Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunking with Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Session Border Controller Release 6.0 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of Avaya Communication Server 1000 release 7.5 and MTS Allstream SIP Trunking. During the interoperability testing, Avaya Communication Server 1000 was able to interoperate with the MTS Allstream system via SIP trunk. This test was performed to verify SIP trunk features including basic call, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls are placed in both directions with various set types.

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.

1. Introduction

This document provides a typical network configuration deployment of Avaya Communication Server 1000 (hereafter referred to as CS1000) and MTS Allstream SIP Trunking (hereafter referred to as MTS Allstream system). During the interoperability testing, all SIP trunk applicable feature test cases were executed to ensure the interoperability between MTS Allstream system and Avaya CS1000.

2. General Test Approach and Test Results

CS1000 release 7.5 was connected to Avaya Aura® Session Border Controller (hereafter referred to as AA-SBC) via Avaya Aura® Session Manager. AA-SBC was connected to the MTS Allstream system via SIP trunk. Various call types were made from CS1000 to the MTS Allstream system and vice versa to ensure the interoperability between CS1000 and the MTS Allstream system.

2.1. Interoperability Compliance Testing

The focus of this testing is to verify that CS1000 release 7.5 can interoperate with the MTS Allstream system. The following interoperability areas were covered.

- General call processing between CS1000 and MTS Allstream including:
  - Codec (G.711 u-law/ G.729/ ptime 20ms, VAD disabled)
  - Hold/Retrieve on both ends
  - Music On Hold
  - CLID displays
  - Ring-back tone
  - Speech paths
  - Dialing plan support
  - Advanced features (Call on Mute, Call Park, Call Waiting)
  - Abandoned Call
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends
- RFC2833/DTMF on both direction
- SIP Transport UDP
- Thru dialing via PBX Call Pilot
- Voice Mail Server CallPilot (hosted on Avaya system)
- Fax Transmission: fax was transmitted from both ends with codec G.711.
- Early Media Transmission.
- Static Registration

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. For outbound calls from CS1000 to PSTN, MTS Allstream did not offer alternate CLID-Name and CLID-Number delivery.
   - Call scenario: Make an outbound SIP call from a CS1000 phone to a PSTN phone.
   - SIP observation: CS1000 sent “From” header with CLID-Name and CLID-Number.
   - Expected result: The call is established with 2 way speech paths. CLID Number and Name are displayed correctly.
   - Actual result: MTS Allstream did not modify CLID-Name provided by CS1000.
   - Recommendation: The CLID-Name from CS1000 should be verified and alternated by MTS Allstream. However, MTS Allstream currently passes through CLID provided by customer. There is no resolution available at this time.

2. Outbound E911 calls from CS1000 to PSTN are not supported by MTS Allstream.
   - Call scenario: Make an outbound 911 SIP call from a CS1000 phone.
   - SIP observation: N/A.
   - Expected result: The call is established with 2 way speech paths. The CLID Name/ Number and location information are displayed correctly on PSAT.
   - Actual result: N/A.
   - Resolution: Allstream did not support outbound E911 calls. There is no available resolution at this time.

3. For inbound toll free calls, the CLID Name was not delivered to CS1000.
   - Call scenario: Make an inbound SIP call from a PSTN phone to a CS1000 toll free number.
   - SIP observation: MTS Allstream translated inbound toll free calls to a DID number to send to CS1000 over SIP Trunks.
   - Expected result: Calls are established with 2 way speech paths. CLID Number and Name are displayed correctly.
   - Actual result: the call was established with good RTPs, CS1000 phones displayed the CLID Number, but the CLID Name was not delivered to CS1000.
   - Resolution: There is no available resolution at this time.

4. Outbound calls from CS1000 to PSTN with “Privacy: user” to hide CLID-Name, but MTS Allstream still delivers CLID-Name to PSTN.
   - Call scenario: Make an outbound SIP call from a CS1000 phone to a PSTN phone with “Privacy: user”.
   - SIP observation: CS1000 sent “Privacy: user” header to MTS Allstream.
   - Expected result: Calls are established with 2 way speech paths. PSTN either does not display CLID Name of CS1000 phones or displays “private” or “anonymous”, but it still is able to display CLID Number.
   - Actual result: CLID-Name was still being displayed at PSTN phones.

- Recommendation: MTA Allstream does not support "Privay:user". Thus, in order to hide CLID-Name, CS1000 should send CLID-Name "Anonymous" and "Privacy:none" to MTS Allstream system.

5. Recorded announcement lost about 3 seconds when PSTN phone calls to Voicemail hosted on CS1000.
   - Call scenario: Make a SIP call from PSTN to Voicemail DN hosted on CS1000.
   - SIP observation: CS1000 sent 180/SDP to transmit the early media for announcement.
   - Expected result: The recorded announcement is fully (in length) transmitted to PSTN.
   - Actual result: The early media was lost for about 3 seconds. First 3 seconds (of the recorded message) are not heard when the call goes to Voicemail.
   - Resolution: Known issue against Avaya CS1000 and there is no resolution available at this time.

6. MTS Allstream could not offer codec order G.711, G.729.
   - Call scenario: Make an inbound SIP call from PSTN to CS1000 which has codec profile G.711, G.729 in order.
   - SIP observation: N/A.
   - Expected result: Calls are established with 2 way speech paths using the preferred codec. CLID Number and Name are displayed correctly.
   - Actual result: N/A
   - Resolution: MTS Allstream cannot offer codec order G.711, G.729 for testing. Thus codec negotiation with codec order G.711, G.729 offered by MTS Allstream has not being verified. There is no resolution available at this time.

7. CS1000 phone held/ retrieved an outgoing call causing the display to be changed.
   - Call scenario: Make a SIP call from a CS1000 phone to PSTN, and perform "hold/ retrieve".
   - SIP observation: N/A
   - Expected result: Calls are established with 2 way speech paths. Number and Name are displayed correctly with "hold/ retrieve" action.
   - Actual result: After retrieving the call, the telephone number previously displayed on CS1000 phones will be unavailable and replaced by Route ACOD – Trunk Channel ID.
   - Resolution: This is a known CS1000 issue and there is no resolution available at this time.

2.3. Support

For technical support on MTS Allstream, please contact MTS Allstream technical support at:

- Phone: 204-941-8557 or 1-800-542-8703
- Email: mts.special.needs@mts.ca
- Website: http://www.mts.ca/mts/personal/support

3. Reference Configuration

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

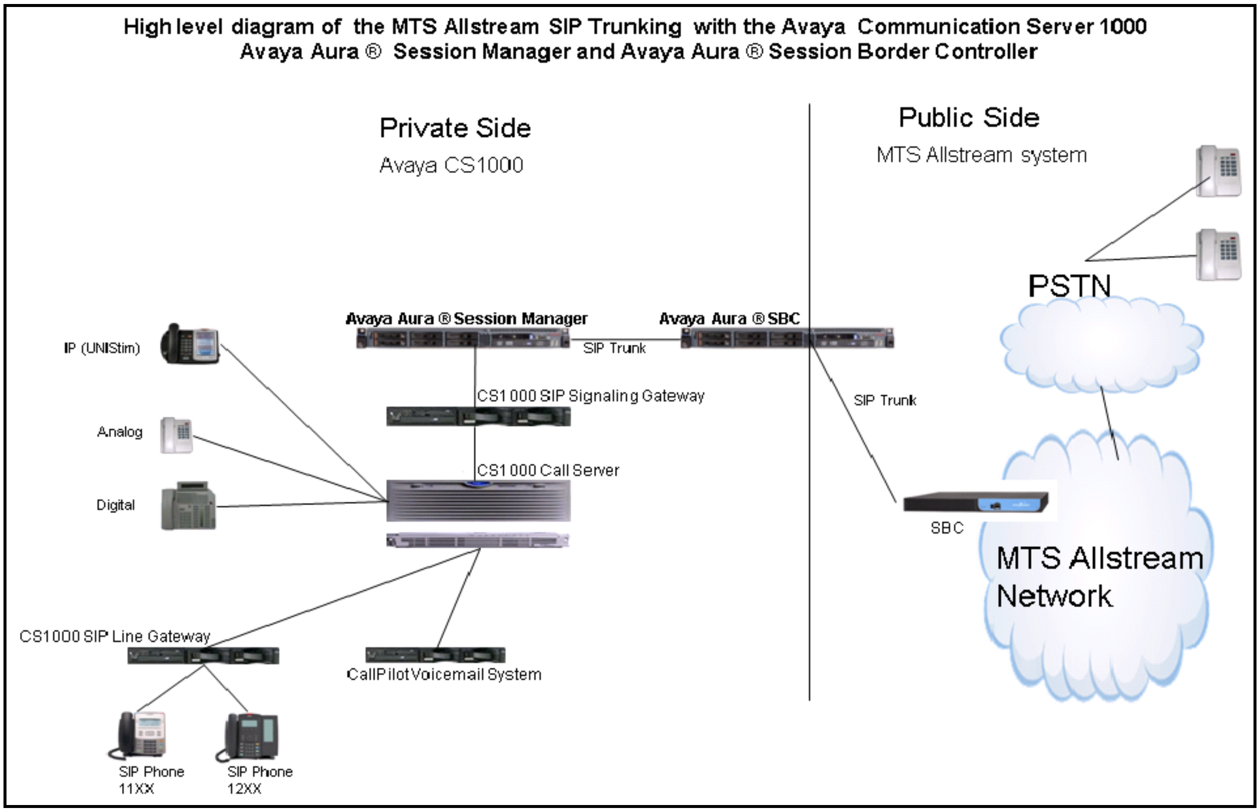

Figure 1- Network Diagram for Avaya CS1000 – MTS Allstream system

The following assumptions were made for this lab test configuration.

1. CS1000 R7.5 software and implementation of latest patches
2. MTS Allstream provides support to setup, configure, and troubleshoot on carrier switch for the duration of the testing.

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, name 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. The call server maintenance terminal window was used for the monitoring of BUG(s), ERR and AUD messages.
8. Speech path and display checked before and after calls were put on/off hold from each end.
9. Applicable files were screened on an hourly basis during the testing for messages that may indicate technical issues. This refers to Avaya PBX files.
10. Calls were checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs are released when a call scenario ends.

4. Equipment and Software Validated

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

Avaya system:

System	Software/Loadware version
Avaya CS1000 7.5 (CPPM)	• Call Server: 7.50 Q GA plus latest DEPLIST – Issue: 01 Release: x2107.50, 2011-07-19 11:40:08 (est) • SSG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20110719.ntl • SLG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20110719.ntl
Avaya phones	• 2002 p2: 0604DCJ (UNIStim) • 2004 p2: 0604DCJ (UNIStim) • 1140: 0625C6O (UNIStim) • 1120: 0624C6O (UNIStim) • 2007: 0621C6M (UNIStim) • 1220: 062AC6O (UNIStim) • SIP 1120, 1140: SIP12x0e04.00.04.00 • SIP 1220,1240: SIP12x0e04.00.04.00
Avaya Aura® Session Border Controller	• SBCT 6.0.2.0.3 (sbc E362P4)

MTS Allstream system:

System	Software/Loadware version
Genband S3	• Release 5.2.2.12
CS2K	• CVM13

The output of "dstat" command on Call Server:

```
pdt> dstat
Call Server:
------------
```

```
DepList name: core
        Filename: /var/opt/nortel/cs/fs/u/patch/deplist/mcore_01.cpl
        Issue   :  01
        Release :  x2107.50
        Created :  2011-07-19 11:40:08 (est)
        Number of patches: 60
        Patches Loaded: 60
        Patches In-service: 60
pdt>
```

The output of "pstat" command on SSG Server:

```
[admin@car2-mas ~]$ pstat
Product Release: 7.50.17.00
In system patches: 0

In System service updates: 10
PATCH#  IN_SERVICE   DATE      SPECINS   REMOVABLE   NAME
0       Yes         07/01/11   NO       YES        cs1000-baseWeb-7.50.17.01-1.i386.000
1       Yes         11/05/11   NO       YES        cs1000-sps-7.50.17-01.i386.000
2       Yes         25/08/11   NO       YES        cs1000-patchWeb-7.50.17.16-1.i386.000
4       Yes         11/05/11   NO       YES        cs1000-shared-pbx-7.50.17-01.i386.000
5       Yes         11/05/11   NO       YES        cs1000-dbcom-7.50.17-02.i386.000
7       Yes         06/07/11   NO       YES        cs1000-vtrk-7.50.17.16-02.i386.000
9       Yes         06/07/11   NO       YES        cs1000-linuxbase-7.50.17.16-1.i386.000
10      Yes         06/07/11   NO       YES        cs1000-dmWeb-7.50.17.16-1.i386.000
11      Yes         06/07/11   NO       YES        cs1000-tps-7.50.17.16-4.i386.000
12      Yes         06/07/11   YES      YES        cs1000-Jboss-Quantum-7.50.17.16-4.i386.000
[admin@car2-mas ~]$
```

5. Avaya Communication Server 1000 Configuration

These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 9.**

The following sections describe the configuration details of CS1000 with a SIP trunk to the MTS Allstream system.

5.1. Login to CS1000 System

5.1.1. Login Unified Communications Management (UCM) and Element Manager (EM)

a) Open an instance of a web browser and connect to the UCM GUI at the following address: http://<UCM IP address> as shown in **Figure 2**. Log in using an appropriate Username and Password.

Figure 2 – Login Unified Communications Management

b) The **Unified Communications Management** screen is displayed. Click on the **Element Name** of the CS1000 Element as highlighted in the red box as shown in **Figure 3**.

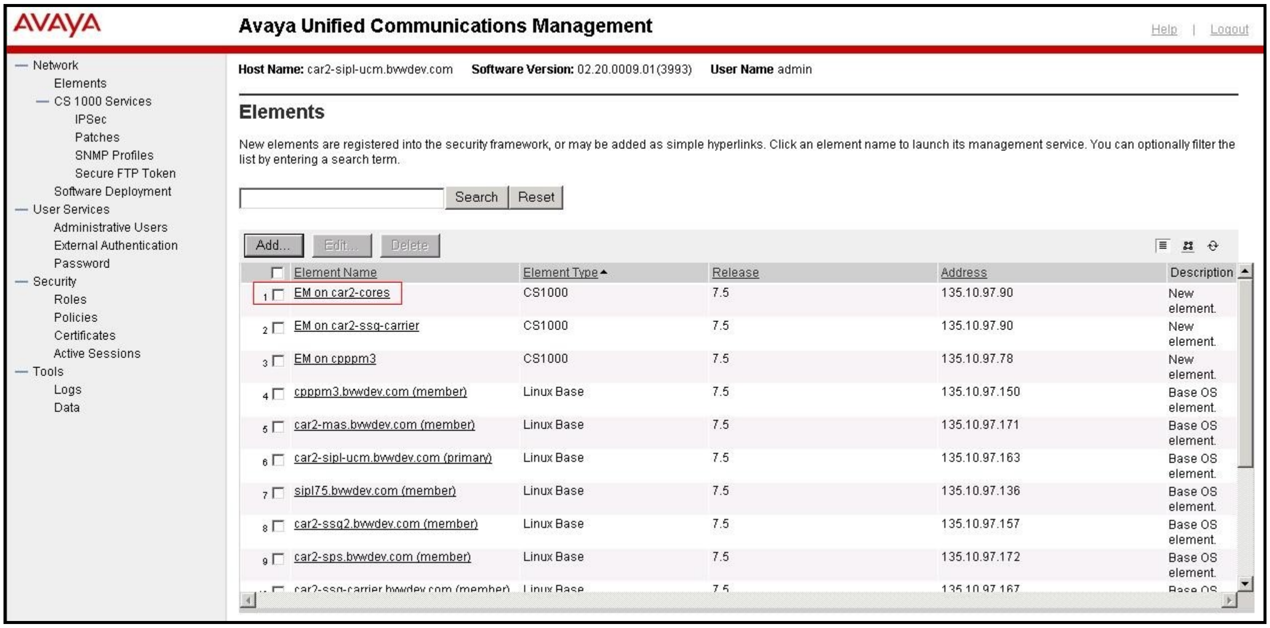

Figure 3 – Unified Communications Management

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

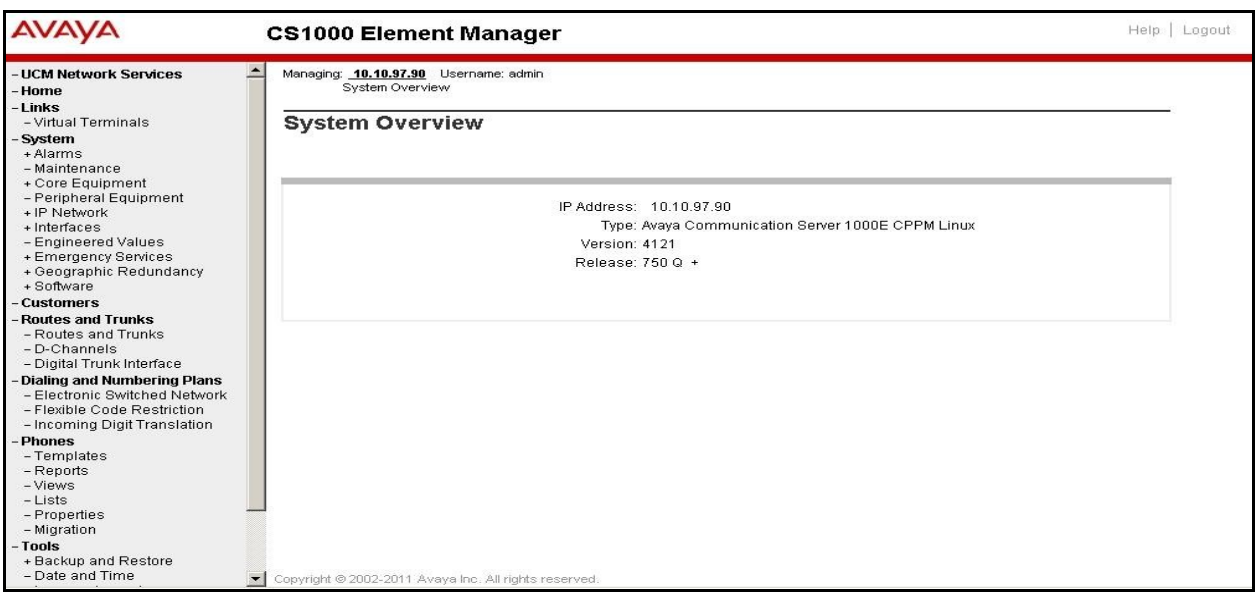

Figure 4 – Element Manager System Overview

5.1.2. Login to Call Server Command Line Interface (CLI)

a) Using Putty, SSH to the IP address of the SSG Server with the admin account.
b) Run the command "cslogin" and login with the appropriate admin account and password.
c) Here are the logs.

```
login as: admin

            Avaya Inc. Linux Base  7.50
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@110.10.97.168's password:
Last login: Thu Mar 10 17:38:16 2011 from 110.10.97.172



/usr/bin/xauth:  creating new authority file /home/admin/.Xauthority
[admin@car2-ssg-carrier ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without authentica
ting
login
USERID? admin
PASS?
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 logout immediately. This system may be monitored for
operational purposes at any time.

.
TTY #09 LOGGED IN ADMIN 17:42  10/3/2011

>
```

5.2. Administer a Node IP Telephony

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

5.2.1. Obtain Node IP address

These Application Notes assume that the basic configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 2004) in the CS1000 IP network to work with MTS Allstream system. For further information on Avaya Communications Server 1000, please consult reference in **Section 9**.

a) Select **System** -> **IP Network** -> **Nodes: Servers, Media Cards. Figure 5** displays the **IP Telephony Nodes** page. Click on the Node ID of the CS1000 Element.

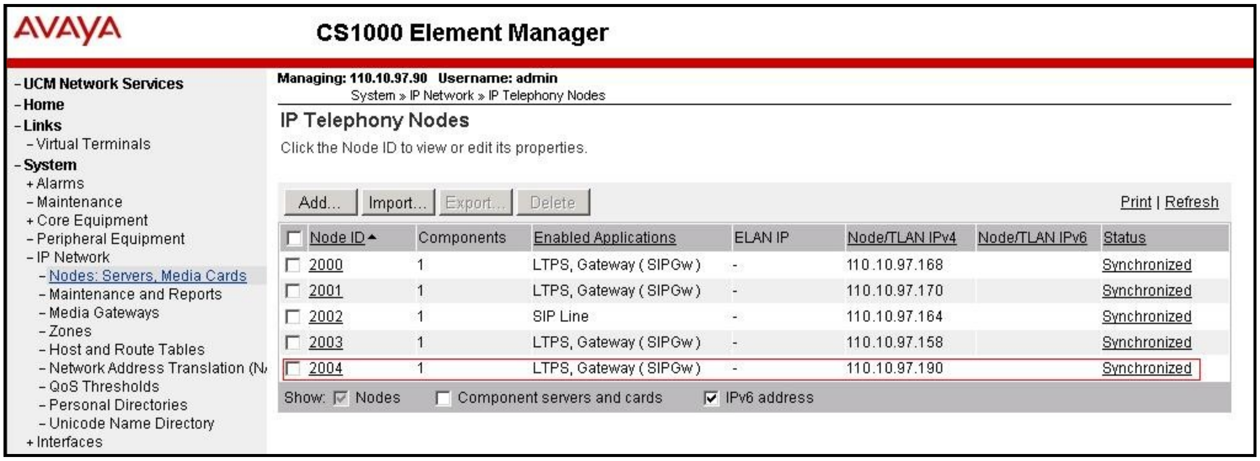

Figure 5 – IP Telephony Nodes

b) The **Node Details** screen is displayed in **Figure 6** with the IP address of the CS1000 node. The **Node IP Address** is a virtual address which corresponds to the TLAN IP address of the SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IP Address** to communicate with other components to process the SIP call.

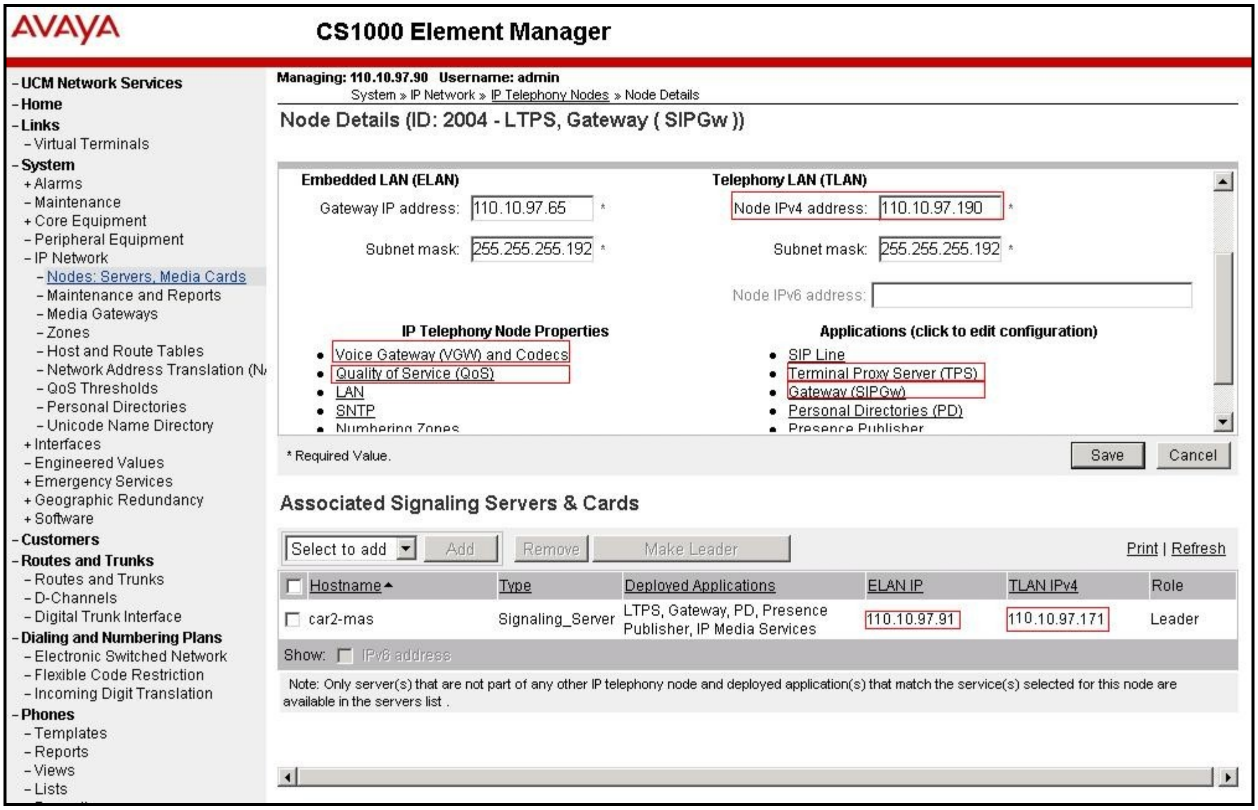

Figure 6 –Node Details

5.2.2. Administer TPS

c) Continue from **Section 5.2.1**. On the **Node Details** page, select the **Terminal Proxy Server** (**TPS**) link as shown in **Figure 6**.

d) Check the **UNIStim Line Terminal Proxy Server** check box and then click **Save** as shown in **Figure 7**.

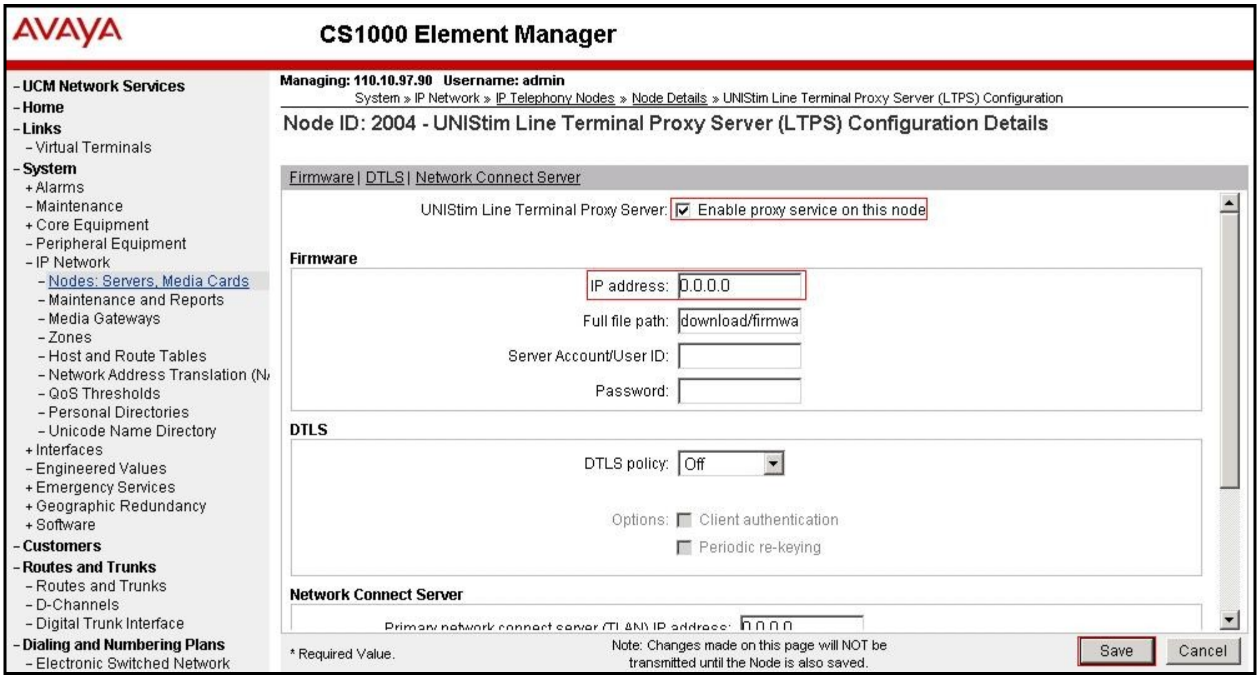

Figure 7 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

e) Continue from **Section 5.2.1**. On the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 6**.
f) The default Diffserv values are as shown in **Figure 8**. Click the **Save** button.

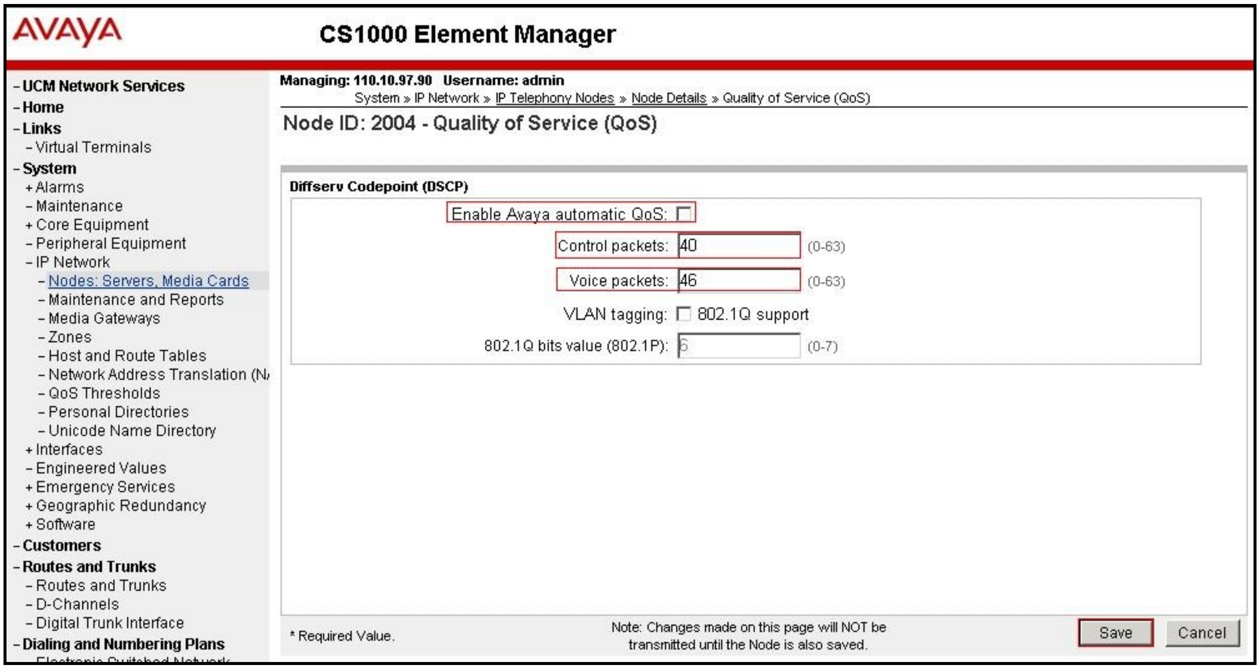

Figure 8 – QoS Configuration Details

5.2.4. Synchronize the New Configuration

g) Continue from **Section 5.2.3**, return to the **Node Details** page (**Figure 6**) and click on the **Save** button.
h) The **Node Saved** screen is displayed. Click on the **Transfer Now** (not shown).
i) The **Synchronize Configuration Files** screen is displayed. Check the Signaling Server check box and click on the **Start Sync** (not shown).
j) When the synchronization completes, check the Signaling Server check box and click on the **Restart Applications** (not shown).

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec, Node IP Telephony.

a) Select **IP Network** -> **Nodes: Servers, Media Cards** -> Configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed. (See in **Section 5.2.1** for more detail).
b) On the **Node Details** page as shown in **Figure 6**, click on **Voice Gateway (VGW) and Codec.**
c) The MTS Allstream SIP Trunk supports voice codec G.729 and G.711 as fallback, payload size 20 ms, with VAD disabled. **Figures 9a** and **9b** show voice codec profile configured on CS1000.

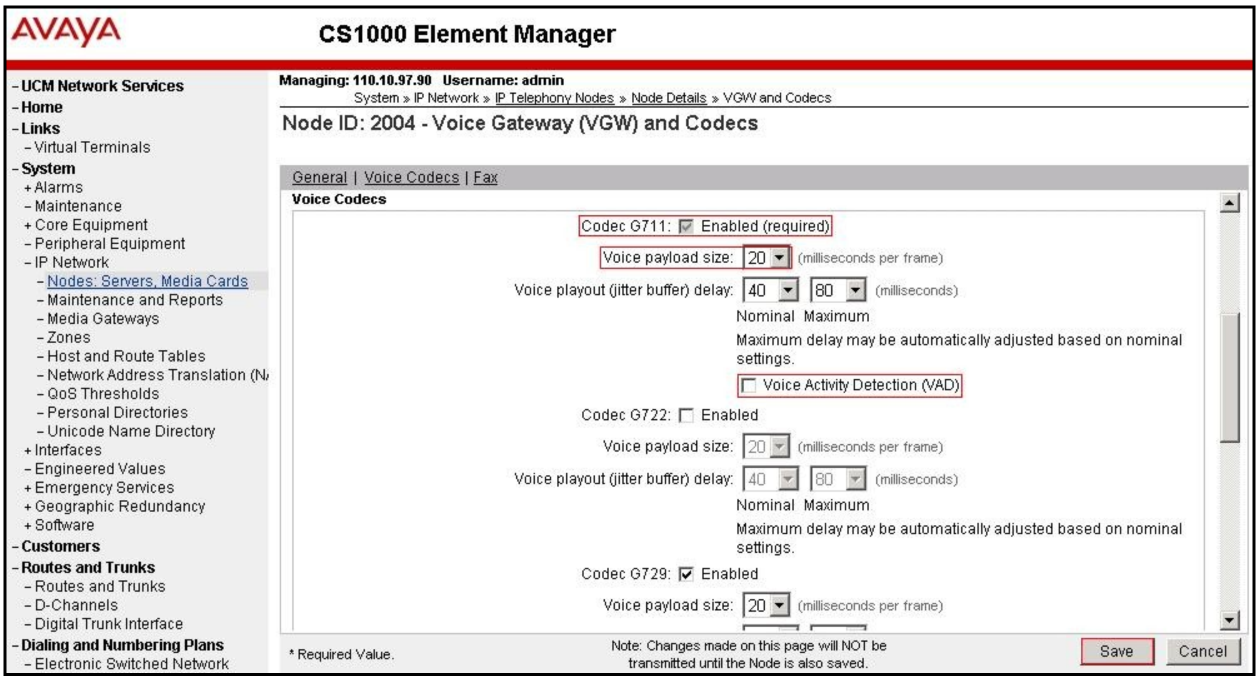

Figure 9a – Voice Codec G.711 Configuration Details

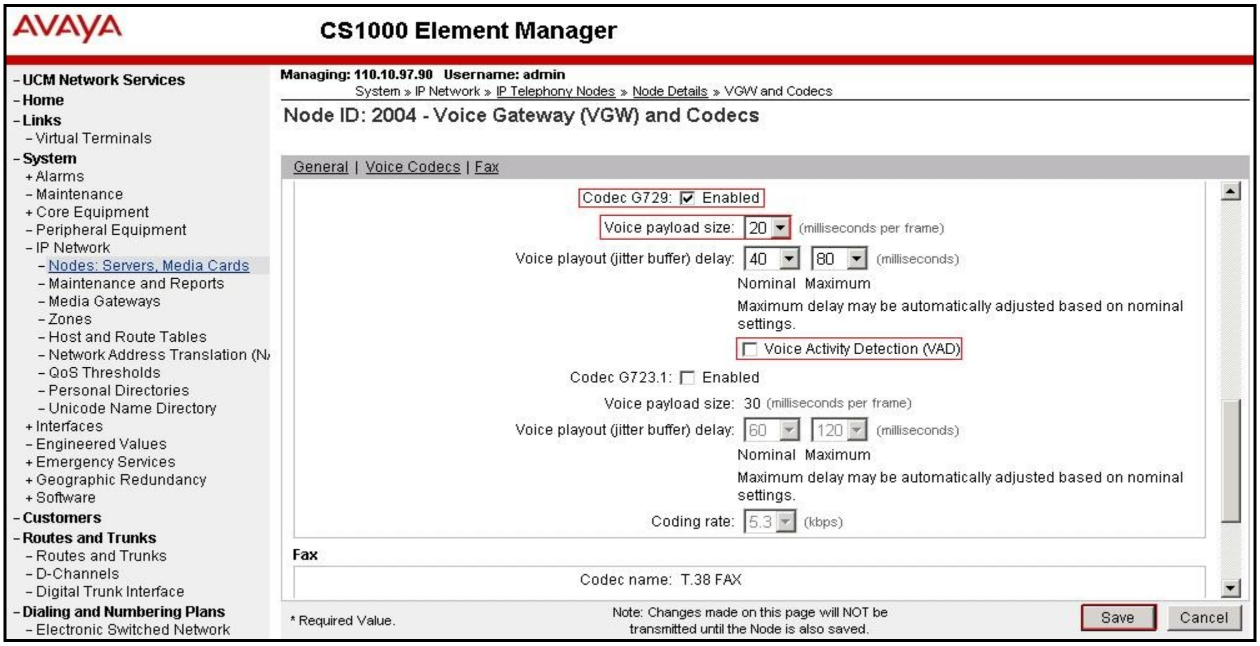

Figure 9b – Voice Codec G.729 Configuration Details

d) For Fax over IP, MTS Allstream supports G.711 as default and does not support T.38. Even though CS1000 does not have an option to disable T.38, it is still capable to use G.711 for fax calls. **Figure 9c** shows **Modem Pass Through** was selected for Node 2004; this configuration enables codec G.711 to be used to transmit or receive fax calls between CS1000 and MTS Allstream.

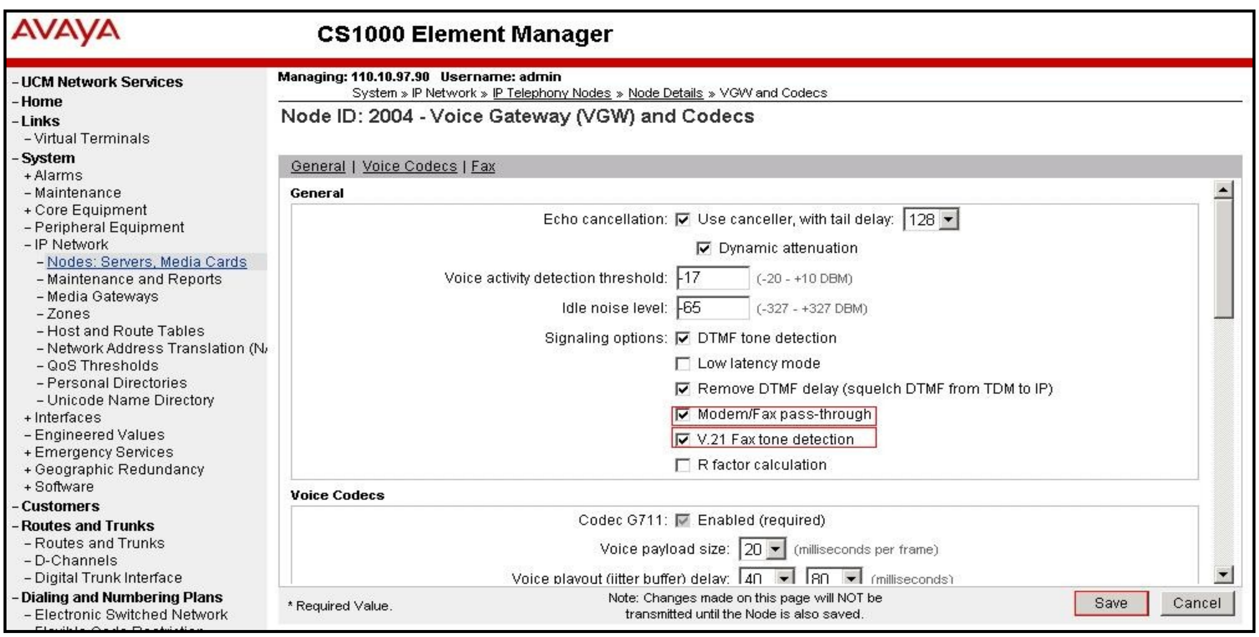

Figure 9c – Fax Codec G.711 Configuration Details

e) Click **Save**.
f) Synchronize the new configuration (please refer to **Section 5.2.4** for more detail).

5.3.2. Enable Voice Codec on Media Gateways.

CS1000 uses Media Gateways to support traditional analog and digital phones for voice calls over SIP Trunk. Media Gateways is also needed to support analog terminals to send fax over IP.

a) From the left menu of the Element Manager page in **Figure 6**, select the **IP Network** -> **Media Gateways** menu item. The Media Gateways page will appear (not shown). Click on **MGC** which is located on the right of the page.
b) The MTS Allstream SIP Trunk supports voice codec G.729 and G.711 as fallback, payload size 20 ms, with VAD disabled**. Figure 10a** shows codec profile configured for Media Gateway.

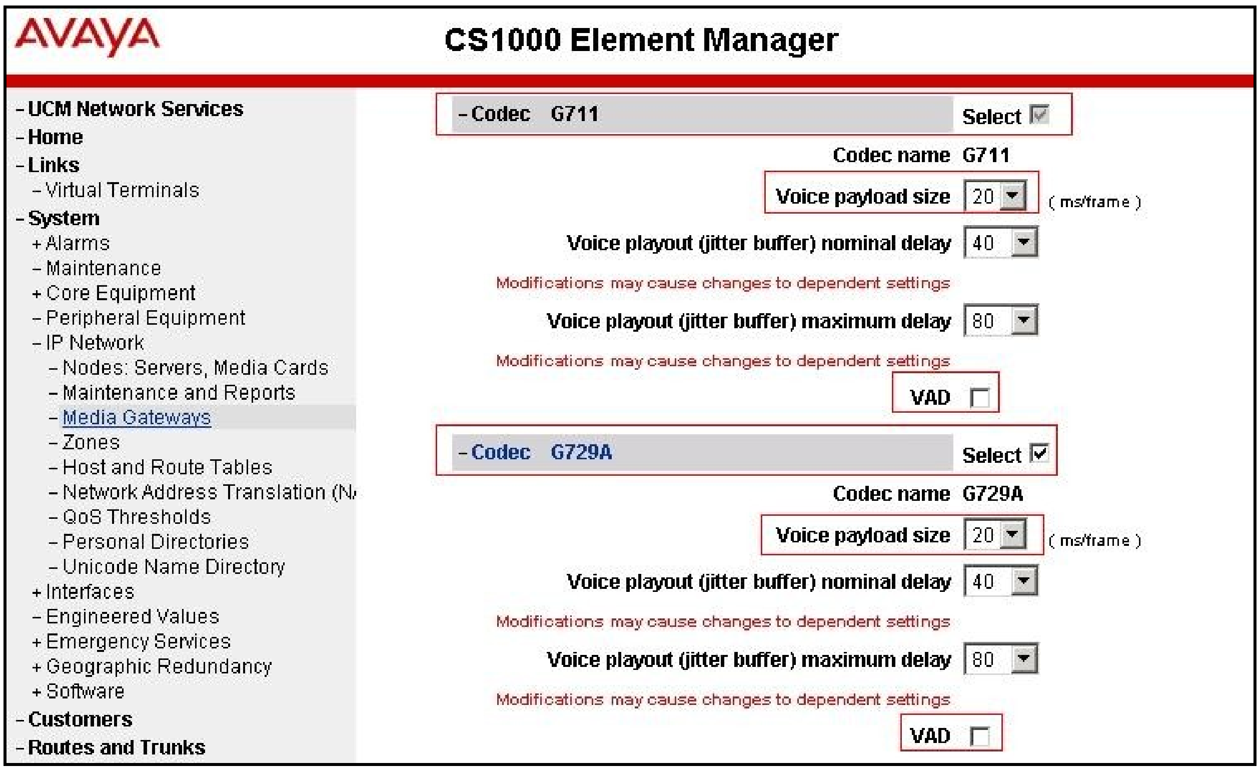

Figure 10a – Media Gateways G.729 and G.711 Configuration Details

c) For Fax over IP, MTS Allstream supports G.711 as default and does not support T.38. Even though CS1000 does not have an option to disable T.38, it is still capable to use G.711 for fax calls. **Figure 10b** shows **Modem Pass Through** was selected for Media Gateway; this configuration enables codec G.711 to be used to transmit or receive fax call between CS1000 and MTS Allstream.

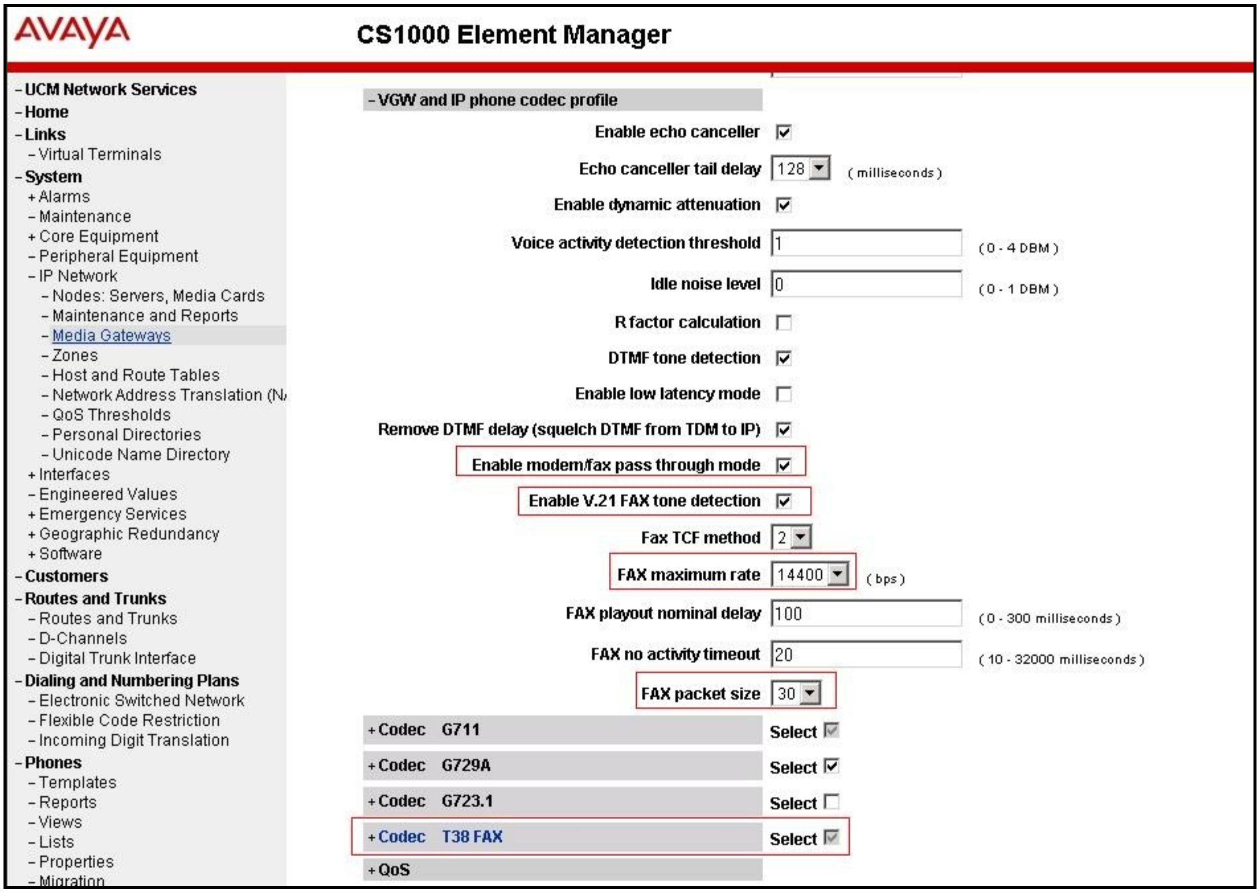

Figure 10b – Media Gateways ModemPassThrough (G.711) Configuration Details

5.4. Administer Zones and Bandwidth

This section describes the steps to create 2 zones: zone 10 for VGW and IP phones, and zone 255 for IP SIP Trunk.

5.4.1. Create a zone for IP phones (zone 10)

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

a) Select **IP Network** -> **Zones** configuration from the left pane, click on the **Bandwidth Zones** as shown in **Figure 11**.

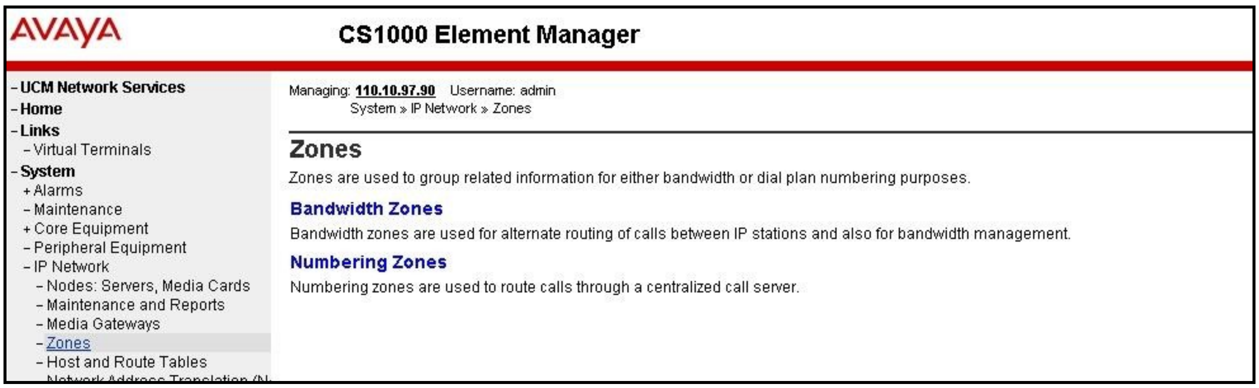

Figure 11 –Zones Page

b) The **Bandwidth Zones** screen is displayed as shown in **Figure 12**. Click **Add**.

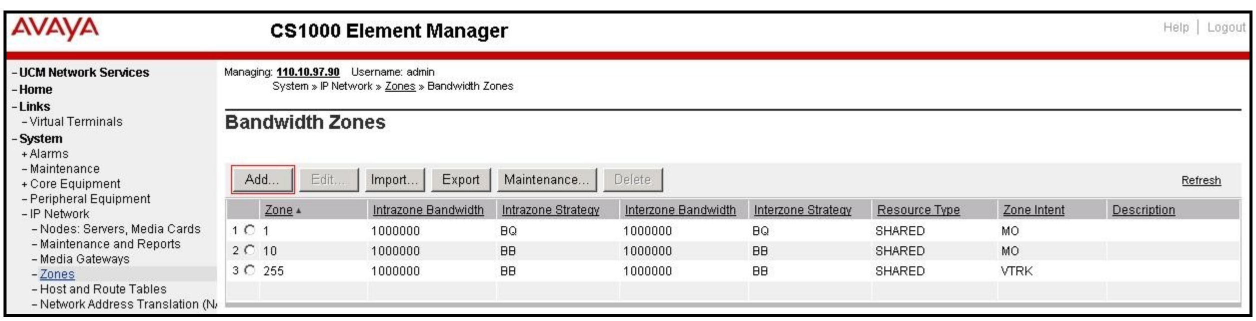

Figure 12 –Bandwidth Zones

c) In the **Add Bandwidth Zone** screen (not shown), click on **Zone Basic Property and Bandwidth Management**, select the values as shown (in red box) in **Figure 13,** and click on the **Submit** button.

- **INTRA_STGY**: bandwidth configuration for local calls.
- **INTER_STGY**: bandwidth configuration for the calls over trunk.
- **BQ**: G711 is first choice and G729 is second choice.
- **BB**: G729 is first choice and G711 is second choice.
- **MO**: is used for IP phones, VGW
- **VTRK**: is used for virtual trunk.

The MTA Allstream SIP Trunk support G.729 as the first choice, G.711 as fallback. So the **MO** Zone 10 was configured with **Strategy Best Bandwidth (BB)**.

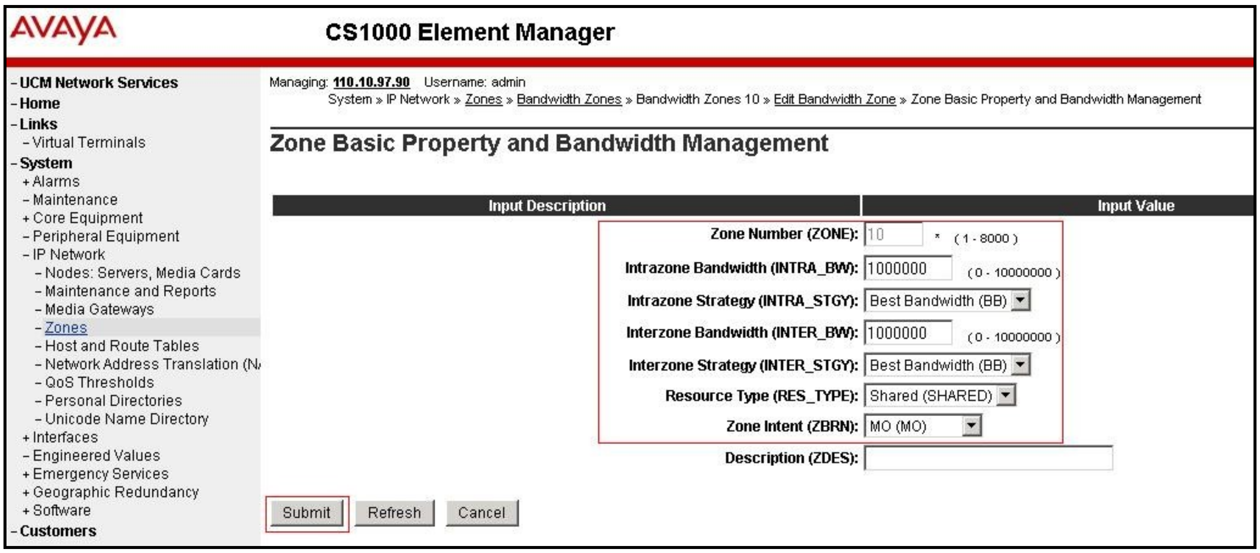

Figure 13 –Bandwidth Management Configuration Details– IP phone

5.4.2. Create a zone for virtual SIP trunk (zone 255)

Follow **Section 5.4.1** to create a zone for the virtual trunk. The difference is in the **Zone Intent (ZBRN)** field. Select **VTRK** for virtual trunk (**Figure 14**) and then click on the **Submit** button.

The MTS Allstream SIP Trunk support G.729 as the first choice, G.711 as fallback. So the **VTRK** Zone 255 was configured with **Strategy Best Bandwidth (BB)**.

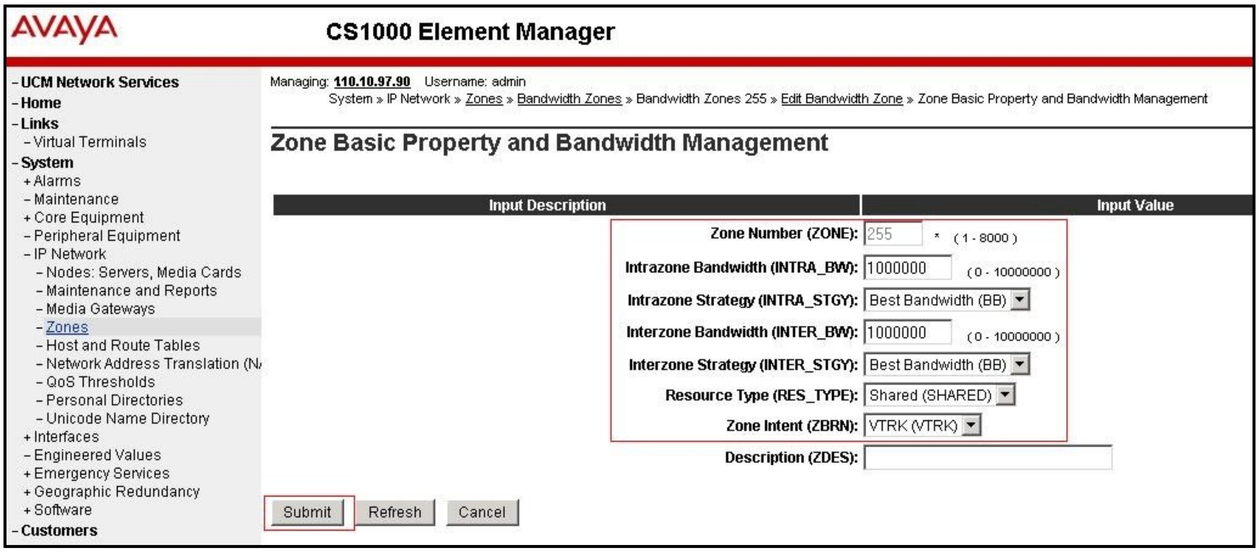

Figure 14 –Bandwidth Management Configuration Details– Virtual Trunk

5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP IP connection between SIP Signalling Gateway (SSG) to Session Manager.

5.5.1. Integrated Services Digital Network (ISDN)

a) Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **04**. The system can support more than one customer with different network settings and options. The **Customer 04 Edit** page will appear (not shown). Select the **Feature Packages** option from this page.
b) The screen is updated with a list of F**eature Packages** populated. Select **Integrated Services Digital Network** to edit its parameters. The screen is updated with parameters populated below **Integrated Services Digital Network**. Check the **Integrated Services Digital Network** (ISDN) checkbox, and retain the default values for all remaining fields (**Figure 15**). Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page.

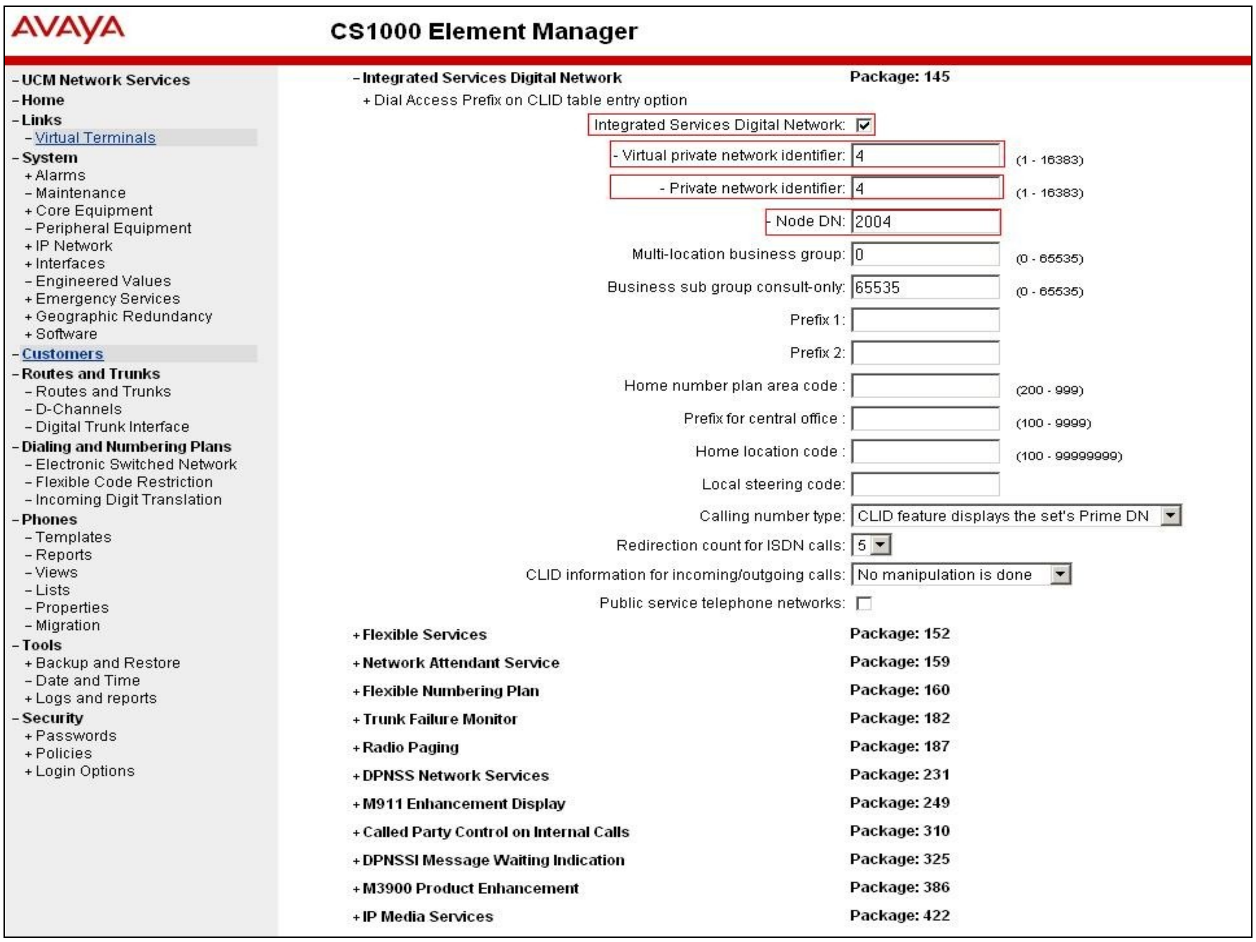

Figure 15 –Customer – ISDN Configurations

5.5.2. Administer SIP Trunk Gateway to Session Manager

a) Select **IP Network** -> **Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** of this CS1000 system. The **Node Details** screen is displayed as shown in **Figure 6, Section 5.2.1.**

b) On the **Node Details** screen, select **Gateway (SIPGw)** (not shown).

c) Under **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following testing values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 16**. The parameters (highlighted in red boxes) are filled in, which were obtained when user creates a SIP Entity on the Session Manager (these are shown in **Section 5.8.4**).

- **Vtrk gateway application**: **SIP Gateway (SIPGw)**
- **SIP domain name**: mtsallstream.com
- **Local SIP port**: 5060
- **Gateway endpoint name**: car2-ssg-mtsallstream
- **Application node ID**: 2004

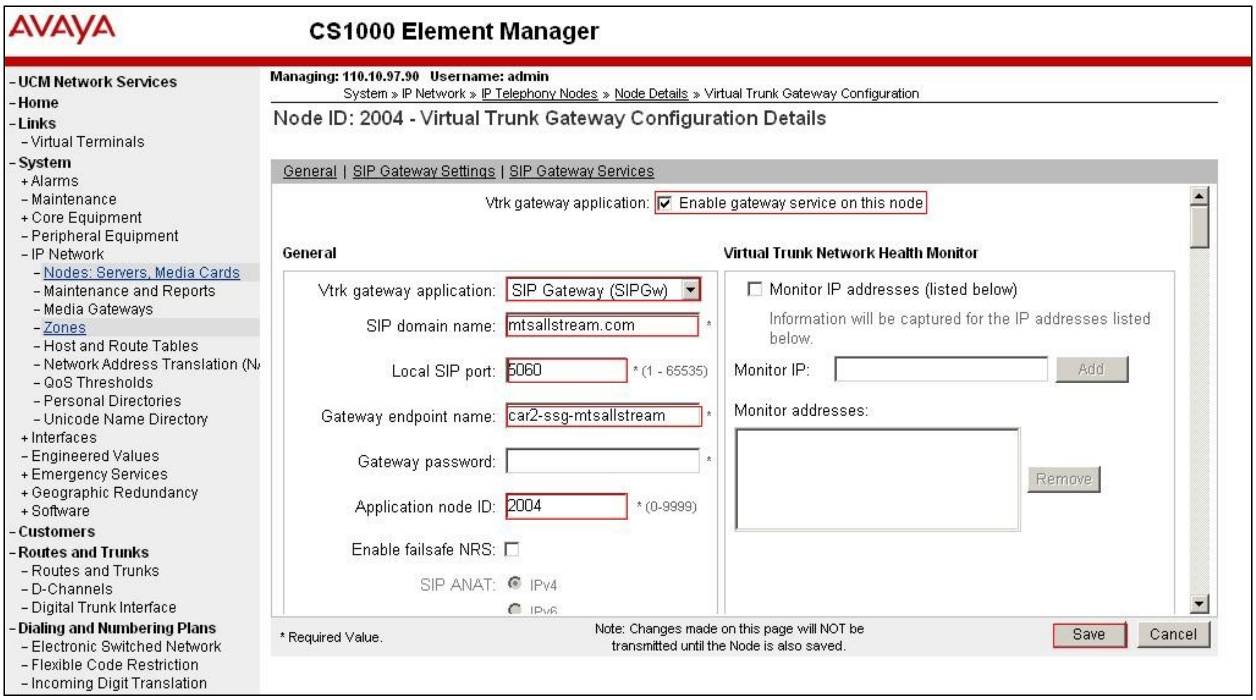

Figure 16 – Virtual Trunk Gateway Configuration Details Page 1

d) Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the IP address of Session Manager and value highlighted in the red box for the specified fields, and retain the default values for the remaining fields as shown in **Figure 17**.

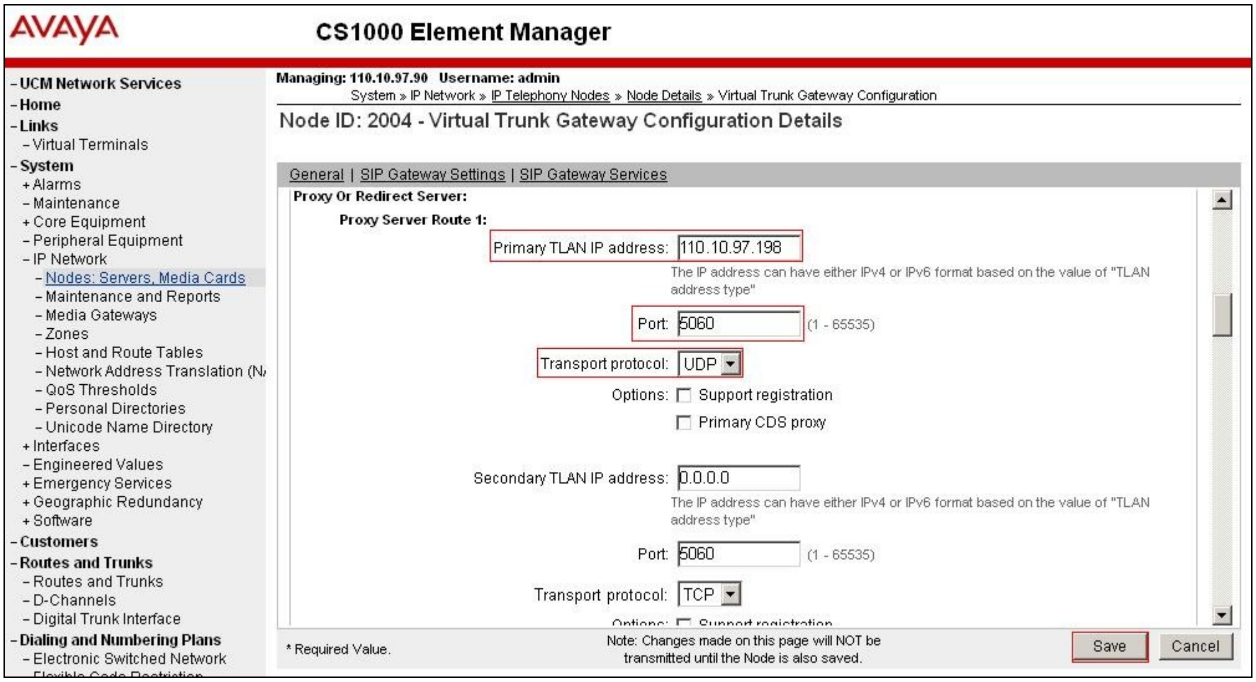

Figure 17 – Virtual Trunk Gateway Configuration Details Page 2

e) On the same page as shown in **Figure 17**, scroll down to the **SIP URI Map** section (**Figure 18**).

Under the **Public E.164 Domain Names**:
- **National**: leave this SIP URI field as blank
- **Subscriber**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

Under the **Public E.164 Domain Names**:
- **UDP**: leave this SIP URI field as blank
- **CDP**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Vacant number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

Then click on the **Save** button.

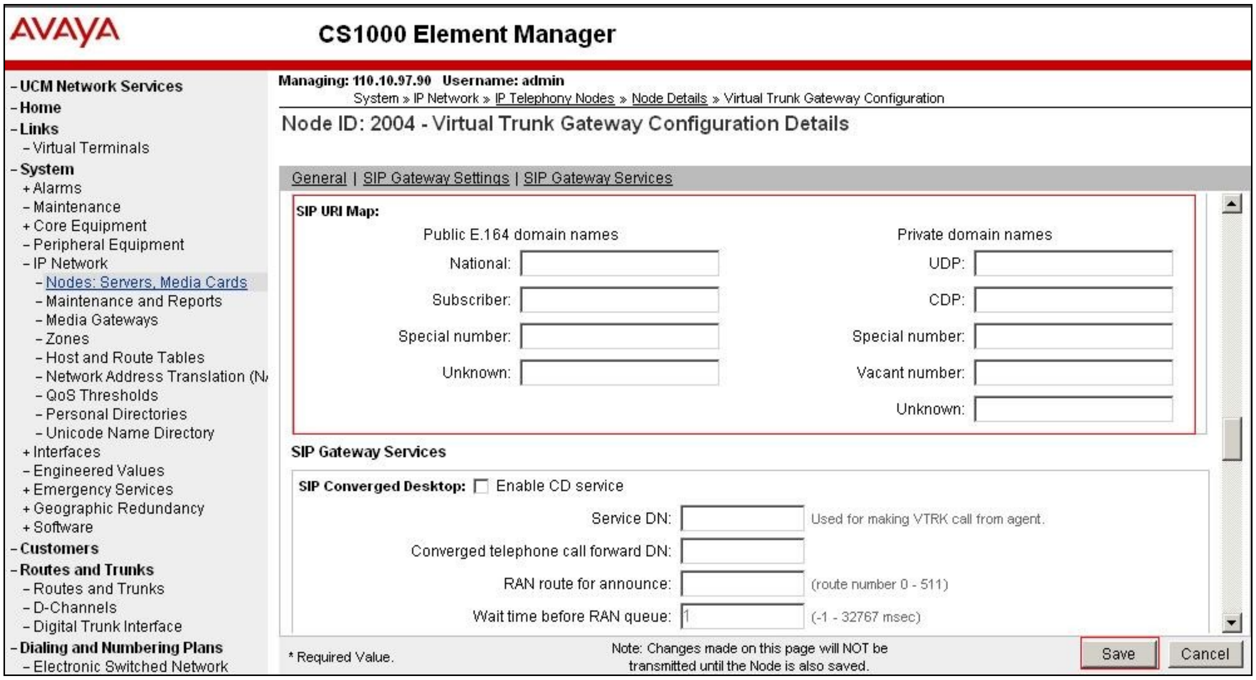

Figure 18 – Virtual Trunk Gateway Configuration Details Page 3

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

5.5.3. Administer Virtual D-Channel

a) 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 as shown in **Figure 19**. Click on **to Add** button**.**

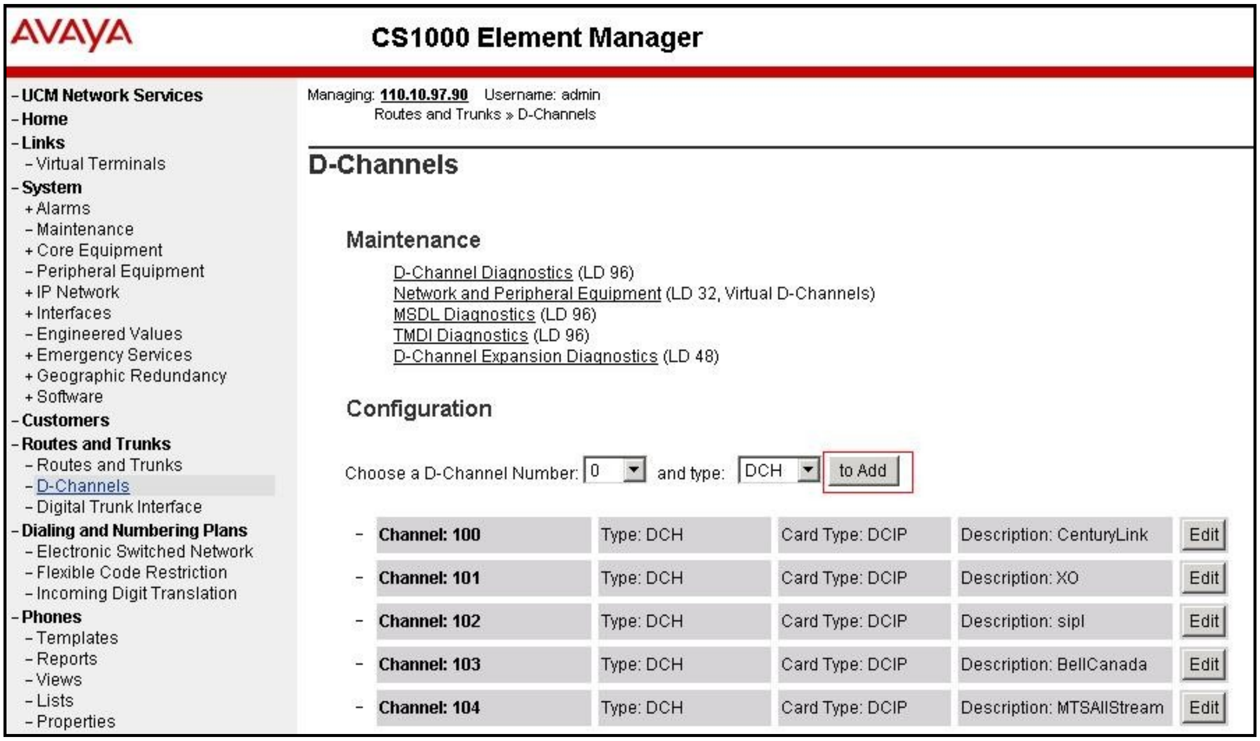

Figure 19 – D-Channels

b) The D-Channels Property Configuration screen is displayed as shown in **Figure 20**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D channel Card Type (CTYP): D-Channel is over IP (DCIP)**
- **Designator (DES)**: A descriptive name
- **Interface type for D-channel (IFC): Meridian Meridian1 (SL1)**
- **Meridian 1 node type: Slave to the controller (USR)**
- **Release ID of the switch at the far end (RLS): 25**
- **Advanced options (ADVOPT):** check on **Network Attendant Service Allowed**

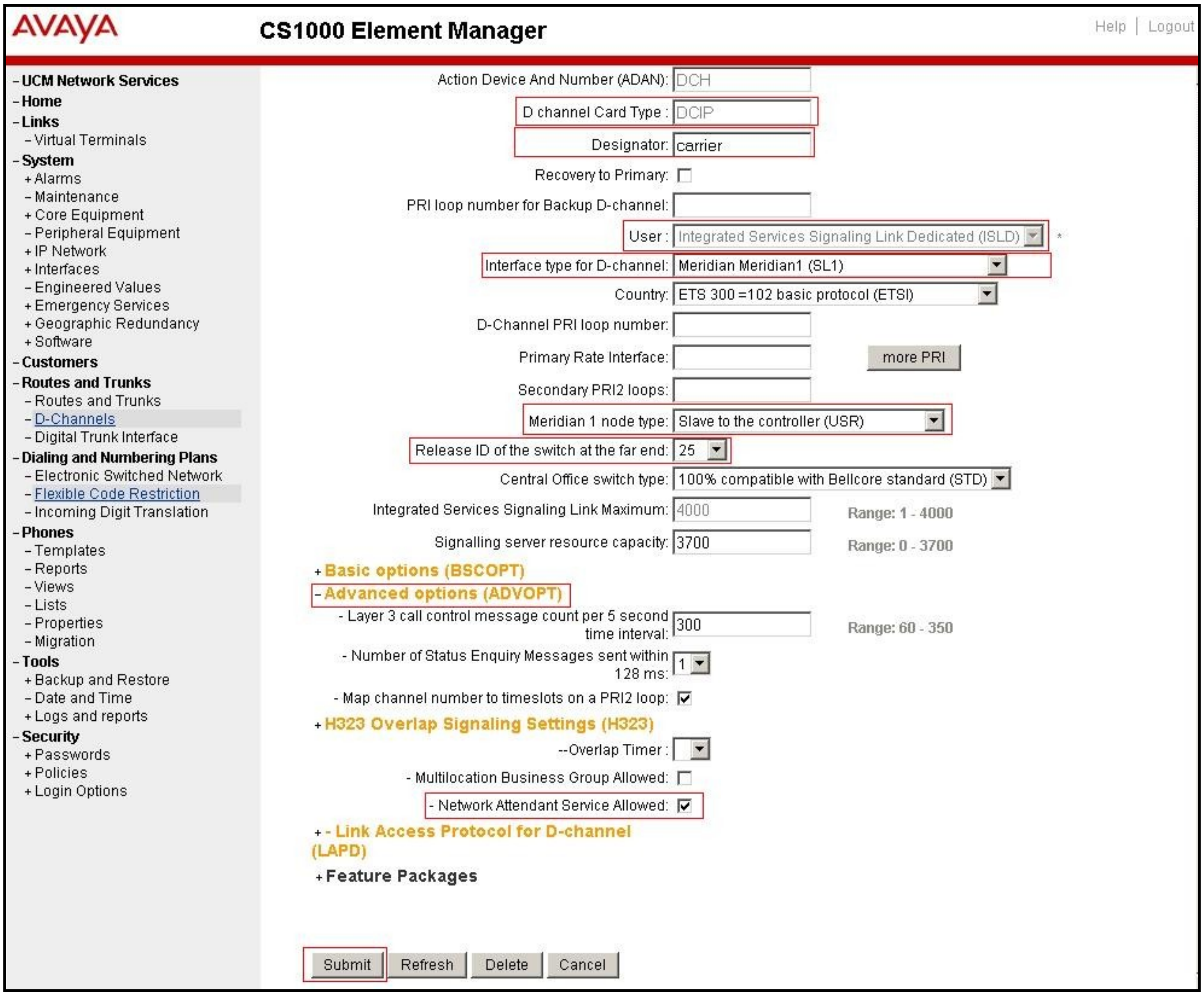

Figure 20 – D-Channels Configuration Details

c) Click on the **Basic Options** and click on the **Edit** button at the **Remote Capabilities** (**RCAP**) attribute. The **Remote Capabilities Configuration** page will appear. Then check on the **ND2** and the **MWI** checkboxes as shown in **Figure 21** and **Figure 22**.

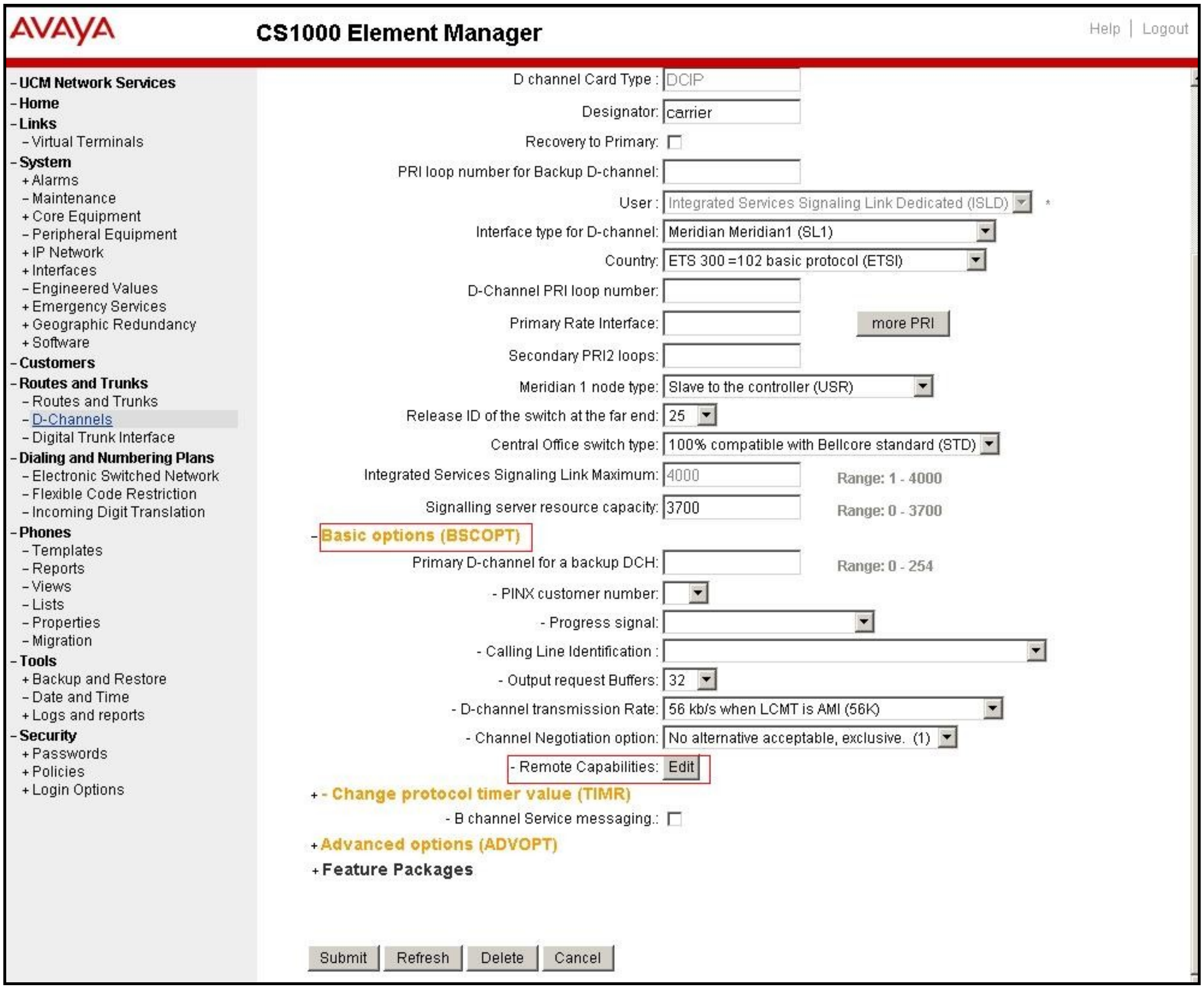

Figure 21 – D-Channels Configuration Details

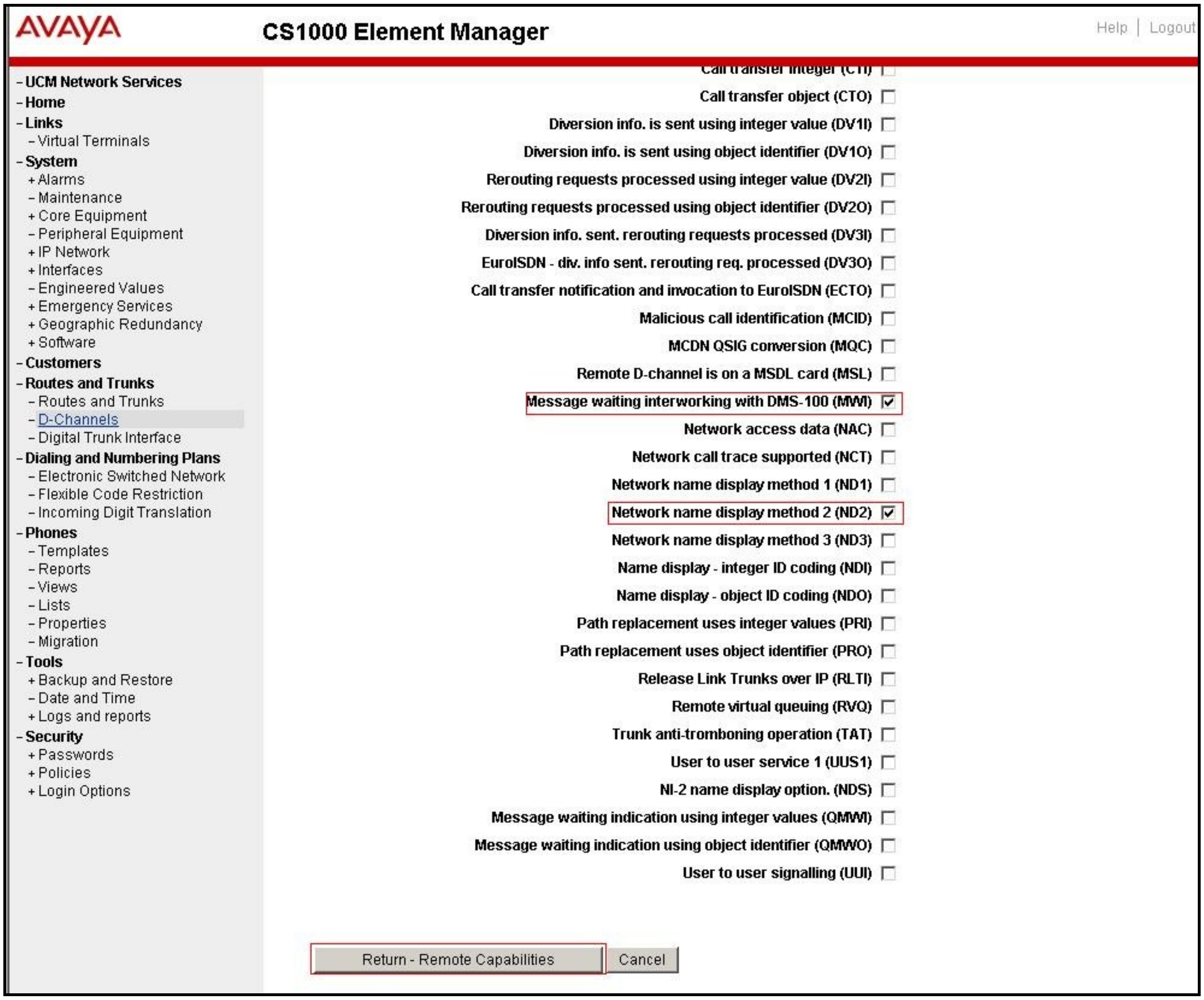

Figure 22 – Remote Capabilities Configuration Details

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

5.5.4. Administer Virtual Super-Loop

Select **System** -> **Core Equipments** -> **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click "**Add**" button to create a new one as shown in **Figure 23**. In this example, Superloop 100 is being added and used.

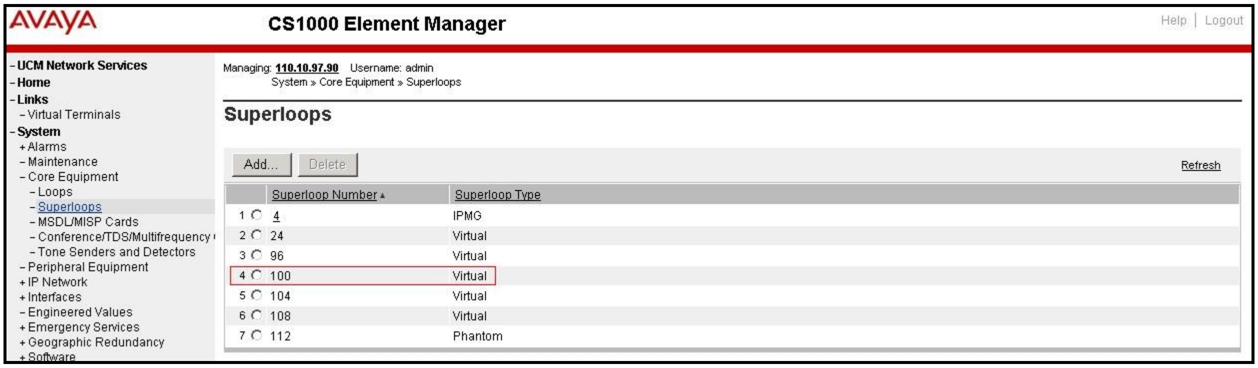

Figure 23 – Administer Virtual Super-Loop

5.5.5. Enable Music for Customer Data Block

a) Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **04**. The system can support more than one customer with different network settings and options. The **Customer 04 Edit** page will appear (not shown). Select the **Feature Packages** option from this page.

b) The screen is updated with a list of F**eature Packages** populated. Select **Enhanced Music** to edit its parameters. Check to enable music for Customer 04, define music route 54 as shown in the redbox of **Figure 24**. The CS1000 system has been pre-configured with music route 54.

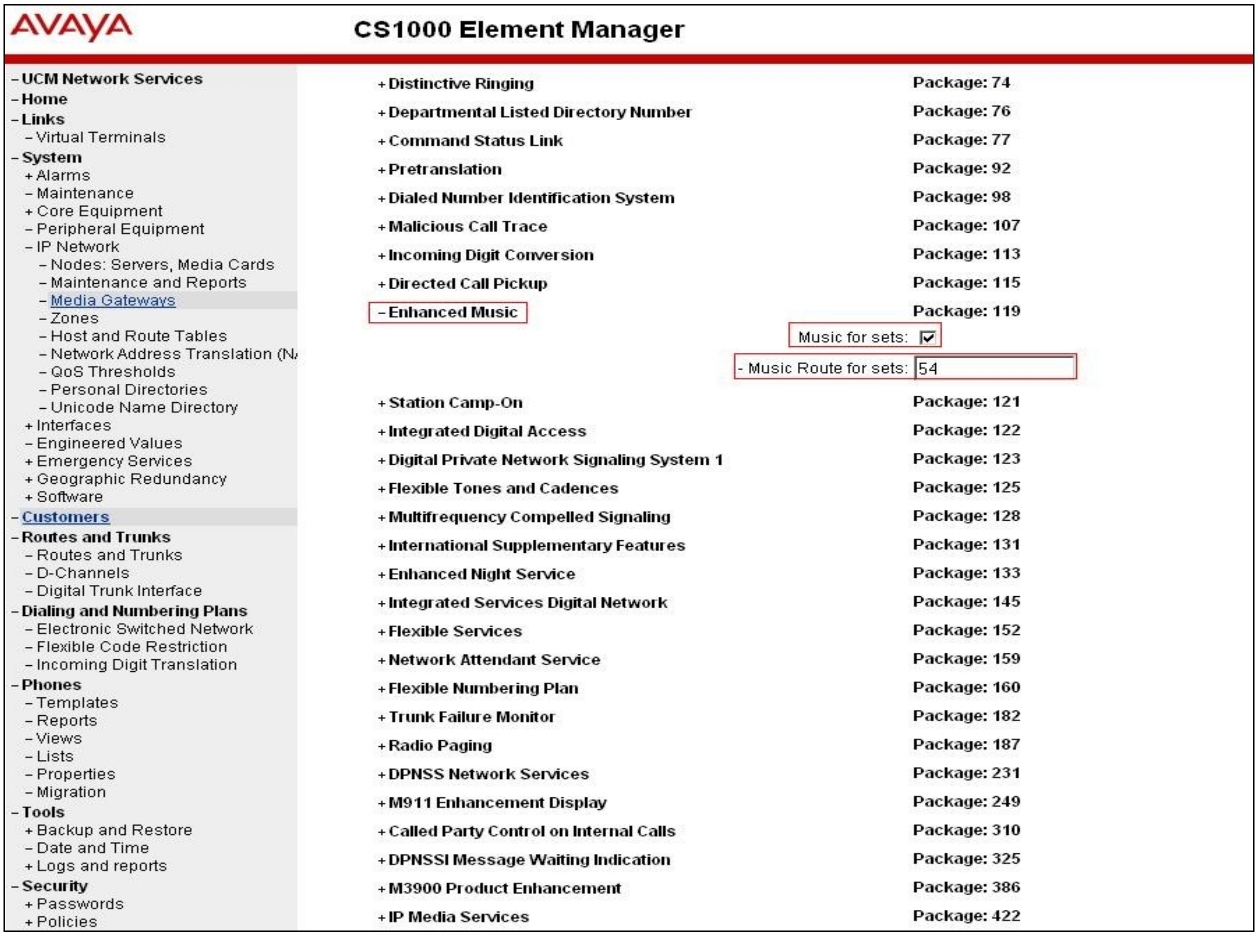

Figure 24 – Enable Music for Customer 04

c) Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page.

5.5.6. Administer Virtual SIP Routes

a) Select **Routes and Trunks** -> **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 04** is being used. Click on the **Add route** button as shown in **Figure 25**.

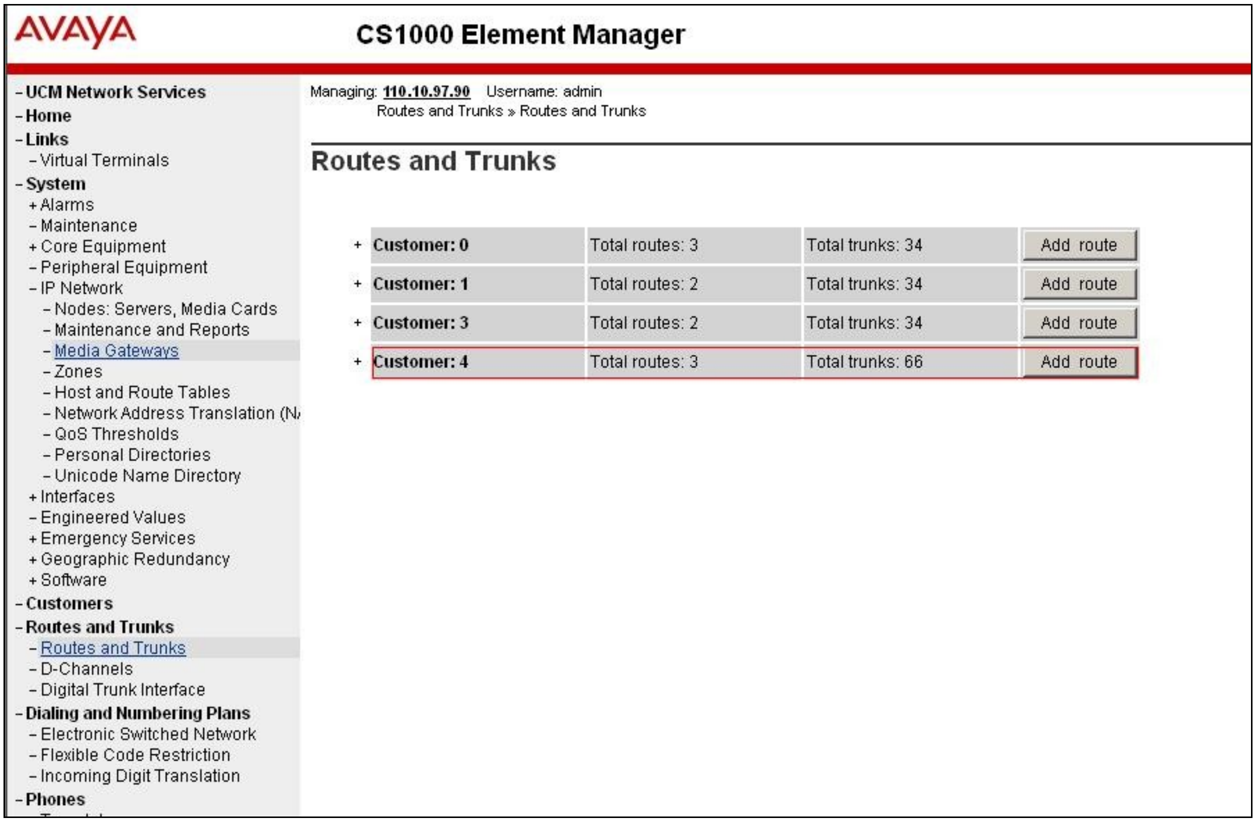

Figure 25 – Add route

b) The **Customer 4**, New **Route Configuration** screen is displayed next. Scroll down until the **Basic Configuration** section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figure 26a**.

- **Route Number (ROUT)**: Select an available route number.
- **Designator field for trunk (DES)**: A descriptive text.
- **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.
- Check the field **The route is for a virtual trunk route (VTRK)**, 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**).

- For the **Node ID of signaling server of this route (NODE)** field, enter the node number 2004 (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. 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.
    - **Mode of operation (MODE)**: Route uses **ISDN Signalling Link (ISLD)**
    - **D channel number (DCH)**: D-Channel number 104 (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.

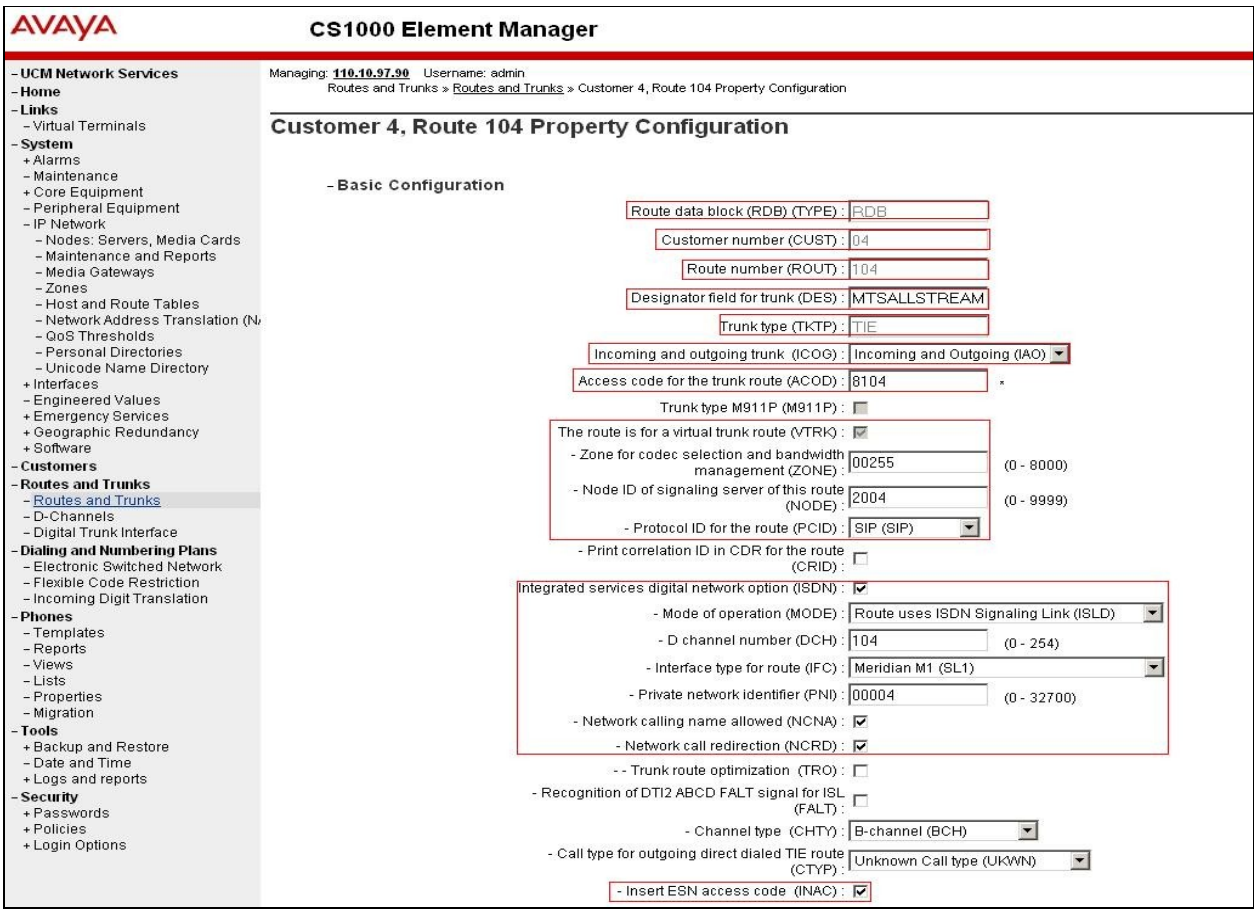

Figure 26a – Route Configuration Details Pages 1

- Click on **Basic Route Options**, check **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 0** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown in **Figure 26b**.

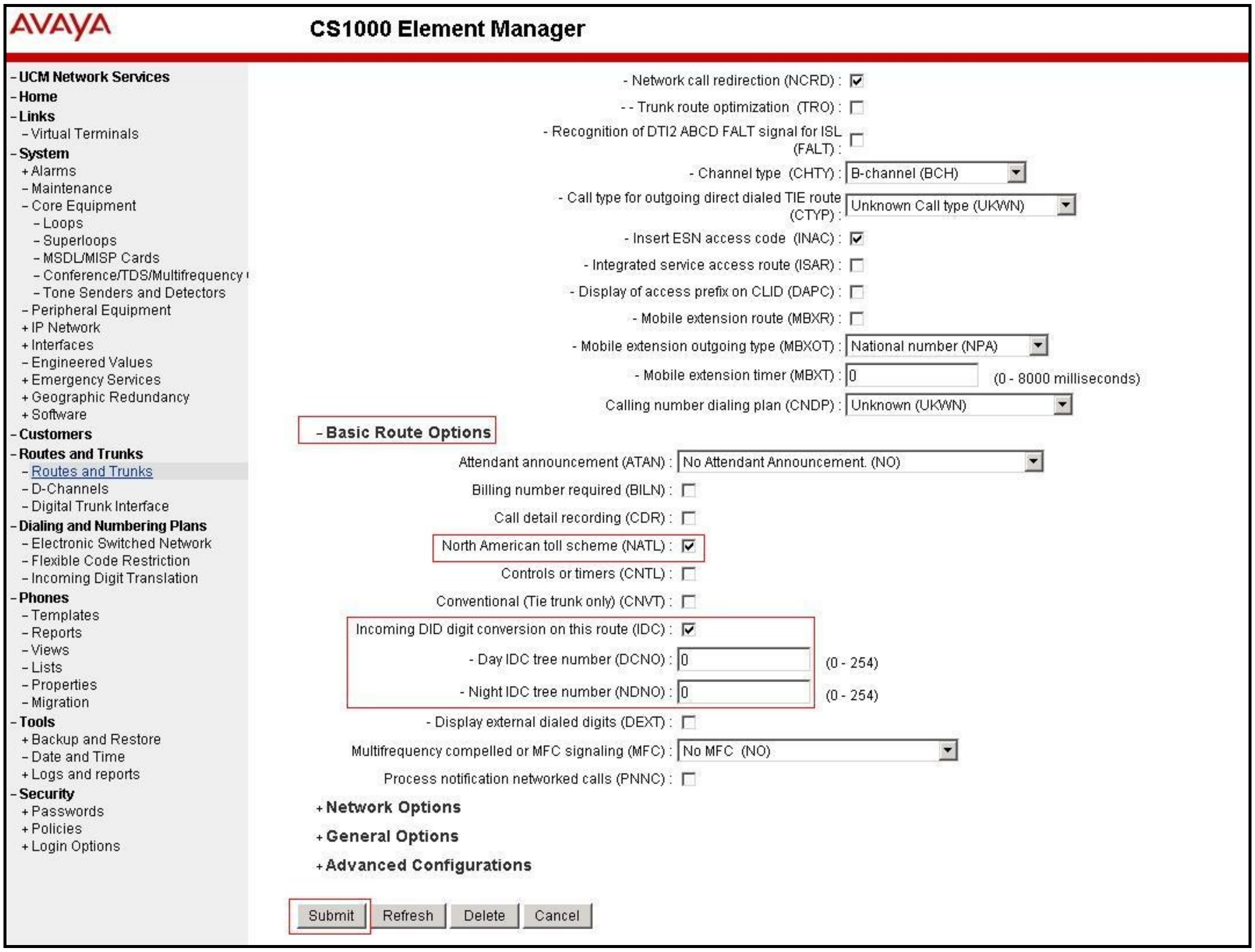

Figure 26b – Route Configuration Details Pages 2

- Click on **Advance Configurations**; check **Music-on-holds** to enable music on hold on the route. Input music route 54 to the boxes as shown in **Figure 26c**. The CS1000 system has been pre-configured with route 54 as a music route.

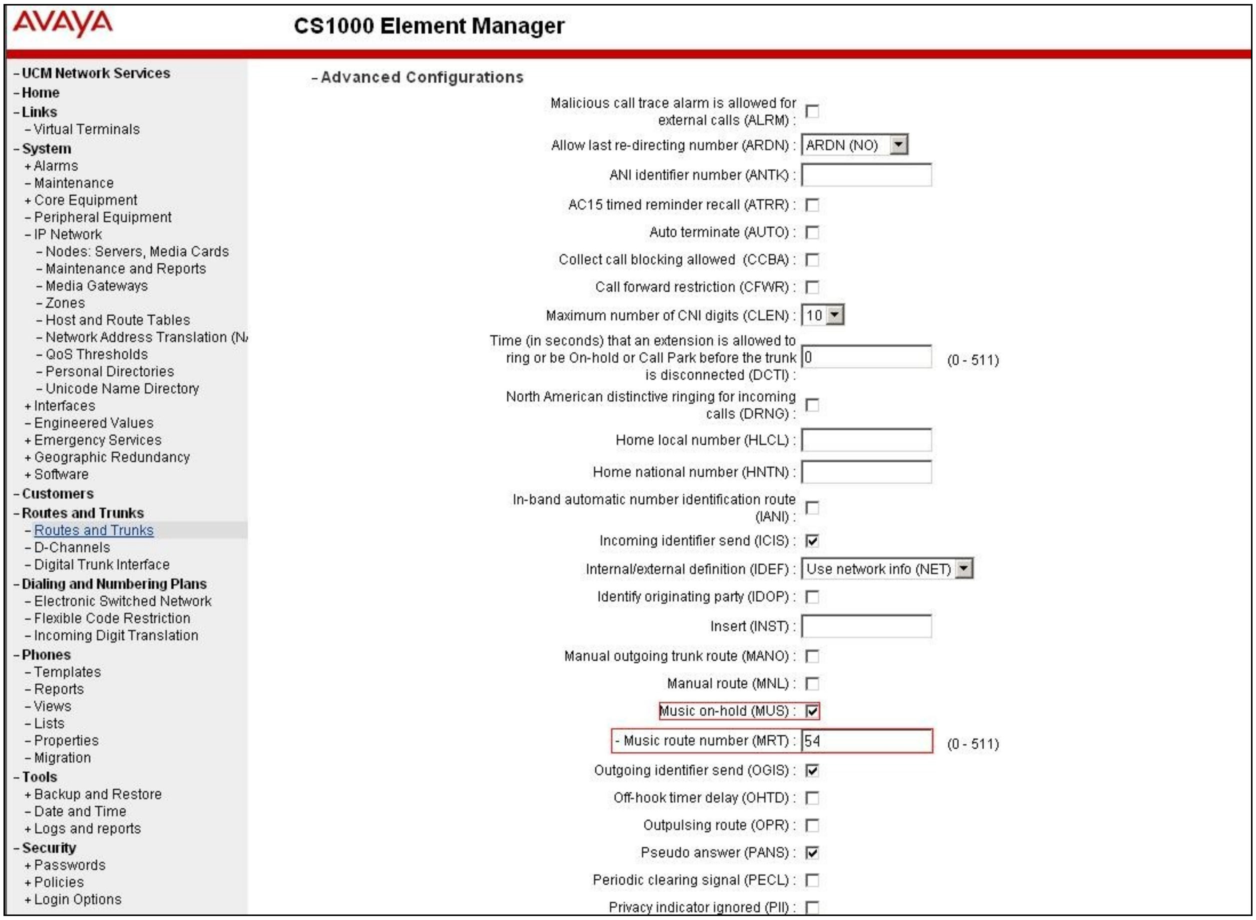

Figure 26c – Route Configuration Details Pages 3

c) Click on the **Submit** button.

5.5.7. Administer Virtual Trunks

a) Continue from **Section 5.5.5**, click **Submit**, the **Routes and Trunks** screen is displayed and updated with the newly added route. In the example, Route 104 was being added. Click on the **Add trunk** button next to the newly added route 104 as shown in **Figure 27**.

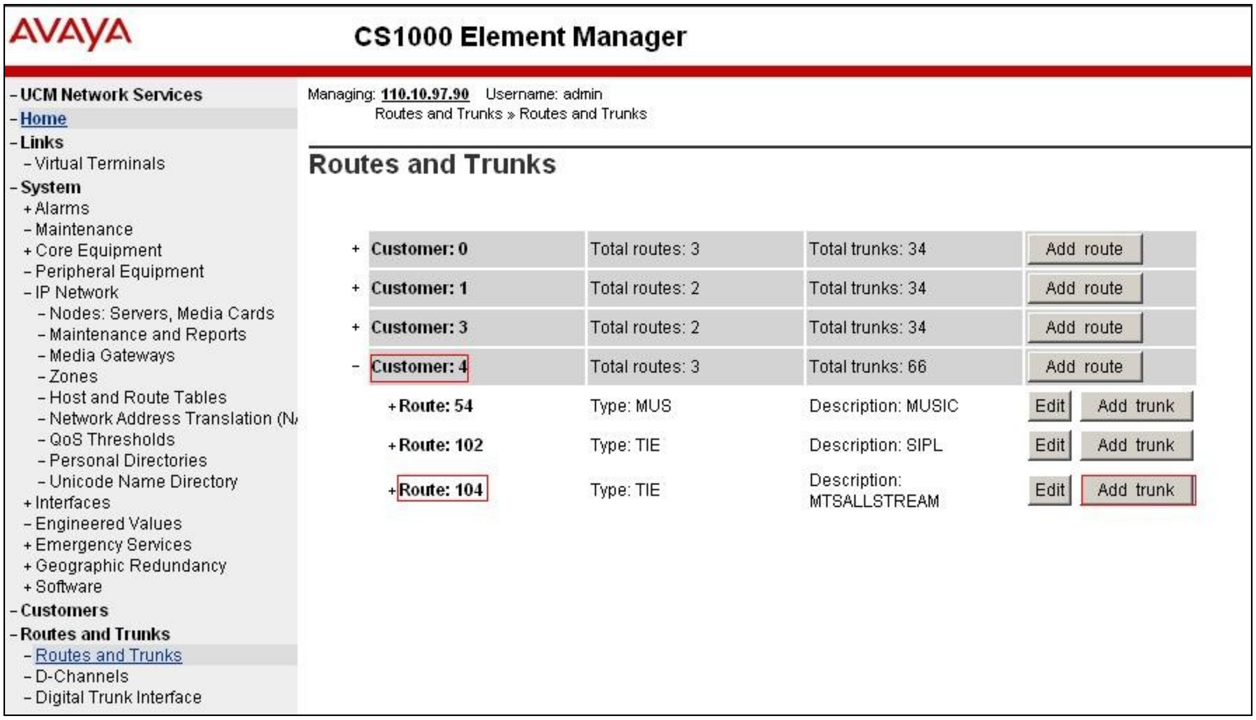

Figure 27 – Route and Trunks

b) The **Customer 4, Route 104, Trunk 1 Property Configuration** screen is displayed in **Figure 28**. Enter the following values for the specified fields and retain the default values for the remaining fields. The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service** (CLS) at the bottom basic trunk configuration page. Click on the **Edit** button as shown in **Figure 28**.

- 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** (**TYPE**): **IP Trunk (IPTI)**
- **Terminal Number** (**TN**): Available terminal number (created in **Section 5.5.4**)
- **Designator field for trunk** (**DES**): A descriptive text
- **Extended Trunk (XTRK): Virtual trunk (VTRK)**
- **Member number** (**RTMB**): Current route number and starting member
- **Start arrangement Incoming** (**STRI**): **Immediate (IMM)**

- **Start arrangement Outgoing (STRO)**: **Immediate (IMM)**
- **Trunk Group Access Restriction (TGAR)**: Desired trunk group access restriction level
- **Channel ID for this trunk** (**CHID**): An available starting channel ID

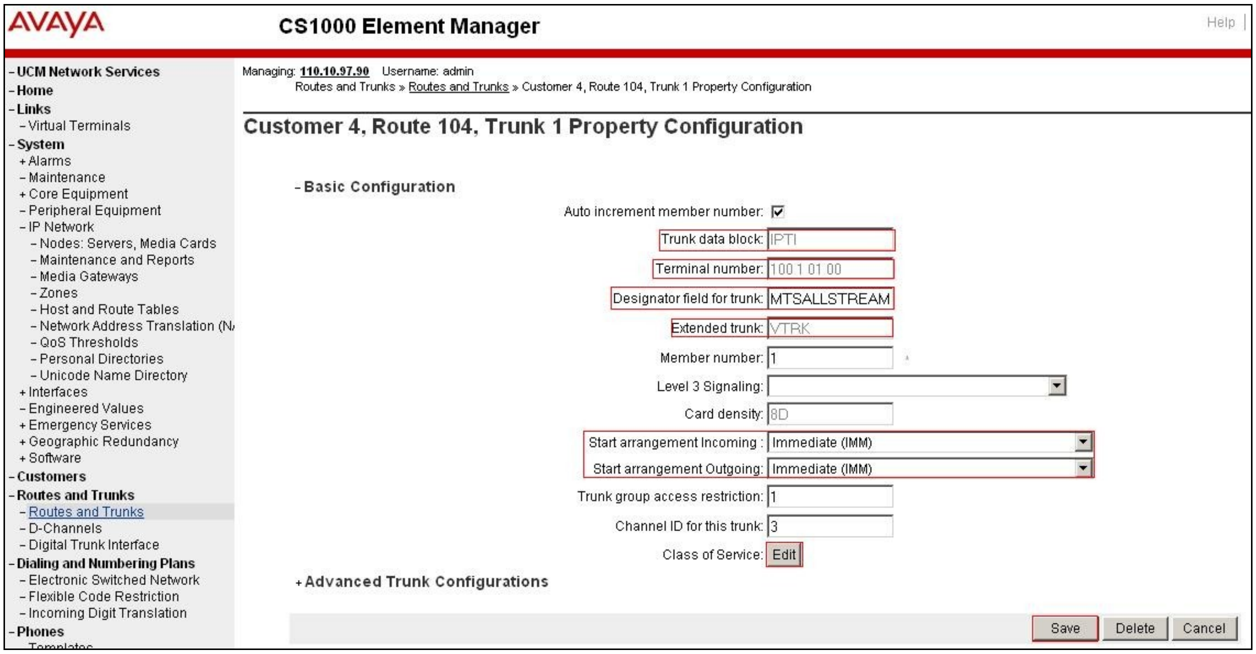

Figure 28 – New Trunk Configuration Details

c) For **Media Security**, select **Media Security Never (MSNV)**. Enter the remaining values for the specified fields as shown in **Figure 29**. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the **Save** button (not shown).

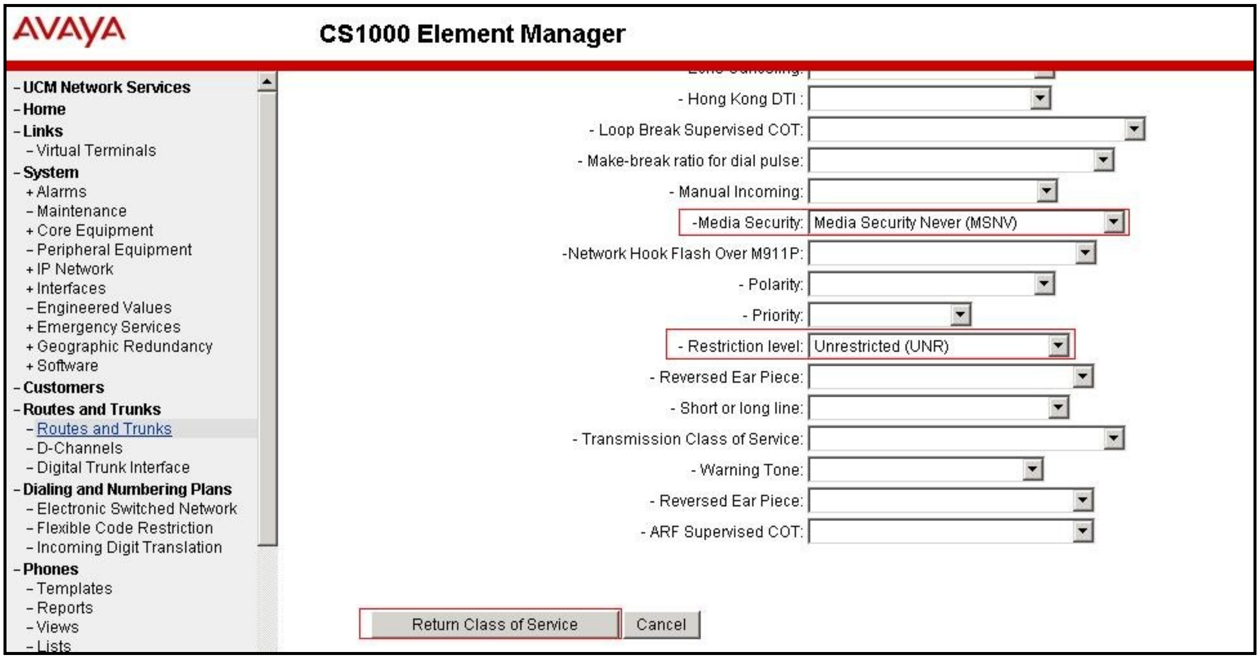

Figure 29 – Class of Service Configuration Details Page

5.5.8. Administer Calling Line Identification Entries

a) Select **Customers** > **04** > **ISDN and ESN Networking**. Click on **Calling Line Identification Entries** as shown in **Figure 30**.

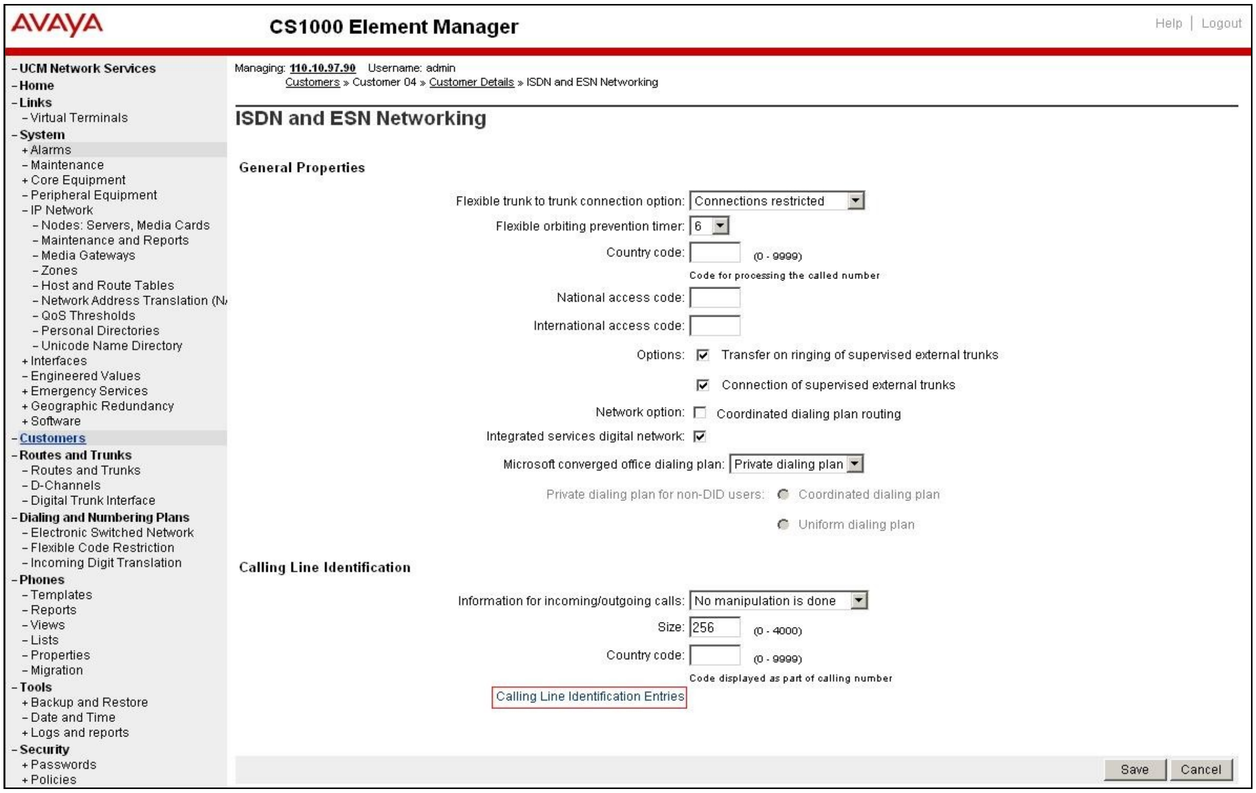

Figure 30 – ISDN and ESN Networking

b) Click on **Add** as shown in **Figure 31**.

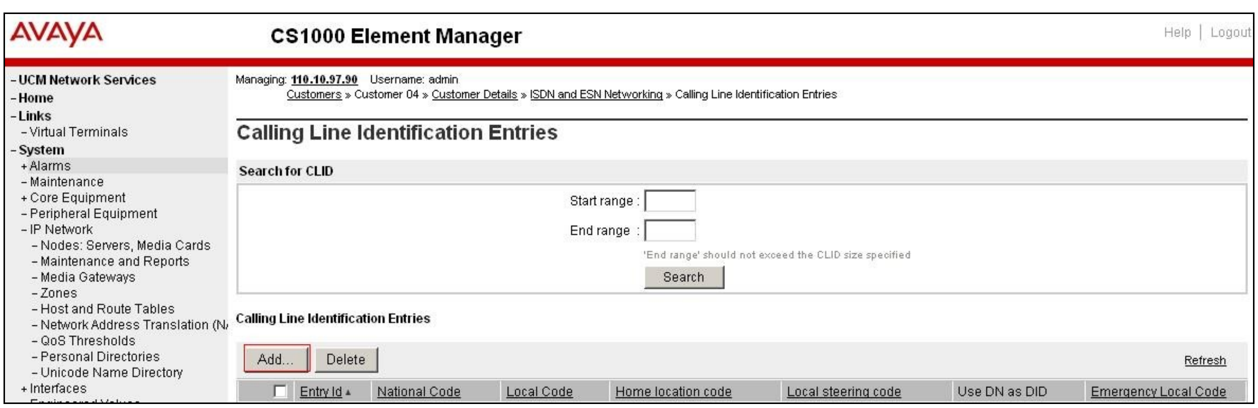

Figure 31 – Calling Line Identification Page

c) Add entry **0** as shown in **Figure 32**

- **National Code**: leave as blank
- **Local Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits – 647776. This **Local Code** will be used for call display purpose of outbound international call configuration in **Section 5.6.6** where the **Special Number 0** is associated with Call Type = Unknown.
- **Home Location Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits - 647776. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code**: input prefix digits assigned by Service Provider, in this case it is 6 digits - 647776. This **Local Steering Code** will be used for call display purpose for Call Type = Local Subscriber (NXX).
- **Calling Party Name Display**: Uncheck for **Roman characters**.

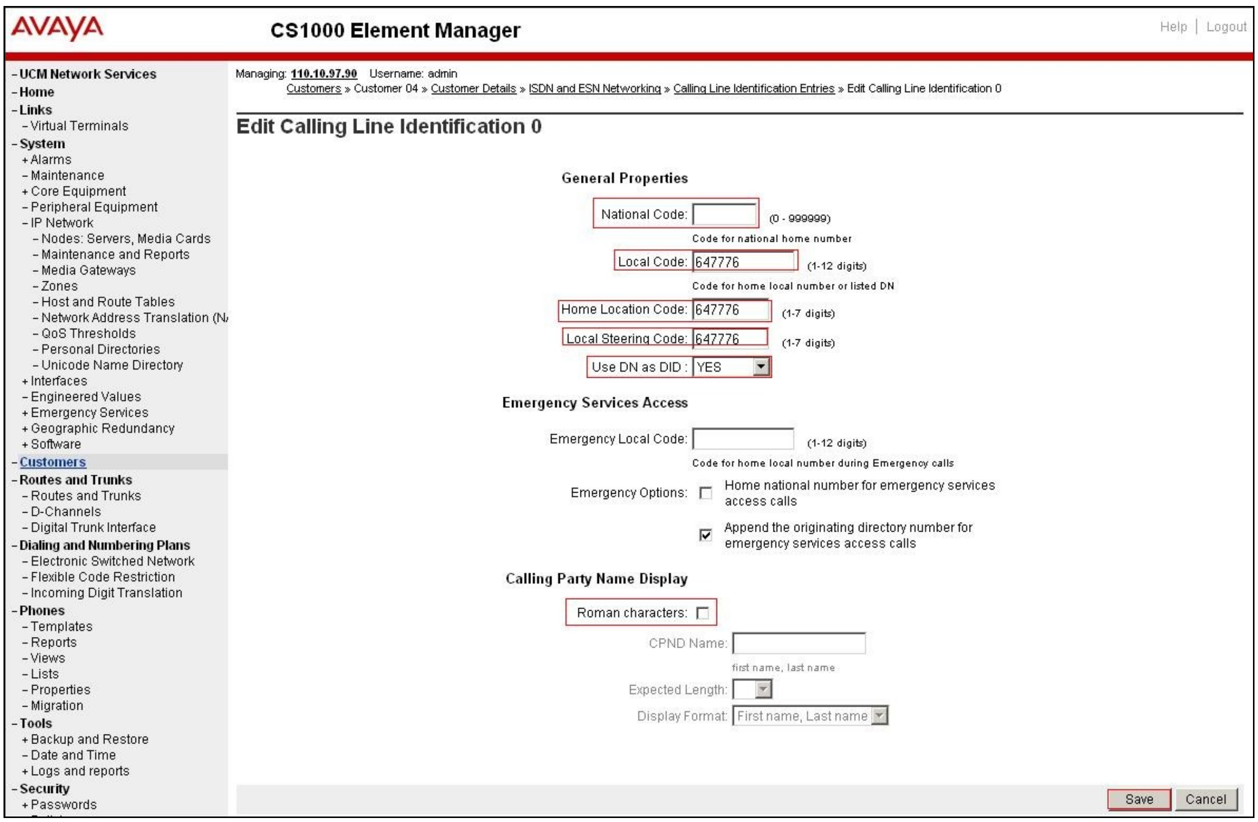

Figure 32 – Edit Calling Line Identification 0

d) Click on **Save**.

5.5.9. Enable External Trunk to Trunk Transferring

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

a) Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
b) Allow External Trunk To Trunk Transferring for **Customer Data Block** by using LD 15.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600176    USED U P: 8325631 954062    TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 4
OPT
…
TRNX YES
EXTT YES
…
```

5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen. **Select ESN Access Code and Parameters (ESN)** as shown in **Figure 33**.

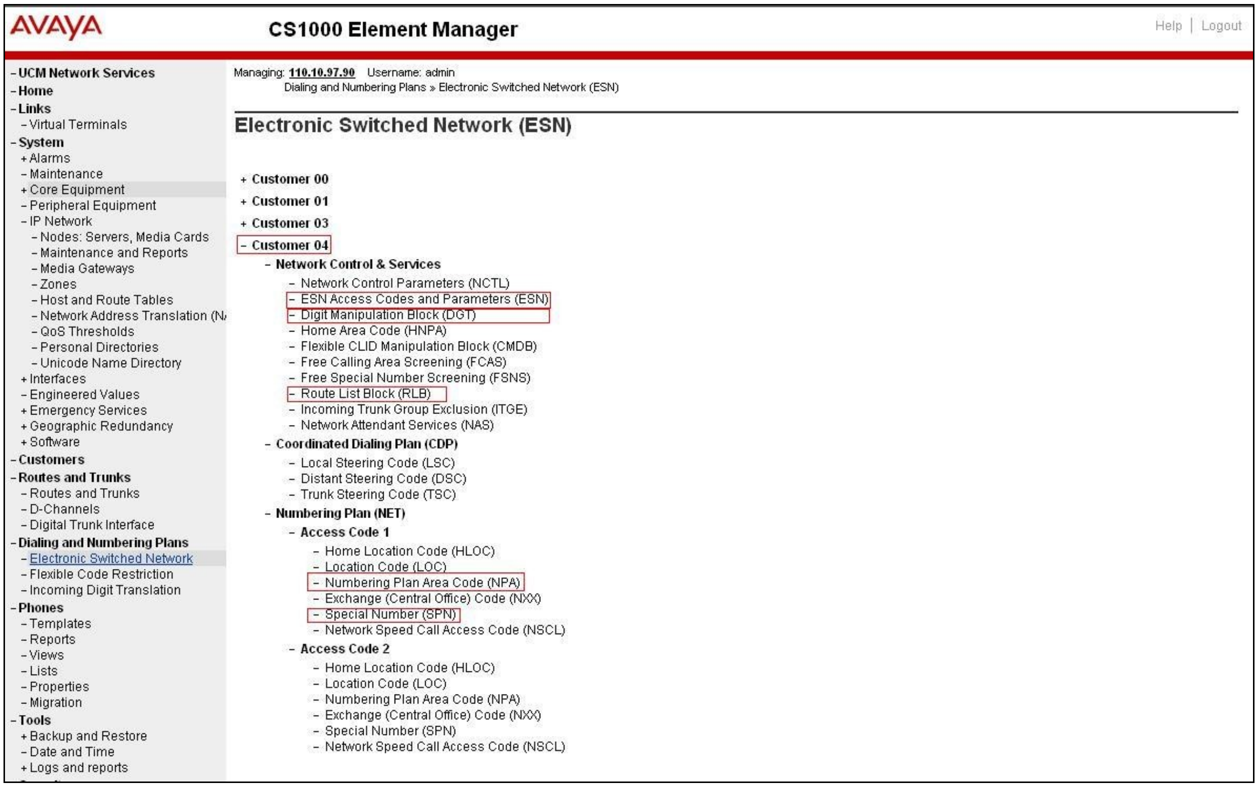

Figure 33 – Electronic Switch Network (ESN)

b) In the **ESN Access Codes and Basic Parameters** page, define **NARS/ BARS Access Code 1** as shown in **Figure 34**.

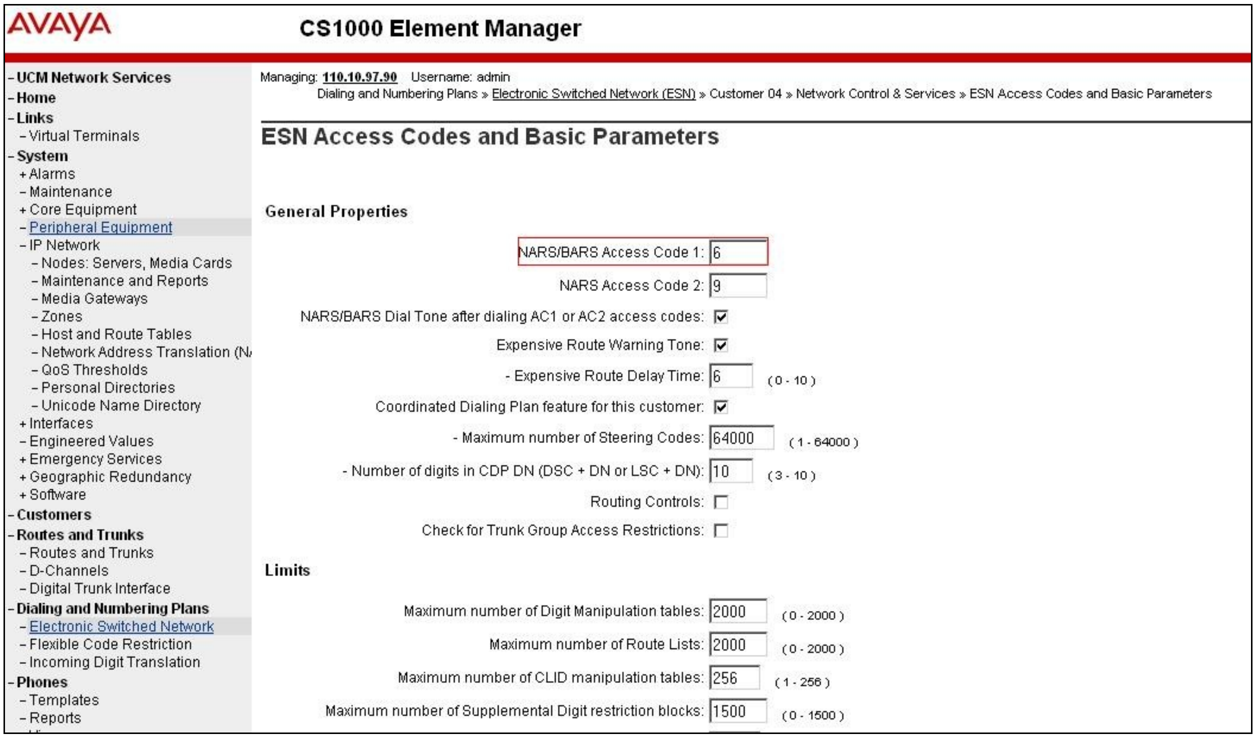

Figure 34 – ESN Access Codes and Basic Parameters

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

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

a) Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
b) In LD 15, change Customer Net_Data block by disabling NPA and SPN to be associated to Access Code 2. It means Access Code 1 will be used for NPA and SPN calls.

```
>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 4
OPT
AC2 xNPA xSPN
FNP
CLID
…
```

c) Verify Customer Net_Data block by using LD 21.

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 4

TYPE NET_DATA
CUST 01
OPT RTA
AC1 INTL NPA SPN NXX LOC
AC2
FNP YES
…
```

5.6.3. Digit Manipulation Block (DMI)

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Digit Manipulation Block** (DGT) as shown in **Figure 33**.

b) In the Choose a DMI Number field, select an available DMI from the drop-down list and click **to Add** as shown in **Figure 35**.

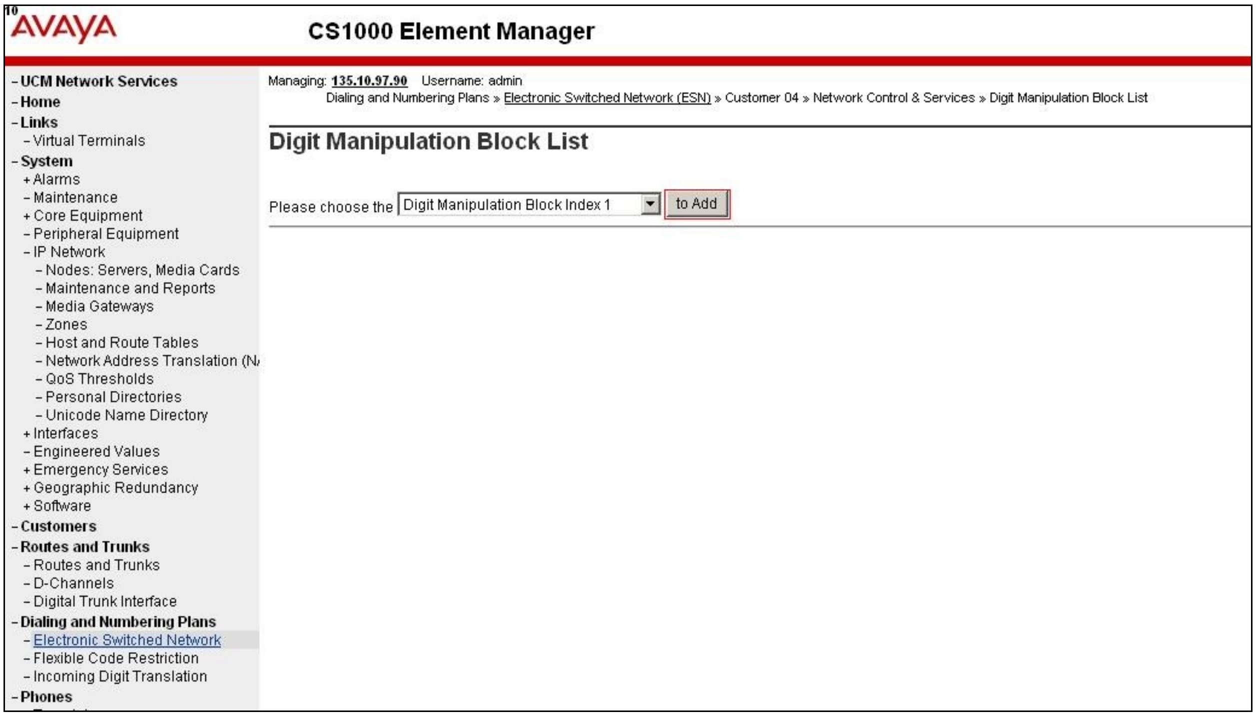

Figure 35 – Digit Manipulation Block List

c) Enter **0** for the **Number of leading digits to be Deleted** (Del) field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits** (CTYP) and then click **Submit** as shown in **Figure 36**.

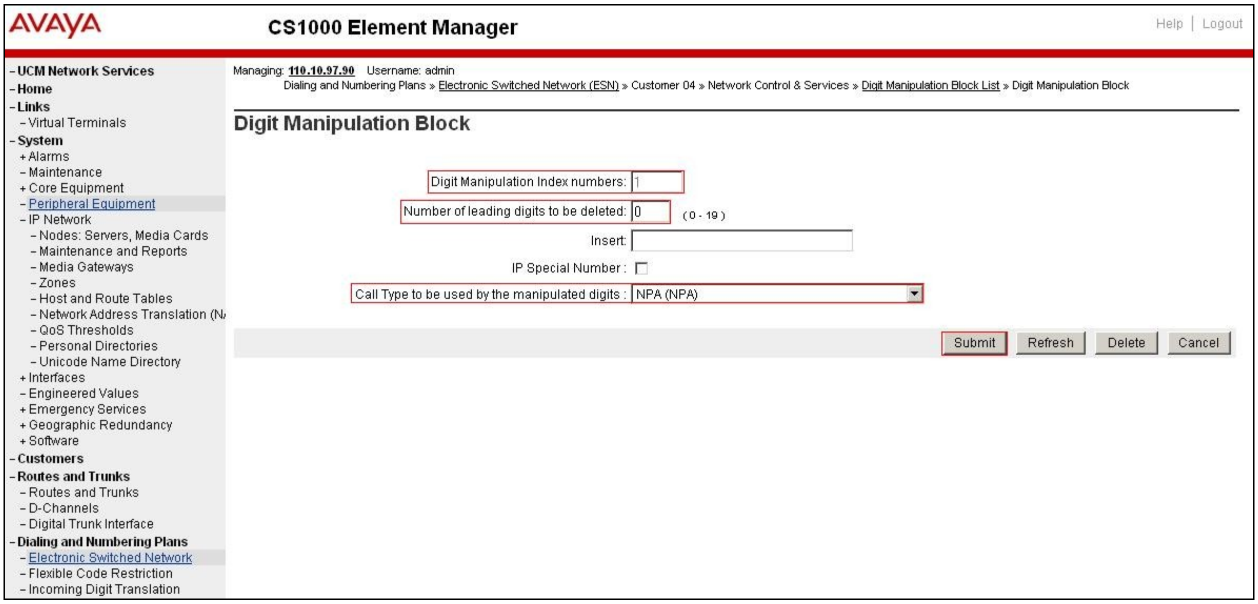

Figure 36 – Digit Manipulation Block

5.6.4. Route List Block (RLB) (RLB 104)

This section shows how to add a RLB associated with the DMI created in **Section 5.6.3**.

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Route List Block** (RLB) as shown in **Figure 33**.
b) Select an available value in the textbox for the **route list index** and click on the "**to Add"** button (in this case is 104) (**Figure 37**).

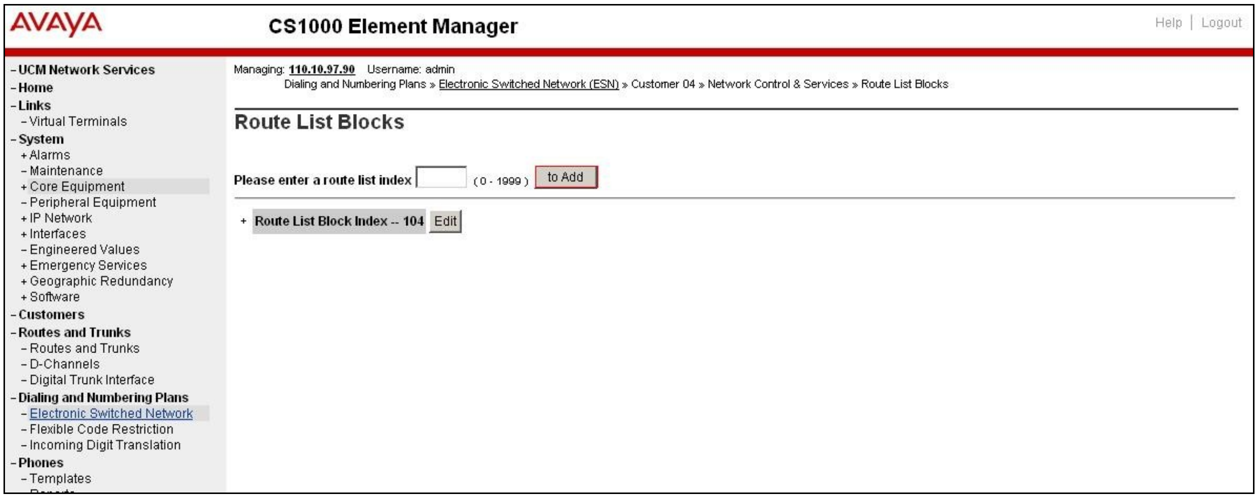

Figure 37 – Route List Blocks

c) Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 38**). Scroll down to the bottom of the screen, and click on the **Submit** button.

- **Route number** (ROUT): 104 (created in **Section 5.5.5**)
- **Digit Manipulation Index** (DMI): 1 (created in **Section 5.6.3**)

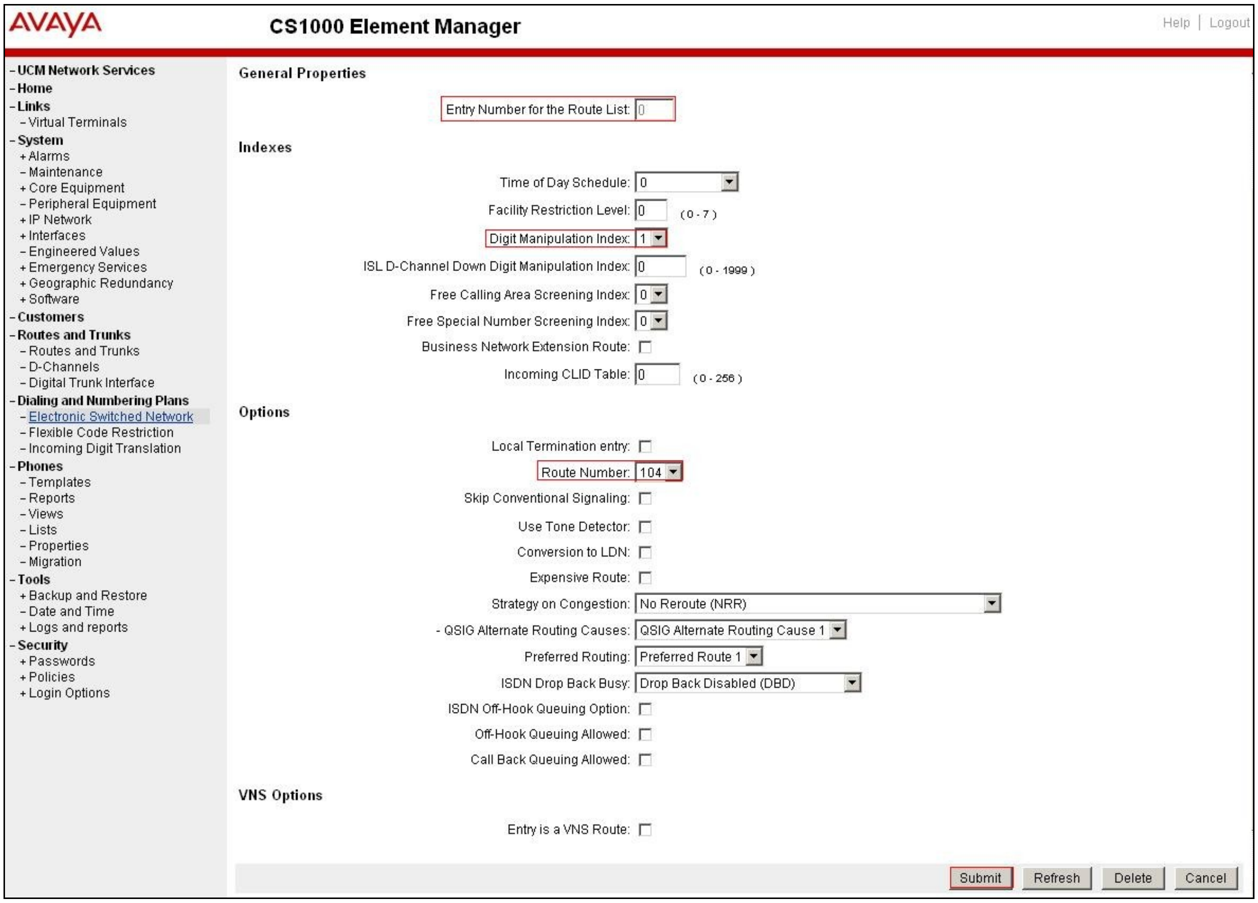

Figure 38 – Route List Blocks Configuration Details

5.6.5. Inbound Call Digit Translation

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

a) 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 (**Figure 39**).

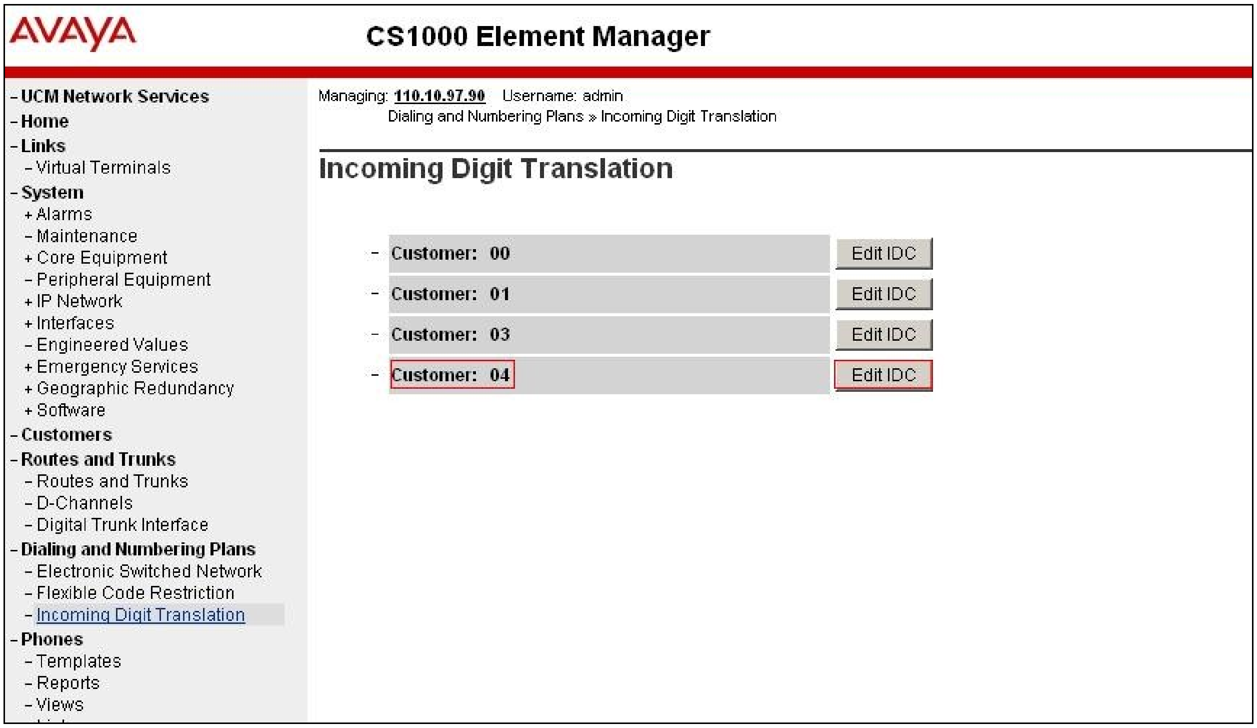

Figure 39 – Incoming Digit Translation

b) Click on **New DCNO** to create the digit translation mechanism. In this example, Digit Conversion Tree Number (**DCN0**) **0** has been created as shown in **Figure 40**.

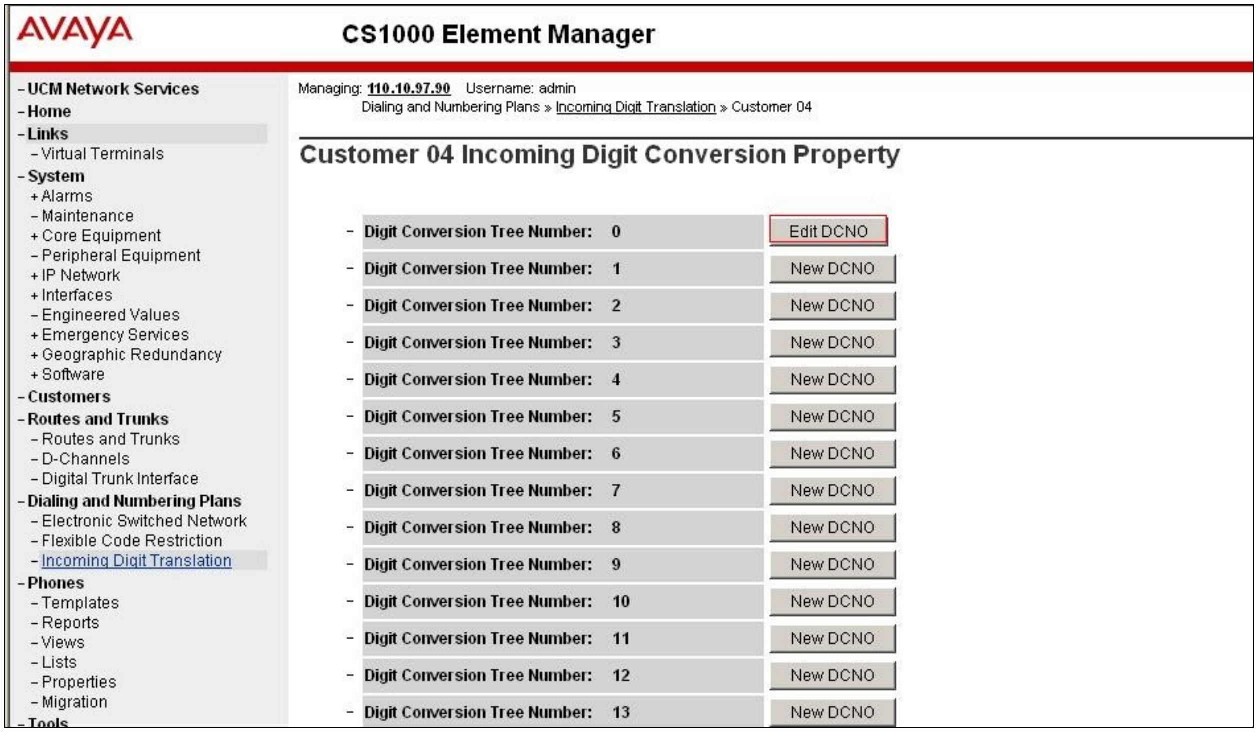

Figure 40 – Incoming Digit Conversion Property

c) Detail configuration of the **DCNO** is shown in **Figure 41**. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 system phones DN. This **DCN0** has been assigned to route 104 as shown in **Figure 26**.

In the following configuration, incoming calls from PSTN with prefix 64777612XX will be translated to CS1K DN 12XX. The DID 6477761233 is translated to 3111 for Voicemail accessing purpose.

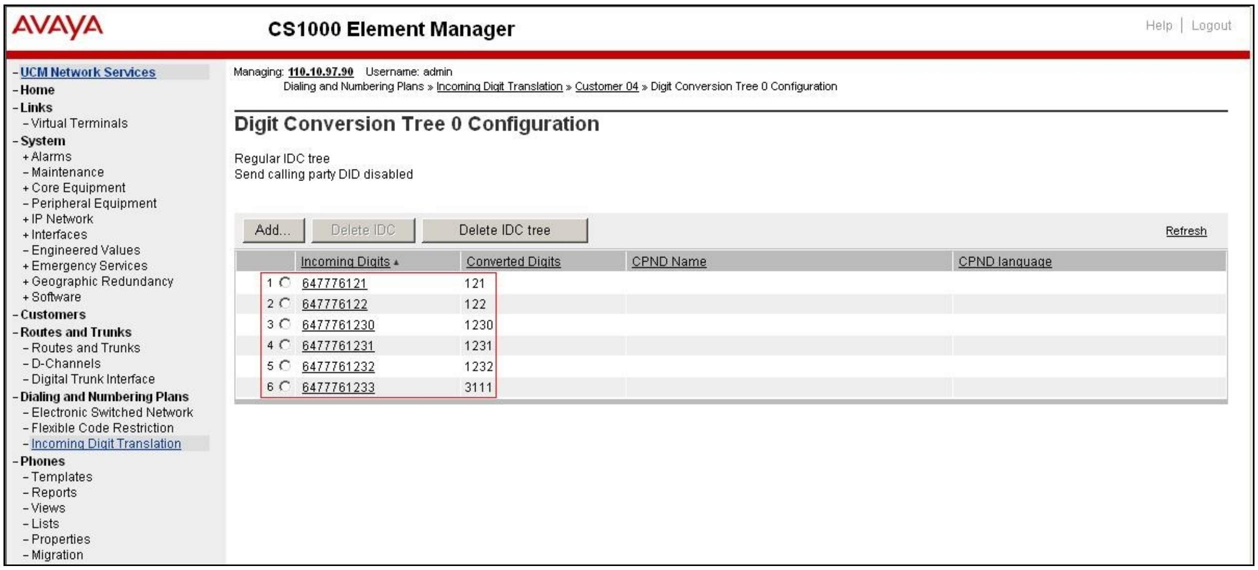

Figure 41 – Digit Conversion Tree Configuration

5.6.6. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing. For example, **0** to reach Service Provider operator, **0+10** digits to reach Service Provider operator assistant, **011** prefix for international call, **1** for national long distance call, **411**, **911** and so on.

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Special Number** (SPN) as shown in **Figure 33.**
b) Enter SPN and then click on the "**to Add**" button. **Figure 42** shows all the special numbers used for this testing.

Special Number: 0

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number)
- **CallType:** NONE
- **Route list index:** 104, created in **Section 5.6.4**

Special Number: 1

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number)
- **CallType**: NATL
- **Route list index**: 104, created in **Section 5.6.4**

Special Number: 411

- **Flexible length**: 3
- **CallType**: NATL
- **Route list index**: 104, created in **Section 5.6.4**

Special Number: 911

- **Flexible length**: 3
- **CallType**: NATL
- **Route list index**: 104, created in **Section 5.6.4**

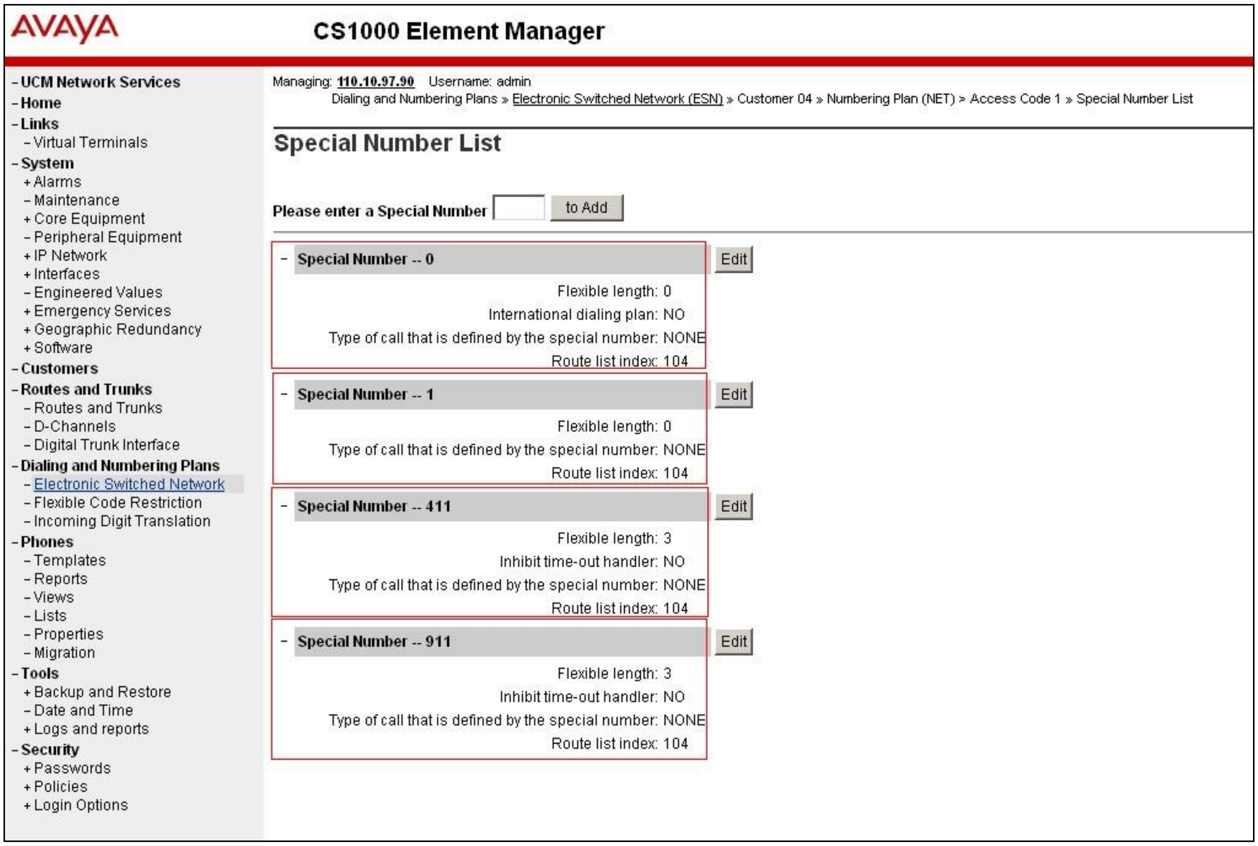

Figure 42 – Special Number List

5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Numbering Plan Area Code** (NPA) as shown in **Figure 33**.
b) Enter area code desired in the textbox and click on the "**to Add"** button. **Figure 43** shows NPA numbers **613** and **416** were configured for this testing. These codes are associated to the SIP route.

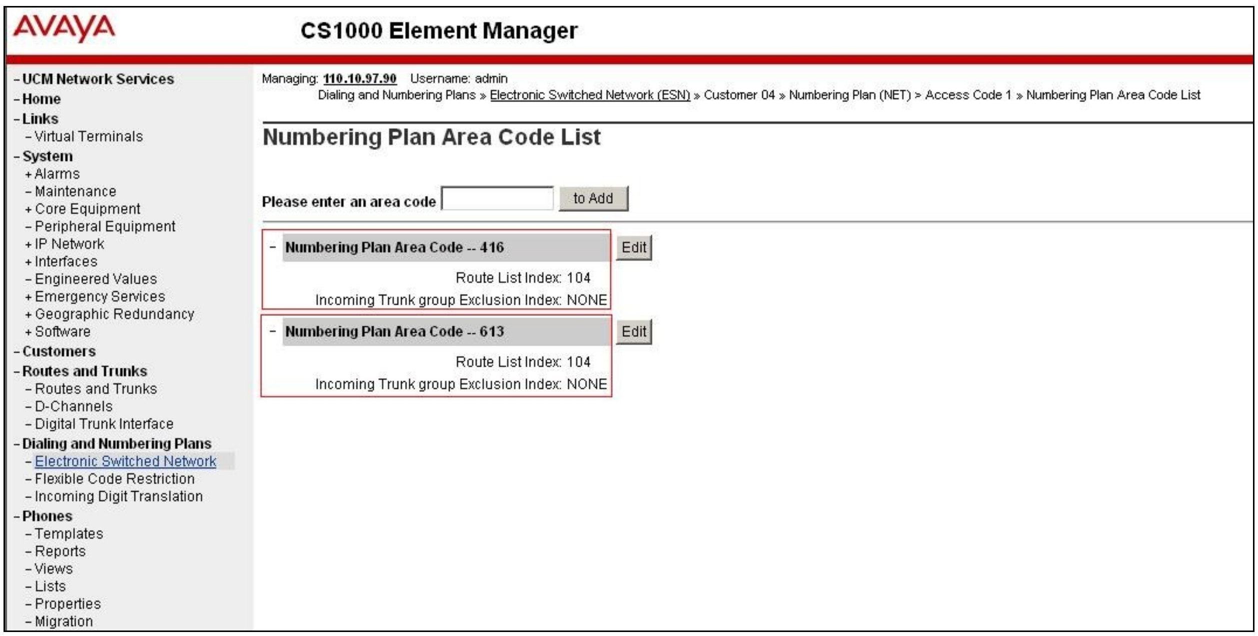

Figure 43 – Numbering Plan Area Code List

5.7. Administer Phone

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

5.7.1. Phone creation

a) Refer to **Section 5.5.4** to create a virtual super-loop - **108** used for IP phone.
b) Refer to **Section 5.4.1** to create a bandwidth zone - **10** for IP phone.
c) Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
d) Create an IP phone by using LD 11.

```
REQ: prt
TYPE: 2002p2
TN   108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED
KEM_RANGE

DES  MTS
TN   108 0 00 15  VIRTUAL
TYPE 2002P2
CDEN 8D
CTYP XDLC
CUST 4
NUID
NHTN
CFG_ZONE 00010
CUR_ZONE 00010
MRT
ERL  12345
ECL  0
FDN  1230
TGAR 2
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 HFA 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 FITD 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
    KEM2 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD
CPND_LANG ENG
RCO  0
HUNT 1230
LHK  0
PLEV 02
PUID
UPWD
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 SCR 1223 0     MARP
       CPND
        CPND_LANG ROMAN
         NAME MTS i2002p2
         XPLN 13
         DISPLAY_FMT FIRST,LAST
    01
    02 MSB
    03
    04
    05
    06
    07
    08
    09
    10
    11
    12
    13
    14
    15
    16
    17 TRN
    18 AO6
    19 CFW 16
    20 RGA
    21 PRK
    22 RNP
    23
    24 PRS
    25 CHG
    26 CPN
    27
```

```
    28
    29
    30
    31
DATE  8 AUG 2011


NACT
```

5.7.2. Enable Privacy for Phone

In this section, it shows how to enable Privacy for a phone by changing its class of service (CLS). By modifying the configuration of the phone created in **Section 5.7.1**, the display of outbound calls will be changed appropriately.

a) To hide display name, set CLS to **namd**. CS1000 will include “Privacy:user” in the SIP message header before sending to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN   108 0 0 15
SCH3928
TN   108 0 0 15
ECHG yes
ITEM cls namd
…
```

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

```
>ld 11
REQ: chg
TYPE: 2002p2
TN   108 0 0 15
SCH3928
TN   108 0 0 15
ECHG yes
ITEM cls ddgd
…
```

c) To hide display name and number, set CLS to **namd, ddgd**. CS1000 will include "Privacy:id, user" in the SIP message header before sending to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN   108 0 0 15
SCH3928
TN   108 0 0 15
ECHG yes
ITEM cls namd ddgd
…
```

d) To allow display name and number, set CLS to **nama, ddga**. CS1000 will send header "Privacy:none" to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN   108 0 0 15
SCH3928
TN   108 0 0 15
ECHG yes
ITEM cls nama ddga
…
```

5.7.3. Enable Call Forward for Phone

In this section, it shows how to configure Call Forward feature at the system level and phone level.

a) Select **Customer** > **04** > **Call Redirection**. The Call Redirection page is shown as **Figure 45**.

- **Total redirection count limit**: **7**
- **Call Forward: Originating**
- **Number of normal ring cycle of CFNA: 4**

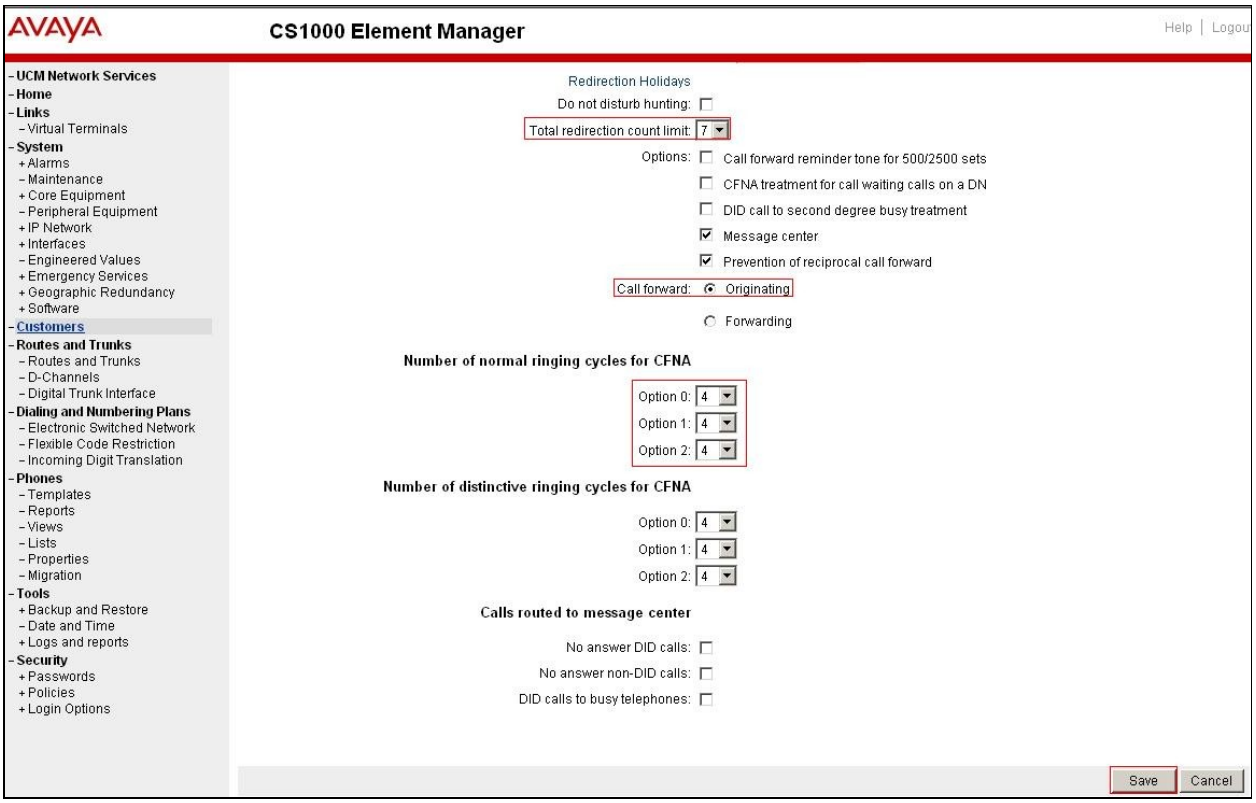

Figure 44 – Call Redirection

b) To enable **Call Forward All Call** (**CFAC**) for phone over trunk by using LD 11, change its CLS to **CXFA**, **SFA** then program the forward number on the phone set. The following is the configuration of a phone with CFAC enabled and forwarding number is 66139675279.

```
REQ: prt
TYPE: 2002p2
TN   108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  MTS
TN   108 0 00 15  VIRTUAL
TYPE 2002P2
…
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
    ICDA CDMA LLCN MCTD CLBD AUTU
    GPUD DPUD DNDD CFXA ARHD CLTD ASCD
…
    19 CFW 16  66139675279
…
```

c) To enable **Call Forward Busy (CFB)** for phone over trunk by using LD 11, change its CLS to **FBA, HTA, SFA** then program the forward number as **HUNT**. The following is the configuration of a phone with CFB enabled and forward number 66139675279.

```
REQ: prt
TYPE: 2002p2
TN   108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  MTS
TN   108 0 00 15  VIRTUAL
TYPE 2002P2
…
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
…
HUNT 66139675279
…
```

d) To enable **Call Forward No Answer (CFNA)** for phone over trunk by using LD 11, change its CLS to **FNA, SFA** then program the forward number as **FDN**. The following is the configuration of a phone with CFNA enabled and forward number 66139675279.

```
REQ: prt
TYPE: 2002p2
TN   108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  MTS
TN   108 0 00 15  VIRTUAL
TYPE 2002P2
…
FDN  66139675279
…
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
   MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
   POD SLKD CCSD SWD LNA CNDA
   CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBD
  …
```

5.7.4. Enable Call Waiting for Phone

In this section, it shows how to configure Call Waiting feature at phone level.

a) Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
b) Configure Call Waiting feature for phone by using LD 11 to change CLS to **HTD**, **SWA** and adding a **CWT** key.

```
REQ: prt
TYPE: 2002p2


TN   108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED
KEM_RANGE

DES  MTS
TN   108 0 00 15  VIRTUAL
TYPE 2002P2
…
CLS  UNR FBD WTA LPR MTD FNA HTD TDD HFD CRPD
   MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
   POD SLKD CCSD SWA LNA CNDA
…
KEY  00 SCR 1223 0     MARP
      CPND
       CPND_LANG ROMAN
        NAME MTS i2002p2
        XPLN 13
        DISPLAY_FMT FIRST,LAST
   01 CWT
…
```

5.8. Administer Avaya Aura® Session Manager

In this section, it shows how to configure the routing on Session Manager. It is assumed that Session Manager has been successfully deployed and connected to System Manager. System Manager is the web interface to configure the Session Manager.

5.8.1. Create a SIP domain name

This section shows how to create a new SIP domain name for this test configuration. Session Manager uses this domain name to route calls from Bell Canada to enterprise CS1000 and vice versa.

a) Login to System Manager. Open a web browser, https://<SMGR_IP_Adress> then login with user "admin" and appropriate password as shown in **Figure 45**.

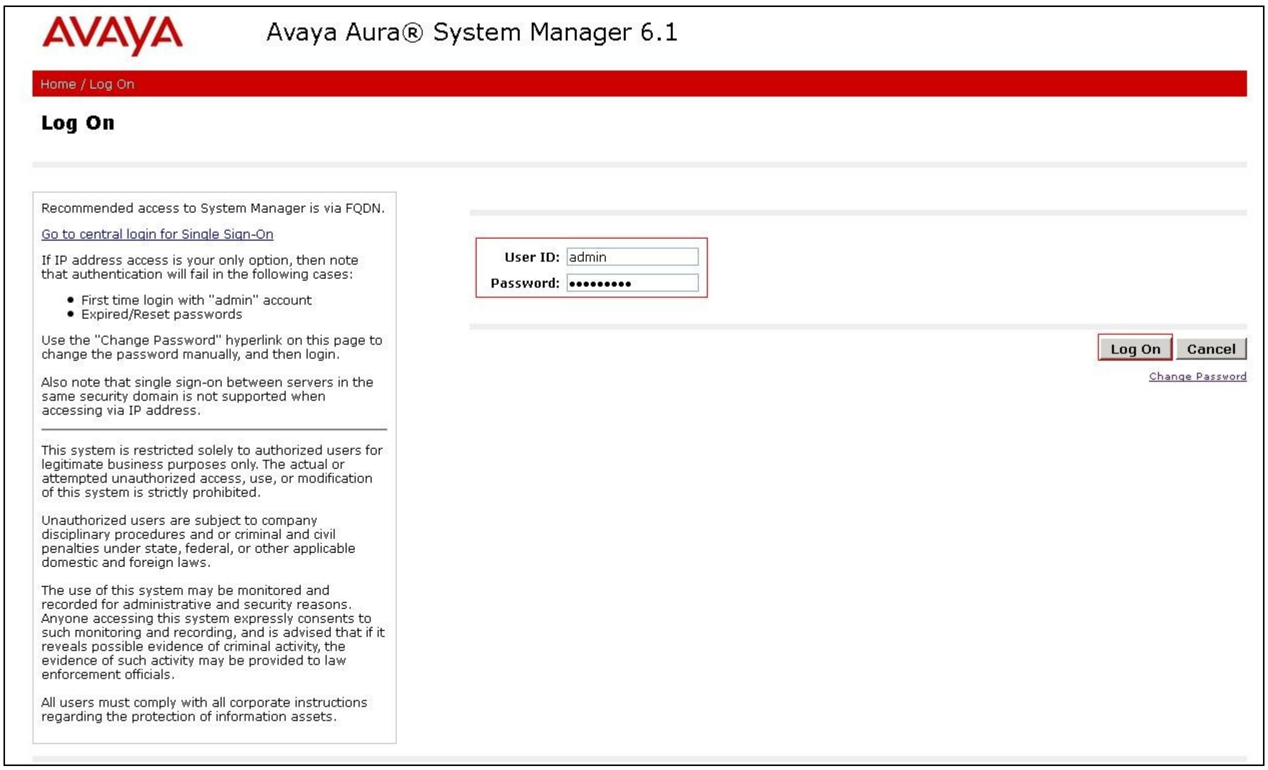

Figure 45: Login to System Manager

b) The System Manager home page displays as shown in **Figure 46**. Select **Routing** to configure the **Network Routing Policy**.

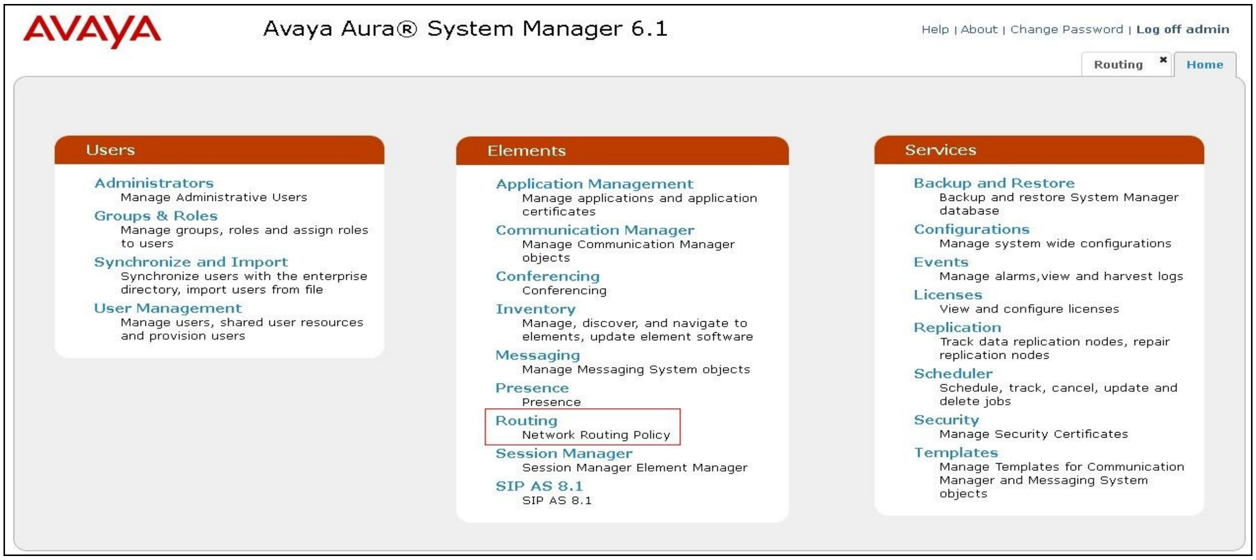

Figure 46 – Select Routing to configure Network Routing Policy

c) In the **Introduction to Network Routing Policy** page (not shown), click **Domains** link on the left menu to open **Domains - Domain Management** page. Then click button **New** (not shown) to add a new test domain. **Figure 47** shows domain **mtsallstream.com** was successfully added.

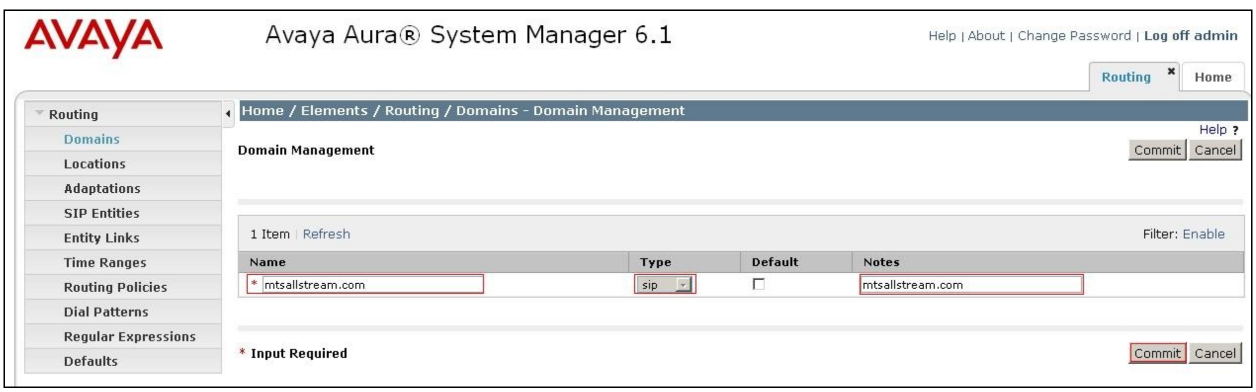

Figure 47 – Adding SIP domain mtsallstream.com

d) Click **Commit**.

5.8.2. Create a Location

Other than domain name, Session Manager binds a SIP Entity to a Location to for bandwidth and location management purposes. It inserts SIP header "P-Location" tell the Far End Gateway (Service Provider) where the call is made from.

The procedure to configure a location is as follows.

a) In the **Introduction to Network Routing Policy** page (not shown), click **Locations** link on the left menu to open **Locations - Location** page. Then click button **New** (not shown) to add a new test location. **Figure 48** shows location **Belleville,Ont,Ca** was successfully added with default settings in the red boxes.

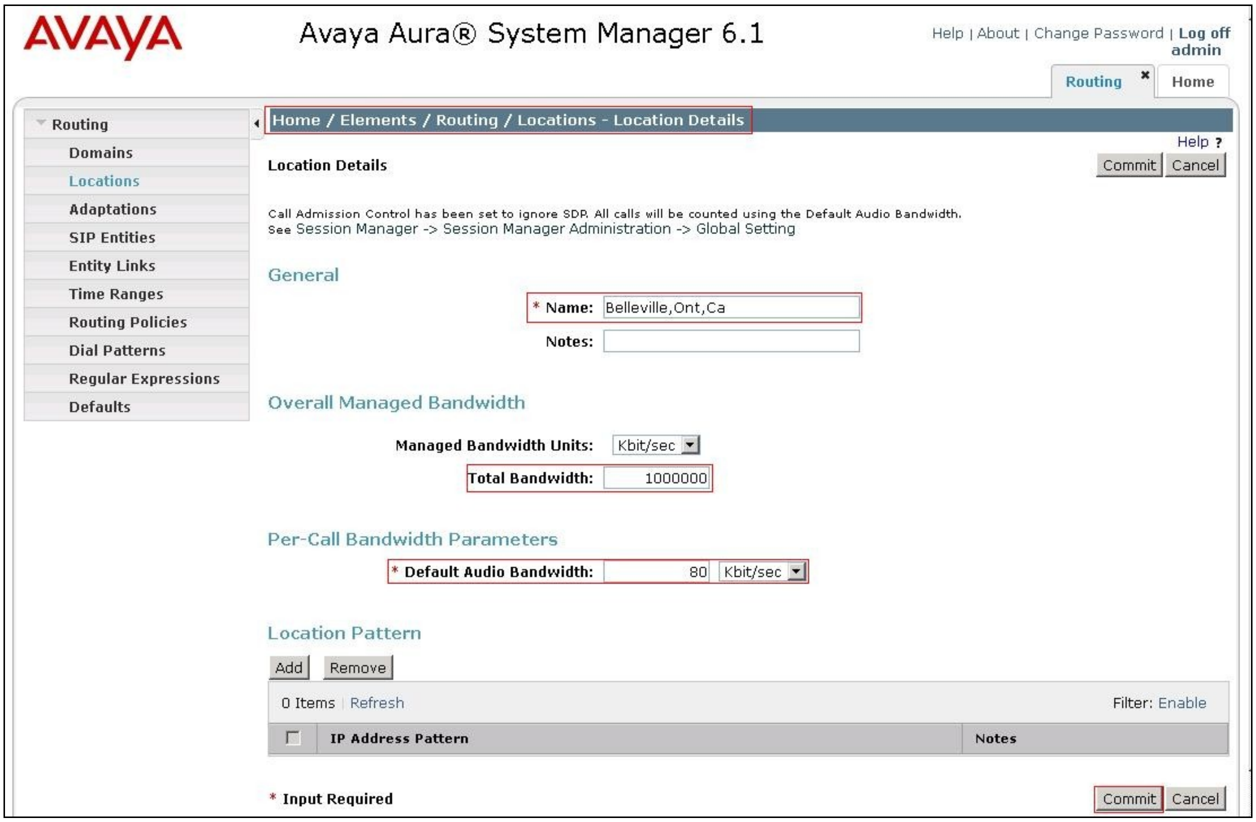

Figure 48 – Adding a Location

b) Click **Commit**.

5.8.3. Create SIP Entity for Session Manager

This section shows how to configure System Manager to add a **SIP Entity** for Session Manager as a static gateway.

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for Session Manager. **Figure 49** shows entity **DevASM** was successfully added. Session Manager was configured to use transport protocol UDP with port 5060.

- **Name**: DevASM
- **FQDN or IP Address**: 110.10.97.198
- **Type**: Session Manager
- **Location**: Belleville,Ont,Ca
- **Port**: 5060, **Protocol**: UDP
- **SIP Link Monitoring**: Use Session Manager Configuration

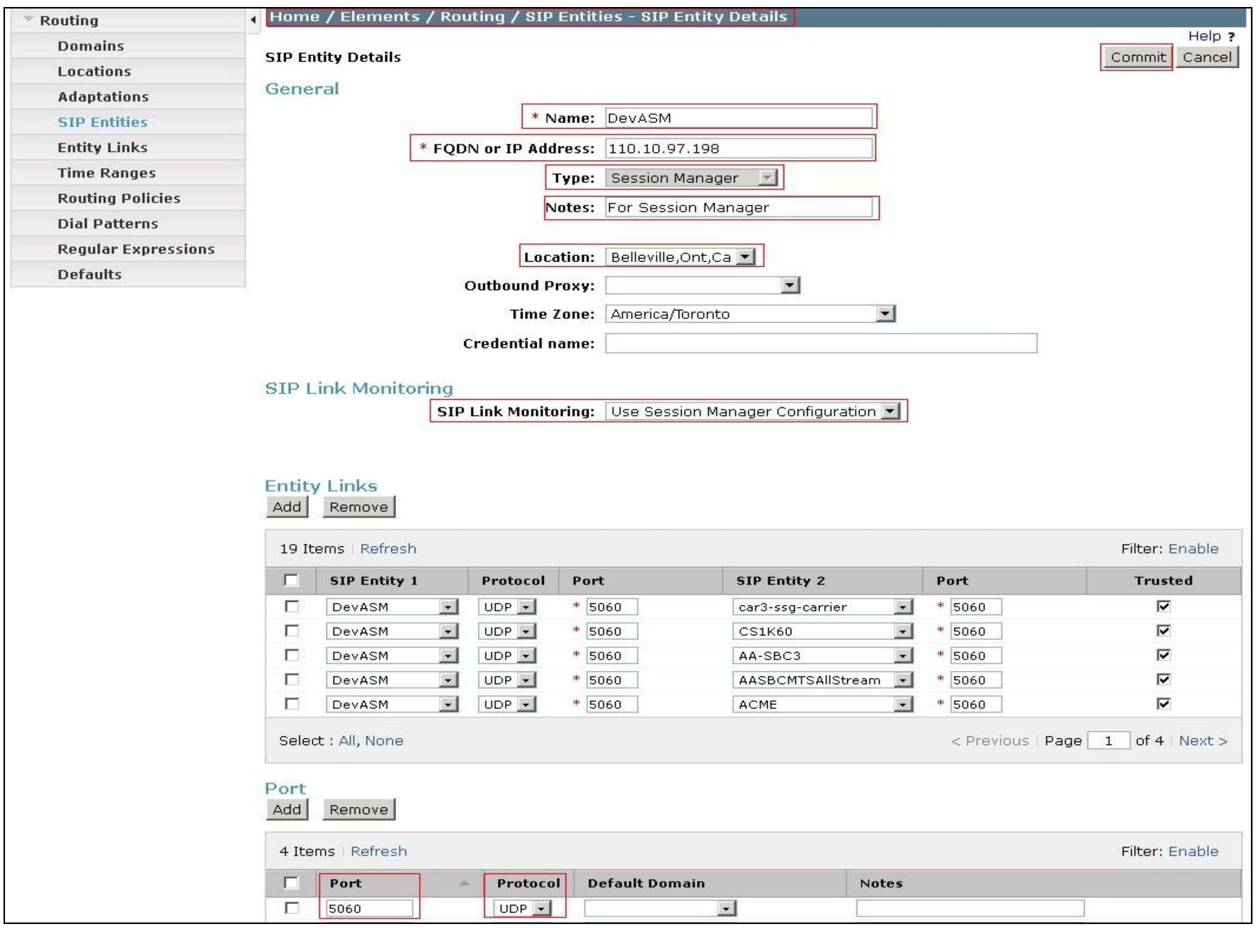

Figure 49 – Adding SIP Entity for Session Manager

b) Click **Commit**.

Note: The IP Address used for SIP Entity - Session Manager has to be different than the IP address used for management interface of Session Manager. The management IP was associated to physical interface eth0 and was defined during software installation. While the IP for SIP Entity was associated to physical interface eth2.

5.8.4. Create SIP Entity for CS1000 SIP Gateway

This section shows how to configure System Manager to add a SIP Entity for CS1000 SIP Gateway.

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for CS1000 SIP Gateway.

The **Entity Links** configuration is to define the network connection between Session Manager and CS1000 SIP Gateway. In this testing, the trusted link was configured with protocol UDP and port 5060. **Figure 50** shows SIP Entity **car2-ssg-mtsallstream** was successfully added.

- **Name**: **car2-ssg-mtsallstream**
- **FQDN or IP Address**: 110.10.97.190
- **Type**: Other
- **Location**: Belleville,Ont,Ca
- **SIP Link Monitoring**: Use Session Manager Configuration

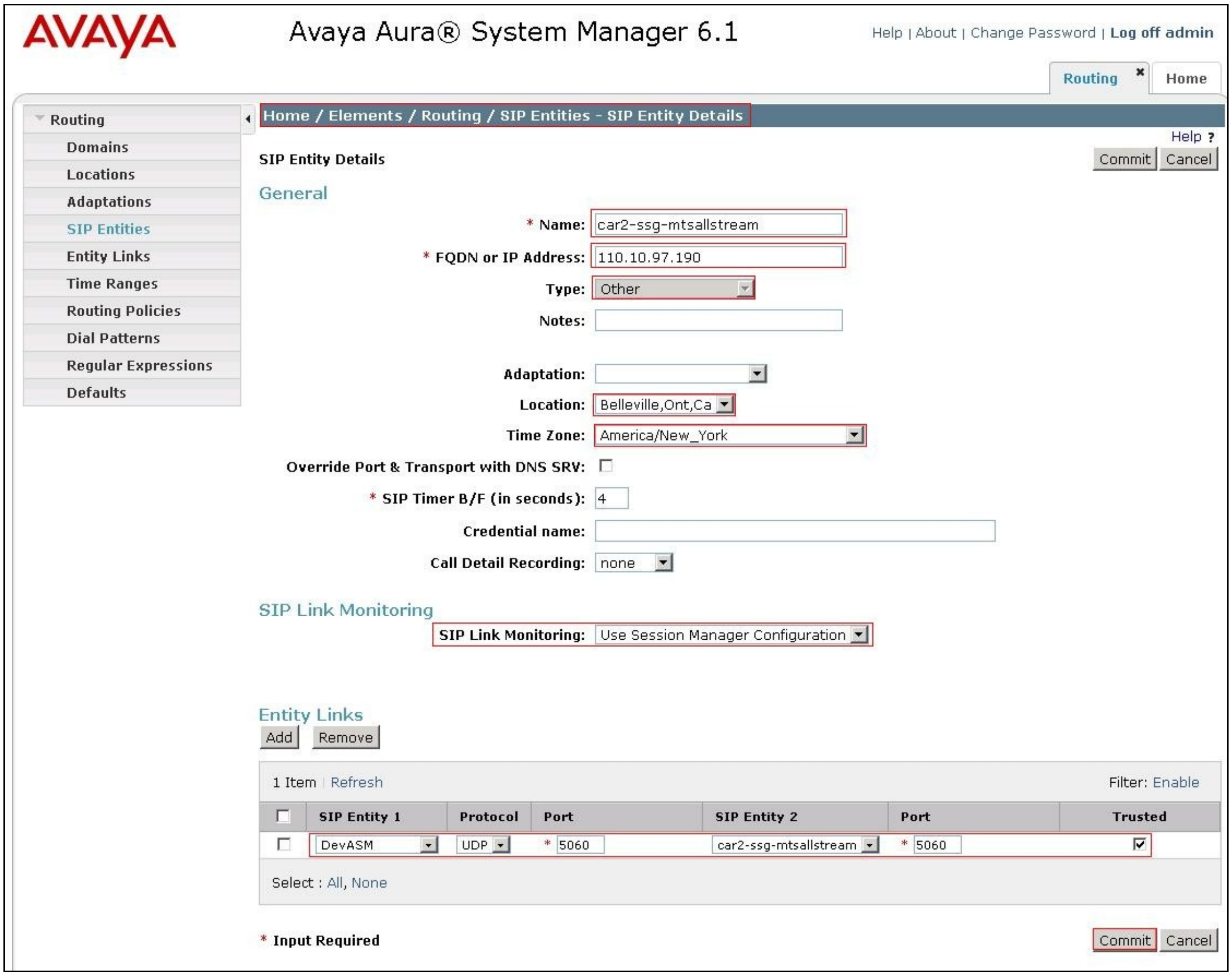

Figure 50 – Adding SIP Entity for CS1000 SIP Gateway

b) Click **Commit**.

Note: In the **Entity Links** configuration, the option “**Trusted**” is mandatory.

5.8.5. Create SIP Entity for Avaya Aura SBC

This section shows how to configure System Manager to add a SIP Entity for Avaya Aura SBC (hereafter referred to as AA-SBC).

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for AA-SBC.

The **Entity Links** configuration is to define the network connection between Session Manager and AA-SBC. In this testing, the trusted link was configured with protocol UDP and port 5060. **Figure 51** shows SIP Entity **AA-SBCMTSAllStream** was successfully added.

- **Name**: **AA-SBCMTSAllStream**
- **FQDN or IP Address**: 110.10.97.216
- **Type**: Other
- **Location**: Belleville,Ont,Ca
- **SIP Link Monitoring**: Use Session Manager Configuration
- **SIP Entity Link**: Trusted

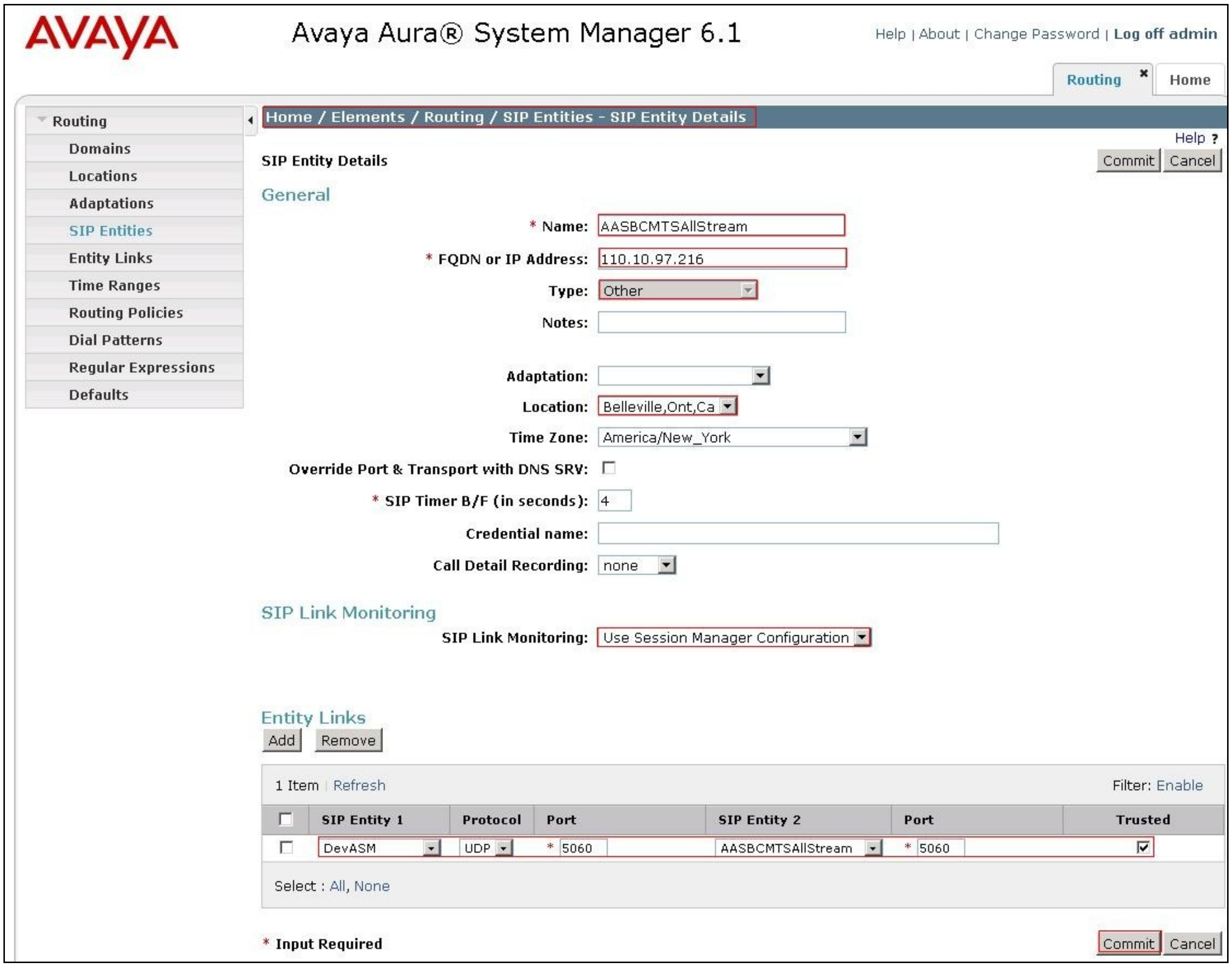

Figure 51 – Adding SIP Entity for Acme Packet SBC

b) Click **Commit**.

Note: In the **Entity Links** configuration, the option “**Trusted**” is mandatory.

5.8.6. Create Routing Policy for inbound call

This section shows how to configure Session Manager to add a **Routing Policy** for inbound call from MTS Allstream to CS1000. As part of the dialing plan configuration, the **Routing Policy** instructs Session Manager to route SIP calls from PSTN to the CS1000 SIP Gateway to terminate.

The "**Time of Day**" setting defines the range to apply the **Routing Policy** during the day. In this testing, just simply select the default name **24/7**. It means the **Routing Policy** is always in effect.

Figure 52 shows policy **MTSAllStream_To_CS1K** was created.

- Name: MTSAllStream_To_CS1K
- SIP Entity as Destination: car2-ssg-mtsallstream
- Time of Day: 24/7

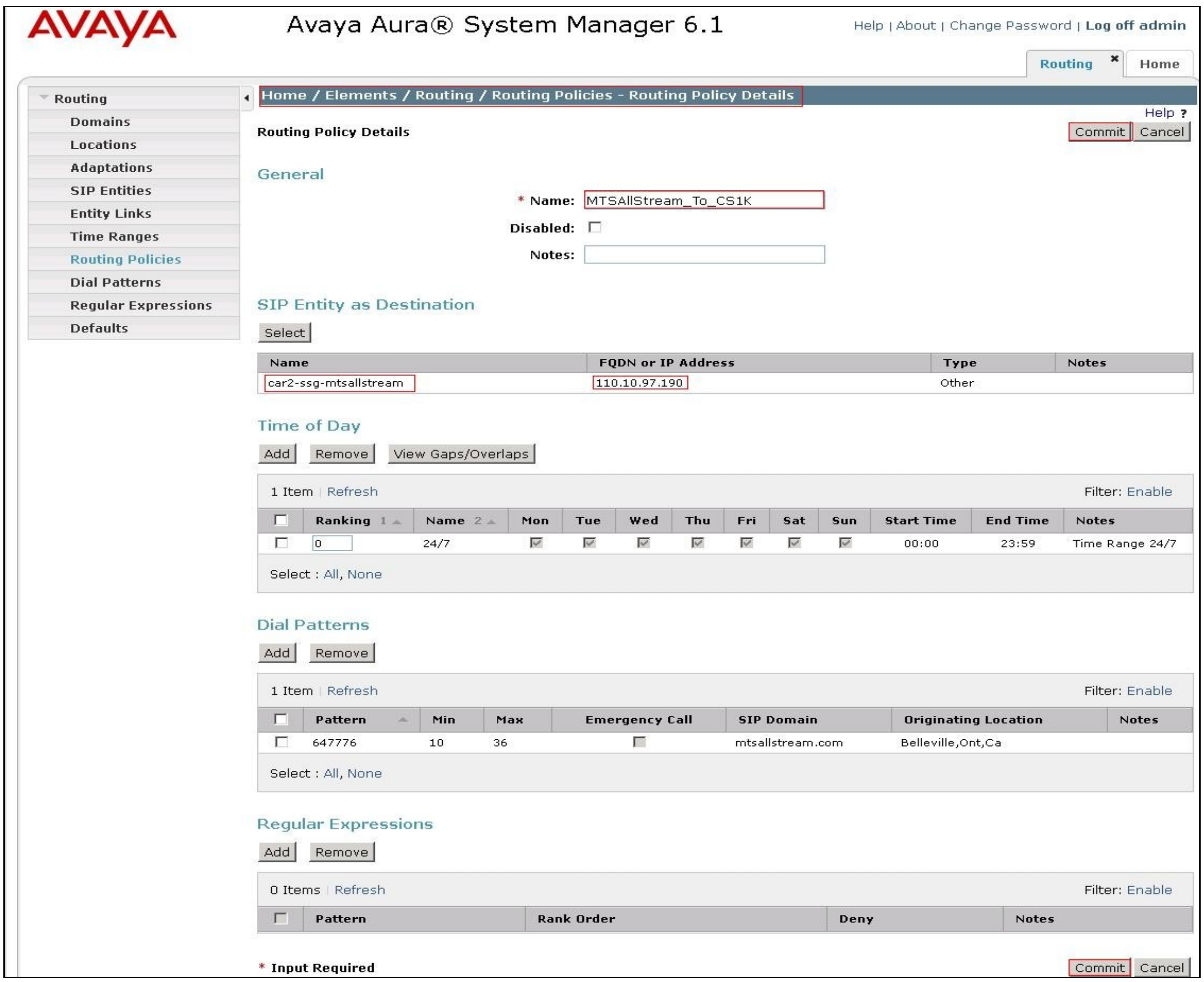

Figure 52 – Adding Routing Policy for inbound call

5.8.7. Create Routing Policy for outbound calls

Please refer to **Section 5.8.6** to create a **Routing Policy** for outbound calls. Based on the policy, Session Manager routes calls from CS1000 to SIP Entity AA-SBC (created in **Section 5.8.5**) as destination, then AA-SBC sends the request to Bell Canada.

Figure 53 shows policy **CS1K_To_MTSAllStream** was created.

- Name: CS1K_To_MTSAllStream
- SIP Entity as Destination: AA-SBCMTSAllStream
- Time of Day: 24/7

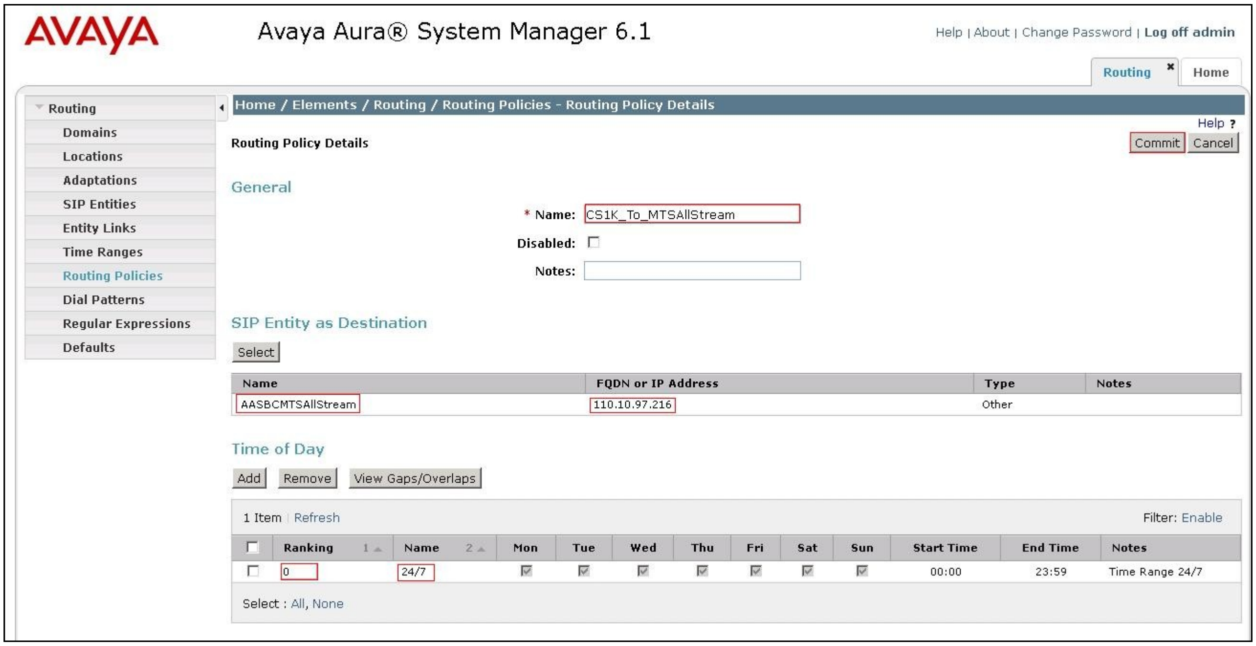

Figure 53 – Adding Routing Policy for outbound call

5.8.8. Create Dial Pattern for inbound call

In this testing, MTS Allstream assigns DID numbers with prefix **647** to CS1000. The DIDs are in 10 digits format. The Dial Pattern **647** on Session Manager is configured as an entry of Routing Policy MTSAllStream_To_CS1K (created in **Section 5.8.6**). It means when Session Manager receives inbound calls with prefix **647**, it routes calls to the CS1000 SIP Gateway car2-ssg-mtsallstream as the destination. **Figure 54** shows policy **Dial Pattern 647** was created.

a) In the **Introduction to Network Routing Policy** page (not shown), click **Dial Patterns** link on the left menu to open **Dial Patterns – Dial Pattern Details** page. Then click button **New** (not shown) to add a new Dial Pattern for inbound calls with prefix **647**.

b) Under **Originating Locations and Routing Policy**, click **Add** (not shown). In the **Dial Patterns – Originating Locations and Routing Policy List** page (not shown), select

Originating Location entry **Belleville,Ont,Ca** (created in **Section 5.8.2**) and **Routing Policies** entry **MTSAllStream_To_CS1K** (created in **Section 5.8.6**).

- Pattern: **647**
- Min: 10 (digits)
- Max: 36 (default)
- SIP Domain: mtsallstream.com
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: MTSAllstream_To_CS1K
- Routing Policy Destination: car2-ssg-mtsallstream

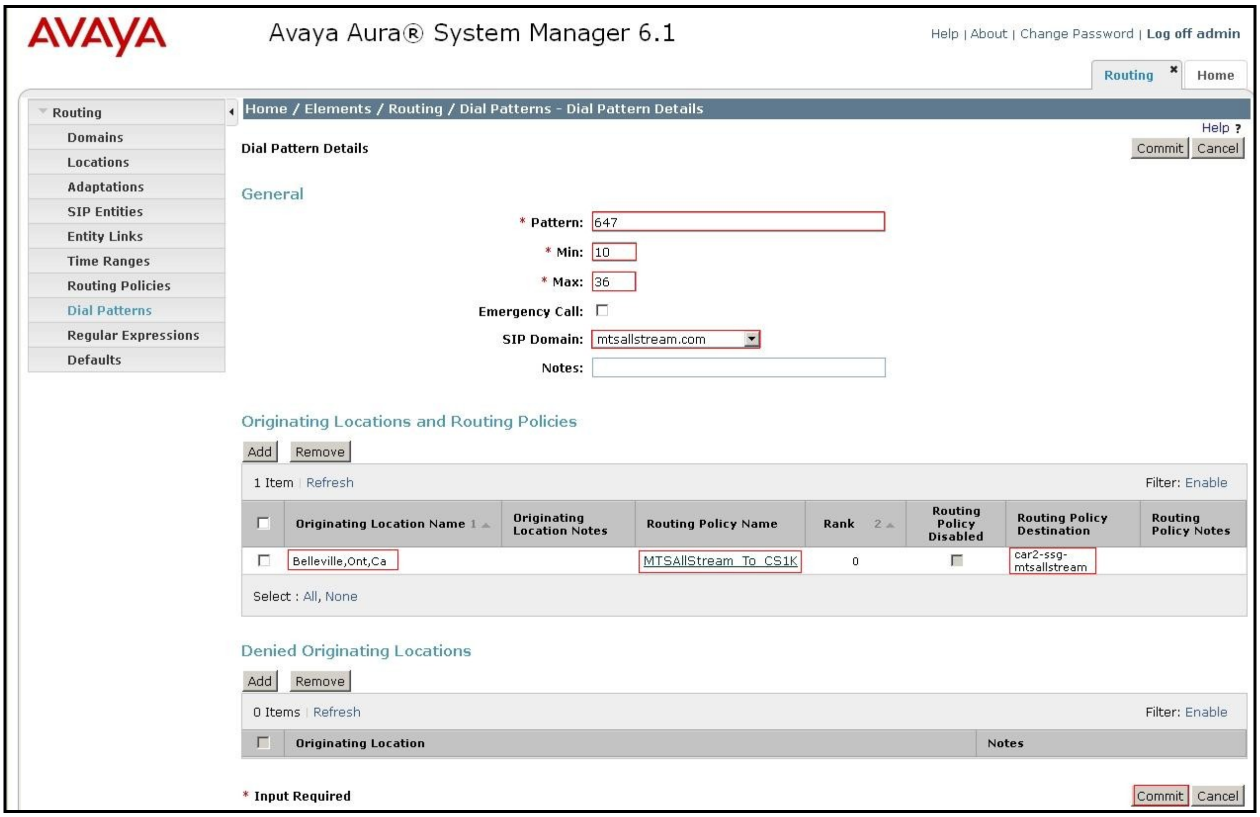

Figure 54 – Adding Dial Pattern for inbound call

c) Click **Commit**.

5.8.9. Create Dial Pattern for outbound calls

The **Dial Pattern** for outbound calls is associated to the **Routing Policy CS1K_To_MTSAllStream** (created in **Section 5.8.7**). The **Dial Pattern** configuration on Session Manager has to match the dialing plan configure on CS1000 (**Section 5.6**).

a) Dial Pattern with prefix **1**. For long distance calls, CS1000 sends 11 digits with prefix **1** to MTS Allstream via AA-SBC. Please refer to **Section 5.8.8** to create a Dial Pattern. The detail configuration of **Dial Pattern 1** is shown in **Figure 55**.

- Pattern: **1**
- Min: 11 (digits)
- Max: 36 (default)
- SIP Domain: mtsallstream.com
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: CS1K_To_MTSAllstream
- Routing Policy Destination: AA-SBCMTSAllStream

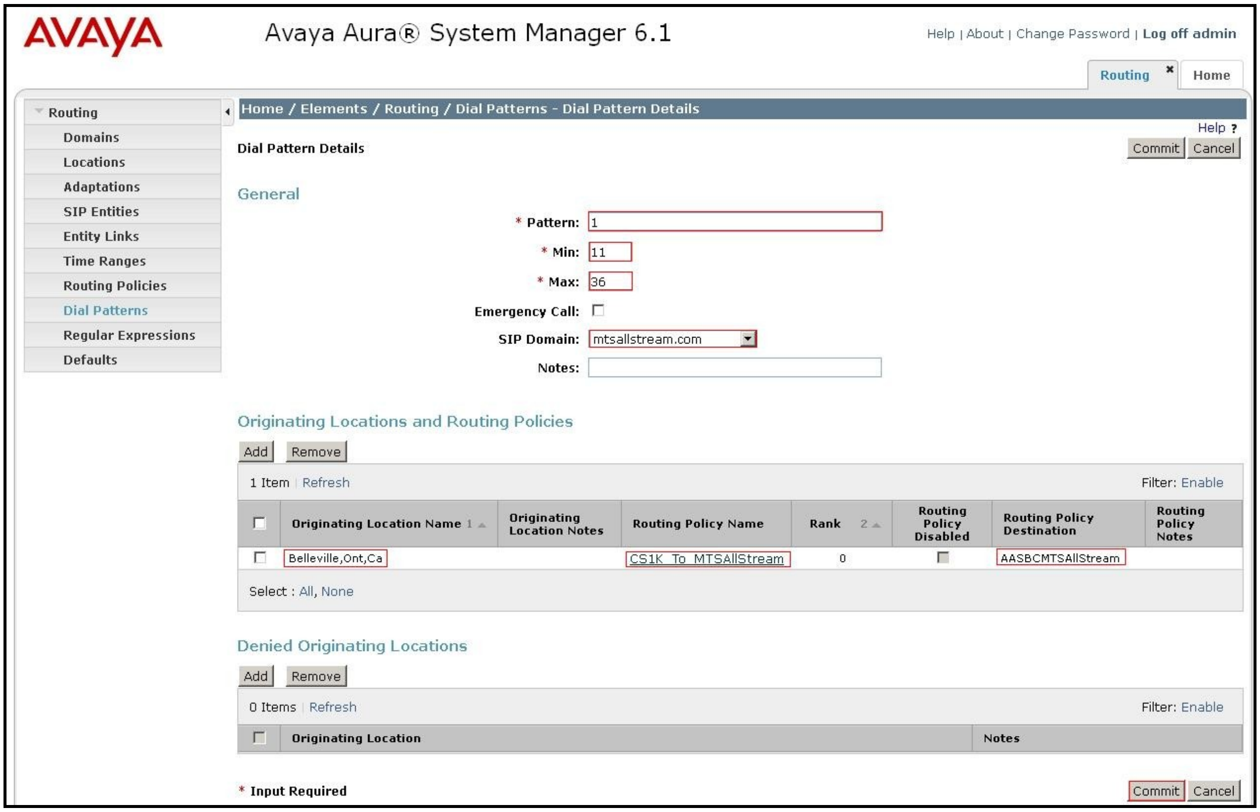

Figure 55 – Adding Dial Pattern for outbound long distance call with prefix 1

b) Dial Pattern with prefix **0**. CS1000 sends **0** or **0+10** digits to reach operator at MTS Allstream. MTS Allstream also uses the same prefix **011** for outbound international calls. Thus, the Dial Pattern **0** should have flexible length. Please refer to **Section 5.8.8** to create a Dial Pattern. The detail configuration of **Dial Pattern 0** is shown in **Figure 56**.

- Pattern: **0**
- Min: 1 (digits)
- Max: 36 (default)
- SIP Domain: mtsallstream.com
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: CS1K_To_MTSAllstream
- Routing Policy Destination: AA-SBCMTSAllStream

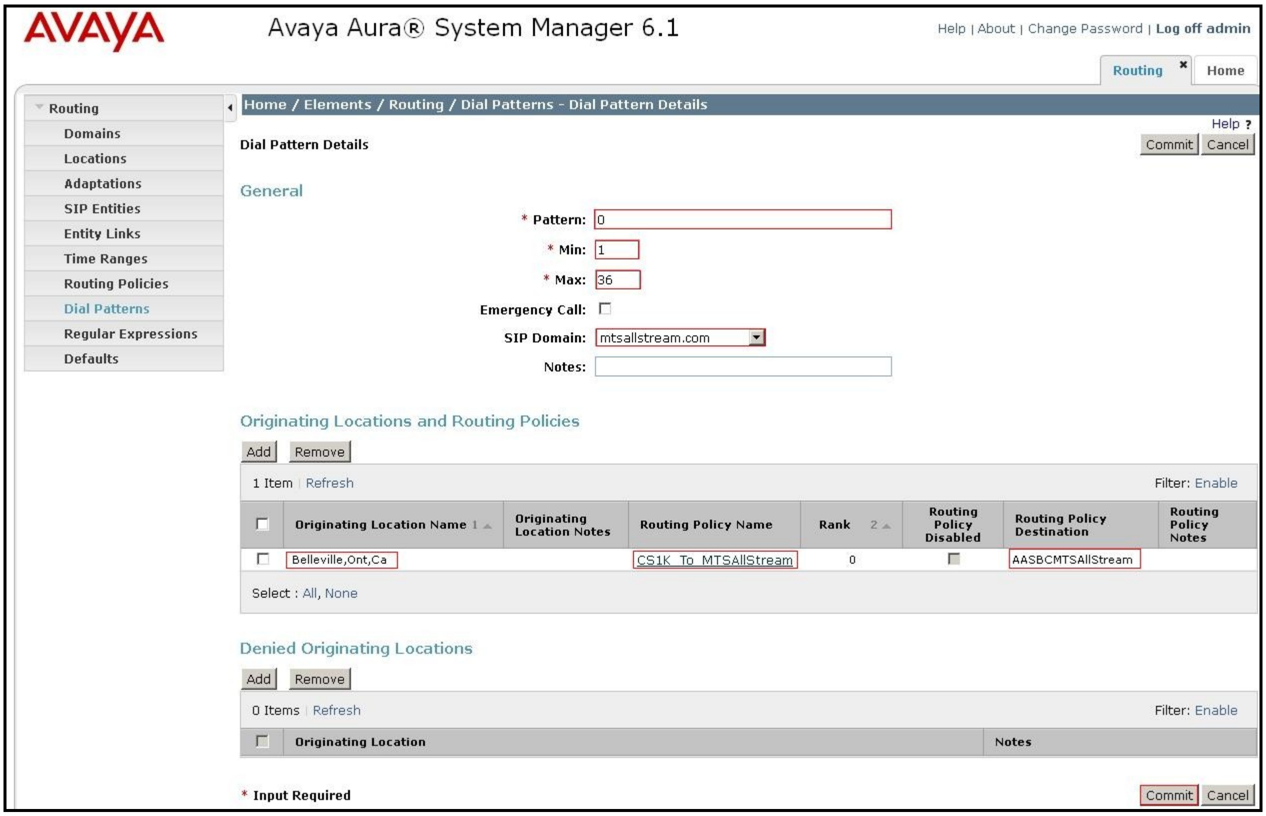

Figure 56 – Adding Dial Pattern for outbound special call with prefix 0

c) Dial Pattern with prefix **411**. As a part of the dialing plan, the **Dial Pattern 411** routes calls from CS1000 to 411 services hosted on MTS Allstream. Please refer to **Section 5.8.8** to create a Dial Pattern. The detail configuration of **Dial Pattern 411** is shown in **Figure 57**.

- Pattern: **411**
- Min: 3 (digits)
- Max: 36 (default)
- SIP Domain: mtsallstream.com
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: CS1K_To_MTSAllstream
- Routing Policy Destination: AA-SBCMTSAllStream

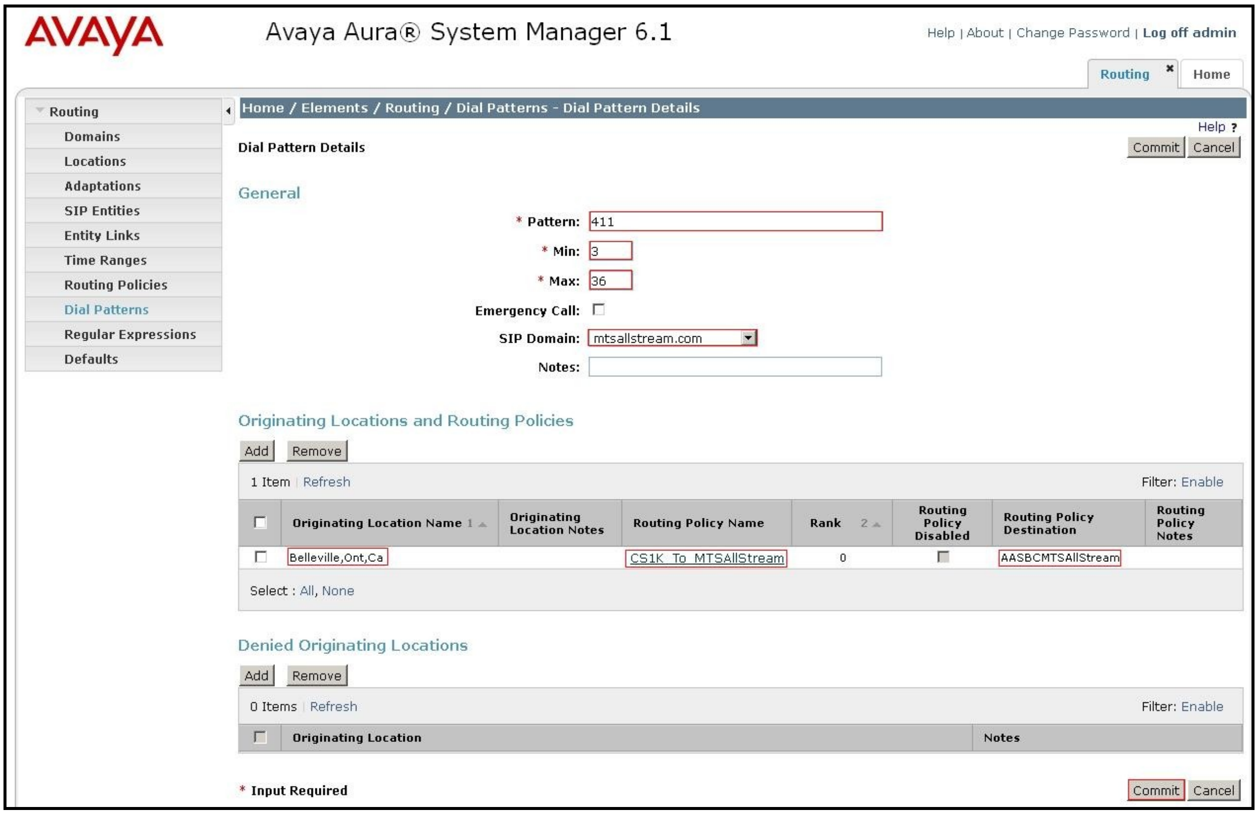

Figure 57 – Adding Dial Pattern for outbound 411 calls

e) Dial Pattern with prefix **911**. As a part of the dialing plan, the **Dial Pattern 911** routes calls from CS1000 to 911 emergency services hosted on MTS Allstream. Please refer to **Section 5.8.8** to create a Dial Pattern. The detail configuration of **Dial Pattern 911** is shown in **Figure 58**.

- Pattern: **911**
- Min: 3 (digits)
- Max: 36 (default)
- SIP Domain: siptrunking.bell.ca
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: **CS1K75_TO_BELLCANADA**
- Routing Policy Destination: ACME

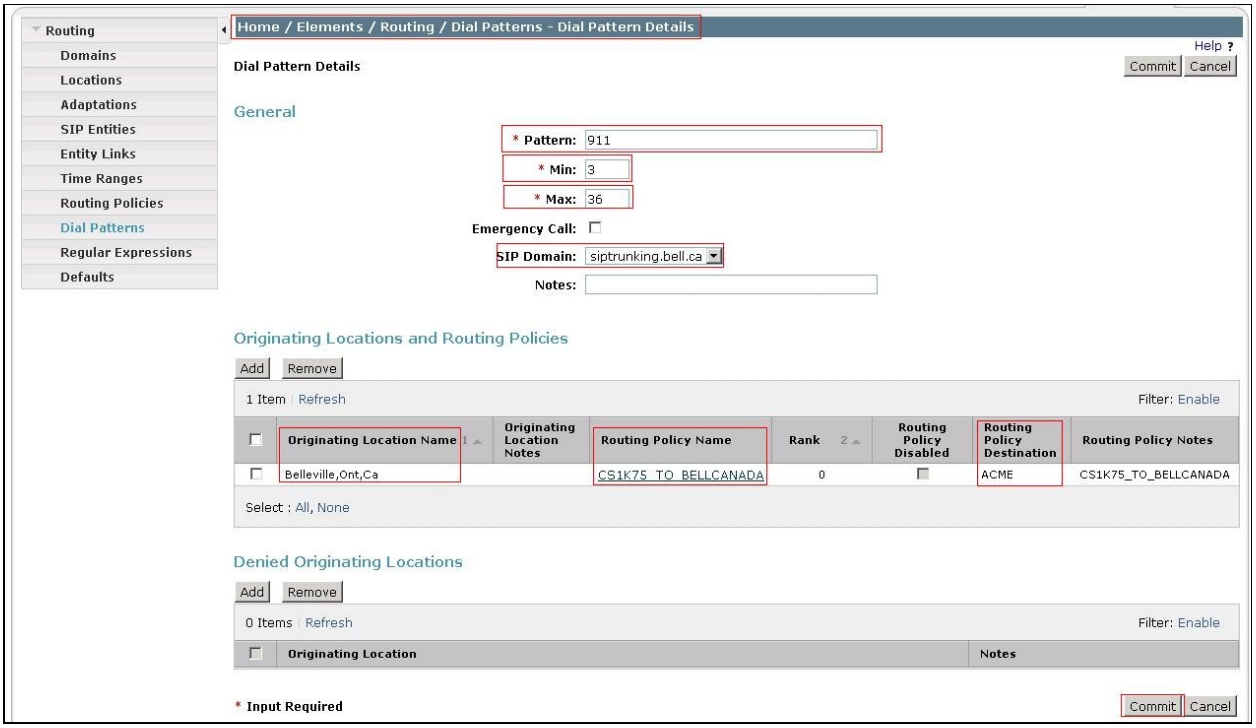

Figure 58 – Adding Dial Pattern for outbound 911 calls

6. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the Avaya Aura® Session Border Controllers necessary for interoperability with the CS1000 and MTS Allstream systems.

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes and the direct connection to CS1000. The remaining fields are generally the default/standard value used by the AA-SBC for that field.

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

6.1. Service Provider Pre-installation Wizard

Service Provider Pre-installation Wizard is a tool distributed along with SBC release 6.0 installation packages. This wizard collects network configuration information relevant to MTS Allstream, and generates template file with extension EPW. Later on, EPW file is uploaded to the wizard during SBC installation.

Run **SP_Pre-Installation_Wizard_5273.exe** to install the **Service Provider Pre-installation Wizard** on a Window based PC. After the installation is complete, invoke the wizard from **Start > All Programs > SP Pre-installation Wizard > Run SP Pre-installation Wizard.**

a) The **SP Pre-installation Wizard** will be run in a web browser. Under **Select a template**, select **SBCT** from the drop down list, and then click **Next Step** as shown in **Figure 60.**

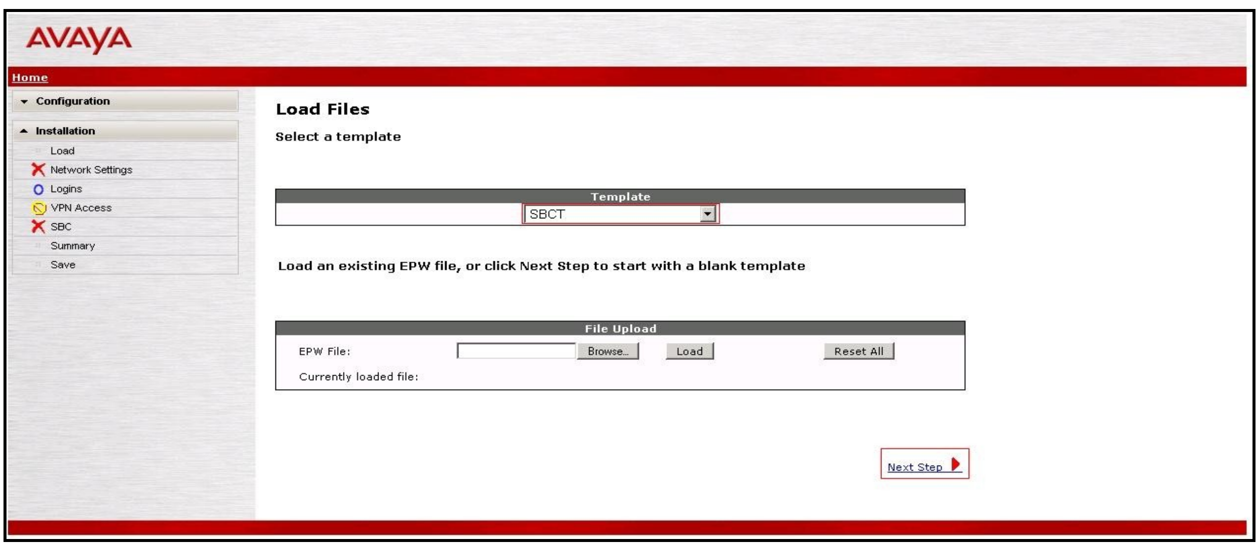

Figure 59: SP Pre-installation Wizard; Select a template

b) **Network Settings** is to configure internal interface of the AA-SBC to connect to the enterprise CS1000 network as shown in **Figure 60**.

- **Domain0 IP Address**: IP address of System Platform system domain 0, e.g. 110.10.97.214
- **CDom IP Address**: IP address of System Platform console domain, e.g 110.10.97.215
- **Gateway IP Address**: 110.10.97.193
- **Network Mask**: 255.255.255.192
- **SBC**: IP address of SBC internal interface, e.g. 110.10.97.216
- **Hostname**: AA-SBC
- **Domain**: bvwdev.com

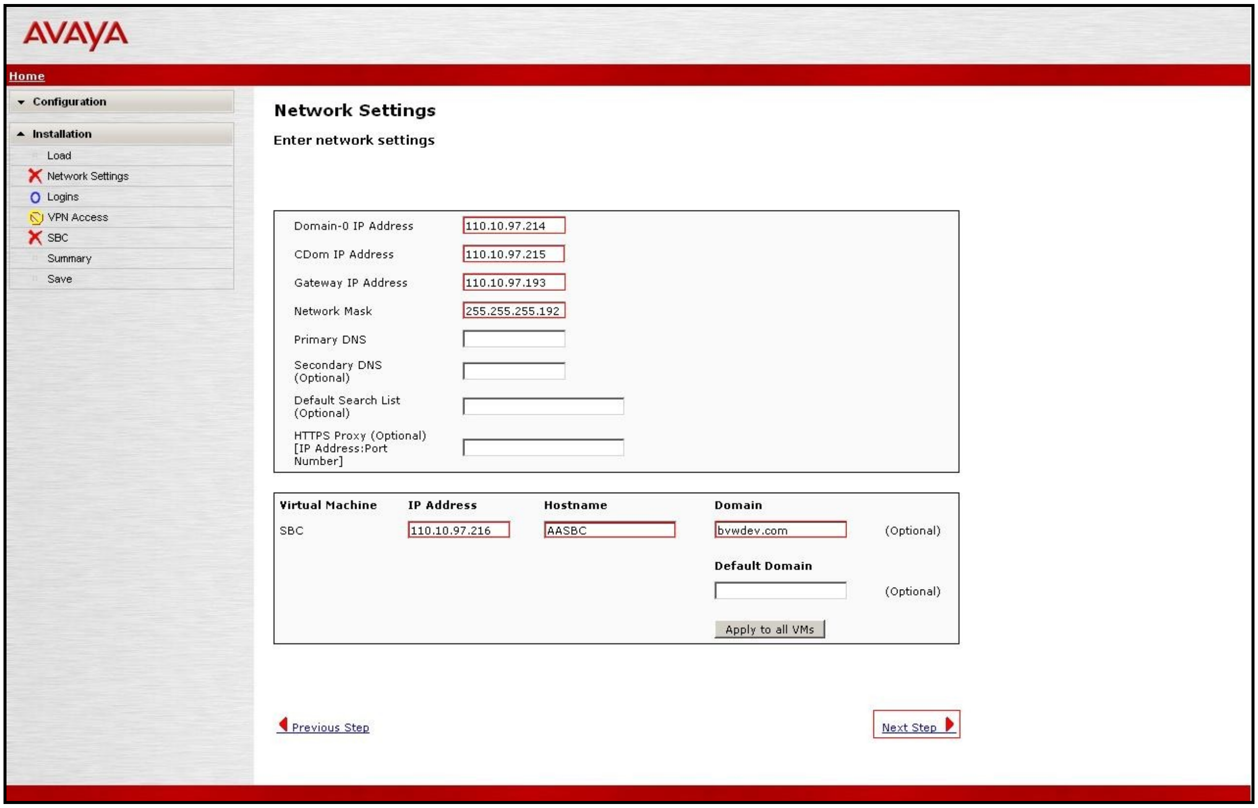

Figure 60: SP Pre-installation Wizard; Network Settings

c) The **Service logins for SBC (optional)** is to define password for account **craft**, **init** and **dadmin** as shown in **Figure 61**.

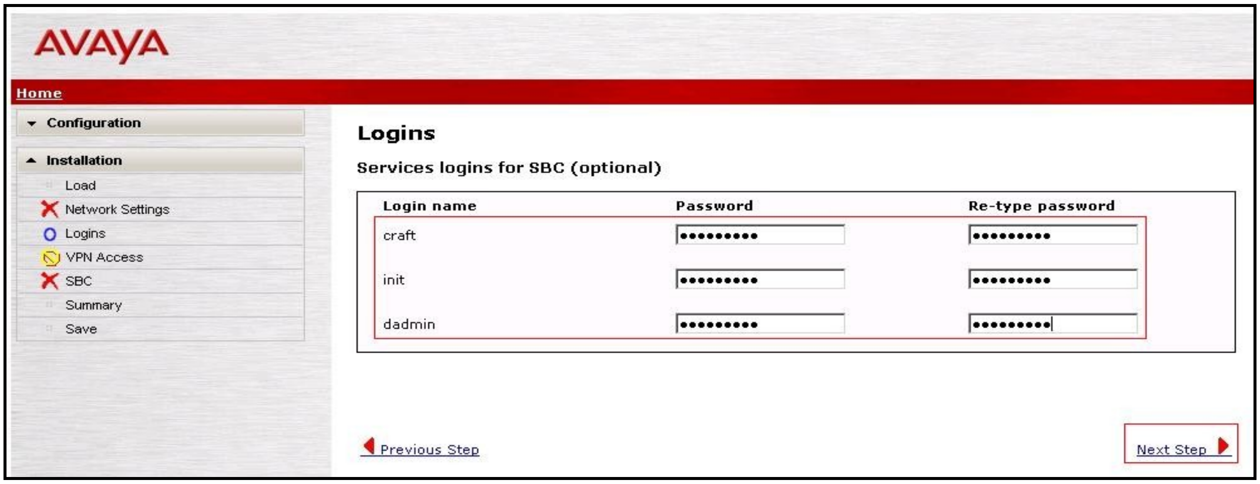

Figure 61: SP Pre-installation Wizard; Services logins for SBC (optional)

d) Next step is the **VPN Access**. The SIP Trunk connect to MTS Allstream is not behind the VPN, so select **No** (VPN mode is disabled) and click **Next Step**.

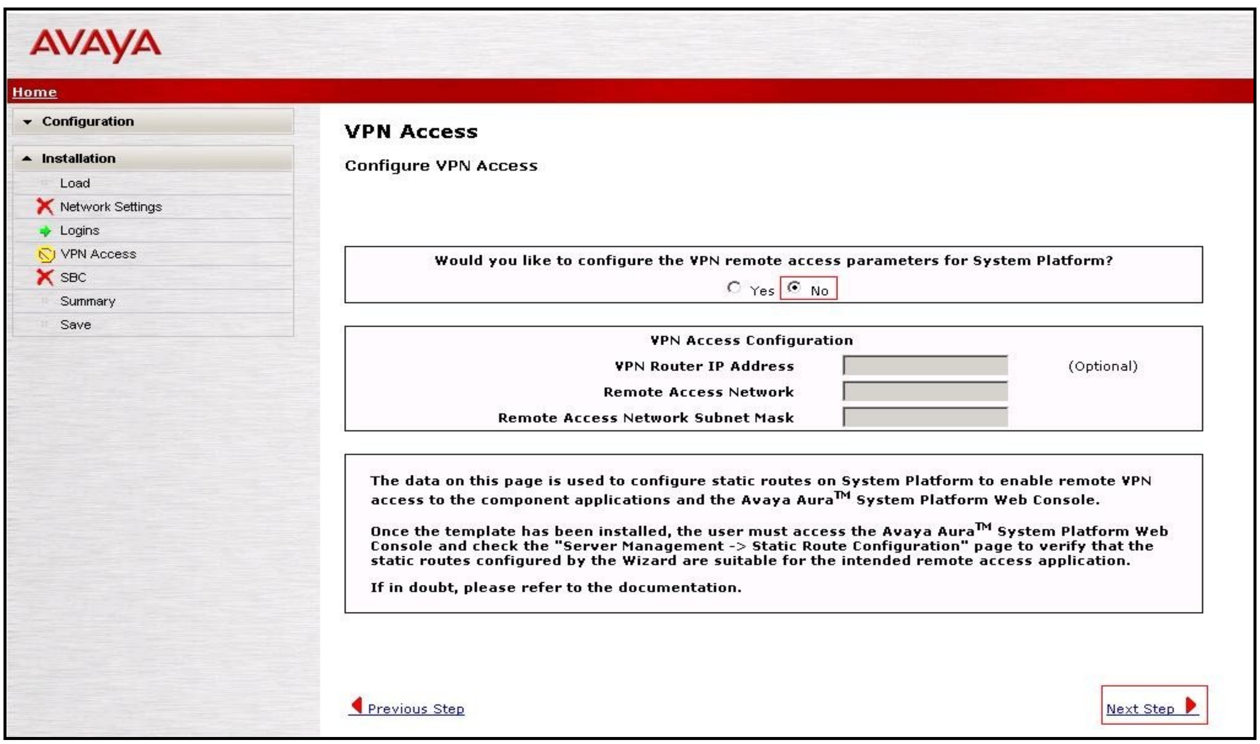

Figure 62: SP Pre-installation Wizard; VPN Access

e) **Session Border Controller Data** is to define IP address of MTS Allstream SBC used for SIP signaling and for RTP as shown in **Figure 63**.

SIP Service Provider Data:

- **Service Provider**: Generic
- **Port**: 5060
- **IP Address1**: IP address of MTS Allstream SBC used for SIP signaling, e.g. 220.20.1.12
- **Signaling/media network1**: network address of MTS Allstream SBC, e.g. 220.20.1.10/27

SBC Network Data:

- **Public**: IP address of AA-SBC to connect to MTS Allstream system, e.g. 110.10.98.108
- **Net Mask**: 255.255.255.224
- **Gateway**: 110.10.98.97

Enterprise SIP Server:

- **SIP Domain**: mtsallstream.com
- **IP Address1**: the IP address of Session Manager (please refer to **Section 5.8**), e.g. 110.10.97.198
- **Transport1**: UDP

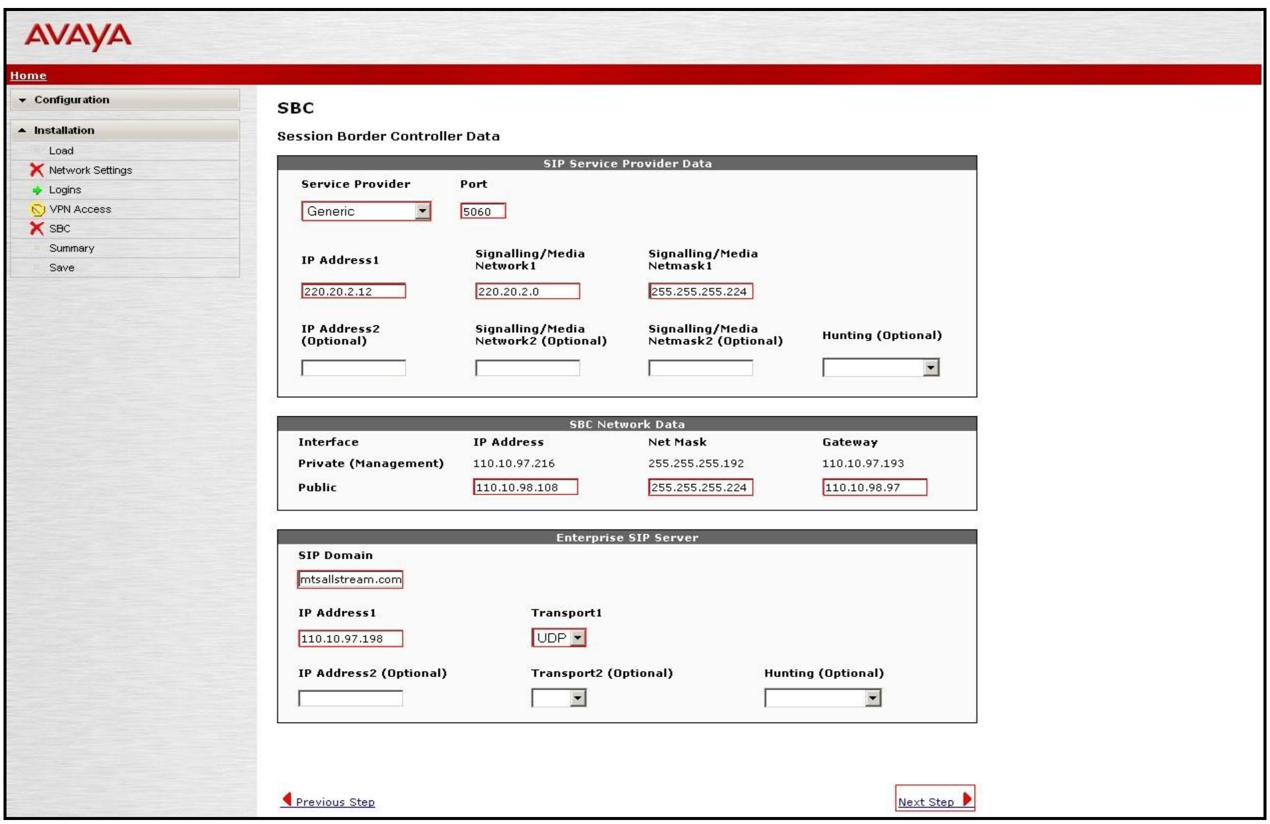

Figure 63: SP Pre-installation Wizard; Session Border Controller Data

f) **Summary** is to give an overview of the configuration as shown in **Figure 64**. Scroll down and click on **Next Step** (not shown).

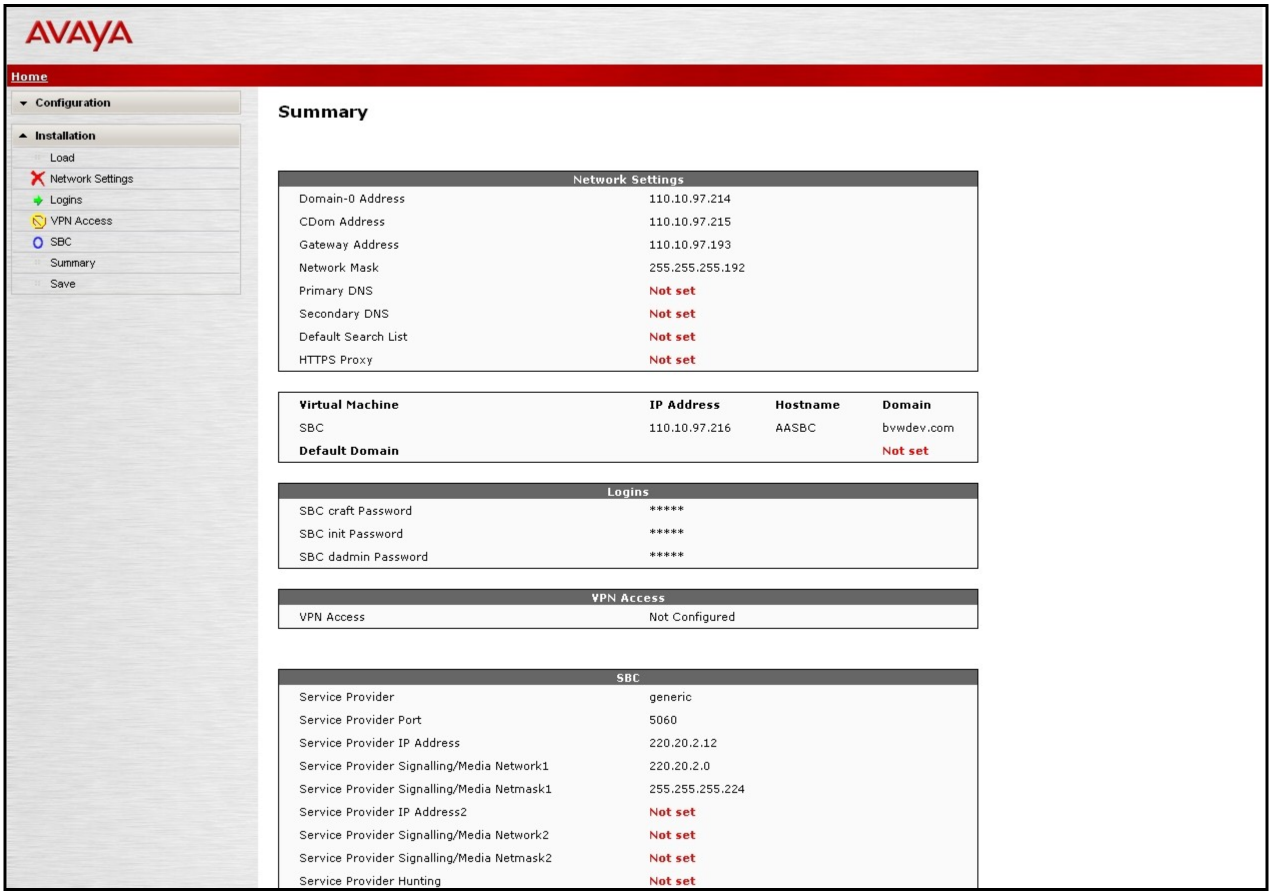

Figure 64: SP Pre-installation Wizard; Summary

g) **Save** is to give an option to save the configuration as an EPW file. Click **Accept** then **Save EPW file** as shown in **Figure 65**.

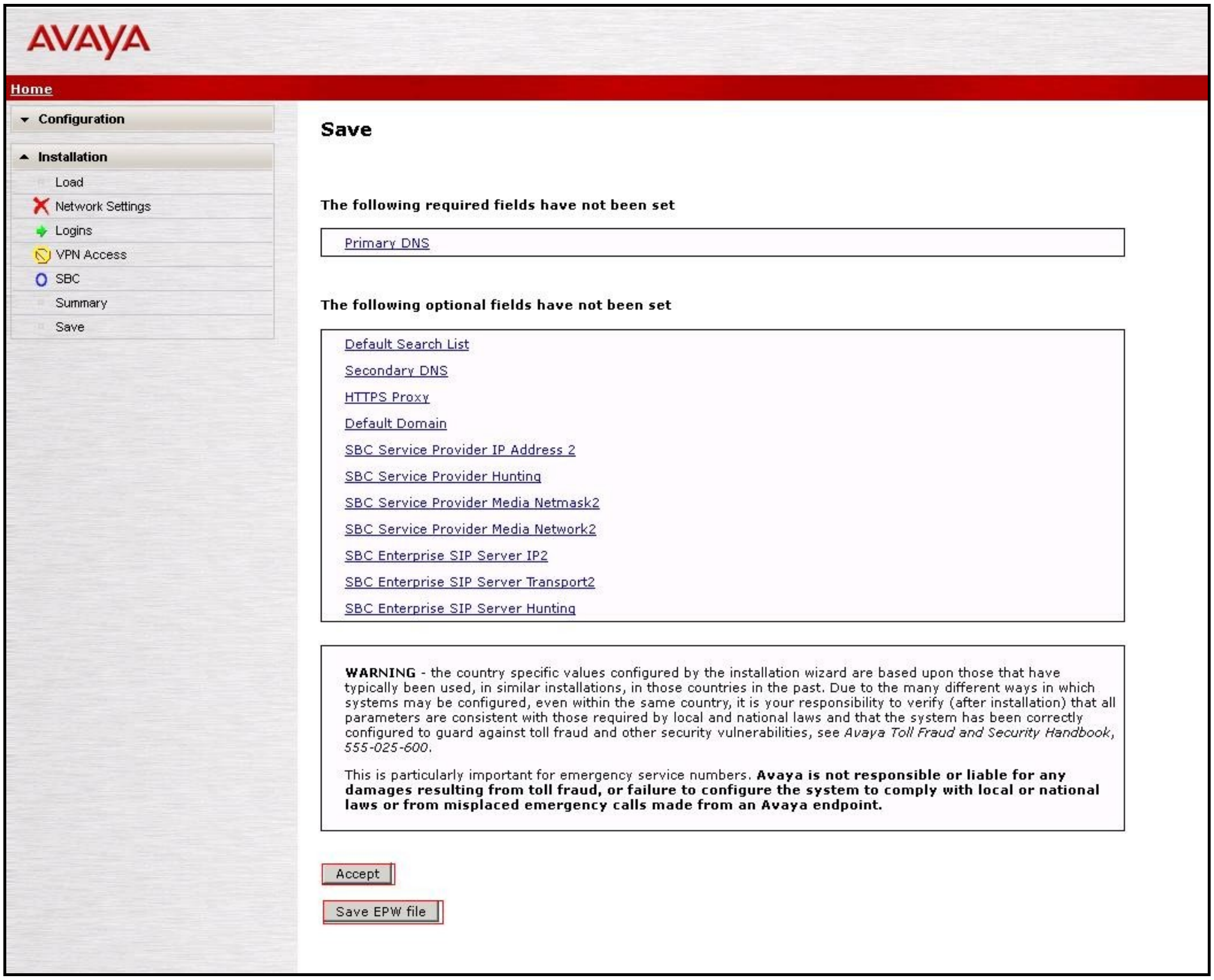

Figure 65: SP Pre-installation Wizard; Save

h) Download and save the EPW file.

6.2. AA-SBC Installation

To install Avaya Aura SBC, follow installation guide provided on http://support.avaya.com. The installation wizard (not shown) is an automation tool.

During installation, EPW file is needed. Please use EPW file created in **Section 6.1** to upload to the wizard. After the installation is complete, continue to configure the SBC as described in **Section 6.3**.

6.3. Administer Enterprise Servers

To login to AA-SBC, go to https://SBCIPAddress/ and enter username as craft and appropriate password.

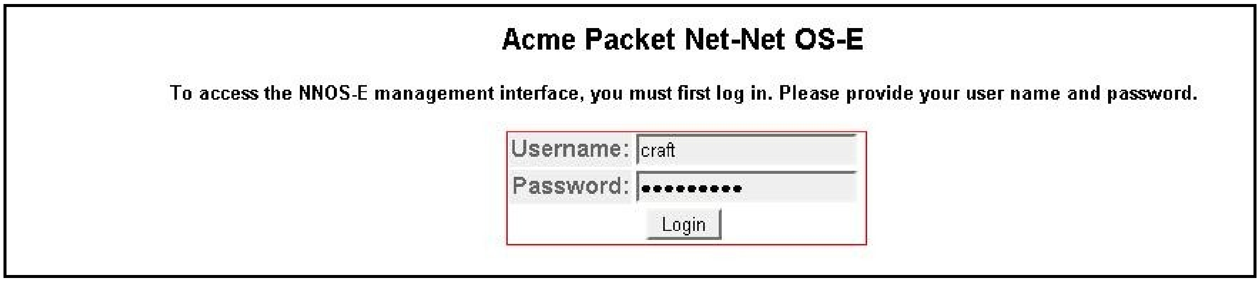

Figure 66: Login to AA-SBC

During installation, the information in the EPW file was used to populate the entry "**server Telco1**", which is the information of MTS Allstream SBC for SIP Trunking and the entry "**server PBX1**" which is the information of Session Manager.

6.3.1. Configuration of "server Telco1"

Select **Configuration > vsp > enterprise > servers > sip-gateway Telco**. **Figure 67** shows detail configuration of IP connectivity of entry **Telco1**. Verify IP address, transportation protocol, and port as defined in step e of **Section 6.1**.

Under **Policy** setting, configure **outbound-session-config-pool-entry** to associate to **vsp\session-config-pool\entry ToTelco.**

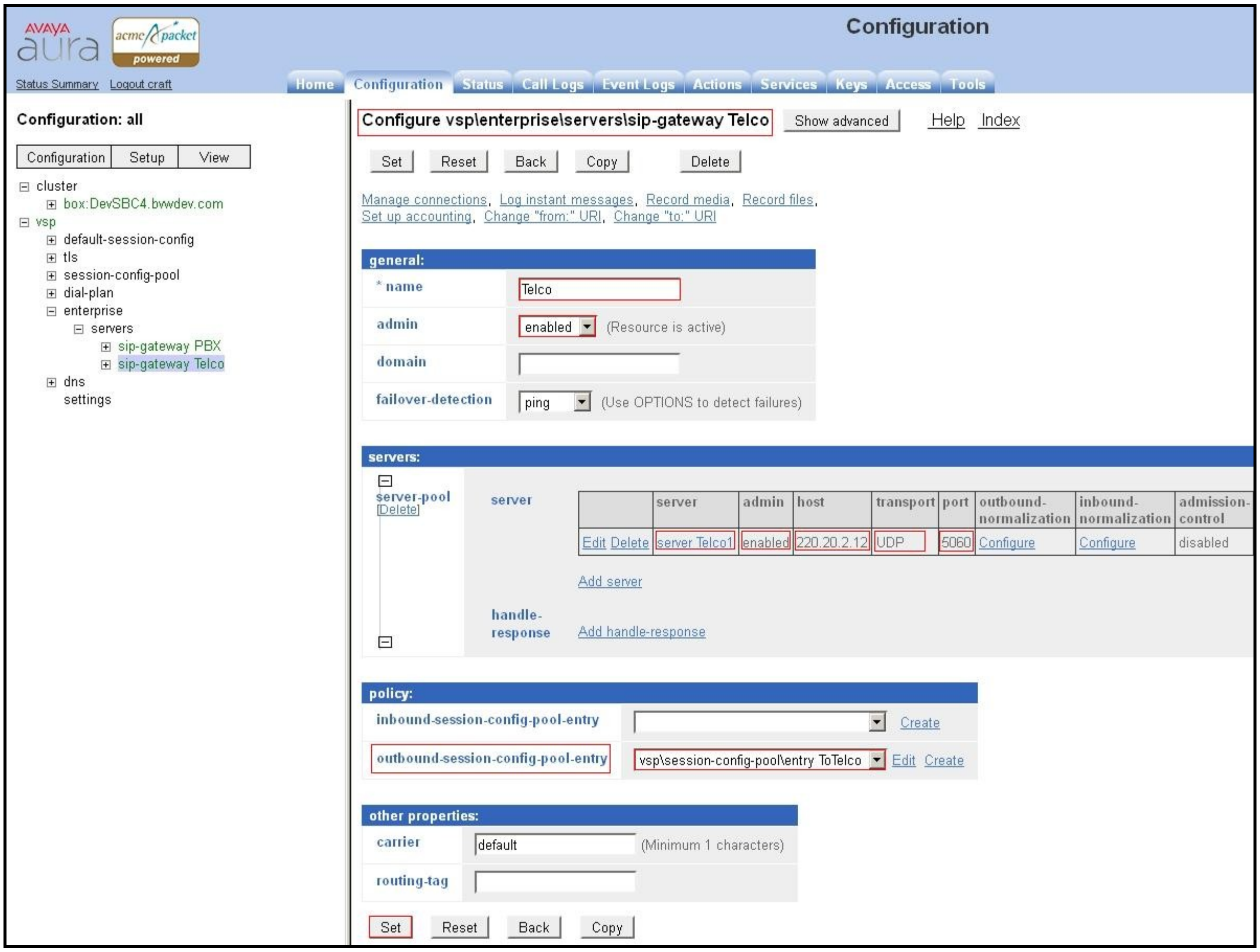

Figure 67: server-Telco1 Configuration

6.3.2. Configuration of "server PBX1"

Select **Configuration > vsp > enterprise > servers > sip-gateway PBX**. **Figure 68** shows detail configuration of IP connectivity of entry **PBX1**. Verify IP address, transportation protocol, and port as defined in step b of **Section 6.1**.

Under **Policy** setting, configure **outbound-session-config-pool-entry** to associate to **vsp\session-config-pool\entry ToPBX.**

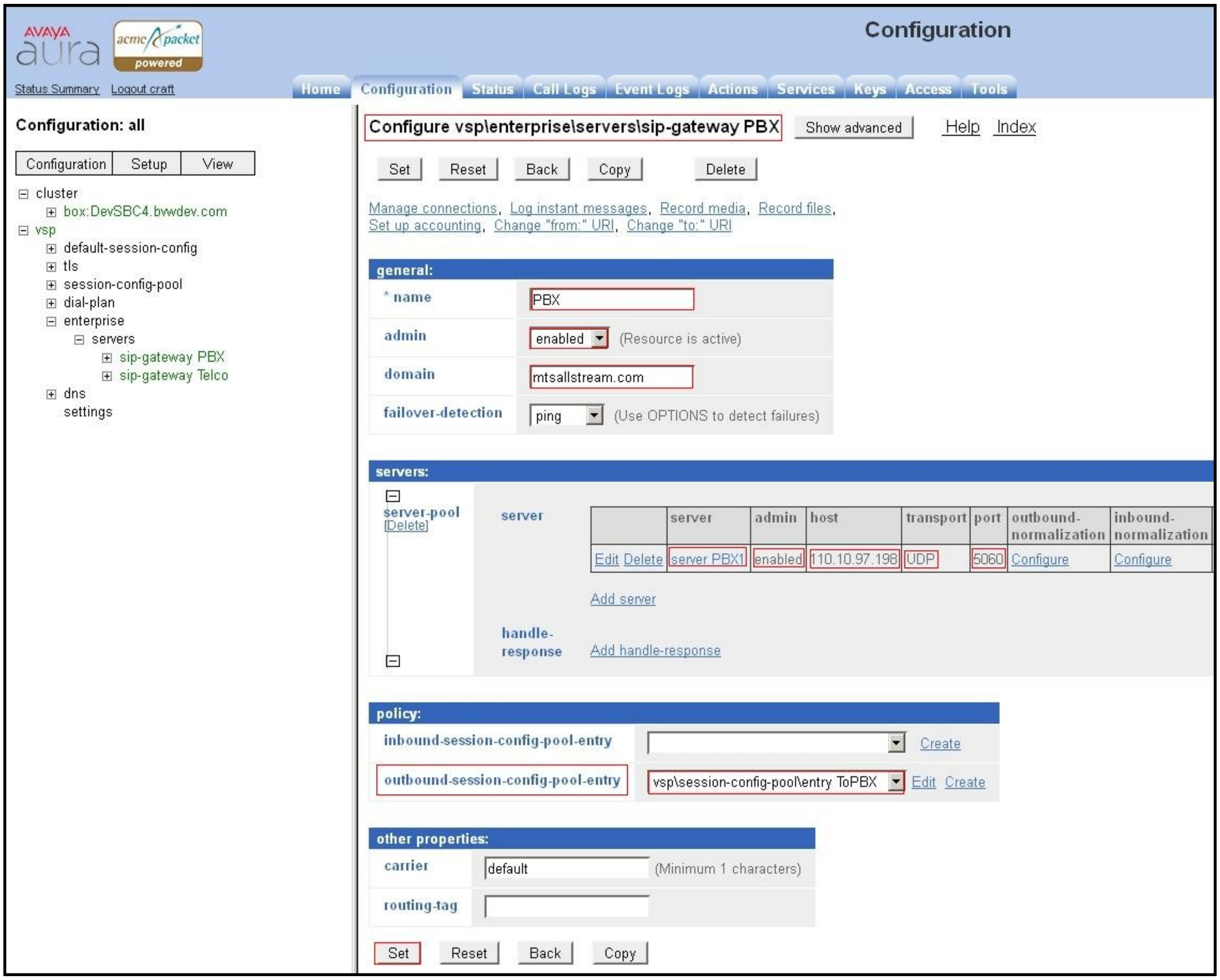

Figure 68: server-PBX1 Configuration.

6.4. Administer Heartbeat

AA-SBC was configured to send OPTION/ping to MTS Allstream and Session Manager for keep alive purpose.

To send OPTION/ping to MTS Allstream, select **Configuration > vsp > enterprise > servers > sip-gateway Telco** then select **"ping"** for **"failover-detection**" as shown in **Figure 69**.

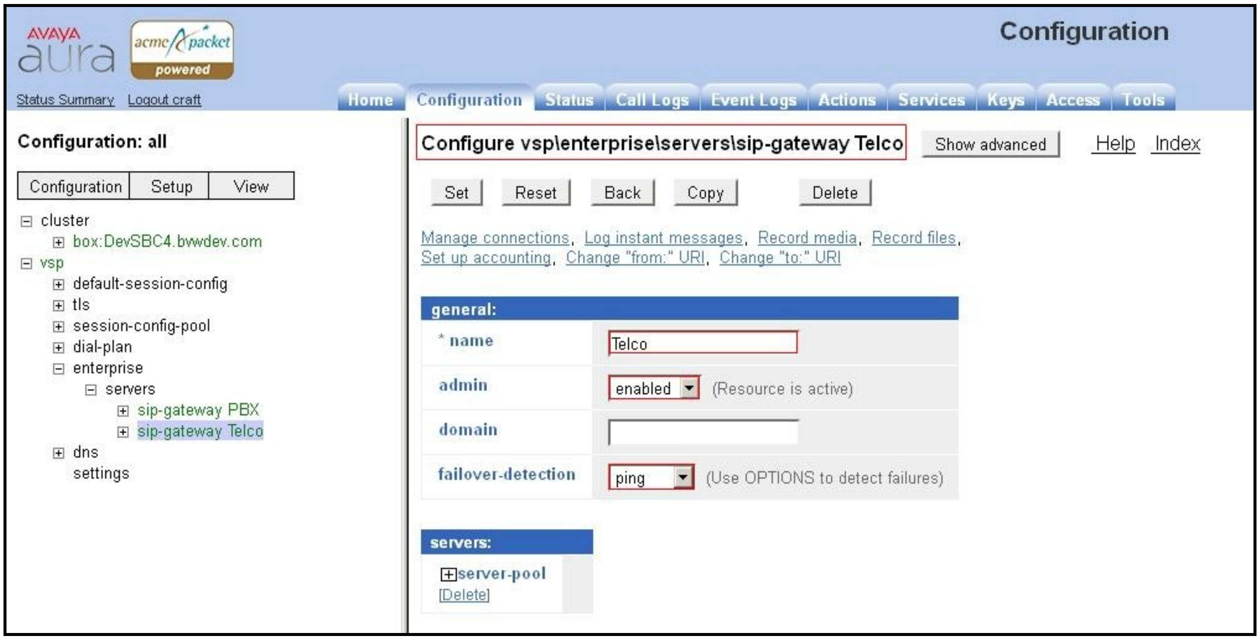

Figure 69: KeepAlive Configuration for sip-gateway Telco

To send OPTION/ping to the Session Manager, select **Configuration > vsp > enterprise > servers > sip-gateway PBX** then select **"ping"** for **"failover-detection**" as shown in **Figure 70**.

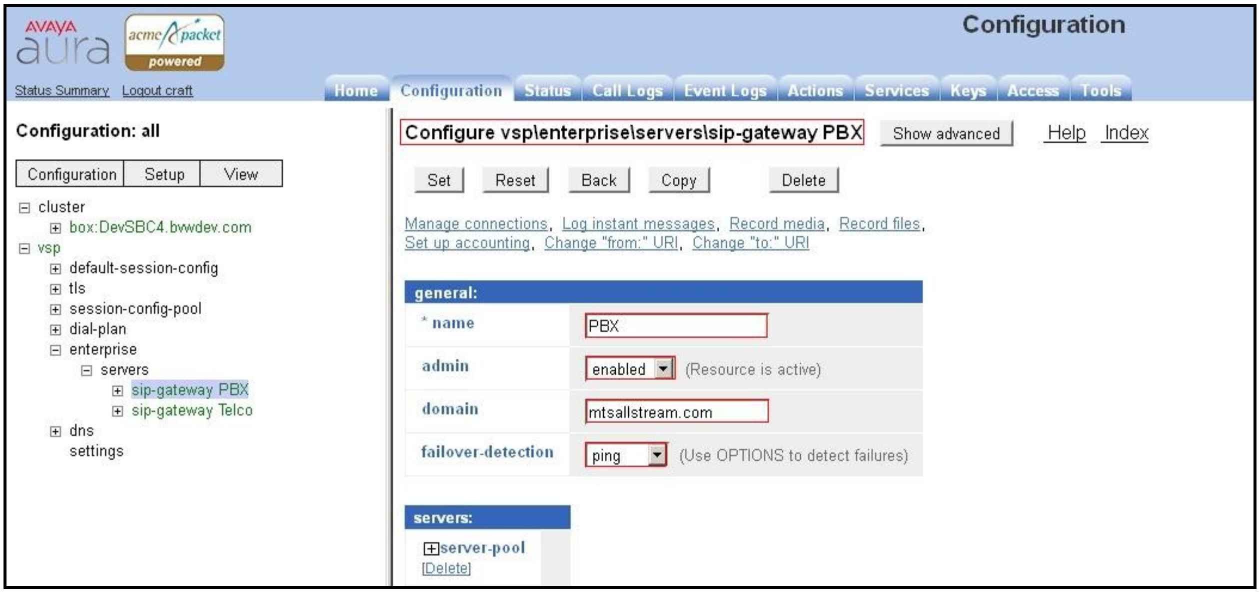

Figure 70: KeepAlive Configuration for sip-gateway PBX

6.5. Administer dial-plan

AA-SBC was pre-configured with typical dial-plans to route SIP calls from CS1000 to MTS Allstream and vice versa.

6.5.1. The entry “source-route FromPBX”

The entry “**source-route FromPBX**” as shown in **Figure 71** below is to route SIP calls from CS1000 to MTS Allstream.

- **source-server**: vsp\enterprise\servers\sip-gateway **PBX**
- **peer server**: vsp\enterprise\servers\sip-gateway **Telco**
- **location-match-preferred**: up-to-outbound-peer
- **priority**: 100 (default)
- **condition-list-match-secondary**: false
- **other properties:**
  - **admin**: enabled
  - **action**: forward
  - **apply-to-methods**: Select All

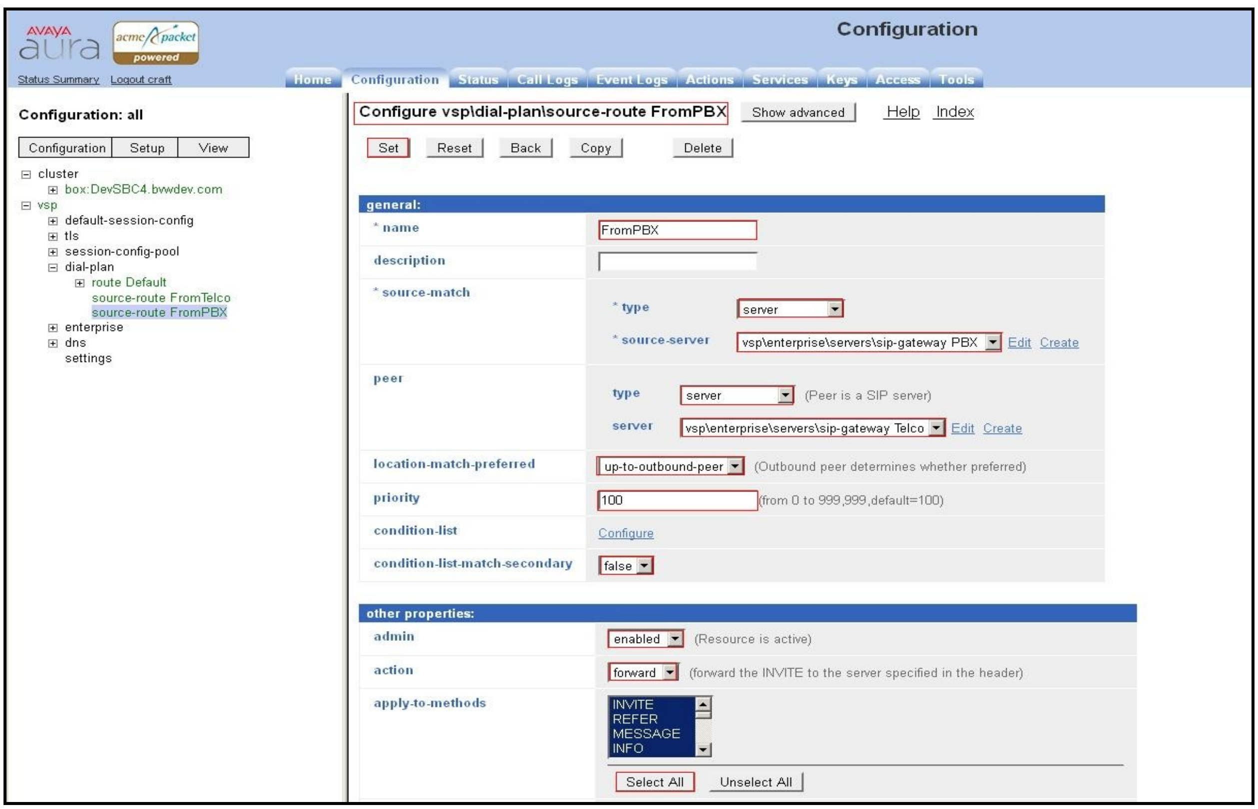

Figure 71: dial-plan “source-route FromPBX”

6.5.2. The entry "source-route FromTelco"

The entry "**source-route FromTelco**" as shown in **Figure 72** below is to route SIP calls from MTS Allstream to CS1000.

- **source-server**: vsp\enterprise\servers\sip-gateway **Telco**
- **peer server**: vsp\enterprise\servers\sip-gateway **PBX**
- **location-match-preferred**: up-to-outbound-peer
- **priority**: 100 (default)
- **condition-list-match-secondary**: false
- **other properties:**
  - **admin**: enabled
  - **action**: forward
  - **apply-to-methods**: Select All

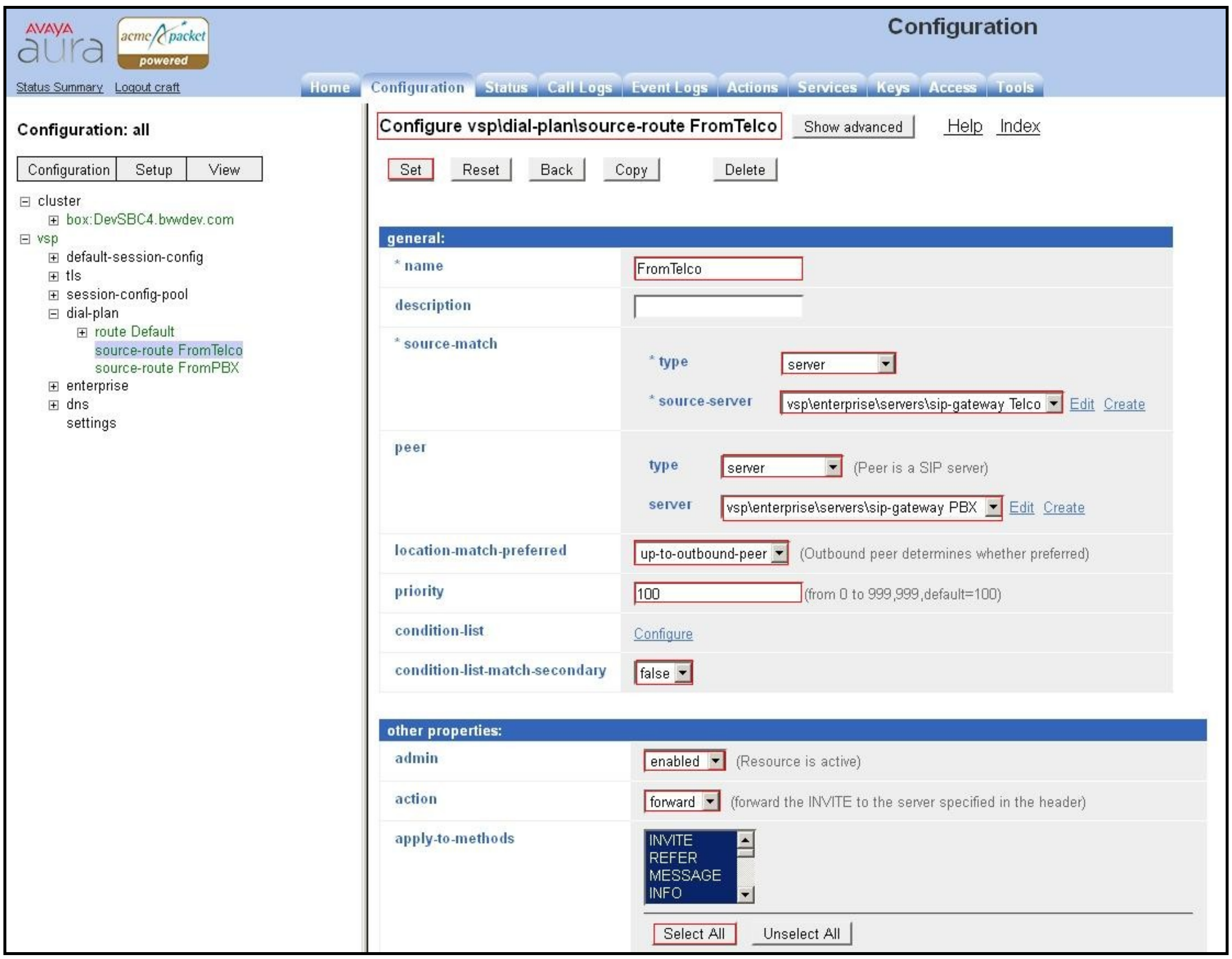

Figure 72: dial-plan "source-route Telco"

6.6. Administer session-config-pool “entry ToTelco”

6.6.1. Administer sip-settings

AA-SBC has a feature to re-transmit IP packets to prevent packet lost when travel over internet. By default, **max-retransmissions** value is set to 1. To increase **max-retransmissions**, select **Configuration vsp\session-config-pool\entry ToTelco\sip-settings\other properties,** and change the value of **max-retransmissions** from 1 to 5 as shown in **Figure 73.**

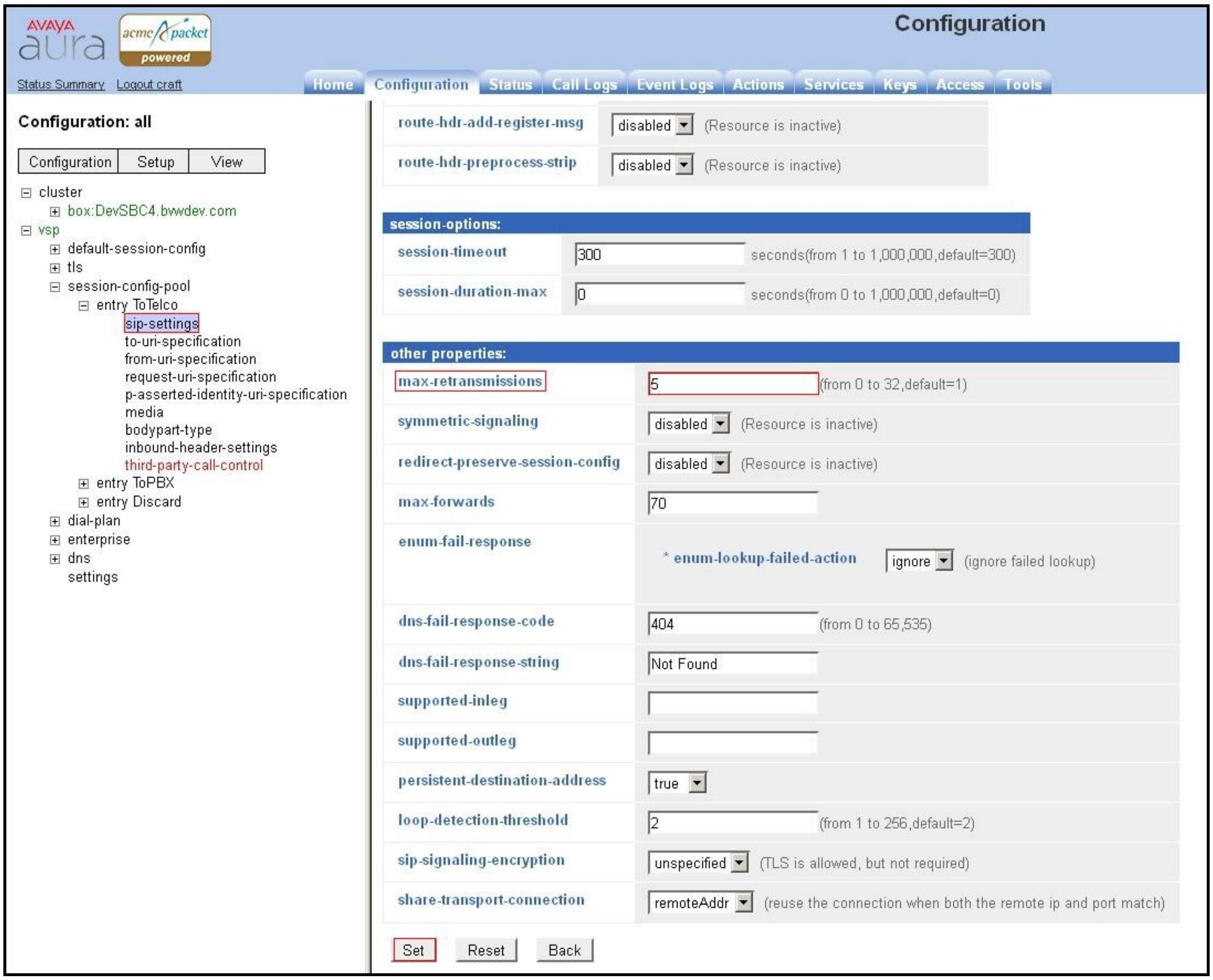

Figure 73: Increase the max- retransmissions

AA-SBC can **overwrite** the Quality of Service (DSCP) value for SIP packets. This value can be set at **Configuration vsp\session-config-pool\entry ToTelco\sip-settings\message options\outleg-tos**. **Figure 74** shows **outleg-tos** was set to **overwrite** with DSCP 20.

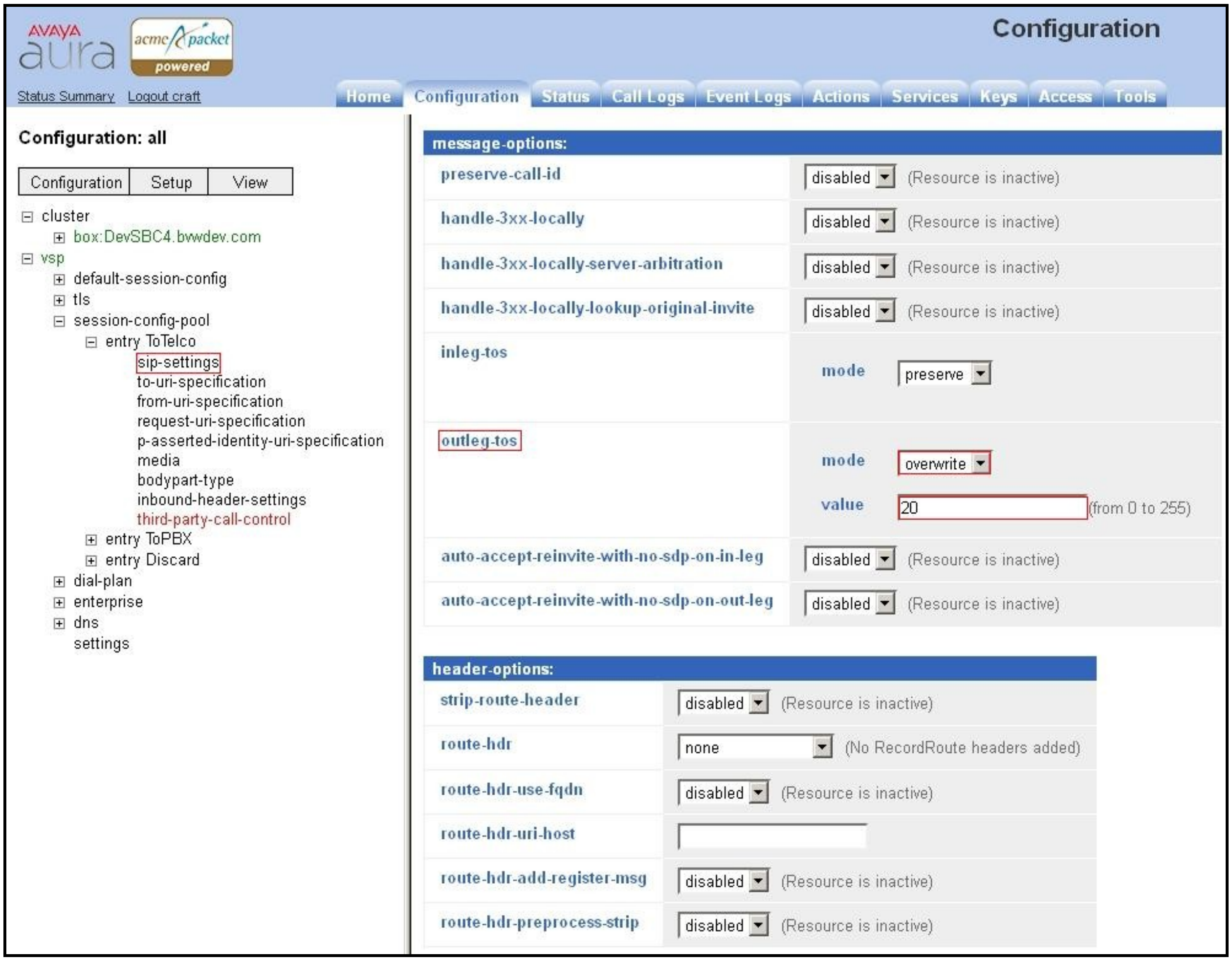

Figure 74: DSCP setting for SIP message

By default AA-SBC does not forward PRACK from CS1000 to MTS Allstream. It causes issue with ringback tone cannot be sent to PSTN in case of offnet call forward no answer. To enable PRACK forwarding, go to **Configuration vsp\session-config-pool\entry ToTelco\sip-settings** click "**Show advance**" (not shown), then under "**message-options**" set "**forward-provisional-ack**" to **enable** (as shown in **Figure 75**).

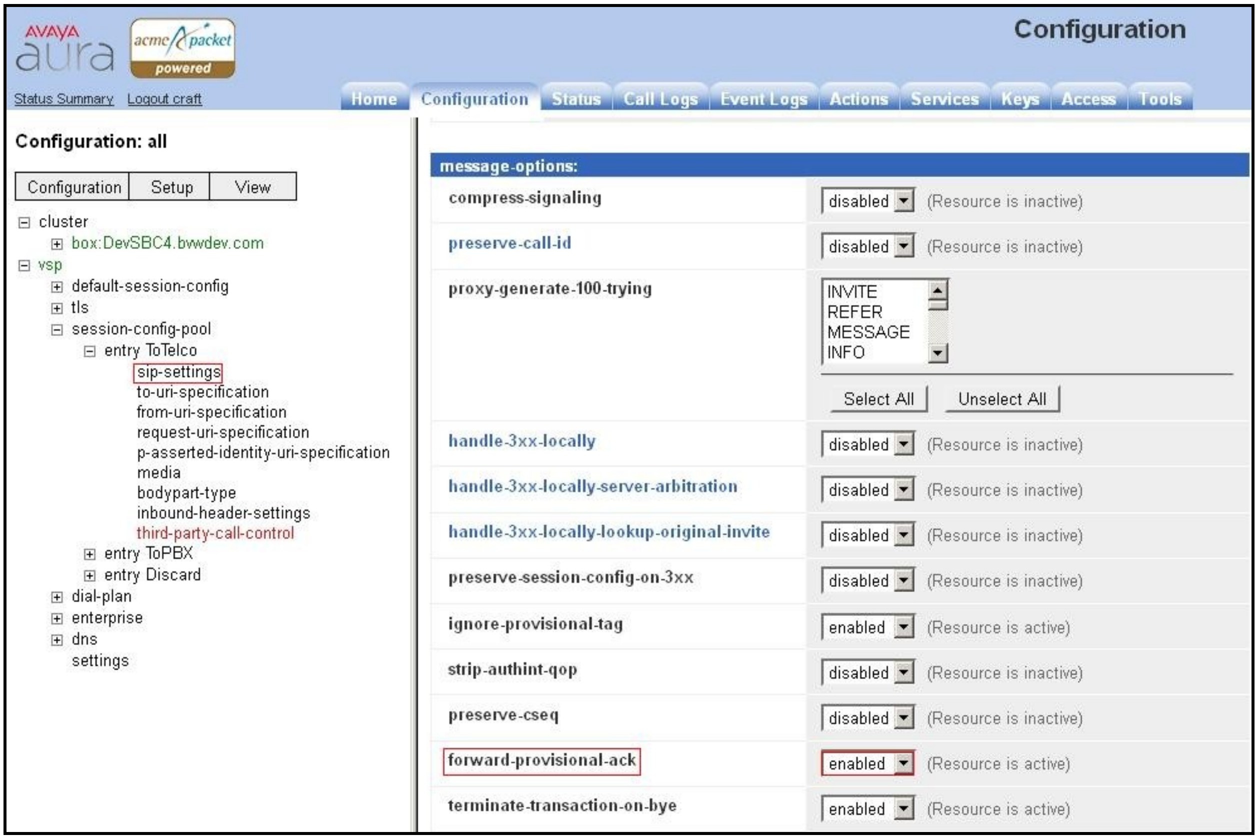

Figure 75: Enable PRACK forwarding

6.6.2. Manipulate From, To, Request-URI, and P-Asserted-Identity headers.

The CS1000 SIP gateway was configured with domain name mtsallstream.com (please refer to **Section 5.5**). However, MTS Allstream expects to receive IP address instead of a domain name.

This section shows the configuration on AA-SBC to change domain name mstallstream.com to an IP address. The change is applied to SIP headers From, To, Request-URI and P-Asserted-Identity.

a) Manipulate **From** header.
Select **Configuration vsp\session-config-pool\entry ToTelco\from-uri-specification.** Then change **host** to send **local-ip** as shown in **Figure 76.** AA-SBC presents its public IP address in the **From** header.

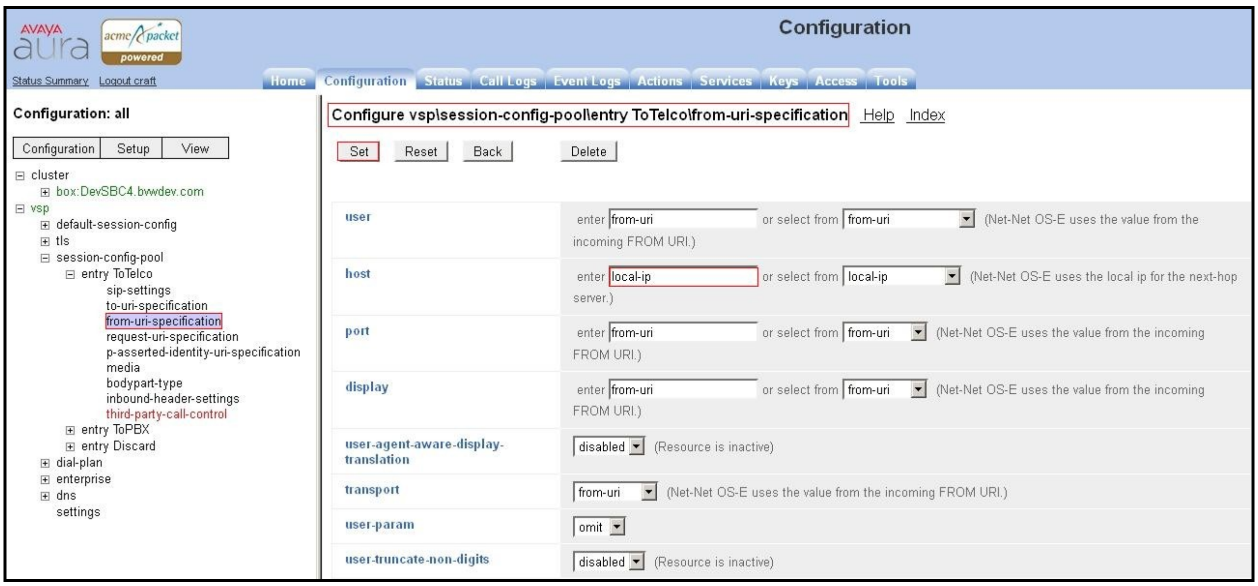

Figure 76: Manipulate From header of session-config-pool "entryToTelco"

b) Manipulate **To** header.
Select **Configuration vsp\session-config-pool\entry ToTelco\to-uri-specification.** Then change **host** to send **next-hop** as shown in **Figure 77.** AA-SBC presents MTS Allstream SBC IP address in the **To** header.

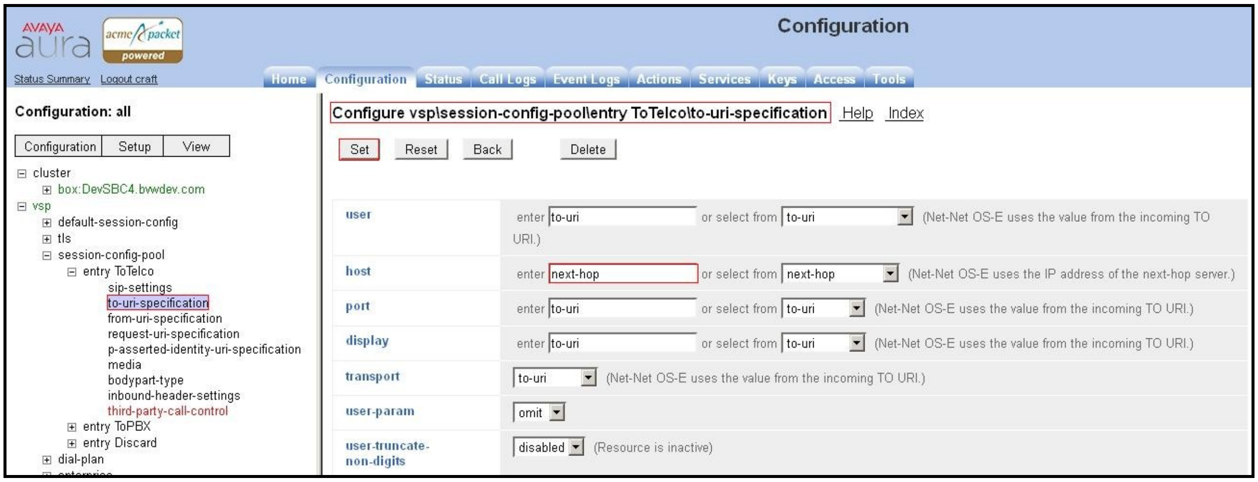

Figure 77: Manipulate To header of session-config-pool "entryToTelco"

c) Manipulate **Request-URI** header.
Select **Configuration vsp\session-config-pool\entry ToTelco\request-uri-specification.** Then change **host** to send **next-hop** as shown in **Figure 78.** AA-SBC presents MTS Allstream SBC IP address in the **Request-URI** header.

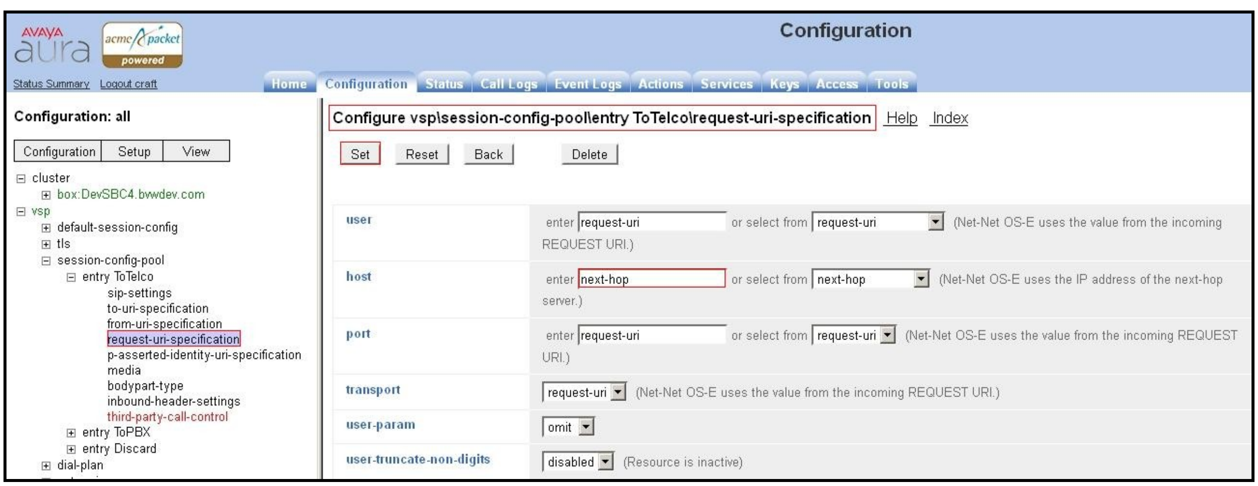

Figure 78: Manipulate Request-URI header of session-config-pool "entryToTelco"

d) Manipulate **P-Asserted-Identity** header.
Select **Configuration vsp\session-config-pool\entry ToTelco\p-asserted-identity-uri-specification.** Then change **host** to send **local-ip** as shown in **Figure 79.** AA-SBC presents its public IP address in the **P-Asserted-Identity** header.

Figure 79: Manipulate P-Asserted-Identity header of session-config-pool "entryToTelco"

6.6.3. Administer media

This session shows the configuration to enable media anchoring on AA-SBC and set DSCP value for RTP.

To enable media anchoring, select **Configuration vsp\session-config-pool\entry ToTelco\media.** Then change **anchor** to **enable** as shown in **Figure 80.**

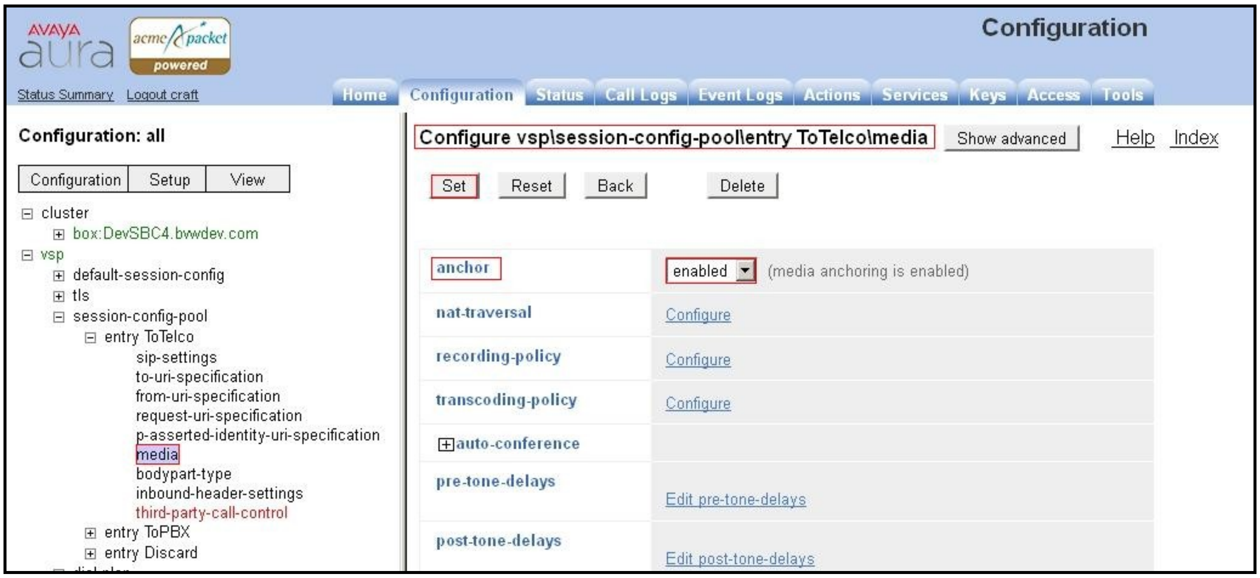

Figure 80: Enable media anchoring

AA-SBC can **overwrite** the Quality of Service (DSCP) value for RTP packets. This value can be set at **Configuration vsp\session-config-pool\entry ToTelco\media**. **Figure 81** shows **packet-marking** was set to **tos** with DSCP 60.

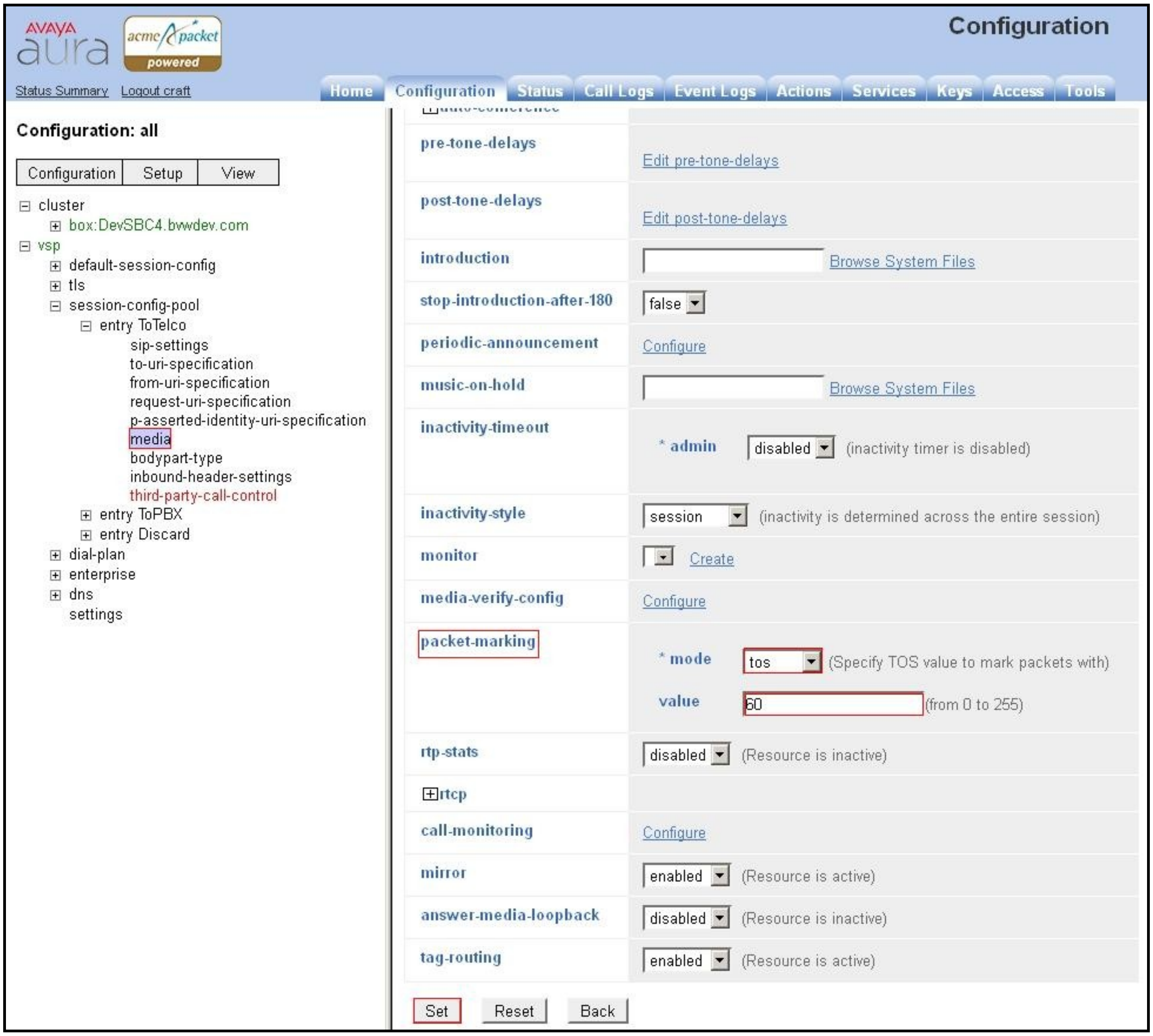

Figure 81: Define DSCP value for RTP

6.6.4. Administer bodypart-type to delete MIME/multiple parts in SIP message body

This section shows the configuration for **bodypart-type** of **“entry ToTelco”** to send only SDP part to MTS Allstream.

a) Add SDP to allowed-body-part.

Select **Configuration > vsp > session-config-pool > entry ToTelco > bodypart-type.** Click on link **Add allowed-body-part** as shown in **Figure 82.**

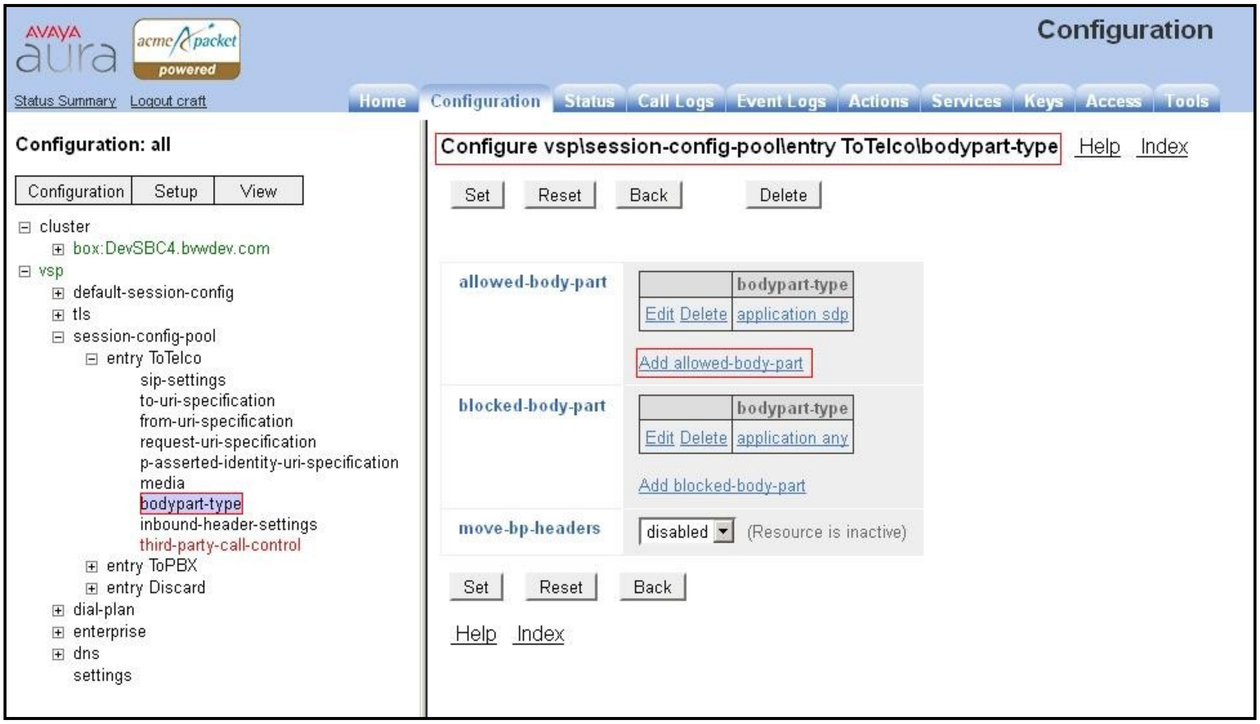

Figure 82: Add an allowed-body-part entry

b) Create a new entry to allow SDP body part. Select **bodypart-type** as **application**; **application sub-type** as **sdp** then click "**Create**" as shown in **Figure 83**.

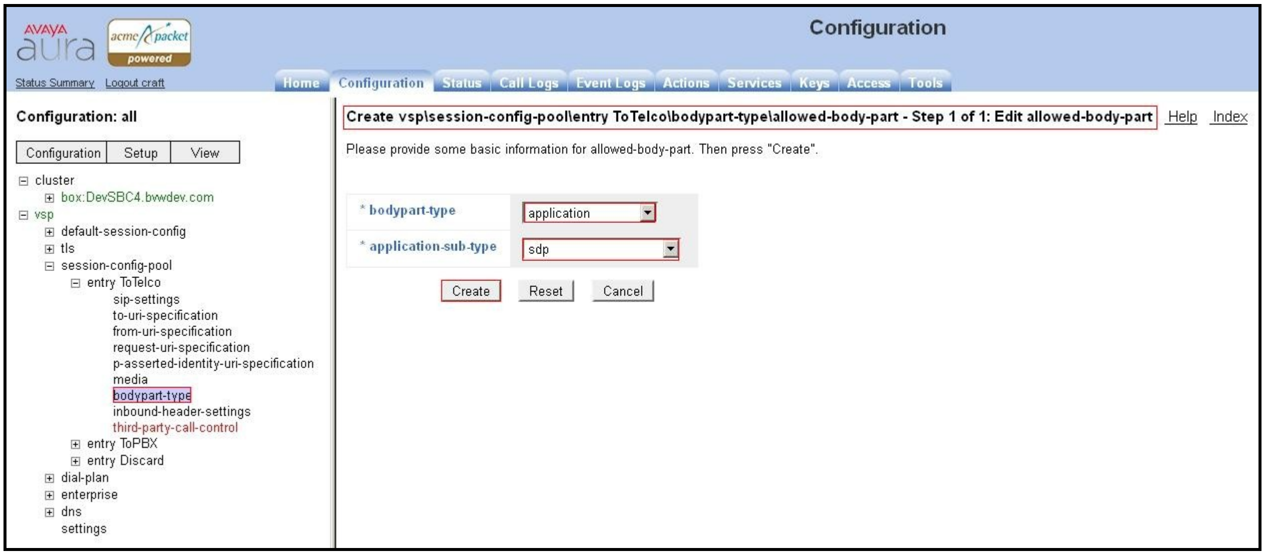

Figure 83: Create an entry to allow SDP body part

c) Configure AA-SBC to block all body parts other than SDP.
Select **Configuration > vsp > session-config-pool > entry ToTelco > bodypart-type.** Click on link **Add blocked-body-part** as shown in **Figure 84.**

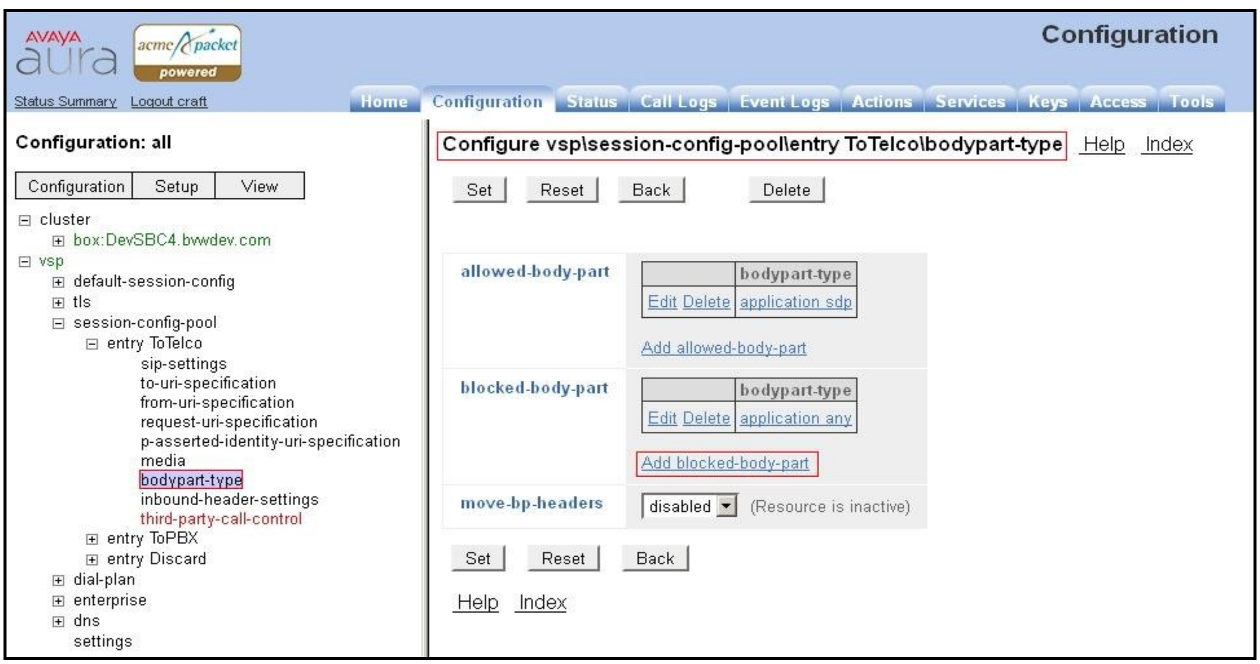

Figure 84: Add a blocked-body-part entry

d) Create a new entry to block other body parts. Select **bodypart-type** as **application**; **application sub-type** as **any** then click "**Create**" as shown in **Figure 85**.

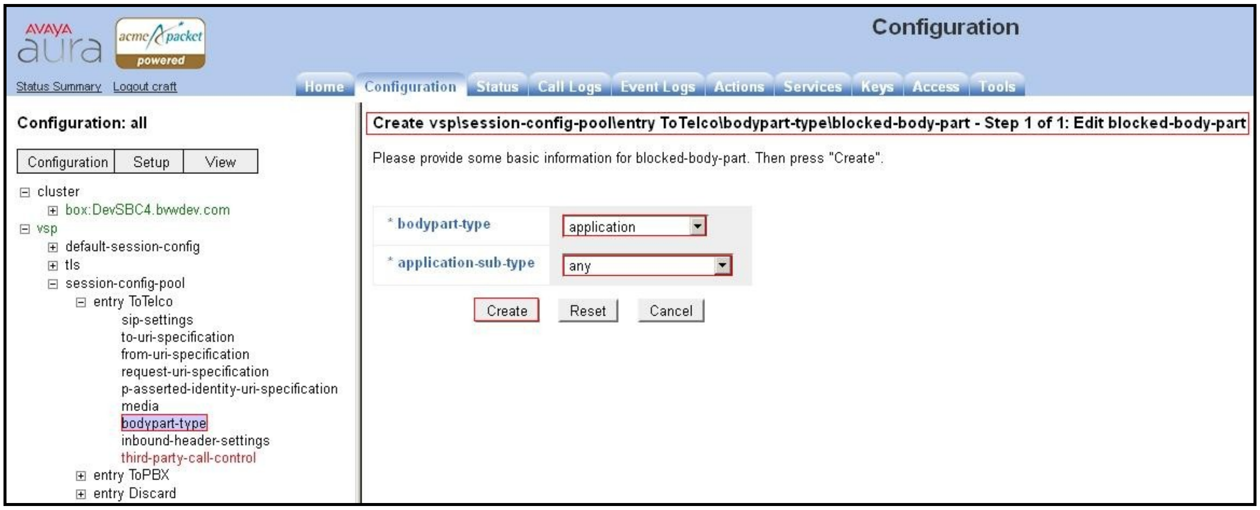

Figure 85: Create an entry to block body parts other than SDP

6.6.5. Administer inbound-header-setting to block X-nt-e164-clid, Alert-Info Request and P-Location headers

MTS Allstream SIP Trunking does not support X-nt-e164-clid, Alert-Info, Request and P-Location in SIP message headers for outbound calls. This section shows the configuration for **inbound-header-setting** of **"entry ToTelco"** to block mentioned headers to be sent to MTS Allstream.

Select **Configuration > vsp > session-config-pool > entry ToTelco > inbound-header-settings.** Click on link **Edid blocked-header** to add X-nt-e164-clid; Alert-Info; Request and P-Location to blocked headers as shown in **Figure 86.**

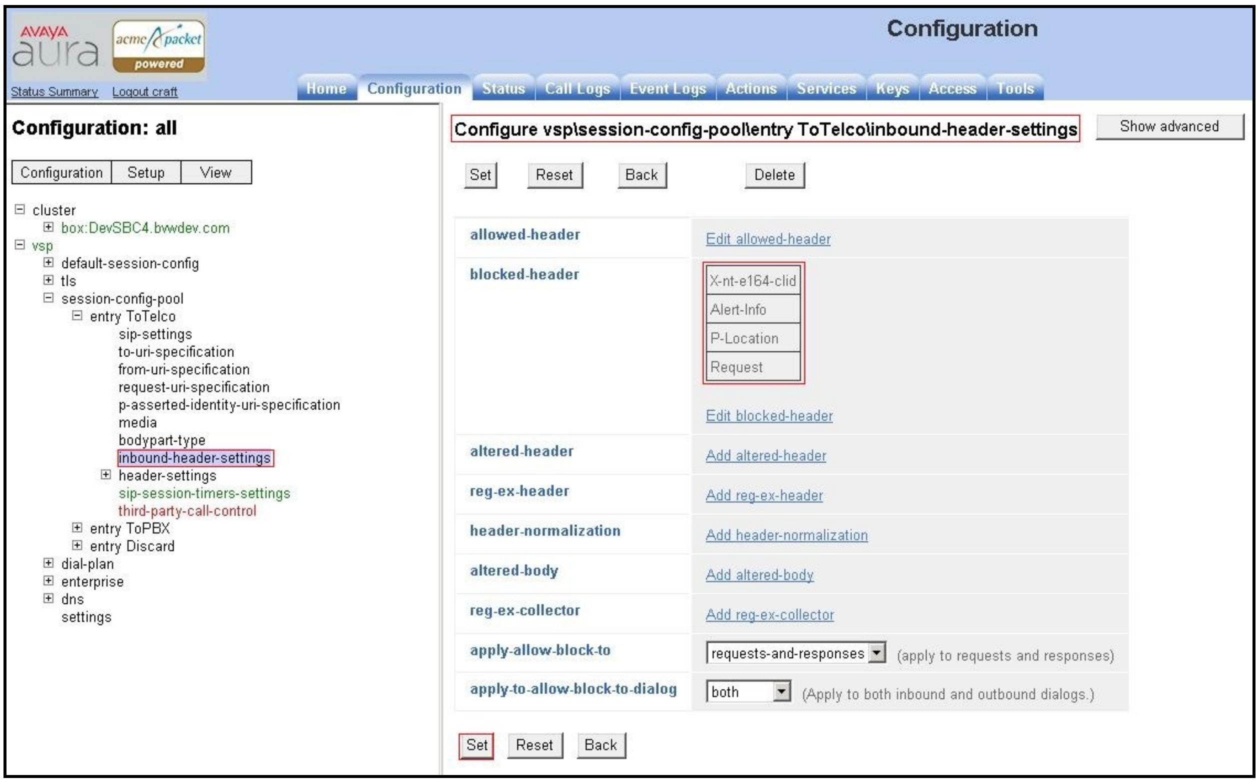

Figure 86: Edit blocked-header in inbound-header-settings

6.6.6. Administer sip-session-timers-setting

By default the **sip-session-timers-setting** was disabled on AA-SBC. The session timers should be turned on to let AA-SBC terminate the unsuccessfully call attempts to PSTN.

In order to support Session Timer, CS1000 system has to send header "Supported: timer" to MTS Allstream. But CS1000 does not send this header by nature. The following configuration in **Figure 87a**, shows how to configure AA-SBC **Configuration vsp\session-config-pool\entry ToTelco\header-setting\reg-ex-header20** to insert "Supported: timer".

- destination: Supported
- source: Supported
- expression: .*
- replacement: 100rel,timer
- apply-to-method: Select All
- apply-to-responses: both
- apply-to-dialog: both

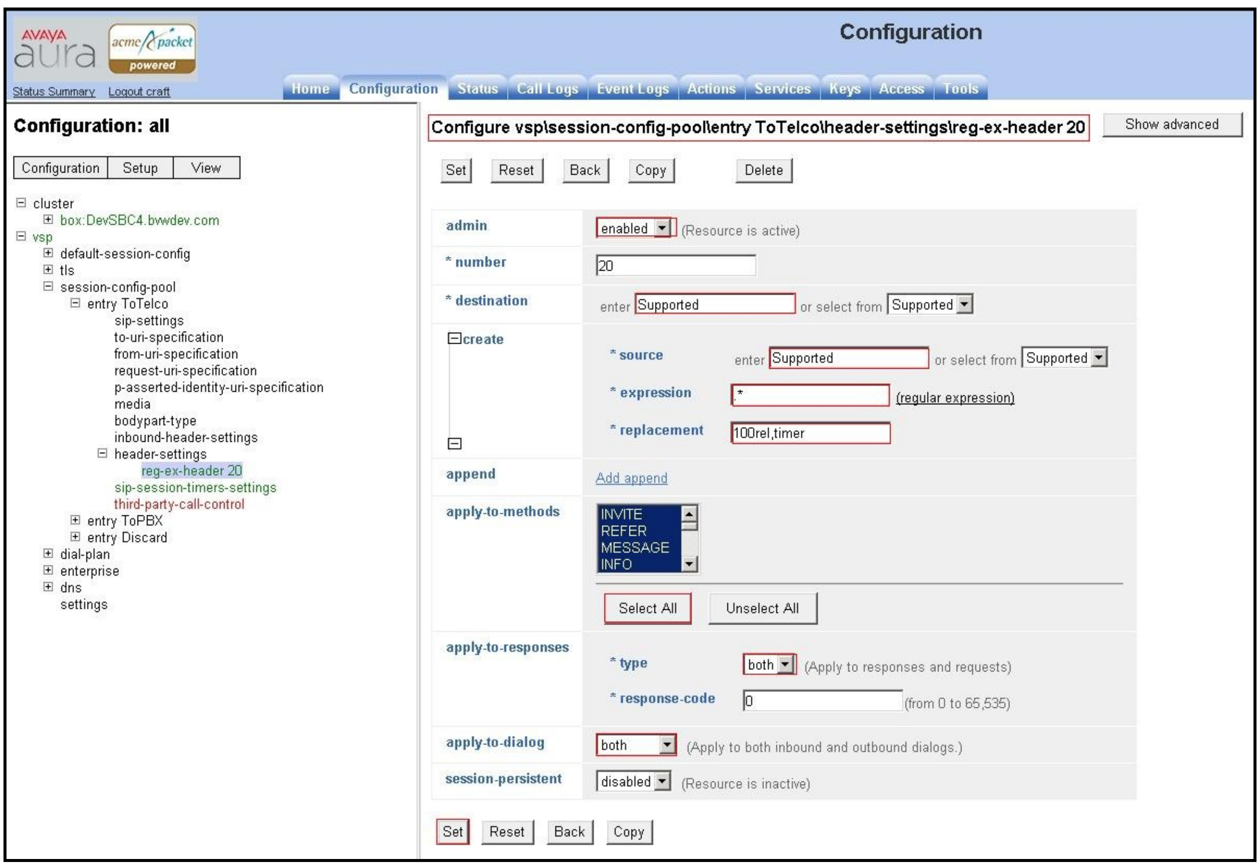

Figure 87a: Configure the regular expression to insert header "Supported: timer"

To enable **sip-session-timers-setting**, select **Configuration vsp\session-config-pool\entry ToTelco\ sip-session-timers-setting.** Then change **admin** state to **enable** as shown in **Figure 87b.** The refresher was configured to **UAS** to let MTS Allstream in charge of refreshing the session timer. MTA Allstream sets Min-SE 600 for SIP Trunk, so the Session-Expires has to be set 600 or greater. In this testing Session-Expires was set to 600, it means every 300 seconds the session refresher (MTA Allstream) will send UPDATE.

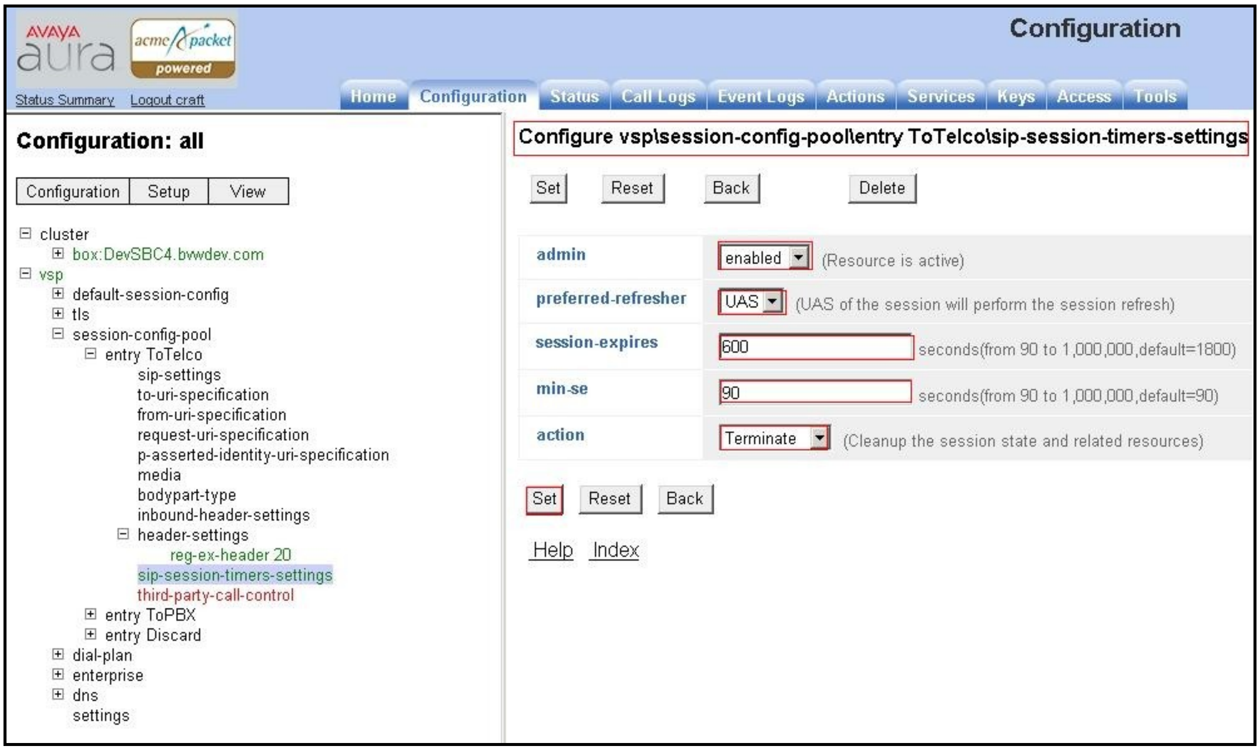

Figure 87b: Enable SIP session timers

6.6.7. Disable third-party-call-control

The third-party-call-control should be disabled on AA-SBC to interwork with MTS Allstream.

To disable **third-party-call-control**, select **Configuration > vsp > session-config-pool > entry ToTelco > third-party-call-control.** Then change the **admin** state to **disabled** as shown in **Figure 88.**

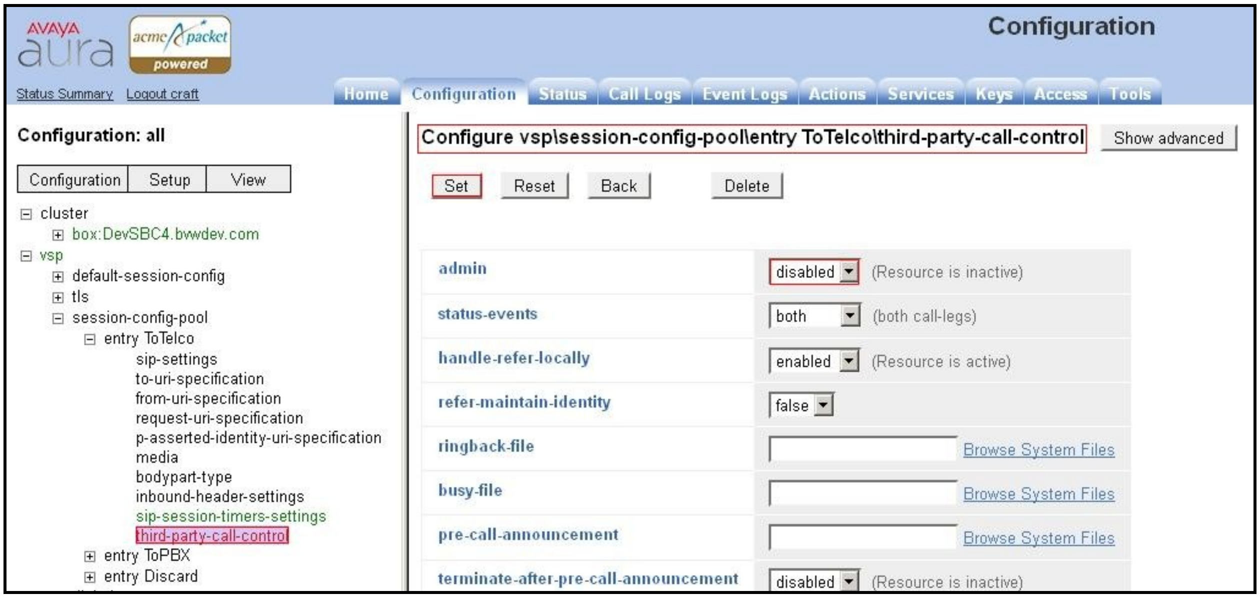

Figure 88: Disable third-party-call-control

6.7. Administer session-config-pool "entry ToPBX"

6.7.1. Manipulate To, Request-URI headers.

The CS1000 SIP gateway was configured with domain name mtsallstream.com (please refer to **Section 5.5**). However, MTS Allstream prefers to IP address in SIP headers. This section shows the configuration on AA-SBC to manipulate SIP headers To and Request-URI before sending to CS1000.

a) Manipulate **To** header.
Select **Configuration vsp\session-config-pool\entry ToPBX\to-uri-specification.** Then change **host** to send **next-hop-domain** as shown in **Figure 89.** AA-SBC presents domain **mtsallstream.com** in the **To** header sent to CS1000.

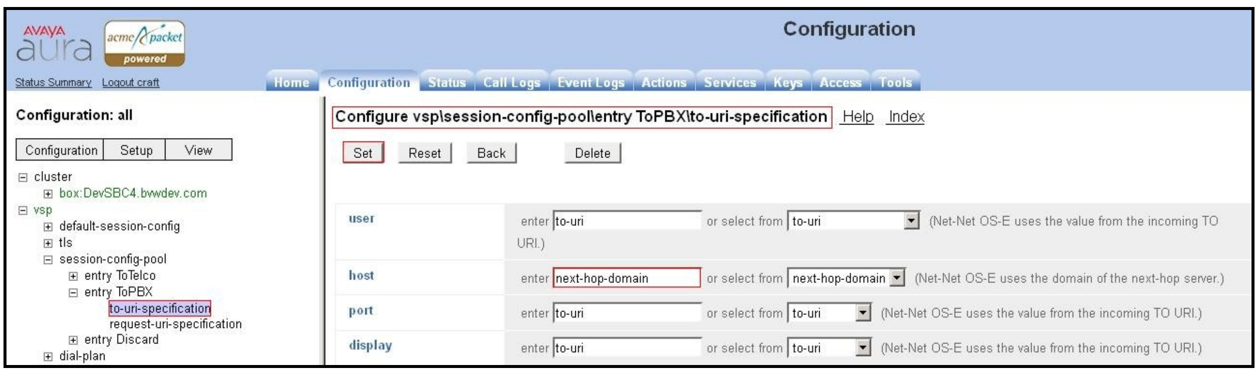

Figure 89: Manipulate To header of session-config-pool "entryToPBX"

b) Manipulate **Request-URI** header.
Select **Configuration vsp\session-config-pool\entry ToPBX\request-uri-specification.** Then change **host** to send **next-hop-domain** as shown in **Figure 90.** AA-SBC presents domain **mtsallstream.com** in the **Request-URI** header sent to CS1000.

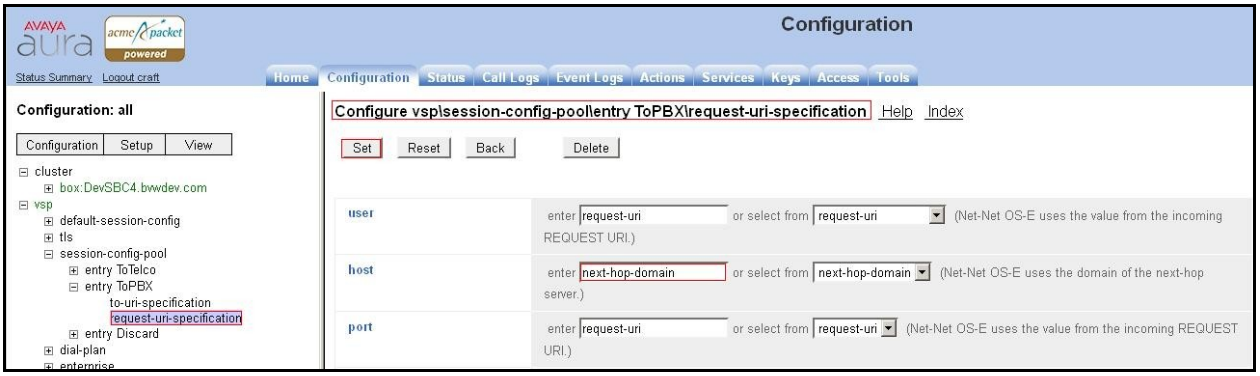

Figure 90: Manipulate Request-URI header of session-config-pool "entryToPBX"

6.7.2. Administer media

This session shows the configuration to enable media anchoring on AA-SBC.

To enable media anchoring, select **Configuration vsp\session-config-pool\entry ToPBX\media.** Then change **anchor** to **enable** as shown in **Figure 91.**

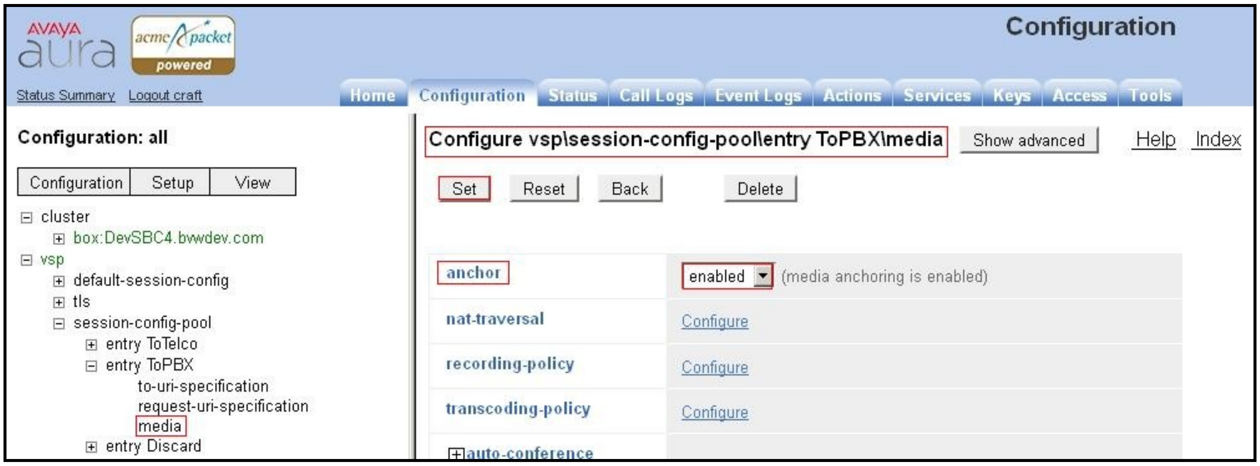

Figure 91: Enable media anchor

6.7.3. Administer inbound-header-setting to block X-nt-e164-clid, Alert-Info Request and P-Location headers

MTS Allstream SIP Trunking does not support X-nt-e164-clid, Alert-Info, Request and P-Location in SIP message headers for outbound calls. This section shows the configuration for **inbound-header-setting** of **"entry ToPBX"** to block mentioned headers to be sent to MTS Allstream.

Select **Configuration > vsp > session-config-pool > entry ToPBX > inbound-header-settings.** Click on link **Edid blocked-header** to add X-nt-e164-clid; Alert-Info; Request and P-Location to blocked headers as shown in **Figure 92.**

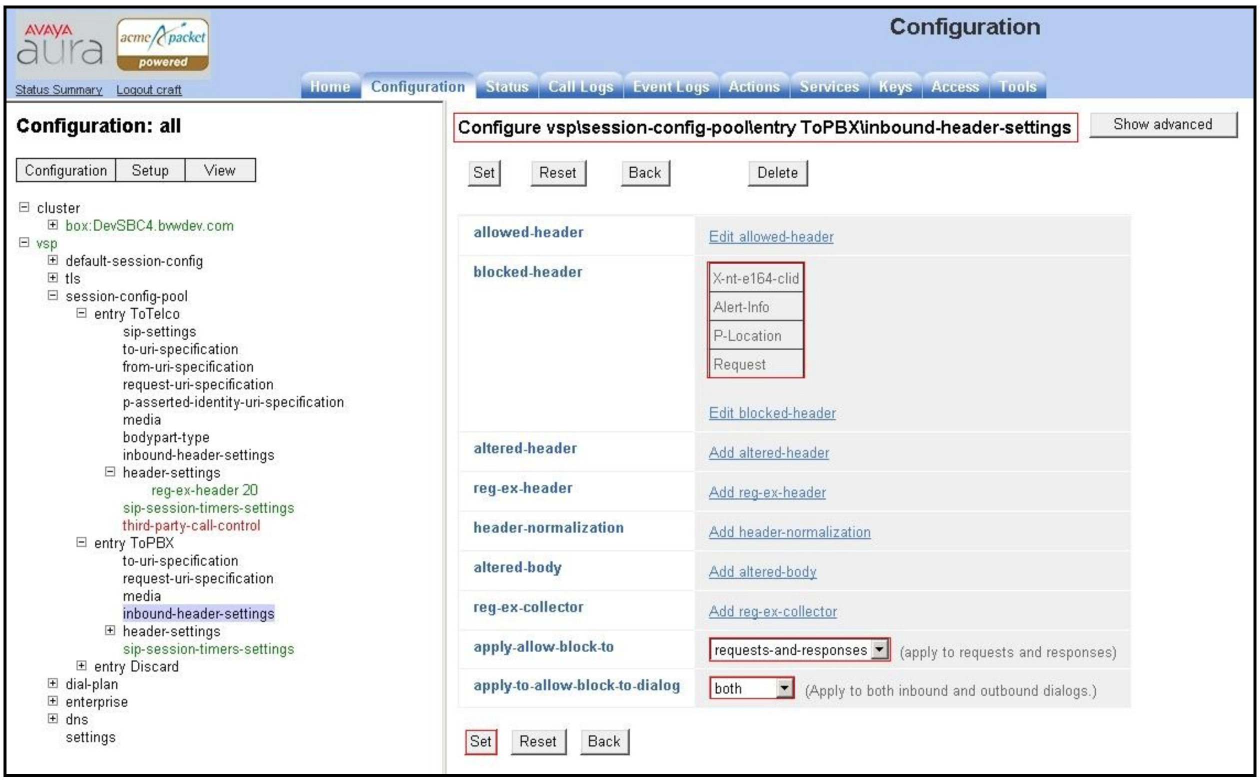

Figure 92: Edit blocked-header in inbound-header-settings

6.7.4. Administer sip-session-timers-setting

By default the **sip-session-timers-setting** was disabled on AA-SBC. The session timers should be turned on to let AA-SBC terminate the unsuccessfully call attempts to PSTN.

In order to support Session Timer, CS1000 system has to send header “Supported: timer” to MTS Allstream. But CS1000 does not send this header by nature. The following configuration in **Figure 93a**, shows how to configure AA-SBC **Configuration vsp\session-config-pool\entry ToPBX\header-setting\reg-ex-header20** to insert “Supported: timer”.

- destination: Supported
- source: Supported
- expression: .*
- replacement: 100rel,timer
- apply-to-method: Select All
- apply-to-responses: both
- apply-to-dialog: both

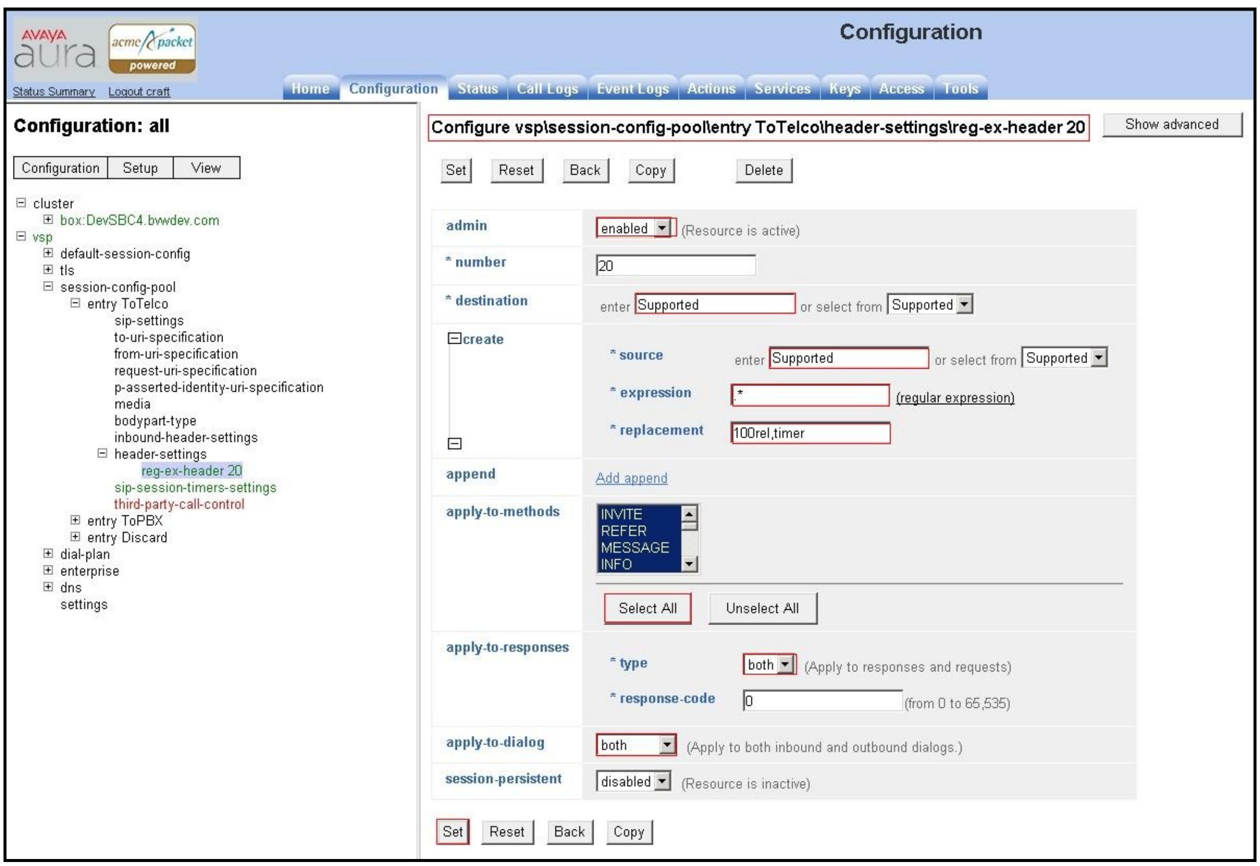

Figure 93a: Configure the regular expression to insert header “Supported: timer”

To enable **sip-session-timers-setting**, select **Configuration vsp\session-config-pool\entry ToTelco\ sip-session-timers-setting.** Then change **admin** state to **enable** as shown in **Figure 93b.** The refresher was configured to **UAC** to let MTS Allstream in charge of refreshing the session timer. MTA Allstream sets Min-SE 600 for SIP Trunk, so Session-Expires has to be set 600 or greater. In this testing Session-Expires was set to 600, it means every 300 seconds the session refresher (MTA Allstream) will send UPDATE.

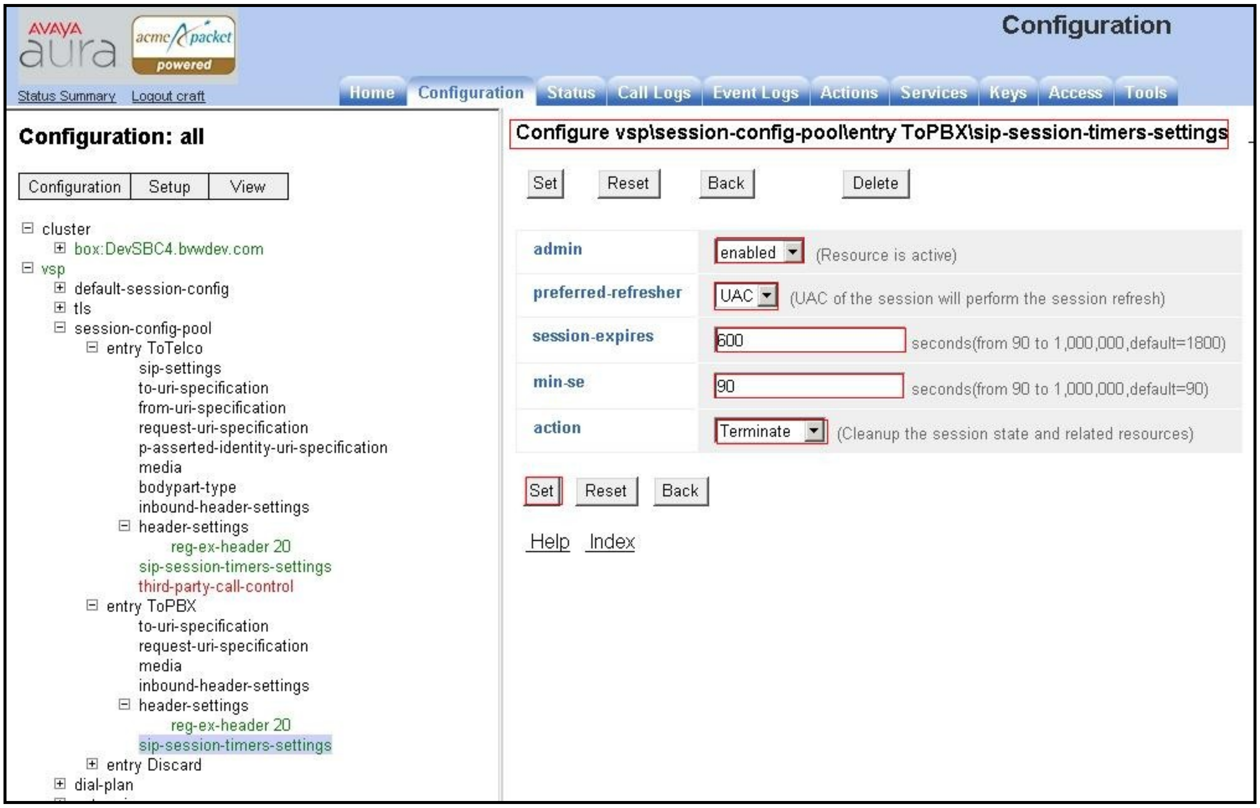

Figure 93b: Enable SIP session timers

7. Verification Steps

The following steps may be used to verify the configuration.

7.1. General

Place an **inbound/ outbound** call from/ to a PSTN phone to/ from an internal CS1000 phone, answer the call, and verify that two-way speech path exists. Check call display name and number to ensure the correct information was sent/ received. Perform hold/ retrieve. Verify the call remains stable for several minutes and disconnect properly.

7.2. Verify Call Establishment on CS1000 Call Server

a) Active Call Trace (LD 80)

The following is an example of one of the commands available on CS1000 to trace the DN when the call is in progress. The call scenario involved the PSTN phone number 6139675258 calling 6477761230 on CS1000.

- Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
- Login to the Overlay command prompt, issue the command **LD 80** and then **trace 4 1230**.
- After the call is released, issue the command **trac 4 1230** again to see if the DN is released back to idle state.

Below is the actual output of the Call Server Command Line mode when the 1230 is in call state:

```
>ld 80
>*ld 80
TRA000
.trac 4 1230

ACTIVE  VTN 108 0 00 18

ORIG   VTN 100 1 01 00   VTRK IPTI  RMBR  104 1 INCOMING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 207.245.2.12
  FAR-END MEDIA ENDPOINT IP: 135.10.97.216  PORT: 21320
  FAR-END VendorID: AVAYA-SM-6.1.1.0.611023
TERM   VTN 108 0 00 18  KEY 0  SCR MARP  CUST 4  DN 1230  TYPE 1140
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 135.10.98.133  PORT: 5200
MEDIA PROFILE: CODEC G.729A NO-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 1230
MAIN_PM  ESTD
TALKSLOT  ORIG  88   TERM  61
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 34784
```

```
----  ISDN ISL CALL (ORIG) ----
CALL REF # =  387
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  6139675258  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
CALLED NO  =  6477761230  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
```

And this is the example after the call on 4685 is completed.

```
.trac 4 1230

IDLE VTN 108 0 00 18   MARP
```

b) SIP Trunk monitoring (LD 32)

Place an inbound call from PSTN (6139675258) to CS1000 (9729414685). Then check the SIP Trunk status by using LD 32.

```
>ld 32
NPR000
.stat 100 1
063 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
.
```

And this is the example after the call is completed; the BUSY trunk changes its state to IDLE.

```
.stat 100 1
064 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
.
```

7.3. Protocol Traces

Below are Wireshark traces of the same call scenario that has been made in **Section 7.2**.

The following SIP headers are inspected:

- RequestURI: verify the request number and either SIP domain
- From: verify the display name and display number.
- To: verify the display name and display number.
- History-Info: verify the call forward information and reason code.
- P-Asserted-Identity: verify the display name and display number.

The following attributes in SIP message body are inspected:

- Connection Information (c): verify IP address of far end endpoint
- Time Description (t): verify session timeout of far end endpoint
- Media Description (m): verify audio port, codec, DTMF event description
- Media Attribute (a): verify specific audio port, codec, ptime, send/ receive ability, DTMF event and fax attributes.

a) Outbound calls.

The SIP/INVITE from CS1000 to MTS Allstream was captured at Avaya Aura® Session Border Controller OUTSIDE interface.

INVITE sip:16139675258@220.20.2.12 SIP/2.0
From: "mts 1230" <sip:6477761230@110.10.98.108>;tag=6c620a87-13c4-4e666911-3137c662-511bdc37
To: <sip:16139675258@220.20.2.12>
Call-ID: CXC-101-5c412850-6c620a87-13c4-4e666911-3137c662-2f2f46d1@110.10.98.108
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.10.98.108:5060;branch=z9hG4bK-285b1-4e666911-3137c662-4f7fb5a4
Supported: 100rel,x-nortel-sipvc,replaces
User-Agent: Nortel CS1000 SIP GW release_7.0 version_linux-6.50.00 AVAYA-SM-6.1.1.0.611023
P-Asserted-Identity: "mts 1230" <sip:6477761230@110.10.98.108>
Privacy: none
History-Info: <sip:16139675258@mtsallstream.com;user=phone>;index=1
Max-Forwards: 65
Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
Contact: <sip:6477761230@110.10.98.108:5060;maddr=110.10.98.108;transport=udp>
Min-SE: 90
Session-Expires: 1800
Content-Type: application/SDP
Content-Length: 263

v=0
o=- 79 1 IN IP4 110.10.98.108
s=-
c=IN IP4 135.10.98.108
t=0 0
m=audio 20320 RTP/AVP 18 0 8 101 111
c=IN IP4 135.10.98.108
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 X-nt-inforeq/8000
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=ptime:20
a=sendrecv

The SIP/200OK MTS Allstream to CS1000 was captured at Avaya Aura® Session Border Controller OUTSIDE interface.

SIP/2.0 200 OK
Via: SIP/2.0/UDP 110.10.98.108:5060;branch=z9hG4bK-285b1-4e666911-3137c662-4f7fb5a4
To: <sip:16139675258@220.20.2.12>;tag=3524323349-604795
From: "mts 1230" <sip:6477761230@110.10.98.108>;tag=6c620a87-13c4-4e666911-3137c662-511bdc37
Call-ID: CXC-101-5c412850-6c620a87-13c4-4e666911-3137c662-2f2f46d1@135.10.98.108
CSeq: 1 INVITE
Allow: INVITE, BYE, OPTIONS, CANCEL, ACK, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:16139675258@220.20.2.12:5060>
Call-Info: <sip:220.20.2.12>;method="NOTIFY;Event=telephone-event;Duration=1000"
Content-Type: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 529412758 529412758 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 31964 RTP/AVP 18 0 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

b) Inbound calls.

The SIP/INVITE from MTS Allstram to CS1000 was captured at Avaya Aura® Session Border Controller OUTSIDE interface.

INVITE sip:6477761230@110.10.98.108;user=phone SIP/2.0
Max-Forwards: 69
Session-Expires: 3600;refresher=uac
Min-SE: 600
Supported: timer, 100rel
To: <sip:6477761230@110.10.98.108;user=phone>
From: <sip:6139675258@220.20.2.12;user=phone>;tag=3524324116-575879
P-Asserted-Identity: <sip:6139675258@220.20.2.12;user=phone>
Call-ID: 118327-3524324116-575873@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Allow: INVITE, BYE, OPTIONS, CANCEL, ACK, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bK71df5f993f6beda8d0e8f5137d6140a3
Contact: <sip:6139675258@220.20.2.12:5060;tgrp=TOROONSBCIOT1>
Call-Info: <sip:220.20.2.12>;method="NOTIFY;Event=telephone-event;Duration=1000"
Content-Type: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 537084383 537084383 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 31986 RTP/AVP 18 0 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

The SIP/200OK MTS Allstream to CS1000 was captured at Avaya Aura® Session Border Controller OUTSIDE interface.

SIP/2.0 200 OK
From: <sip:6139675258@220.20.2.12;user=phone>;tag=3524324116-575879
To: <sip:6477761230@110.10.98.108;user=phone>;tag=6c620a87-13c4-4e666c12-314380e5-37050cb4
Call-ID: 118327-3524324116-575873@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Supported: 100rel,x-nortel-sipvc,replaces
Require: timer

User-Agent: Nortel CS1000 SIP GW release_7.0 version_linux-6.50.00
P-Asserted-Identity: "mts 1230" <sip:6477761230@mtsallstream.com;user=phone>
Privacy: none
Server: AVAYA-SM-6.1.1.0.611023
Request:
Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSC
RIBE,UPDATE
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bK71df5f993f6beda8d0e8f5137d6140a3
Contact:
<sip:6477761230@110.10.98.108:5060;user=phone;maddr=110.10.98.108;transport=udp>
Content-Type: application/sdp
Content-Length: 259

v=0
o=- 85 1 IN IP4 110.10.98.108
s=-
c=IN IP4 135.10.98.108
t=0 0
m=audio 20264 RTP/AVP 18 101 111
c=IN IP4 135.10.98.108
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=sendrecv

8. Conclusion

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test result met the objectives outlined in **Section 2.1**. The MTS Allstream system is considered **compliant** with Avaya Communication Server 1000 Release 7.5.

9. Additional References

Product documentation for Avaya products may be found at:
http://support.avaya.com/css/appmanager/public/support

[1] *Network Routing Service Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.*

[2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010*

[3] *Communication Server 1000E Overview, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011*

[4] *Communication Server 1000 Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011*

[5] *Communication Server 1000 Dialing Plans Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010*

[6] *Product Compatibility Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011*

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.