Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Bell Canada SIP Trunking Service with Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 with the Bell Canada SIP Trunking service.

The Bell Canada SIP Trunking service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The Bell Canada SIP Trunking service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

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 Aura® Session Manager Release 6.3 (SM) and Avaya Session Border Controller for Enterprise (ASBC) Release 6.2 with Bell Canada SIP Trunking service (Bell). Bell provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

2. General Test Approach and Test Results

The CS1000 connects to ASBC via SM SIP trunk connectivity. The ASBC connects to Bell system using SIP trunks. Various call types were made from CS1000 to and from Bell system to verify the 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:

- Response to SIP OPTIONS queries
- Registration and Authentication
- General call processing between CS1000 and Bell system including:
    - Codec/ptime G.711 u-law/20ms
    - Hold/Resume on both ends
    - Calling Line Identification Display (CLID)
    - Ring-back tone
    - Speech path
    - Dialing plan support (Local, long distance, international, outbound toll-free, Assisted Operator, 411 and 911 services)
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends.
- 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 Avaya CS1000 system)

The following assumptions were made for these compliance tested configuration:

1. CS1000CS1000 R7.6 software with latest patches.
2. Bell 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 telephone holds/resumes an outbound call, the dialed digits are no longer displayed. This is a CS1000CS1000 known issue.
2. **SIP Telephone Conference** – During a conference call hosted by the CS1000 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 CS1000 transferee's telephone is not updated accordingly. This is known CS1000 limitation.
4. **Blind Call Transfer to PSTN using SIP telephone does not completed until transferee pick up the call** – Call scenario is when PSTN telephone calls to enterprise SIP extension (CS1000 SIP telephone), CS1000 answers the call and performs blind transfer the call to another PSTN endpoint. The expected behavior of the enterprise SIP telephone is after transfer, the telephone 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 telephone is ringing and the SIP telephone should be released and displayed "transfer successfully". Instead, the SIP telephone still displayed "transferring" and not released until the transferee PSTN telephone answered the call. The work around is to hang up the SIP telephone. This is a minor and known limitation on CS1000 SIP telephone without any user impact. Transfer is still completed with two way speech paths.

5. **Bell system incorrect response to Querying for Capabilities OPTIONS –** Following 183 Session Progress with SDP from Bell, CS1000 sends OPTIONS to query Bell system capability, Bell system responses with 500 Internal Server Error. When CS1000 sees codecs list in 183 SDP's response from Bell is less than what it is offering in the INVITE, CS1000 will send out OPTIONS following 183 response's message in order to query the full capability of the receiving system (Bell). CS1000 is conforming with RFC 3261, Section 11, Querying for Capabilities (page 66). The OPTIONS will allow CS1000 learn receiving system capabilities. This minor issue has been brought to Bell's team attention. **This issue has NO user impact**.

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 Trunking 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, SM, ASBC and Bell system. In this configuration, ASBC on enterprise side is configured to periodically perform OPTIONS ping to Bell system. Also outbound calls from enterprise CS1000 to PSTN will require authentication with Bell system.

For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

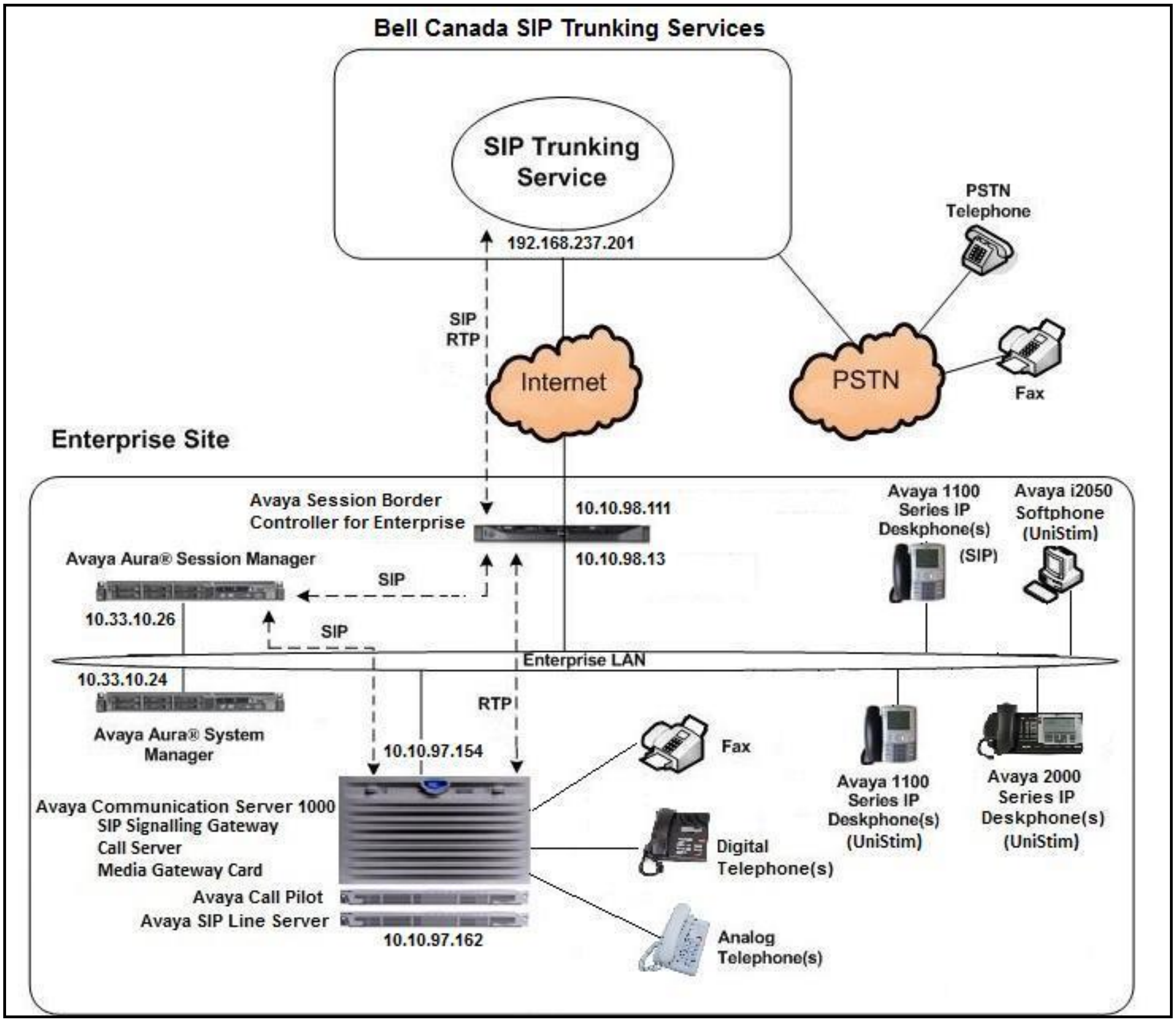


Figure 1- Network diagram for Avaya and Bell SIP Trunking Service

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment/Software	**Release/Version**
Avaya Communication Server 1000 (CPPM)	Call Server: 7.65 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 Aura® Session Manager running on an Avaya S8800 Server	6.3.0 (Build No. 6.3.0.0.630002-6.3.4.634012)
Avaya Session Border Controller for Enterprise	6.2.1.Q07
Avaya IP Deskphones: 2050 (Soft) 1140 (SIP) 1140 (UniStim) 2007 (UniStim) 3904 (Digital) Analog	 4.04.0106 04.03.12.00 0625C8Q 0621C8Q N/A N/A
HP Officejet 4500 Fax	N/A
Bell Canada SIP Trunking Components	
Component	**Release**
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 CS1000 listed as below:

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

5. Configure Avaya Communication Server 1000

These Application Notes use the Incoming Digit Translation feature to receive the calls, the Numbering Plan Area Code (NPA), and Special Number (SPN) features to route calls from the CS1000, over a SIP trunk via Bell system, to PSTN.

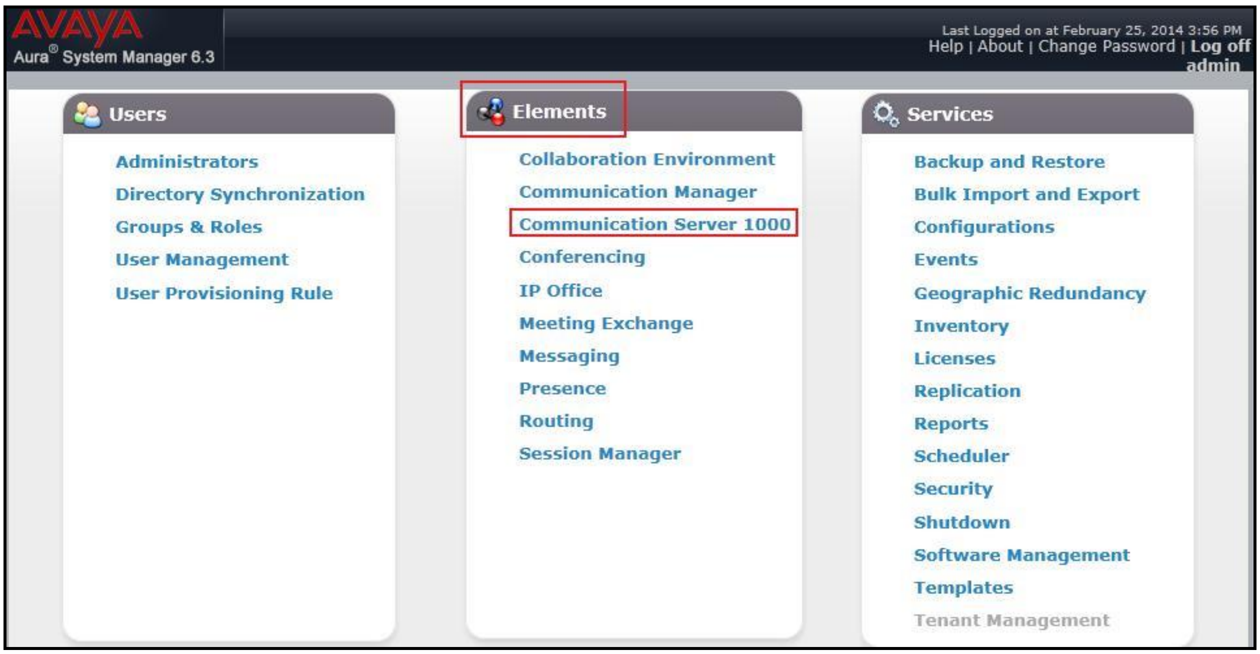
These application notes assume that the basic CS1000 configuration has already been administered. For further information on CS1000, please consult the references in **Section 11.**

The procedures below describe the configuration details of configuring a CS1000 SIP trunk.

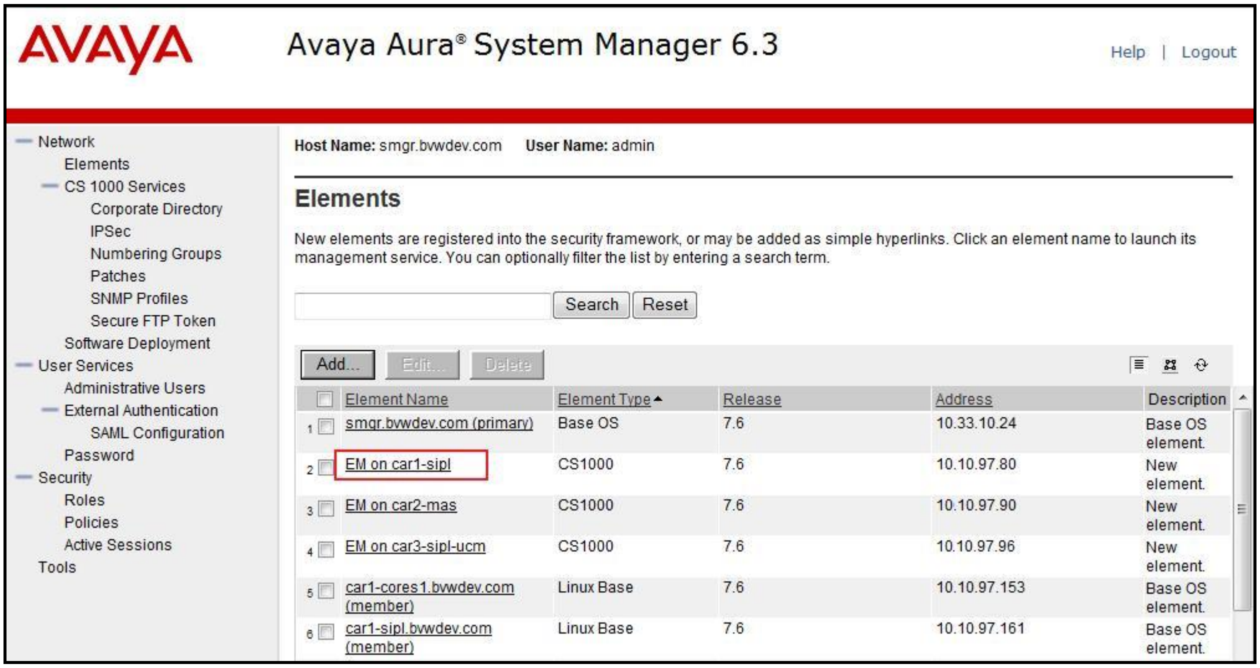
5.1. Log in to Communication Server 1000 System

5.1.1. Log in to System Manager and Element Manager (EM)

Open an instance of a web browser and connect to the Avaya Aura® 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**.



The **Elements** screen is displayed. Click on the **Element Name** of the CS1000 Element as highlighted in red box as below:



The CS1000 Element Manager **System Overview** page is as bellow.

5.1.2. Log in to Call Server

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

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

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

login as: **< --- enter an account with administrator credentials**

Nortel Networks Linux Base 7.65
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@10.10.97.154's password: **<----enter the password**
Last login: Thu Feb 20 16:02:14 2014 from 10.10.98.78
[admin2@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 #09 LOGGED IN ADMIN 11:09 24/02/2014
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.

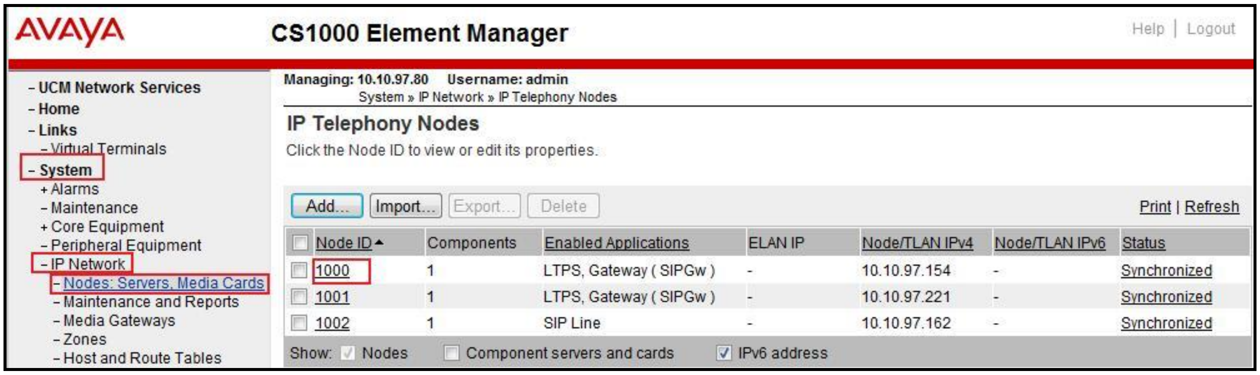
>

5.2. Administer an IP Telephony Node

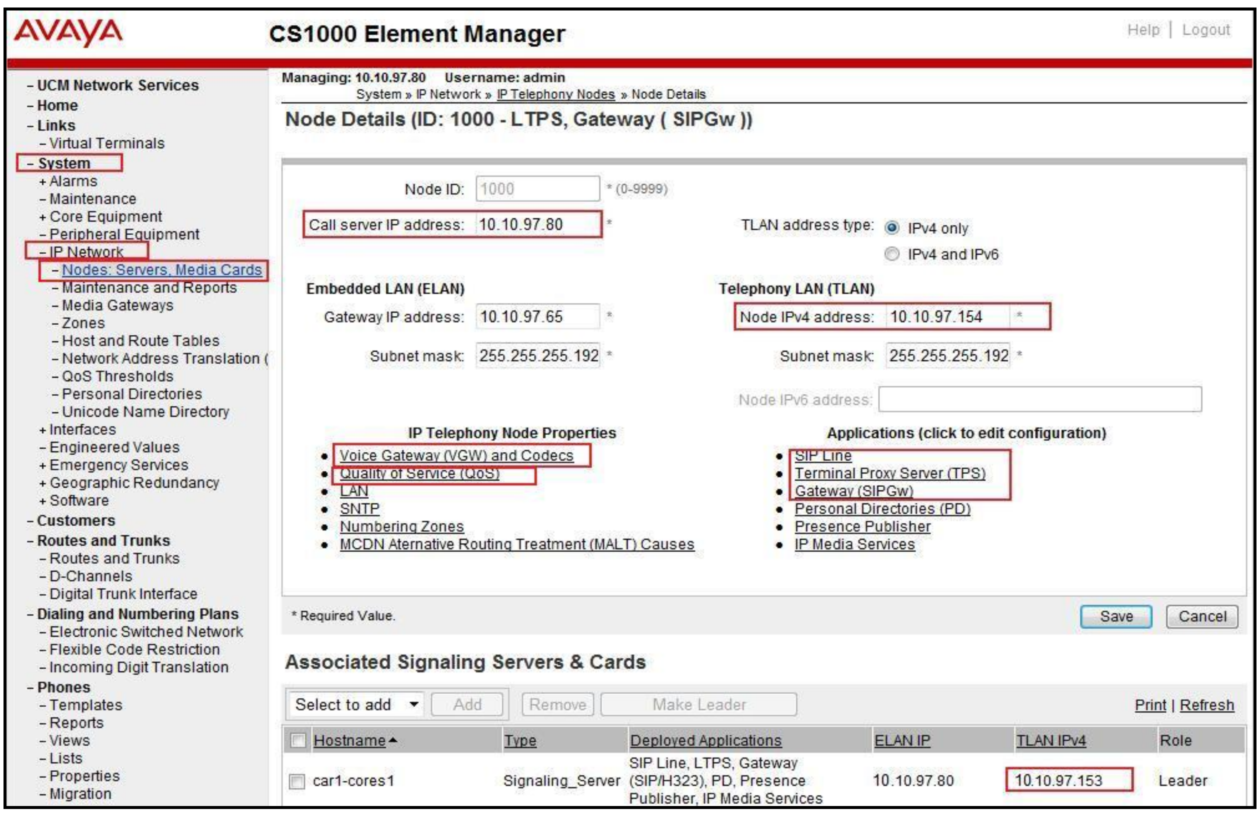
This section describes how to configure an IP Telephony Node on CS1000.

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 1000) in CS1000 IP network to work with Bell. For further information on CS1000, please consult the references in **Section 11**. Select **System → IP Network → Nodes: Servers, Media Cards** and then click on the **Node ID** as shown.

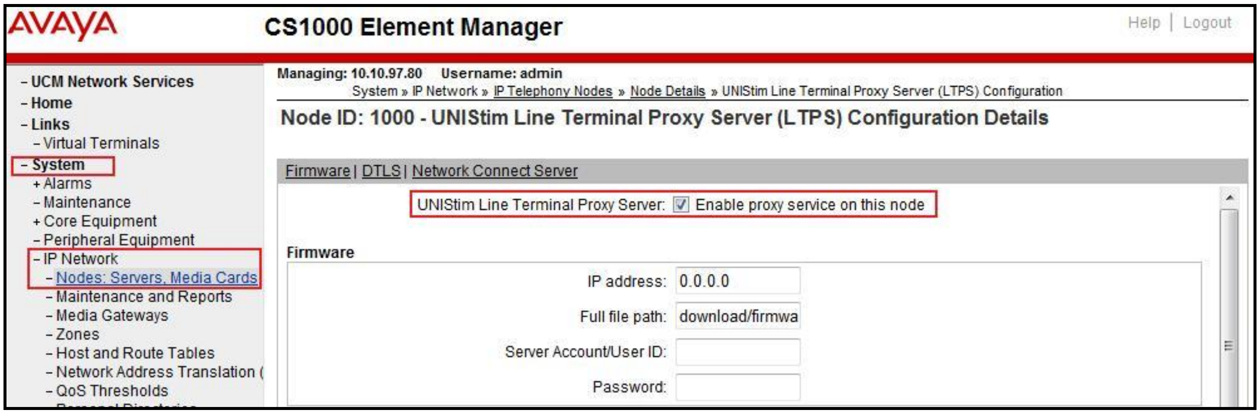


The **Node Details** screen is displayed with the IP address of the CS1000 node. **Call server IP address: 10.10.97.80**. The **Node IPv4 address 10.10.97.154** is a virtual address which corresponds to the **TLAN IPv4 10.10.97.153** of the Signaling Server/SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP address to communicate with other components to process SIP calls. The **Node Details** screen is displayed bellow with the IP Telephony Node Properties and Applications.



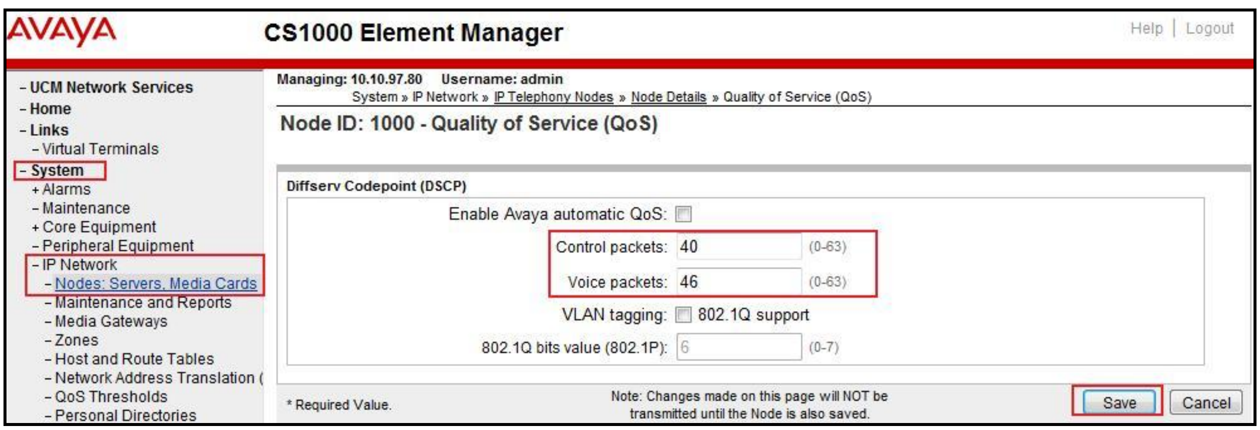
5.2.2. Administer Terminal Proxy Server (TPS)

Continuing from **Section 5.2.1**, on the **Node Details** page select **Terminal Proxy Server** (**TPS**). Check the **UNIStim Line Terminal Proxy Server** checkbox to enable proxy service on this node and then click **Save** (not shown).



5.2.3. Administer Quality of Service (QoS)

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



5.2.4. Synchronize New Configuration

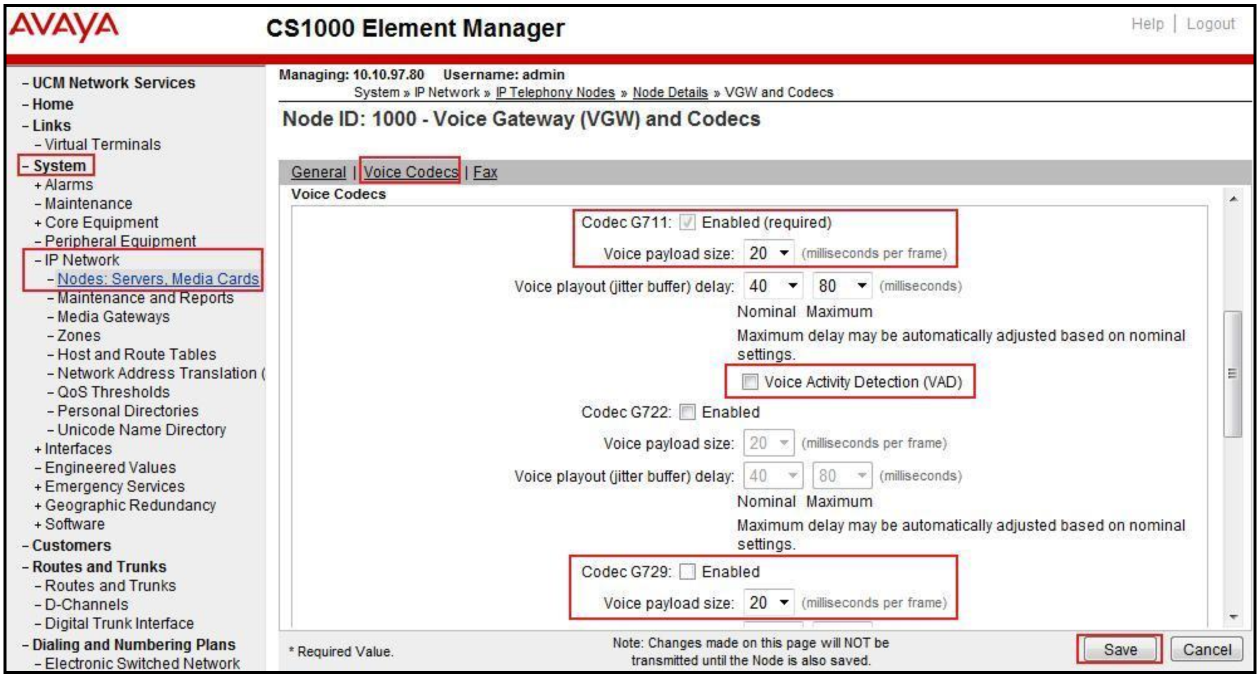
Continuing from **Section 5.2.3**, return to the **Node Details** page and click the **Save** button. The **Node Saved** screen is displayed. Click **Transfer Now** (not shown). The **Synchronize Configuration Files (Node ID <1000>)** screen is displayed (not shown). Check the **Signaling Server** checkbox and click **Start Sync** (not shown). When the synchronization completes, check the **Signaling Server** checkbox and click **Restart Applications** (not shown).

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec G.711

On the **Node Details** page shown in **Section 5.2.1,** click on **Voice Gateway (VGW) and Codecs** and then under **Voice Codecs** section.

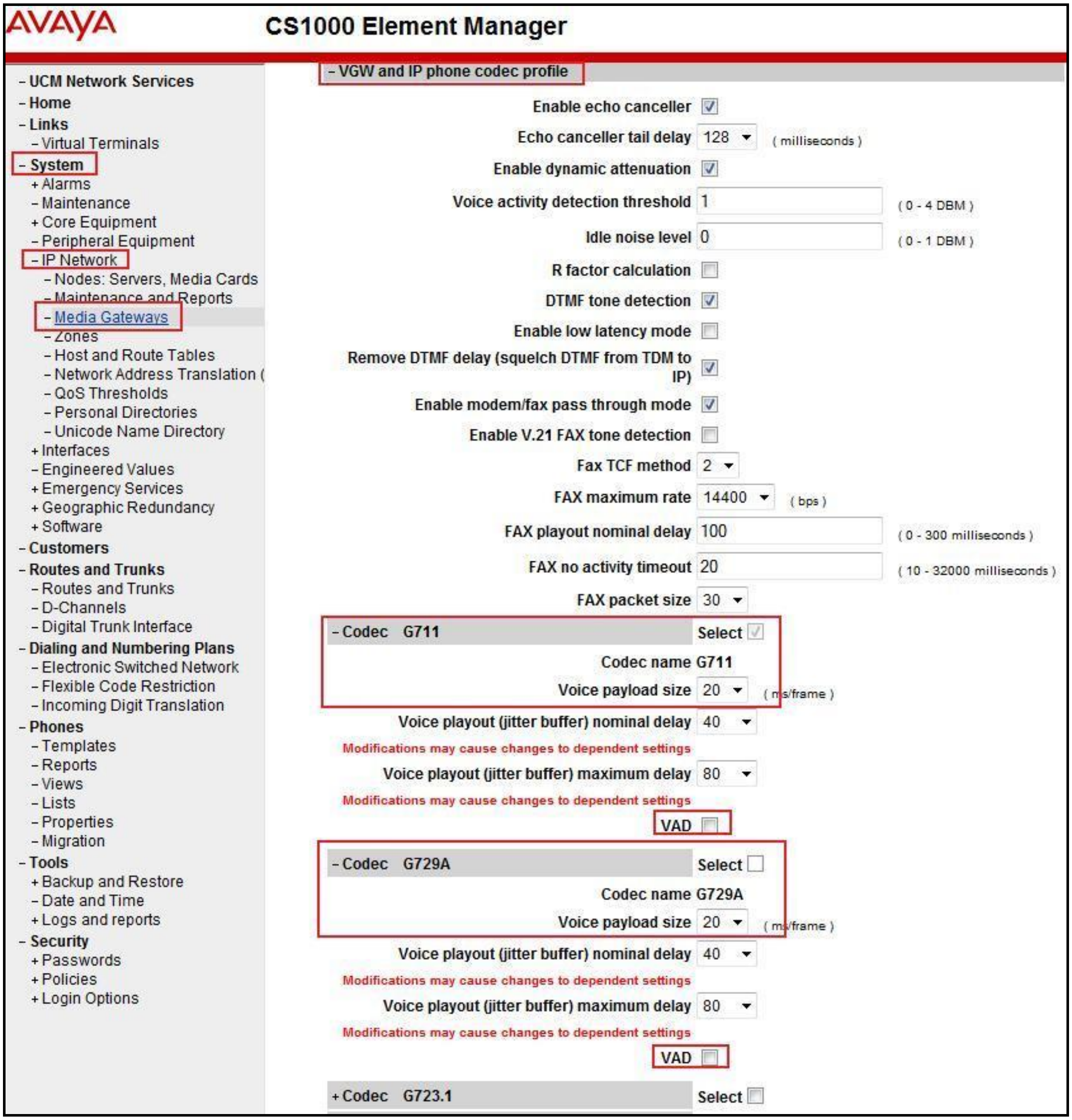
The Bell system supports **G.711/time 20ms** with **Voice Activity Detection (VAD)** checkbox unchecked. Ensure **Codec G.729** is unchecked. Click **Save**.



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, select **System → IP Network → Media Gateways**. The Media Gateways page will appear (not shown). Click on **MGC** which is located on the right of the page (not shown). In the following screen, scroll down to select **Codec G.711** and deselect **Codec G.729A** and uncheck both **VAD** as shown below. Scroll down to the bottom of the page and click the **Save** button (not shown).

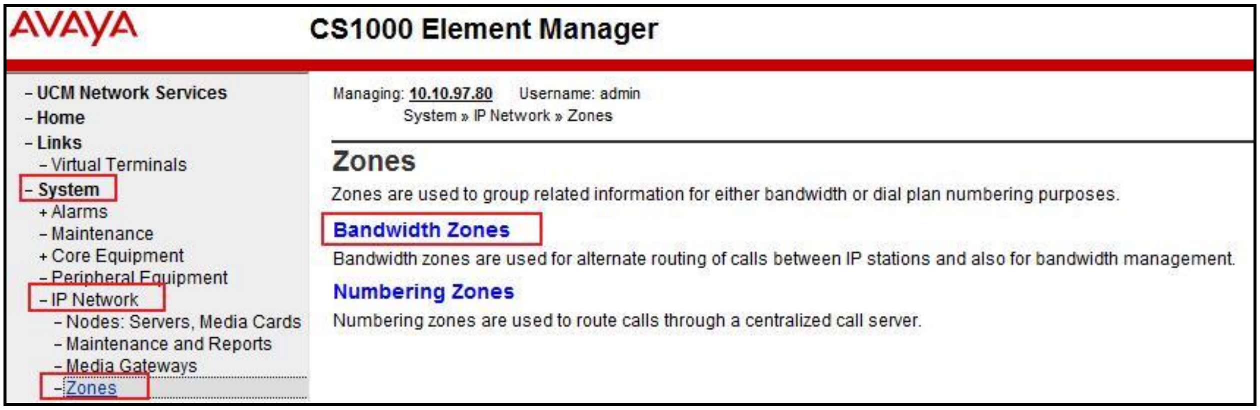


5.4. Zones and Bandwidth Management

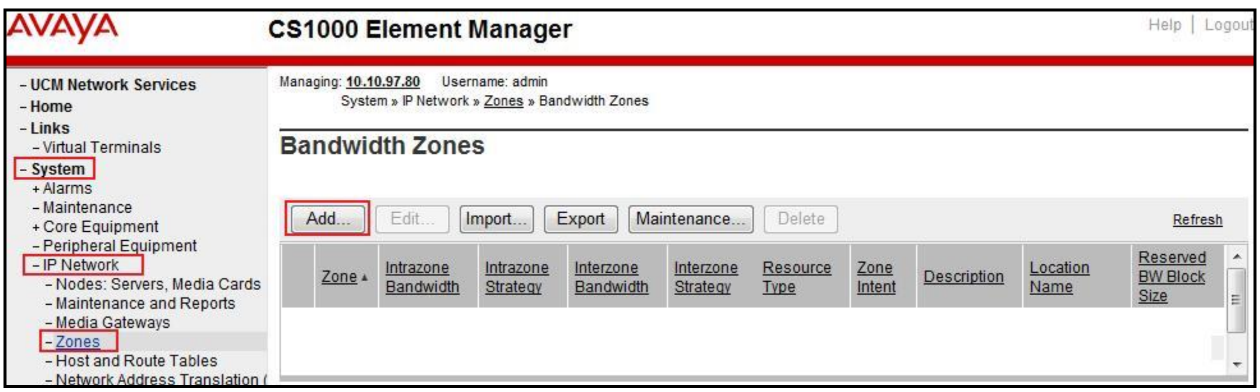
This section describes the steps to create two zones: zone 10 for the VGW and IP sets, and zone 255 for the SIP Trunk.

5.4.1. Create a Zone for IP Telephones (Zone 10)

The following figures show how to configure a zone for VGW and IP sets for bandwidth management purposes. The bandwidth strategy can be adjusted to preference. Select **IP Network** → **Zones** configuration from the left pane (not shown), click **Bandwidth Zones**.

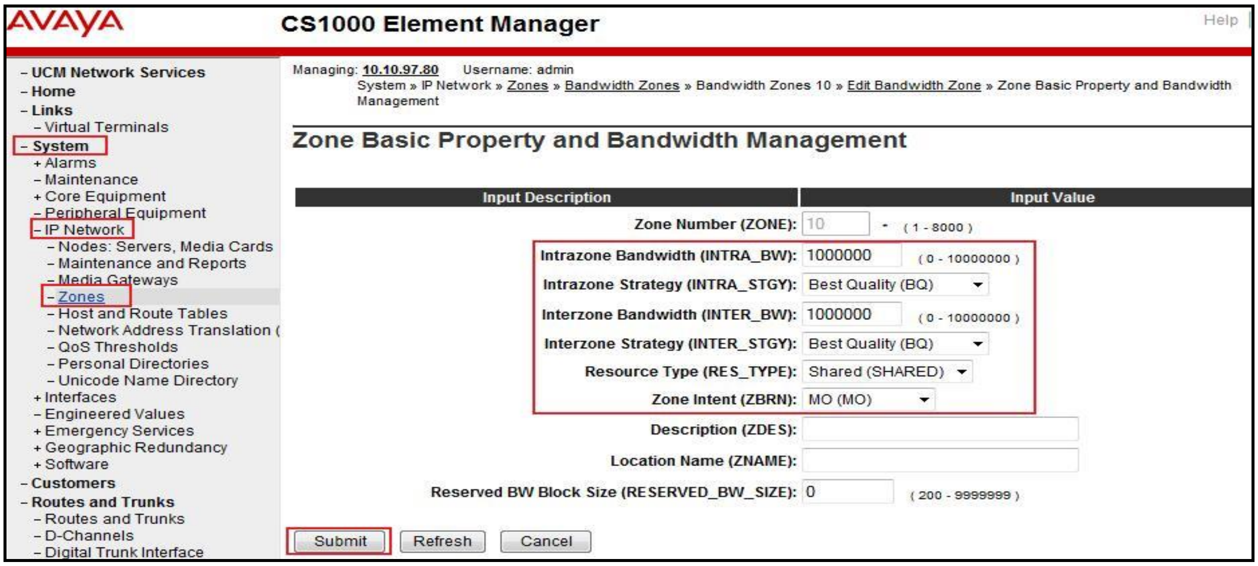


The **Bandwidth Zones** screen is displayed as shown below. Click **Add** to create new zone for IP Telephones.



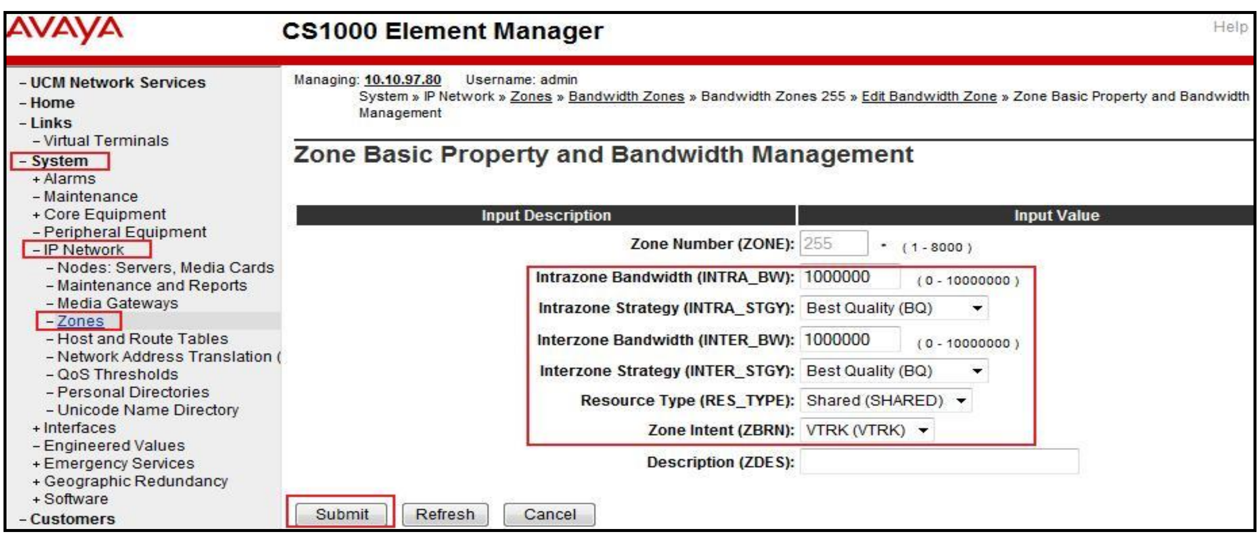
Select and input the values as shown below (in the red boxes), and click on **Submit** button.

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



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 (VTRK)** for virtual trunk as shown and then click **Submit** button.

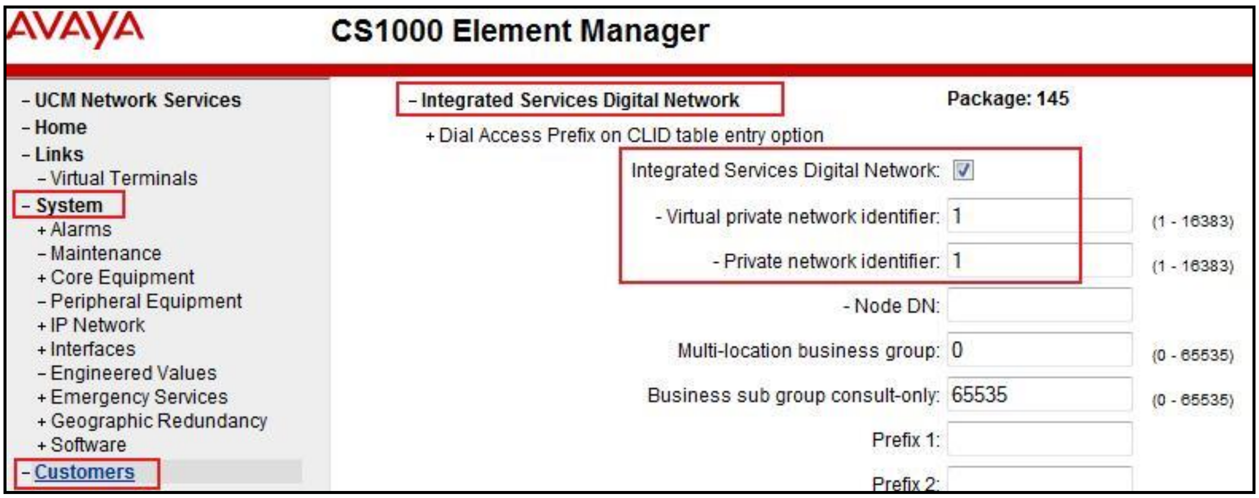


5.5. Administer SIP Trunk Gateway

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

5.5.1. Integrated Services Digital Network (ISDN)

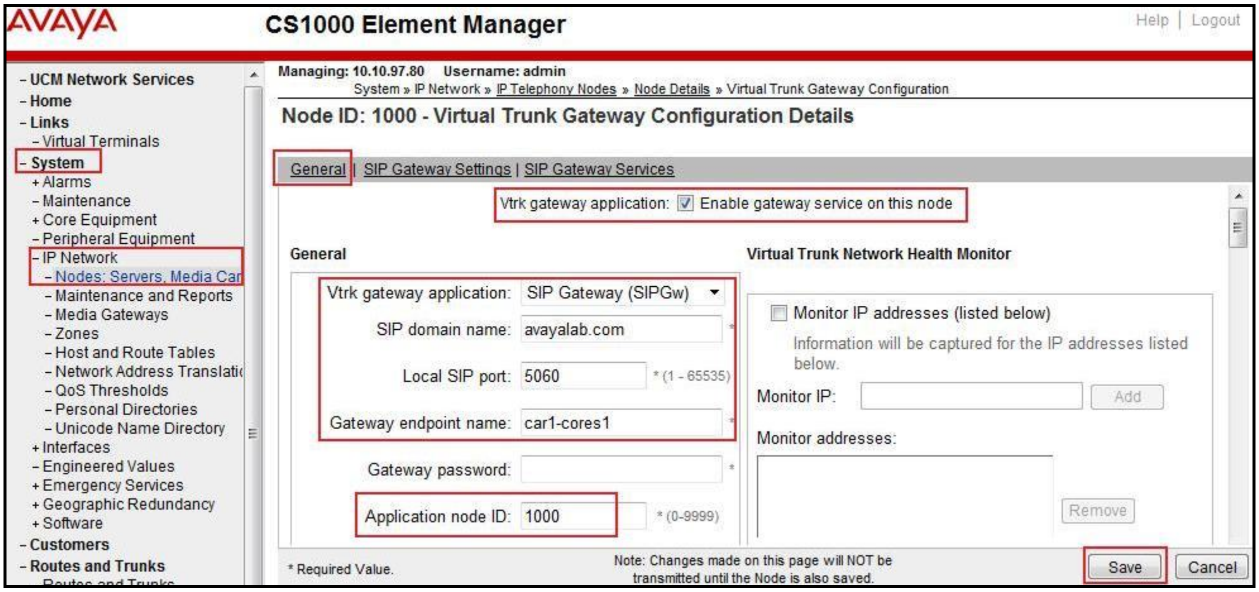
Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00** (not shown). The system can support more than one customer with different network settings and options. The **Customer 00 Edit** page will appear (not shown). Select the **Feature Packages** option from **Customer 00 Edit** page (not shown). The screen is updated with a listing of available **Feature Packages** (not all features are shown in capture 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 the **Save** button (not shown).



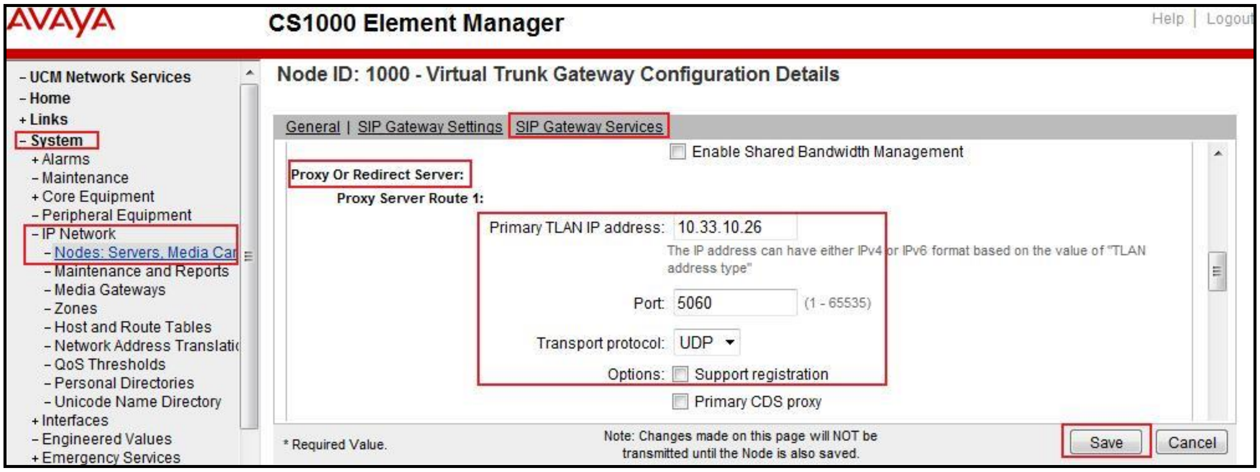
5.5.2. Administer SIP Trunk Gateway to Avaya Aura® Session Manager

On the **Node Details** page as shown in **Section 5.2.1**, 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.

- **SIP domain name**: Create a domain name, which will be used for enterprise network.
- **Local SIP port: 5060** is used.
- **Gateway endpoint name:** SIP gateway endpoint name during set up of CS1000 system.
- **Application node ID**: Node ID that is used in Section 5.2.1
- Click **Save**.



Click on the **SIP Gateway Services** 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 capture below. Enter the internal interface IP address of SM in the **Primary TLAN IP address** field (This IP address pattern is defined in **Section 6.4**). Enter **Port**: **5060** and **Transport protocol**: **UDP**. Uncheck **Support registration** checkbox. Click **Save**.



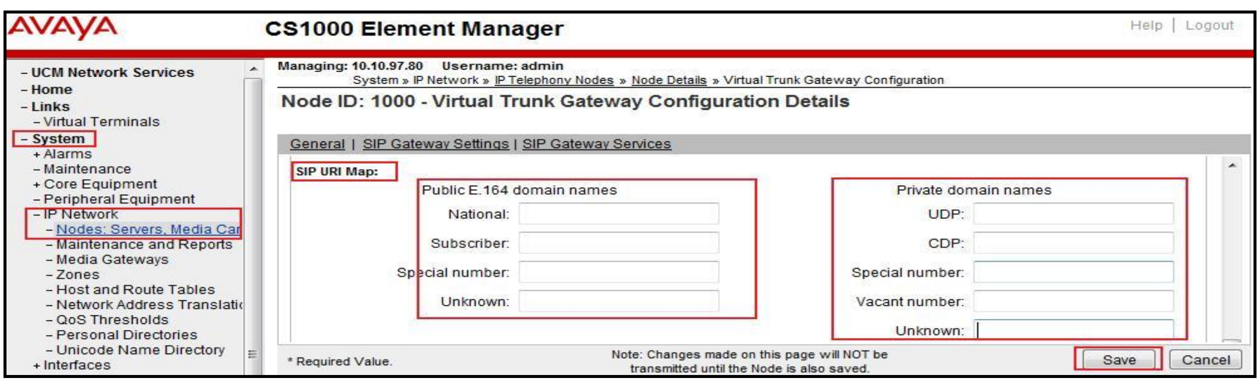
Continue with **Virtual Trunk Gateway Configuration Details** page above, scroll to the **SIP URI Map** section.
Under the **Public E.164 domain names**, enter the following:

- **National**: Empty this field
- **Subscriber**: Empty this field
- **Special Number**: Empty this field
- **Unknown**: Empty this field

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

- **UDP**: Empty this field
- **CDP**: Empty this field
- **Special Number**: Empty this field
- **Vacant number**: Empty this field
- **Unknown**: Empty this field

The remaining fields can be left at their default values. Click **Save**.



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

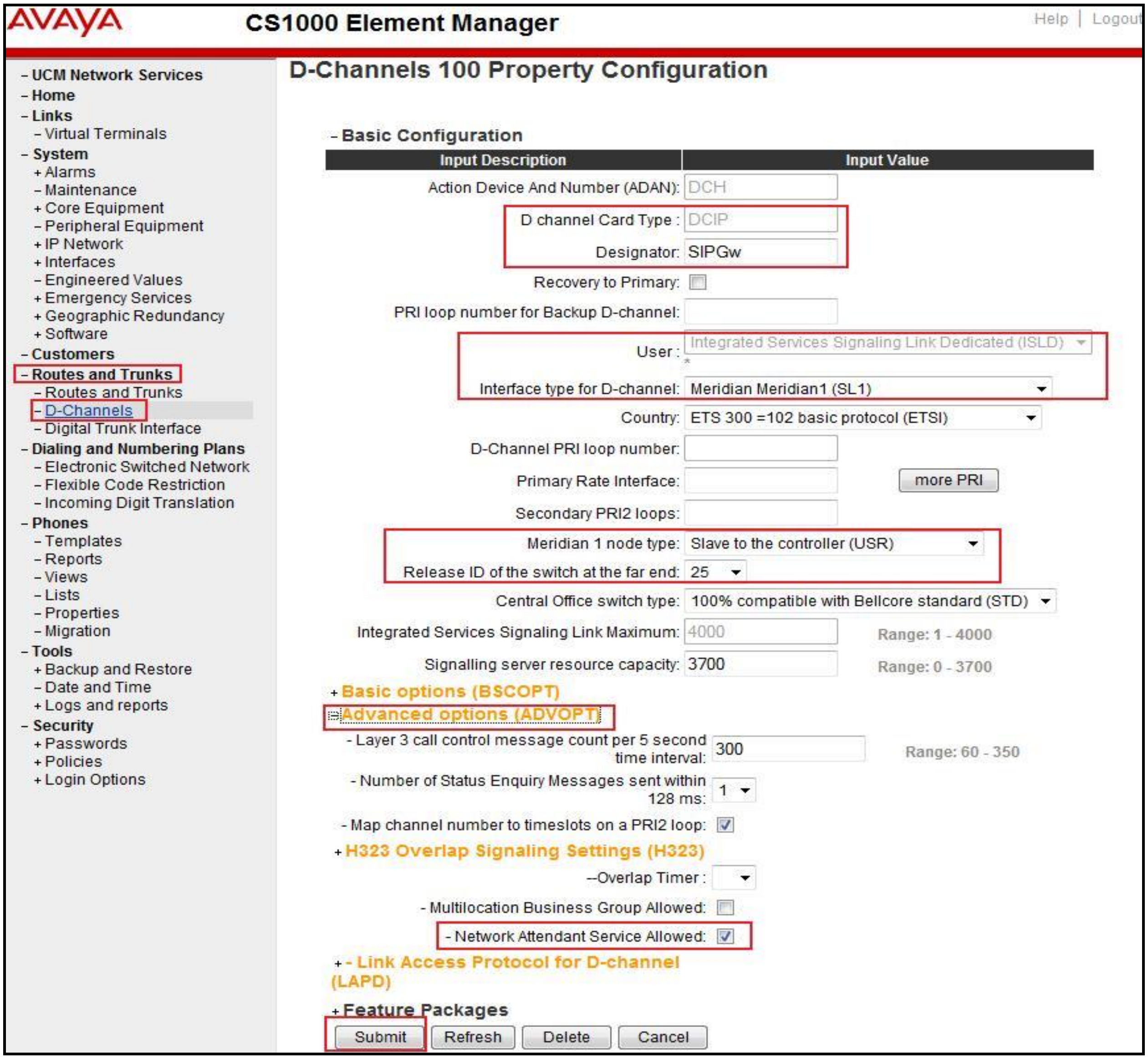
5.5.3. Administer Virtual D-Channel

Select **Routes and Trunks** → **D-Channels** 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 (in this case is **100**) and type **DCH** as shown. Click **to Add** button.

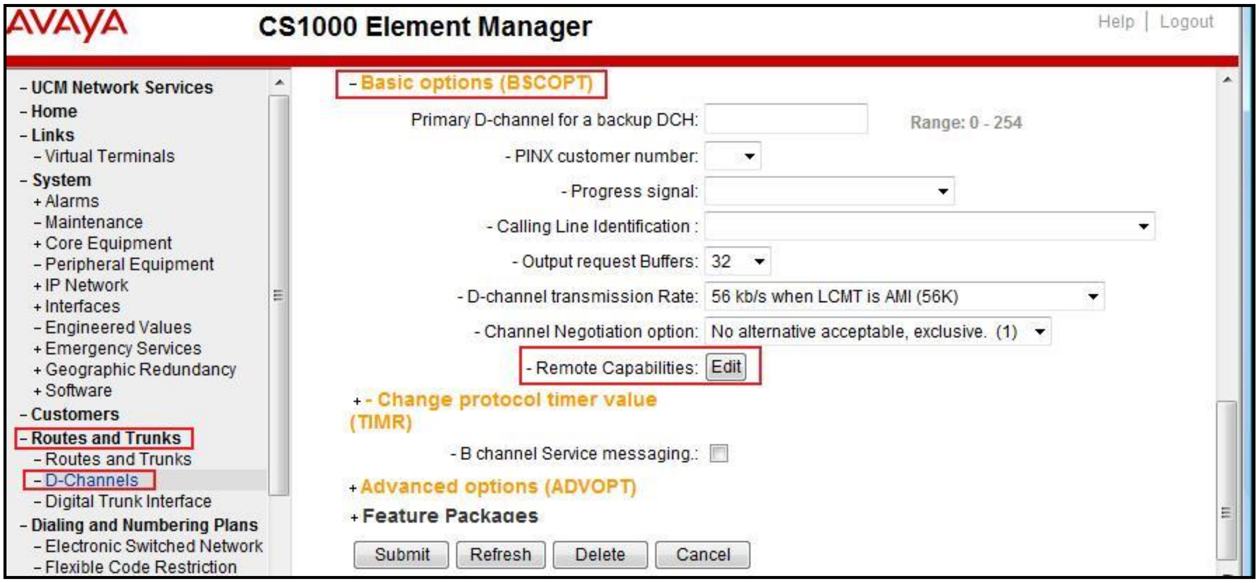
The **D-Channels 100 Property Configuration** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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**

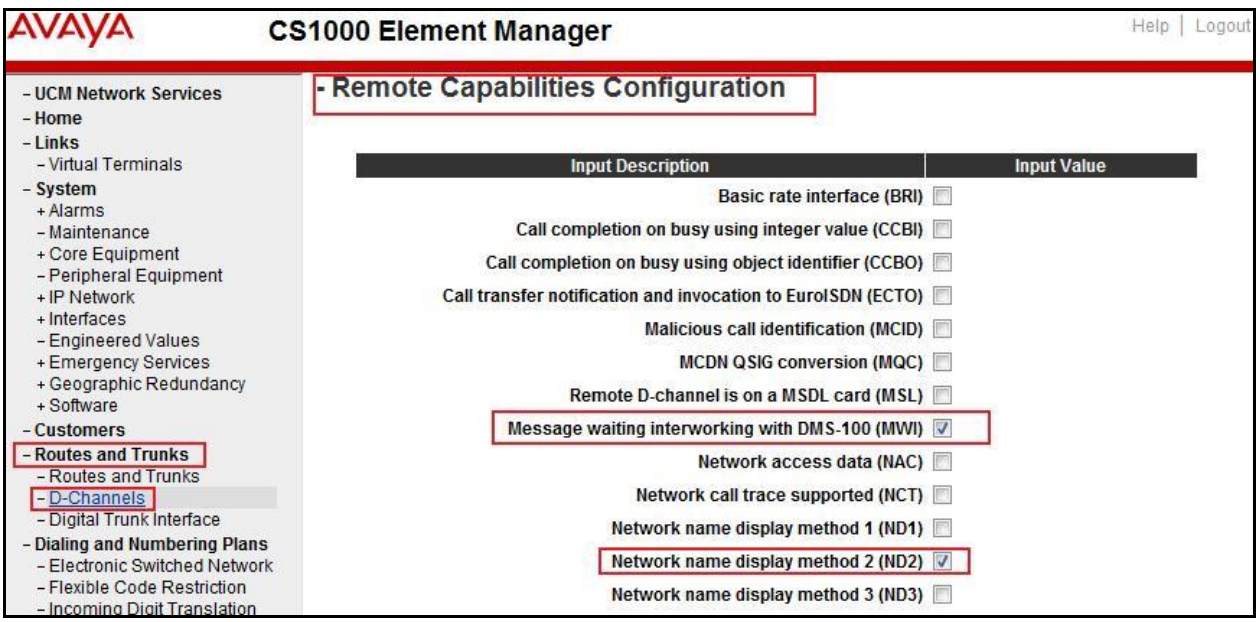
Click on **Advanced options (ADVOPT)**. Check on the **Network Attendant Service Allowed** checkbox as shown. Other fields are left as default. Click **Submit** button.



On the same page, choose the **Basic Options (BSCOPT)** and click **Edit** button on the **Remote Capabilities** field.



The **Remote Capabilities Configuration** page appears as shown below. Check **Network name display method** (**ND2)** and **Message waiting interworking with DMS-100** (**MWI)** checkboxes.



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

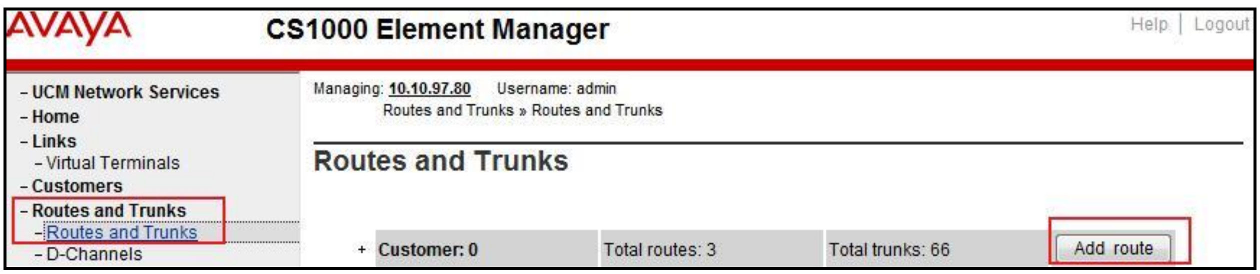
Click **Submit** button (not shown).

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, click **Add** button to create a new one as shown below. In this example, **Superloop Numbers 4**, **96**, **100**, and **104** have been added and are being used.

5.5.5. Administer Virtual SIP Routes

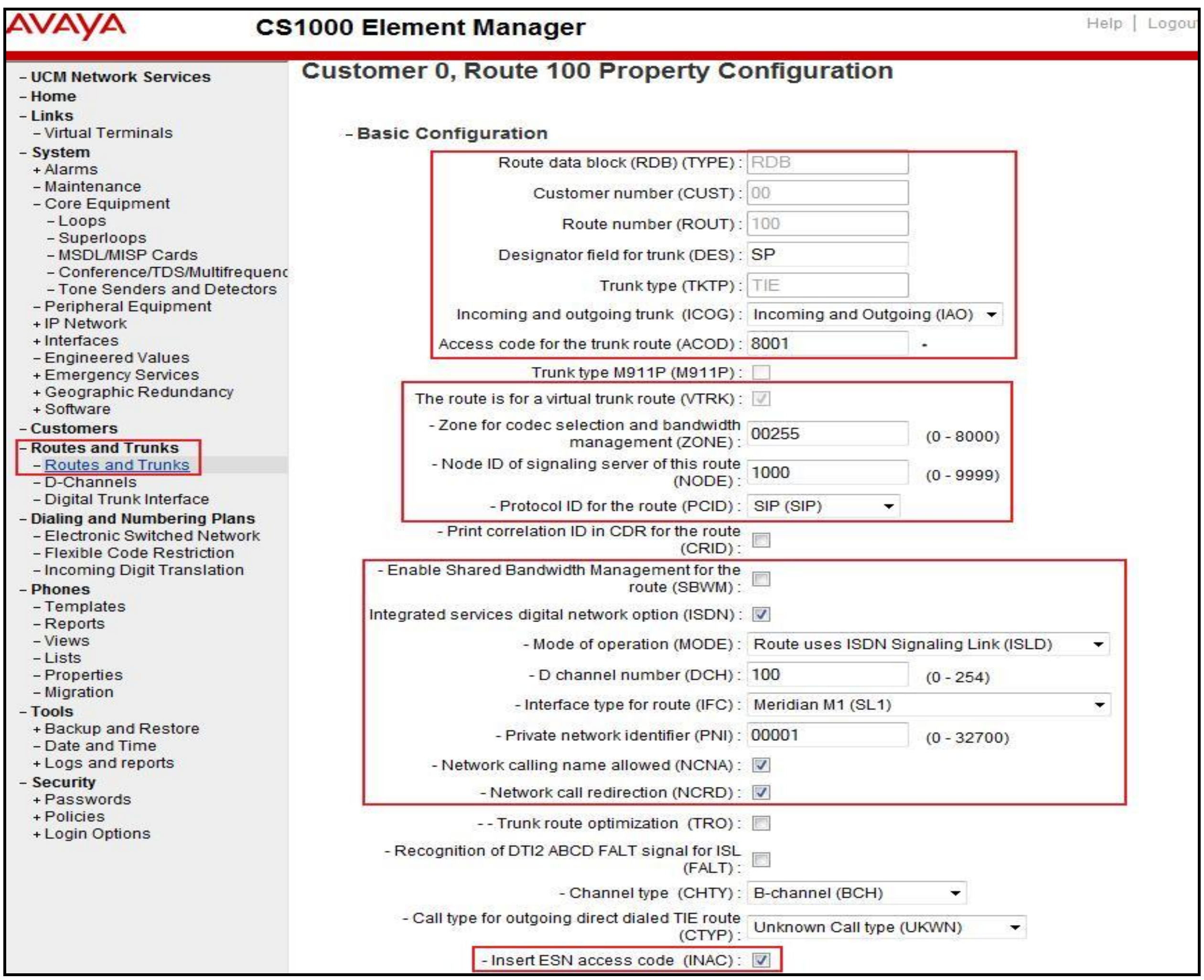
Select **Routes and Trunks → Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click **Add route** button as shown.



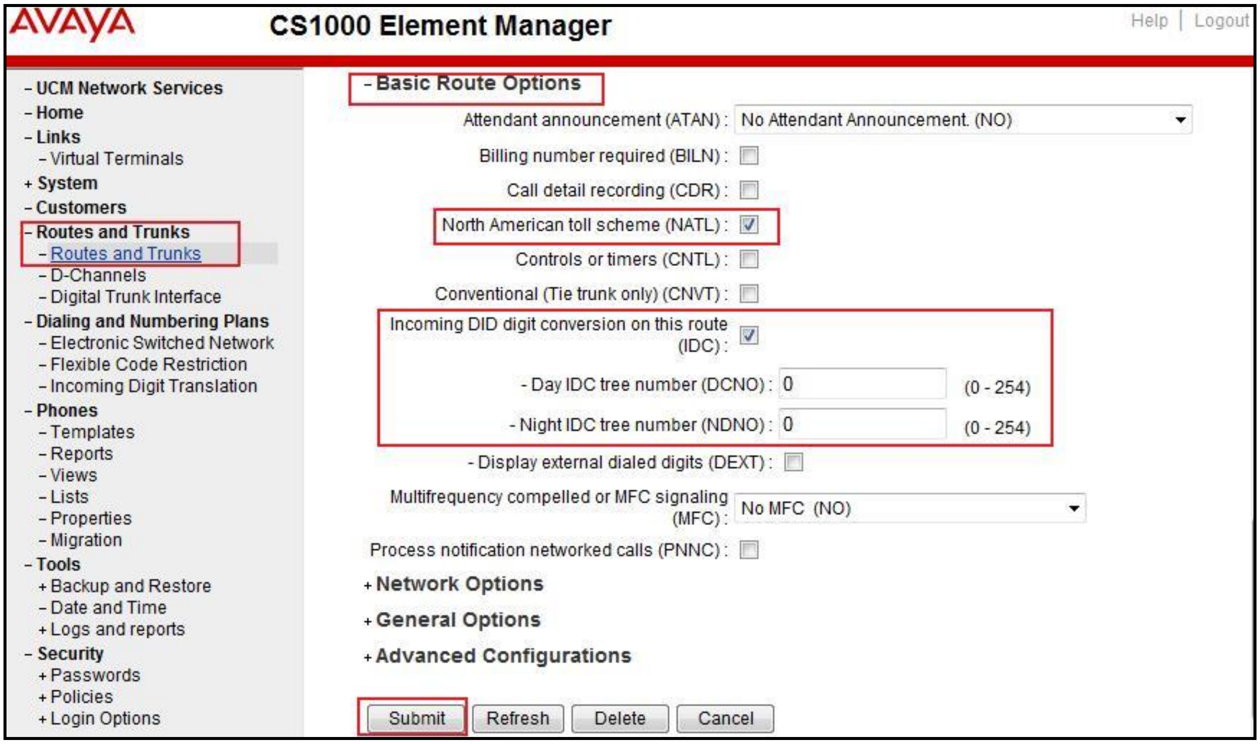
The **Customer 0**, new **Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed to put the following values for the specific fields, and retain the default values for the remaining fields. The screenshot of Basic Configuration section of existing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

- **Route number (ROUT)**: Select an available route number (example: route **100**).
- **Designator field for trunk (DES)**: A descriptive text (**SP**).
- **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: **8001**).
- 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 **1000** (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.
  - **Route data block (RDB)**: Type **RDB** is used as default
  - **Customer number (CUST)**: Customer **00** is used
  - **Mode of operation (MODE)**: Select Route uses ISDN Signalling Link (**ISLD**)
  - **D channel number (DCH)**: Enter **100** (created in **Section 5.5.3**)
  - **Network calling name allowed (NCNA)**: Check the field.
  - **Network call redirection (NCRD)**: Check the field.
  - **Insert ESN access code (INAC):** Check the field.
  - **Enable Shared Bandwidth Management for the route (SBWM):** uncheck.
  - **Interface type for route (IFC)**: Select **Meridian M1 (SL1)**.
  - **Private network identifier (PNI)**: **00001** is used.

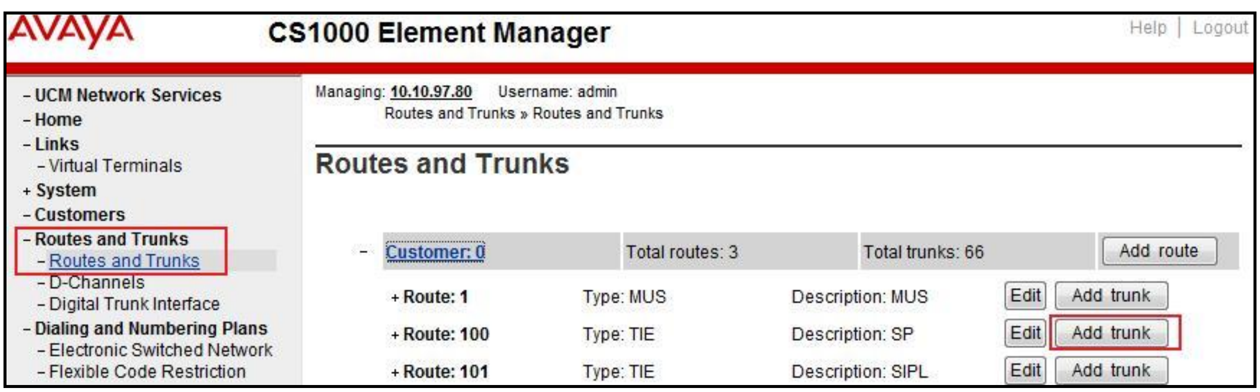


Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)** checkboxes. Enter **0** for both **Day IDC tree number** and **Night IDC tree number**. Click **Submit** button.



5.5.6. Administer Virtual Trunks

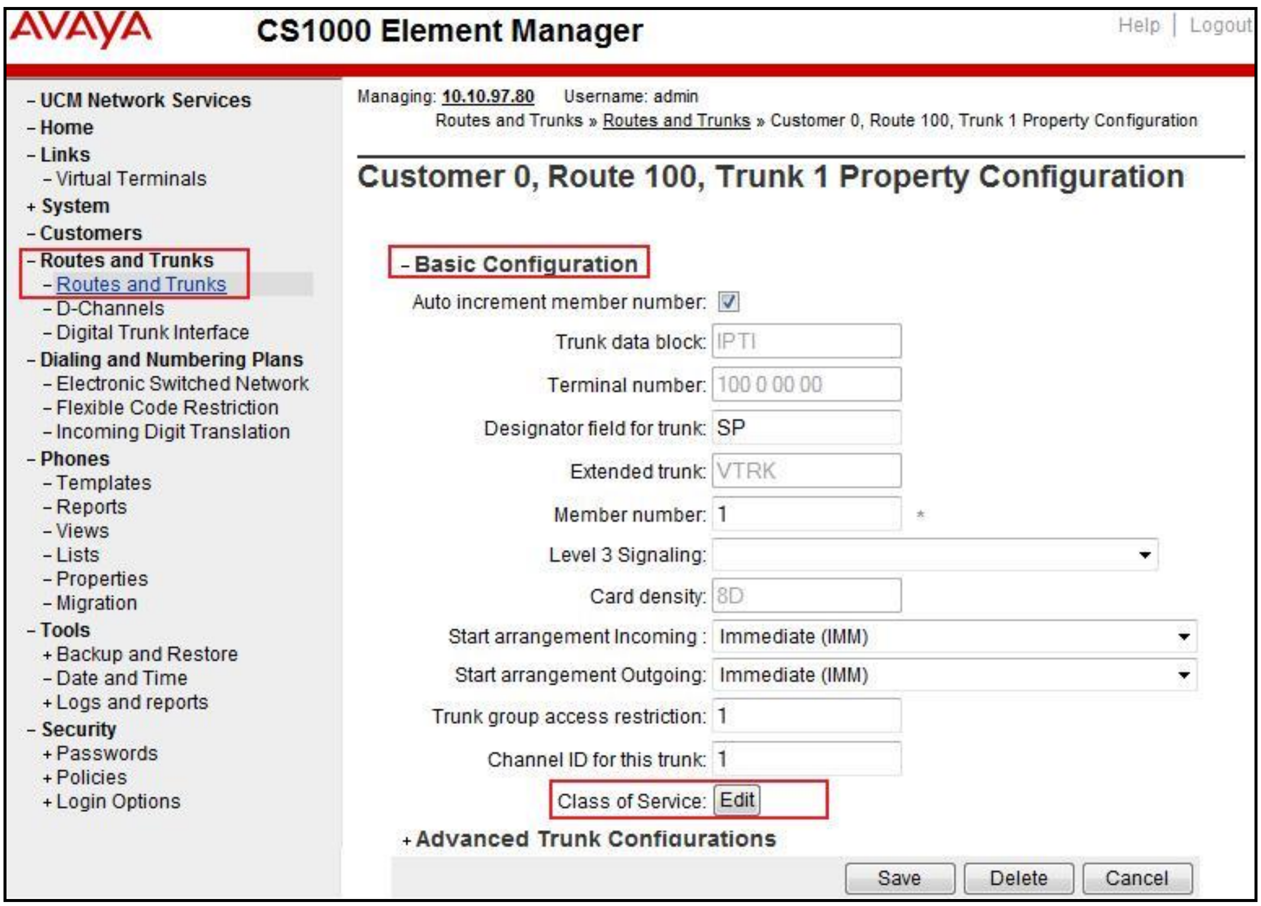
Select **Routes and Trunks → Route and Trunks**. The Route list is now updated with the newly added routes. In the example, the **Route 100** was added. Click **Add trunk** button as shown below.



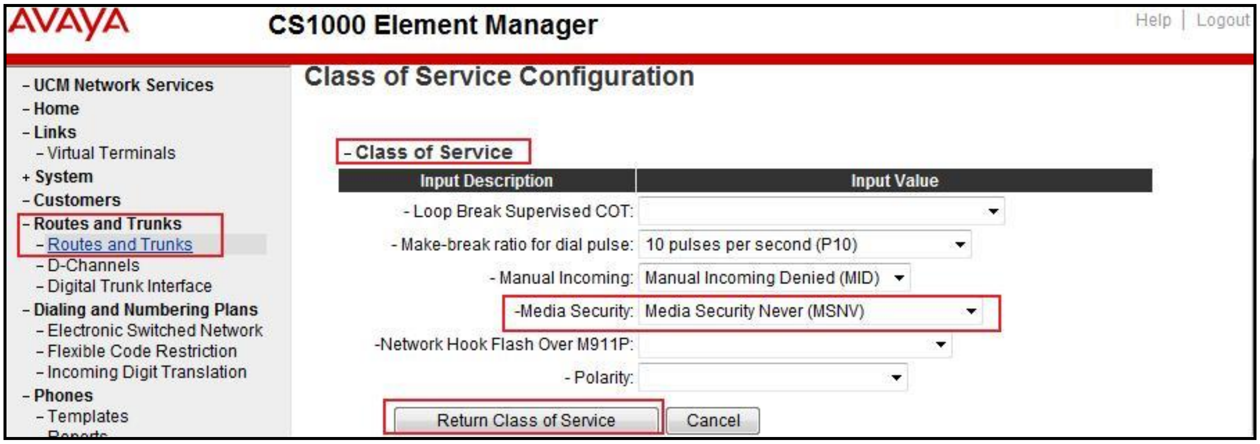
The **Customer 0, Route 100, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. The Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service** at the bottom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

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 (not shown). In the screen capture bellow, Trunk 1 is used in this testing.

- **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



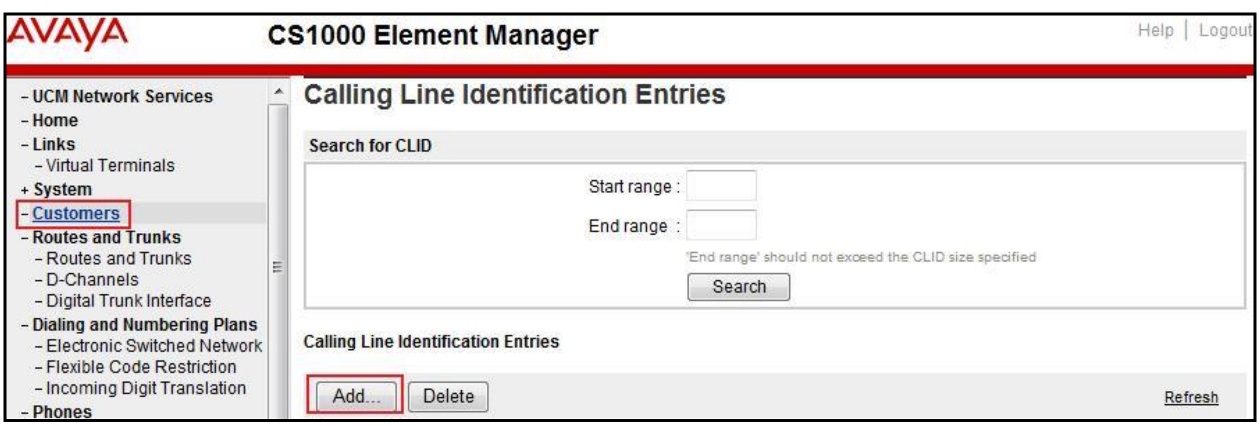
For **Media Security**, select **Media Security Never** (**MSNV)**. Enter the values for the specified fields as shown in capture below. Scroll down to the bottom of the screen, click **Return Class of Service** and then the **Save** button (not shown in capture above).



5.5.7. Administer Calling Line Identification Entries

Select **Customers** (on the left pane) → **00** → **ISDN and ESN Networking** (not shown). Click **Calling Line Identification Entries**.

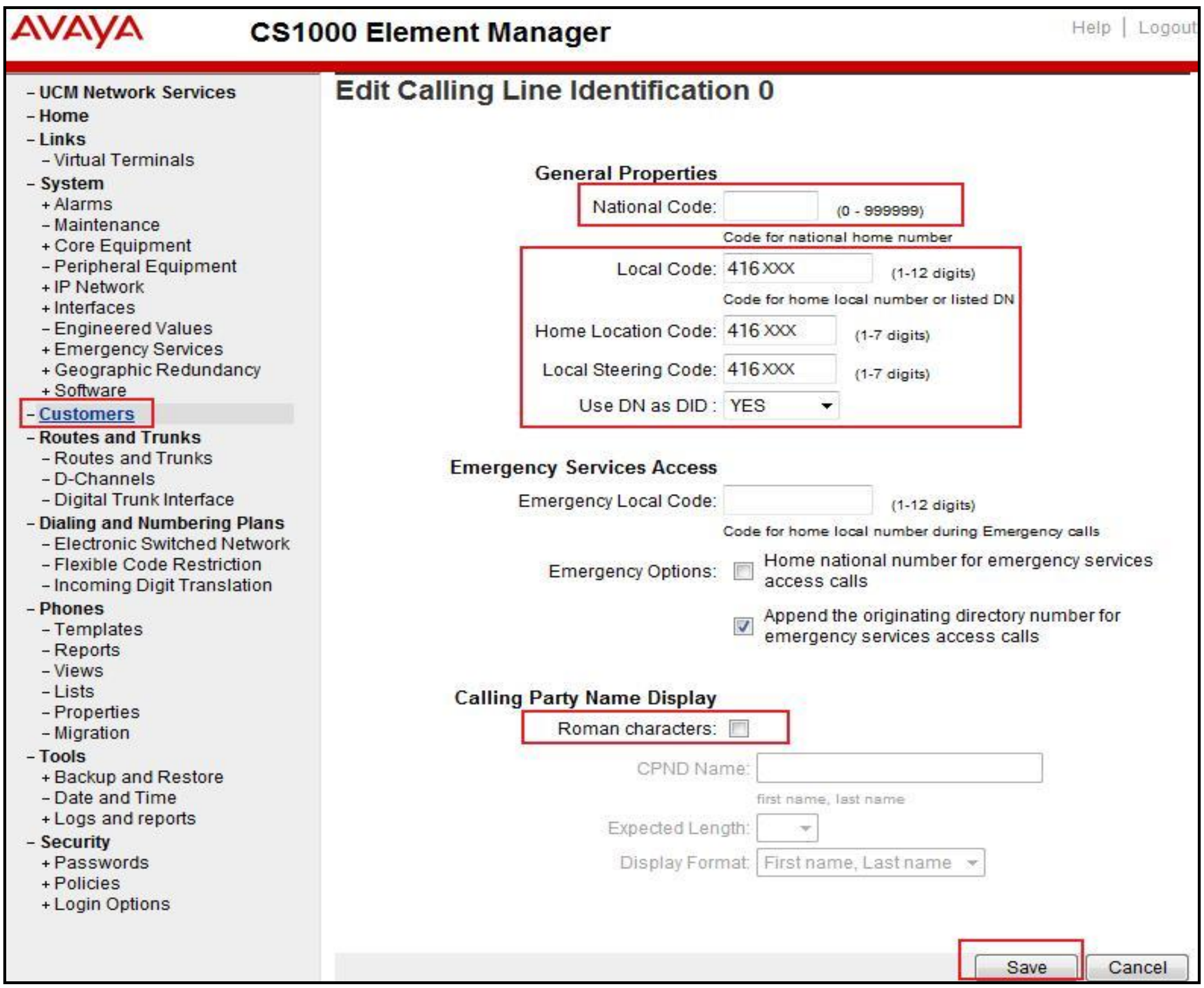
Click **Add** button as shown.



The add entry **0** screen is displayed (not shown). Enter 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 capture below:

- **National Code**: left blank.
- **Local Code**: input prefix digits assigned by Bell, in this case it is 6 digits – **416XXX**. This will be used for call display purpose for **Call Type = Unknown**.
- **Home Location Code**: input prefix digits assigned by Bell, in this case it is 6 digits – **416XXX**. This will be used for call display purpose for **Call Type = National (NPA)**.
- **Local Steering Code**: input prefix digits assigned by Bell, in this case it is 6 digits – **416XXX**. This 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 **Save**.



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.

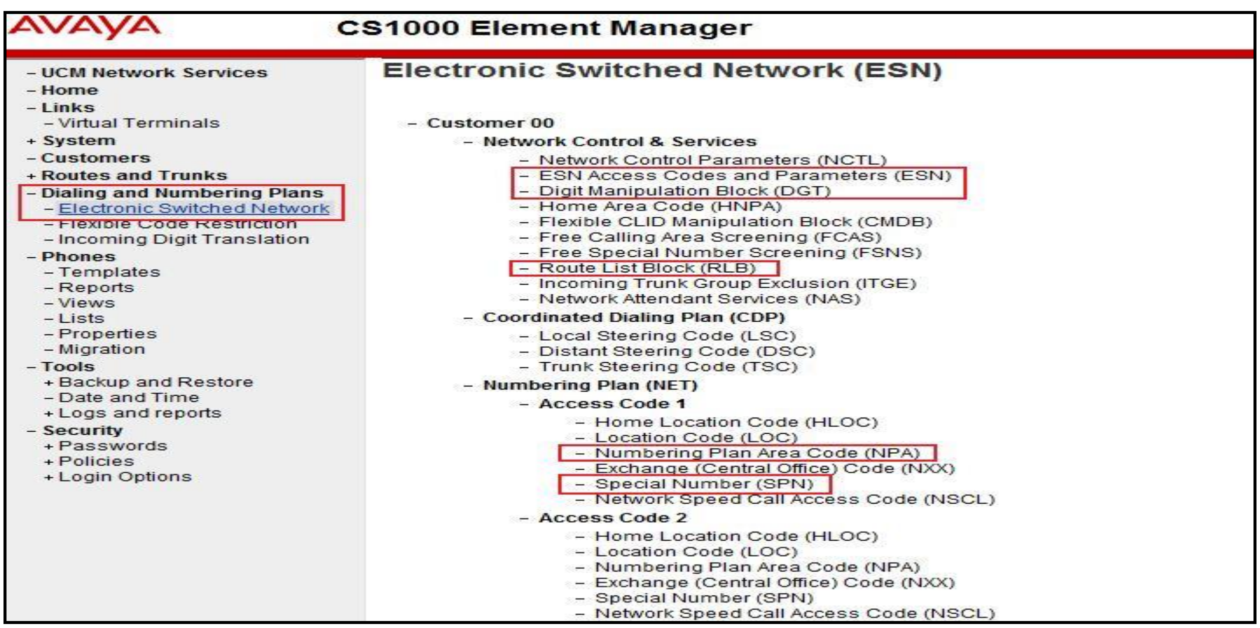
Log in to the Call Server Overlay CLI (please refer to **Section 5.1.2** for more details). Allow External Trunk to Trunk Transfer for Customer Data Block by using **ld 15**.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35359353    USED U P: 8485941 1034575    TOT: 45879869
DISK SPACE NEEDED: 1883 KBYTES
REQ: chg
TYPE: net

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

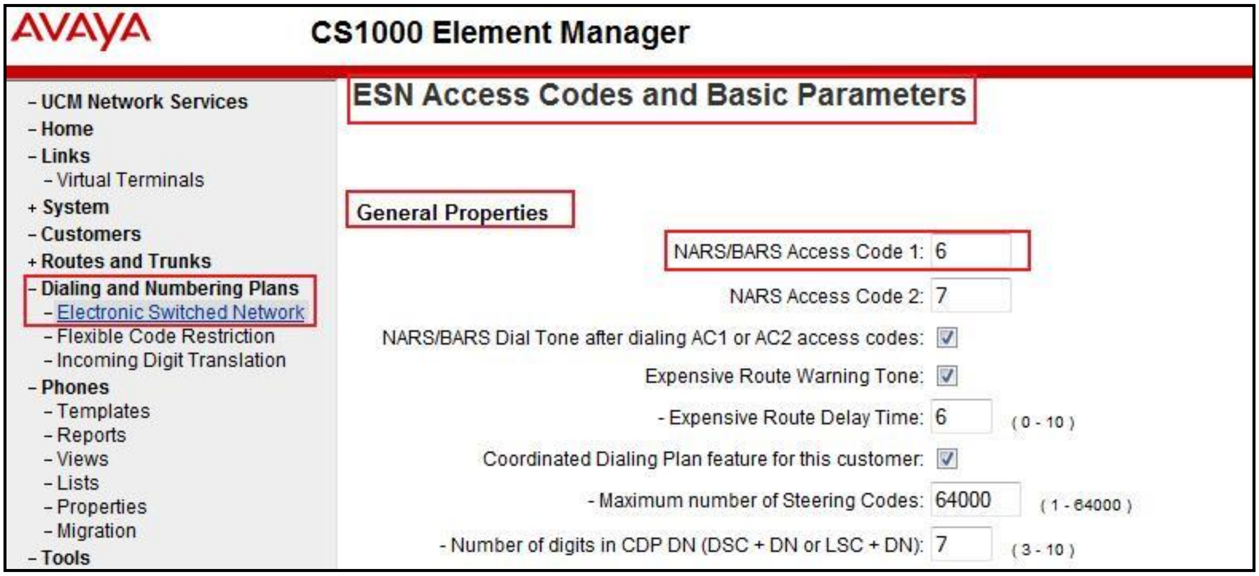
5.6. Administer Dialing Plans

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.



Select **ESN Access Codes and Paramenters (ESN)**. In the **ESN Access Codes and Basic Parameters** page, define **NARS/BARS Access Code 1** as shown. Click **Submit** button (not shown).



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**. In this provisioning, the idea is to disassociate the **NPA** and **SPN** in **AC2** so that the system will be forced to associate **NPA** and **SPN** with **AC1** (not shown).

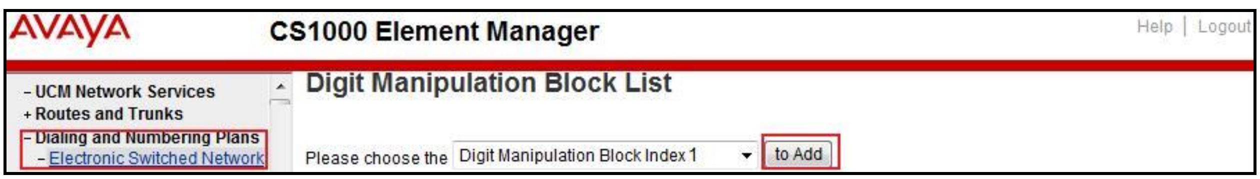
```
>ld 15
CDB000
MEM AVAIL: (U/P): 35359353    USED U P: 8485941 1034575    TOT: 45879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

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**.

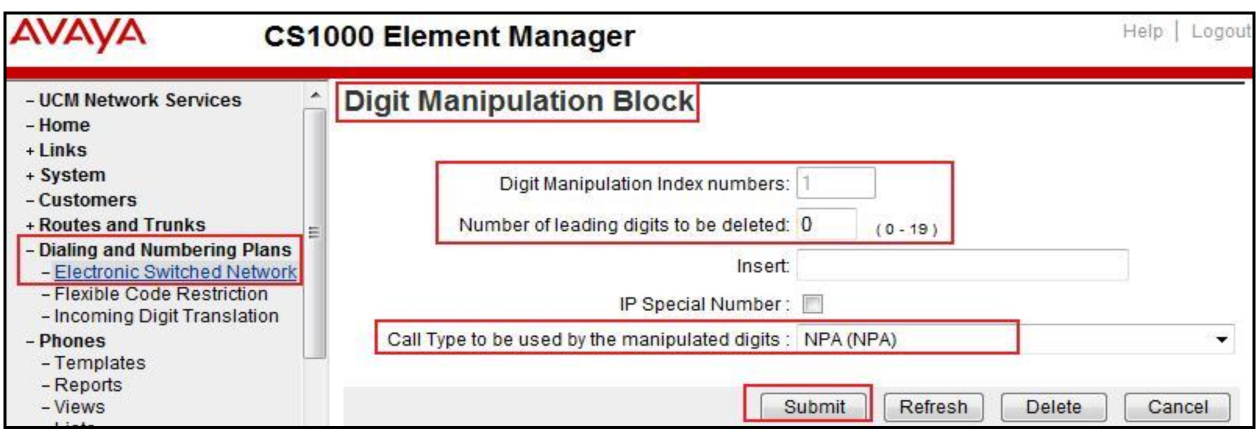
```
>ld 21
PT1000

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 (DMI)

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen (not shown). Select **Digit Manipulation Block** (DGT) as shown in capture **Section 5.6.1**. Select an available DMI from the drop-down list and click **to Add** as shown. In testing example, **Digit Manipulation Block Index 1** is added.



The **DMI_1** screen will open (not shown). In this testing, there is no leading digit to delete, 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 **Submit** button.



5.6.4. Digit Manipulation Block Index (DMI) for Outbound Call

To add DMI for outbound calls, there is an index, which was added to the **Digit Manipulation Block Index 1** as shown in **Section 5.6.3**. **Digit Manipulation Block Index 1** is used for outbound calls.

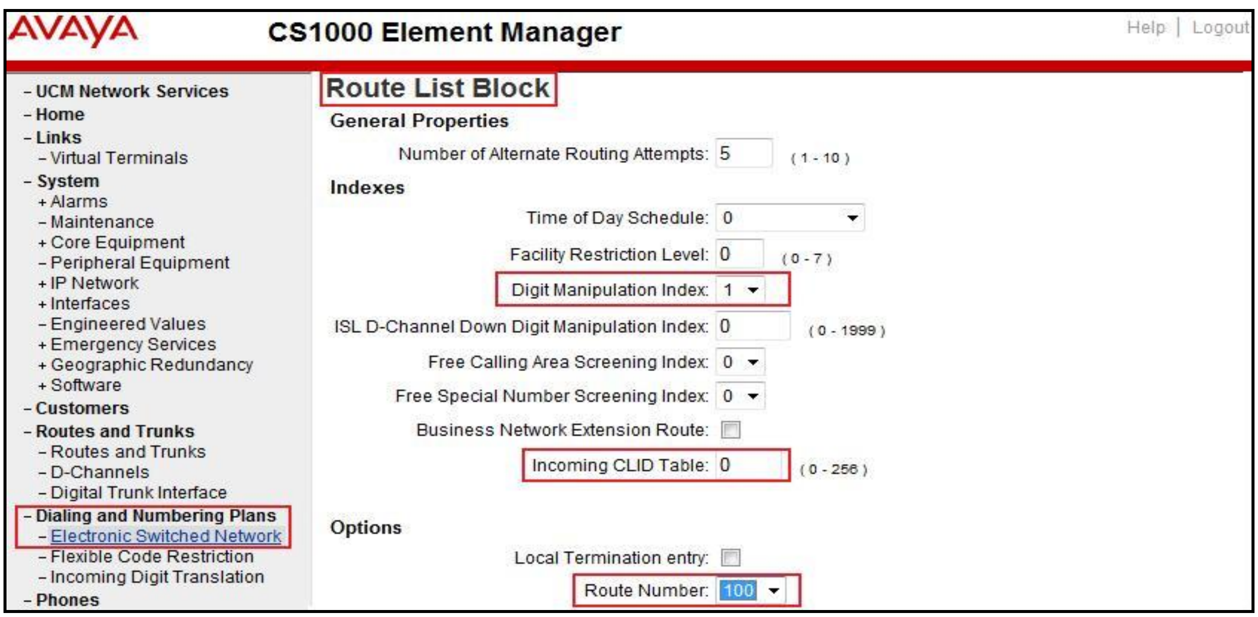
5.6.5. Route List Block (RLB) (RLB 14)

To add a RLB associated with the DMI 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 (not shown). Select **Route List Block (RLB)** as shown in capture of **Section 5.6.1**.

Enter an available value in the textbox for the **Please enter a route list index** (in this case 100) and click **to Add** button as shown.

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

- **Digit Manipulation Index**: **1** (created in **Section 5.6.4**)
- **Incoming CLID Table**: **0** (created in **Section 5.5.7**)
- **Route Number**: **100** (created in **Section 5.5.5**)

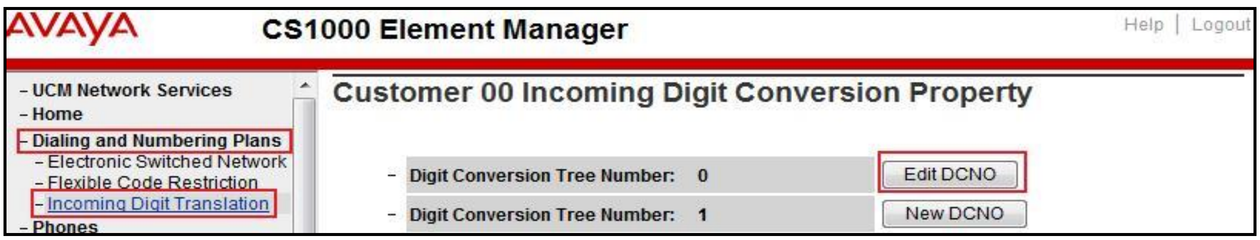


5.6.6. Inbound Call – Incoming Digit Translation Configuration

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

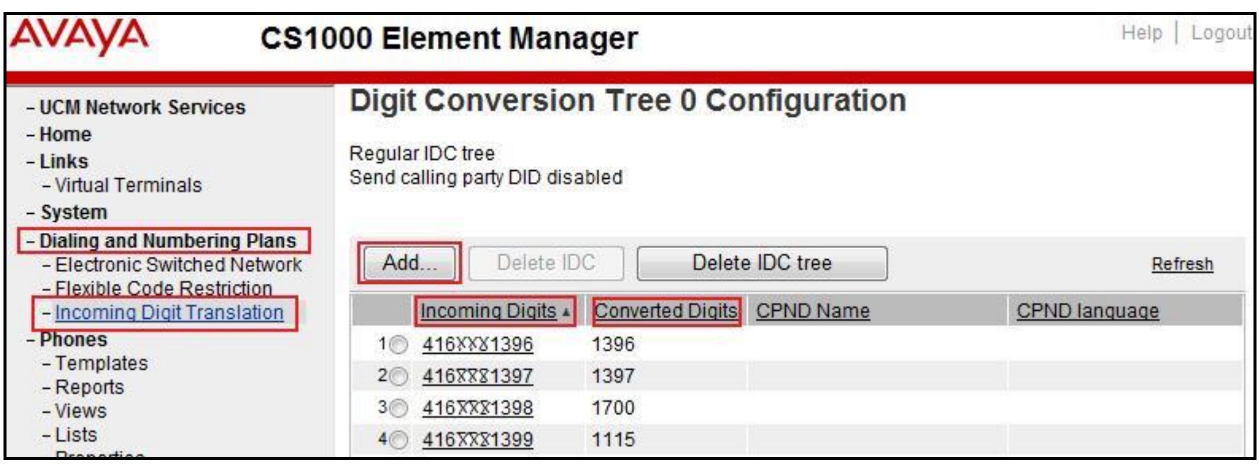
Select **Dialing and Numbering Plans → Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click **Edit IDC** button.

Click on the **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number 0** has been created.



Detail configuration of the Digit Conversion Tree Configuration is shown in capture below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the associated CS1000 system telephone DN. This **DCNO** has been assigned to route 100.

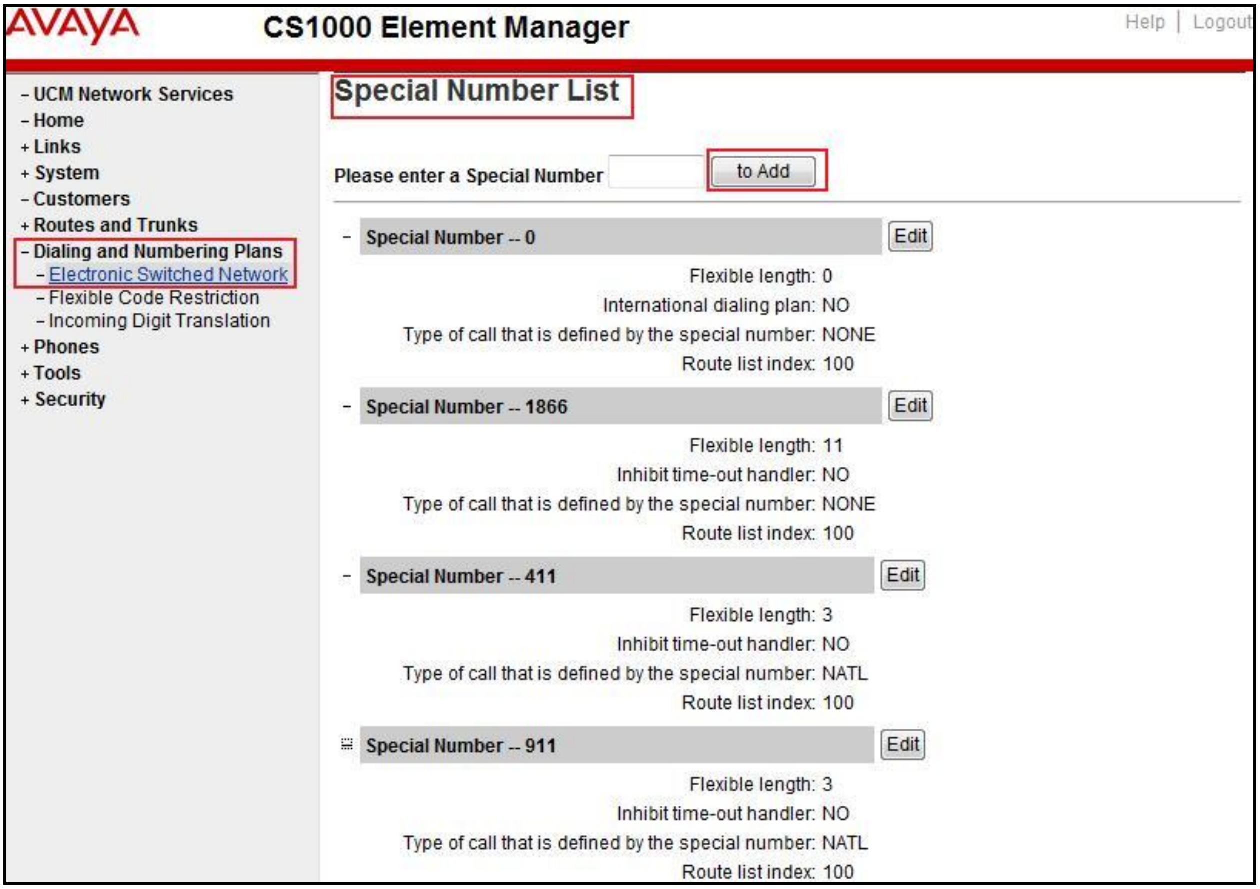
In the following configuration, the incoming call from PSTN with DID prefix **416XXX** will be translated to associated 4 digits DN. DID number **416XXX1398** is translated to **1700** for Voicemail accessing purpose and **416XXX1399** is translated to **1115** for Mobile Service Access DN.



5.6.7. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 0, 1866, 411, 911 and so on.

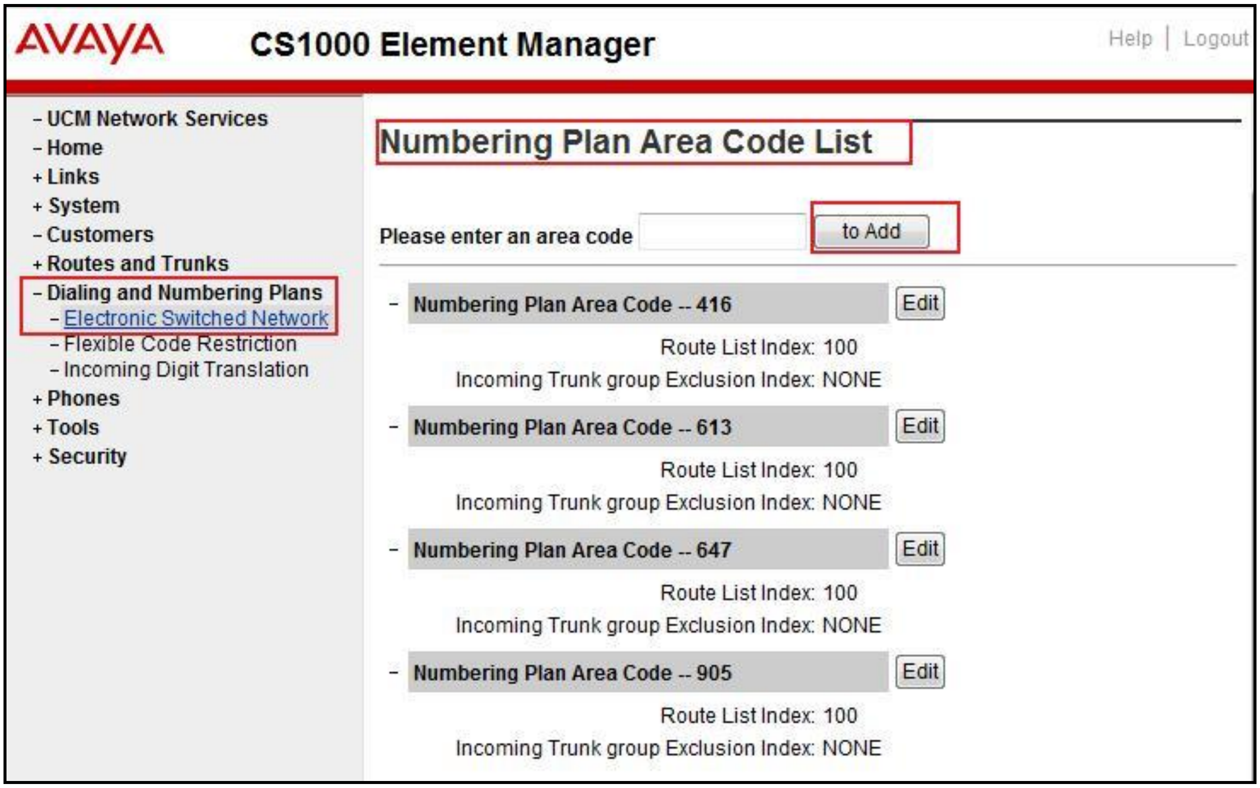
Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Select **Special Number (SPN)** under **Access Code 1** (not shown). Enter a SPN number and then click **to Add** button (not shown). Capture below shows all the special numbers used for this testing.



5.6.8. 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)** under **Access Code 1** (not shown). Enter the area code desired in the textbox and click **to Add** button. **416**, **613**, **647** and **905** area codes were used in this configuration.



5.7. Administer Telephone

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

5.7.1. Telephone creation

Refer to **Section 5.5.4** for creation of virtual superloop **96** and **Section 5.4.1** for creation of bandwidth zone **10** used for IP telephones. Log in to the Call Server Command Line Interface (please refer to **Section 5.1.2** for more detail). Create an IP telephone by using **ld 11** as shown below:

```
>ld 11
REQ: new
TYPE: 2007
TN   96 0 0 2
DATE
PAGE
DES
MODEL_NAME
EMULATED
DES  2007                          < --- Describe information for IP Telephone
TN   96 0 00 02  VIRTUAL     < --- Set Terminal Number for IP Telephone
TYPE 2007
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010 < --- Set bandwidth zone for IP telephone
CUR_ZONE 00010
MRT
ERL  0
ECL  0
FDN
TGAR 1
LDN  NO
NCOS 7
SGRP 0
RNPG 0
SCI  0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR FBD WTA LPR MTD FND HTD TDD CRPD
     MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LNA CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDD CFXD 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 1396 0     MARP < --- Set the position of DN 1396 to display on key 0 of the telephone
       CPND
         CPND_LANG ROMAN
           NAME Bell1396 < --- Set name to display
           XPLN 13
           DISPLAY_FMT FIRST,LAST
    01
<Text removed for brevity>
```

5.7.2. Enable Privacy for the Telephone

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

To hide the display number, set **cls** to **ddgd**. CS1000 will include “Privacy:id” in the SIP message header before sending it to the Service Provider.

```
>ld 11
REQ: chg
TYPE: 2007
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 the Service Provider.

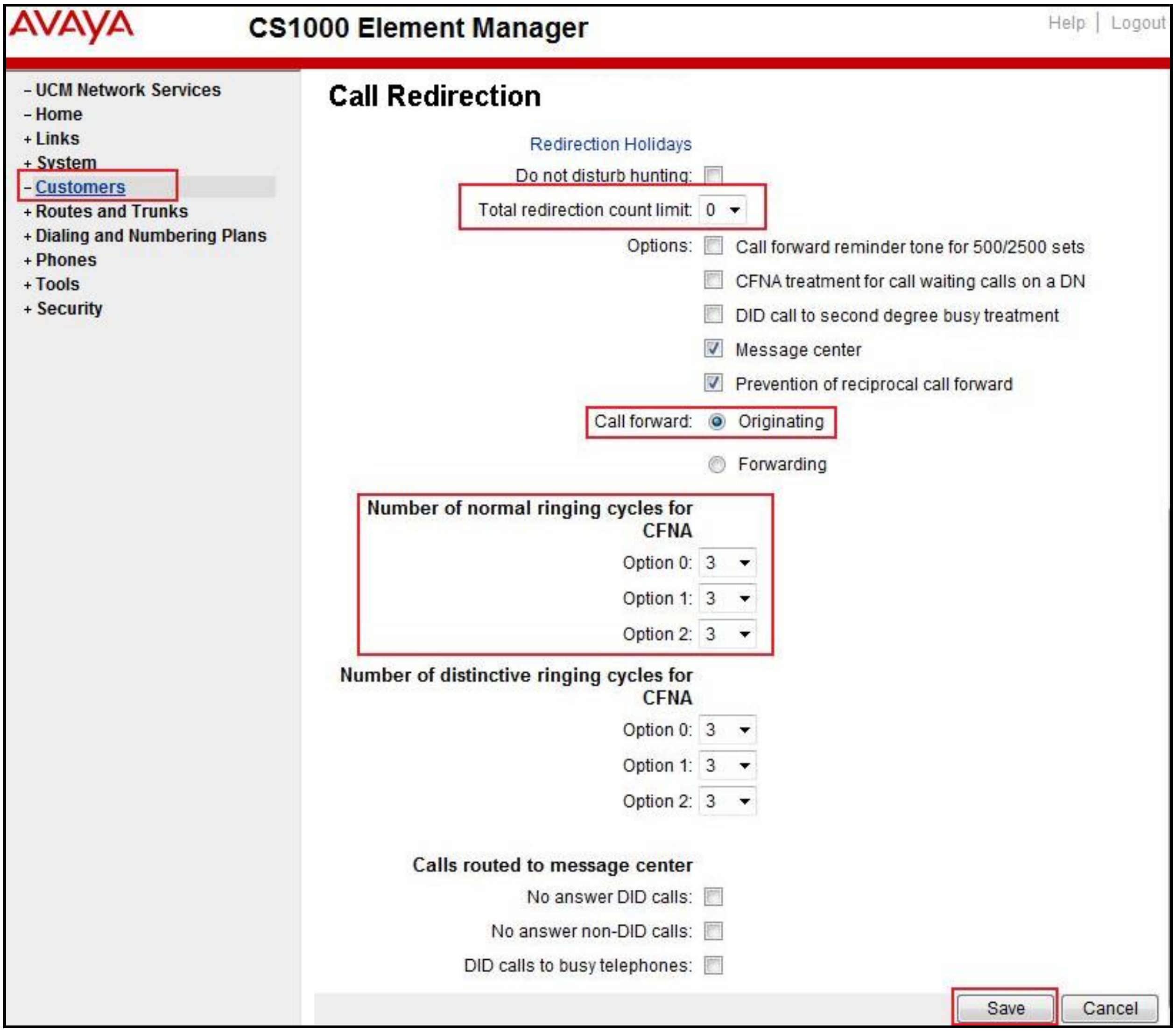
```
>ld 11
REQ: chg
TYPE: 2007
TN   96 0 0 2
ECHG yes
ITEM cls ddga
…
```

5.7.3. Enable Call Forward for Telephone

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

Select **Customers → 00 → Call Redirection**. The **Call Redirection** page is shown.

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



To enable Call Forward All Call (CFAC) for a telephone over a trunk, use **ld 11**. Set **cls** to **CFXA**, and **SFA,** then program the forward number on the telephone set. The following is the configuration of a telephone that has CFAC enabled with forwarding number **616139675204**.

```
ld 11
REQ: chg
TYPE: 2007
TN   96 0 0 2

ECHG yes
ITEM cls CFXA SFA
ITEM key 19 CFW 16 616139675204
```

To enable **Call Forward Busy (CFB)** for telephone over trunk, use **ld 11**. Set **cls** to **FBA**, **HTA**, and **SFA**, then program the forward number as **hunt** and **fdn**. Following is the configuration of a telephone with **CFB** enabled and forward number **616139675204**.

```
ld 11
REQ: chg
TYPE: 2007
TN   96 0 0 2
ECHG yes
ITEM cls FBA HTA SFA
ITEM hunt 616139675204
ITEM fdn 616139675203
```

To enable **Call Forward No Answer (FNA)** for a telephone over a trunk, use **ld 11**. Set **cls** to **FNA**, and **SFA**, and program the forward number as **hunt** and **FDN**. Following is the configuration of a telephone that has **FNA** enabled with forward number **616139675204**.

```
ld 11
REQ: chg
TYPE: 2007
TN   96 0 0 4
ECHG yes
ITEM cls FNA SFA
ITEM hunt 616139675204
ITEM fdn 616139675203
```

5.7.4. Enable Call Waiting for Telephone

This section shows how to configure the Call Waiting feature at the telephone level.

Log in to the Call Server CLI (please refer to **Section 5.1.2** for more details), configure Call Waiting feature for telephone by using **ld 11** to change **cls** to **HTD**, and **SWA** and adding a **CWT** key.

```
ld 11
REQ: chg
TYPE: 2007
TN   96 0 0 2
ECHG yes
ITEM cls HTD SWA
ITEM key 2 cwt
…
```

6. Configure Avaya Aura® Session Manager

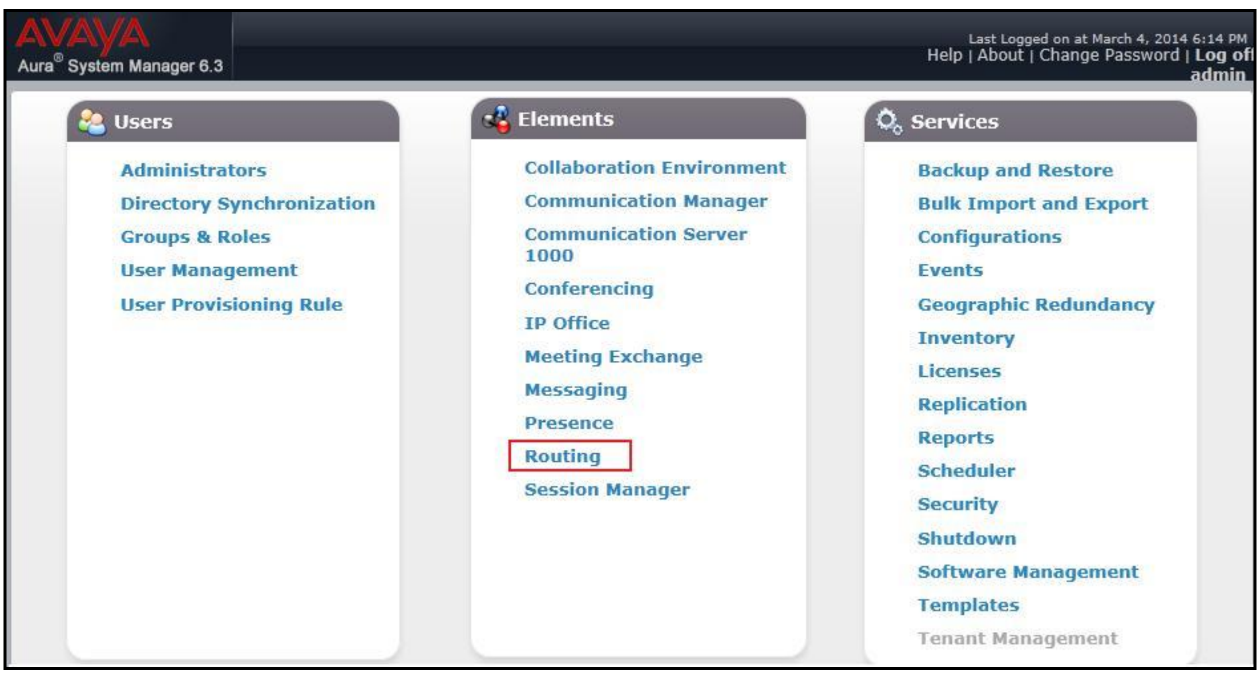
This section provides the procedures for configuring SM. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, SM and the ASBC
- Entity Links, which define the SIP trunk parameters used by SM when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- SM, corresponding to the SM server to be managed by System Manager

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

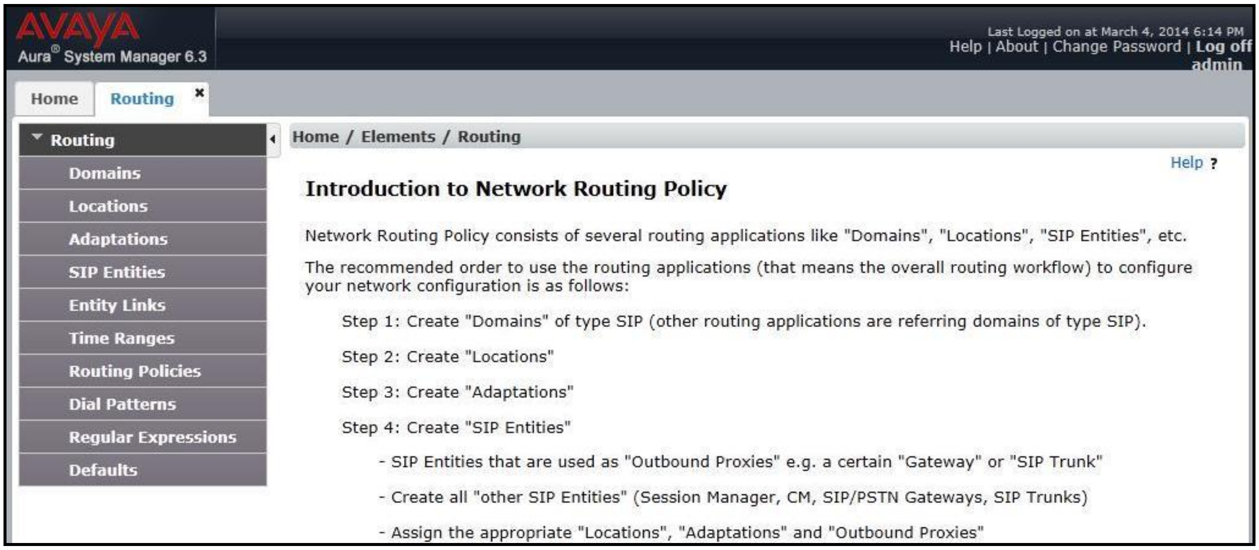
6.1. System Manager Login and Navigation

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



Most of the configuration items are performed in the Routing element. Click on **Routing** in the **Elements** column (not shown) to bring up the **Introduction to Network Routing Policy** screen.

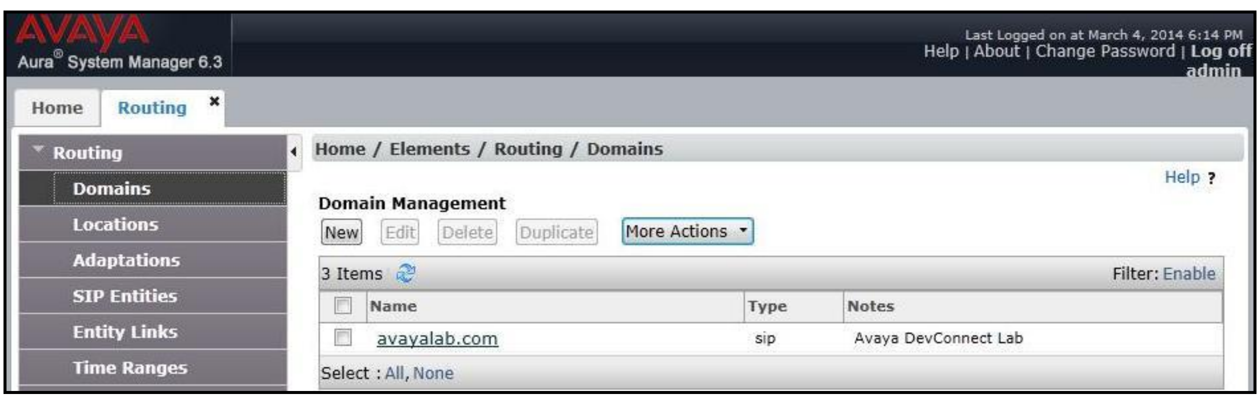
The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



6.2. Specify SIP Domain

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

The following screen shows the list of configured SIP domains. The domain "avayalab.com" was already created for communication between SM and CS1000. The domain "avayalab.com" is not known to Bell. It will be adapted by the ASBC to IP address based URI-Host to meet the SIP specification of Bell system.



6.3. Add Adaptations

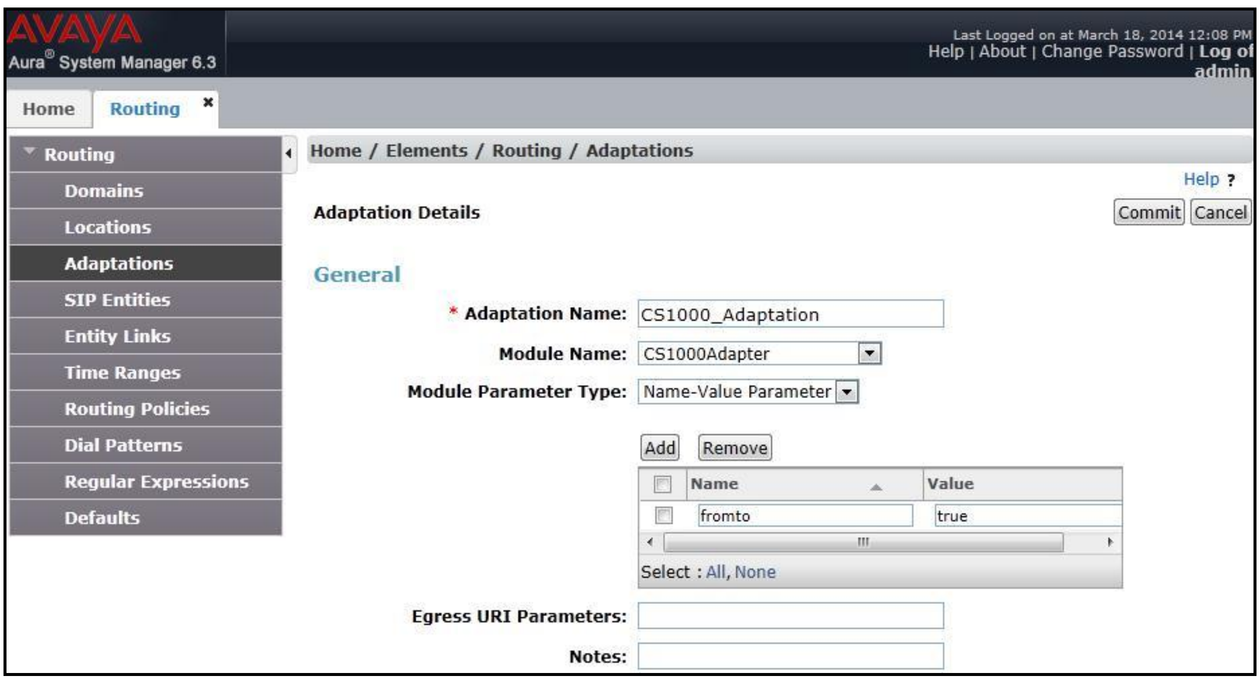
Adaptations can be used to modify SIP messages that are leaving a SM instance (egress adaptation) and that are entering a SM instance (ingress adaptation). This adaptation function is needed to convert strings containing calling and called party numbers from the local dial-plan of a SIP entity to the dial-plan administered on the SM, and vice versa. Adaptation is also needed when other SIP entities require special SIP protocol conventions. Each administered SIP entity may have its own unique adaptation, or one adaptation can be shared among multiple entities.

To add an Adaptation, navigate to **Routing → Adaptations** in the left-hand menu pane and click **New** button in the right pane (not shown).

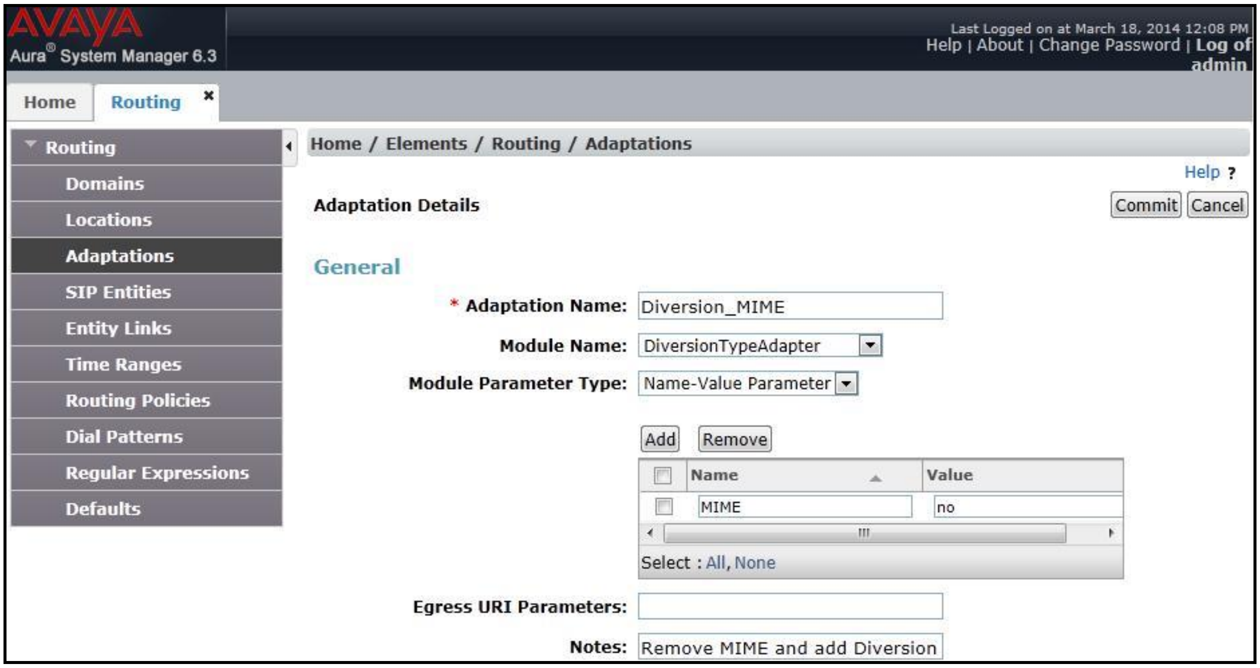
In **General** section, enter the following values:

- **Adaptation Name**: Enter a descriptive name for the adaptation.
- **Module Name**: Choose predefined Module Name from drop down list.
- **Module Parameter Type**: Choose a module from drop down list.

An Adaptation, using Module Name **CS1000Adapter,** was created to support CS1000 source based routing.



An Adaptation, using Module Name **DiversionTypeAdapter**, was created to add Diversion header and to remove MIME (CS1000 proprietary SIP info.).



6.4. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for bandwidth management and call admission control purposes. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click **New** button in the right pane (not shown).

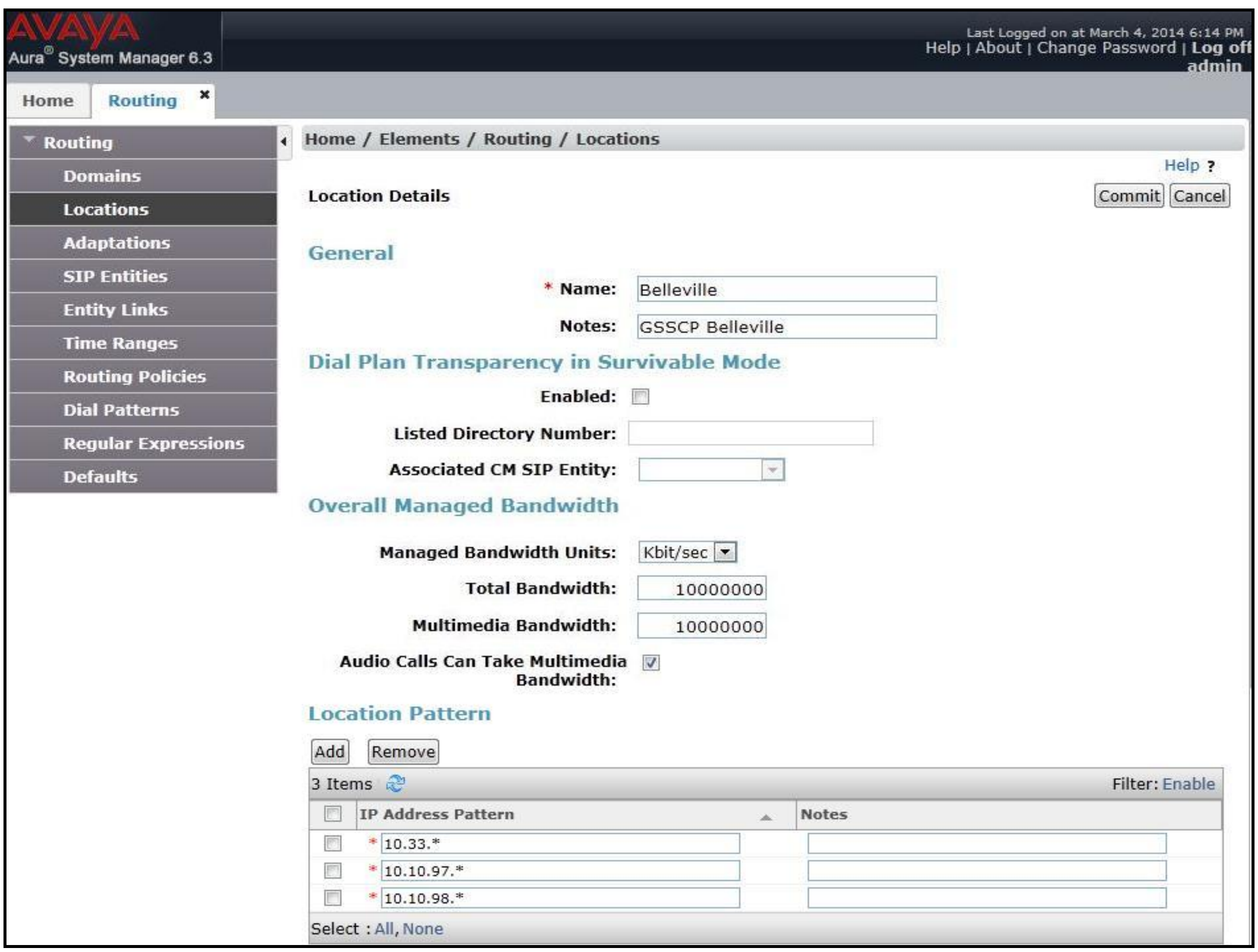
In **General** section, enter the following values:

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

In the **Location Pattern** section (see the screen below), click **Add** and enter following values:

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

Displayed below is the screenshot for location **Belleville**, which includes all equipment on the **10.33.x.x, 10.10.98.x** and **10.10.97.x** subnets including CS1000, SM and ASBC. Click **Commit** to save.



6.5. Add SIP Entities

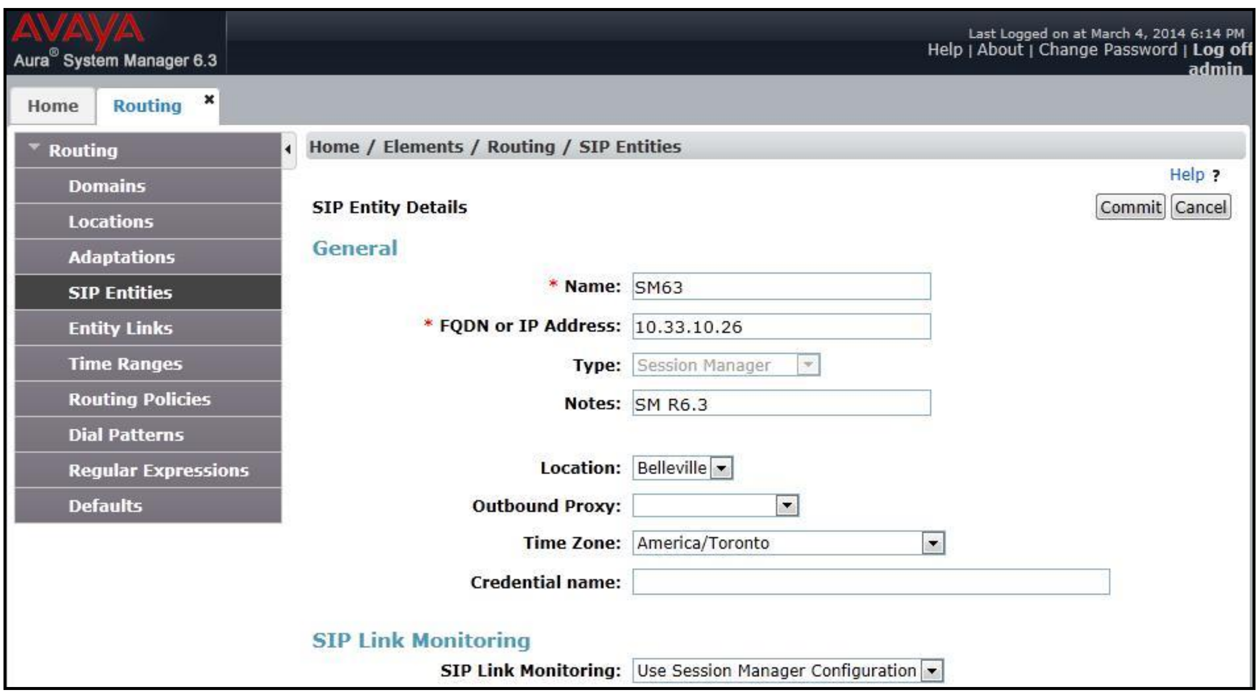
A SIP Entity must be added for SM and for each SIP telephony system connected to it which includes CS1000 and the ASBC.

To add a new SIP Entity, navigate to **Routing → SIP Entities** in the left navigation pane and click **New** button in the right pane (not shown).

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

- **Name**: Enter a descriptive name.
- **FQDN or IP Address**: Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for SM, **Other** for CS1000 and **Other** for the ASBC.
- **Location:** Select the location defined previously in **Section** Error! Reference source not found..
- **Time Zone**: Select the time zone for the location above.

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

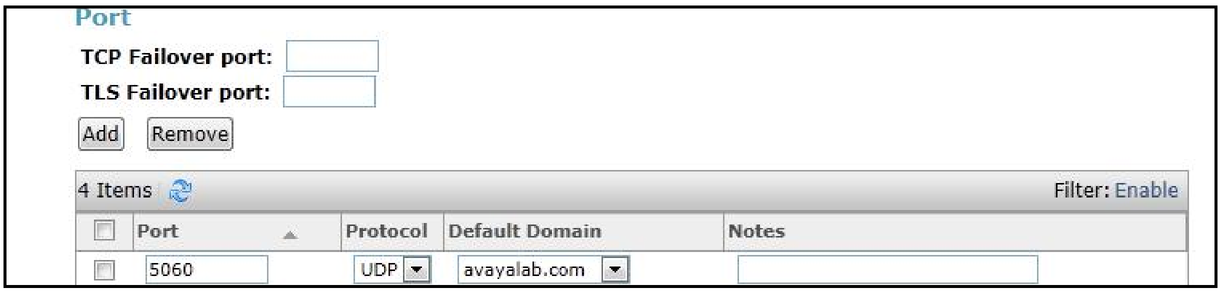


To define the ports used by SM, scroll down to the **Port** section. This section is only present for the **Session Manager** SIP Entity.

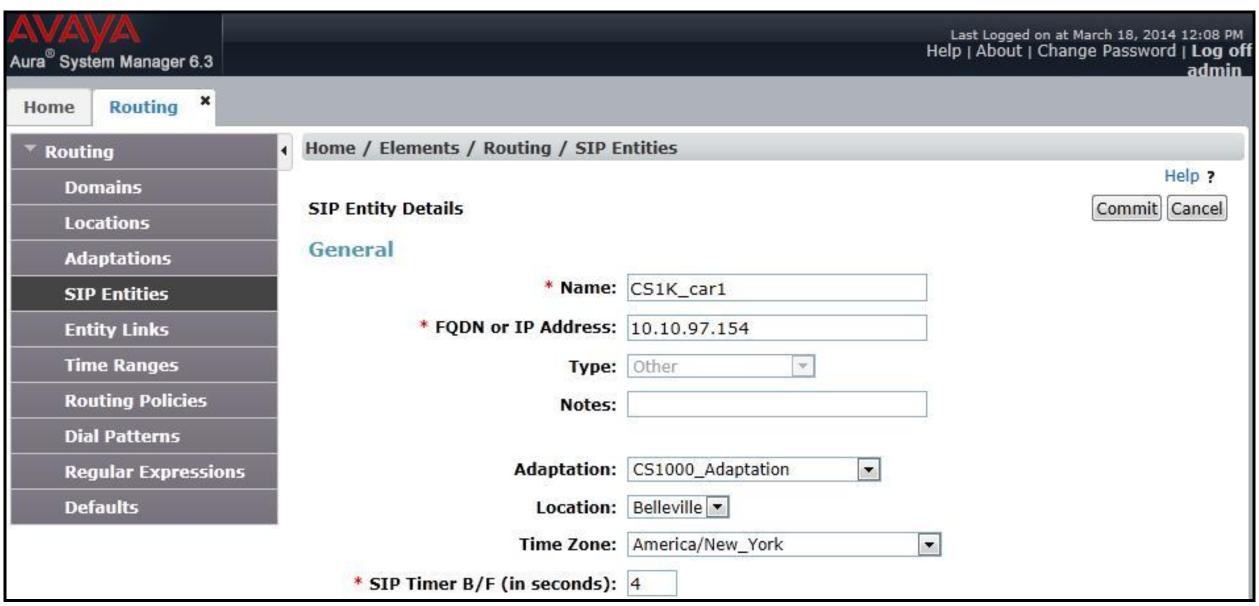
In the **Port** section, click **Add** and enter following values. Use default values for all remaining fields:

- **Port:** Port number on which the SM can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.
- Defaults can be used for the remaining fields.
- Click **Commit** to save (not shown).

The compliance test used **Port** entry **5060** with **UDP** for connecting to CS1000 and **Port** entry **5060** with **UDP** for connecting to the ASBC.

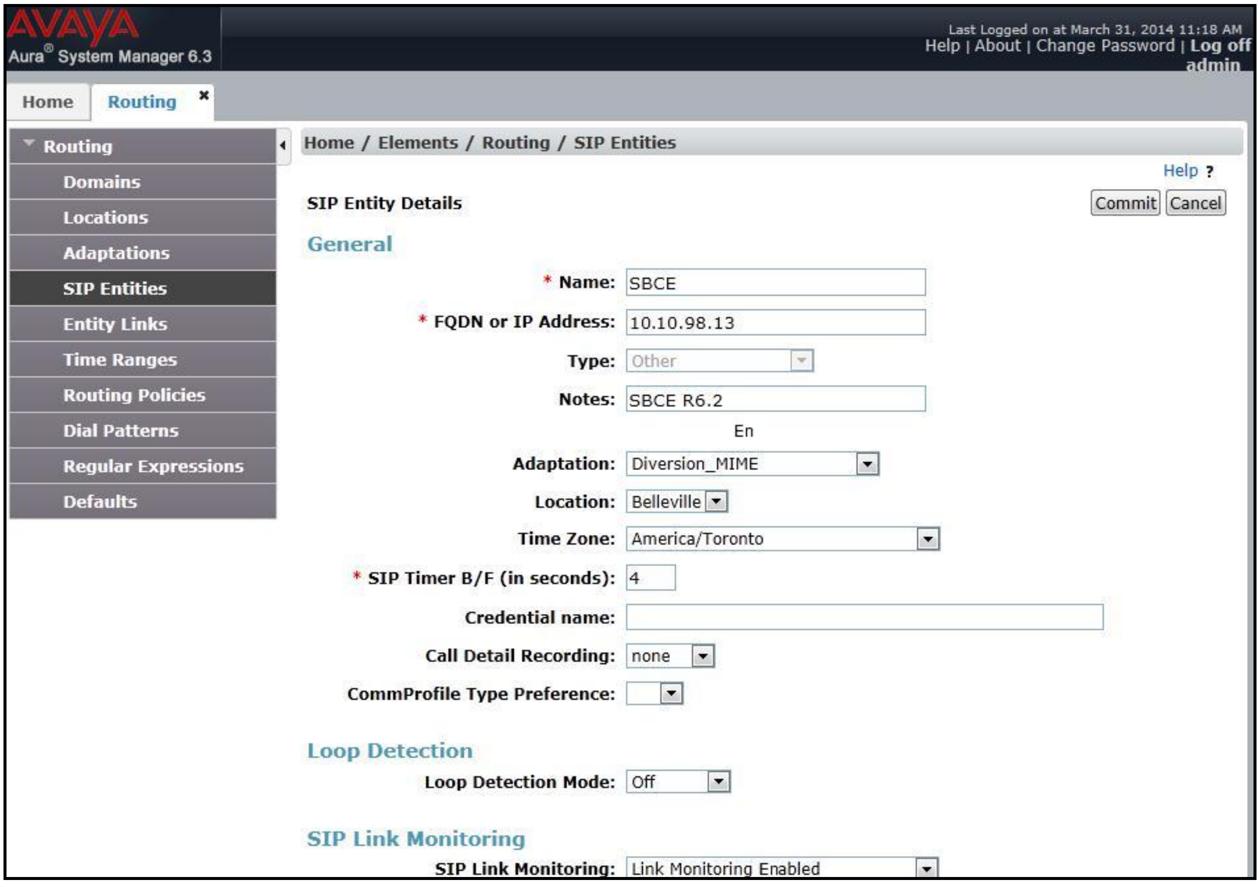


The following screen shows the addition of CS1000 SIP Entities. In order for SM to send SIP traffic on an entity link to CS1000, it is necessary to create a SIP Entity for CS1000. The **FQDN or IP Address** field is set to IP address of CS1000. Select **Other** as **Type**.



The following screen shows the addition of the SIP Entity for ASBC. The **FQDN or IP Address** field is set to the IP address of ASBC's private network interface (see **Figure 1**). Select **Other** as

Type. Select **Link Monitoring Enabled** as **SIP Link Monitoring** with the interval of 60 seconds (not shown). This setting allows SM to send outbound OPTIONS heartbeat in every 60 seconds to service provider (which is forwarded by the ASBC) to query for the status of the SIP trunk connecting to service provider.



6.6. Add Entity Links

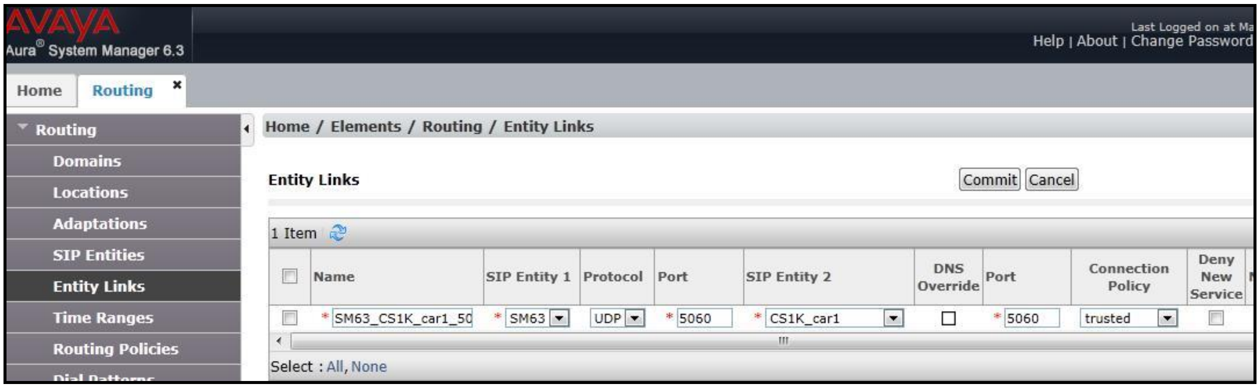
A SIP trunk between SM and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for CS1000 and other for ASBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link, UDP for the Entity Link to CS1000 and UDP for the Entity Link to the ASBC.
- **Port:** Port number on which SM will receive SIP requests from the far-end. For CS1000, this must match the **Far-end Listen Port** defined on the CS1000 in **Section 5.5.2**.
- **SIP Entity 2:** Select the name of the other systems. For CS1000, select the CS1000 SIP Entity defined in **Section** Error! Reference source not found.. For ASBC, select ASBC SIP Entity defined in **Section** Error! Reference source not found..

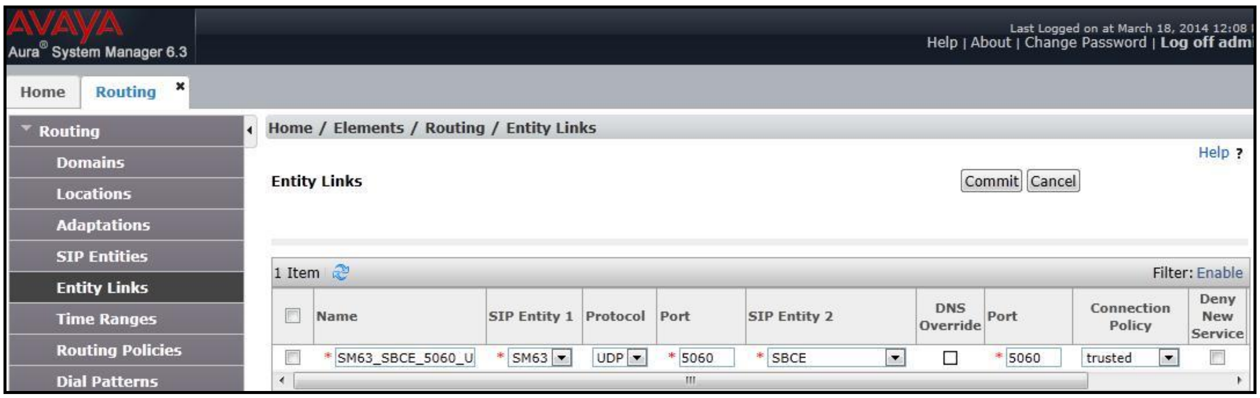
- **Port:** Port number on which the other system receives SIP requests from SM. For CS1000, this must match the **Near-end Listen Port** defined on the CS1000 in **Section 5.5.2**.
- **Connection Policy:** Select **Trusted**. **Note**: If this is not selected, calls from the associated SIP Entity specified in **Section** Error! Reference source not found. will be denied.
- Click **Commit** to save.

The following screens illustrate the Entity Links to CS1000 and to ASBC.

Below is Entity Link to CS1000.



Below is Entity Link to ASBC.



6.7. Add Routing Policies

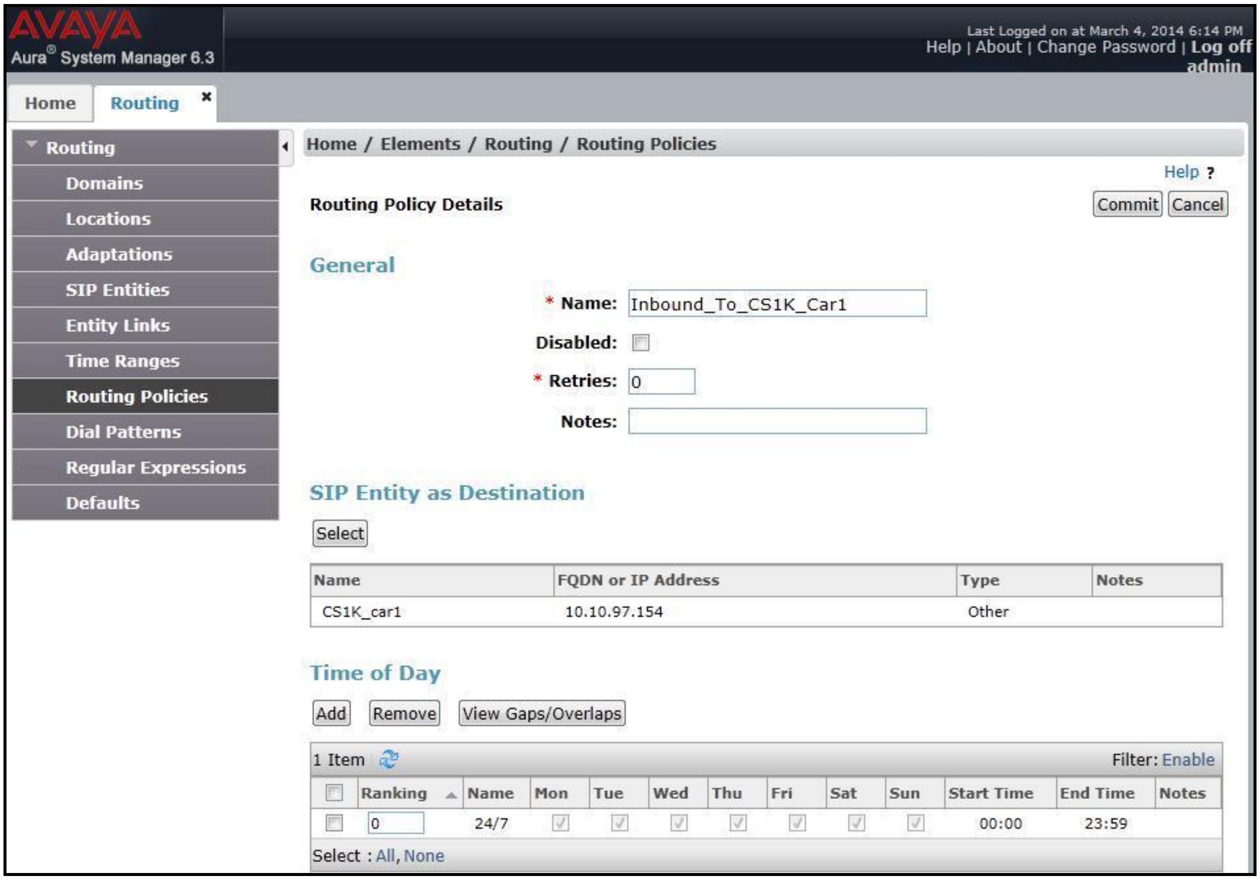
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section** Error! Reference source not found.. Two routing policies were added, one for CS1000 and other for ASBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click **New** button in the right pane (not shown). The following screen is displayed.

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

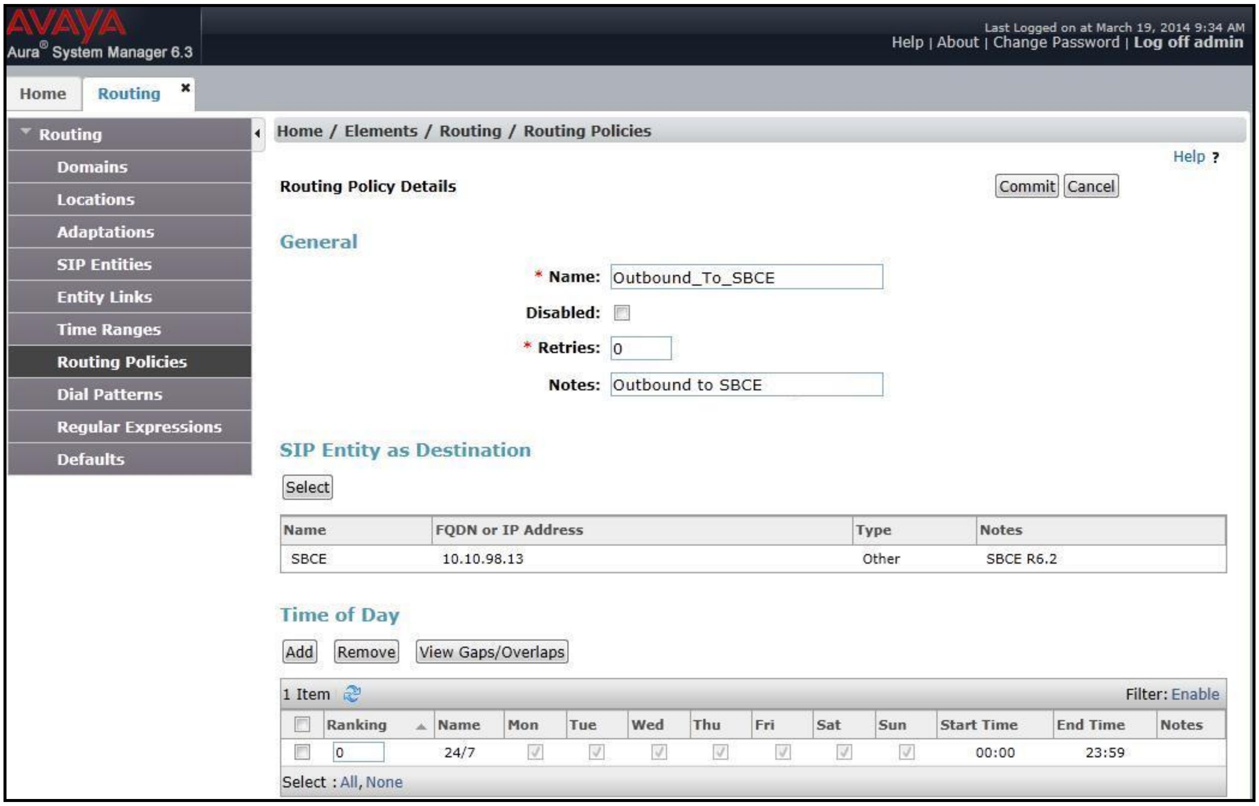
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

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

The following screens show the Routing Policies for CS1000.



The following screens show the Routing Policies for ASBC.



6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through SM. For the compliance testing, dial patterns were needed to route calls from CS1000 to Bell system and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click **New** button in the right pane (not shown).

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

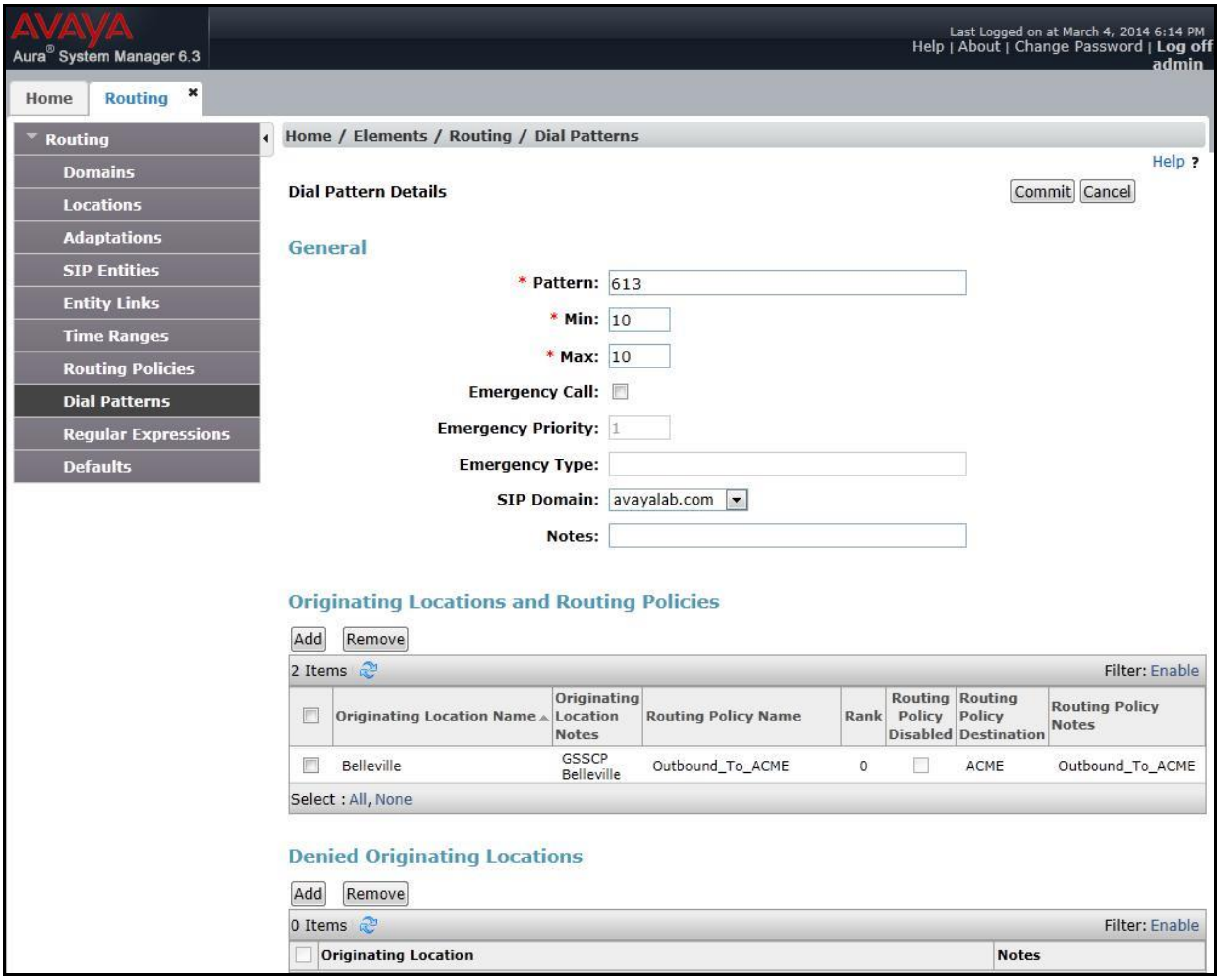
- **Pattern:** Enter a dial string that will be matched against the "Request-URI" of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, **Section 6.2**.
- **Notes:** Add a brief description (optional).

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

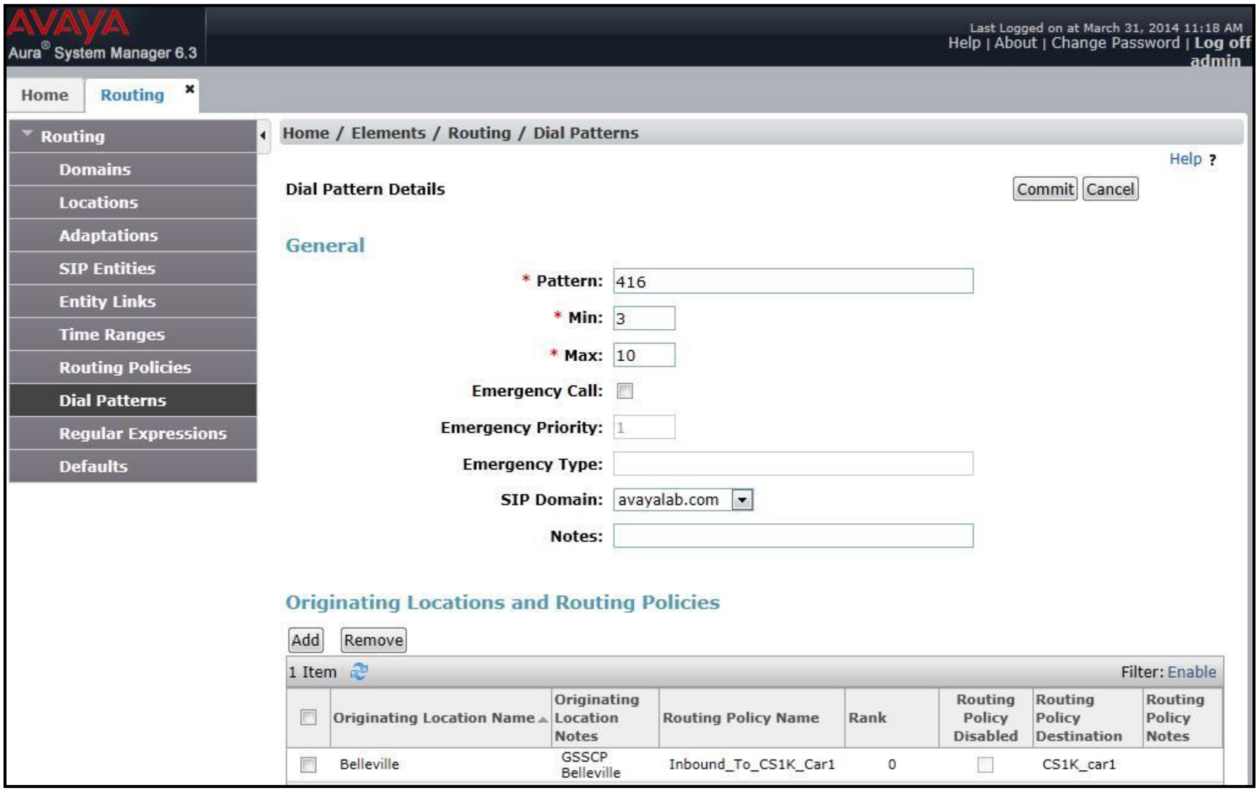
Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance testing were shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

The first example shows that 10-digit dialed numbers that has a destination domain of "avayalab.com" uses route policy to ASBC as defined in **Section** Error! Reference source not found..



The second example shows that inbound 10-digit numbers that start with 416 to domain “avayalab.com” uses route policy to CS1000 as defined in **Section** Error! Reference source not found.**.8**. These are the DID numbers assigned to the enterprise by Bell.



6.9. Add/View Session Manager

The creation of a SM element provides the linkage between System Manager and SM. This is most likely done as part of the initial SM installation. To add a SM, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click **New** button in the right pane (not shown). If the SM Instances already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

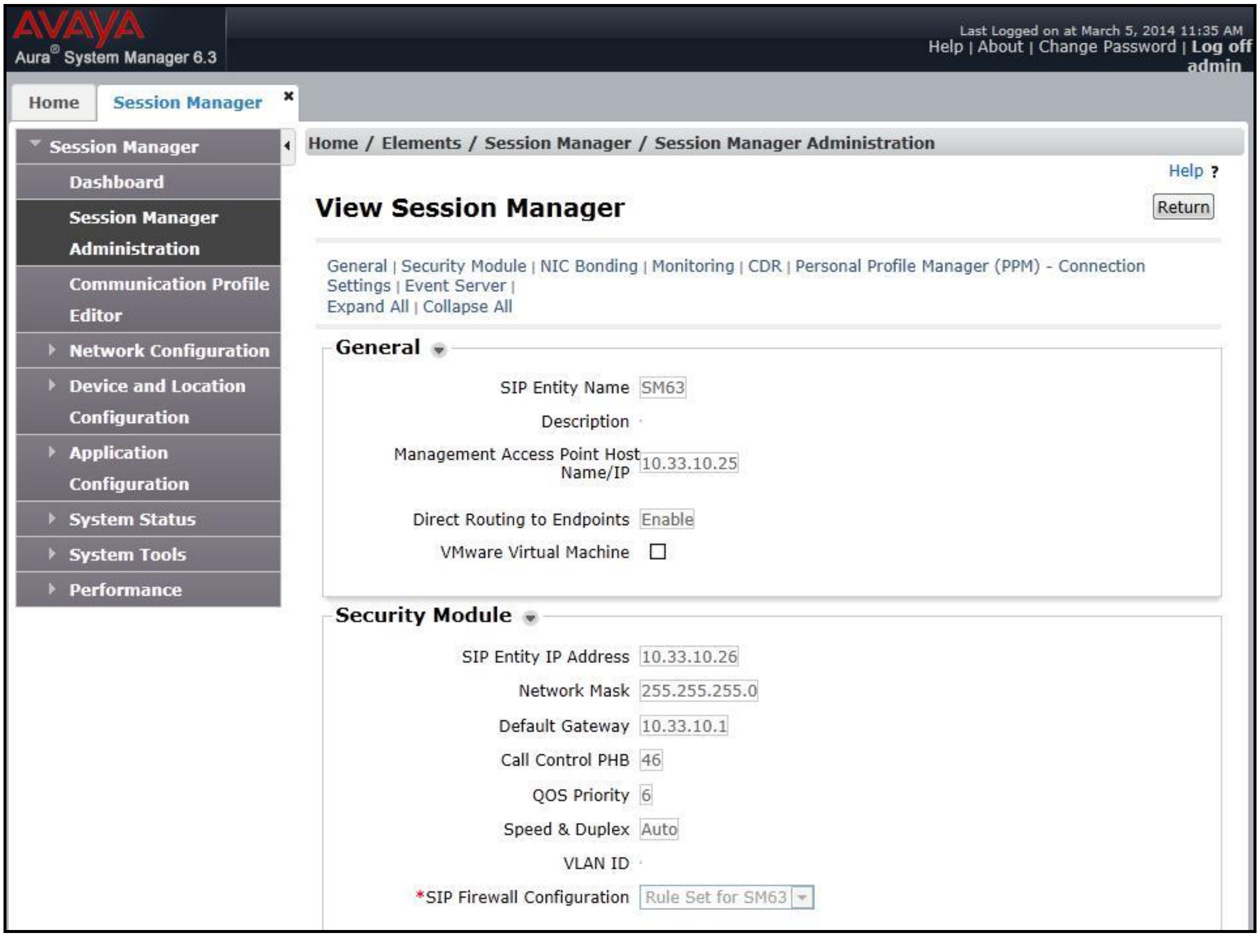
- **SIP Entity Name:** Select the SIP Entity created for SM.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the SM management interface.
- **Direct Routing to Endpoints**: Enable, to enable call routing on the SM.

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name.
- **Network Mask:** Enter the network mask corresponding to the IP address of SM.

- **Default Gateway**: Enter the IP address of the default gateway for SM.
- Use default values for the remaining fields. Click **Commit** to save (not shown).

The screen below shows the SM values used for the compliance testing.



7. Configure Avaya Session Border Controller

This section describes the configuration of ASBC necessary for interoperability with CS1000, SM and Bell system.

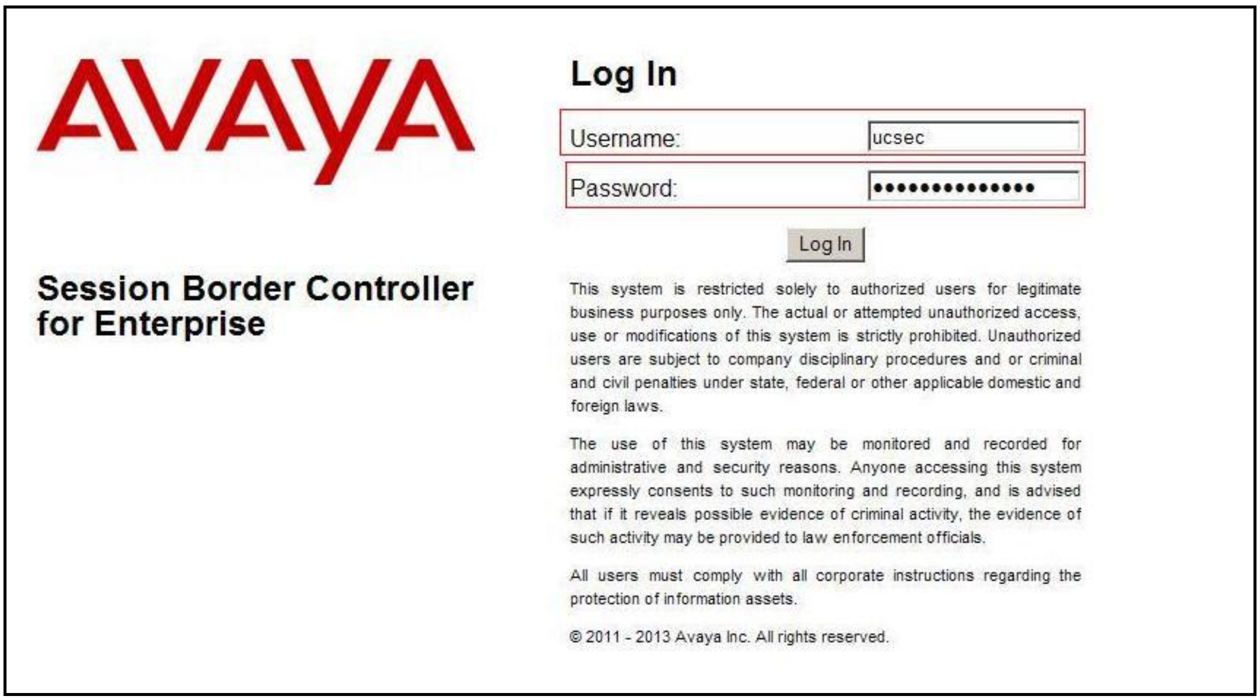
In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Bell system resides on the Public side of the network.

Note: The following section assumes that ASBC has been installed and that network connectivity exists between the systems. For more information on ASBC, see **Section 11** of these Application Notes.

7.1. Log in Avaya Session Border Controller

Access the web interface by typing "**https://x.x.x.x/sbc/**" (where x.x.x.x is the management IP of ASBC).

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



7.2. Global Profiles

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

7.2.1. Configure Server Interworking Profile – Avaya

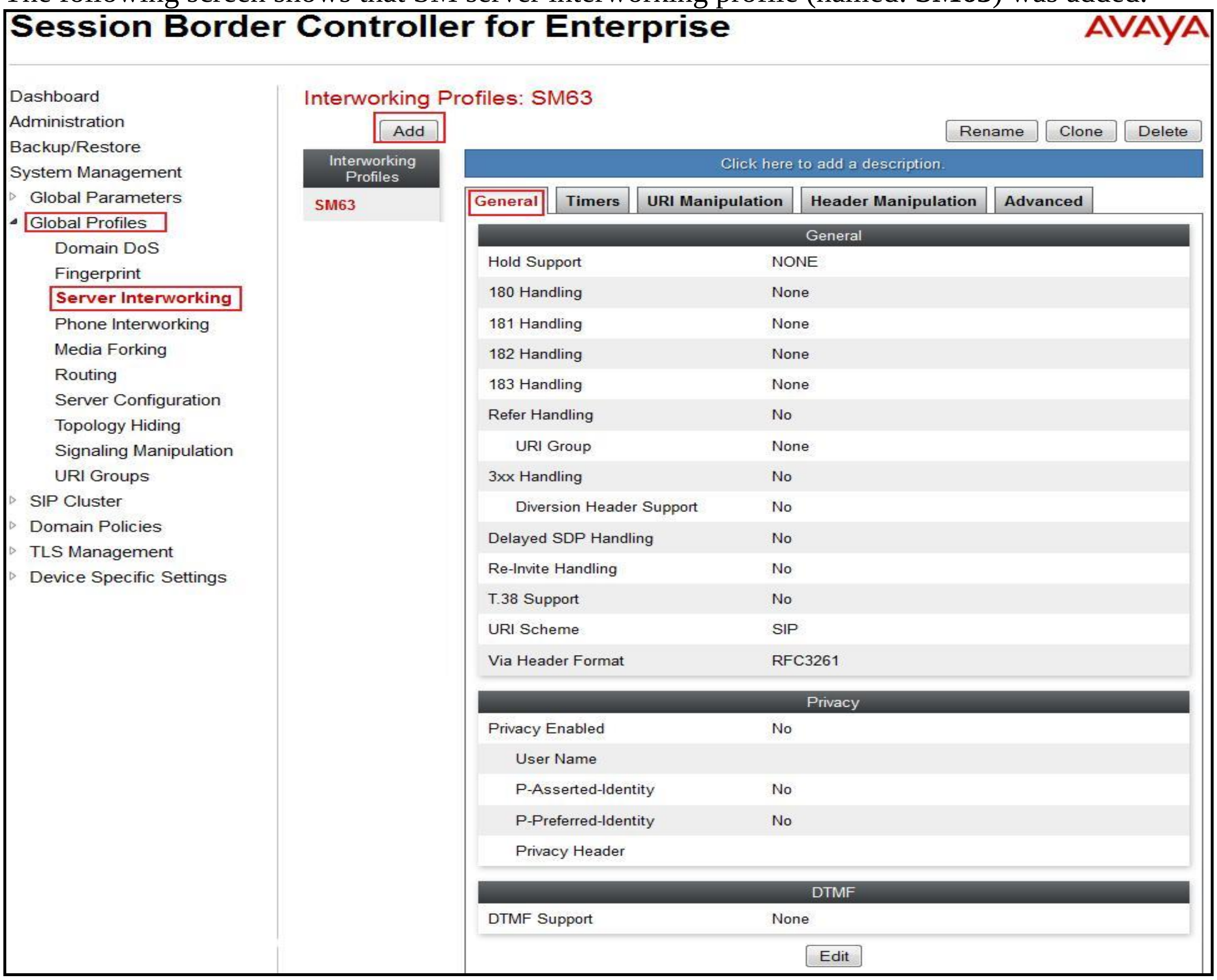
Server Interworking profile allows administrator to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.

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

- Enter Profile name**: SM63**
- 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 shows that SM server interworking profile (named: **SM63**) was added.



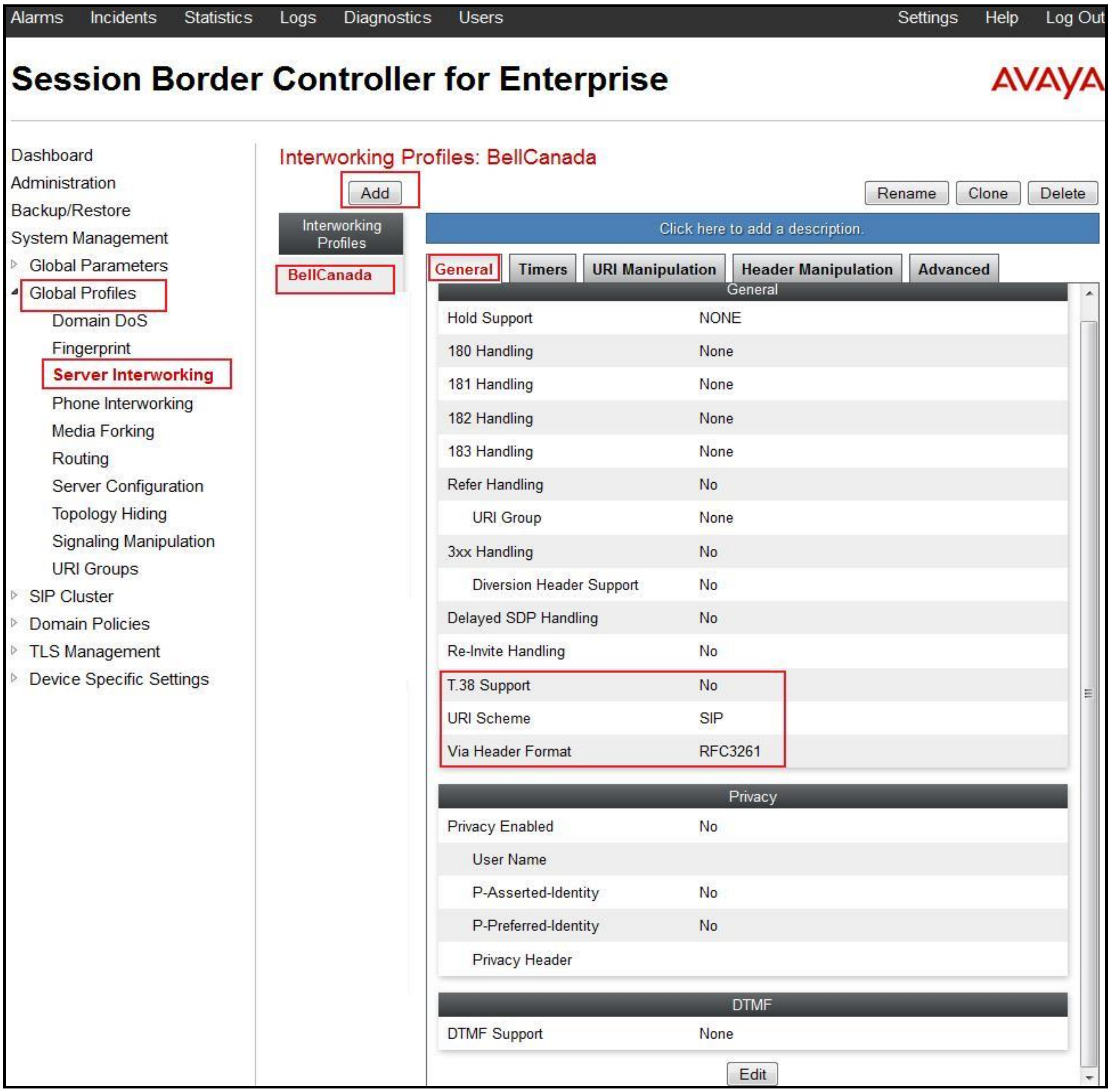
7.2.2. Configure Server Interworking Profile – Bell

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

- Enter Profile name**: BellCanada**
- 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 shows that Bell server interworking profile (named: **BellCanada**) was added.



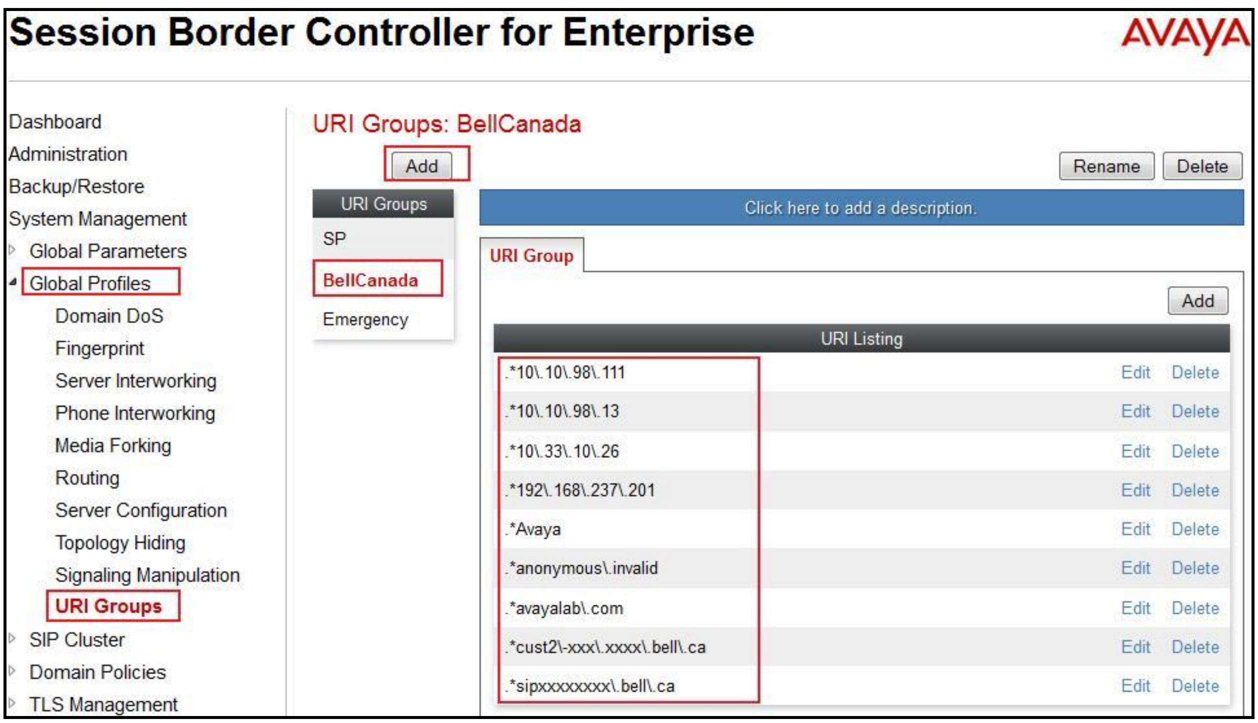
7.2.3. Configure URI Groups

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 for Bell was used to match the "From" and "To" headers in a SIP call dialog received from both Enterprise and Bell. If there is a match, the ASBC will apply the appropriate Routing profile, Server Flow, and Session Flow 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: **BellCanada**
- Edit the URI Type: **Regular Expression** (not shown).
- **Add** URI: **.*10\.10\.98\.111** (ASBC public interface IP address), **.*10\.10\.98\.13** (ASBC internal interface IP address), **.*10\.33\.10\.26** (SM IP address), **.*192\.168\.237\.201** (Bell System IP address**)**, **.*anonymous\.invalid** (Anonymous URI**)**, **.*avayalab\.com** (Enterprise domain), .*Avaya (Receiving OPTIONS ping from Bell), .***sipxxxxxxxx\.bell\.ca** and **.*cust2\-xxx\.xxxx\.bell\.com** (Bell domain).

Click **Finish** (not shown).



7.2.4. Configure Routing – Avaya

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: **To_SM63**.

- **URI Group**: **BellCanada**.
- **Next Hop Server 1: 10.33.10.26:5060** (SM IP address).
- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport: UDP** (not shown).
- Click **Finish** (not shown).

7.2.5. Configure Routing – Bell

The Routing Profile allows administrator 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: **To_BellCanada**.

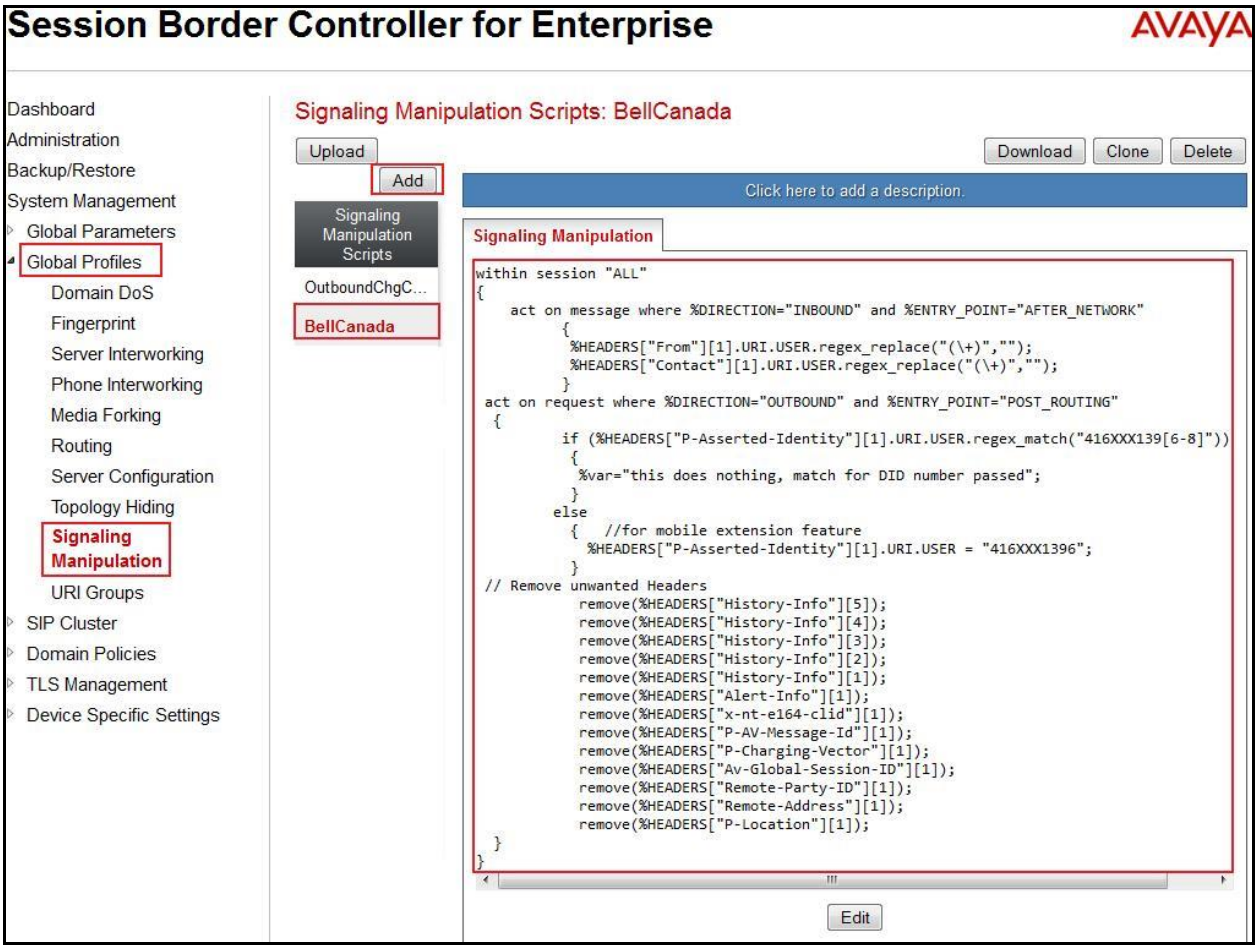
- **URI Group**: **BellCanada**.
- **Next Hop Server 1: 192.168.237.201:5060** (Bell System IP address).
- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport** as **UDP** (not shown).
- Click **Finish** (not shown).

7.2.6. Configure Signalling Manipulation

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

To create a Signaling Manipulation script, select **Global Profiles → Signaling Manipulation**. Click **Add Script** (not shown).

In the compliance testing, a SigMa script is created for Server Configuration for Bell and the details are captured below.



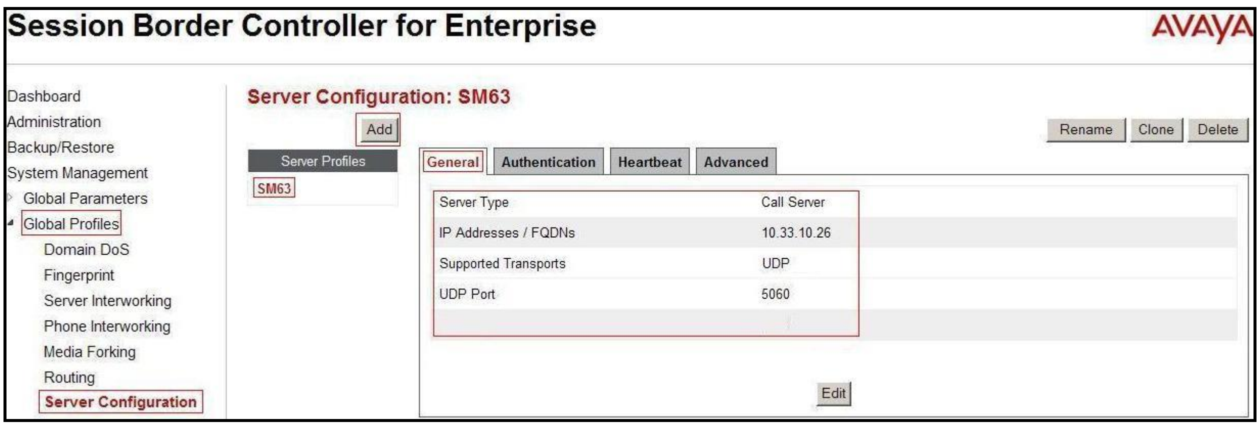
7.2.7. Configure Server Configuration – Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow administrator 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: **SM63**.

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

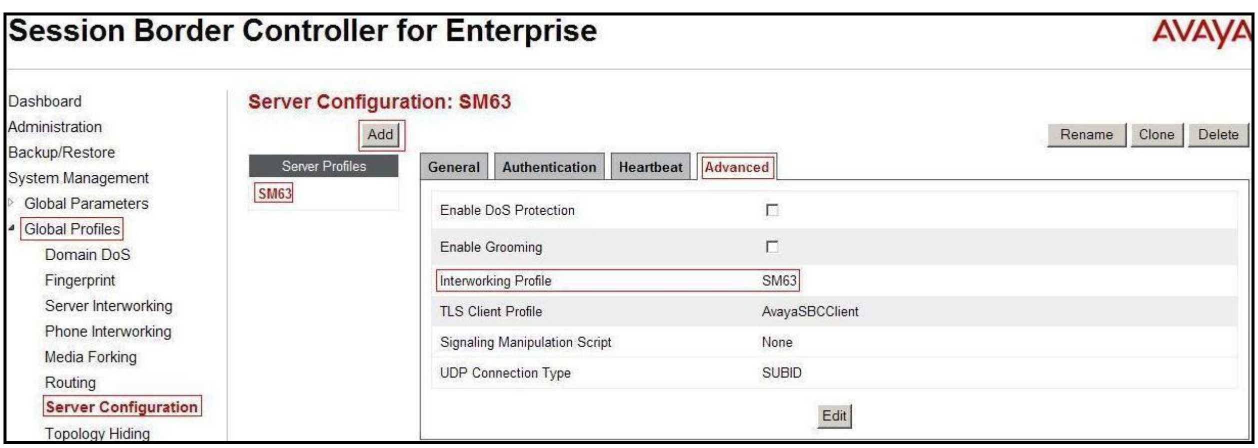
- **Server Type**: Select **Call Server**
- **IP Address/FQDNs**: **10.10.33.26** (SM IP Address)
- **Supported Transports**: **UDP**
- **UDP Port**: **5060**



On the **Advanced** tab:

- Select **SM63** for **Interworking Profile**.

Click **Finish** (not shown).



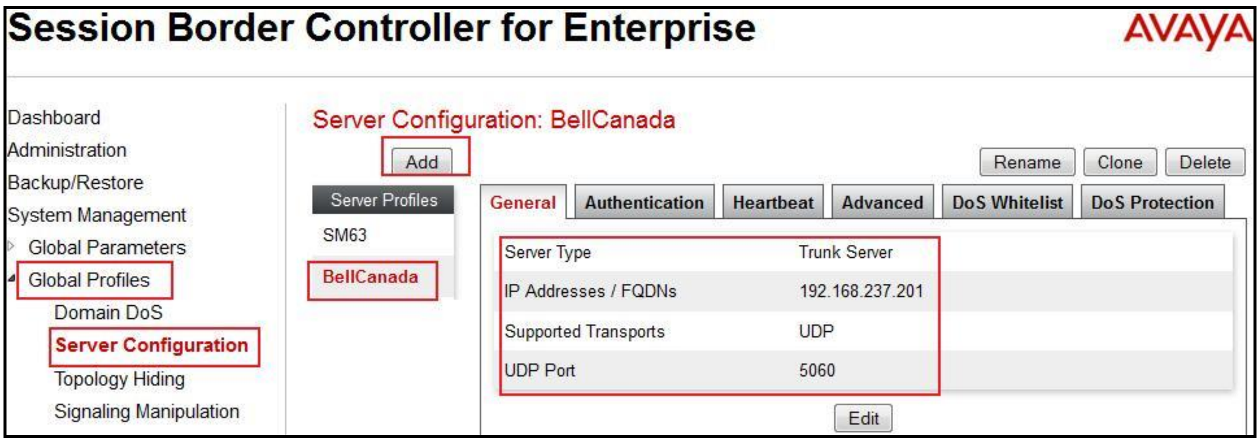
7.2.8. Configure Server Configuration – Bell

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

Enter profile name: **BellCanada**

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

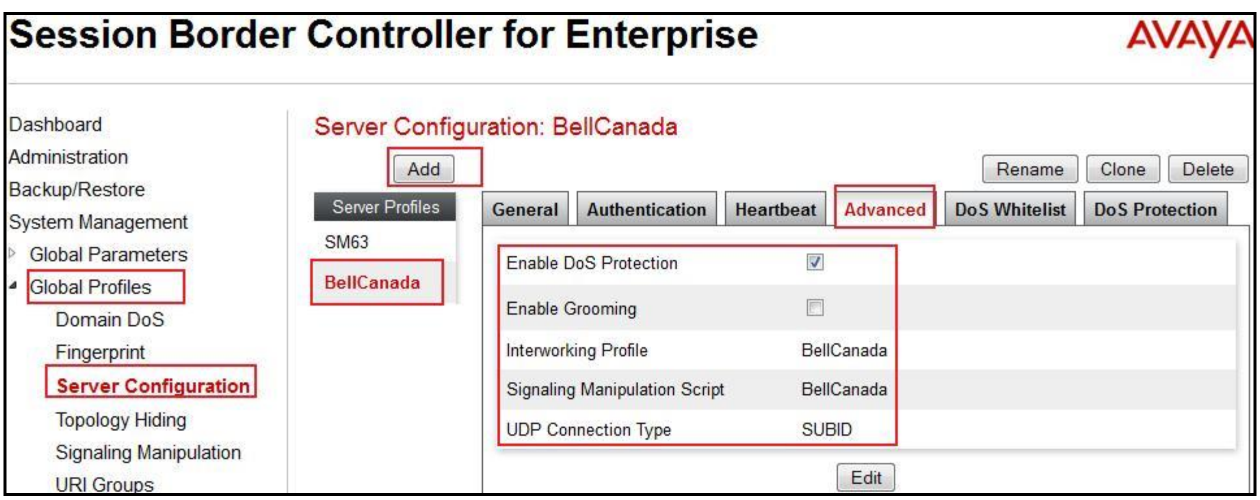
- **Server Type:** Select **Trunk Server**
- **IP Address: 192.168.237.201** (Bell system IP Address)
- **Supported Transports**: **UDP**
- **UDP Port: 5060**



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

- **Interworking Profile**: select **BellCanada**, defined in **Section 7.2.2**
- **Signaling Manipulation Scrip**: Select **BellCanada,** defined in **Section 7.2.6**

Click **Finish** (not shown).



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

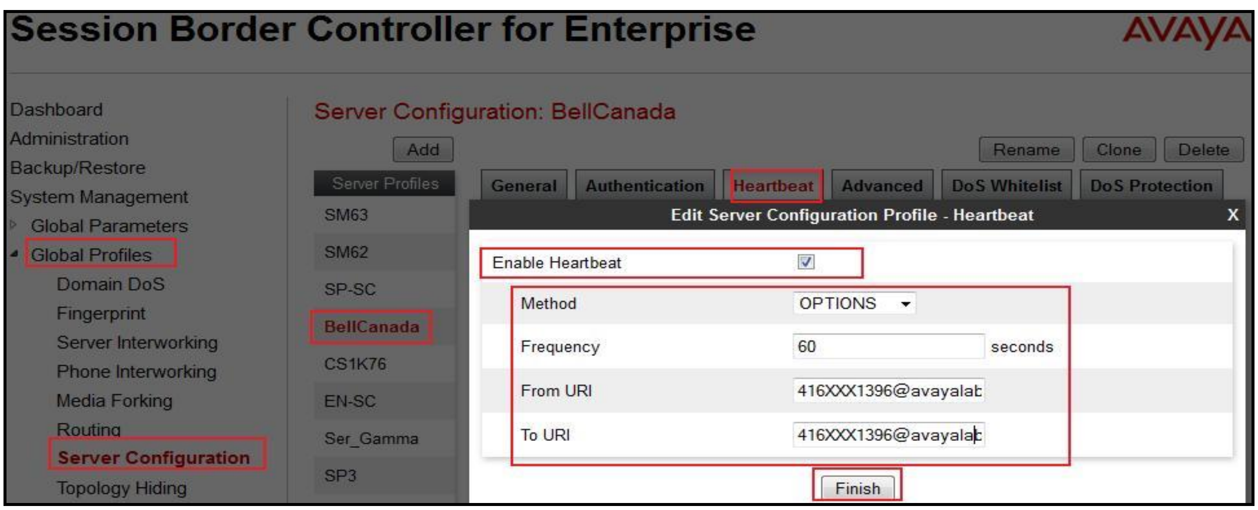
- Check **Enable Authentication**.
- Enter **User Name**: **416XXX1396** (Provided by Bell).
- Enter **Password: ********** (Provided by Bell).
- Enter **Realm**: sipxxxxxxxx.bell.ca (Provided by Bell).

Click **Finish**.

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

- Check **Enable Heartbeat**.
- Select **Method**: **OPTIONS**
- Enter **Frequency**: **60 seconds**
- Enter **From URI**: **416XXX1396@avayalab.com**
- Enter **To URI**: **416XXX1396@avayalab.com**

Click **Finish** (not shown).



7.2.9. Configure Topology Hiding – Avaya

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

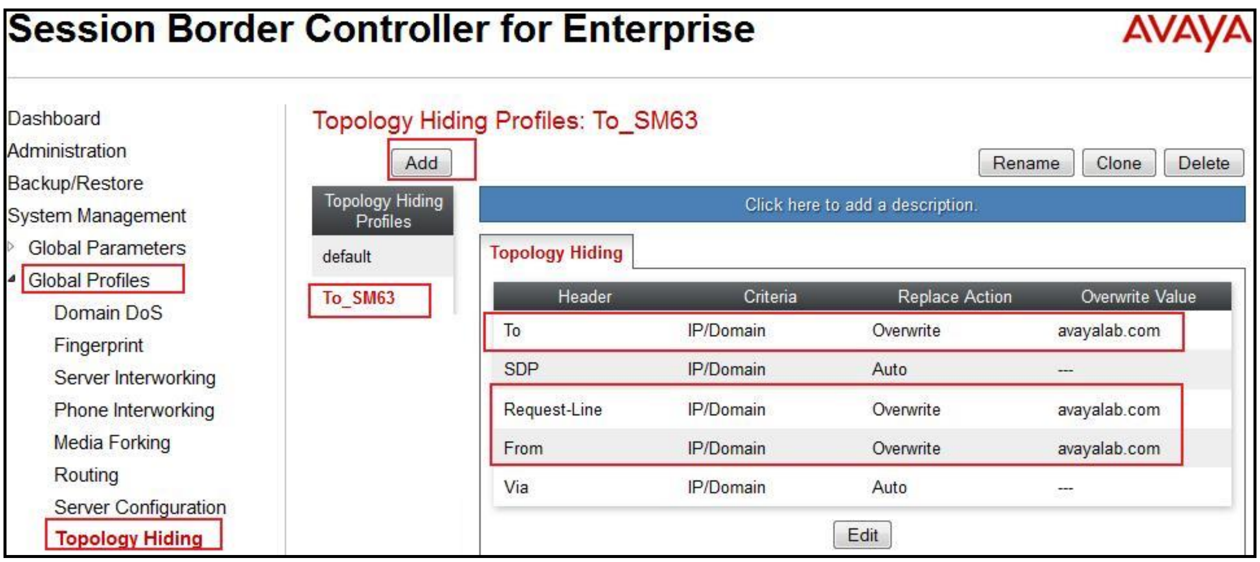
From the menu on the left-hand side, select **Global Profiles → Topology Hiding**.

Select **Add**, enter Profile Name: **To_SM63**.

- For the Header **To,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select **Overwrite**
  - In the **Overwrite Value** column **avayalab.com,** defined in **Section 6.2.**
- For the Header **Request-Line,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select **Overwrite**
  - In the **Overwrite Value** column select **avayalab.com,** defined in **Section 6.2.**
- For the Header **From,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select **Overwrite**

    In the **Overwrite Value** column select **avayalab.com**

Click **Finish** (not shown).



7.2.10. Configure Topology Hiding – Bell

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

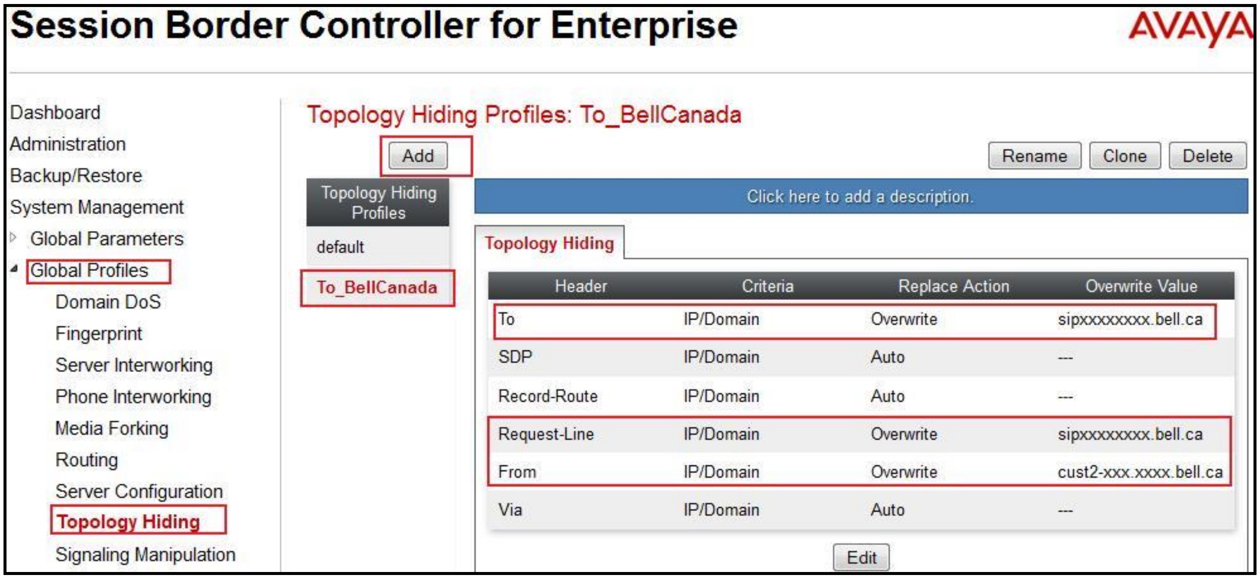
Select **Add Profile**, enter Profile Name: **To_BellCanada**.

- For the Header **To,**
  - In the **Criteria** column select **IP/Domain**

- In the **Replace Action** column select **Overwrite**
- In the **Overwrite Value** column select **sipxxxxxxxx.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 select **sipxxxxxxxx.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 select **cust2-xxx.xxxx.bell.ca**

Click **Finish** (not shown).



7.3. Domain Policies

The Domain Policies feature allows administrator 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 administrator can create a custom domain policy.

7.3.1. Application Rules

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

In this testing, the default-trunk rule is used for both; Enterprise (Avaya) and Bell.

7.3.2. Border Rules

Border Rules allow administrator to control NAT Traversal. The NAT Traversal feature allows administrator 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.

In this testing, the default rule is used for both; Enterprise (Avaya) and Bell.

7.3.3. Media Rules

Media Rules allow administrator 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 UC-Sec security product.

In this testing, the default-low-med rule is used for both; Enterprise (Avaya) and Bell.

7.3.4. Security Rules

Security Rules allow administrator 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, administrator can also define the security feature profile, so that the feature is applied in a specific manner to a specific situation.

In this testing, the default-high rule is used for both; Enterprise (Avaya) and Bell.

7.3.5. Signalling Rules

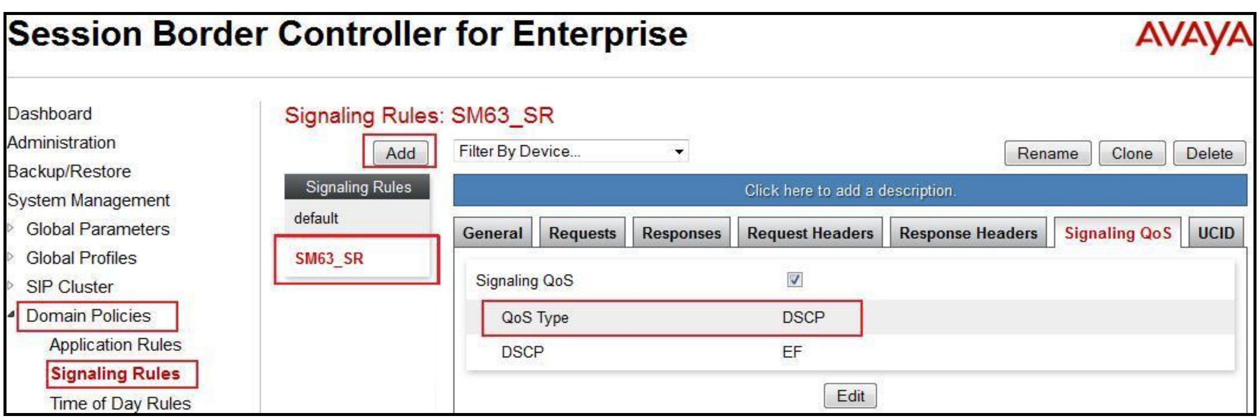
Signaling Rules allow administrator to define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and “pattern matched” against the particular signaling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

In the compliance testing, two **Signaling Rules** were created for Enterprise (Avaya) and Bell.

For Bell Signaling Rules, navigate to **Domain Policies→ Signaling Rules**, select the **default** rule. Then click on the **Clone Rule** button (not shown).

- Select **Add**.
- Enter **Rule Name: BellCanada_SR**
- Select **Next** (not shown).
- Select **Next** again (not shown).
- Enable **DSCP** under **QoS.**
- Select **Next** (not shown).
- Select **Finish** (not shown).

Similarly for Enterprise (Avaya), the **Rule Name** is **SM63_SR**.



7.3.6. Time of Day Rules

A Time-of-day (ToD) Rule allows administrator 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.

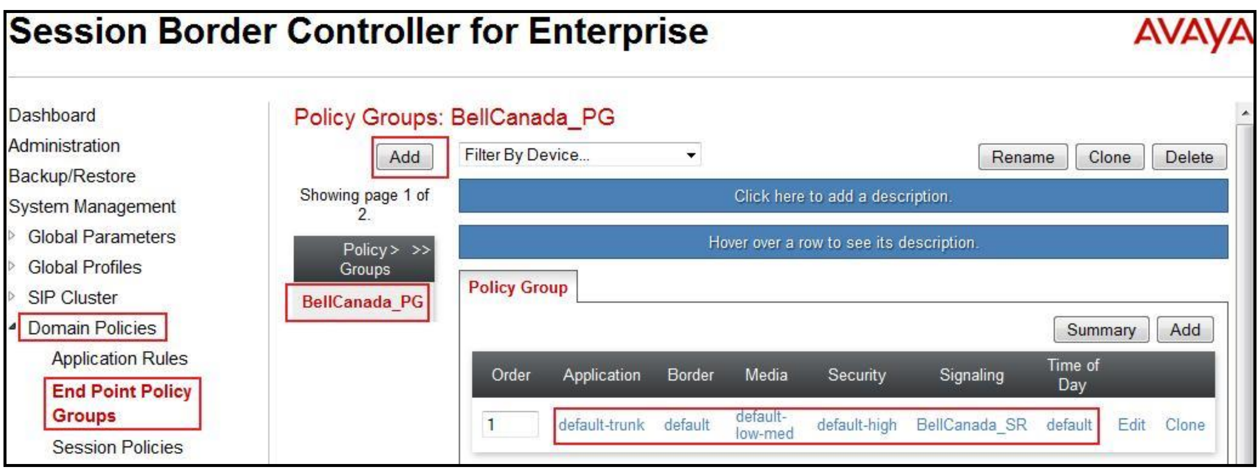
In this testing, **default** rule is used for both; Enterprise (Avaya) and Bell.

7.3.7. Endpoint Policy Groups

The End-Point Policy Group feature allows administrator 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 UC-Sec security features to very specific types of SIP signaling messages traversing through the enterprise.

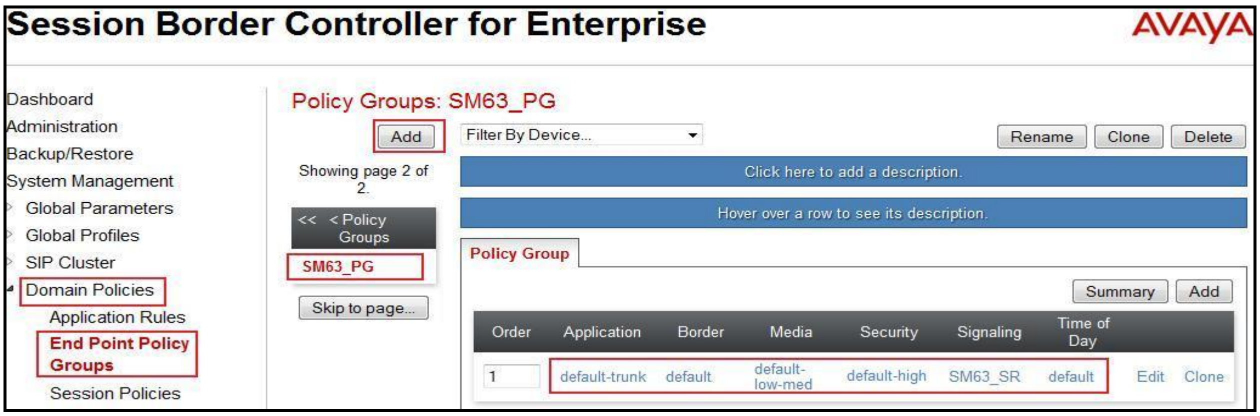
From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

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



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

- Select **Add**.
- Enter **Group Name**: **SM63_PG**
  - **Application Rule**: **default-trunk**
  - **Border Rule**: **default**
  - **Media Rule**: **default-low-med**
  - **Security Rule**: **default-high**
  - **Signaling Rule**: **SM63_SR**
  - **Time of Day**: **default**
- Select **Finish** (not shown).



7.3.8. 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 criterions will be handled by the Avaya SBCE product.

In this testing, **default** rule is used.

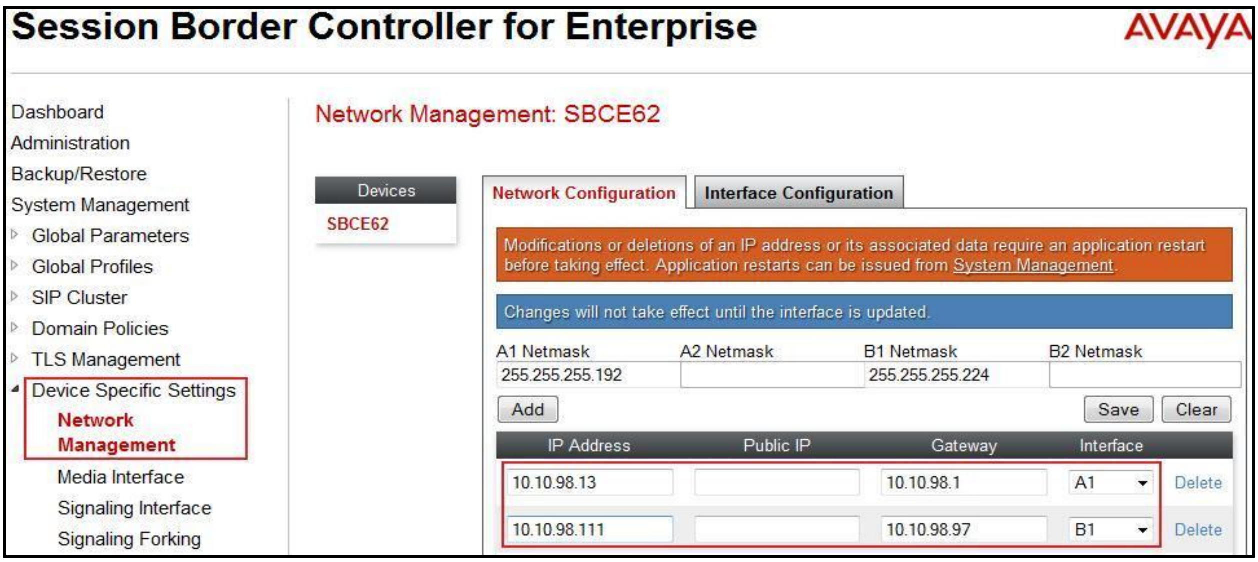
7.4. Device Specific Settings

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

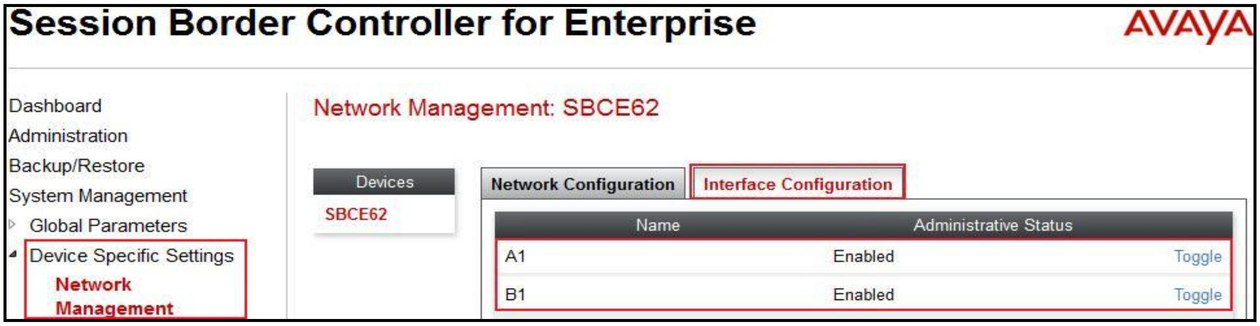
7.4.1. Manage Network Settings

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

- 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**.



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

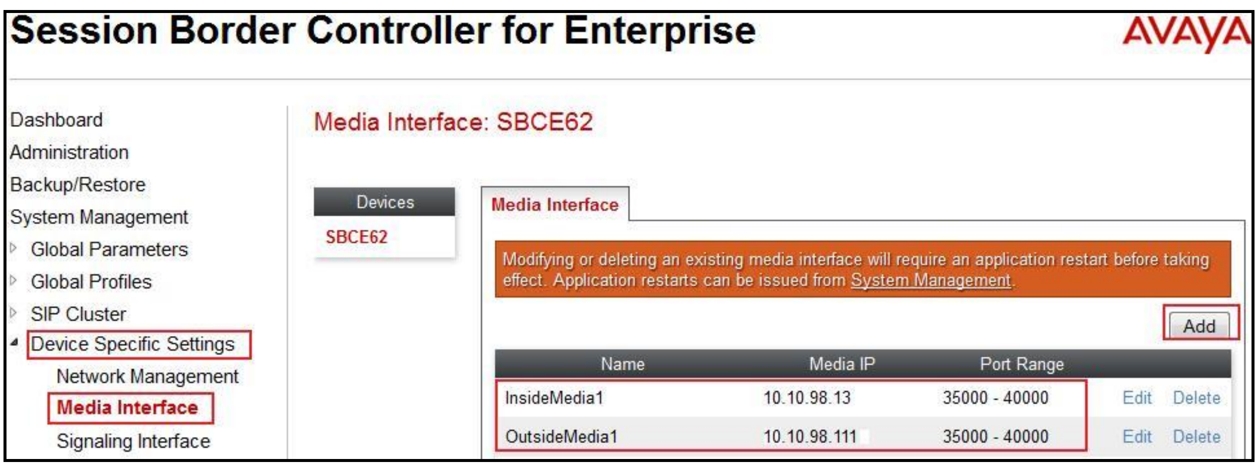


7.4.2. Create Media Interfaces

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

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

- Select **Add**
  - **Name**: **InsideMedia1**
  - **Media IP**: **10.10.98.13** (Internal IP Address toward SM)
  - **Port Range**: **35000 - 40000**
- Click **Finish** (not shown).
- Select **Add**
  - **Name**: **OutsideMedia1**
  - **Media IP**: **10.10.98.111** (External IP Address toward Bell SIP trunk)
  - **Port Range**: **35000 - 40000**
- Click **Finish** (not shown).



7.4.3. Create Signaling Interfaces

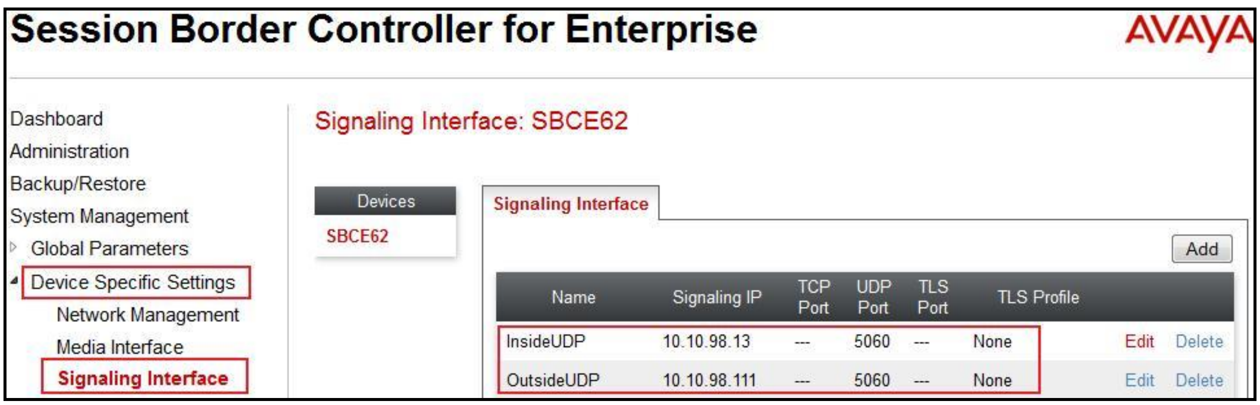
Signaling Interfaces define the type of signaling on the ports.

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

- Select **Add**
  - **Name**: **InsideUDP**
  - **Signaling IP**: **10.10.98.13** (Internal IP Address toward SM)
  - **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**
  - **Signaling IP**: **10.10.98.111** (External IP Address toward Bell SIP trunk)
  - **UDP Port**: **5060**
- Click **Finish** (not shown).



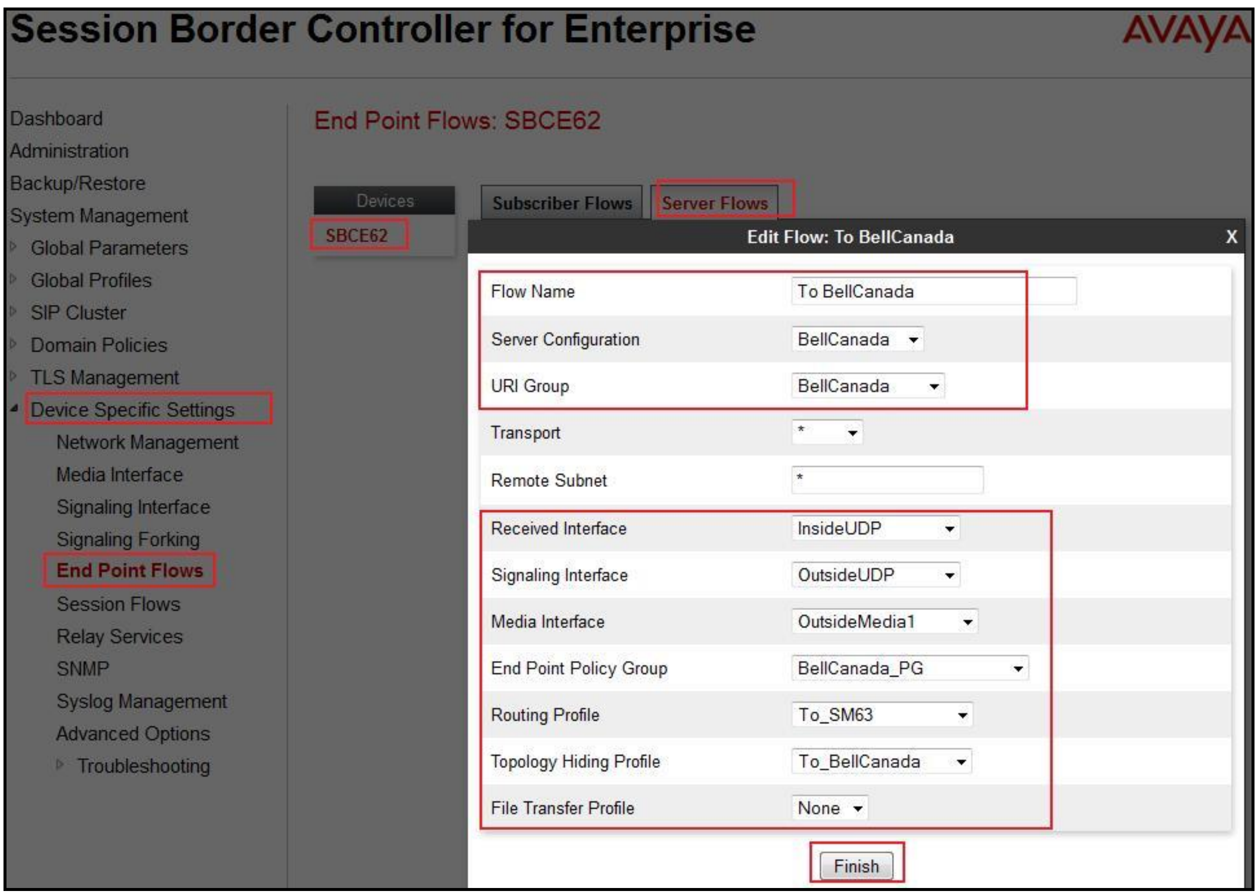
7.4.4. Configuration Server Flows

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

7.4.4.1 Create End Point Flows – To BellCanada

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

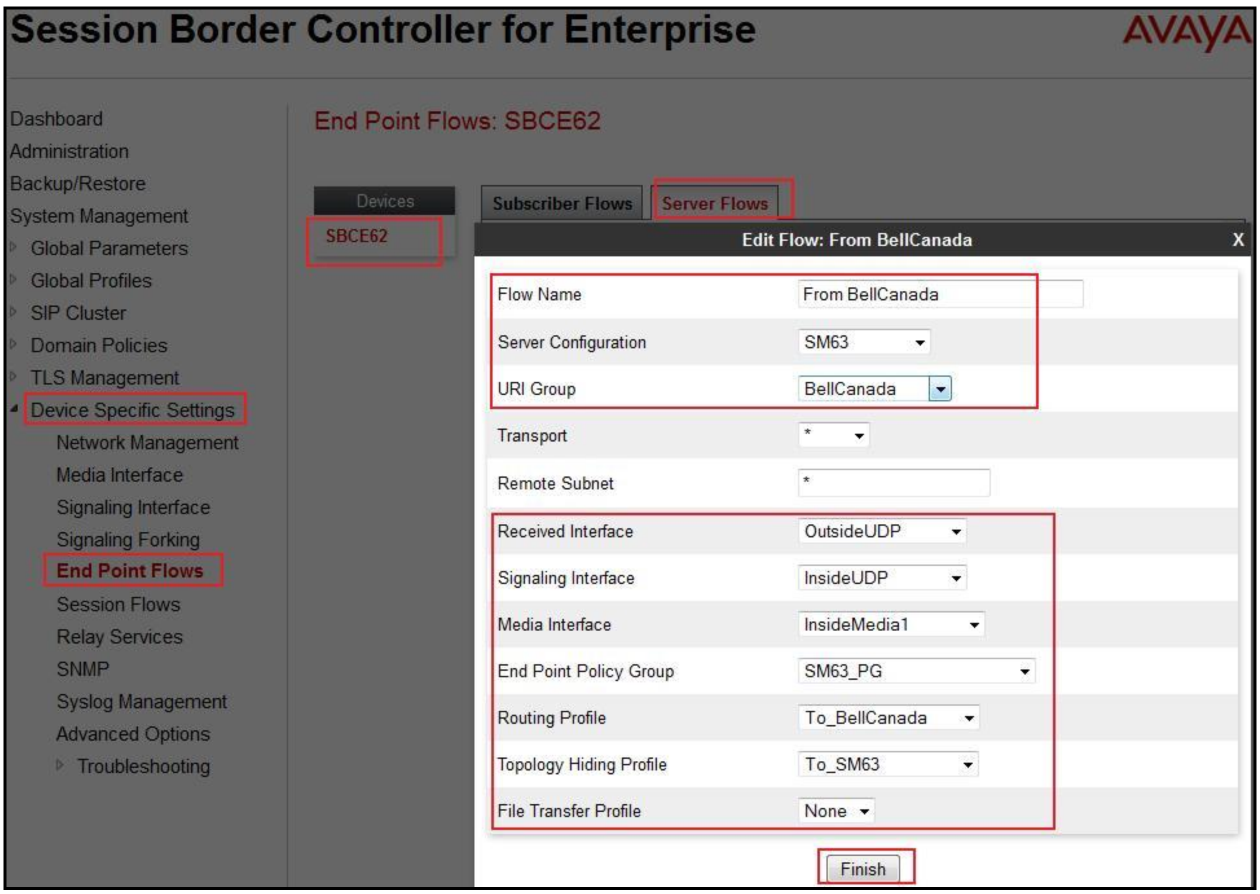
- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name**: **To BellCanada**
  - **Server Configuration**: **BellCanada,** defined in **Section 7.2.8**
  - **URI Group**: **BellCanada,** defined in **Section 7.2.3**
  - **Transport:** Default value, *
  - **Remote Subnet:** Default value, *
  - **Received Interface**: **InsideUDP**
  - **Signaling Interface**: **OutsideUDP**
  - **Media Interface**: **OutsideMedia1**
  - **End Point Policy Group**: **BellCanada_PG,** defined in **Section 7.3.7**
  - **Routing Profile**: **To_SM63,** defined in **Section 7.2.4**
  - **Topology Hiding Profile**: **To_BellCanada,** defined in **Section 7.2.10**
  - **File Transfer Profile**: **None**
- Click **Finish** (not shown).



7.4.4.2 Create End Point Flows – From BellCanada

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

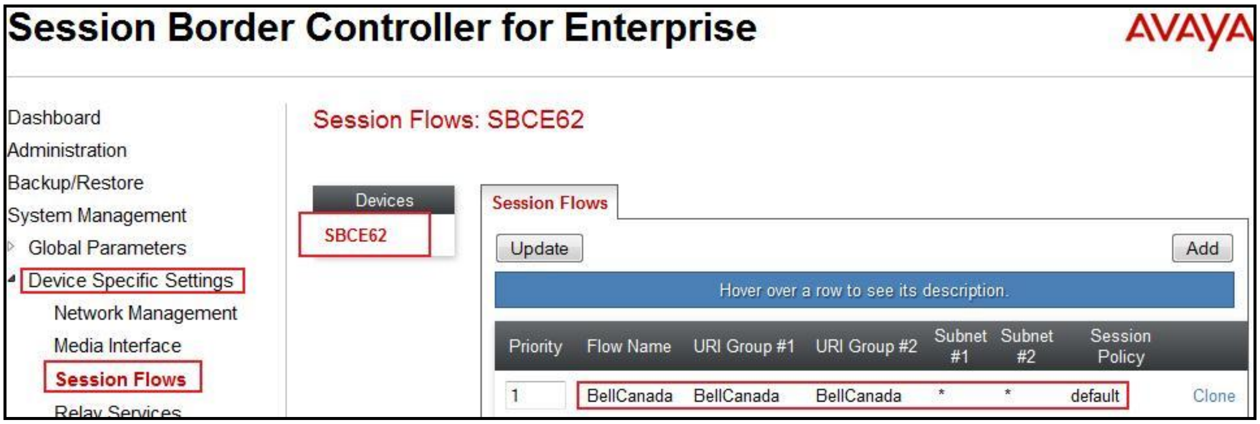
- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name**: **From BellCanada**
  - **Server Configuration**: **SM63**, defined in **Section 7.2.7**
  - **URI Group**: **BellCanada**, defined in **Section 7.2.3**
  - **Transport:** Default value,*****
  - **Remote Subnet:** Default value,*****
  - **Received Interface**: **OutsideUDP**
  - **Signaling Interface**: **InsideUDP**
  - **Media Interface**: **InsideMedia1**
  - **End Point Policy Group**: **SM63_PG**, defined in **Section 7.3.7**
  - **Routing Profile**: **To_BellCanada**, defined in **Section 7.2.5**
  - **Topology Hiding Profile**: **To_SM63**, defined in **Section 7.2.9**
  - **File Transfer Profile**: **None**
- Click **Finish** (not shown).



7.4.5. 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**.
- **Flow Name**: **BellCanada**
  - **URI Group#1**: **BellCanada**
  - **URI Group#2**: **BellCanada**
  - **Session Policy**: **default**
- Click **Finish** (not shown).



8. Bell Canada SIP Trunking Service Configuration

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

The configuration between Bell system and Avaya enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to Bell system network.

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

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

9.2. Verification of an Active Call on CS1000

Active Call Trace (LD 80)

The following is an example of one of the commands available on the CS1000 to trace a DN (1396) for which the call is in progress or idle. The call scenario involved PSTN telephone number 6139675203 calling 416XXX1396 (which is mapped to telephone 1396).

- Log in to CS1000 Signaling Server 10.10.97.154 with administrator 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 **trac 0 1396**. It should show the TN is active as show bellow.

Below is the actual output of the CS1000 Call Server Command Line mode when the 1396 is in call state:

```
>ld 80

.trac 0 1396

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: 10.10.97.184
  FAR-END MEDIA ENDPOINT IP: 10.10.97.184  PORT: 21582
  FAR-END SIP SIGNALLING IP: 10.10.97.184
  FAR-END MEDIA ENDPOINT IP: 10.10.97.184  PORT: 21582
TERM   VTN 096 0 00 02  KEY 0  SCR MARP  CUST 0  DN 1396  TYPE 2007
```

```
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 10.33.5.4  PORT: 5200
MEDIA PROFILE: CODEC G.729A NO-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 1396
MAIN_PM  ESTD
TALKSLOT  ORIG  10   TERM  15
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 34385


----  ISDN ISL CALL (ORIG) ----
CALL REF # =  385
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  6139675203  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
CALLED NO  =  416XXX1396  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
```

- After the call is released, issue command **trac 0 1396** again to see if the DN is released back to idle state. It should show the TN is in idle state.

Below is the example after the call to 1396 is finished.

```
.trac 0 1396
IDLE VTN 096 0 00 02   MARP
```

SIP Trunk monitoring (LD 32)

Place a call inbound from PSTN (6139675203) to an internal device (416XXX1396). Then check the SIP trunk status by using LD 32, and verify that one trunk is BUSY.

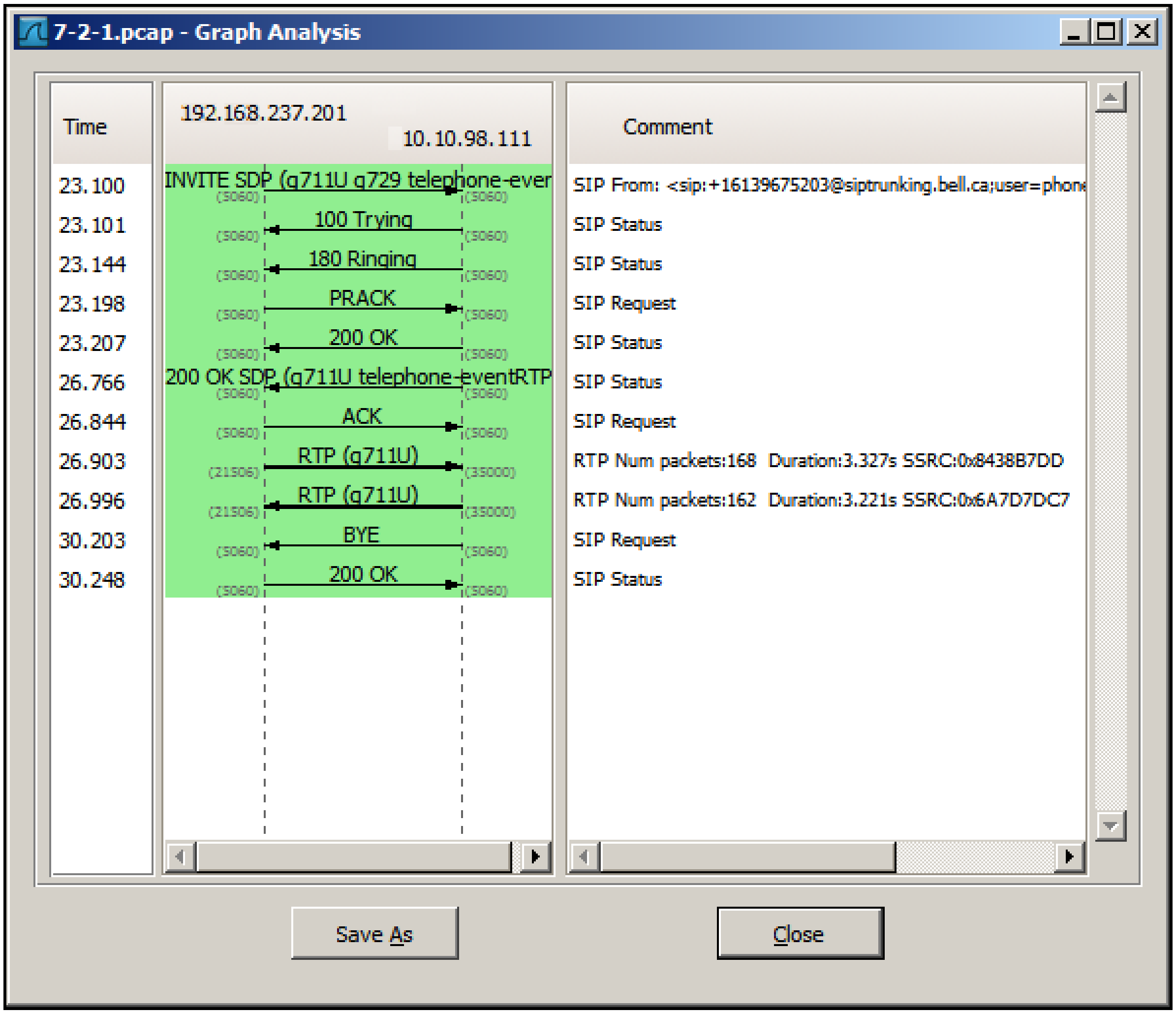
```
>ld 32
NPR000
.stat 100 0
063 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

After the call is released, check all SIP trunk status changed to IDLE state.

```
.stat 100 0
064 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

9.3. Protocol Trace

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



10. Conclusion

All of the test cases have been executed. The test results met the objectives outlined in **Section 2.1**, within the constraints described in **Section 2.2**. The Bell Canada SIP Trunking service is considered **compliant** with Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2.

11. Additional References

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

[1] *Network Routing Service Fundamentals, Avaya CS1000, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013.*

[2] *IP Peer Networking Installation and Commissioning, Avaya CS1000, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013.*

[3] *CS1000E Overview, Avaya CS1000, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013.*

[4] *Unified Communications Management Common Services Fundamentals, Avaya CS1000, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013.*

[5] *Dialing Plans Reference, Avaya CS1000, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.*

[6] *Product Compatibility Reference, Avaya CS1000, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013.*

[7] *Administering Avaya Aura® Session Manager, Release 6.3, Issue 2, June 2013*

[8] *Maintaining and Troubleshooting Avaya Aura® Session Manager, Release 6.3, Issue 2, May 2013*

[9] *Administering Avaya Aura® System Manager, Release 6.3, Issue 2, May 2013*

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

[11] *Installing Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, June 20 2013.*

[12] *Upgrading Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, July 2013.*

Product services for Bell Canada SIP Trunking Services may be found at:
http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page

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.