Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunk Service with Avaya Communication Server 1000 Release 7.6, and Avaya Session Border Controller for Enterprise Release 6.3 – Issue 1.0

Abstract

These Application Notes describe the procedure for configuration of the MTS Allstream SIP Trunk Service with Avaya Communication Server 1000 Release 7.6, and Avaya Session Border Controller for Enterprise Release 6.3.

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.

MTS Allstream SIP Trunk Service provides PSTN access via SIP trunks between the enterprise and the MTS Allstream SIP Trunk Service'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, and Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.3 with MTS Allstream SIP Trunk Service. MTS Allstream SIP Trunk Service provides PSTN access via SIP Trunks between the enterprise and the MTS Allstream SIP Trunk Service's network as an alternative to legacy analog or digital trunks.

2. General Test Approach and Test Results

CS1000 was connected to Avaya SBCE by using SIP Trunks. Avaya SBCE was connected to MTS Allstream SIP Trunk Service's network via SIP trunks. Various call types were made from CS1000 to MTS Allstream SIP Trunk Service 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 MTS Allstream SIP Trunk Service, including the following:
    - Codec/ptime (G.711 a-law/20ms, G.711 mu-law/20ms, and G.729/20ms), no Voice Activity Detection (VAD).
    - Calling Line Identification Display (CLID).
    - Ring-back tone.
    - Speech (audio) path.
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya IP Softphone 2050.
- Dialing plan support: local, long distance, international, outbound toll-free, 911 Emergency, 411 Service, and Operator Assisted Call.
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference). Call redirection was performed from both ends. Note: MTS Allstream SIP Trunk Service supports Diversion Header for off-net call forwarding.
- Response to SIP OPTIONS queries.

- Response to incomplete call attempts and trunk errors.
- Fax T.38 and G.711 pass-through.
- Inbound and outbound long hold time call stability.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF (RFC2833) in inbound and outbound calls.
- SIP Transport UDP, port 5060.
- Voicemail navigation for inbound and outbound calls.
- CS1000 Mobile-X feature.
- Early Media Transmission.

The following is item not tested:

- Inbound toll-free is supported but was not tested as part of the compliance test.

The following assumptions were made for the compliance tested configuration:

- CS1000 R7.6 software with latest patches.
- MTS Allstream 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 tested scenario:

- Calls were checked for the correct call progress tones and cadences.
- During the ringing state, the ring back tone and destination ringing were checked.
- Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
- Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
- The display(s) of the sets/clients involved were checked for consistent and expected CLID and redirection information both prior to answer and after call establishment.
- The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
- The call server maintenance terminal window was open during the test execution for the monitoring of BUG(s), ERROR and AUD messages (See **Section 5.1.2**).
- Speech path was checked before and after calls were put on/off hold from each end.
- Calls were checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and Voice Gateways (VGWs) were released when calls were ended (See SIP Trunk monitoring in **Section 8.2**).

2.2. Test Results

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

- **The Calling Line Identification Display (CLID) was not available after hold/resume** – If the CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed. This is a CS1000 known issue.
- **There is no ring-back tone after the off-net blind transfer is completed** - PSTN1 phone calls the CS1000 phone, the user could not press the transfer button on the CS1000 phone to complete a blind transfer to PSTN2. In this particular scenario, SIP UPDATE support was required on the CS1000 for blind transfer, but for some reason, the SIP UPDATE on the PSTN-to-SIP gateway that MTS Allstream service used for this interoperability testing was not supported. In order to resolve this, plug-in 501 was enabled on the CS1000 to allow blind transfer to work without the UPDATE method (On CS1000 Element Manager, select **System → Software → Plug-ins** and then click on number **501** to enable plug-in 501). After the user was able to press the transfer button on the CS1000 to complete blind transfer, the PSTN1 phone could not hear ring-back-tone from the PSTN2. This is a CS1000 limitation.
- **There is no ring-back tone in Mobile-X phone to PSTN** – Mobile-X phone dials Mobile Service Access(MSA) number, then dials any PSTN phone number. Mobile-X phone could not hear ring-back-tone from the PSTN. This is CS1000 limitation.

2.3. Support

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

For technical support on the MTS Allstream SIP Trunk Service, please contact customer service at 855-299-7050 or visit: http://www.allstream.com/support.

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance test between CS1000 and MTS Allstream 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.

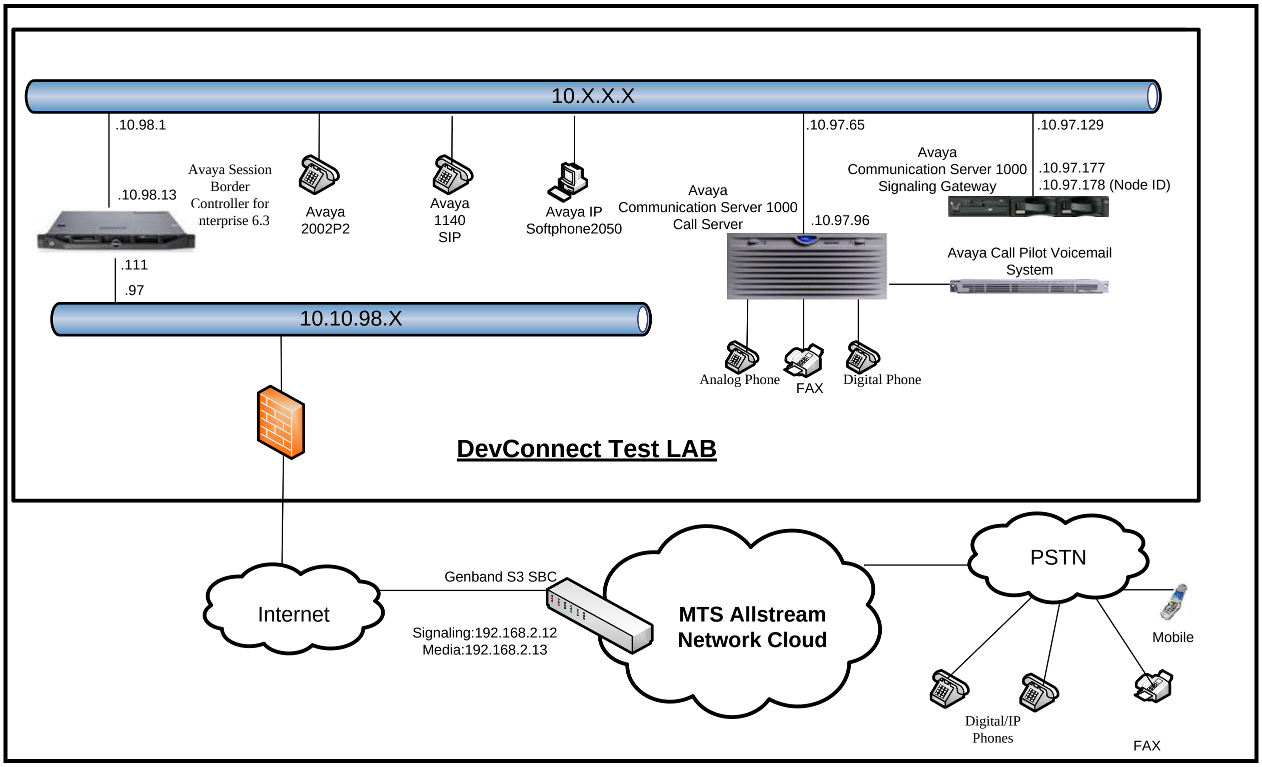

Figure 1 - Network diagram for Avaya and MTS Allstream SIP Trunk Service

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 Session Border Controller for Enterprise	6.3.000-19-4338
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
Analog Symphony 2000	N/A
HP Office jet 4500 Fax	N/A

MTS Allstream SIP Trunk Service systems:

System	Software
Genband S3 SBC	7.1.15.2
Genband CS2K Hybrid SoftSwitch	CVM17

Additional patch lineup for the configuration is listed as follows:

Call Server: 7.65 P+ GA plus latest DEPLIST – CPM_7.6_6.zip (X2107.65P)
Signaling Server: 7.65.16 GA plus latest DEPLIST – SP_7.6_6.ntl (7.65.16.00)
CS1000 Signaling Server patch list:

```
[admin@car3-cores ~]$ pstat
Product Release: 7.65.16.00
In system patches: 5
PATCH#   NAME      IN_SERVICE   DATE     SPECINS  TYPE   RPM
38     p31484_1   Yes        20/02/14  NO      FRU    cs1000-shared-general-7.65.16-00.i386
47     p33125_1   Yes        23/12/14  NO      FRU    cs1000-OS-1.00.00.00-00.noarch
48     p33274_1   Yes        23/12/14  YES     FRU    initscripts-8.45.25-1.el5.i386
49     p33331_1   Yes        23/12/14  YES     FRU    cs1000-OS-1.00.00.00-00.noarch
50     p33384_1   Yes        23/12/14  NO      FRU    cs1000-OS-1.00.00.00-00.noarch

In System service updates: 31
PATCH#  IN_SERVICE   DATE      SPECINS   REMOVABLE   NAME
0      Yes        23/12/14   YES      YES        cs1000-linuxbase-7.65.16.23-3.i386.000
```

1	Yes	23/12/14	NO	YES	cs1000-Jboss-Quantum-7.65.16.23-3.i386.000
2	Yes	23/12/14	YES	YES	cs1000-patchWeb-7.65.16.22-4.i386.000
3	Yes	23/12/14	YES	YES	cs1000-dmWeb-7.65.16.23-1.i386.000
4	Yes	23/12/14	YES	YES	cs1000-csoneksvrmgr-7.65.16.22-5.i386.000
5	Yes	23/12/14	YES	YES	cs1000-baseWeb-7.65.16.22-4.i386.000
6	Yes	23/12/14	YES	YES	cs1000-oam-logging-7.65.16.22-4.i386.000
7	Yes	23/12/14	YES	YES	cs1000-csv-7.65.16.22-2.i386.000
8	Yes	23/12/14	YES	YES	cs1000-mscTone-7.65.16.22-2.i386.000
9	Yes	23/12/14	YES	YES	cs1000-mscMusc-7.65.16.22-4.i386.000
10	Yes	23/12/14	YES	YES	cs1000-mscConf-7.65.16.22-2.i386.000
11	Yes	23/12/14	YES	YES	cs1000-mscAnnc-7.65.16.22-2.i386.000
12	Yes	23/12/14	YES	YES	cs1000-mscAttn-7.65.16.22-2.i386.000
13	Yes	23/12/14	NO	YES	cs1000-gk-7.65.16.22-1.i386.000
14	Yes	23/12/14	YES	YES	cs1000-shared-pbx-7.65.16.22-3.i386.000
15	Yes	20/02/14	NO	YES	cs1000-pd-7.65.16.21-00.i386.000
16	Yes	20/02/14	NO	YES	cs1000-shared-carrdtct-7.65.16.21-01.i386.000
17	Yes	20/02/14	NO	YES	cs1000-shared-tpselect-7.65.16.21-01.i386.000
18	Yes	20/02/14	NO	yes	cs1000-dbcom-7.65.16.21-00.i386.000
26	Yes	20/02/14	NO	YES	cs1000-snmp-7.65.16.21-00.i686.000
31	Yes	20/02/14	NO	YES	cs1000-shared-omm-7.65.16.21-2.i386.000
34	Yes	20/02/14	YES	YES	cs1000-ipsec-7.65.16.22-1.i386.000
36	Yes	20/02/14	NO	YES	cs1000-cppmUtil-7.65.16.22-1.i686.000
39	Yes	23/12/14	YES	YES	cs1000-shared-xmsg-7.65.16.22-1.i386.000
40	Yes	23/12/14	NO	YES	cs1000-sps-7.65.16.23-1.i386.000
41	Yes	23/12/14	YES	YES	jdk-1.6.0_81-fcs.i586.000
42	Yes	23/12/14	YES	YES	cs1000-cs-7.65.P.100-03.i386.000
43	Yes	23/12/14	NO	YES	bash-3.2-33.el5_11.4.i386.000
44	Yes	23/12/14	NO	YES	tzdata-2014g-1.el5.i386.000
45	Yes	23/12/14	YES	YES	cs1000-tps-7.65.16.23-7.i386.000
46	Yes	23/12/14	YES	YES	cs1000-vtrk-7.65.16.23-24.i386.000

5. Configure Avaya Communication Server 1000

These Application Notes use the Incoming Digit Translation feature to receive calls, the Numbering Plan Area Code (NPA), and the Special Number (SPN) features to route calls from the CS1000 to the PSTN, via SIP trunks to the MTS Allstream SIP Trunk Service network.

These Application Notes assume that the basic CS1000 configuration has already been administered. For further information on CS1000, please consult the references in **Section 10**.

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

5.1. Log into Communication Server 1000 System

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

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

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

Figure 2 – Communication Server 1000 Log In Screen

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

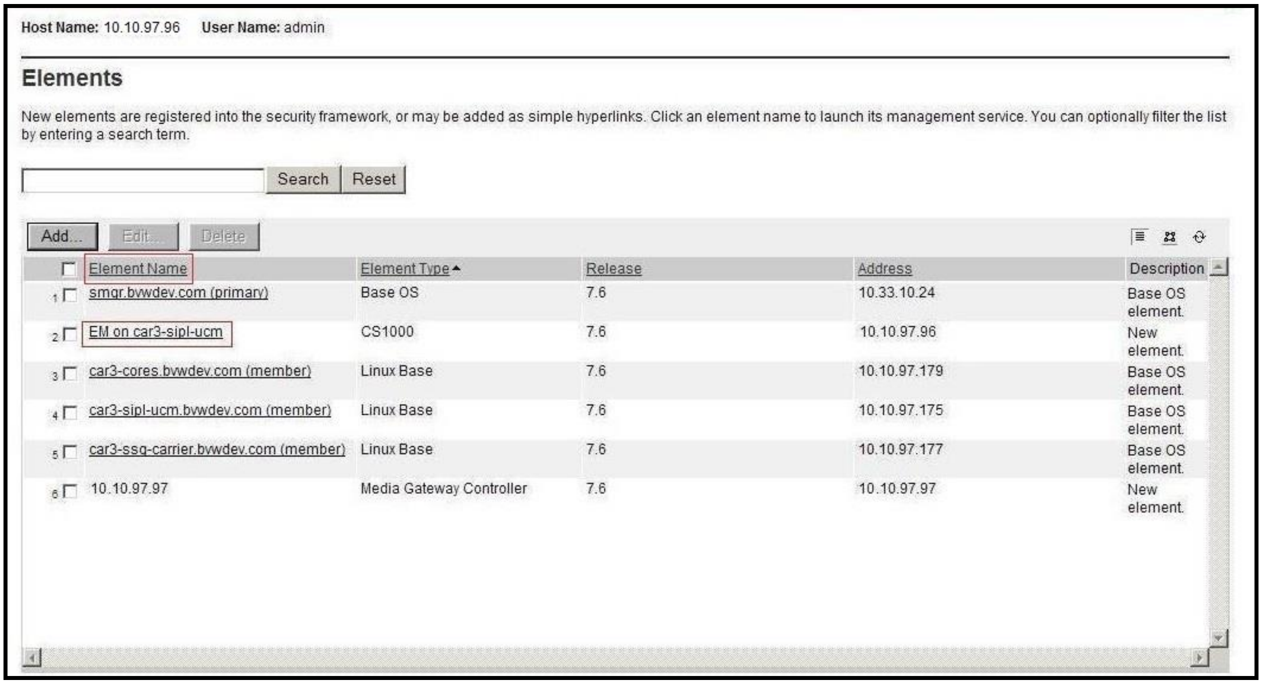

Figure 3 – Communication Server 1000 Management

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

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

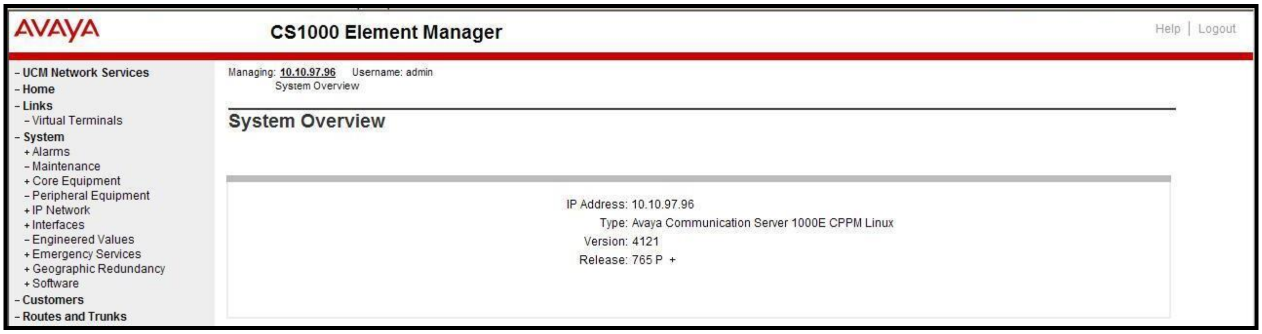

Figure 4 – Element Manager System Overview

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

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

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

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

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

admin@10.10.97.177's password: ← **Enter the password**
Last login: Thur Jan 22 08:22:18 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 01/22/2015

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

>

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

5.2. Administer IP Telephony Node

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

5.2.1. Obtain Node IP address

These Application Notes assume that the basic CS1000 configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 3000) in CS1000 IP network to work with MTS Allstream 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 5**.

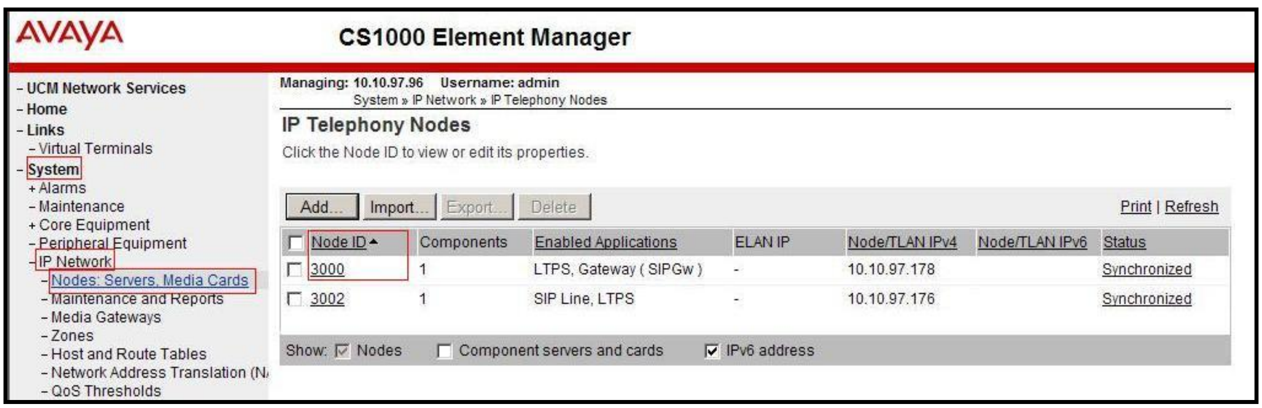

Figure 5 – IP Telephony Node

The **Node Details** screen is displayed in **Figure 6** with the IP address of the CS1000 node. **Call server IP address: 10.10.97.96**. The **Node IPv4 address 10.10.97.178** is a virtual address which corresponds to the **TLAN IPv4** address **10.10.97.177** of the Signaling Server/SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP address to communicate with other components to process SIP calls.

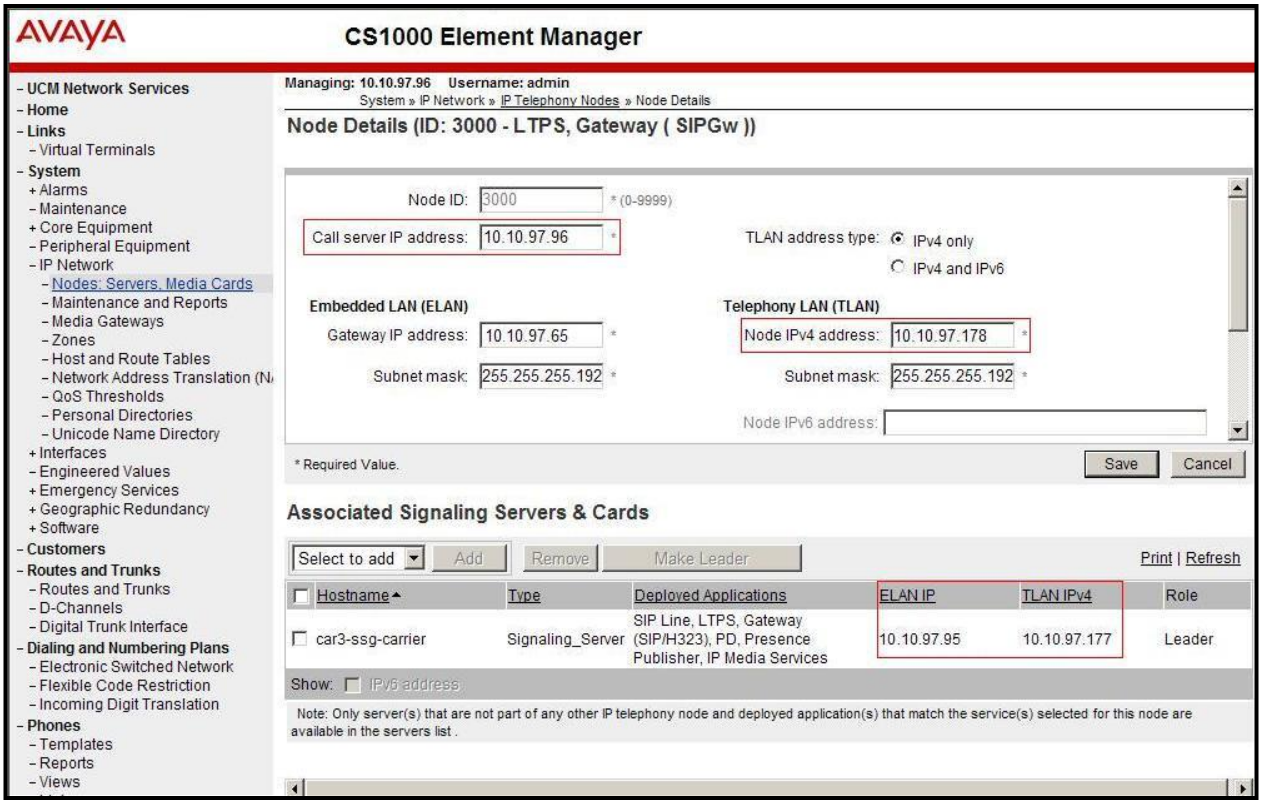

Figure 6 – Node Details 1

The **Node Details** screen is displayed in **Figure 7** with the IP Telephony Node Properties and Applications.

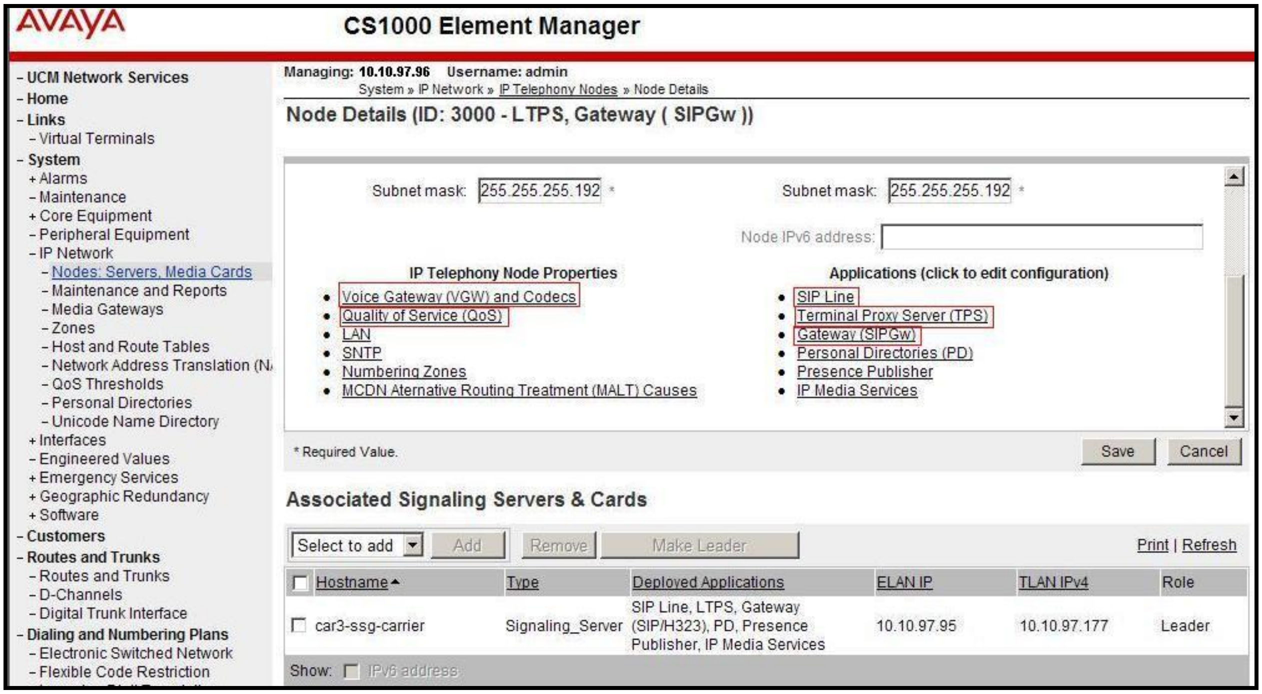

Figure 7 – Node Details 2

5.2.2. Administer Terminal Proxy Server (TPS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Terminal Proxy Server** (**TPS**) link as shown in **Figure 7**. Check the **UNIStim Line Terminal Proxy Server** checkbox to enable proxy service on this node and then click the **Save** button as shown in **Figure 8**.

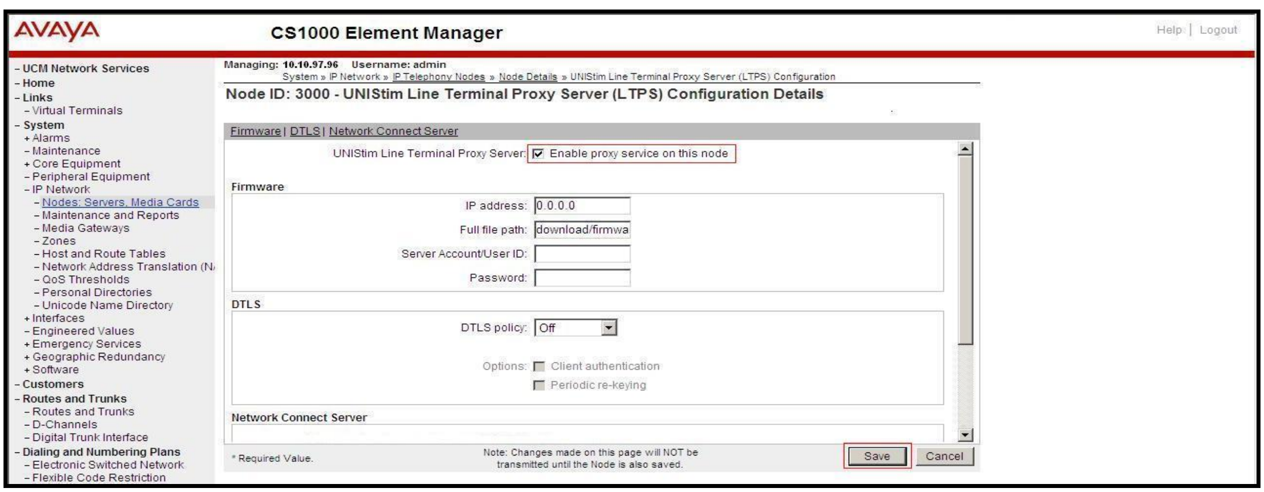

Figure 8 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 7**. The default Diffserv values are as shown in **Figure 9**. Click on the **Save** button.

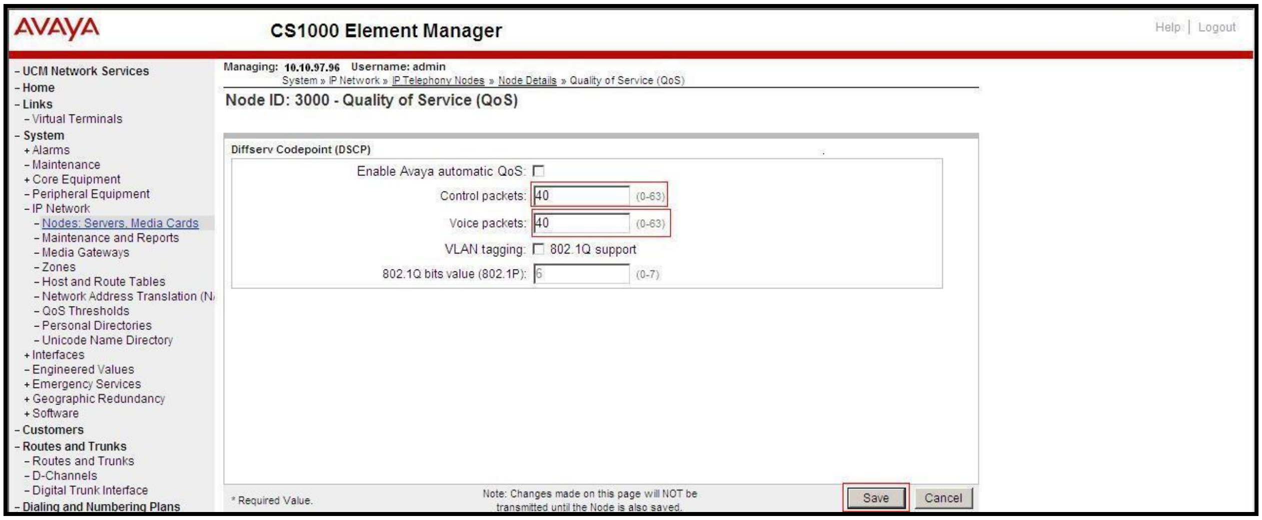

Figure 9 – QoS Configuration Details

5.2.4. Synchronize New Configuration

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

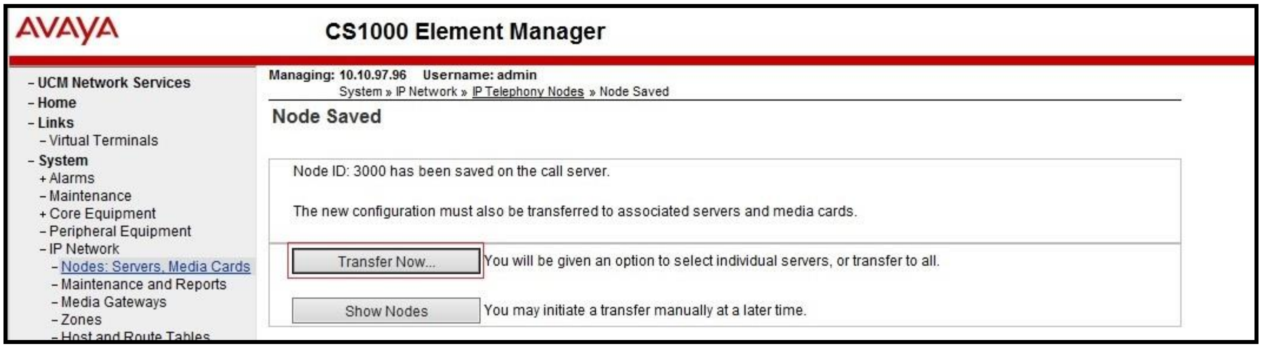

Figure 10 – Node Saved Screen

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

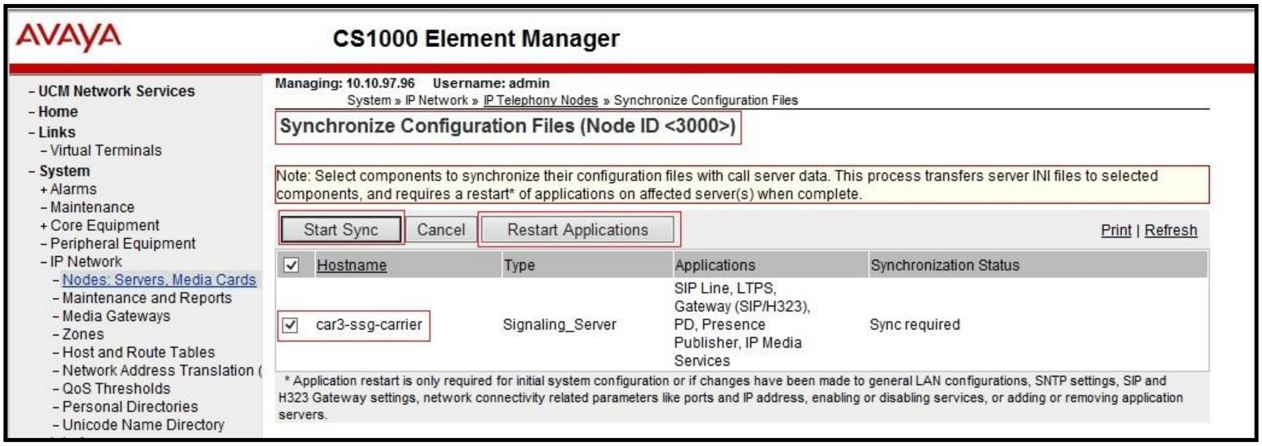

Figure 11 – Node Synchronized Screen

5.3. Administer Voice Codec

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

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 7**, click on **Voice Gateway (VGW) and Codecs**.

MTS Allstream SIP Trunk Service supports **G.711 a-law**, **G.711 mu-law** and **G.729** with **Voice payload size 20 milliseconds per frame.** Uncheck **Voice Activity Detection (VAD)** checkbox. Click on the **Save** button.

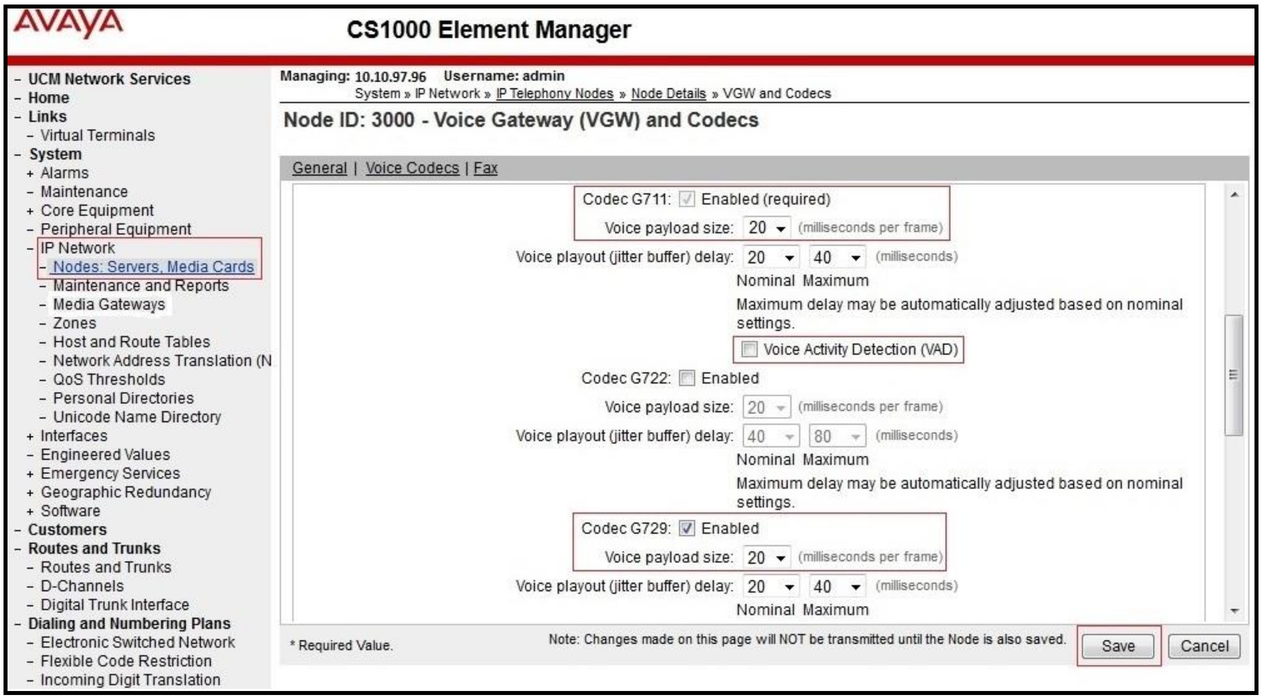

Figure 12 – Voice Gateway and Codec Configuration Details

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

5.3.2. Enable Voice Codec on Media Gateways

From the left menu of the Element Manager page in **Figure 12**, select **IP Network → Media Gateways**. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page. In the following screen, scroll down to select the **Codec G711** and **Code G729A** with **Voice payload size 20 ms/frame** and uncheck **VAD** as shown in **Figure 13**. Scroll down to the bottom of the page and click on the **Save** button (not shown).

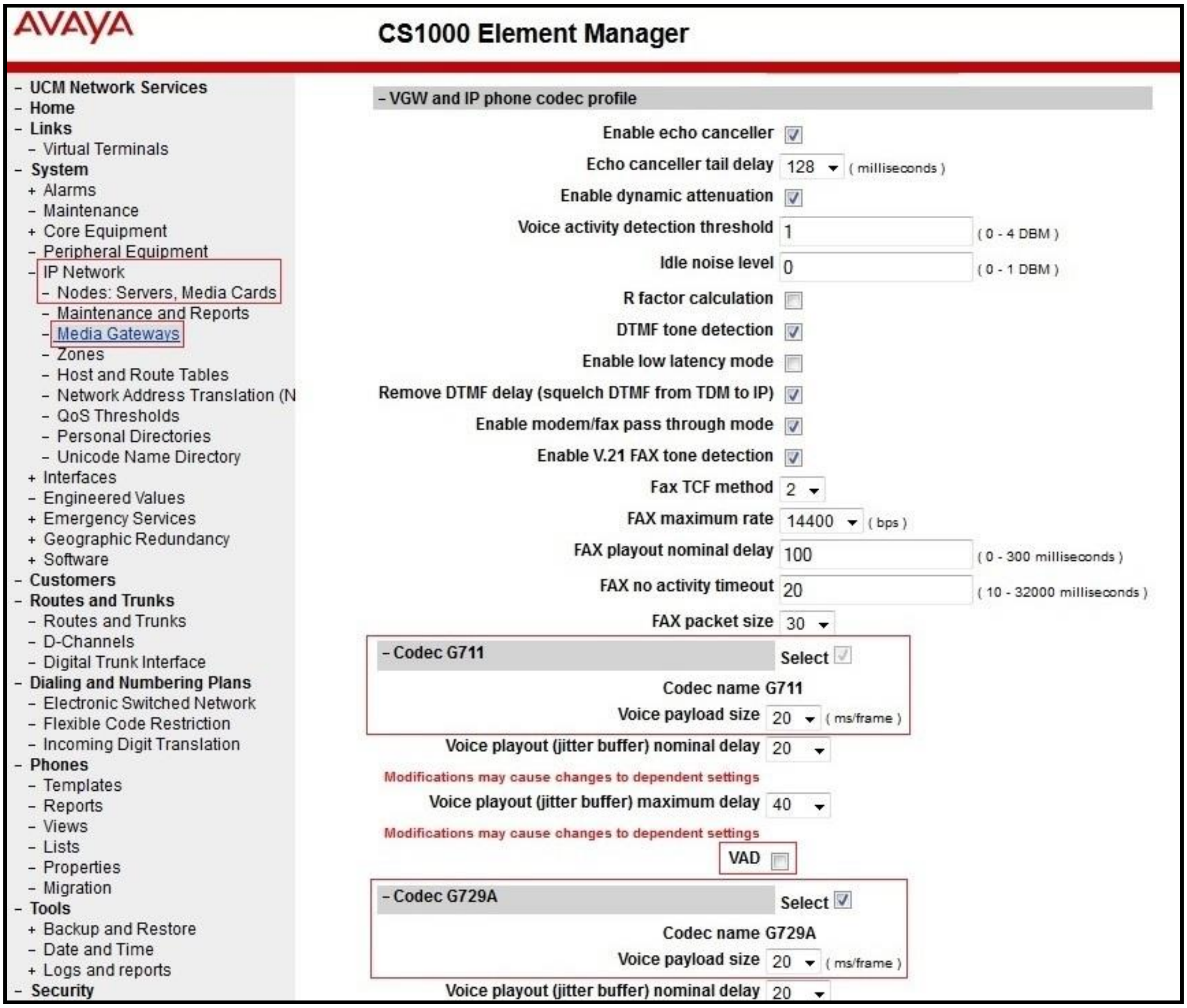

Figure 13 – Media Gateways Configuration Details

5.4. Zones and Bandwidth Management

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

5.4.1. Create Zone for IP Phones (Zone 10)

The following figures show how to configure a zone for VGW and IP phones for bandwidth management purposes. The bandwidth strategy can be adjusted to preference.
Select **IP Network → Zones** from the left pane (not shown), click on **Bandwidth Zones** as shown in **Figure 14**.

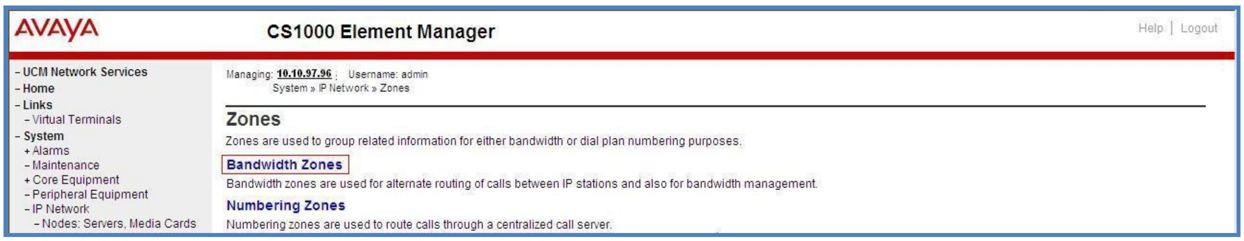

Figure 14 – Zones Page

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

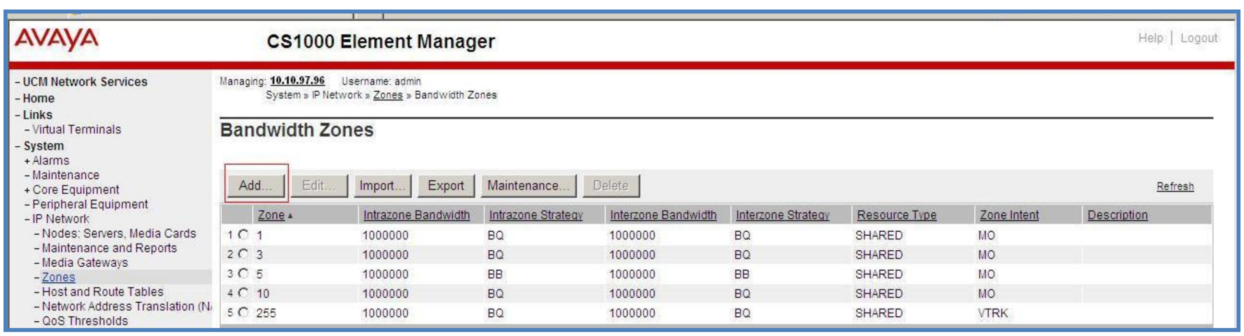

Figure 15 – Bandwidth Zones

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

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

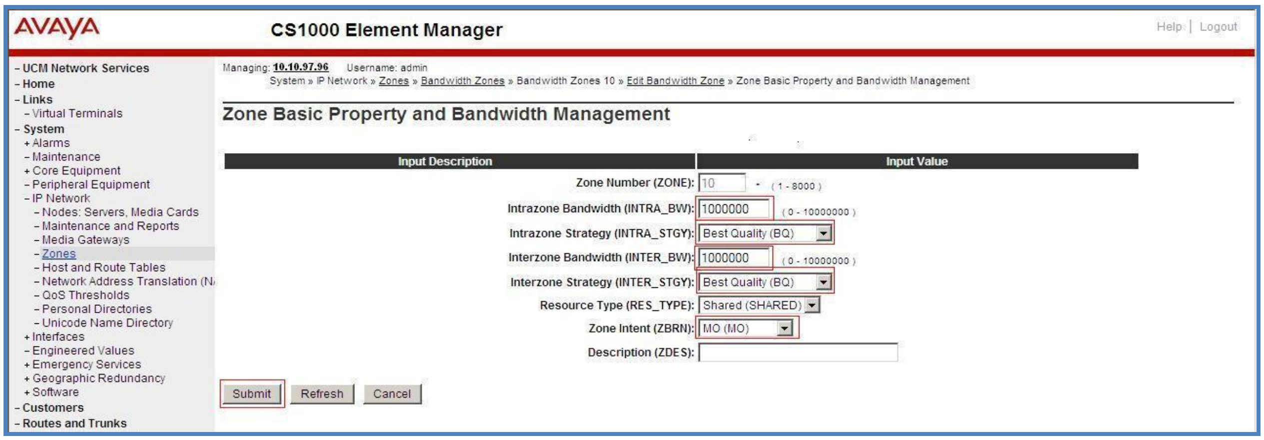

Figure 16 – Bandwidth Management Configuration Details – IP phone

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

Follow the steps described in **Section 5.4.1** to create a zone for the virtual SIP trunk. The difference is in the **Zone Intent (ZBRN)** field. Select **VTRK** for virtual trunk as shown in **Figure 17** and then click on the **Submit** button.

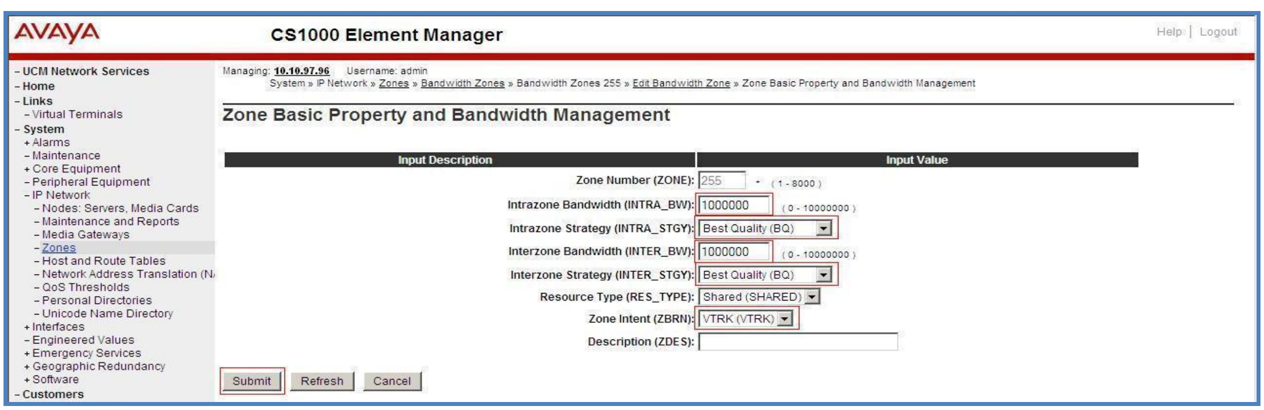

Figure 17 – Bandwidth Management Configuration Details – Virtual SIP trunk

5.5. Administer SIP Trunk Gateway

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

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**.

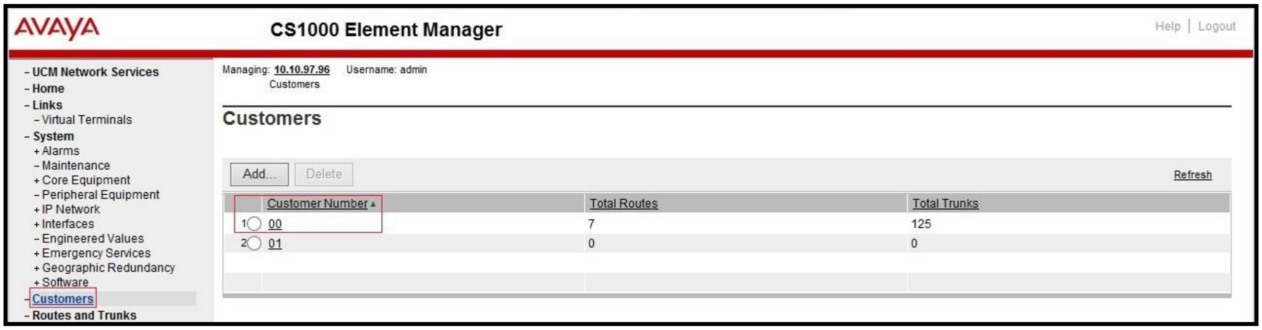

Figure 18 – Customer – ISDN Configuration 1

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

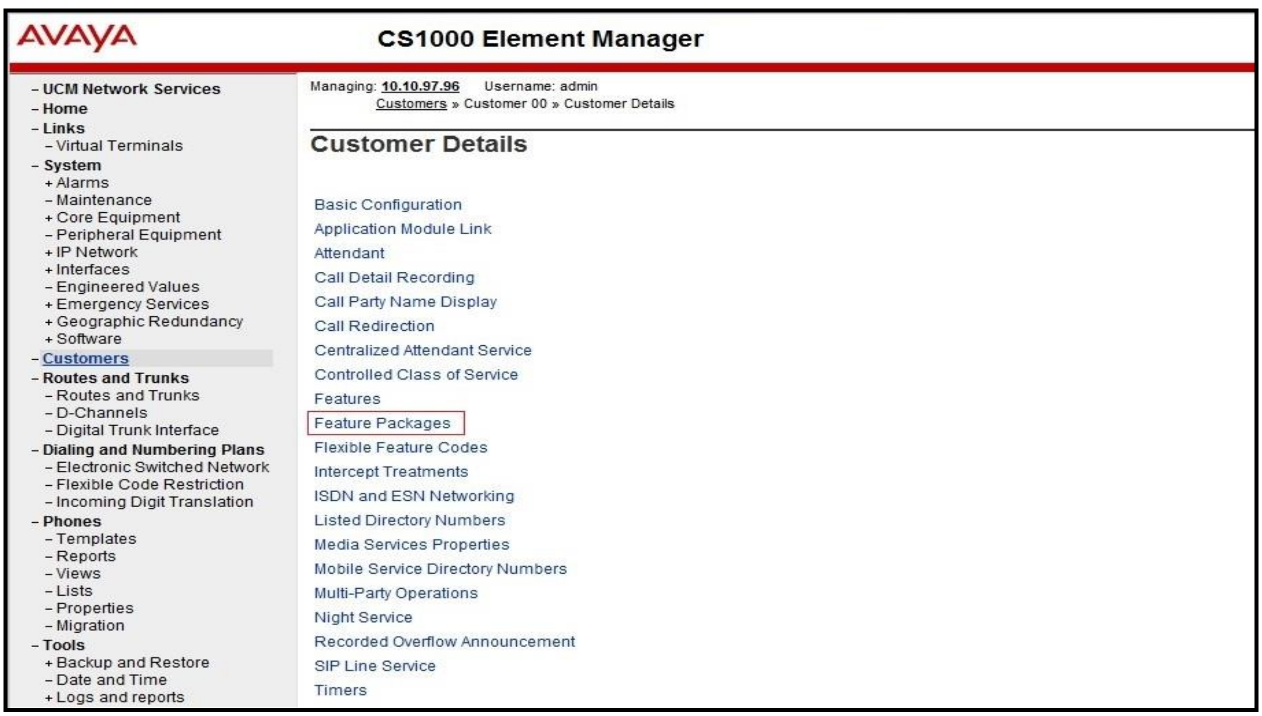

Figure 19 – Customer – ISDN Configuration 2

The screen is updated with a listing of available **Feature Packages** (not all features are shown in **Figure 20** below). Select **Integrated Services Digital Network** to edit the parameters shown below. Check the **Integrated Services Digital Network** option, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click on the **Save** button (not shown).

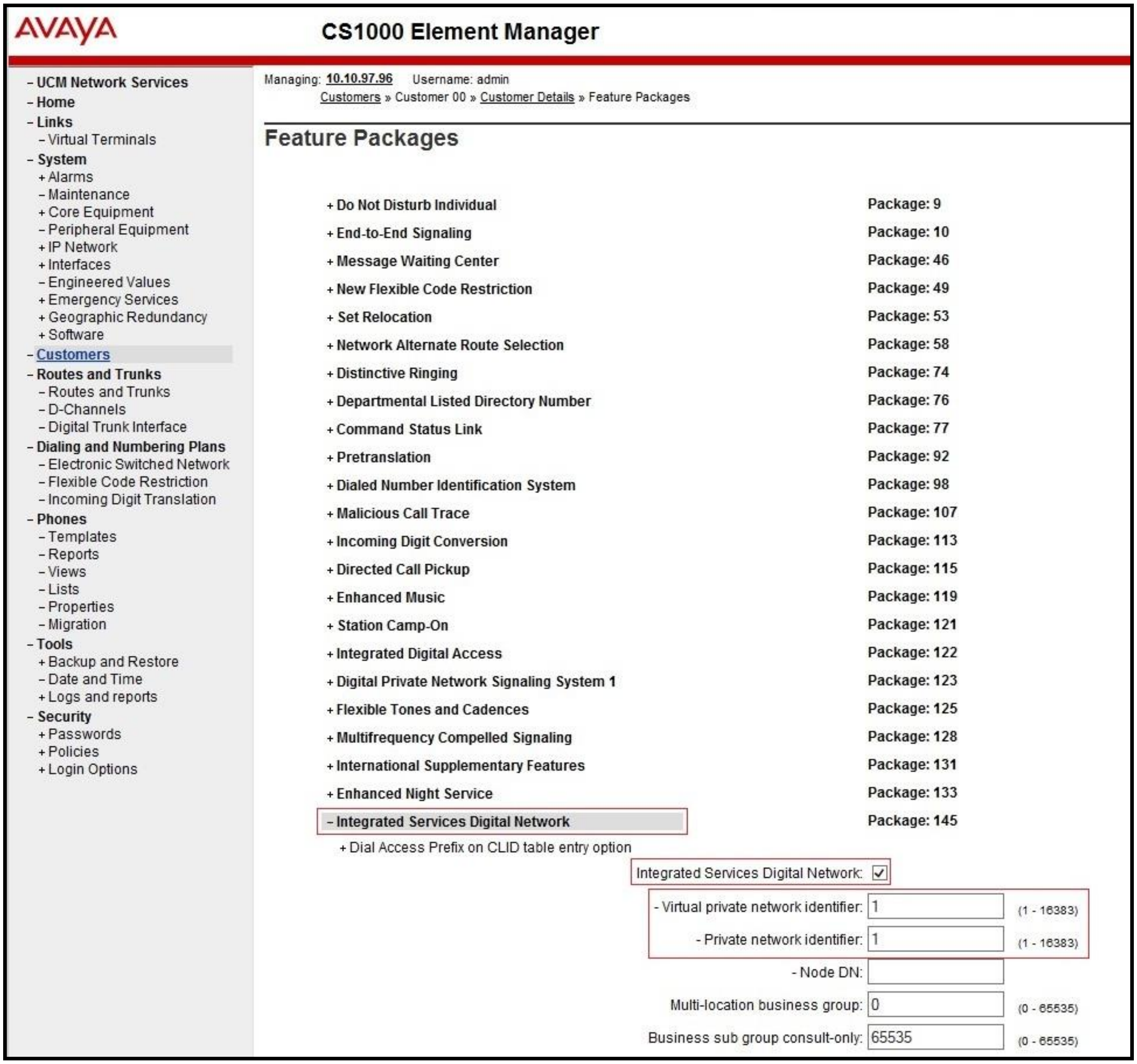

Figure 20 – Customer – ISDN Configuration 3

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 7** (Refer to **Section 5.2.1**).

On the **Node Details** screen, select **Gateway (SIPGw)**. Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 21**. The **SIP domain name** and **Local SIP port** should be matched in the configuration of Avaya SBCE in **Section 6.2.5**, **6.2.7**, and **6.2.9**.

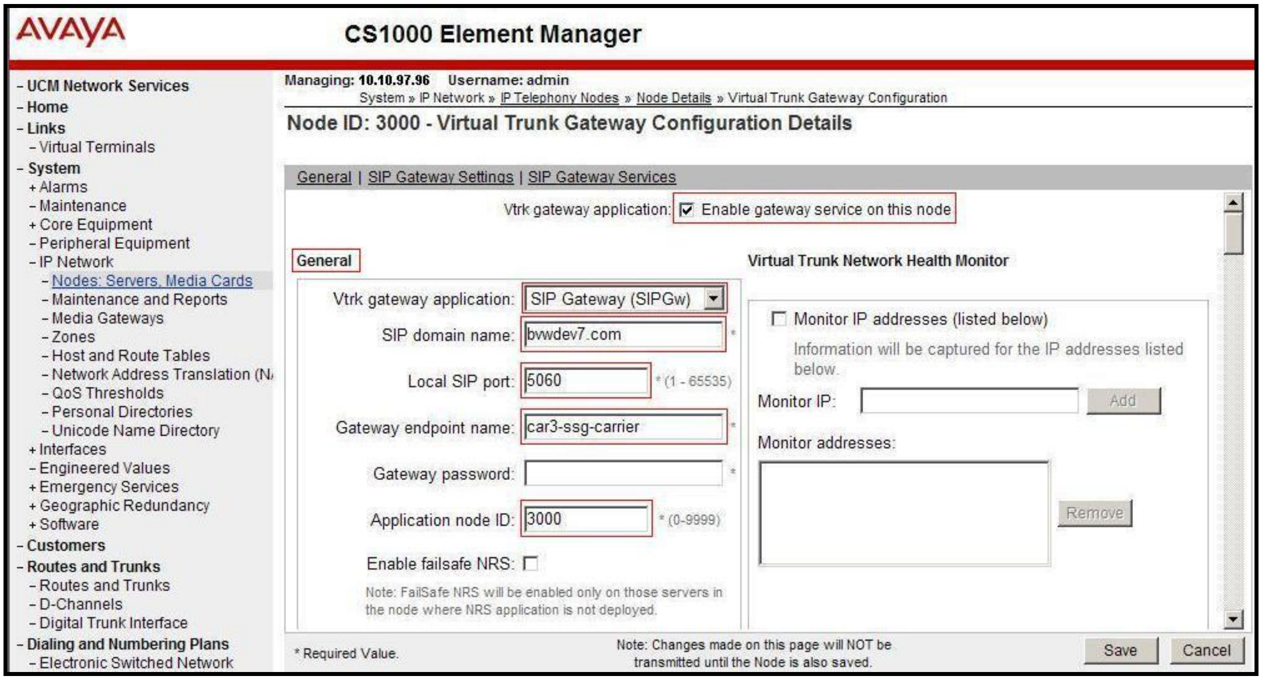

Figure 21 – Virtual Trunk Gateway Configuration Details

Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields and retain the default values for the remaining fields, as shown in **Figure 22**. Enter the internal IP address of Avaya SBCE in the **Primary TLAN IP address** field. Enter **5060** for **Port** and select **UDP** for **Transport protocol**. Uncheck the **Support registration** checkbox.

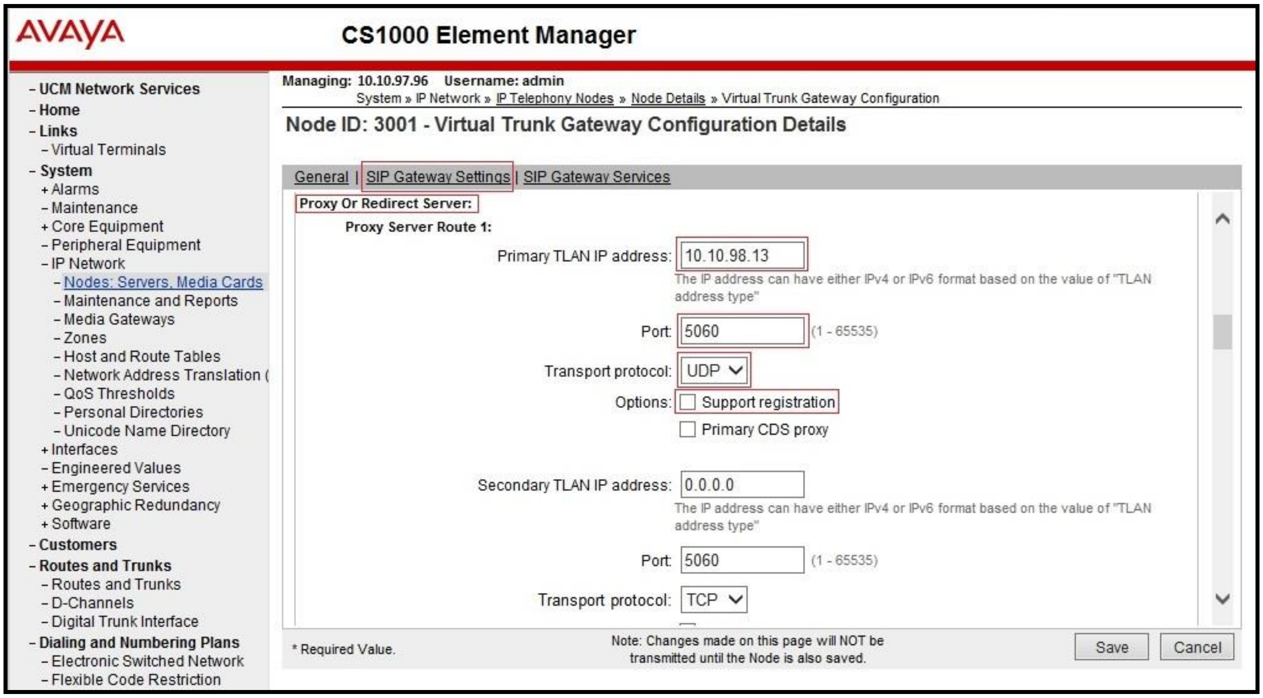

Figure 22 – Virtual Trunk Gateway Configuration Details

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

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

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

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

The remaining fields can be left at their default values as shown in **Figure 23**. Click on the **Save** button.

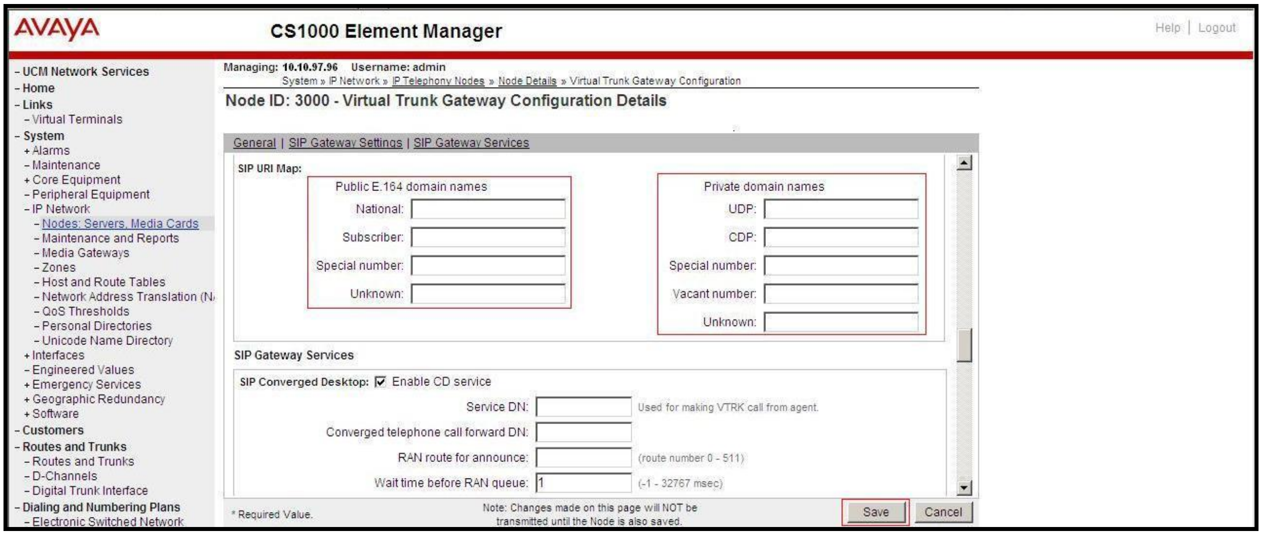

Figure 23 – Virtual Trunk Gateway Configuration Details

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

5.5.3. Administer Virtual D-Channel

Select **Routes and Trunks → D-Channels** (not shown) from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list and type **DCH** as shown in **Figure 24**. Click on the **to Add** button.

Figure 24 – D-Channels

The **D-Channels 100 Property Configuration** screen is displayed next, as shown in **Figure 25**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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

Click on **Advanced options (ADVOPT)**. Check on the **Network Attendant Service Allowed** checkbox as shown in **Figure 25**. Other fields are left as default.

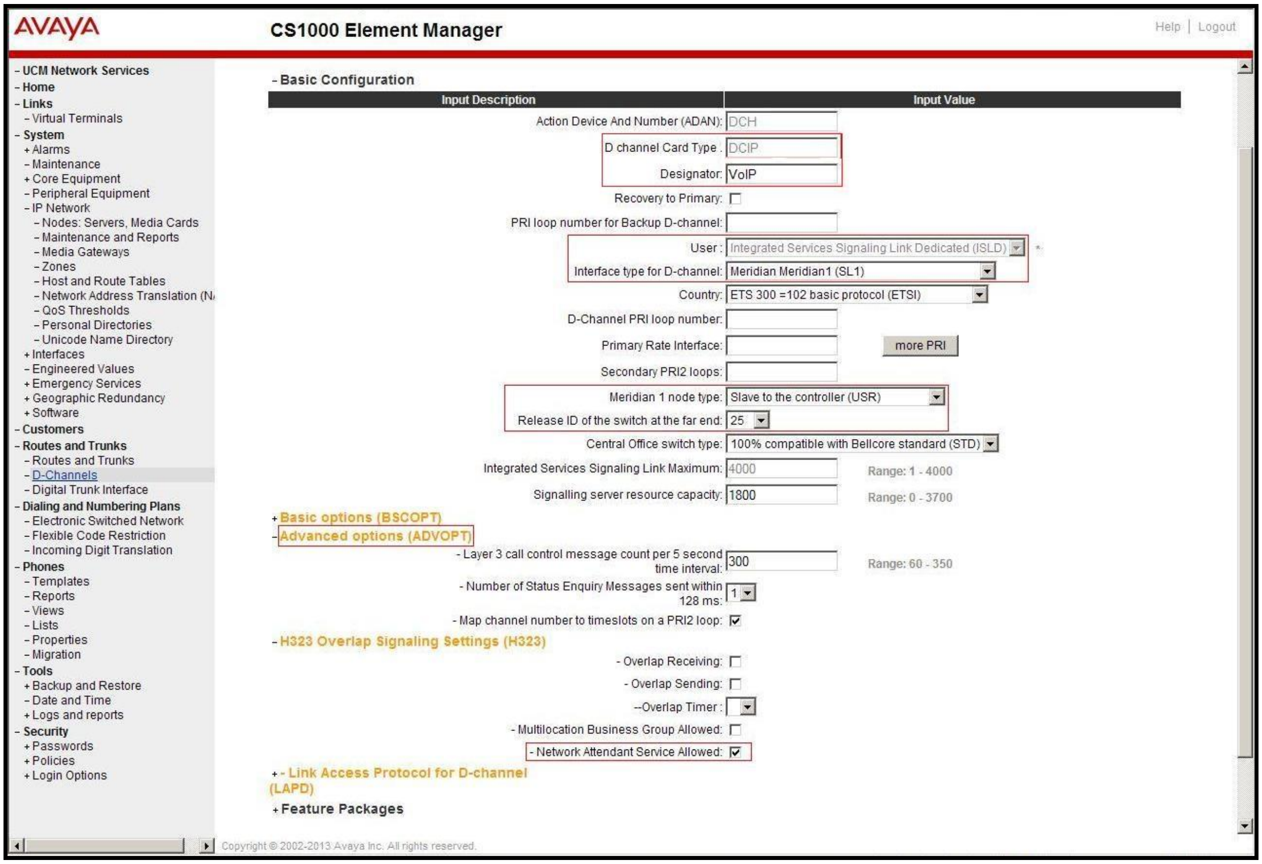

Figure 25 – D-Channel Configuration

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

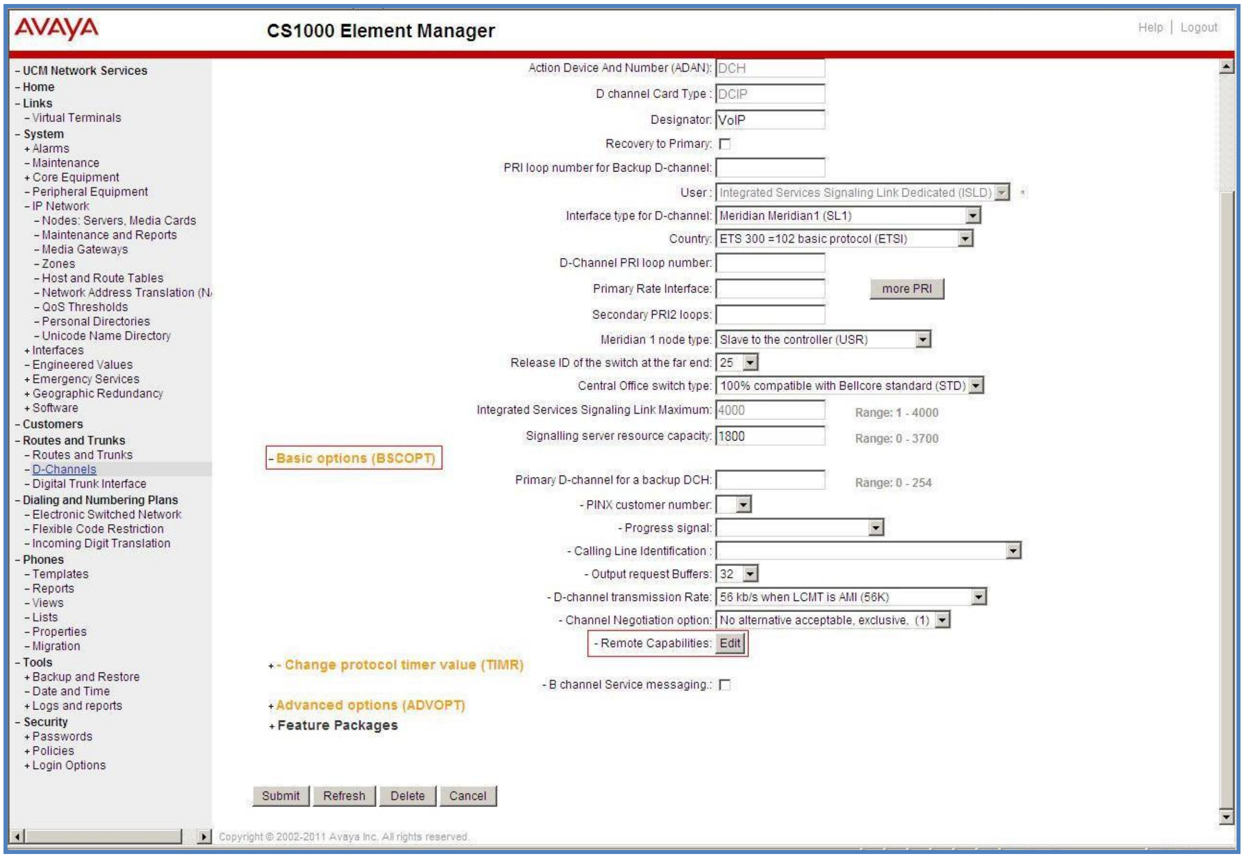

Figure 26 – D-Channel Configuration

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

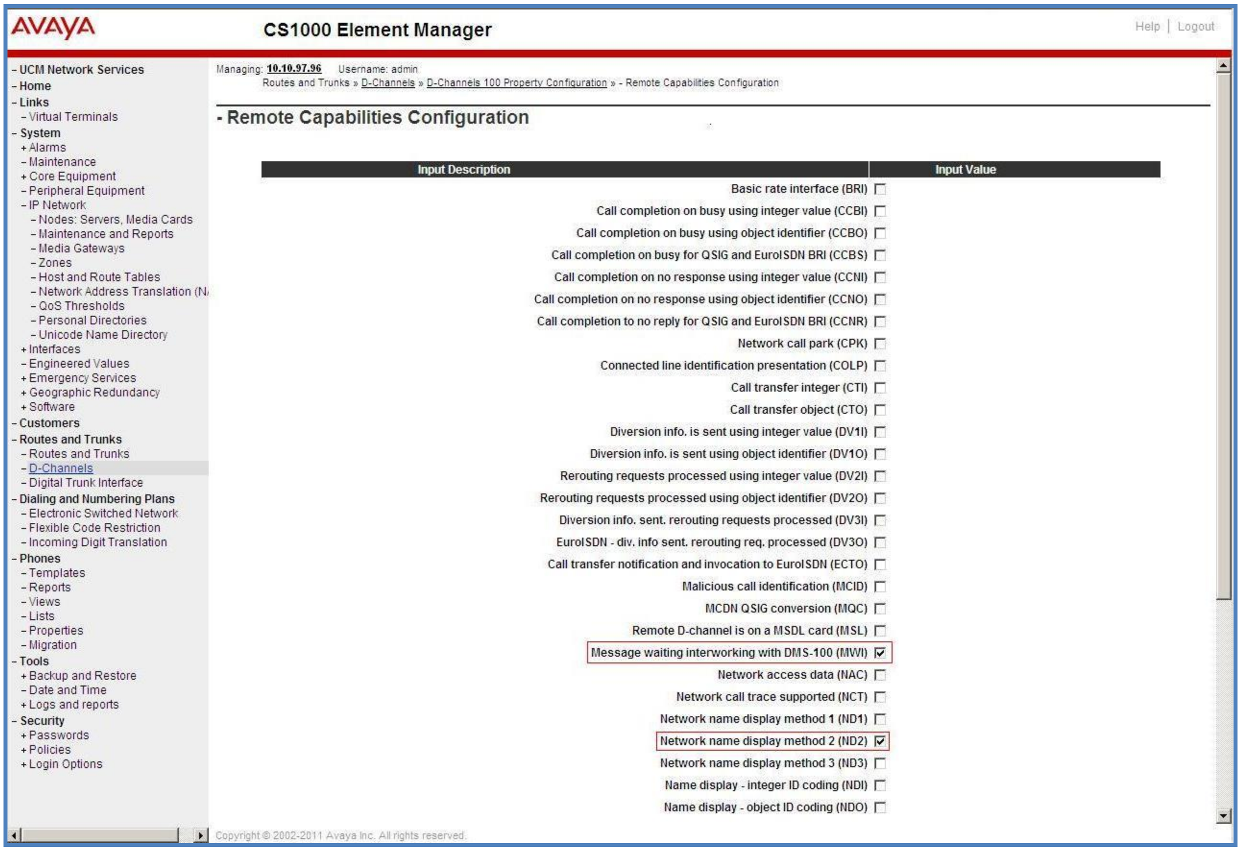

Figure 27 – Remote Capabilities Configuration

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

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

5.5.4. Administer Virtual Super-Loop

Select **System → Core Equipment → Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click the **Add** button to create a new one as shown in **Figure 28**. In this example, Superloop 4, 96, 100, and 124 have been added and are being used.

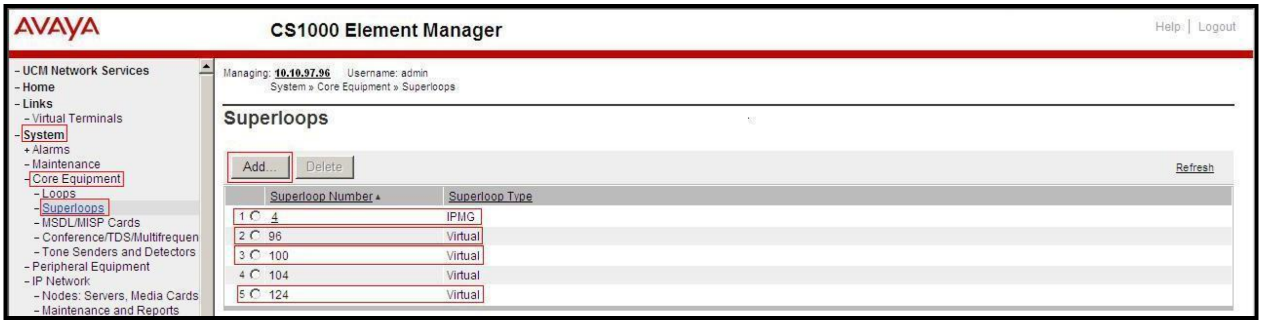

Figure 28 – Administer Virtual Super-Loop Page

5.5.5. Administer Virtual SIP Routes

Select **Routes and Trunks → Routes and Trunks** (not shown) from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown in **Figure 29**.

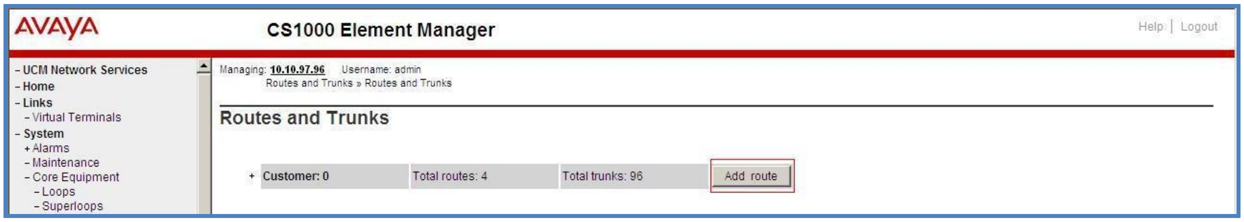

Figure 29 – Add route

The **Customer 0, New Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed. Enter the following values for the specific fields, and retain the default values for the remaining fields. The screenshot of Basic Configuration section of existing route 100 is displayed to edit as shown in **Figures 30**.

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

- Check the **The route is for a virtual trunk route (VTRK)** field, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter **255** (created in **Section 5.4.2**). **Note:** The Zone value is filled out as 255, but after it is added, the screen is displayed with prefix 00.
- For the **Node ID of signaling server of this route (NODE)** field, enter the node number **3000** (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Scrolling down to the bottom of the screen, enter the following values for the specified fields, and retain the default values for the remaining fields.
  - **Mode of operation (MODE)**: Select **Route uses ISDN Signalling Link (ISLD)**.
  - **D channel number (DCH)**: Enter **100** (created in **Section 5.5.3**).
  - **Interface type for route (IFC)**: Select **Meridian M1 (SL1)**.
  - **Private network identifier (PNI)**: Enter **1**. **Note:** The value is filled out as 1, but after it is added, the screen is displayed with prefix 0000.
  - **Network calling name allowed (NCNA)**: Check this option to allow calling name display.
  - **Network call redirection (NCRD)**: Check this option to allow call redirection.
  - **Insert ESN access code (INAC)**: Check this option to insert ESN access code (Refer to **Section 5.6.1**).

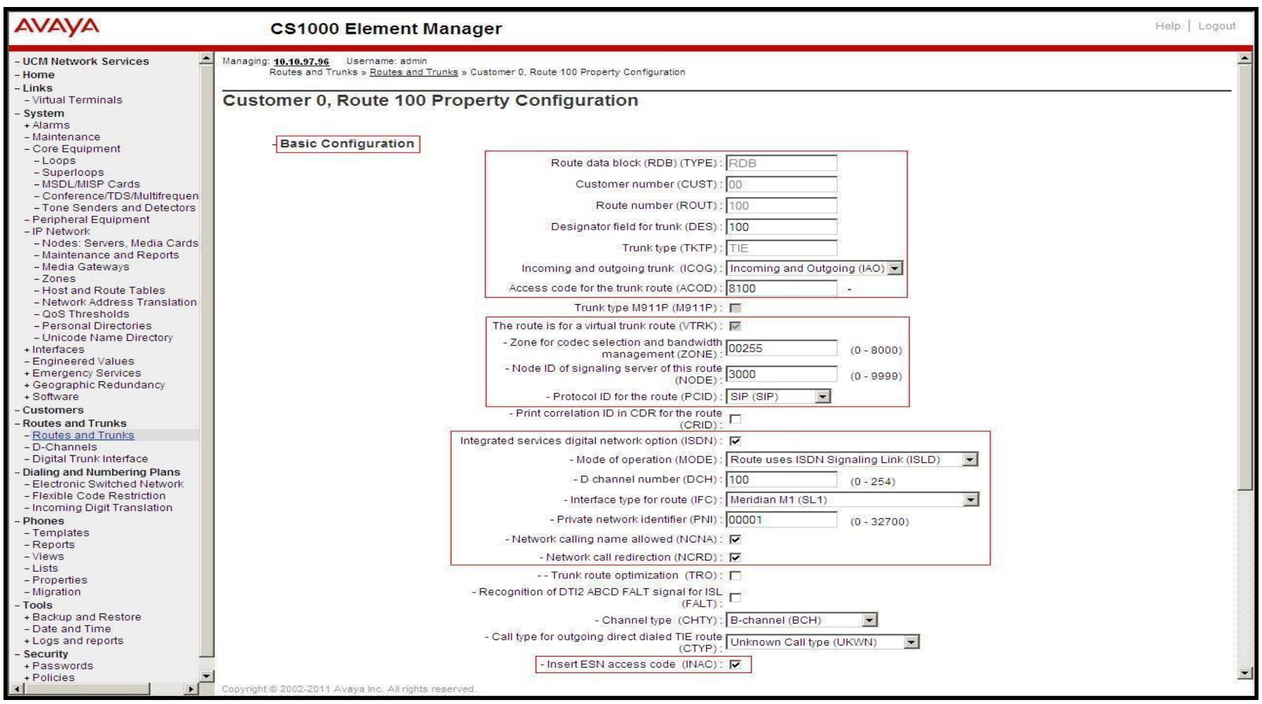

Figure 30 – Route Configuration 1

Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)** checkboxes. Enter **1** for both **Day IDC tree number** and **Night IDC tree number** as shown in **Figure 31**.
Click on the **Submit** button.

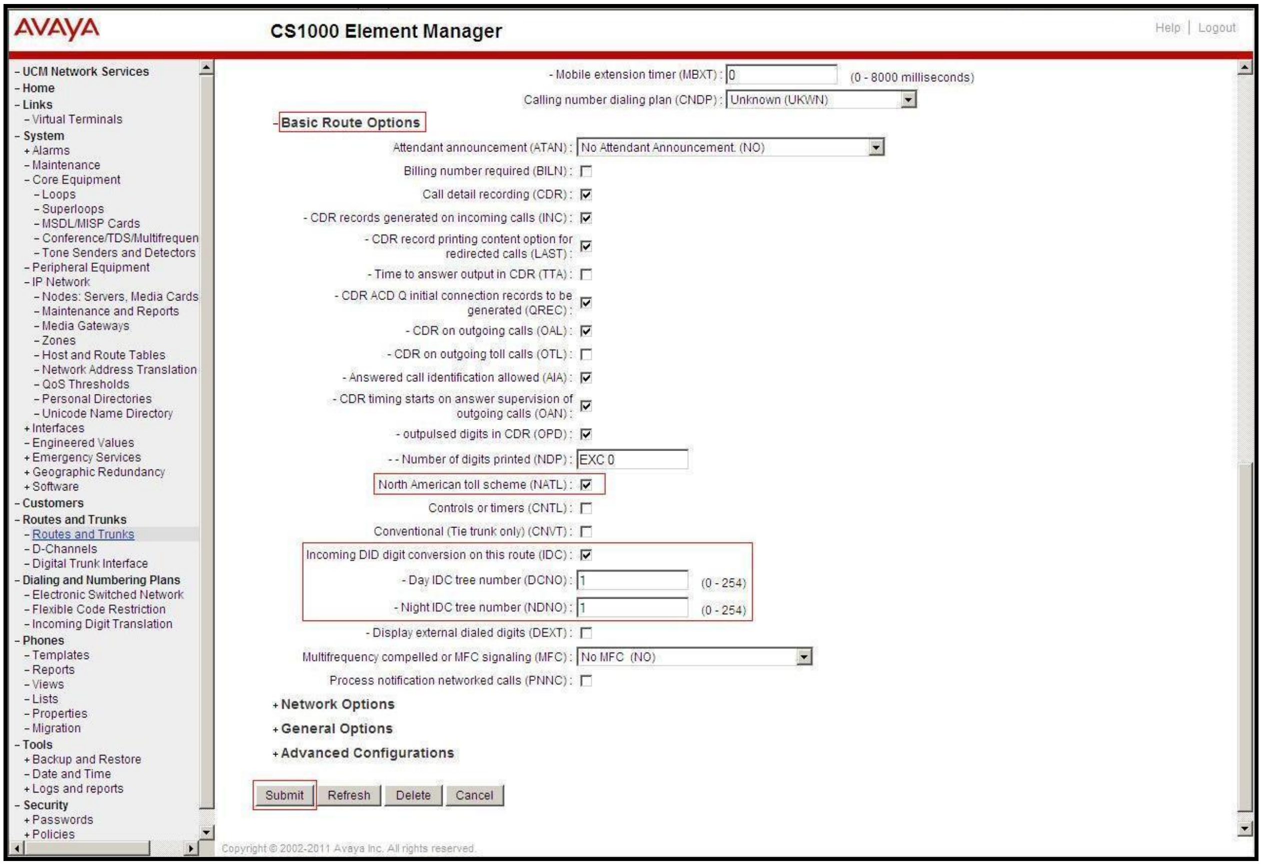

Figure 31 – Route Configuration 2

5.5.6. Administer Virtual Trunks

Select **Routes and Trunks → Route and Trunks** (not shown). The Route list is now updated with the newly added routes. In the example, the Route 100 was being added. Click on the **Add trunk** button as shown in **Figure 32**.

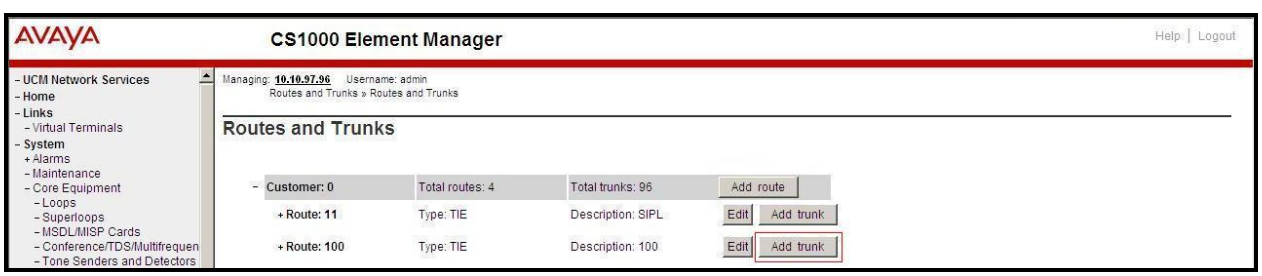

Figure 32 – Routes and Trunks

The **Customer 0, Route 100, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service** (CLS) at the bottom of the basic trunk configuration page. Click on the **Edit** button as shown in **Figure 33**.

Note: The Multiple trunk input number (MTINPUT) field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created.

- **Trunk data block**: IP Trunk (**IPTI**).
- **Terminal Number**: Available terminal number (Superloop 100 created in **Section 5.5.4**).
- **Designator field for trunk**: A descriptive text.
- **Extended Trunk**: Virtual trunk (**VTRK**).
- **Member number**: Current route number and starting member.
- **Card Density**: **8D**.
- **Start arrangement Incoming**: Select **Immediate (IMM)**.
- **Start arrangement Outgoing**: Select **Immediate (IMM)**.
- **Trunk group access restriction**: Desired trunk group access restriction level.
- **Channel ID for this trunk**: An available starting channel ID.

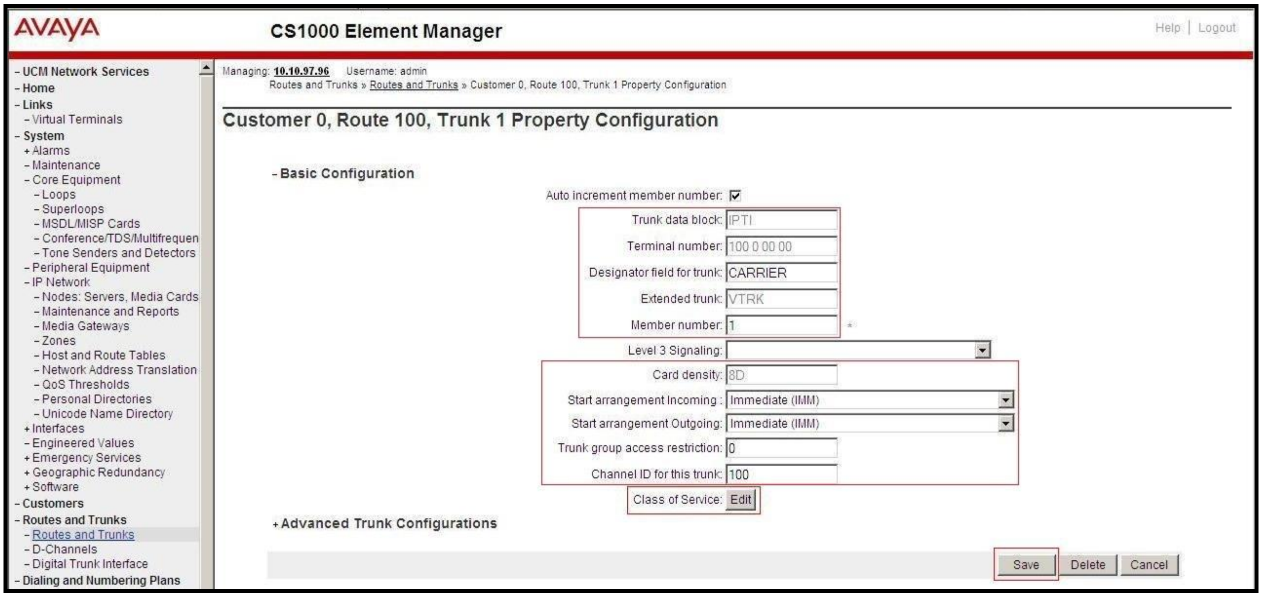

Figure 33 – New Trunk Configuration

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

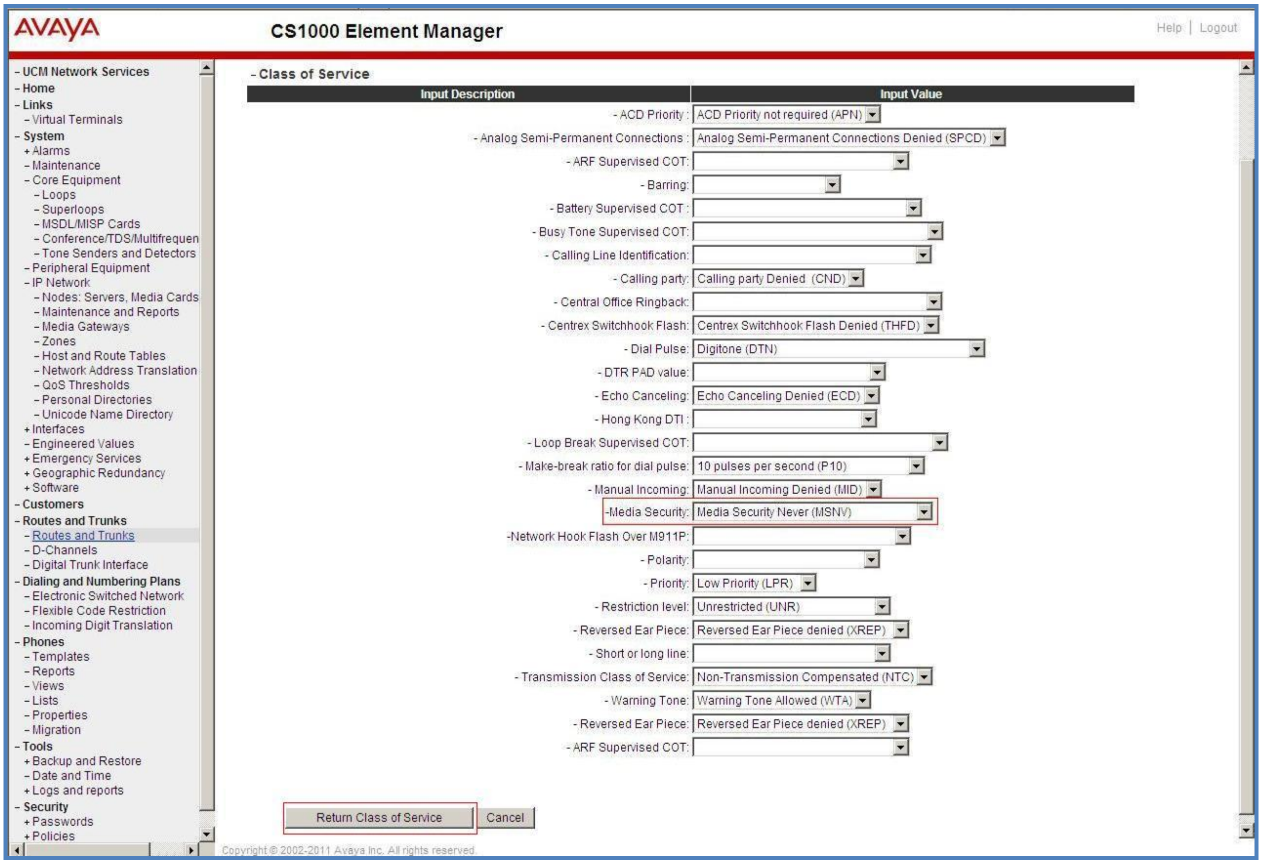

Figure 34 – Class of Service Configuration

5.5.7. Administer Calling Line Identification Entries

Select **Customers** on the left pane, then select **00 → ISDN and ESN Networking** (not shown). Click on **Calling Line Identification Entries** as shown in **Figure 35**.

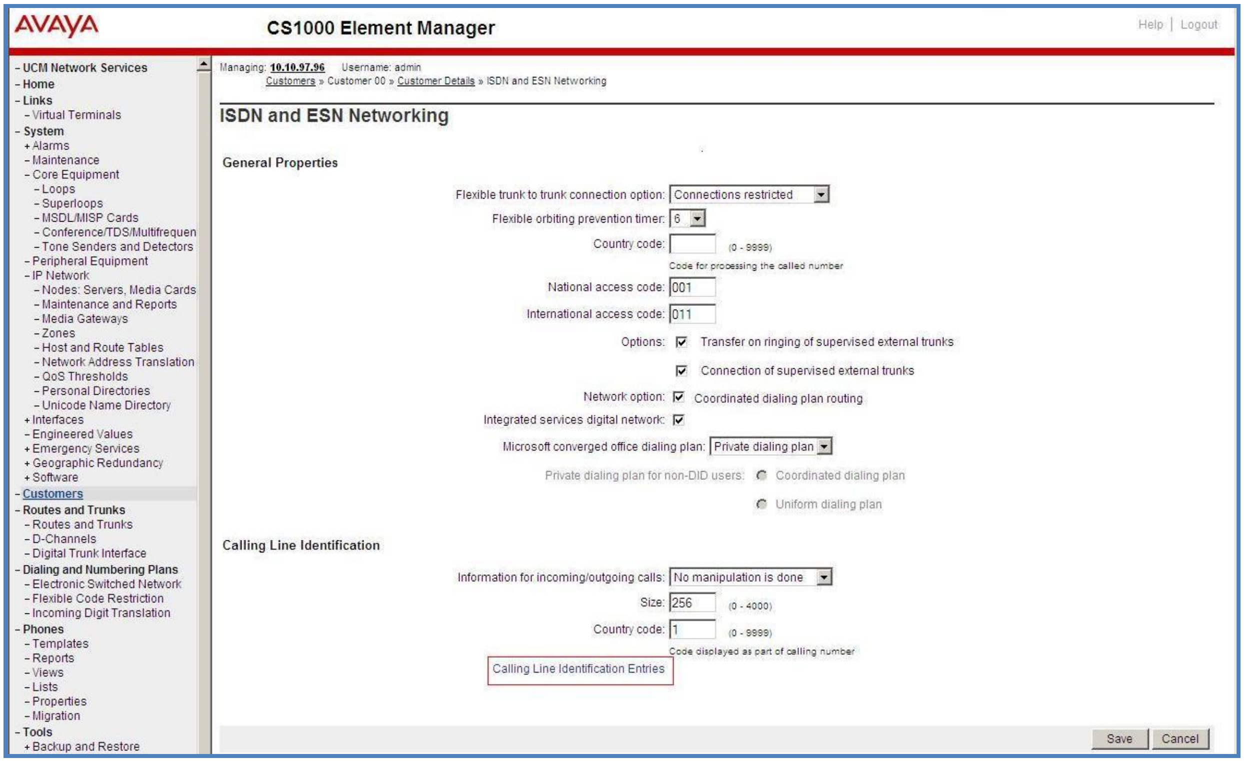

Figure 35 – ISDN and ESN Networking

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

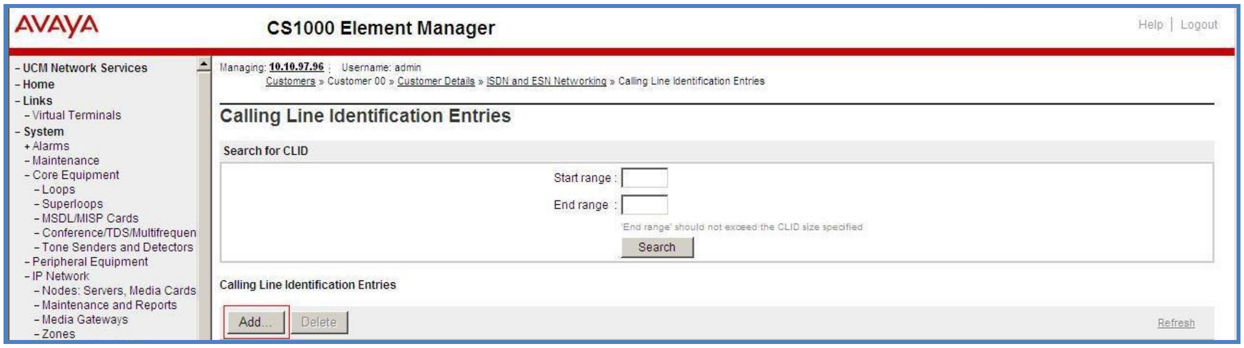

Figure 36 – Calling Line Identification Entries

The add entry **0** screen is displayed. Enter or select the following values for the specified fields and retain the default values for the remaining fields. The **Edit Calling Line Identification** of the existing entry 0 is displayed as shown in **Figure 37**.

- **National Code**: Leave it blank.
- **Local Code**: Input prefix digits assigned by MTS Allstream SIP Trunk Service, in this case 6 digits – **647XXX**. This **Local Code** will be used for call display purpose for Call Type = Unknown.
- **Home Location Code**: Input the prefix digits assigned by MTS Allstream SIP Trunk Service, in this case 6 digits – **647XXX**. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code**: Input prefix digits assigned by MTS Allstream SIP Trunk Service, in this case 6 digits – **647XXX**. 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 37**.

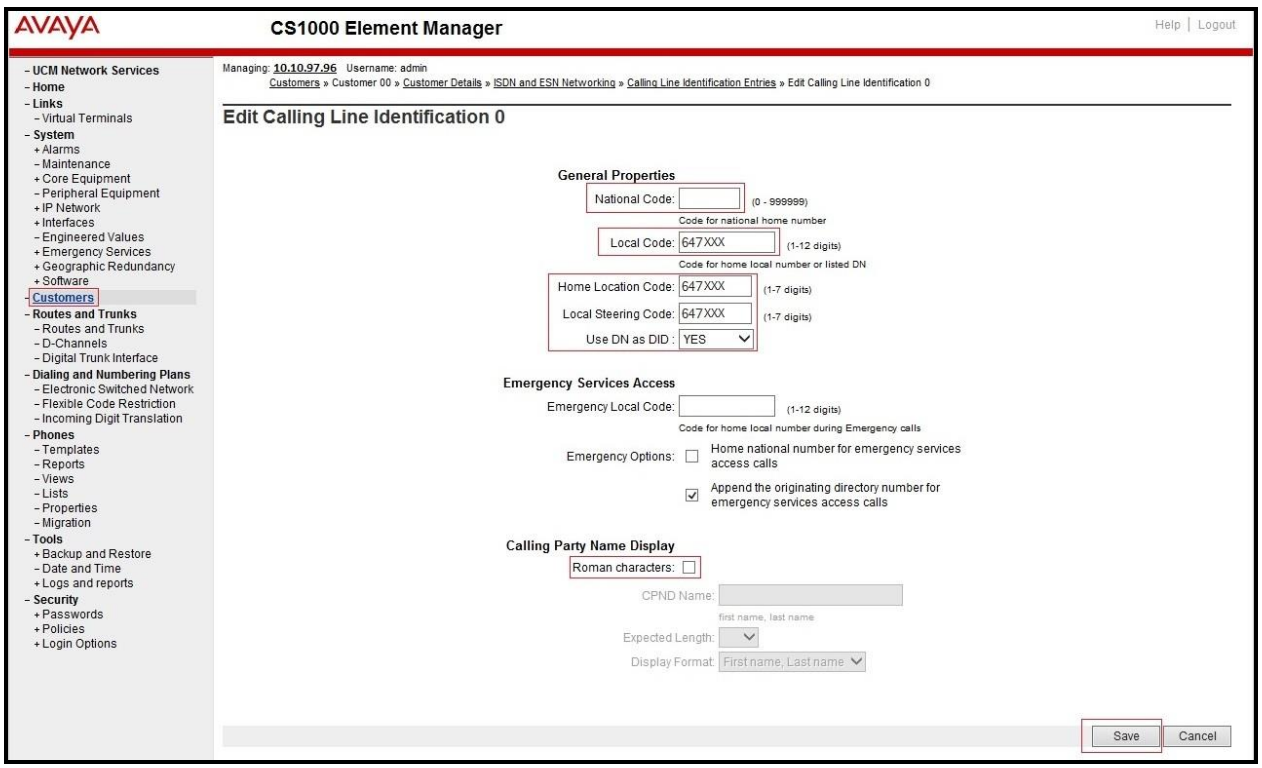

Figure 37 – Edit Calling Line Identification 0

5.5.8. Enable External Trunk to Trunk Transfer

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

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

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

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

5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen as shown in **Figure 38**.

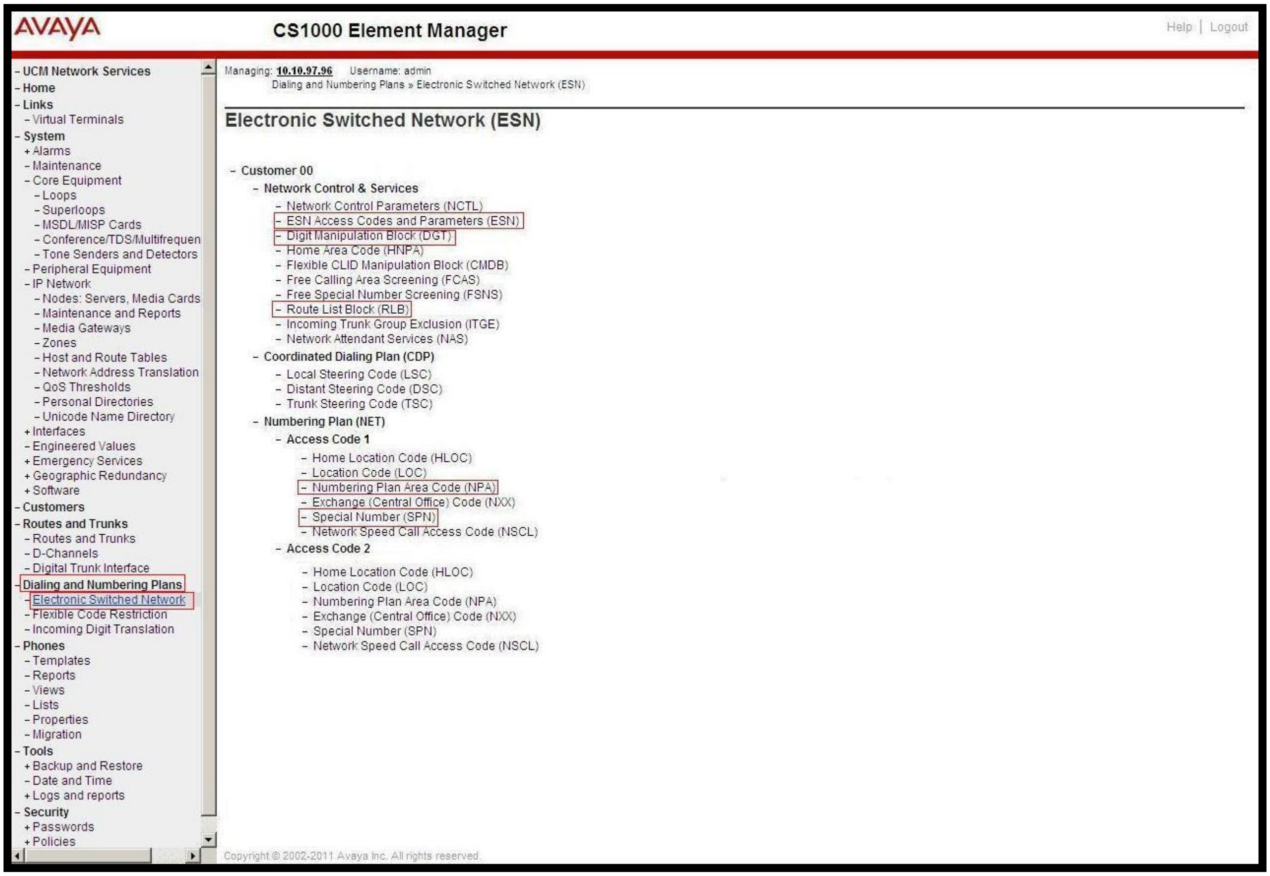

Figure 38 – ESN Configuration

On **Electronic Switched Network (ESN)** screen, select **ESN Access Codes and Parameters** to define **NARS/BARS Access Code 1** as shown in **Figure 39**.

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

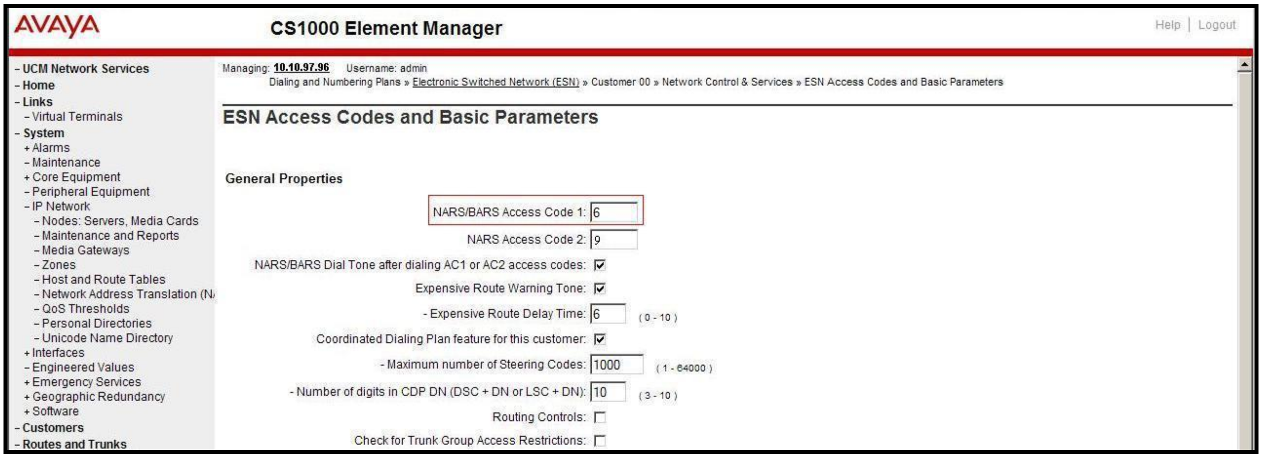

Figure 39 – ESN Access Codes and Parameters

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

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

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

TYPE NET_DATA
CUST 0
OPT
AC2 xNPA xSPN  ← Set NPA, SPN not to associate to ESN Access Code 2
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 38**. Select **Digit Manipulation Block (DGT)**. The **Digit Manipulation Block List** is displayed as shown in **Figure 40**. In the **Please choose the** field, select an available **Digit Manipulation Block Index** from the drop-down list, and click on the **to Add** button.

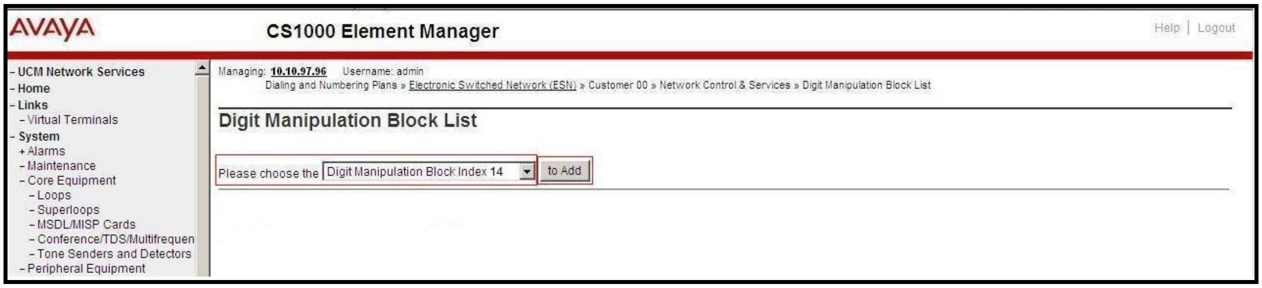

Figure 40 – Add a DMI

The DMI_14 screen will open. In this testing, no leading digits are to be deleted, therefore, enter **0** for **Number of leading digits to be deleted** and select **NPA (NPA)** for **Call Type to be used by the manipulated digits** and then click on the **Submit** button as shown in **Figure 41**.

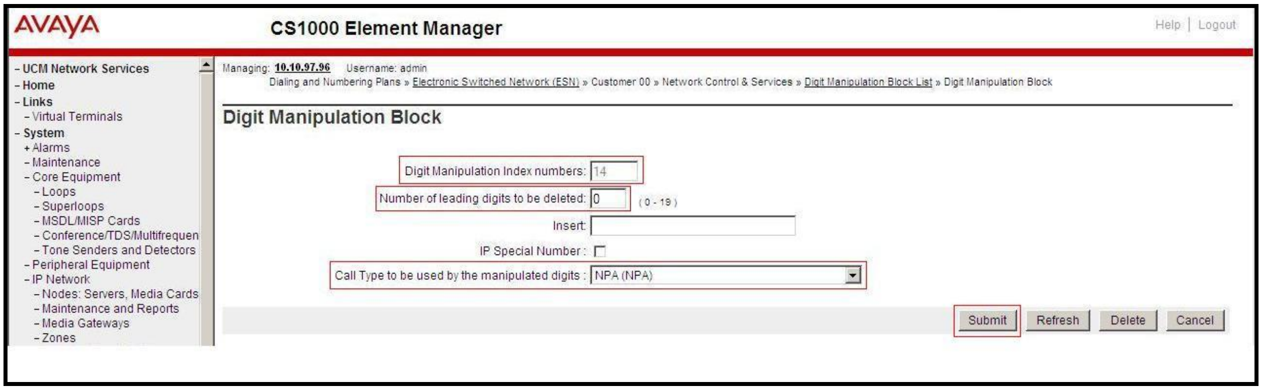

Figure 41 – DMI_14 Configuration

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 38**. 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 42**. The screen shown in **Figure 43** will open.

Figure 42 – Add a Route List Block

Enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figure 43**. Scroll down to the bottom of the screen, and click on the **Submit** button (not shown).

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

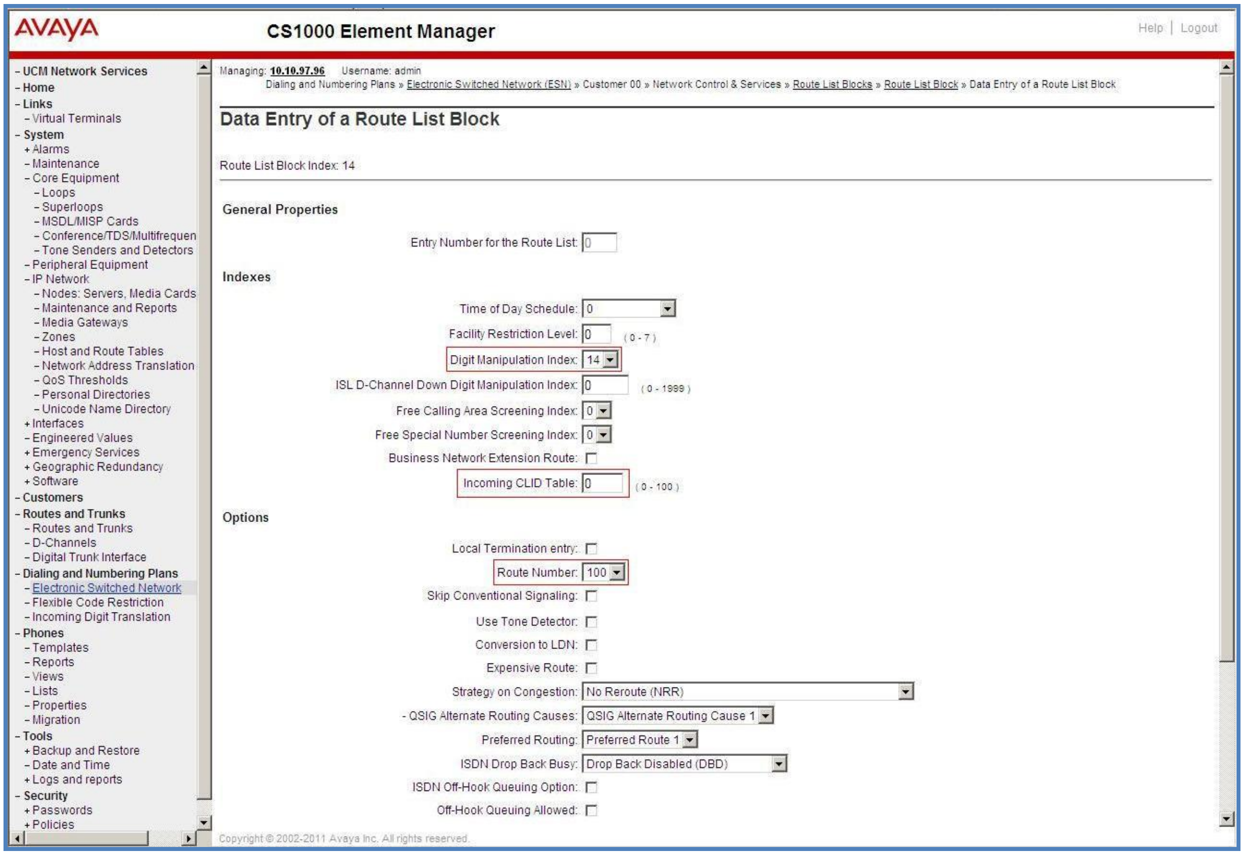

Figure 43 – RLB_14 Route List Block Configuration

5.6.5. Inbound Call – Incoming Digit Translation Configuration

This section describes the configuration steps required in order to receive calls from the PSTN via the MTS Allstream 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 44**.

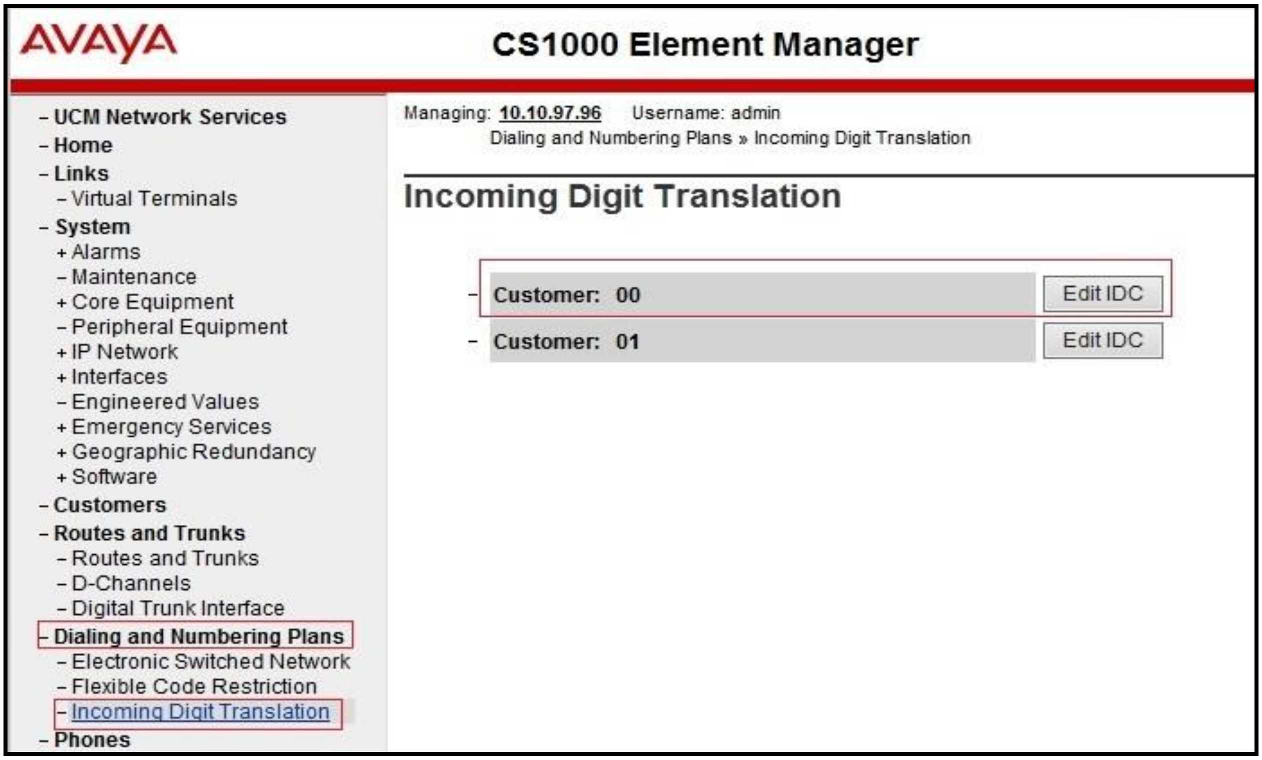

Figure 44 – Incoming Digit Translation

Click on the **New DCNO** to create the digit translation mapping. In this example, **Digit Conversion Tree Number 1** has been previously created as shown in **Figure 45**.

Figure 45 – Incoming Digit Conversion Property

Detailed configuration of the Digit Conversion Tree Configuration is shown in **Figure 46**. The **Incoming Digits** can be added to map to the Converted Digits which would be the associated CS1000 system phone DN. This **DCNO** has been assigned to route 100 as shown in **Figure 31**.

In the following configuration, the incoming call from the PSTN to DID with prefix **647XXX** will be translated to the associated DN with 4 digits. For testing purposes, DID number **647XXX1264** is translated to **1700** for voicemail testing or translated to 1264 for Mobile Service Access DN number.

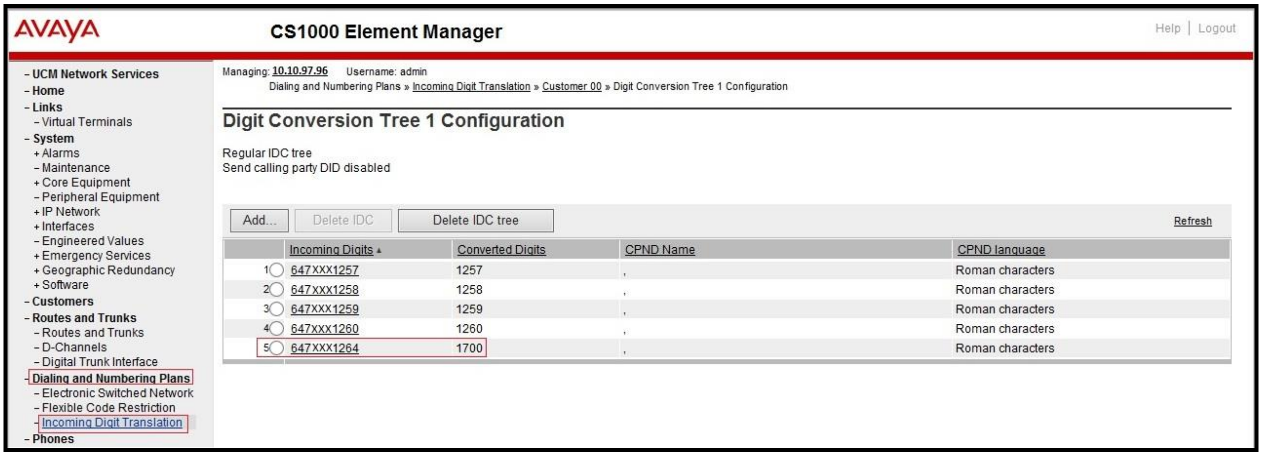

Figure 46 – Digit Conversion Tree

5.6.6. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 0, 1800, 411, 911 and so on.

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as show in **Figure 38**. Select **Special Number (SPN)**. Enter a SPN number and then click on the **to Add** button. **Figure 47** shows all the special numbers used for this testing.

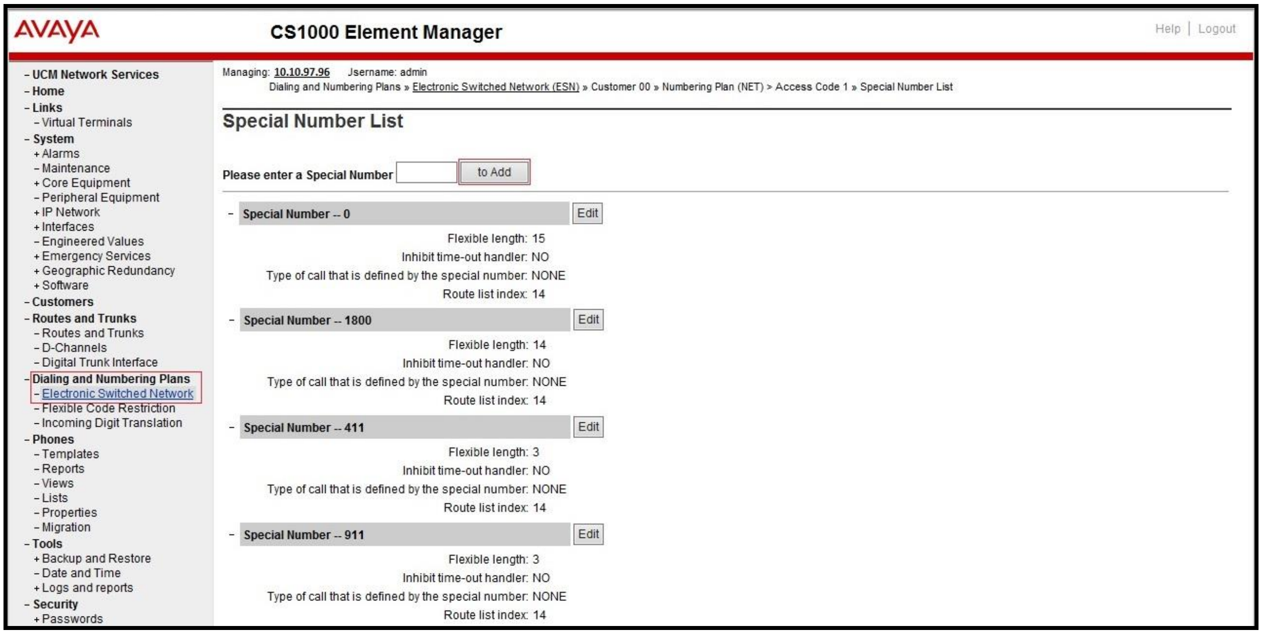

Figure 47 – SPN numbers

5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Select **Numbering Plan Area Code (NPA)** as shown in **Figure 38**. Enter the area code desired in the textbox and click on the **to Add** button. The 1416, 1613, 1647, and 647 area codes were used in this configuration as shown in **Figure 48**.

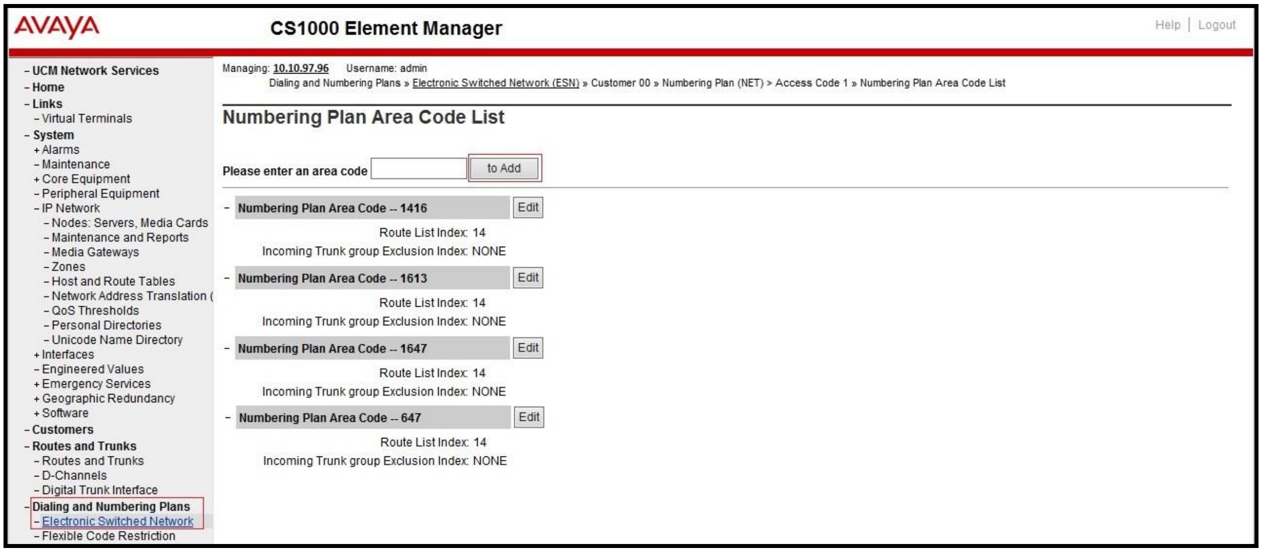

Figure 48 – Numbering Plan Area List

5.7. Administer a Phone

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

5.7.1. Phone creation

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

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

```
    UDI RCC HBTD AHD IPND  DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
    FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
    MSNV FRA  PKCH MWTD DVLD CROD ELCD
CPND_LANG ENG
HUNT
PLEV 02
PUID
UPWD
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 SCR 1257 0     MARP ← Set the position of DN 1257 to display on key 0 of the phone
       CPND
        CPND_LANG ROMAN
          NAME MTS_01 ← Set name to display
          XPLN 13
          DISPLAY_FMT FIRST,LAST
    01
<Text removed for brevity>
```

5.7.2. Enable Privacy for the Phone

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

To hide the display number, set **CLS** (Class of Service) to **DDGD**. CS1000 will include "Privacy:id" in the SIP message header before sending it to MTS Allstream SIP Trunk Service.

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

To allow the display number, set **CLS** to **DDGA**. CS1000 will not send the Privacy header to MTS Allstream SIP Trunk Service.

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

5.7.3. Enable Call Forward for Phone

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

Select **Customer → 00 → Call Redirection**. The Call Redirection page is shown in **Figure 49**.

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

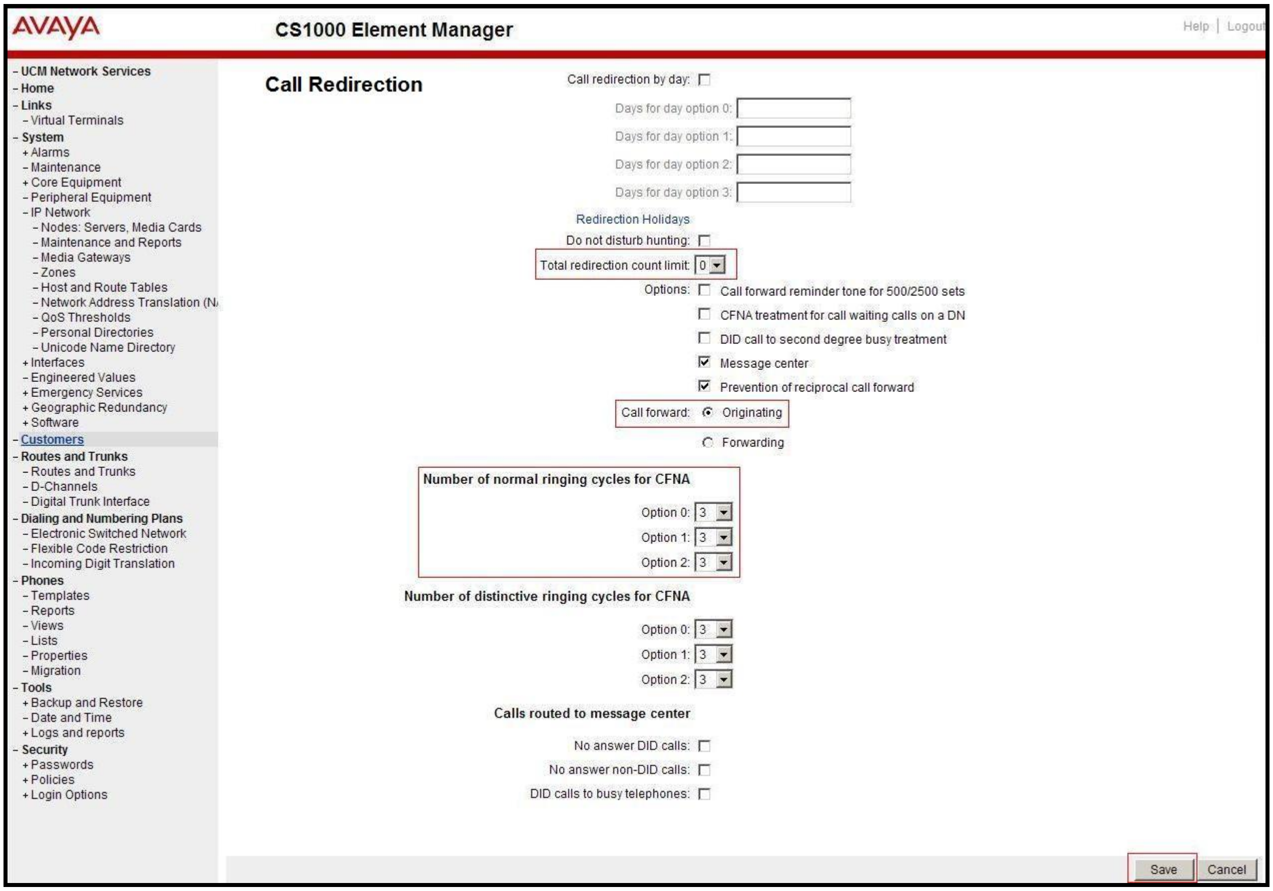

Figure 49 – Call Redirection

To enable Call Forward All Call (CFAC) feature for a phone over SIP trunk, use **ld 11**. Change its **CLS** to **CFXA**, and **SFA**, then program the forward number on the phone set. The following is the configuration of a phone that has CFAC enabled with forwarding number **61613XXX5206**.

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

ECHG yes
ITEM CLS CFXA SFA
ITEM key 19 CFW 16 61613XXX5206
```

To enable Call Forward Busy (CFB) feature for phone over SIP trunk, use **ld 11**. Change its **CLS** to **FBA**, **HTA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. The following is the configuration of a phone with CFB enabled to forwarding number **61613XXX5206**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN   96 0 0 2
ECHG yes
ITEM CLS FBA HTA SFA
ITEM HUNT 61613XXX5206
ITEM FDN 61613XXX5206
```

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 **61613XXX5206**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN   96 0 0 2
ECHG yes
ITEM CLS FNA SFA
ITEM HUNT 61613XXX5206
ITEM FDN 61613XXX5206
```

6. Configure Avaya Session Border Controller for Enterprise

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

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

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see relevant product documentation references in **Section 10** of these Application Notes.

6.1. Log 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 Avaya SBCE).

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

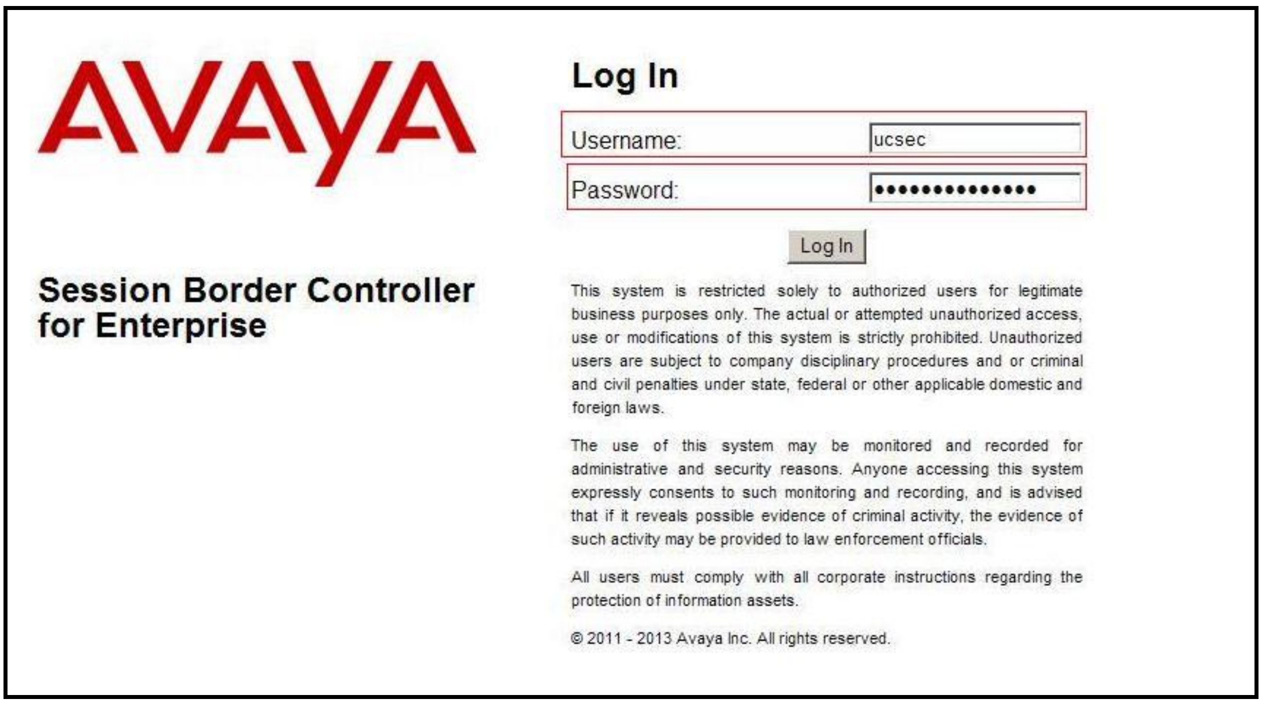

Figure 50 – Avaya SBCE Login

6.2. Global Profiles

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

6.2.1. Configure Server Interworking - Avaya Site

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

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

- Select **avaya-ru** in Interworking Profiles.
- Click **Clone**.
- Enter **Clone Name**: **CS1K76** and click **Finish** (not shown).

From the list of **Interworking Profiles**, click on **CS1K76** to edit.

- On the **General** tab, set **T.38 Support** as **Yes** (if using Fax T.38) or **No** (if using Fax G.711 pass-through). Other 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 shows that CS1000 server interworking profile (named: **CS1K76**) was added.

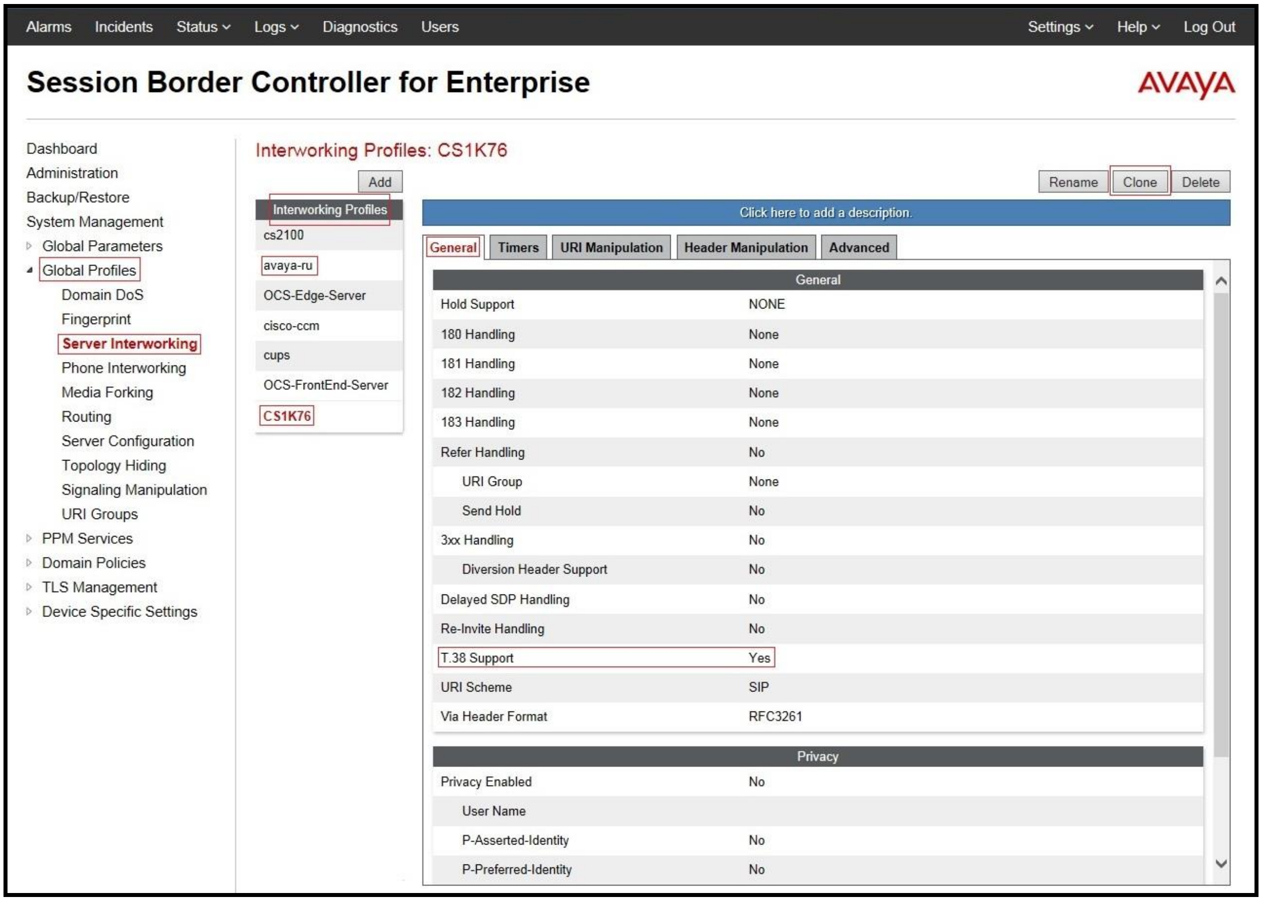

Figure 51 - Server Interworking – Avaya site

6.2.2. Configure Server Interworking – MTS Allstream Site

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

- Enter **Profile Name**: **SP4**.
- On the **General** tab, set **T.38 Support** as **Yes** (if using Fax T.38) or **No** (if using Fax G.711 pass-through). Other 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 shows that the MTS Allstream SIP Trunk Service interworking profile (named **SP4)** was added.

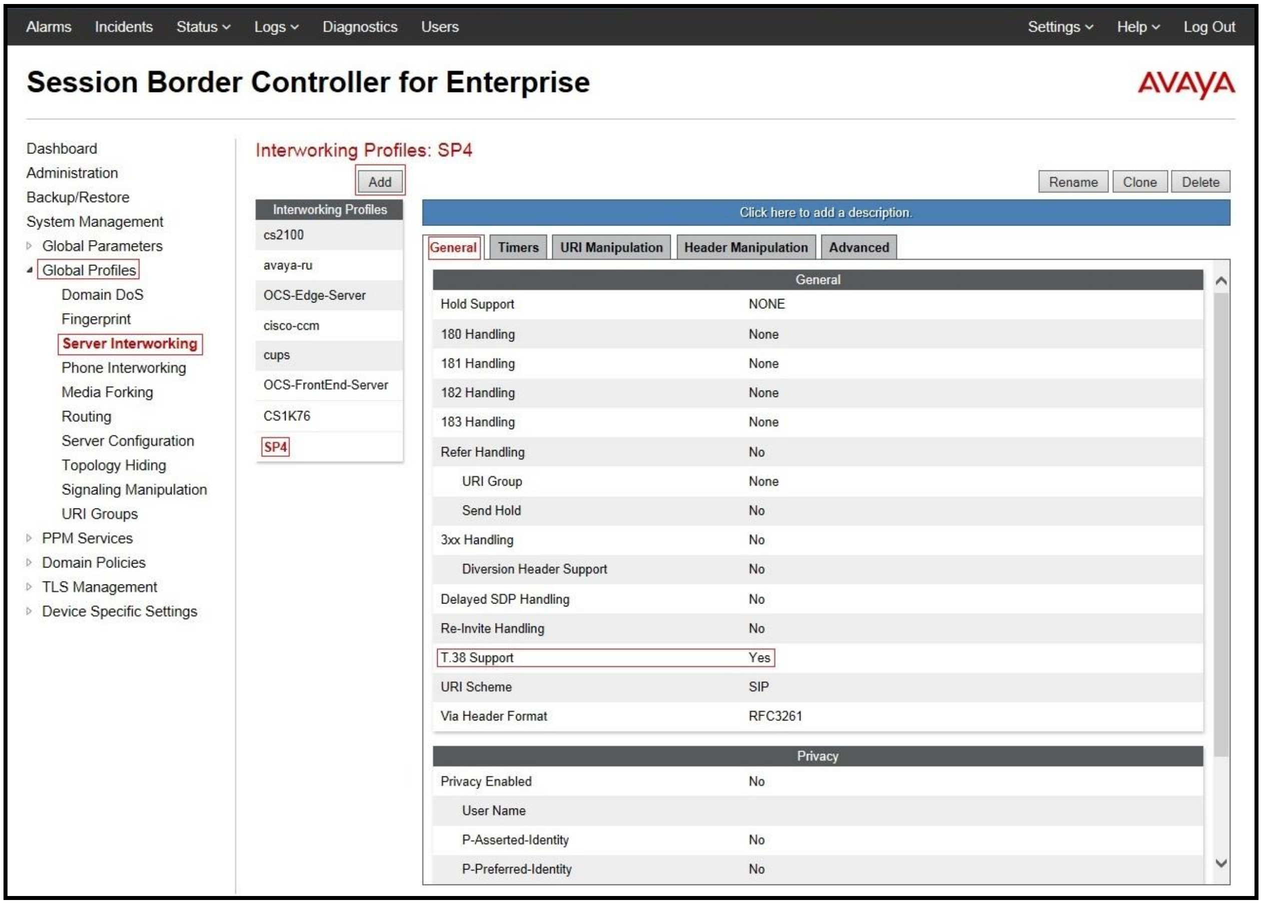

Figure 52 - Server Interworking – MTS Allstream site

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 the particular domain or group.

The following URI Group configuration is used for the compliance test in a lab environment where equipment is for shared use. The URI-Group named **SP4** was used to match the "From" and "To" headers in a SIP call dialog received from both Enterprise and MTS Allstream SIP Trunk Service. If there is a match, the Avaya SBCE will apply the appropriate Routing Profiles (see **Section 6.2.7**, **6.2.8**), and Server Flows (see **Section 6.4.4**) to route incoming and outgoing calls to the right destinations. In the production environment, there is not a requirement to define this URI Group.

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

- Enter **Group Name**: **SP4**.
- Edit the **URI Type**: **Regular Expression** (not shown).
- **Add** URI: **.*10\.10\.97\.178** (CS1000 Node IP address),**.*10\.10\.98\.111** (Avaya SBCE public interface IP address), **.*10\.10\.98\.13** (Avaya SBCE internal interface IP address), **.*192\.168\.2\.12** (MTS Allstream Signaling Server IP address), **.*192\.168\.2\.13** (MTS Allstream Media Server IP address), **.*anonymous\.invalid** (Anonymous URI), **.*bvwdev7\.com** (Enterprise domain).
- Click **Finish** (not shown).

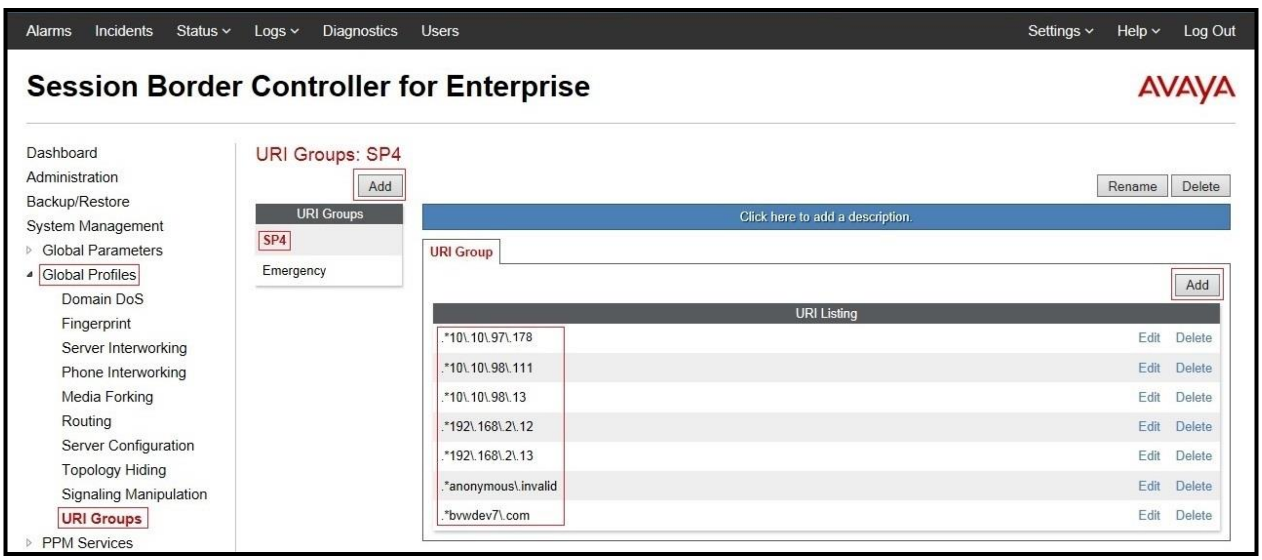

Figure 53 - URI Group

6.2.4. 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: **SP4**
  - Edit the script to replace History Info by Diversion Header for call forward off-net.
  - Click **Save** (not shown).

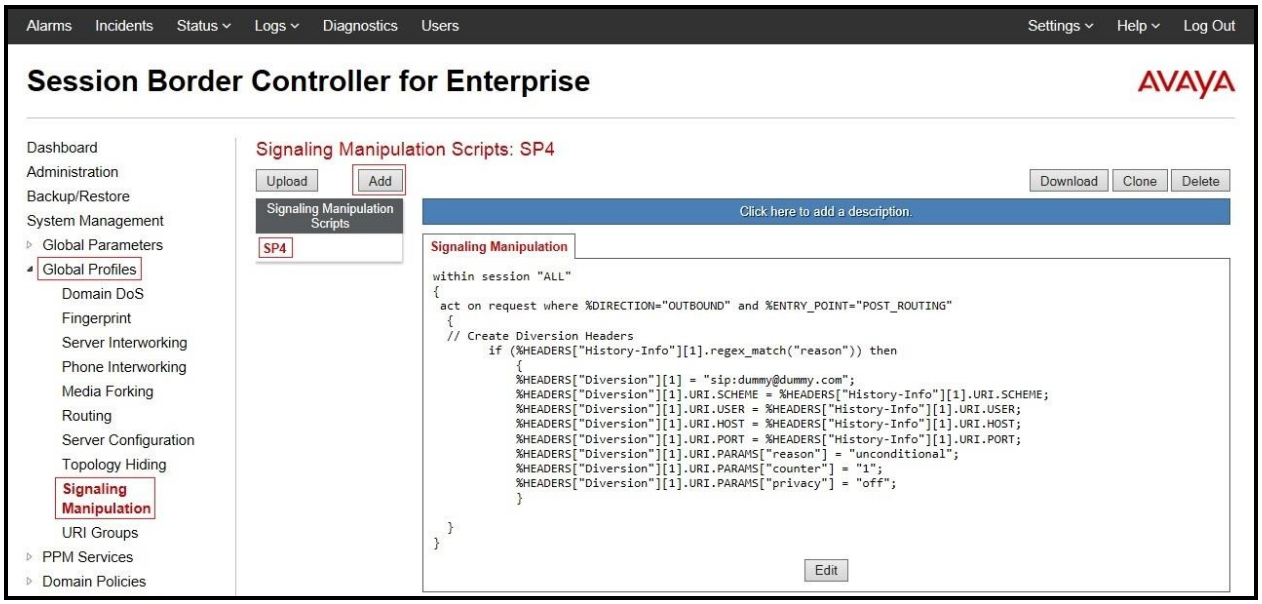

Figure 54 – Signaling Manipulation

6.2.5. 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** and click **Add** as highlighted below.

Enter **Profile Name**: **CS1K76**.

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

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

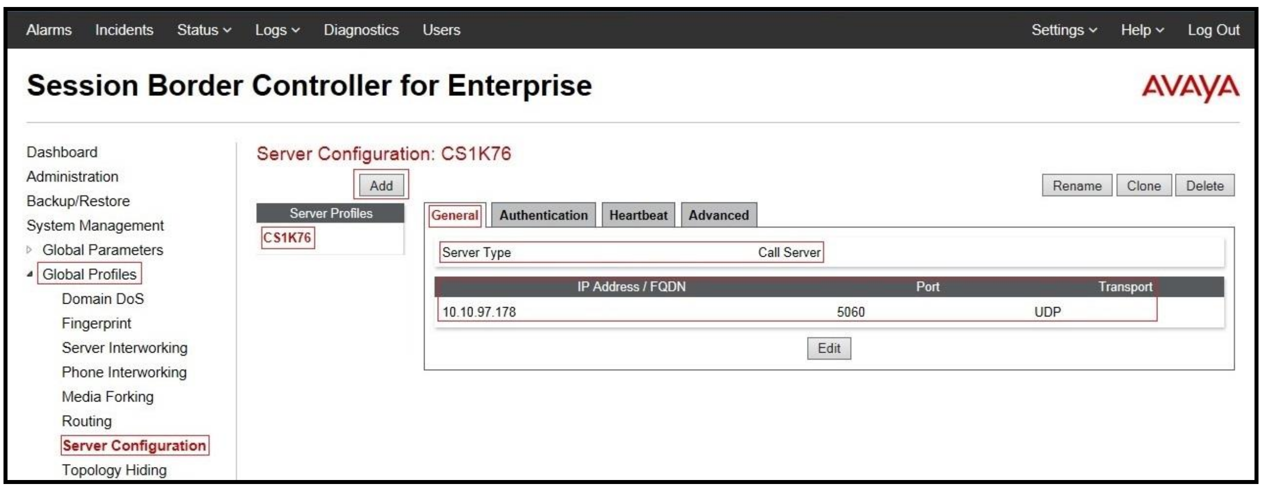

Figure 55 – CS1000 - General Server Configuration

On the **Advanced** tab:

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

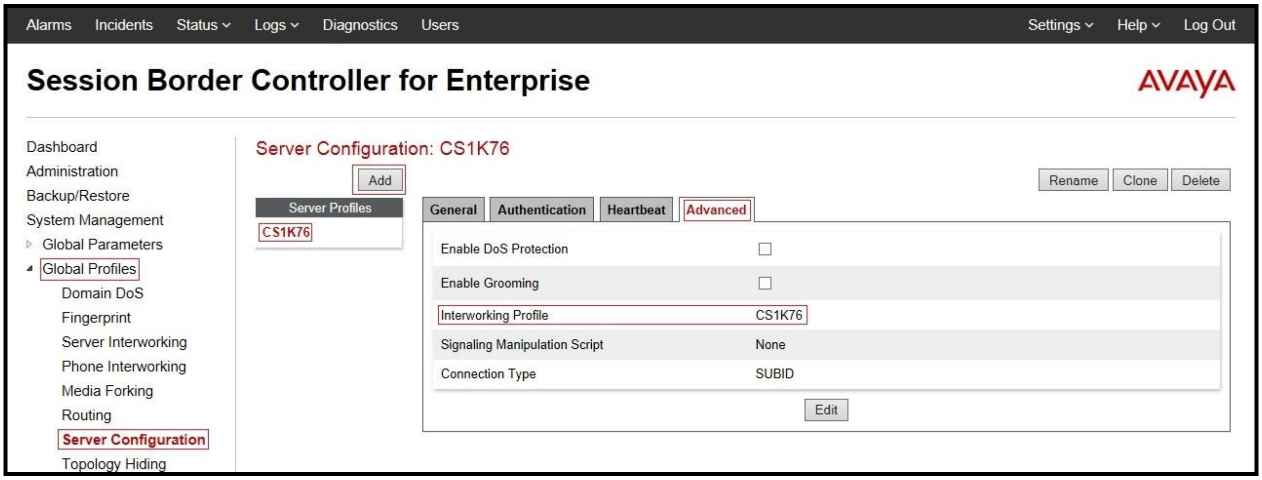

Figure 56 – CS1000 - Advanced Server Configuration

6.2.6. Configure Server – MTS Allstream

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

Enter **Profile Name**: **SP4**.

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

- **Server Type**: Select **Trunk Server**.
- **IP Address/FQDN**: **192.168.2.12** (MTS Allstream Signaling Server IP Address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).

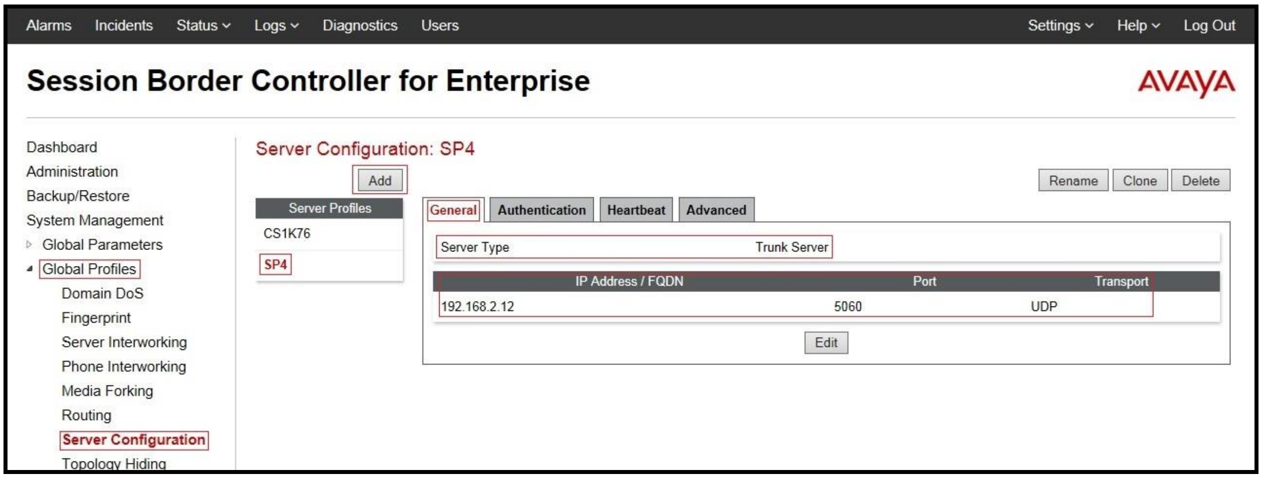

Figure 57 – MTS Allstream - General Server Configuration

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

- **Interworking Profile**: Select **SP4** (Refer to **Section 6.2.2**).
- **Signaling Manipulation Script**: Select **SP4** (Refer to **Section 6.2.4**).
- Click **Finish** (not shown).

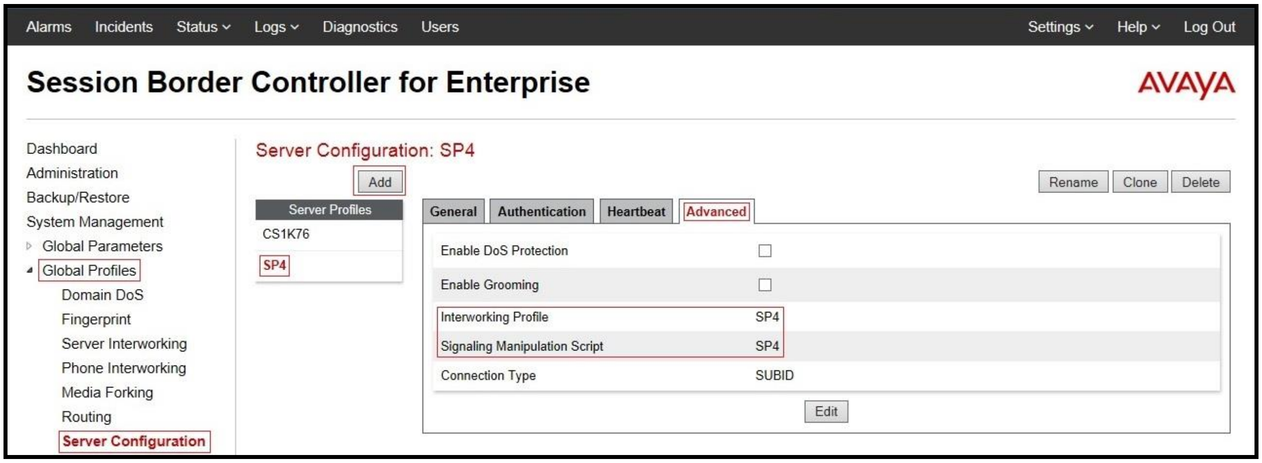

Figure 58 - MTS Allstream - Advanced Server Configuration

6.2.7. 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** and click **Add** as highlighted below.

Enter **Profile Name**: **SP4_To_CS1K76** (not shown).

- **URI Group**: **SP4** (Refer to **Section 6.2.3**).
- **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**.
- **Server Configuration**: **CS1K76** (Refer to **Section 6.2.5**).
- **Next Hop Address**: **10.10.97.178:5060 (UDP)** (CS1000 Node IP address).
- Click **Finish**.

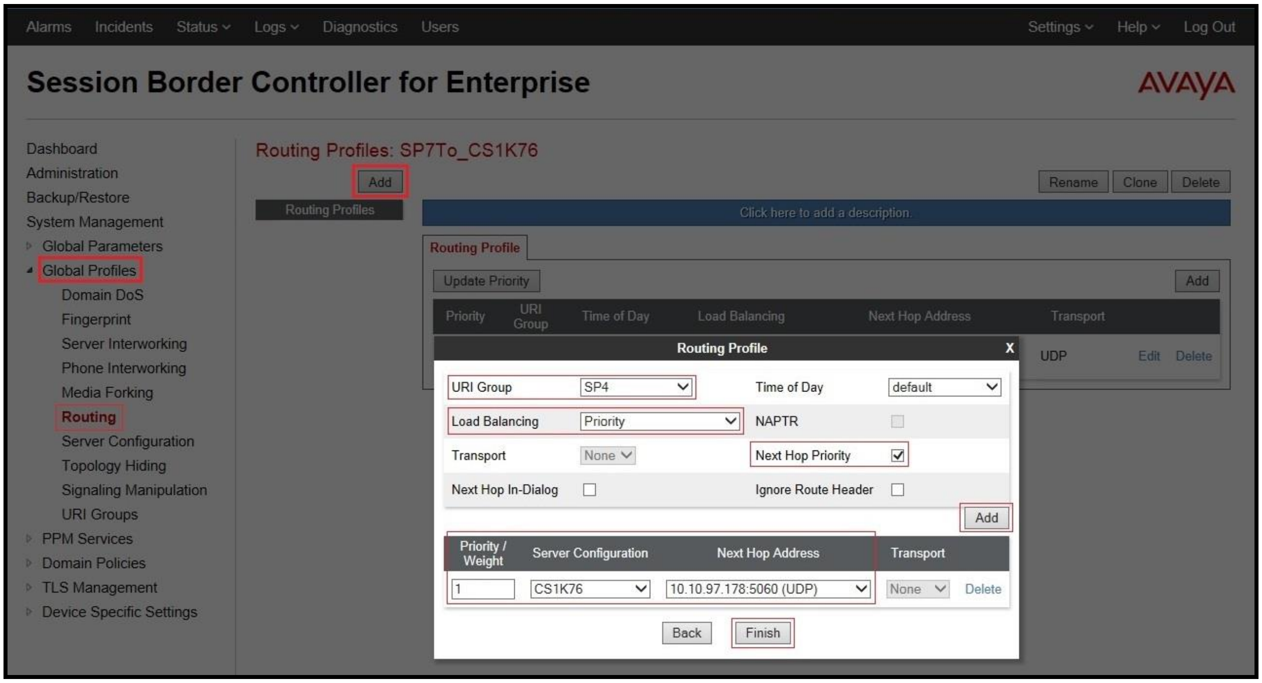

Figure 59 - Routing to Avaya

6.2.8. Configure Routing – MTS Allstream 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** and click **Add** as highlighted below.

Enter **Profile Name**: **CS1K76_To_SP4** (not shown).

- **URI Group**: **SP4** (Refer to **Section 6.2.3**).
  - **Load Balancing**: **Priority**.
  - Check **Next Hop Priority**.
  - Click **Add** button to add a Next-Hop Address
  - **Priority/Weight**: **1**.
  - **Server Configuration**: **SP4** (Refer to **Section 6.2.6**).
  - **Next Hop Address**: **192.168.2.12:5060 (UDP)** (MTS Allstream Signaling Server IP address).
  - Click **Finish**.

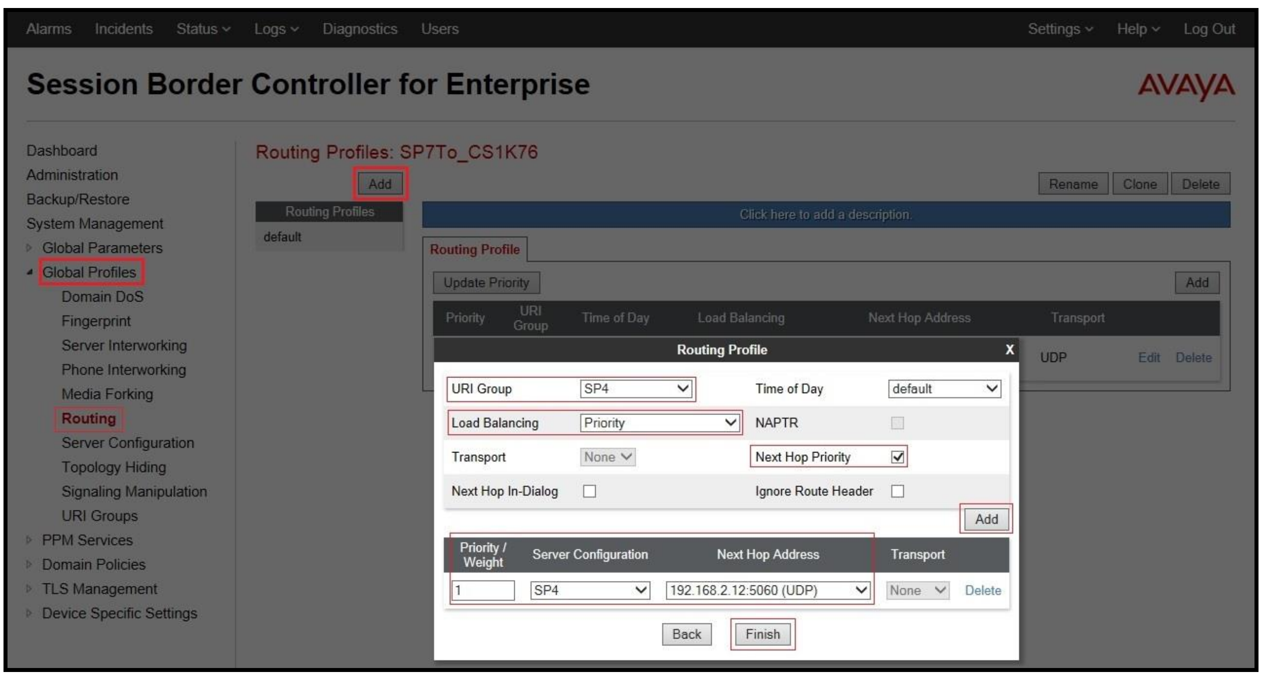

Figure 60 - Routing to MTS Allstream

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 **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name**: **SP4_To_CS1K76**. Click **Finish** (not shown).

Select **SP4_To_CS1K76** under **Topology Hiding Profiles**, and click **Edit**.

- 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**.
- 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**.
- 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**.

Click **Finish** (not shown).

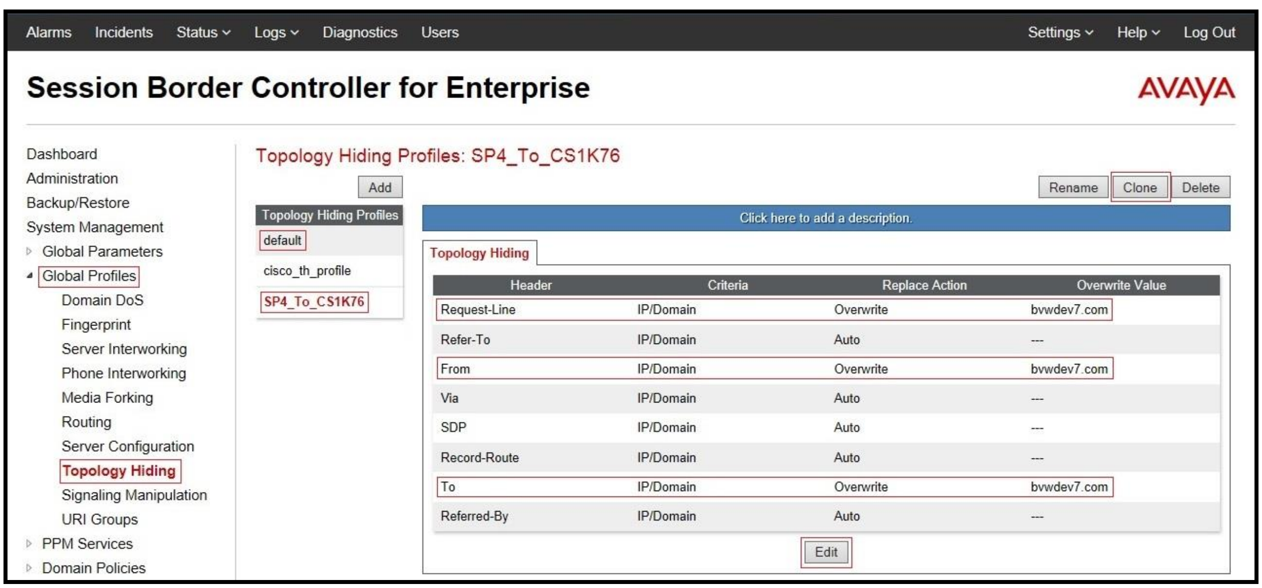

Figure 61 - Topology Hiding CS1000

6.2.10. Configure Topology Hiding – MTS Allstream Site

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

Select **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name**: **CS1K76_To_SP4**. Click **Finish** (not shown).

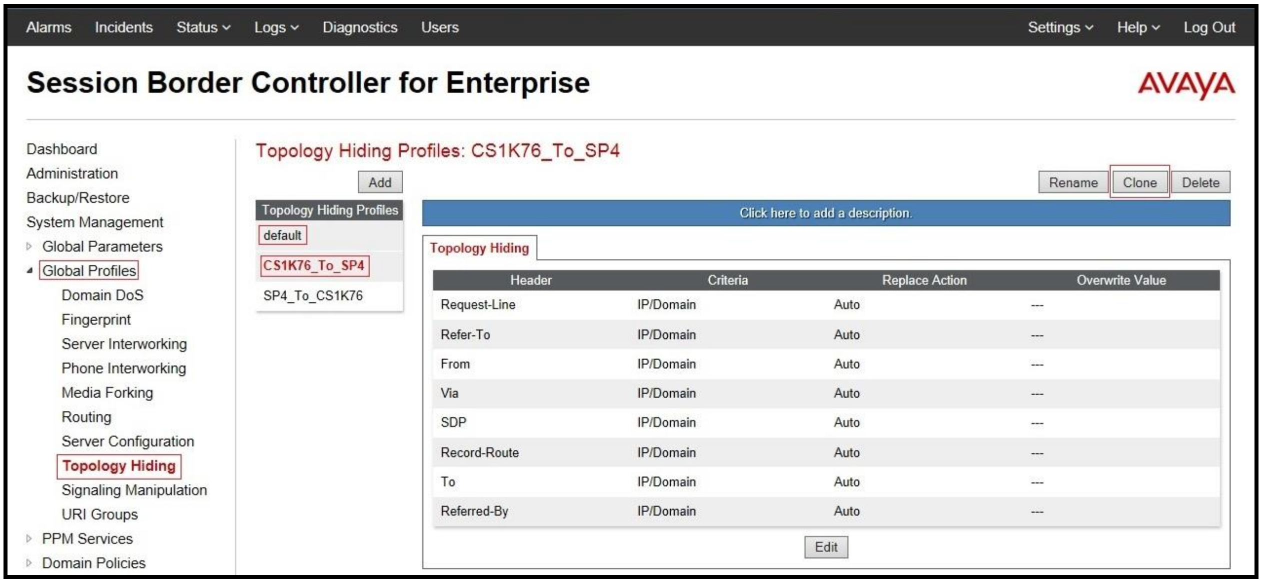

Figure 62 - Topology Hiding MTS Allstream

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 End Point 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_SP4_PolicyG**.
  - **Application Rule**: **default**.
  - **Border Rule**: **default**.
  - **Media Rule**: **default-low-med**.
  - **Security Rule**: **default-med**.
  - **Signaling Rule**: **default**.
  - **Time of Day**: **default**.
- Select **Finish** (not shown).

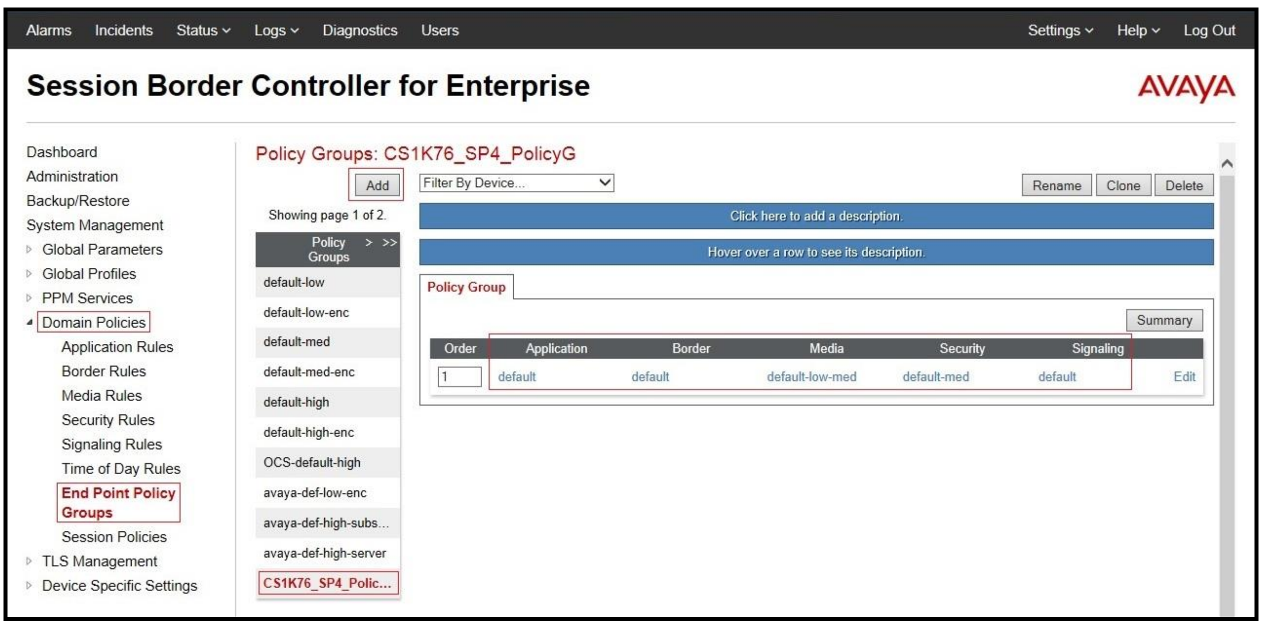

Figure 63 – CS1000 - End Point Policy Group

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

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

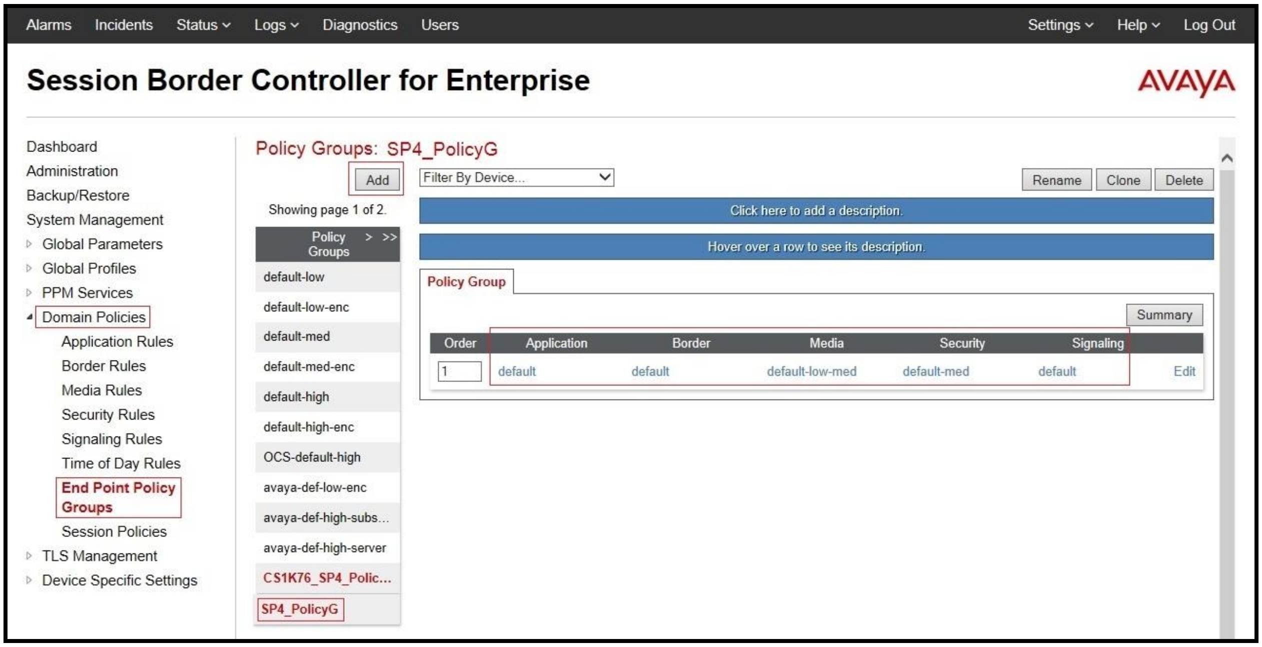

Figure 64 - MTS Allstream - End Point Policy Group

6.4. Device Specific Settings

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

6.4.1. Manage Network Settings

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

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

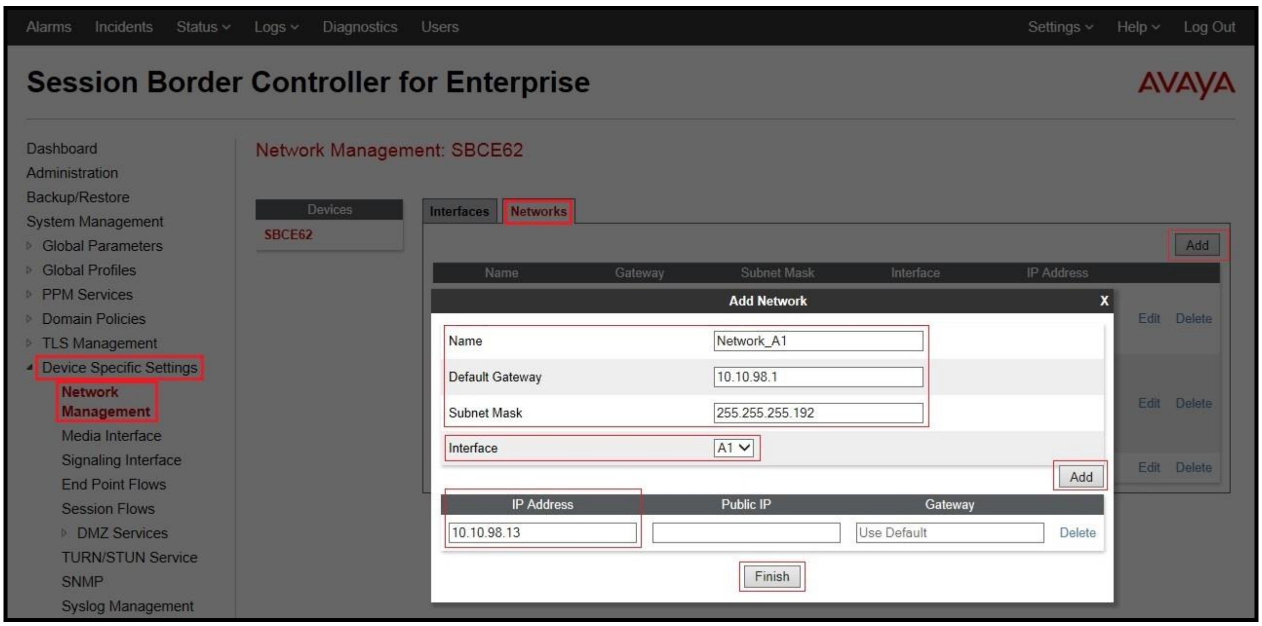

Figure 65 - Network Management – Inside Interface

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

- Select **Networks** tab and click **Add** button to add a network of outside interface as followings:
  - **Name**: **Network_B1**.
  - **Default Gateway**: **10.10.98.97**.
  - **Subnet Mask**: **255.255.255.224**.

- **Interface**: **B1** (This is Avaya SBCE outside interface).
- Click **Add** button to add **IP Address** for outside interface: **10.10.98.111**.
- Click **Finish** button to save the changes.

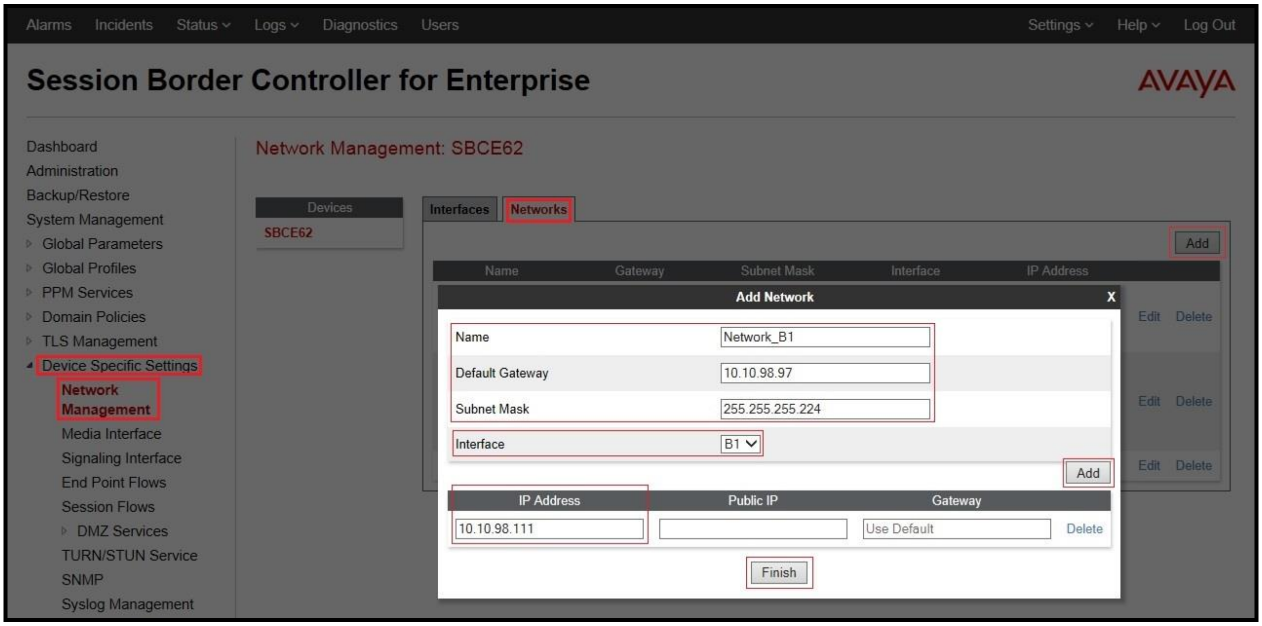

Figure 66 - Network Management – Outside Interface

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

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

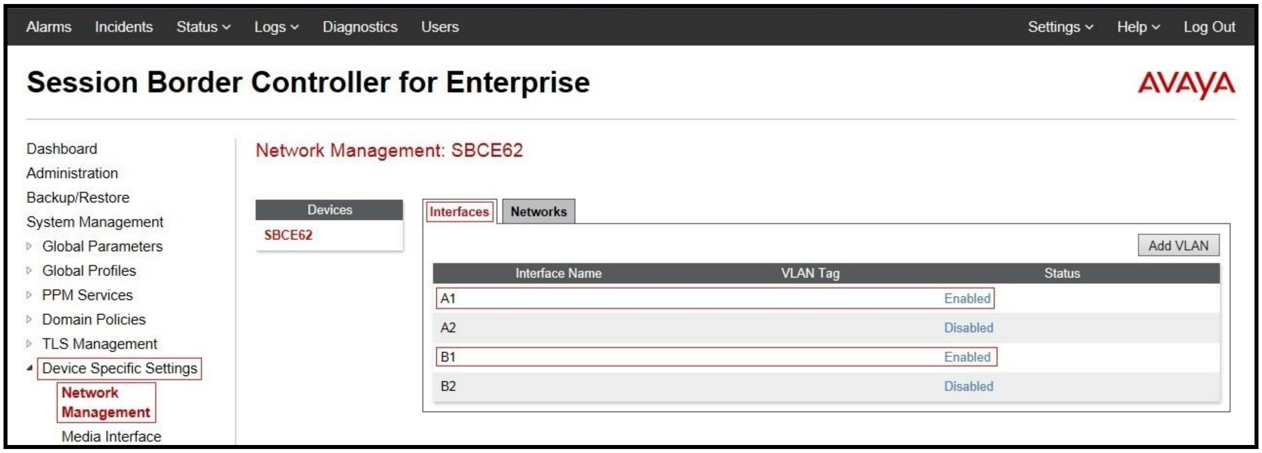

Figure 67 - Network Interfaces Status

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, select **Device Specific Settings** → **Media Interface**.

- Select **Add**.
  - **Name**: **InsideMedia1**.
  - **Media IP**: **10.10.98.13** (Avaya SBCE Internal IP Address toward CS1000).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).
- Select **Add**.
  - **Name: OutsideMedia1**.
  - **Media IP**: **10.10.98.111** (Avaya SBCE External IP Address toward MTS Allstream SIP Trunk Service).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).

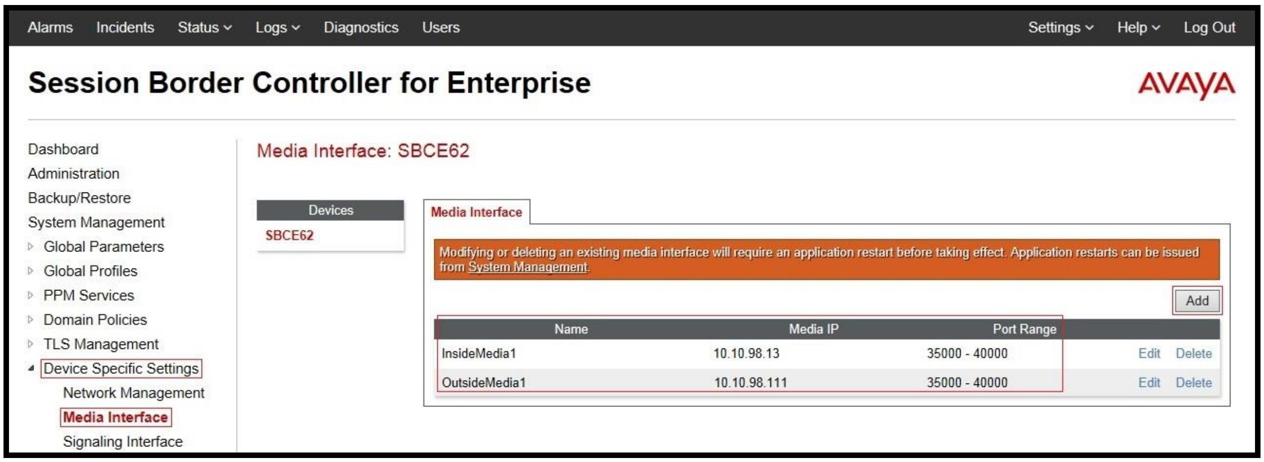

Figure 68 - Media Interface

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**: **InsideUDP1**.
  - **Media IP**: **10.10.98.13** (Avaya SBCE Internal IP Address toward CS1000).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).
- Select **Add**.
  - **Name**: **OutsideUDP1**.
  - **Media IP**: **10.10.98.111** (Avaya SBCE External IP Address toward MTS Allstream SIP Trunk Service).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).

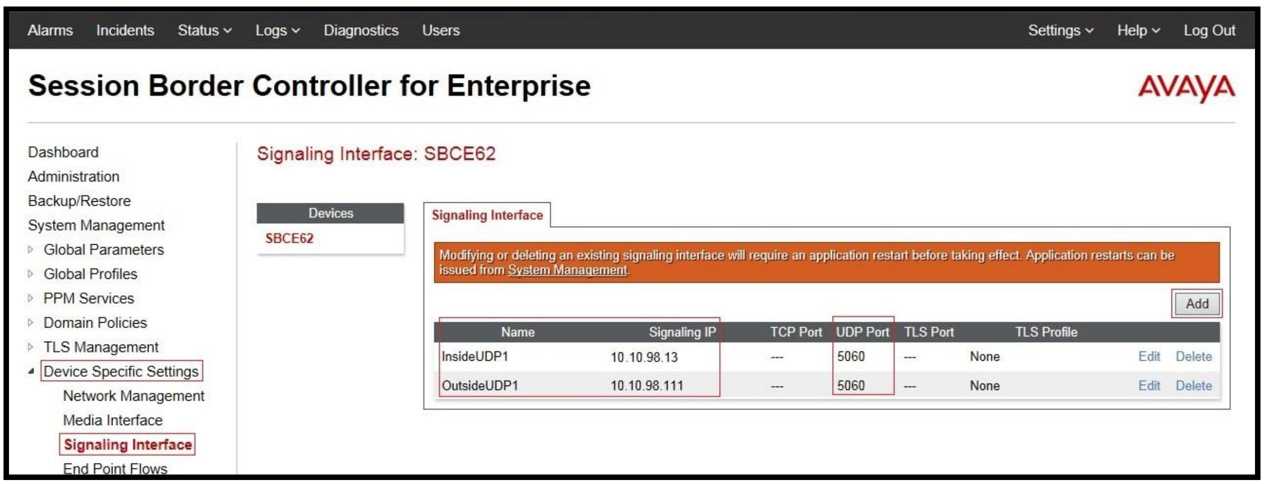

Figure 69 - Signaling Interface

6.4.4. Configuration End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the signaling endpoints are CS1000 and the MTS Allstream SIP Trunk Service.

6.4.4.1 Create End Point Flows – CS1000 Flow

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

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name**: **CS1K76_Flow**.
  - **Server Configuration**: **SP4** (refer to **Section 6.2.6**).
  - **URI Group**: **SP4** (refer to **Section 6.2.3**).
  - **Transport**: *****.
  - **Remote Subnet**: *****.
  - **Received Interface**: **InsideUDP1** (refer to **Section 6.4.3**).
  - **Signaling Interface**: **OutsideUDP1** (refer to **Section 6.4.3**).
  - **Media Interface**: **OutsideMedia1** (refer to **Section 6.4.2**).
  - **End Point Policy Group**: **SP4_PolicyG** (refer to **Section 6.3.1**).
  - **Routing Profile**: **SP4_To_CS1K76** (refer to **Section 6.2.7**).
  - **Topology Hiding Profile**: **CS1K76_To_SP4** (refer to **Section 6.2.10**).
  - Click **Finish**.

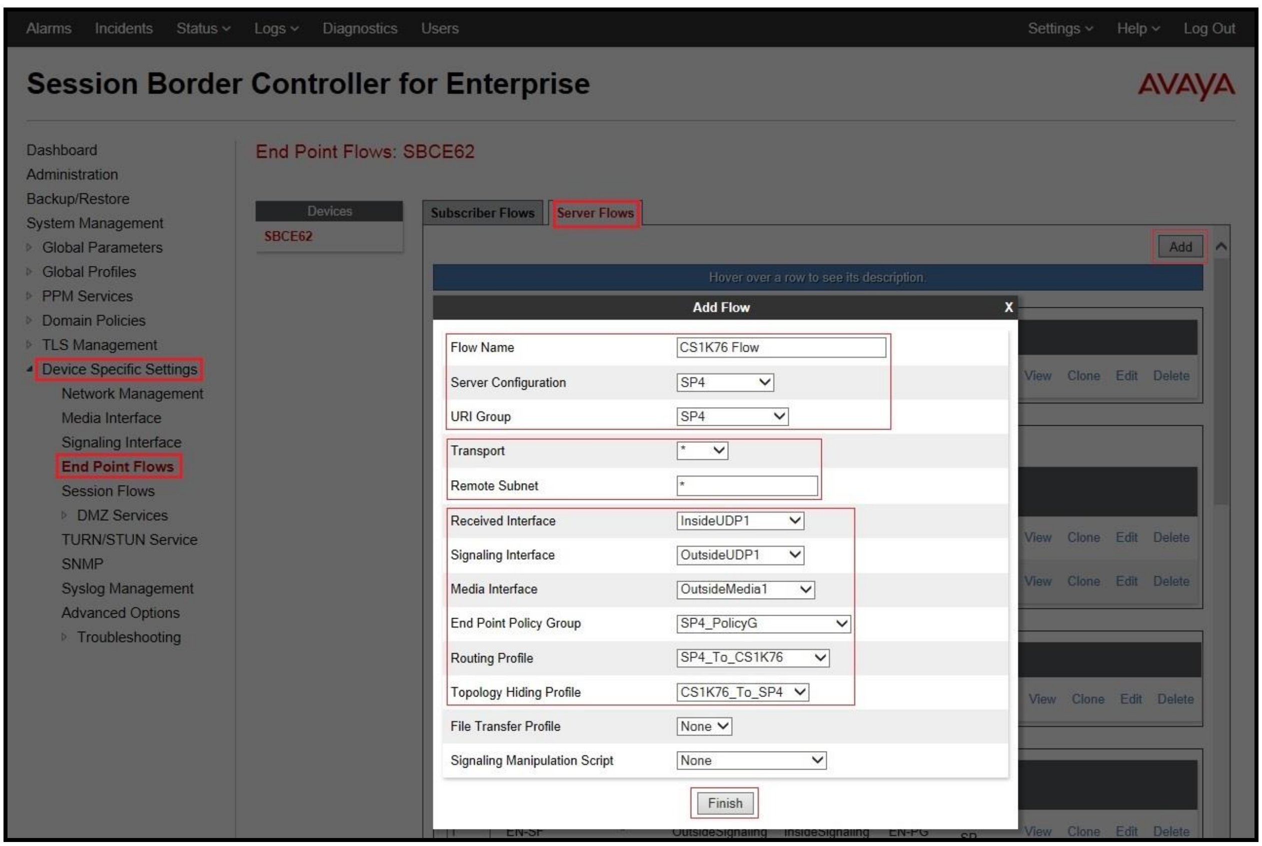

Figure 70 - End Point Flows 1

6.4.4.2 Create End Point Flows – Trunk Flow

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

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name**: **SP4_Flow**.
  - **Server Configuration**: **CS1K76** (Refer to **Section 6.2.5**).
  - **URI Group**: **SP4** (Refer to **Section 6.2.3**).
  - **Transport**: *.
  - **Remote Subnet**: *.
  - **Received Interface: OutsideUDP1** (refer to **Section 6.4.3**).
  - **Signaling Interface**: **InsideUDP1** (refer to **Section 6.4.3**).
  - **Media Interface**: **InsideMedia1** (refer to **Section 6.4.2**).
  - **End Point Policy Group**: **CS1K76_SP4_PolicyG** (refer to **Section 6.3.1**).
  - **Routing Profile**: **CS1K76_To_SP4** (refer to **Section 6.2.8**).
  - **Topology Hiding Profile**: **SP4_To_CS1K76** (refer to **Section 6.2.9**).
  - Click **Finish**.

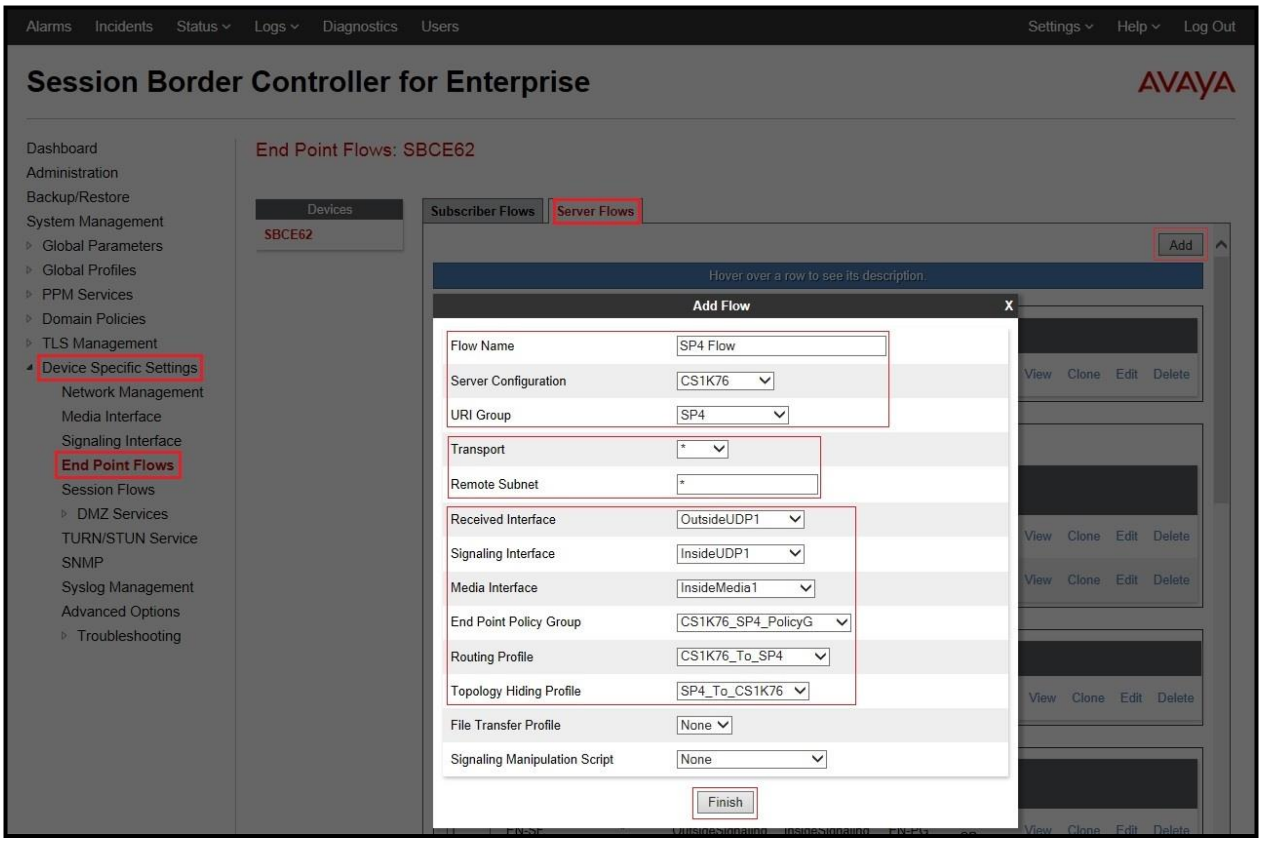

Figure 71 - End Point Flows 2

7. MTS Allstream SIP Trunk Service Configuration

MTS Allstream is responsible for the network configuration of the MTS Allstream SIP Trunk Service. MTS Allstream SIP Trunk Service will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. MTS Allstream SIP Trunk Service will provide the IP addresses of MTS Allstream'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 Avaya SBCE discussed in the previous sections.

The configuration between MTS Allstream SIP Trunk Service and the enterprise is a static configuration. There is no authentication of the SIP trunk from enterprise users to the MTS Allstream's network.

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 audio path exists. Verify that the call remains stable for several minutes and disconnects properly.

8.2. Verification of an Active Call on Communication Server 1000

Active Call Trace (ld 80)

The following is an example of one of the commands available on the CS1000 to trace the DN for which the call is in progress or idle (1257). The call scenario involved PSTN phone number 1613XXX5206 calling 647XXX1257 (which is translated to phone 1257).

- 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 1257**.
- After the call is released, issue command **trac 0 1257** 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 **1257** is in call state:

```
>ld 80
TRA000
.trac 0 1257

ACTIVE  VTN 096 0 00 02

ORIG   VTN 100 0 01 00   VTRK IPTI  RMBR  101 1 INCOMING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 10.10.98.13
  FAR-END MEDIA ENDPOINT IP: 10.10.98.13  PORT: 36660
  FAR-END SIP SIGNALLING IP: 10.10.98.13
  FAR-END MEDIA ENDPOINT IP: 10.10.98.13  PORT: 36660
TERM   VTN 096 0 00 03  KEY 0  SCR MARP  CUST 0  DN 1257  TYPE 2002P2
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 10.33.5.23  PORT: 5200
MEDIA PROFILE: CODEC G.729A NO-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 1257
MAIN_PM  ESTD
TALKSLOT  ORIG  26   TERM  31
EES_DATA:
NONE
QUEU  NONE
CALL ID 501 9

----  ISDN ISL CALL (ORIG) ----
CALL REF # =  385
BEARER CAP =  VOICE
HLC =
```

```
CALL STATE =  10     ACTIVE
CALLING NO =  1613XXX5206  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
CALLED NO  =  647XXX1257  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
```

And this is the example after the call to 1257 is finished.

```
>ld 80
TRA000
.trac 0 1257
IDLE VTN 96 0 00 02   MARP
```

SIP Trunk monitoring (ld 32)
Place a call inbound from PSTN (1613XXX5206) to an internal device (647XXX1257). 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**.

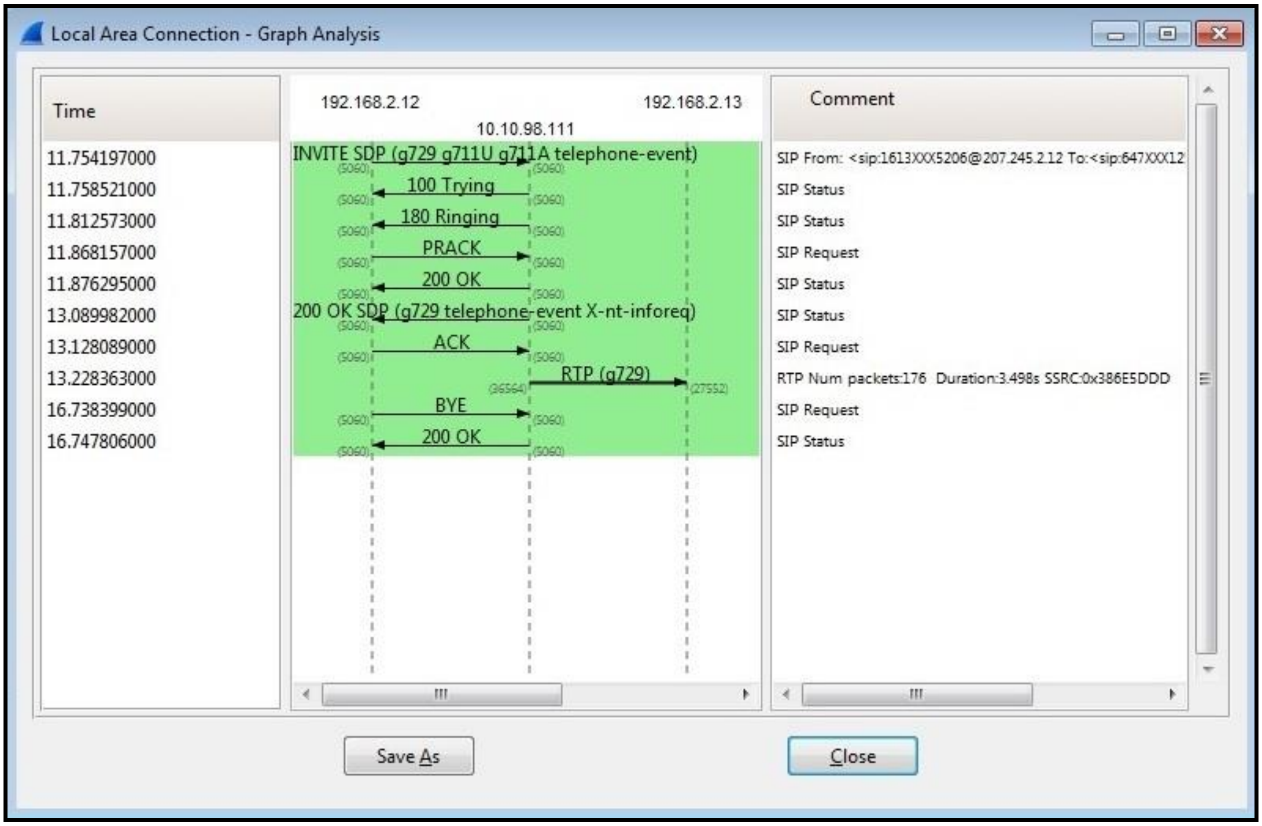

Figure 72 – SIP Call Trace

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 MTS Allstream SIP Trunk Service is considered **compliant** with Avaya Communication Server 1000 Release 7.6, and Avaya Session Border Controller for Enterprise Release 6.3.

10. References

This section references the documentation relevant to these Application Notes.

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

Avaya Communication Server 1000

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

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

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

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

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

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

Avaya Session Border Controller for Enterprise

[7] *Avaya Session Border Controller for Enterprise Overview and Specification,* Release 6.3, Issue 3, October 2014

[8] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014

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.