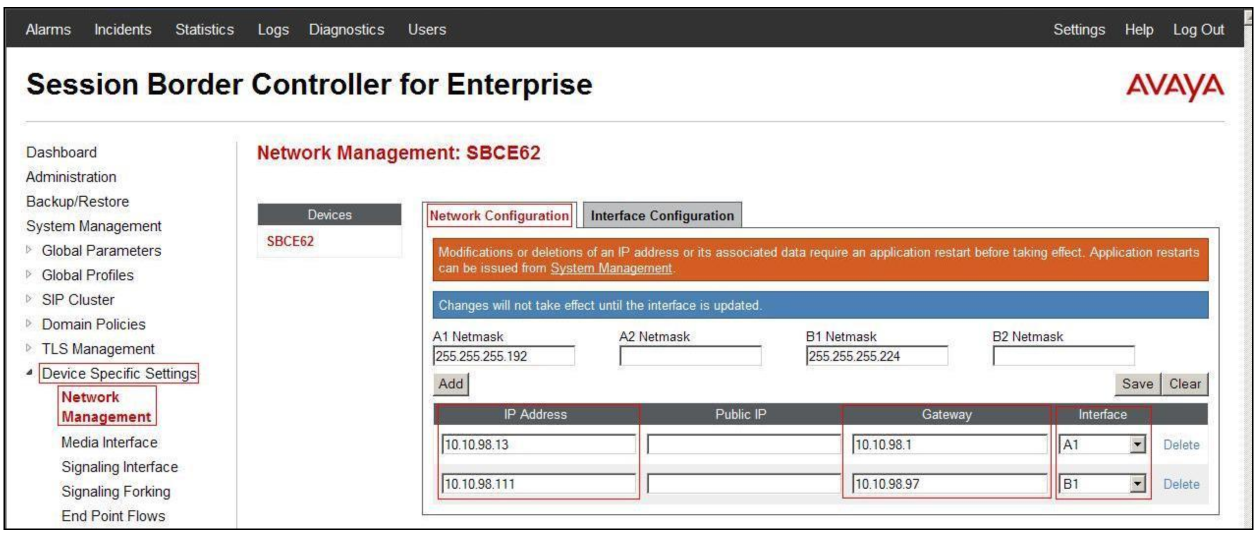

Figure 79 - Network Management

- Select the **Interface Configuration** Tab.
- Toggle the State of the physical interfaces being used to **Enabled**.

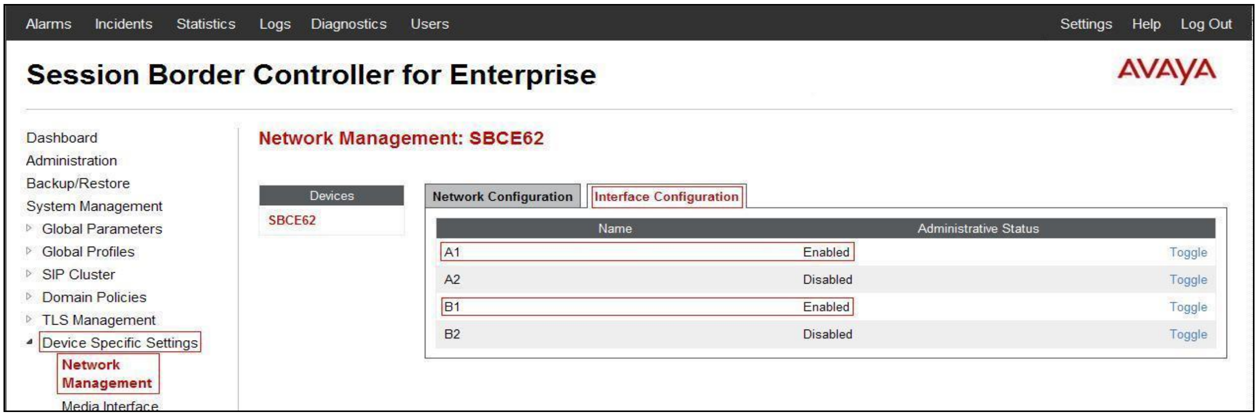

Figure 80 - Network Interface Status

6.4.2. Create Media Interfaces

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

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

- Select **Add**
  - **Name: InsideMedia**
  - **Media IP**: **10.10.98.13** (Internal IP Address toward CS1000)
  - **Port Range**: **35000 - 40000**
  - Click **Finish** (not shown)
- Select **Add**
  - **Name: OutsideMedia**
  - **Media IP**: **10.10.98.111** (External IP Address toward Bell Canada)
  - **Port Range**: **35000 - 40000**
  - Click **Finish** (not shown).

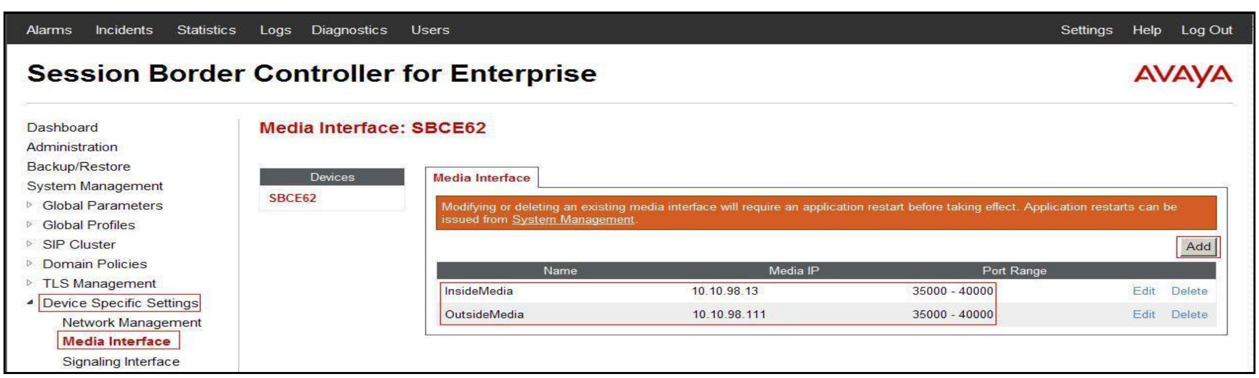

Figure 81 - Media Interface

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 **Add**
  - **Name**: **InsideUDP**
  - **Media IP**: **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 **Add**
  - **Name**: **OutsideUDP**
  - **Media IP**: **10.10.98.111** (External IP Address toward Bell Canada)
  - **UDP Port**: **5060**
  - Click **Finish** (not shown).

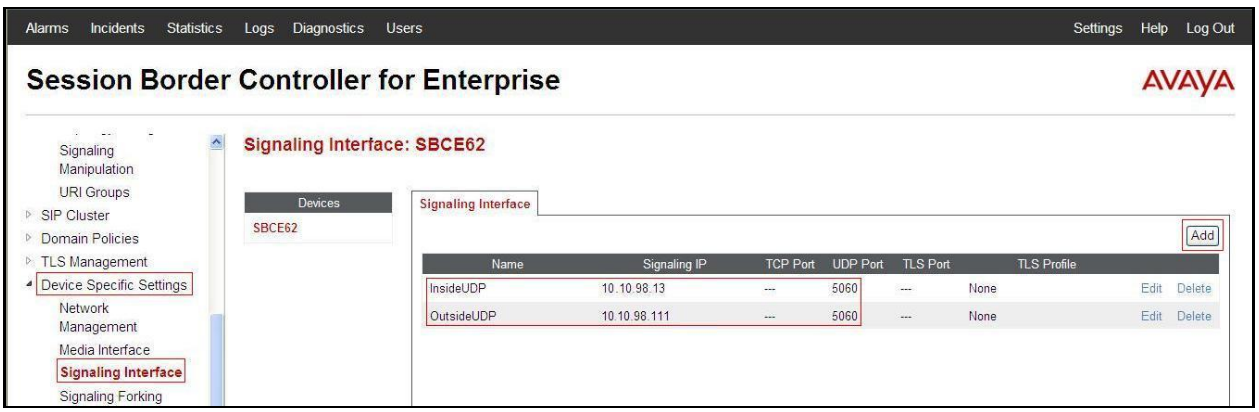

Figure 82 - Signaling Interface

6.4.4. Configuration Server Flows

Server Flows allow to categorize trunk-side signaling and to apply a policy.

6.4.4.1 Create End Point Flows – From 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**: **From BellCanada**
  - **Server Configuration**: **BellCanada** (Refer to **Section 6.2.8**)
  - **URI Group**: **SP3** (Refer to **Section 6.2.3**)
  - **Transport**: *
  - **Remote Subnet**: *
  - **Received Interface**: **InsideUDP** (Refer to **Section 6.4.3**)
  - **Signaling Interface**: **OutsideUDP** (Refer to **Section 6.4.3**)
  - **Media Interface**: **OutsideMedia** (Refer to **Section 6.4.2**)

- **End Point Policy Group**: **SP3_PolicyG** (Refer to **Section 6.3.7**)
- **Routing Profile**: **SP3_To_CS1K76** (Refer to **Section 6.2.4**)
- **Topology Hiding Profile**: **CS1K76_To_SP3** (Refer to **Section 6.2.10**)
- Click **Finish**.

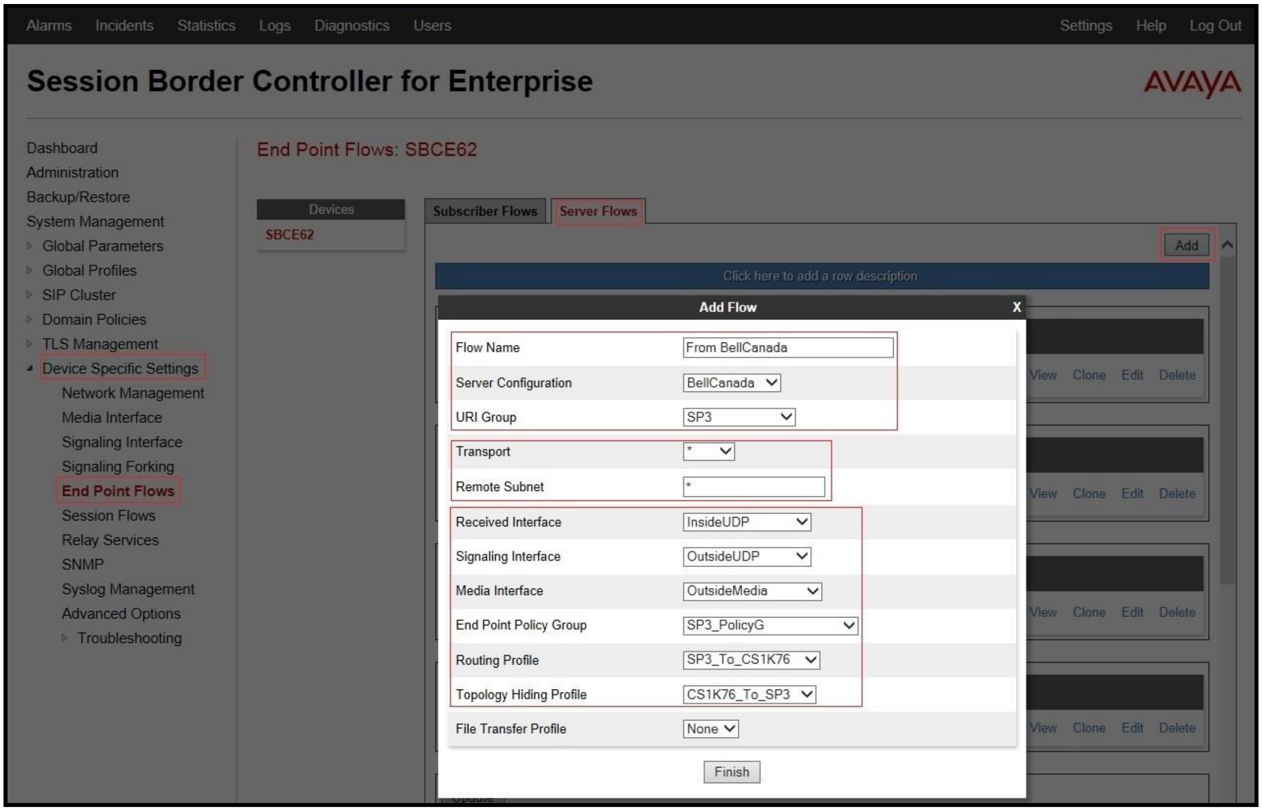

Figure 83 - End Point Flows 1

6.4.4.2 Create End Point Flows – To 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**: **To BellCanada**
  - **Server Configuration**: **CS1K76** (Refer to **Section 6.2.7**)
  - **URI Group**: **SP3** (Refer to **Section 6.2.3**)
  - **Transport**: *
  - **Remote Subnet**: *
  - **Received Interface: OutsideUDP** (Refer to **Section 6.4.3**)
  - **Signaling Interface**: **InsideUDP** (Refer to **Section 6.4.3**)
  - **Media Interface**: **InsideMedia** (Refer to **Section 6.4.2**)
  - **End Point Policy Group**: **CS1K76_PolicyG** (Refer to **Section 6.3.7**)
  - **Routing Profile**: **CS1K76_To_SP3** (Refer to **Section 6.2.5**)
  - **Topology Hiding Profile**: **SP3_To_CS1K76** (Refer to **Section 6.2.9**)
  - Click **Finish**.

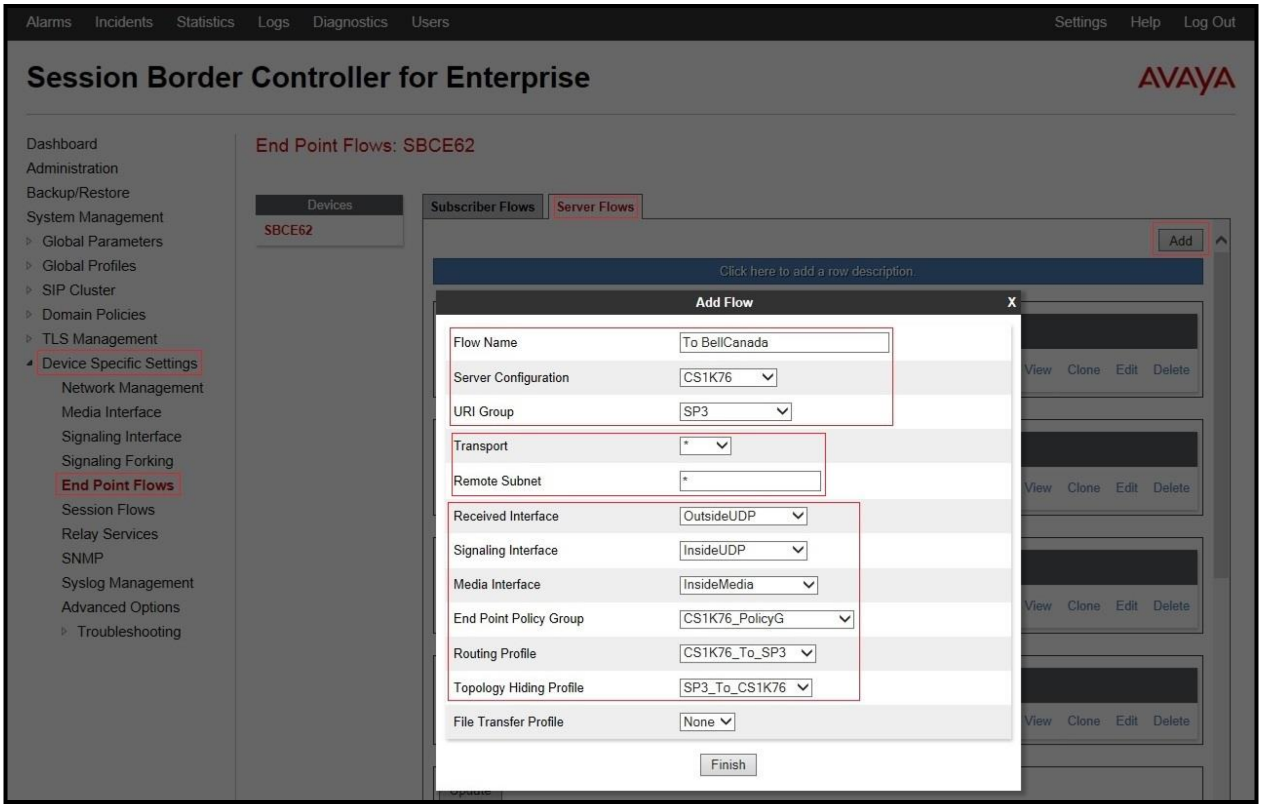

Figure 84 - End Point Flows 2

6.4.5. Create Session Flows

Session Flow determines the media (audio/video) sessions in order to apply the appropriate session policy.

- Select **Device Specific Settings** from the menu on the left-hand side
- Select the **Session Flows**
- Select **Add**
- Enter **Flow Name**: **SP3**
  - **URI Group#1**: **SP3** (Refer to **Section 6.2.3**)
  - **URI Group#2**: **SP3** (Refer to **Section 6.2.3**)
  - **Session Policy**: **SP3** (Refer to **Section 6.3.8**)
- Select **Finish** (not shown)

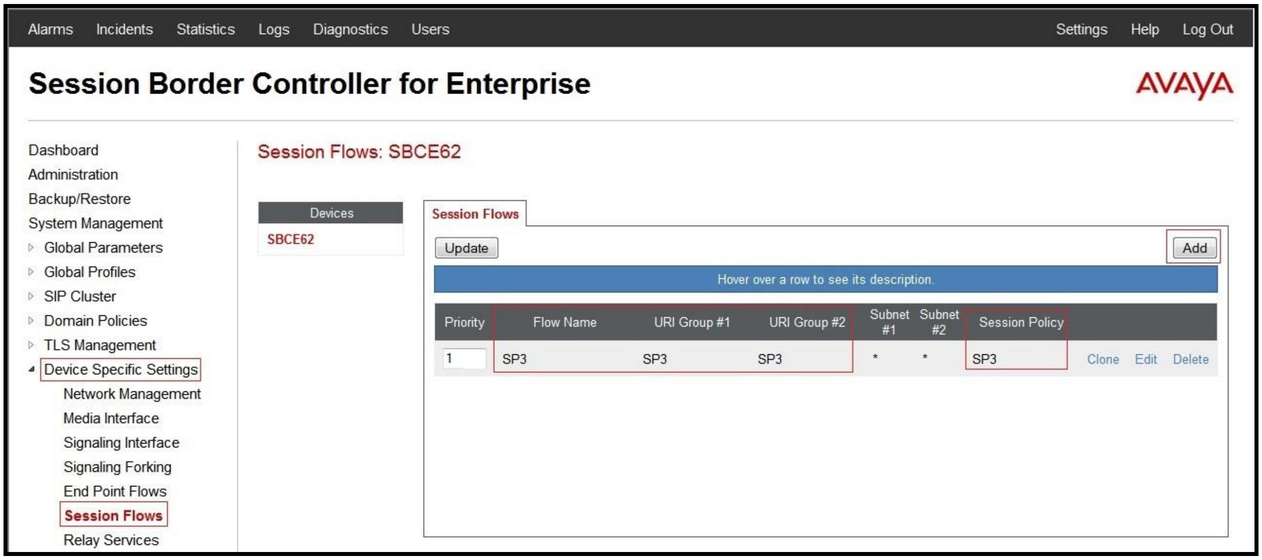

Figure 85 – Session Flows

7. Bell Canada SIP Trunk Service Configuration

Bell Canada is responsible for the network configuration of the Bell Canada SIP Trunk Service. Bell Canada will require that the customer provide the public IP address used to reach the SBCE public interface at the edge of the enterprise. Bell Canada will provide the IP address of Bell Canada's SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete configurations for CS1000, and the SBCE discussed in the previous sections.

The configuration between Bell Canada and the enterprise is a static configuration.

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 CS1000

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 (1397). The call scenario involved PSTN phone number 613XXX5206 calling 416XXX1397 (which is translated to phone 1397).

- 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 1397. This command is used not only to verify of any present calls on this DN, but also to show used SIP trunks, IP address of SIP/Media Servers, Codec, Calling/Called numbers after the call is released, issue command **trac 0 1397** 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 **1397** is in call state:

```
>ld 80
TRA000
.trac 0 1397

ACTIVE  VTN 096 0 00 02

ORIG   VTN 100 0 00 00   VTRK IPTI  RMBR  100 1 INCOMING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 10.10.98.13
  FAR-END MEDIA ENDPOINT IP: 10.10.98.13  PORT: 37426
  FAR-END SIP SIGNALLING IP: 10.10.98.13
  FAR-END MEDIA ENDPOINT IP: 10.10.98.13  PORT: 37426
TERM   VTN 096 0 00 02  KEY 0  SCR MARP  CUST 0  DN 1397  TYPE 2002P2
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 10.33.5.15  PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 1397
MAIN_PM  ESTD
TALKSLOT  ORIG  6   TERM  11
EES_DATA:
NONE
QUEU  NONE
CALL ID 501 77
----  ISDN ISL CALL (ORIG) ----
CALL REF # =  484
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  613XXX5206  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
CALLED NO  =  416XXX1397  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
```

And this is the example after the call to 1397 is finished.

```
>ld 80
TRA000
.trac 0 1397
IDLE VTN 96 0 00 02   MARP
```

SIP Trunk monitoring (ld 32)

Place a call inbound from PSTN (613XXX5206) to an internal device (416XXX1397). Then check the SIP trunk status by using **ld 32**, 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 changed 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**.

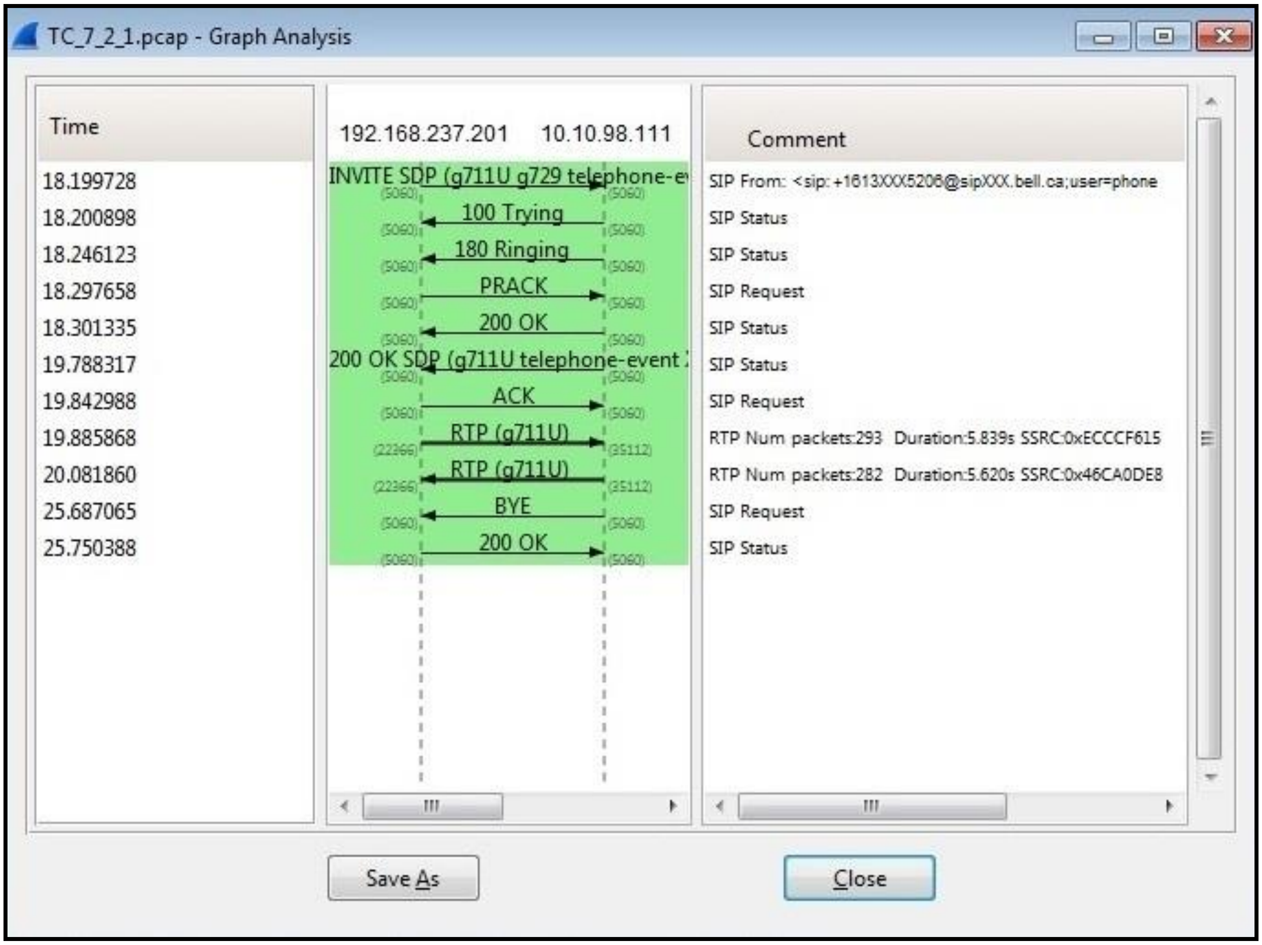

Figure 86 – SIP Call Trace

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 6.2.1 Q07.

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/

[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.

[7] Avaya Aura® System Manager Overview and Specification, Release 6.3, Issue 2, May 2013.

[8] Administering Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, May 2013.

[9] Avaya Session Border Controller for Enterprise Release notes, Release 6.2.1, Issue 5, December 2013.

Other resources:

[11] RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/

[12] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/

11. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 6.2.6**:

```
within session "ALL"
{
   act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
        {
         %HEADERS["From"][1].URI.USER.regex_replace("(\+)","");
         %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
        }
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
        if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("416XXX139[6-9]")) then
         {
          %var="this does nothing, match for DID number passed";
         }
       else
         {

//for mobile extension feature
          %HEADERS["P-Asserted-Identity"][1].URI.USER = "416XXX1396";
         }

// 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].URI.PORT = %HEADERS["History-Info"][1].URI.PORT;
          %HEADERS["Diversion"][1].URI.PARAMS["reason"] = "unconditional";
          %HEADERS["Diversion"][1].URI.PARAMS["counter"] = "1";
          %HEADERS["Diversion"][1].URI.PARAMS["privacy"] = "off";
          }

// Replace MIME by SDP
   %HEADERS["Content-Type"][1].regex_replace("multipart/mixed;boundary=unique-boundary-1","application/sdp");
          remove(%BODY[1]);
          remove(%BODY[1]);
          remove(%BODY[1]);

// Remove unwanted Headers
          remove(%HEADERS["History-Info"][2]);
          remove(%HEADERS["History-Info"][1]);
          remove(%HEADERS["Alert-Info"][1]);
          remove(%HEADERS["x-nt-e164-clid"][1]);
          remove(%HEADERS["Remote-Address"][1]);
  }
}
```

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.