Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunking Service with Avaya Communication Server 1000 Release 7.5 and Avaya Session Border Controller for Enterprise Release 4.0.5 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between MTS Allstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 7.5, Avaya Session Border Controller for Enterprise 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for Enterprise.

MTS Allstream is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing is conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between MTS Allstream SIP Trunking Service (MTS Allstream) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 (CS1000) 7.5, Avaya SBC for Enterprise (Avaya SBCE) 4.0.5 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with MTS Allstream are able to place and receive PSTN calls via a broadband connection. This converged network solution is an alternative to traditional PSTN trunk such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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

MTS Allstream is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to MTS Allstream via the public internet and exercise the features and functionalities listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

To verify MTS Allstream SIP Trunking Service interoperability, the following features and functionalities are covered during the compliance testing:

- Request and response to SIP OPTIONS heartbeat.
- Inbound PSTN call to various phone types including UNIStim, SIP, PC2050 softphone, Avaya one-X® Communicator SIP softphone, digital and analog telephones at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN call from various phone types including UNIStim, SIP, PC2050 softphone, Avaya one-X® Communicator SIP softphone, digital and analog telephones at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Dialing plans including local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411)… etc.
- Calling party presentation and calling party restriction (private call).
- Proper codec negotiation with G.729 and G.711MU codecs.
- Proper early media transmission with G.729 and G.711MU codecs.
- Inbound and outbound fax over IP using G.711MU codec.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.

- Music on hold.
- User features such as hold and resume and conference.
- Off-net call transfer with re-INVITE method.
- Off-net call forwarding using Diversion method.
- Mobility Extension (MobX) to cellular phone.
- Response to incomplete call attempts and trunk errors.
- Session Timers refresh implemented by service provider.

Items are not supported or not tested including the following:

- Inbound toll-free and outbound emergency calls (911) are supported but are not tested as part of the compliance testing because MTS Allstream has not provided the necessary configuration.
- Fax over IP using T.38 codec is not supported.
- Off-net call forward using History-Info method is not supported.

2.2. Test Results

Interoperability testing of MTS Allstream SIP Trunking Service with the Avaya SIP-enabled enterprise solution is completed with successful results for all test cases with the exception of the observations/limitations described below.

1. **MTS Allstream does not refresh the Session Timer**. MTS Allstream sends an inbound initial INVITE with "*Session-Expires: 3600; refresher: uac Min-SE: 600*". It means, as a user agent client, MTS Allstream should refresh the Session Timer every 300 seconds by reINVITE or UPDATE SIP message. In other case of outbound calls, MTS Allstream does not send Session Timer signaling in the response either. This compliance testing observed that the CS1000 did not receive Session Timer refresh signaling for any inbound or outbound calls. This is a known issue of MTS Allstream SIP Trunking Service with no available resolution at this time.

2. **The untrusted Calling Party Name (CPN) from the CS1000 is not examined**. In an outbound call scenario, PSTN displays the original untrusted CPN from the CS1000. MTS Allstream does not examine the CPN before sending to PSTN. This is a known issue of MTS Allstream SIP Trunking Service with no available resolution at this time.

3. **The calling party name for outbound call is not consistent**. In an outbound call scenario, the CS1000 sends both calling party name and number to PSTN. But in some cases, PSTN phone displays the calling party number only and no calling party name. In other cases, PSTN phone displays both calling party name and number. The calling party name may be overridden by MTS Allstream or by intermediate service providers that route the call through PSTN. This issue has low user impact and is listed here simply as an observation.

4. **A CS1000 SIP phone calls local UNIStim phone then blind transfers to PSTN causes the calling party number to change**. The call successfully transfers, however, the UNIStim phone displays Route ACOD – Trunk Channel ID instead of displaying PSTN calling party name and number. This is a known behavior of the CS1000 with no

resolution available at this time. This issue has low user impact and is listed here simply as an observation.

5. **When a CS1000 UNIStim phone places an external call on hold and retrieves the call causes the calling party number to change**. After retrieving a held external call, the calling party number previously displayed on the CS1000 phone is replaced by Route ACOD – Trunk Channel ID. This is a known behavior of the CS1000 with no resolution available at this time. This issue has low user impact and it is listed here simply as an observation.

6. **Off-net call transfer, the calling party name and number are not updated to PSTN parties**. When the CS1000 transfers off-net an inbound call to PSTN, it does not update true connected calling party name and number to PTSN parties. It means both PSTN parties still display the calling party name and number of the CS1000 extension. This is a known behavior of the CS1000 when it interoperates with MTS Allstream where the CS1000 proprietary signaling is not supported. This issue has low user impact and is listed here simply as an observation.

7. **The CS1000 SIP phone transfers off-net to PSTN fails with Music On Hold enabled**. In an inbound or outbound call between the CS1000 SIP phone and PSTN_1, the CS1000 SIP phone performs an off-net transferring to PSTN_2. The call fails to transfer. PSTN_1 continues to hear ringback tone after the call has already been answered by PSTN_2. The same call scenario is successful when SIP phone is replaced by other endpoints .e.g. UNIStim or digital phones. This issue is resolved when Music On Hold is disabled. A product defect has been reported to Avaya team for investigation but there is no resolution available at this time. This issue is listed here as a limitation.

8. **Cellular Voice Mail Avoidance of Mobility Extension (MobX) is corrected and working properly**. When an inbound call being answered by cellular voice mail, the **Mobile extension timer** (MBXT) setting on the SIP route as described in **Section 5.5.6**, cannot ignore the answering as expected. The call then is unexpectedly connected to cellular voice mailbox instead of being connected to enterprise voice mailbox (Call Pilot). This issue has been corrected by patch MPLR32246 With the patch in-service, the answering by cellular voice mail before MBXT will be ignored allowing the inbound call to route to Call Pilot.

9. **Performing an "Application Restart" on Avaya SBCE causes SigmaScript to stop working**. If the SigMa script does not work after an "Application Restart", please contact Avaya for support on the Avaya SBCE by telephone numbers +1-866-861-3113 toll free or +1-214-269-2424. A product defect has been reported to Avaya team for investigation but there is no resolution available at this time. This issue is listed here as a limitation.

2.3. Support

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

For technical support on MTS Allstream SIP Trunking Service, please contact MTS Allstream technical support at:

- Phone: 204-225-5687 or 1-800-883-2054
- Website: http://www.mts.ca/support

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the MTS Allstream SIP Trunking Service (vendor validation circuit) through a public Internet connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance testing are not shown in these Application Notes.

Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to MTS Allstream via internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and MTS Allstream across the public network is UDP; the transport protocol between the Avaya SBCE and the CS1000 across the enterprise network is TCP.

Figure 1 below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

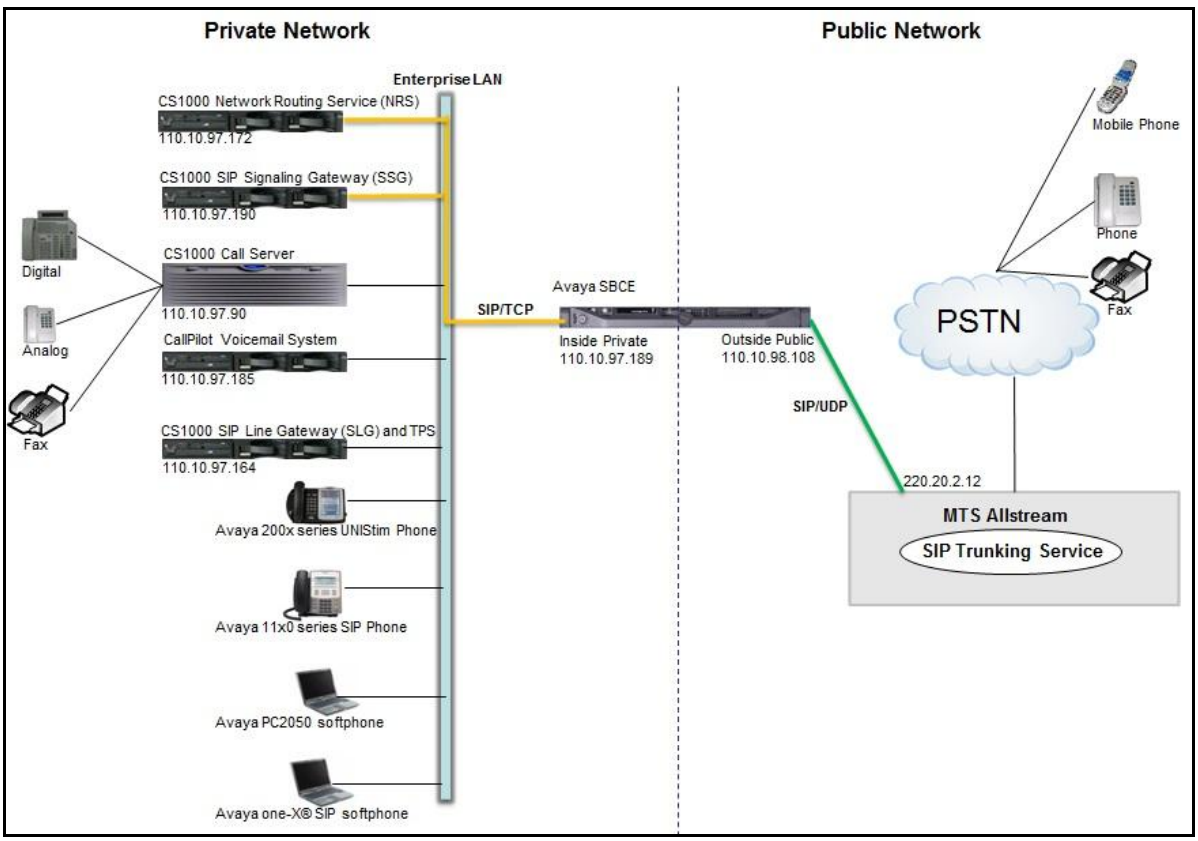


Figure 1: Avaya IP Telephony Network connecting to MTS Allstream SIP Trunking Service

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya CS1000 7.5 (CPPM)	• Call Server: 7.50 Q GA plus latest DEPLIST – Issue: 01 Release: x2107.50, 2012-07-16 17:52:47 (est) with patch MPLR32246SIP Signaling Gateway (SSG) Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20120713.ntl • Network Redirect Server (NRS) Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20120713.ntl • SIP Line Gateway (SLG) Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20120713.ntl
Avaya IP Telephone	• 2002 p2: 0604DCJ (UNIStim) • 2004 p2: 0604DCJ (UNIStim) • 1140: 0625C6O (UNIStim) • 1120: 0624C6O (UNIStim) • 2007: 0621C6M (UNIStim) • 1220: 062AC6O (UNIStim) • SIP 1120, 1140: SIP11x0e04.03.12.00 • SIP 1220,1240: SIP12x0e04.03.12.00
Avaya CallPilot	05.00.41.141
Avaya 2050PC softphone	3.4
Avaya one-X Communicator (SIP)	CS6.1.0.25-GA-33661
Avaya Digital Telephone	n/a
Avaya Analog Telephone	n/a
Avaya Session Border Controller for Enterprise	4.0.5 Q09 with patch HistInfo-mvista-load-Q09.rpm
MTS Allstream SIP Trunking Service Components	
Component	Release
Genband S3	5.2.2.12
CS2K	CVM13

Table 1: Equipment and Software Tested

5. Avaya Communication Server 1000 Configuration

This section describes the procedure for configuring the CS1000 for interoperating with the MTS Allstream.

A two-way SIP trunk is created between the SSG and the NRS to carry traffic to and from service provider respectively via the Avaya SBCE. For inbound call, the call flows from the MTS Allstream to the Avaya SBCE to the SSG via the NRS. Once the call arrives at the CS1000, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. An outbound call to PSTN is first processed by the CS1000 for outbound feature treatment such as route selection and class of service restrictions. Once the CS1000 selected the proper SIP trunk, the call is routed to the NRS toward the Avaya SBCE for egress to MTS Allstream.

For the compliance testing, the Avaya CPE environment was configured with SIP domain “mtsallstream.com” for the enterprise. The Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to MTS Allstream and vice versa. The CS1000 sent 11 digits in the destination headers (e.g. “Request-URI” and “To”) and sent 10 digit in the source headers (e.g. “From”, “Contact”, and “P-Asserted-Identity” (PAI)). MTS Allstream sent 10 digits in destination headers and sent 11 digits in source headers.

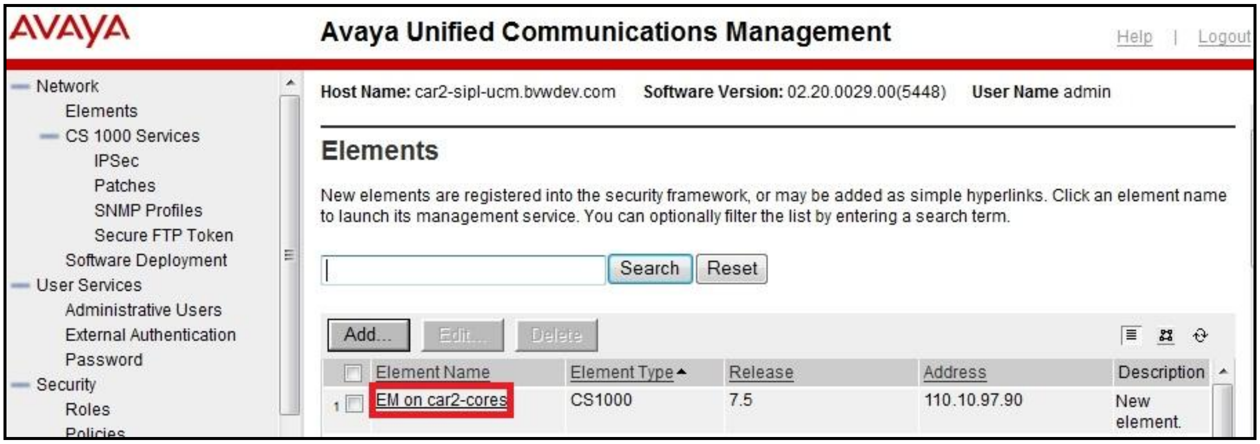
These Application Notes assume the basic configuration has already been administered and is not discussed here. For further information on the CS1000, please consult references in **Section 10**.

5.1. Log into the CS1000

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

a) Open web browser and connect to the UCM GUI https://<UCM IP address> as shown in the screenshot below then log in using an appropriate username and password.

b) The **Avaya Unified Communications Management** is shown in the following screenshot. Click on **Element Name** of the CS1000 Element as highlighted in the red box.



c) The following screenshot shows the CS1000 Element Manager **System Overview** page.

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.

```
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@110.10.97.190's password:
Last login: Fri Aug 10 13:45:14 2012 from 110.10.98.86
[admin@car2-mas ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without
authenticating
```

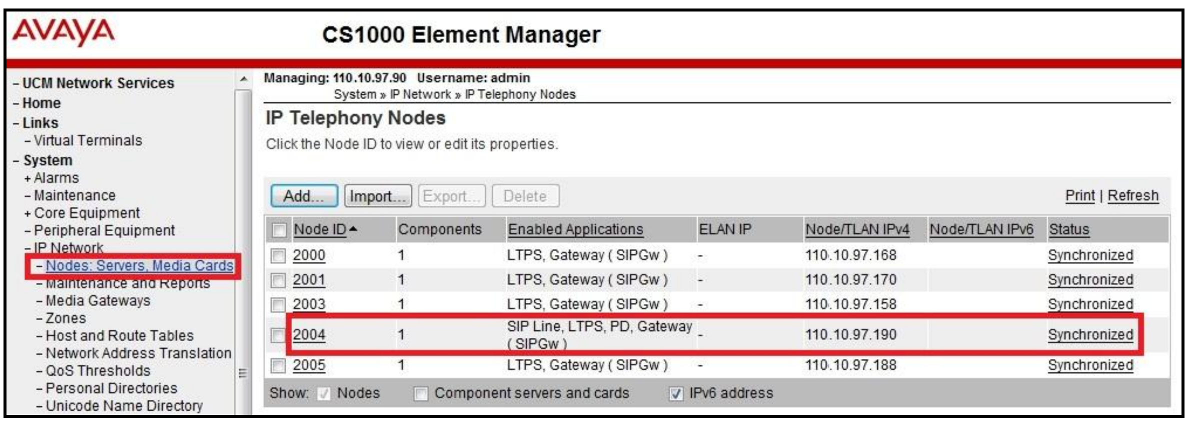
```
login
USERID? admin
PASS?
.
TTY #10 LOGGED IN ADMIN 14:19  10/8/2012

>
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.

OVL000
>
```

5.2. Administer a Node IP Telephony

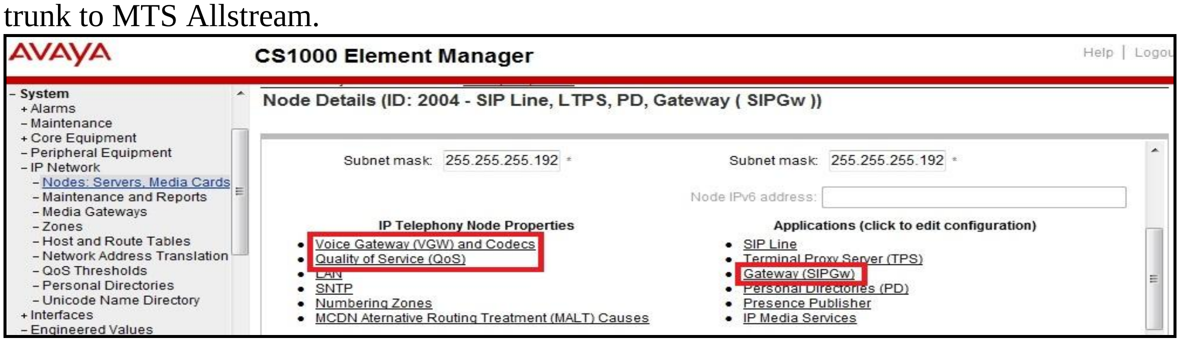
This section describes how to configure a Node IP Telephony on the CS1000.

5.2.1. Obtain Node IP address

These Application Notes assume the basic configuration has already been administered and that a Node has already been created. This section describes configuration steps for Node ID 2004.
a) To create an IP Node, select **System → IP Network → Nodes: Servers, Media Cards**. In the **IP Telephony Nodes** page as shown in the screenshot below, click the Node ID of the CS1000.

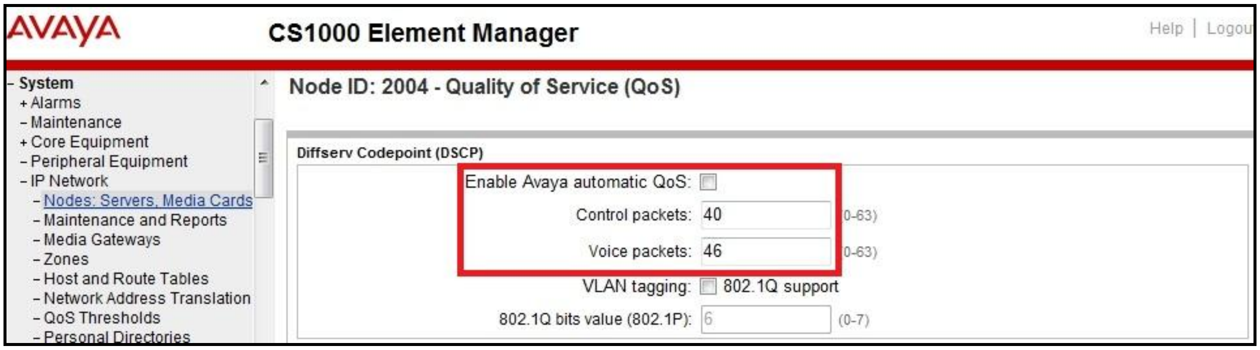


b) The **Node Details** page is shown in the screenshot below with the IP address of the Node ID 2004. The SIP Signaling Gateway uses the **Node IP Address** to connect to the NRS for the SIP trunk to MTS Allstream.



5.2.2. Administer Quality of Service (QoS)

Continued from **Section 5.2.1**. On the **Node Details** page, select **Quality of Service (QoS)** link. The default Diffserv values are shown in the screenshot below. Then click the **Save** button (not shown).



5.2.3. Synchronize the new configuration

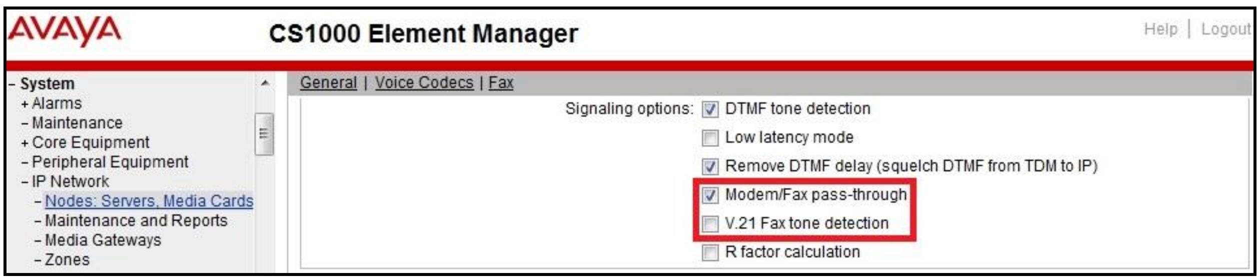
a) Continued from **Section 5.2.1**, return to the **Node Details** page (not shown) and click **Save** button.
b) The **Node Saved** screen is displayed. Click on the **Transfer Now** button (not shown).
c) The **Synchronize Configuration Files** screen is displayed (not shown). Check the **Signaling Server** checkbox and click on the **Start Sync** button (not shown).
d) When the synchronization completes, check the Signaling Server check box and click on the **Restart Applications** button (not shown).

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec, Node IP Telephony

a) To configure Voice Codec, select **IP Network → Nodes: Servers, Media Cards** 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 as described in **Section 5.2.1**.
b) On the **Node Details** page (not shown), click **Voice Gateway (VGW) and Codec** link.
c) MTS Allstream supports voice codec G.729 and G.711, payload size 20 ms, with VAD disabled. The following screenshots show appropriate voice codec profile configured on the CS1000.

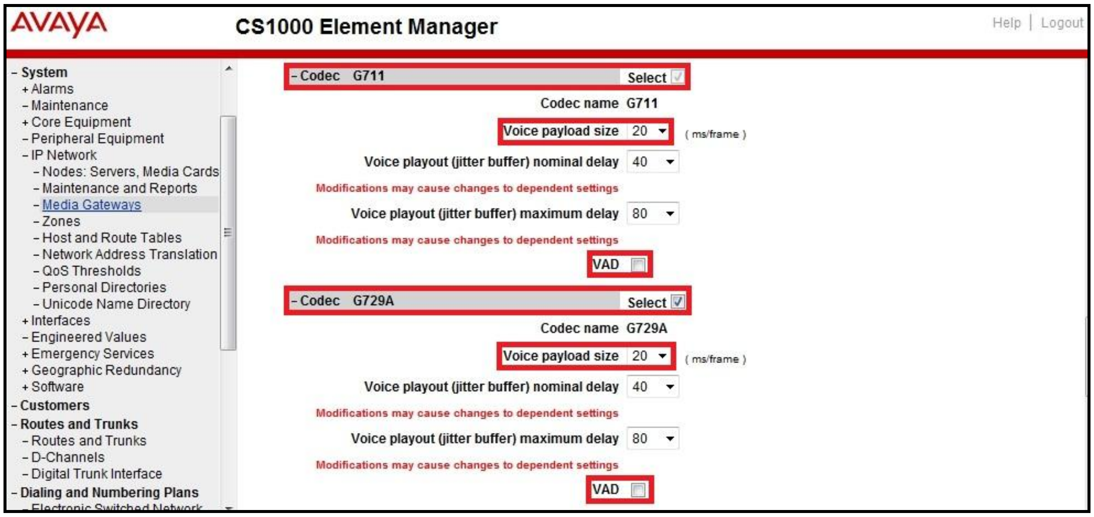
d) For Fax over IP, MTS Allstream supports G.711MU codec as default and does not support T.38. The following screenshot shows **Modem Pass Through** is selected for Node 2004; this configuration enables G.711MU codec to be used for fax calls between the CS1000 and MTS Allstream. **Note**: The **V.21 Fax tone detection** should be unchecked to disable T.38 fax on the SIP trunk.



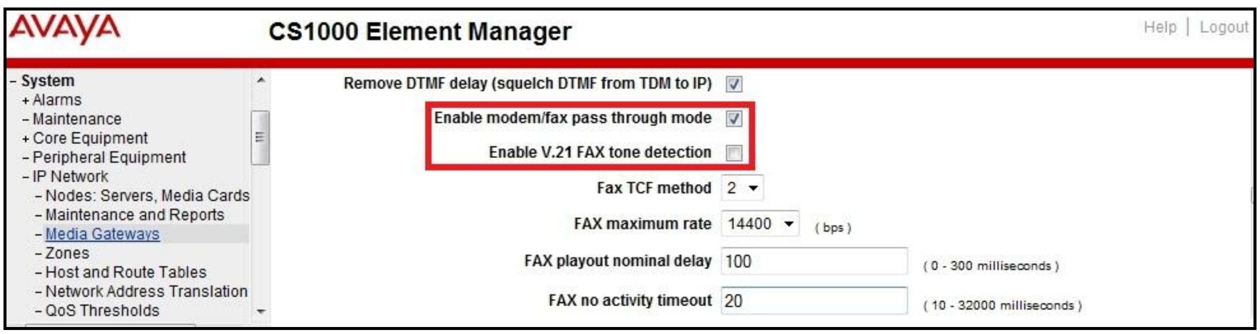
e) Click **Save** button (not shown).
f) Synchronize the new configuration (refer to **Section 5.2.3** for detail).

5.3.2. Administer Voice Codec on Media Gateways

The CS1000 uses Media Gateways to support traditional analog and digital phone for voice calls over SIP trunk. Media Gateways are also needed to support analog terminals to send fax over IP.
a) To configure Voice Codec for Media Gateways, from the left menu of the Element Manager page, select the **IP Network → Media Gateways** menu item. The Media Gateways page will appear (not shown). Click **MGC** link which is located on the right of the page (not shown).
b) MTS Allstream supports voice codec G.729 and G.711, payload size 20 ms, with VAD disabled. Click Next to show the IPMG Media Gateway Controller (MGC) Configuration screen. Scroll down to display the Codec sections. The screenshot on the next page shows appropriate codec profile configured for Media Gateways.



c) For Fax over IP, MTS Allstream supports G.711MU codec as default and does not support T.38. The following screenshot shows **Modem Pass Through** is selected for the Media Gateways, this configuration enables G.711MU codec to be used for fax calls between the CS1000 and MTS Allstream. **Note**: The **V.21 Fax tone detection** should be unchecked to disable T.38 fax on the Media Gateway. Scroll back up to VGW and IP phone codec profile.



5.4. Administer Zones and Bandwidth

This section describes the steps to create 2 zones: zone 10 for VGW and IP phone and zone 255 for SIP trunk. The CS1000 uses zone configuration for bandwidth management purposes.

MTS Allstream supports G.729 as the first choice and G.711 as the second choice. In the sample configuration as shown in the screenshots below, the zone 10 and zone 255 are configured with **Strategy Best Quality (BQ)** to allow the CS1000 select G.711MU as a first choice and G.729 as the second choice for second choice for both voice and fax calls. **Note**: In fax call scenario, the call has to be established with G.711MU otherwise it will fail because the CS1000 cannot switch the codec over to G.711MU.

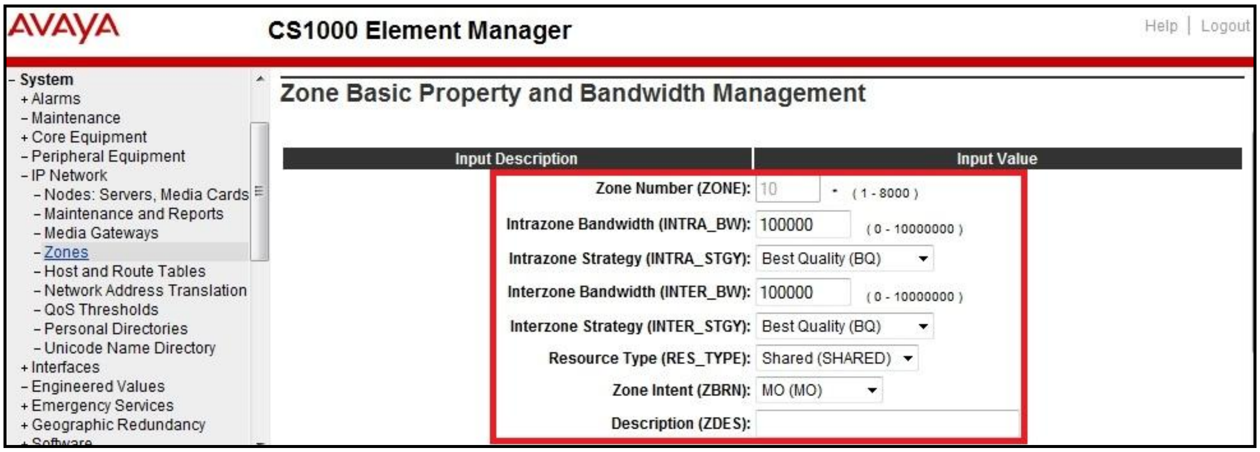
In general, a bandwidth zone is configured with parameters described as following:

- **INTRA_STGY**: bandwidth configuration for local calls
- **INTER_STGY**: bandwidth configuration for the calls over trunk
- **BQ**: G.711 is first choice and G.729 is second choice

- **BB**: G.729 is first choice and G.711 is second choice
- **MO**: the zone type which is used for IP phones and Voice Gateway (VGW)
- **VTRK**: the zone type which is used for SIP trunk

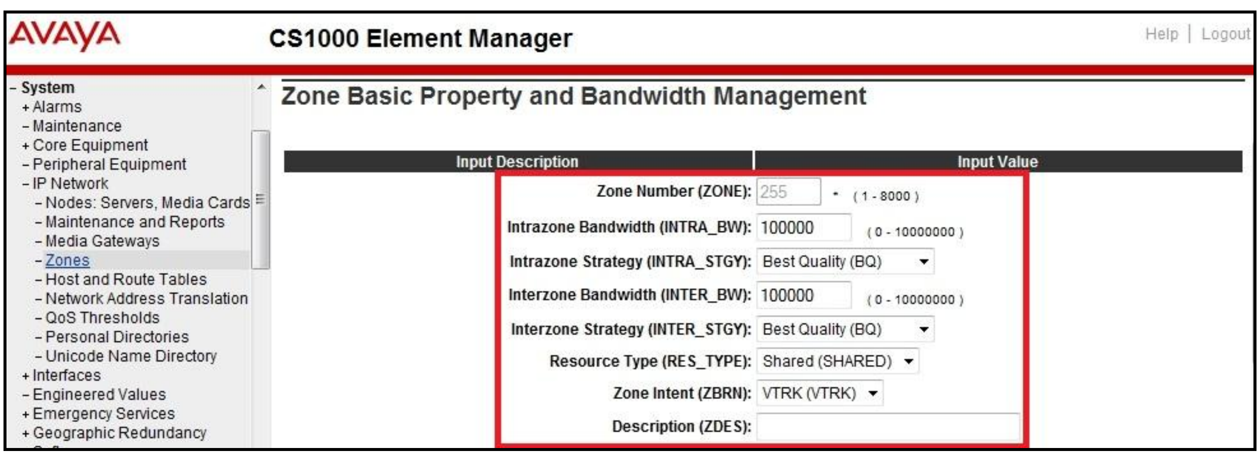
5.4.1. Create a zone for IP phones

a) To create a MO zone 10 for VGW and IP phone, select **IP Network → Zones** configuration from the left pane, then click on the **Bandwidth Zones** (not shown).
b) In **Bandwidth Zones** screen, click **Add** (not shown).
c) In the **Add Bandwidth Zone** screen, click on **Zone Basic Property and Bandwidth Management**, select the values as shown (in red box) in the screenshot below and click **Submit** button (not shown).



5.4.2. Create a zone for virtual SIP trunk

Follow **Section 5.4.1**to create a VTRK zone 255 for the virtual trunk. The difference is in the **Zone Intent (ZBRN)** field. Select **VTRK** for virtual trunk and then click on the **Submit** button (not shown) in the screenshot below.

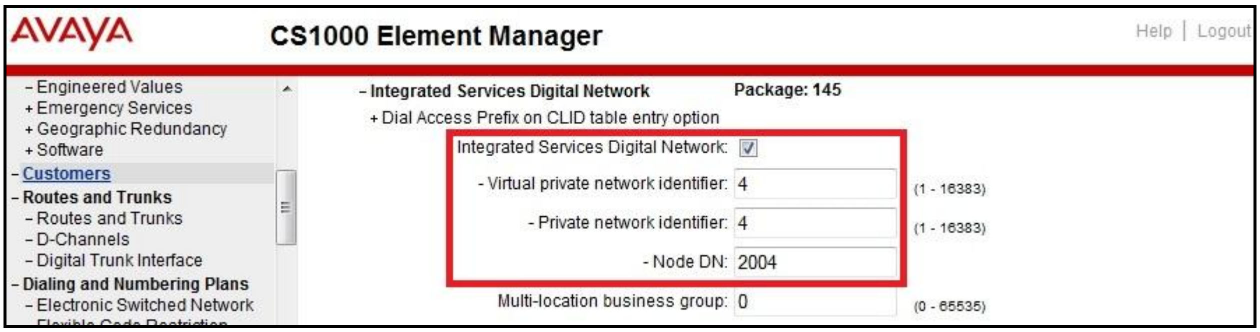


5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP IP connection between the SIP Signalling Gateway (SSG) to the Network Routing Service (NRS).

5.5.1. Integrated Services Digital Network (ISDN)

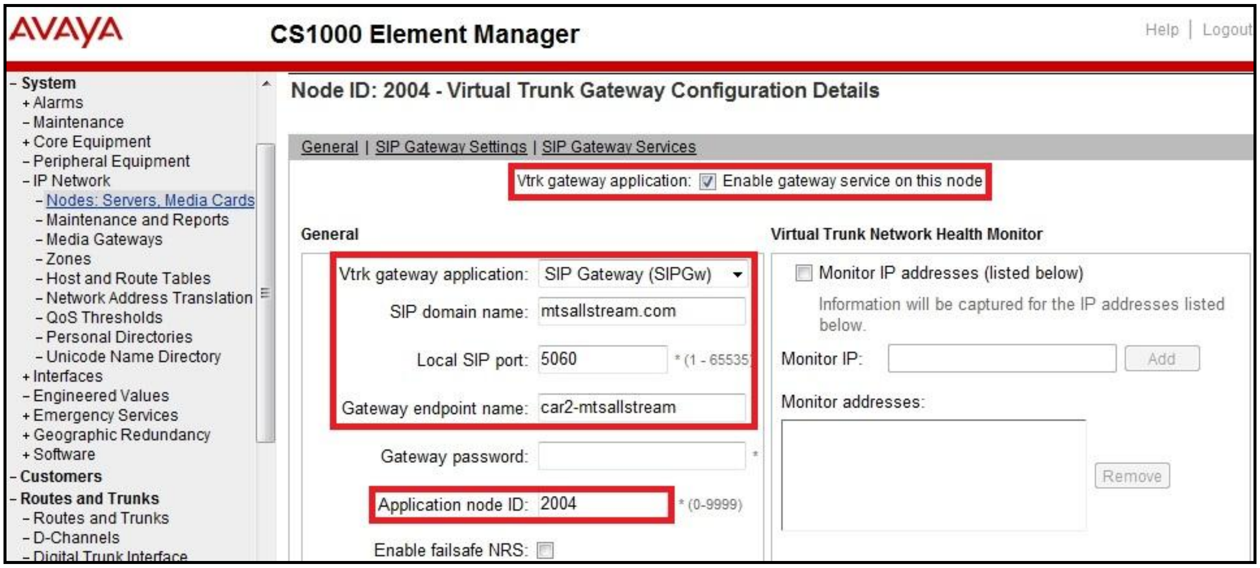
a) To configure ISDN, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case is 04. The system can support more than one customer with different network settings and options. The **Customer 04 Edit** page will appear (not shown) then select **Feature Packages** option from this page (not shown).
b) The screen is populated with a list of F**eature Packages**. Select **Integrated Services Digital Network (Package 145)** to edit its parameters with the values highlighted in red boxes as shown in screenshot below. Retain the default values for all remaining fields. Scroll down to the bottom of the screen and click **Save** button (not shown).



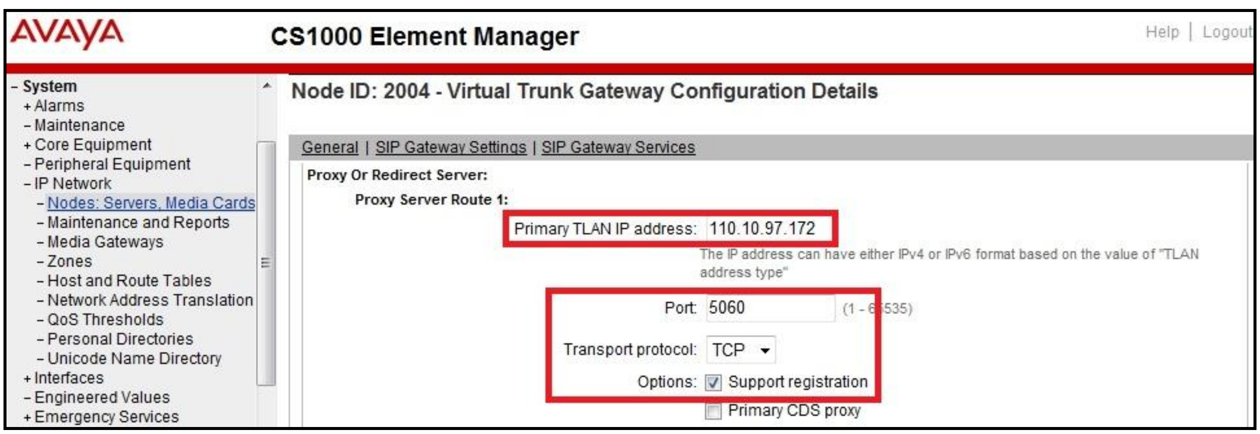
5.5.2. Administer SIP Trunk Gateway to the NRS

a) To configure SIP Trunk Gateway, select **IP Network → Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** 2004. The **Node Details** screen is displayed as shown in **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 values which are highlighted in red boxes as shown in screenshot below. These configurations are obtained when user creates a SIP Gateway Endpoint on the NRS, these are discussed in **Section 5.7**. Retain the default values for the remaining fields.

- **Vtrk gateway application**: Select SIP Gateway (SIPGw)
- **SIP domain name**: An enterprise SIP Domain name .e.g. mtsallstream.com
- **Local SIP port**: A port open to receive SIP traffic .e.g. 5060
- **Gateway endpoint name**: A descriptive name for SIP Gateway .e.g. car2-mtsallstream
- **Application node ID**: A available node ID .e.g. 2004



d) Click on **SIP Gateway Settings** tab. Under **Proxy or Redirect Server 1** setting, enter IP address of the NRS and value highlighted in the red box as shown in the screenshot below. In **Options** list, check **Support registration** to make the SSG to send REGISTER request to the NRS. In order to successfully register to the NRS, the SSG has to send correct information of its **Gateway endpoint name** and **Password** in Register request and the same information has to be defined in the NRS. However, the **Password** is not important as the SSG is set as a trusted endpoint. The detail configuration of the NRS will be discussed in **Section 5.7**. Other remaining fields are kept as default values.

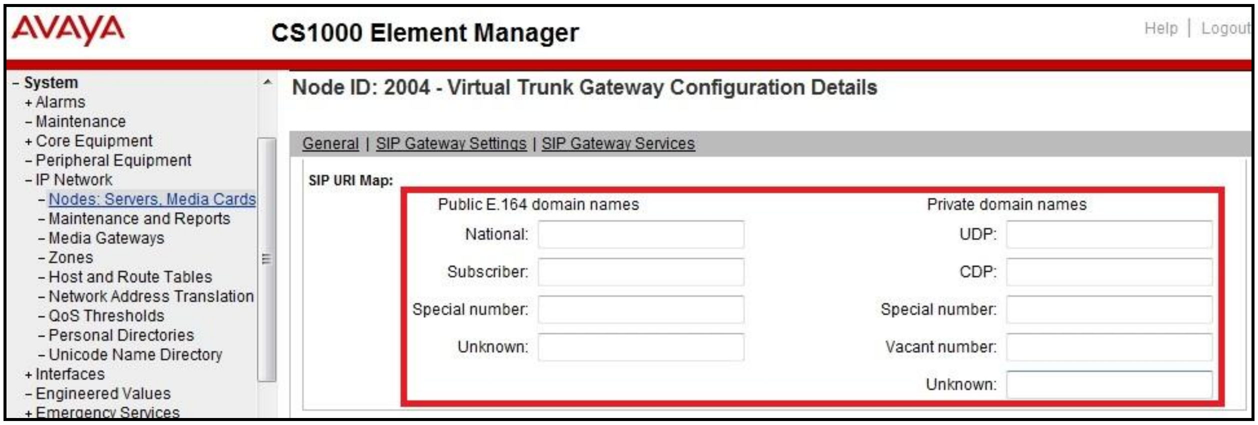


e) On the same page, scroll down to the **SIP URI Map** section as shown in the screenshot below. Under the **Public E.164 Domain Names**:

- **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

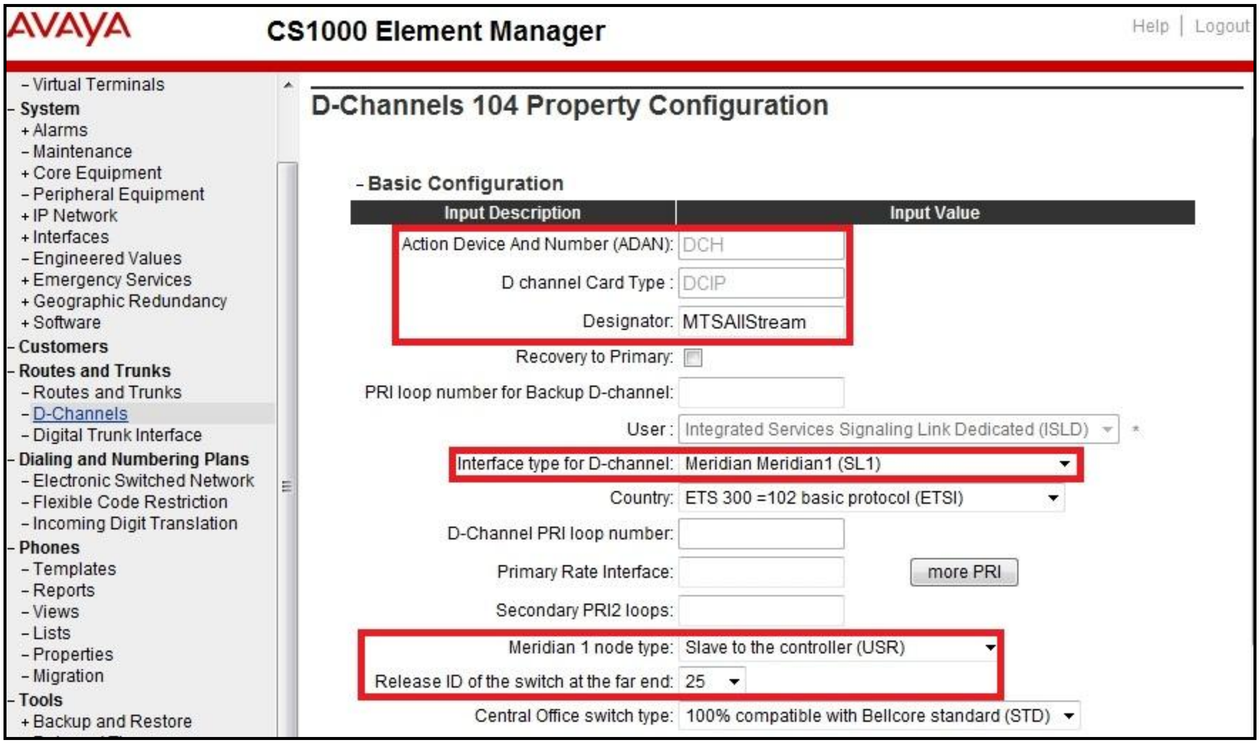


f) Then click on the **Save** button (not shown).
g) **Synchronize** the new configuration (refer to **Section 5.2.3** for detail).

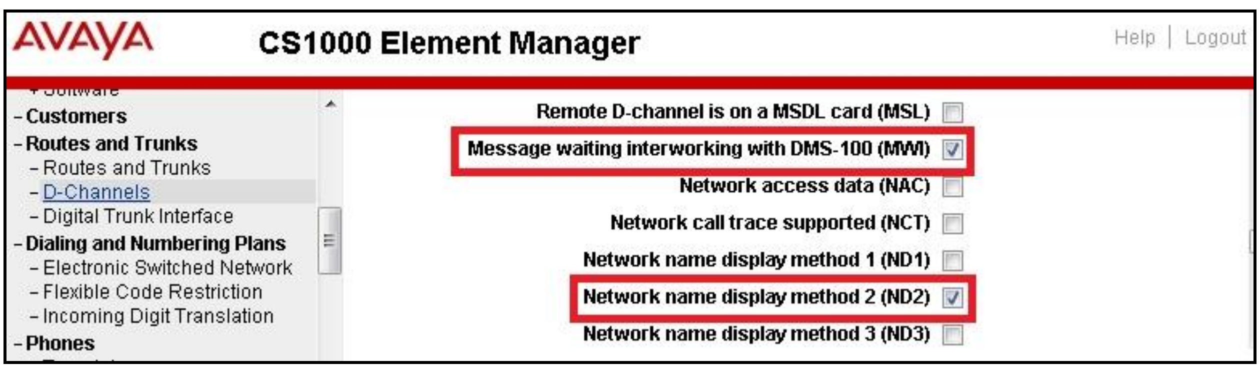
5.5.3. Administer Virtual D-Channel

a) To create a D-Channel, select **Routes and Trunks → D-Channels** from the left pane to display the **D-Channels** screen (not shown). In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list .e.g. 104 then click on **to Add** button (not shown).
b) The **D-Channels Property Configuration** screen is displayed as shown in the screenshot below. 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 e.g. MTSAllstream
- **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



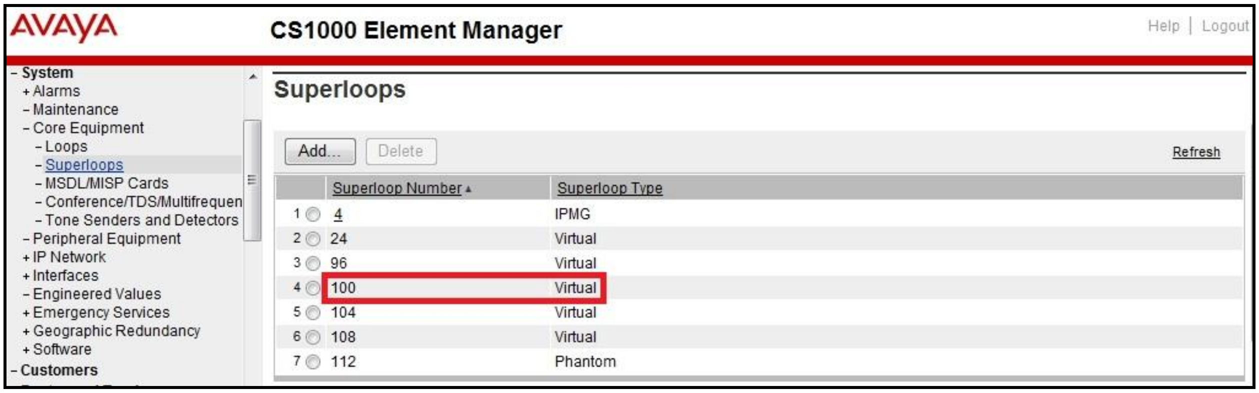
c) Click on **Basic Options** and click on **Edit** button next to **Remote Capabilities** attribute (not shown). The **Remote Capabilities Configuration** page will appear. Then check **ND2** and **MWI** checkboxes as shown in the screenshot below.



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

5.5.4. Administer Virtual Super-Loop

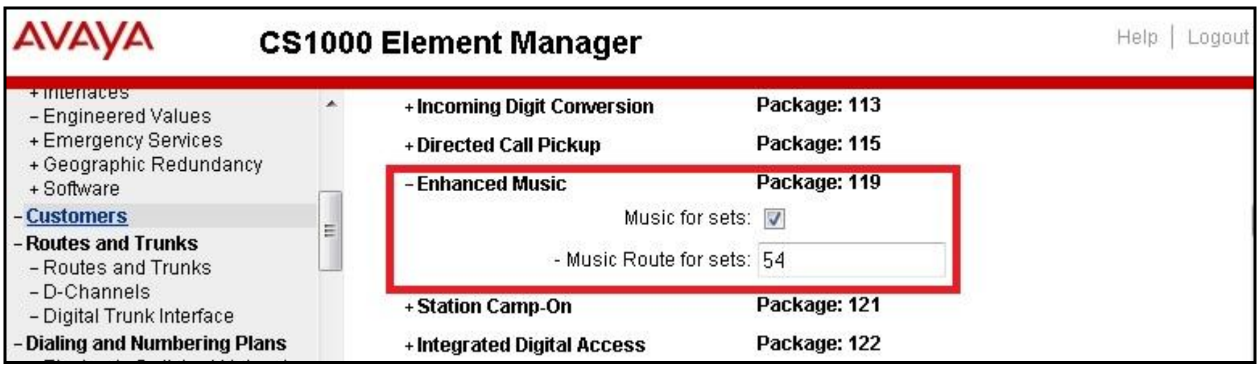
To add a virtual loop, select **System → Core Equipments → Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click "**Add**" button to create a new one as shown in the screenshot on the next page. In this example, Superloop 100 is added and used to create the SIP trunk as discussed in **Section 5.5.7**.



5.5.5. Enable Music for Customer Data Block

a) To enable music for a customer, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case is 04. The **Customer 04 Edit** page will appear (not shown). Select the **Feature Packages** option from this page (not shown).

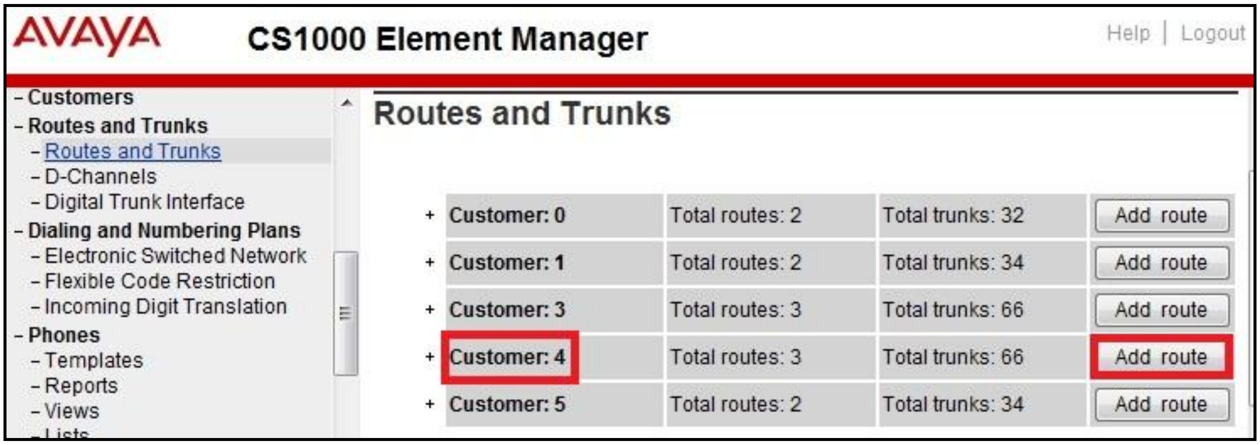
b) The screen is populated with a list of **Feature Packages**. Select **Enhanced Music (Package 119)** to edit its parameters. Check to enable music for Customer 04, define music route 54 as shown in the red box of screenshot below. The CS1000 has been pre-configured with music route 54.



c) Scroll down to the bottom of the screen and click **Save** button (not shown).

5.5.6. Administer Virtual SIP Routes

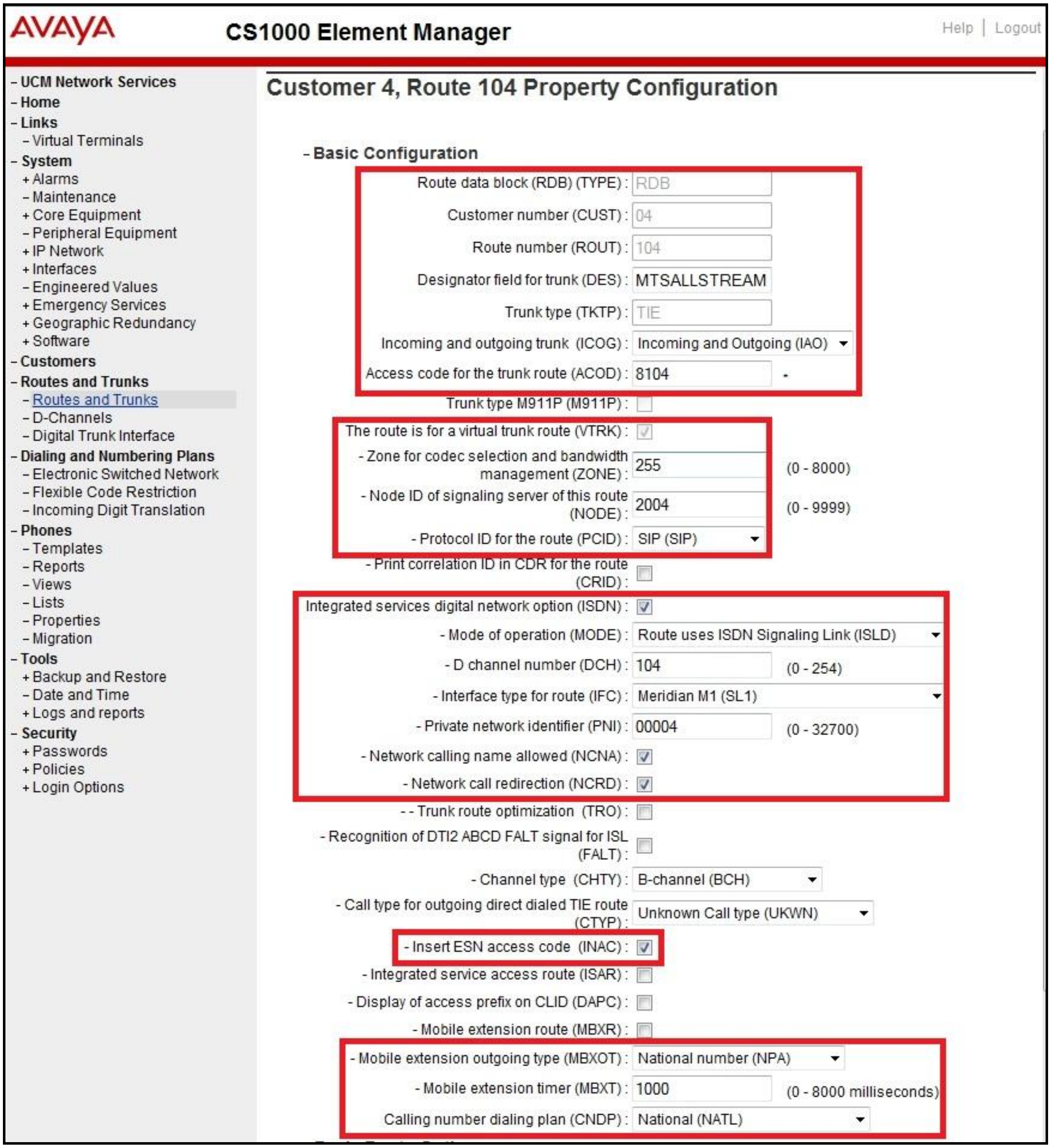
a) To create a SIP Route, select **Routes and Trunks → Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. Under **Customer 4**, click **Add route** button as shown in the screenshot below.



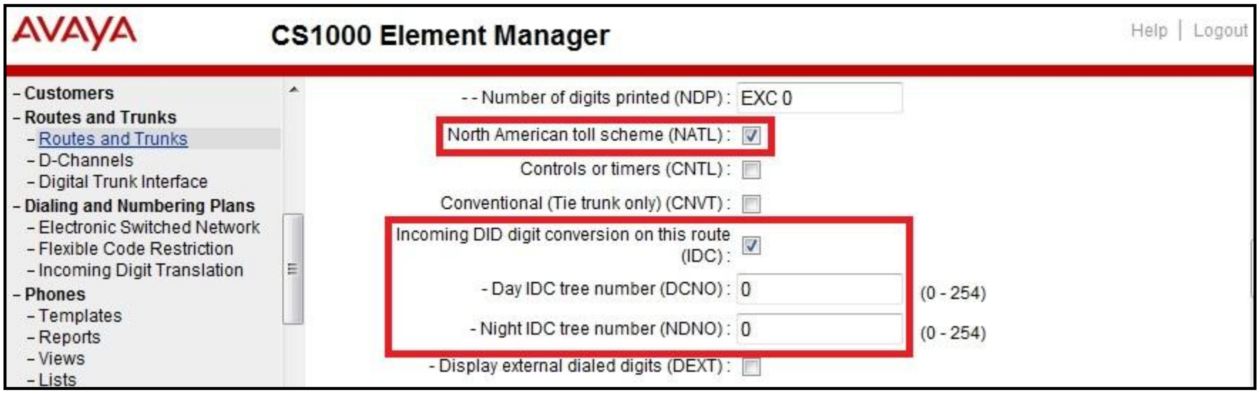
b) The **Customer 4**, **New Route Configuration** screen is displayed (not shown). Scroll down until the **Basic Configuration** section is displayed and enter the following values for the specified fields and retain the default values for the remaining fields as shown in the screenshot below.

- **Route Number (ROUT)**: Select an available route number .e.g. 104
- **Designator field for trunk (DES)**: A descriptive text .e.g. MTSAllstream
- **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 .e.g. 8104
- Check on field **The route is for a virtual trunk route (VTRK**) will enable four additional fields to appear
- For **Zone for codec selection and bandwidth management (ZONE)** field, enter 255 (created in **Section 5.4.2**)
- For **Node ID of signalling 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 **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
    - **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)**: Checked
    - **Network call redirection (NCRD)**: Checked
    - **Insert ESN access code (INAC):** Checked
    - **Mobile extension outgoing type (MBXOT)**: Select National number (NPA)

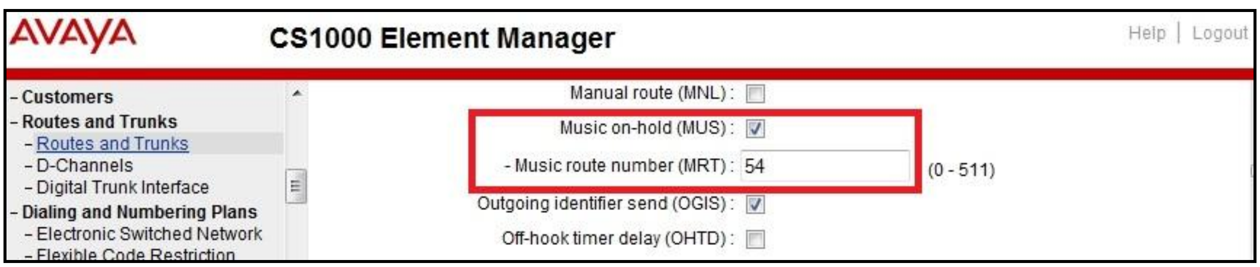
- **Mobile extension timer (MBXT)**: Define an appropriate value to meet the certain deployment at enterprise network. For this compliance testing, a value of 1000ms was used to determine if the outbound call to MobX is answered by cellular voice mail within 1000ms then the answering will be ignored. The caller will be connected to Call Pilot to leave a voice message to enterprise mail box of desk phone user. For more information, please refer to **Section 2.2**, observation **8**. **Note**: The patch MPLR32246 s required to make Cellular Voice Mail Avoidance function properly.
- **Calling number dialling plan (CNDP)**: National (NATL)



- Click on **Basic Route Options**, check **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)** and input DCNO 0 for both Day IDC Tree Number and Night IDC Tree Number as shown in screenshot below. The IDC is discussed in **Section 5.6.5**.



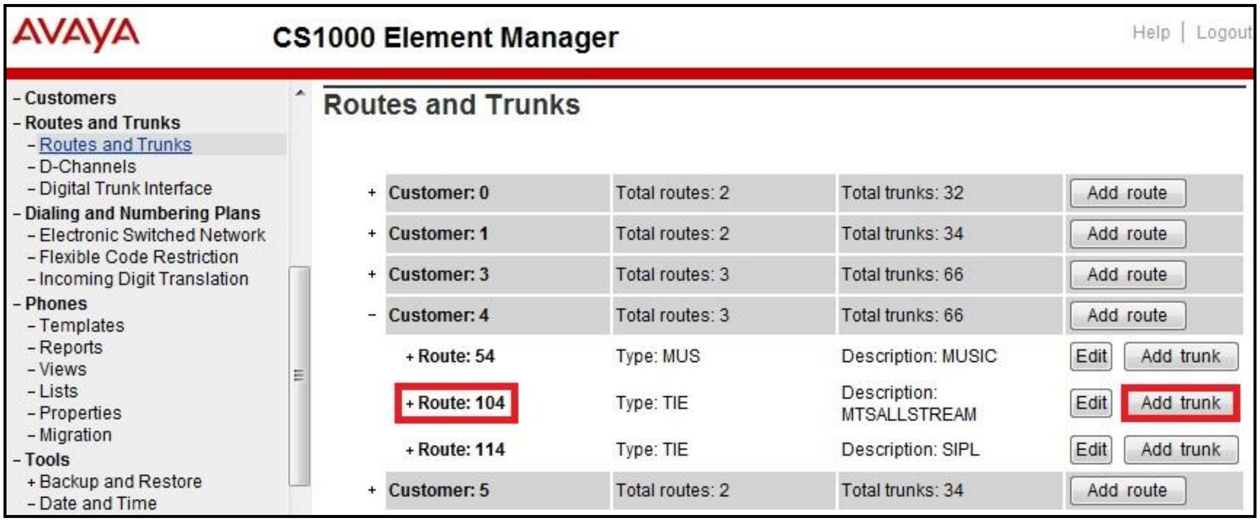
- Click on **Advance Configurations**; check **Music-on-hold** to enable music on hold on the route. Input music route 54 to the boxes as shown in the screenshot below. The CS1000 has been pre-configured with route 54 as a music route. Note: By enabling Music-on-holds, it may cause issue to blind transferred call scenario performed by SIP phone (see **Section 2.2**, observation **7**).



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

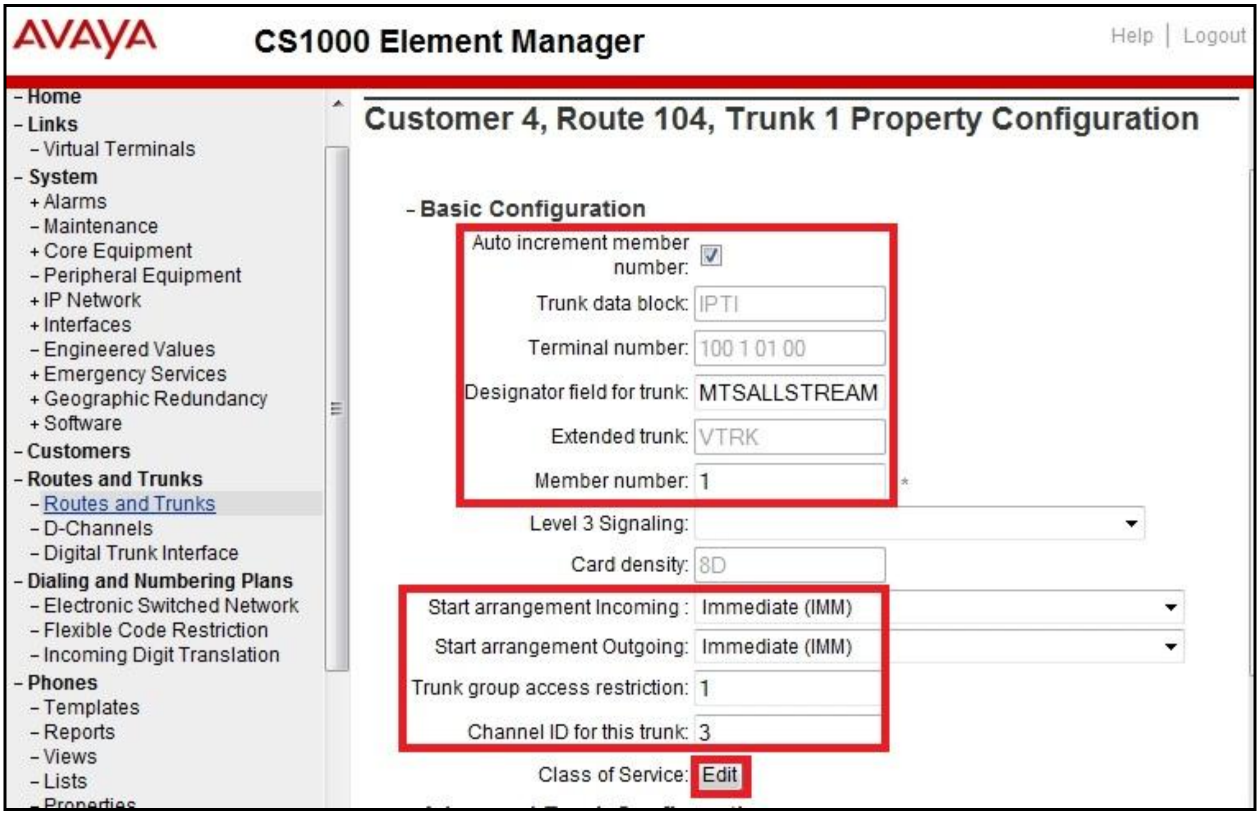
5.5.7. Administer Virtual Trunks

a) Continued from **Section 5.5.6**, the **Routes and Trunks** screen is displayed and updated with the newly added route 104 (not shown). Click on the **Add trunk** button next to the route 104 as shown in the screenshot below.

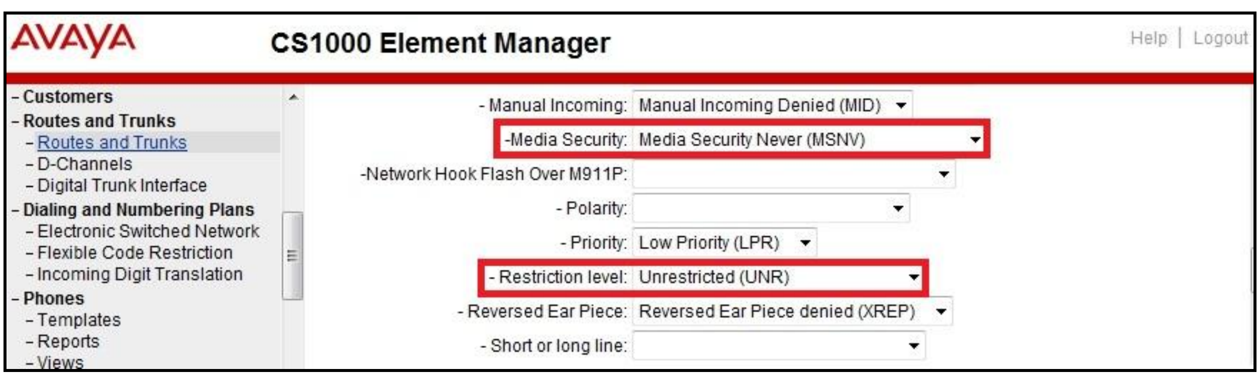


b) The **Customer 4, Route 104, Trunk 1 Property Configuration** is shown in the screenshot below. Enter number of trunks to be create in the **Multiple trunk input number (MTINPUT)** field to add multiple trunks in a single addition or repeat the addition for each individual trunk. In the certification test, 32 trunks are created (not shown). In the screenshot below, the following values are entered for specified fields and retain the default values for the remaining fields.

- **Trunk data block**: Set to IP Trunk (IPTI)
- **Terminal Number**: Available terminal number from the superloop created in **Section 5.5.4**.
- **Designator field for trunk**: A descriptive text e.g. MtsAllstream
- **Extended Trunk**: Set to Virtual trunk (VTRK)
- **Member number**: Current route number and starting member e.g. 1
- **Start arrangement Incoming**: Immediate (IMM)
- **Start arrangement Outgoing**: Immediate (IMM)
- **Trunk Group Access Restriction**: Desired trunk group access restriction level e.g. 1
- **Channel ID for this trunk**: An available channel ID e.g. 3



c) 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 **Edit** button to enter the remaining values for the specified fields as shown in the screenshot below including **Media Security** as **Media Security Never** (**MSNV)** and **Restriction level** as **Unrestricted (UNR)**. Scroll down to the bottom of the screen, click **Return Class of Service** (not shown) and then click **Save** button (not shown).



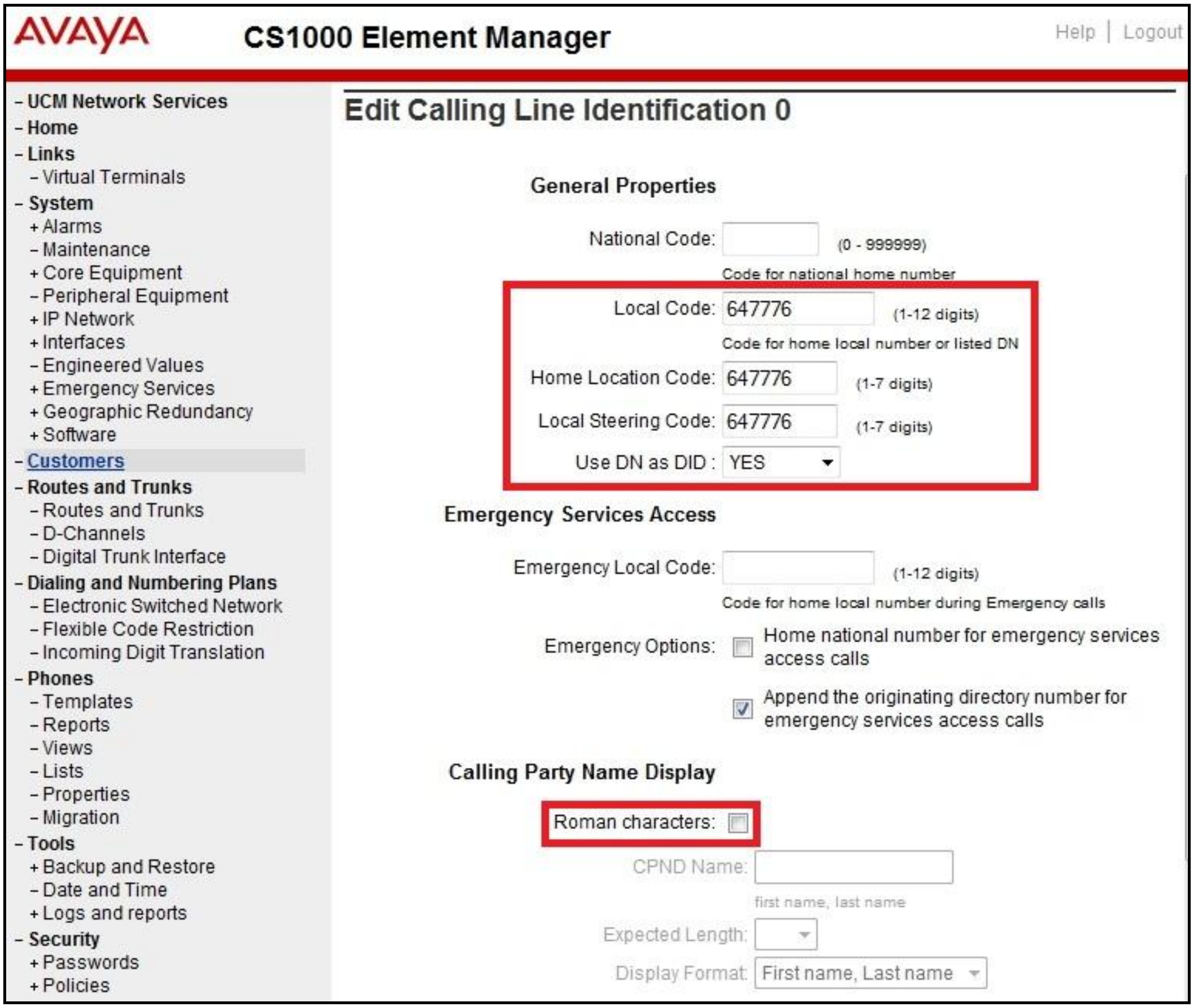
5.5.8. Administer Calling Line Identification Entries

a) To create a Calling Line Identification Entry, select **Customers** > **<u>04</u>** > **ISDN and ESN Networking**. Click on **Calling Line Identification Entries** link at the bottom of the page (not shown)

b) On the **Calling Line Identification Entries** page (not shown), click **Add**.

c) Add entry **0** as shown in the screenshot below**.**

- **National Code**: Leave as blank
- **Local Code**: Input a prefix assigned by service provider, in this case it is 6 digits – 647776. This **Local Code** is 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 a prefix assigned by service provider, in this case it is 6 digits - 647776. This **Home Location Code** is used for call display purpose for Call Type = National (NPA)
- **Local Steering Code**: Input a prefix assigned by service provider, in this case it is 6 digits - 647776. This **Local Steering Code** is be used for call display purpose for Call Type = Local Subscriber (NXX)
- **Use DN as DID**: YES
- **Calling Party Name Display**: Uncheck Roman characters



d) Click **Save** button (not shown).

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 to the Call Server CLI (please refer to **Section 5.1.2** for detail).

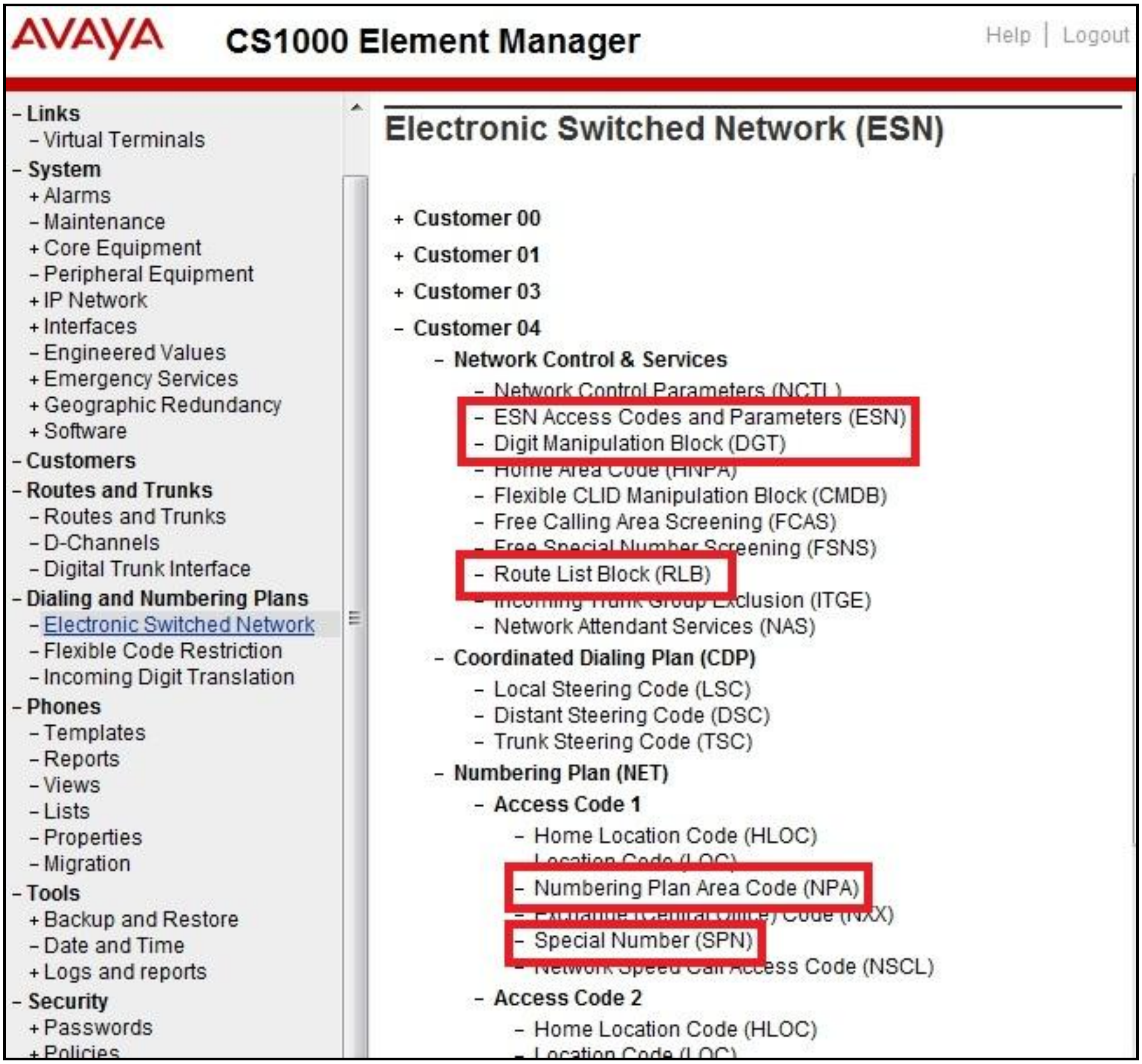
b) Allow **External Trunk To Trunk Transferring** for **Customer Data Block** by using LD 15.

```
>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
…
```

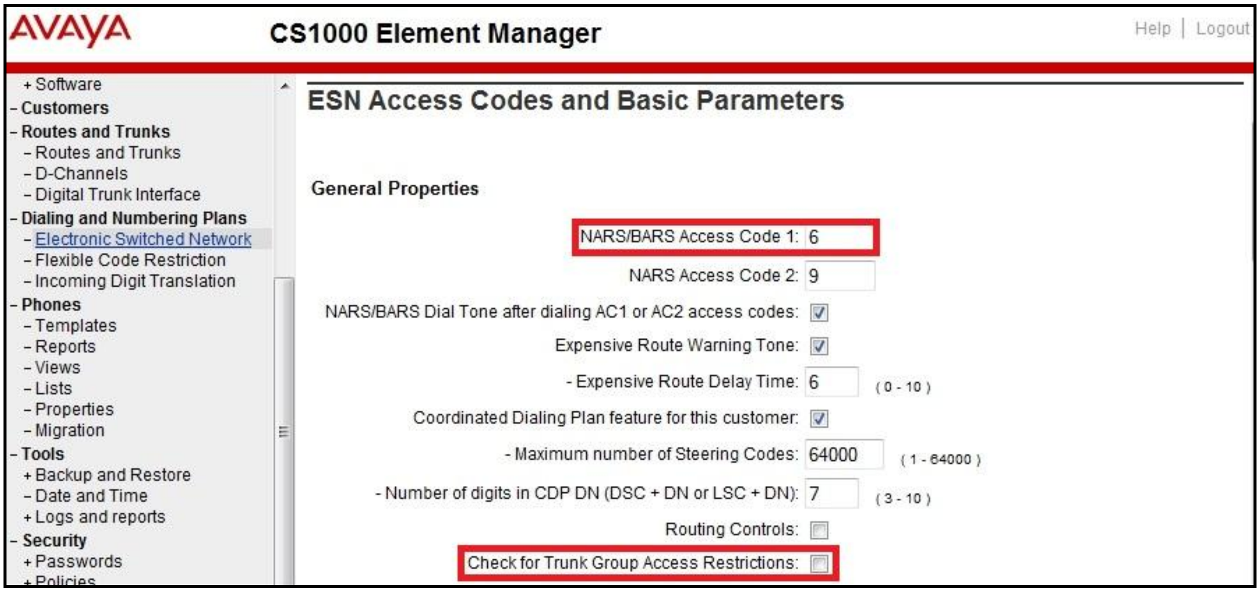
5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

a) To configure ESN parameters, 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)** under **Customer 04** as shown in the screenshot below.



b) In the **ESN Access Codes and Basic Parameters** page, define **NARS/ BARS Access Code 1** as 6 as shown in the screenshot below.



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

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

a) Login Call Server CLI (refer to **Section 5.1.2** for more detail).
b) In **LD 15**, change Customer 4 **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
…
```

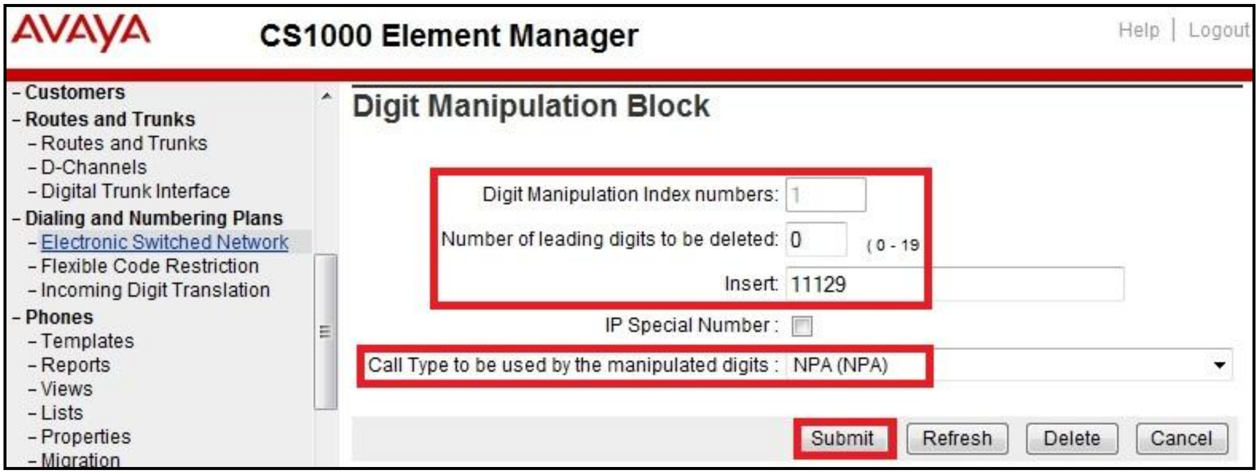
c) Verify Customer Net_Data block by using LD 21.

```
>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) To create a DMI, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown).
b) Select **Digit Manipulation Block (DGT)** (not shown).
b) In the **Choose a DMI Number** field, select an available DMI from the drop-down list and click **to Add** (not shown).
c) The screeshot below shows DMI 1 is created with following values.

- **Number of leading digits to be Deleted** (Del): 0
- **Insert**: 11129
- **Call Type to be used by the manipulated digits** (CTYP): NPA



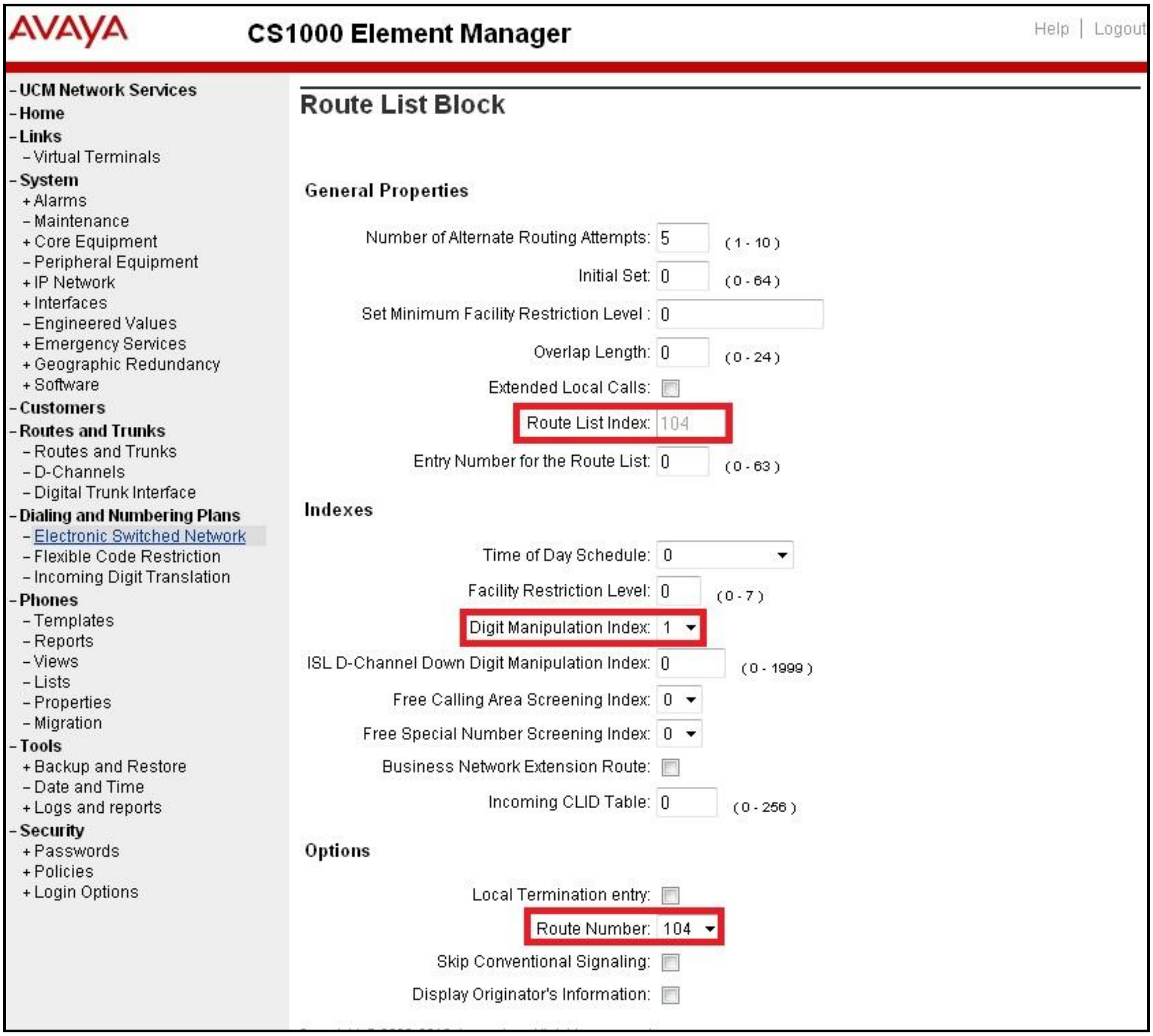
Note: This DMI will add a prefix 11129 to URI-User of Request Line for outbound call. This prefix is defined by MTS Allstream. MTS Allstream requires different prefix per SIP trunk basis. This configuration is to meet the SIP specification of MTS Allstream. The prefix will be automatically deleted by MTS Allstream and not to be sent to PSTN.

d) Click **Submit**.

5.6.4. Route List Block (RLB)

This section shows how to add a RLB associated with the DMI created in **Section 5.6.3**.
a) To create a RLB, 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 **Section 5.6.1**.
b) Select an available value .e.g. 104 in the textbox for the **route list index** and click on the **"to Add"** button (not shown).
c) Enter the following values for the specified fields, and retain the default values for the remaining fields as shown in the screenshot below.

- **Route number (ROUT)**: 104 (created in **Section 5.5.6**)
- **Digit Manipulation Index (DMI)**: 1 (created in **Section 5.6.3**)

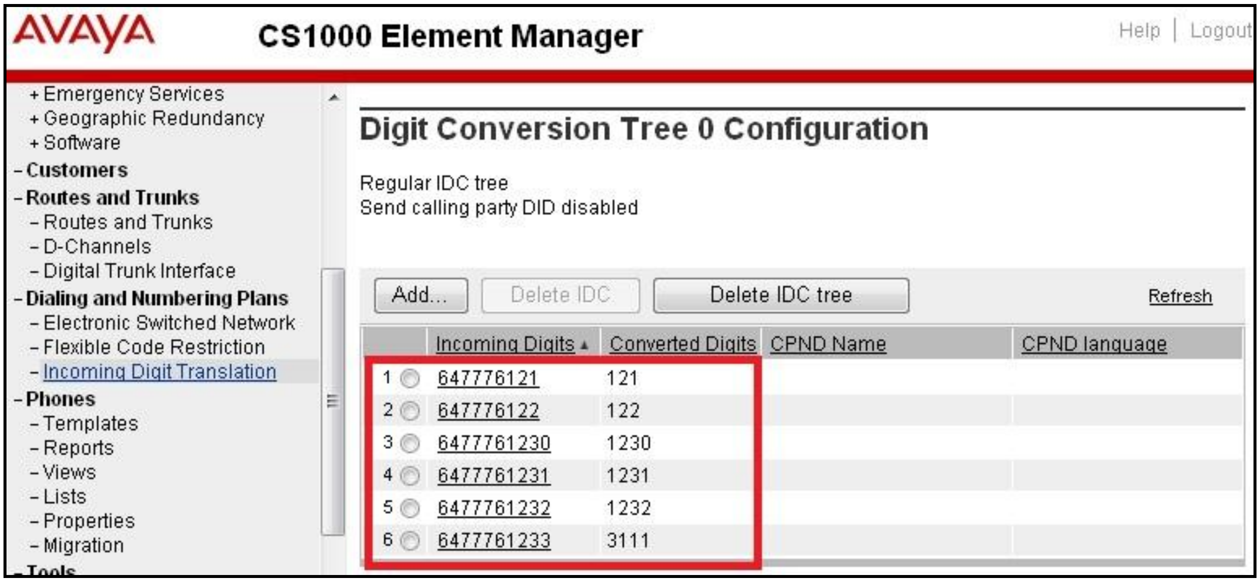


d) On the same page, scroll down to the bottom of the screen, and click on the **Submit** button (not shown).

5.6.5. Incoming Digit Translation (IDC)

This section describes the configuration for receiving calls from PSTN via the MTS Allstream.
a) To create an IDC, 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 (not shown).
b) Click on **New DCNO** (not shown) to create a digit translation entry. In this example, Digit Conversion Tree Number (**DCN0**) **0** is created. Detail configuration of the **DCNO** is shown in screenshot below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 DN. This **DCN0** has been assigned to route 104 as shown in **Section 5.5.6**.

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



5.6.6. Outbound Call - Special Number Configuration

Special numbers is 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 for directory assistant and so on.

a) To create a special number, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen (not shown). Then select **Special Number** (**SPN**) (not shown).

b) Enter SPN and then click on the "**to Add**" button (not shown). The screenshot below shows all the special numbers used for this testing.

Special Number: 0

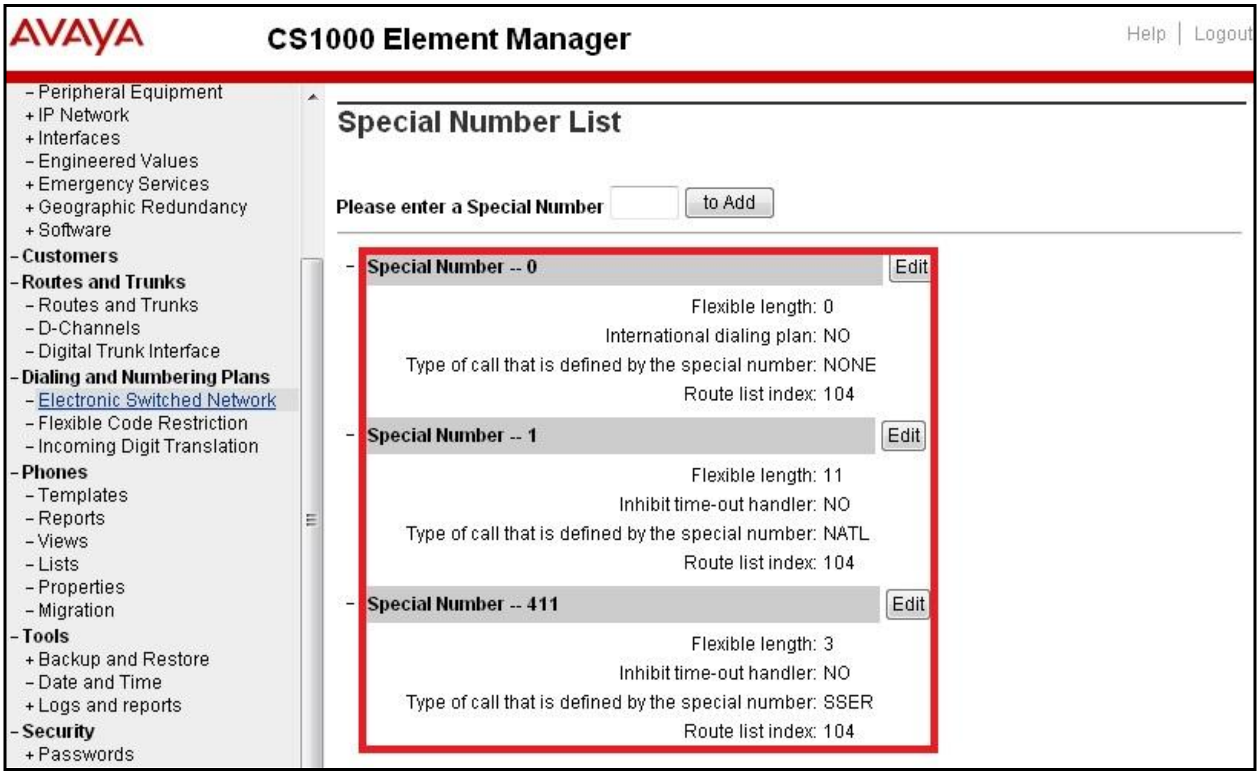
- **Flexible length**: 0 (flexible, unlimited and accept character # to end dial number)
- **Call Type**: NONE
- **Route list index**: 104, created in **Section 5.6.4**

Special Number: 1

- **Flexible length**: 11
- **Call Type**: NATL
- **Route list index**: 104, created in **Section 5.6.4**

Special Number: 411

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

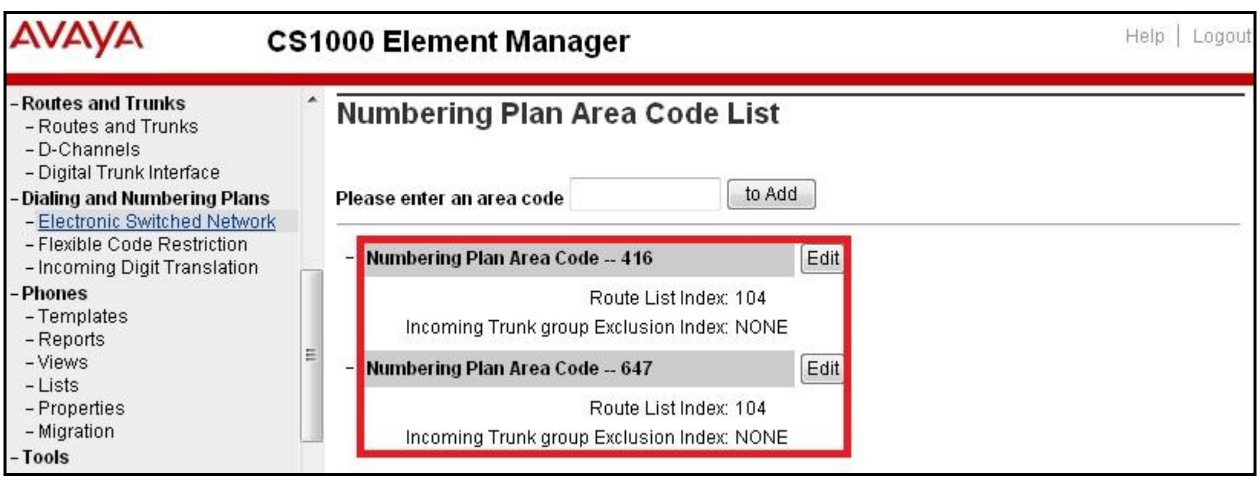


5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

a) To create a NPA number, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen (not shown). Select **Numbering Plan Area Code** (**NPA**) (not shown).

b) Enter area code desired in the textbox and click on the "**to Add"** button (not shown). The screenshot below shows NPA numbers 416 and 647 are configured for this testing. These NPA numbers are associated to the SIP trunk.



5.7. Administer the NRS

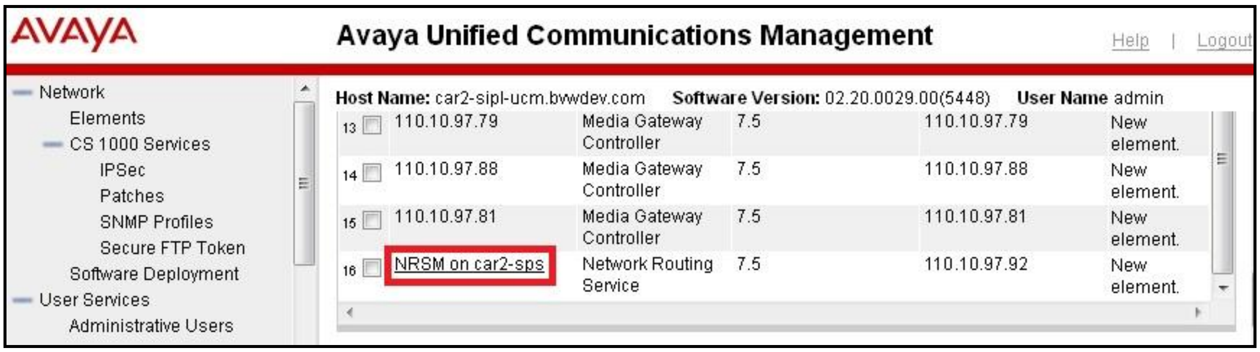
This section shows how to configure a NRS on the CS1000. It is assumed that the NRS server has been installed and managed by the UCM.

5.7.1. Log into the NRS Manager

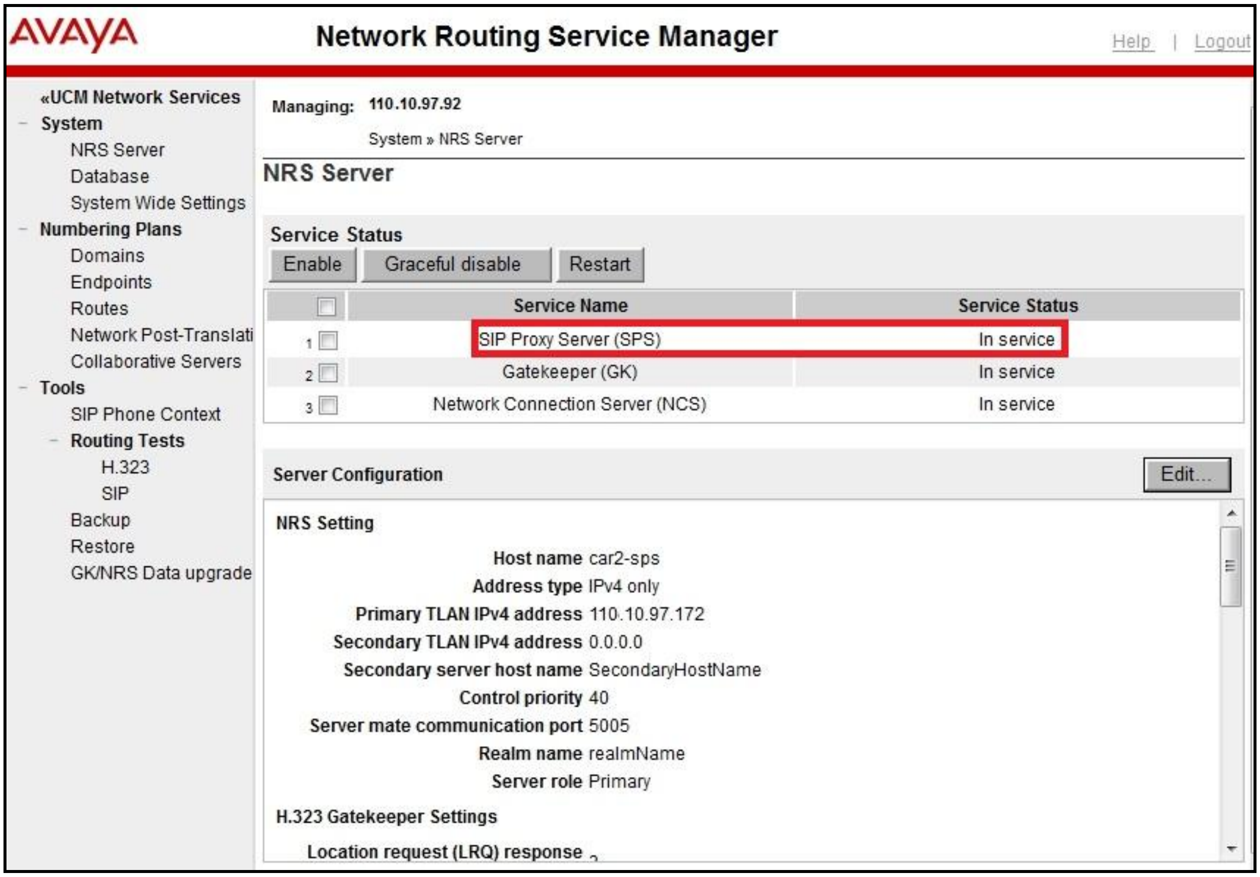
The NRS registered to UCM as a member and it can be access indirectly from UCM.

a) Login to UCM as shown in **Section 5.1.1**.

b) The **Avaya Unified Communications Management** pages displays as the following screenshot. Click on **Element Name** of the NRS as highlighted in the red box.

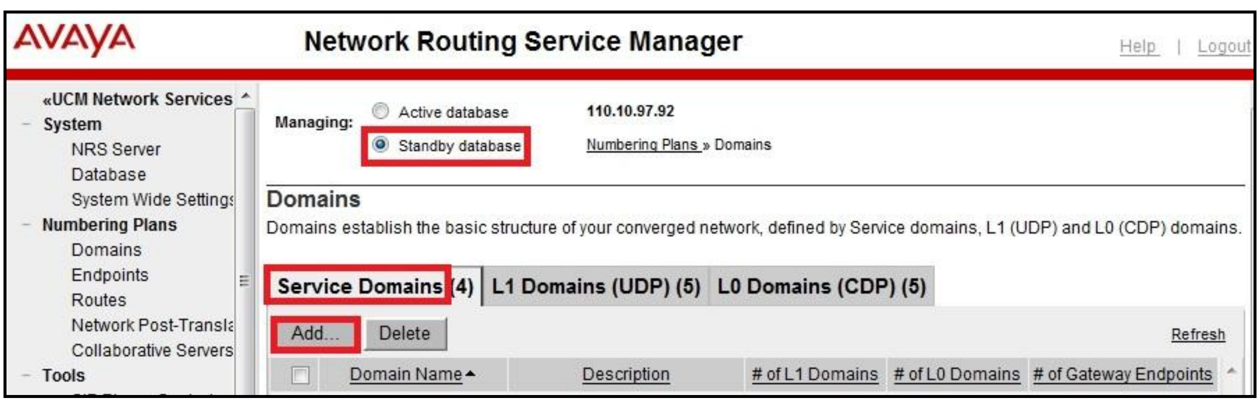


c) The **Network Routing Service Manager** page displays as the following screenshot. Verify to ensure the status of SIP Proxy Server (SPS) component is “In service”.

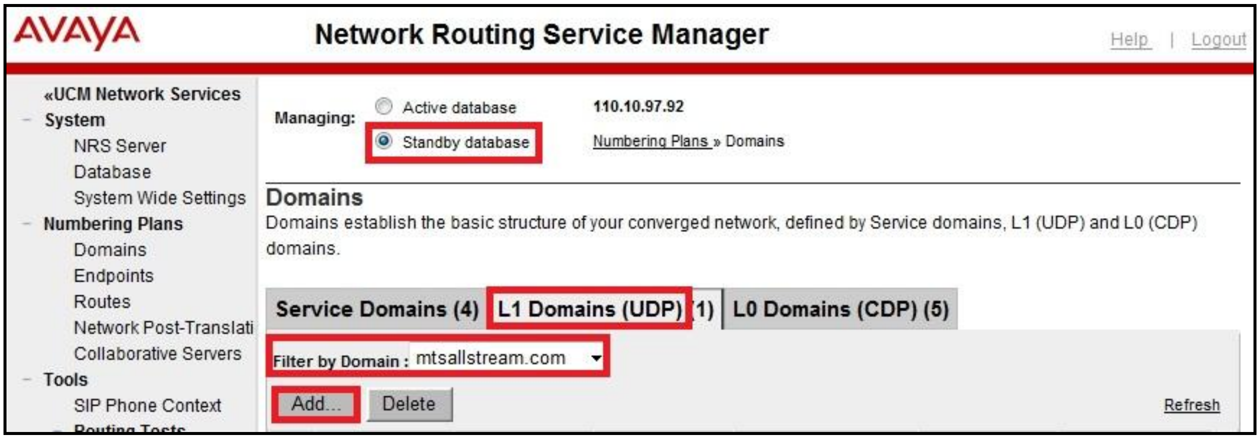


5.7.2. Create a New Domain Name on the NRS

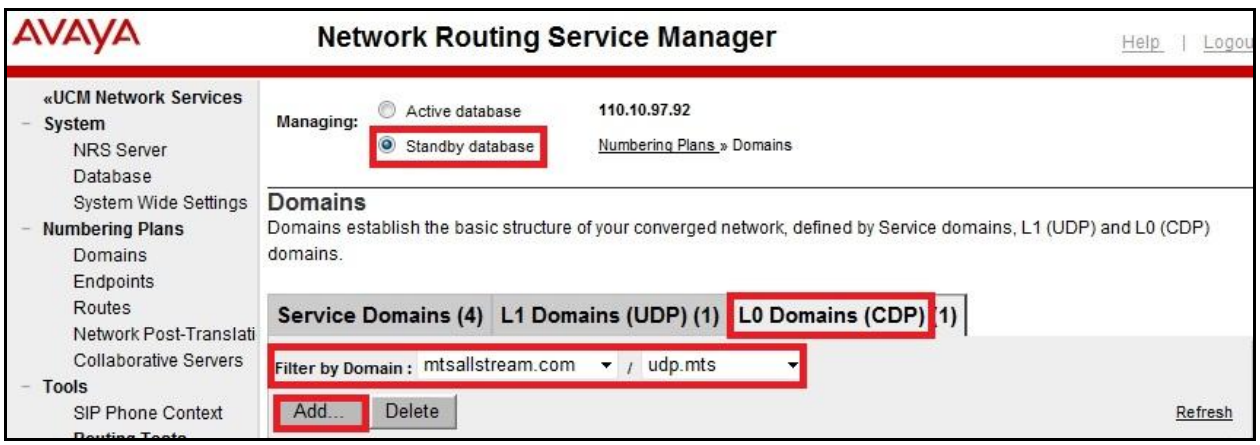
This section shows how to create a new domain name for this test configuration.
a) In **Network Routing Service Manager** page, select **Numbering Plans → Domains** then click on the radio button of the **Standby database**. Click on the **Service Domain** tab to add a new domain name then click **Add** button as shown in the screenshot below.



b) Enter the domain name to be added e.g. **mtsallstream.com** then click **Save** button (not shown).
c) Select **L1 Domains (UDP)**. Under **Filter by Domain** list, select the newly created domain **mtsallstream.com**. Click on **Add** button as shown in the screenshot below.



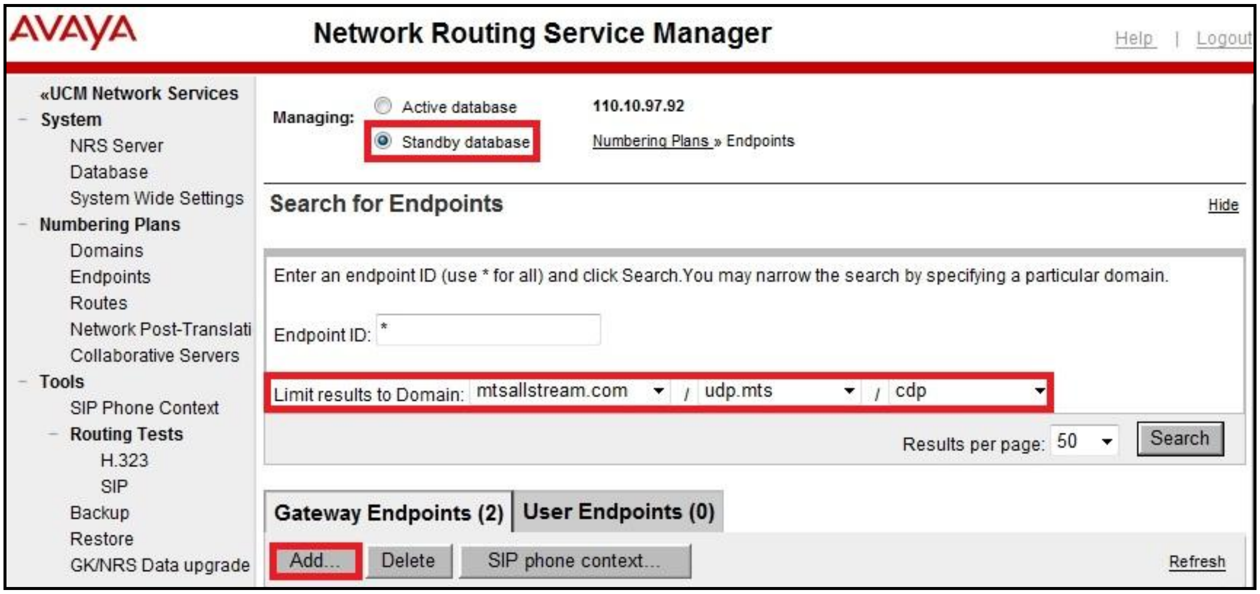
d) Enter **L1 Domains (UDP)** as **udp.mts** then click **Save** button (not shown).
e) Select the **L0 Domains (CDP)**. Under **Filter by Domain** list, select the newly created domain **mtsallstream.com**. Under **All L1 Domain** list, select the udp.mts created above. Click on **Add** button as shown in the screenshot below.



f) Enter **L0 Domain (CDP)** as **cdp** then click **Save** button (not shown).
g) From the left menu column, select **System → Database.** Then click on the **Cut Over** button (not shown) to transfer the configured data of the domain name to save in to the **Active Database.** Click on the **Commit** button (not shown).

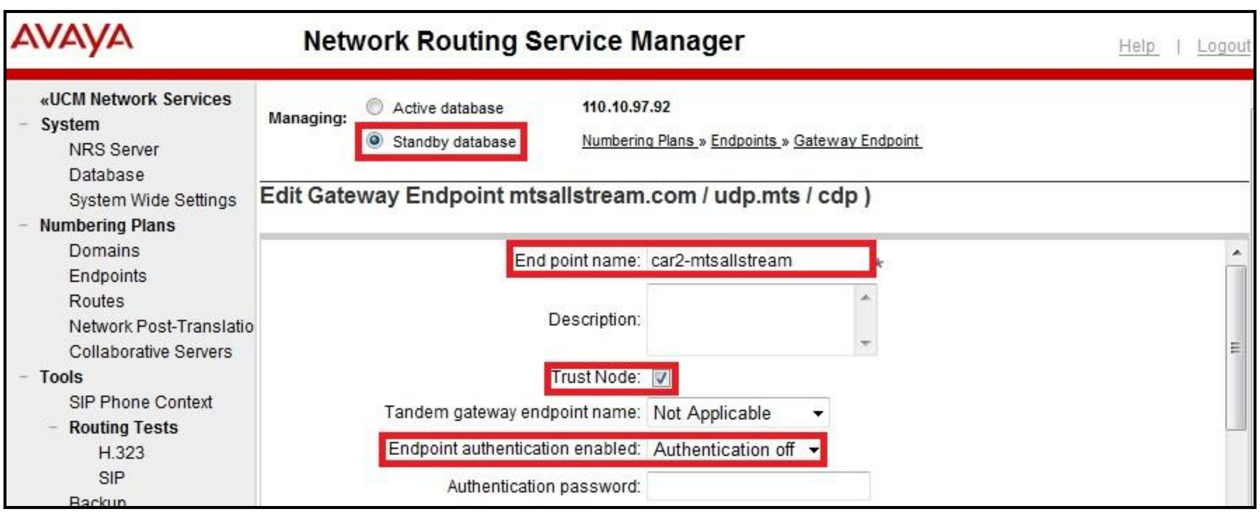
5.7.3. Create Dynamic Gateway Endpoint for the SSG

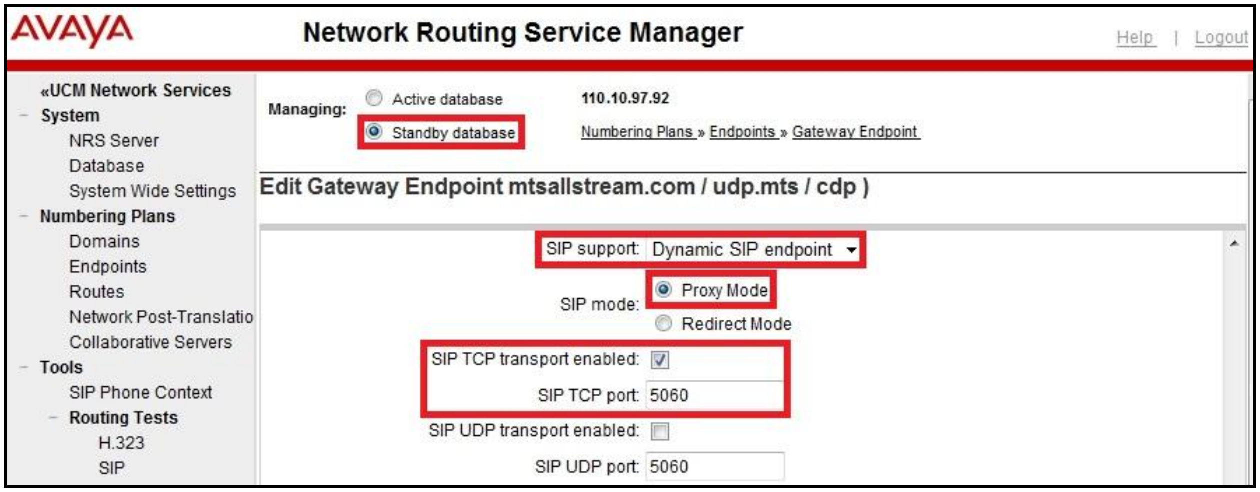
This section shows how to add a dynamic gateway endpoint for the SSG which is used to establish the SIP trunk between the NRS and the SSG.
a) In **Network Routing Service Manager** page, select **Numbering Plans → Endpoints** then click on the radio button of the **Standby database**.
b) Under **Limit results to Domain** list, select **All service domains** as **mtsallstream.com**, **All L1 domains** as **udp.mts**, **All L0 domains** as **cdp**. Then click **Add** button.



c) Enter the endpoint name for the SSG as defined in **Section 5.5.2** and the values which are highlighted in red boxes as shown in the screenshots below. The SSG is defined as a dynamic gateway endpoint. In dynamic mode, the SSG will send REGISTER request to the NRS and the SIP trunk is only established once the registration is successful.

- **End point name**: Input the name of the SSG e.g. car2-mtsallstream
- **Trust Node**: Checked
- **Endpoint authentication enabled:** Authentication off
- **SIP support:** Dynamic SIP endpoint
- **SIP mode:** Proxy Mode
- **SIP TCP transport enabled**: Checked
- **SIP TCP port:** 5060





c) Click **Save** button (not shown)
d) From the left menu column, select **System → Database.** Then click on the **Cut Over** button (not shown) to transfer the configured data of the domain name to save in to the **Active Database.** Click on the **Commit** button (not shown).

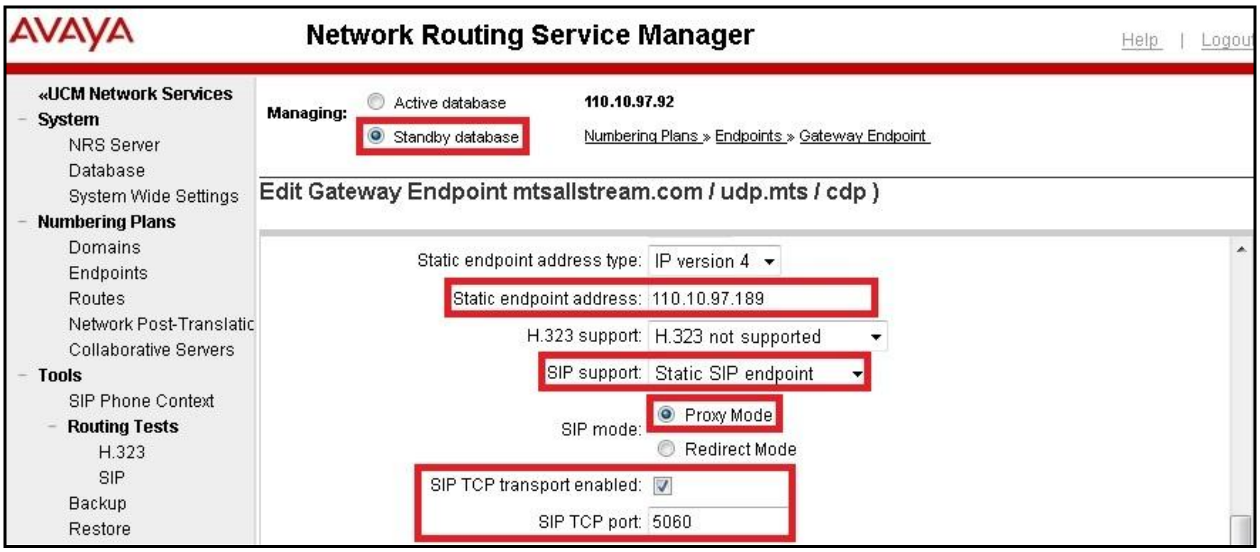
5.7.4. Create Static Gateway Endpoint for the Avaya SBCE

This section shows how to add a static gateway endpoint for the Avaya SBCE which is used to establish the SIP trunk between the NRS and the Avaya SBCE.

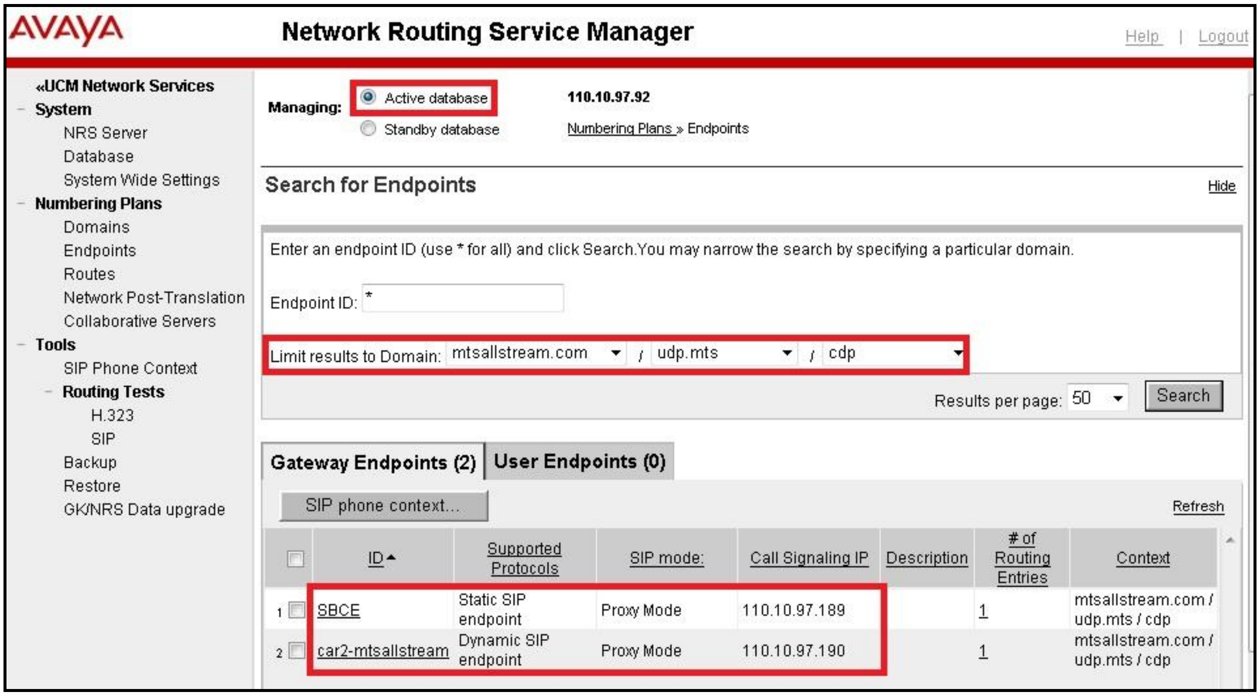
Use the procedure in **Section 5.7.3** to create a static gateway endpoint for the Avaya SBCE. In static mode, the registration is not required. Both the NRS and the Avaya SBCE are peer gateway endpoints and the predefined connection parameters will be used for the SIP trunk. The status of SIP trunk will be maintained by the NRS. As being discussed next in **Section 6.2.6**, the Avaya SBCE is configured to forward OPTIONS heartbeat originated by the NRS to MTS Allstream. If a positive response of 200OK is received, the NRS updates the new state of SIP trunk is “in service”. In other case of negative responses or no response, the NRS updates the new state of SIP trunk is “out of service” accordingly.

Following screenshots show a static gateway endpoint for the Avaya SBCE is already created with the values which are highlighted in red boxes.

- **End point name**: Define a name for the Avaya SBCE e.g. SBCE.
- **Trust Node**: Checked
- **Endpoint authentication enabled:** Authentication off
- **Static endpoint address**: Input IP address of the Avaya SBCE e.g. 110.10.97.189
- **SIP support:** Static SIP endpoint
- **SIP mode:** Proxy Mode
- **SIP TCP transport enabled**: Checked
- **SIP TCP port:** 5060



Note: After adding the configuration for the SSG and the Avaya SBCE, **Active database** of the NRS shows IP addresses of the configured gateways as in **Figure 1**. It means the registration has been successful for dynamic endpoint and all gateways are “in service”.

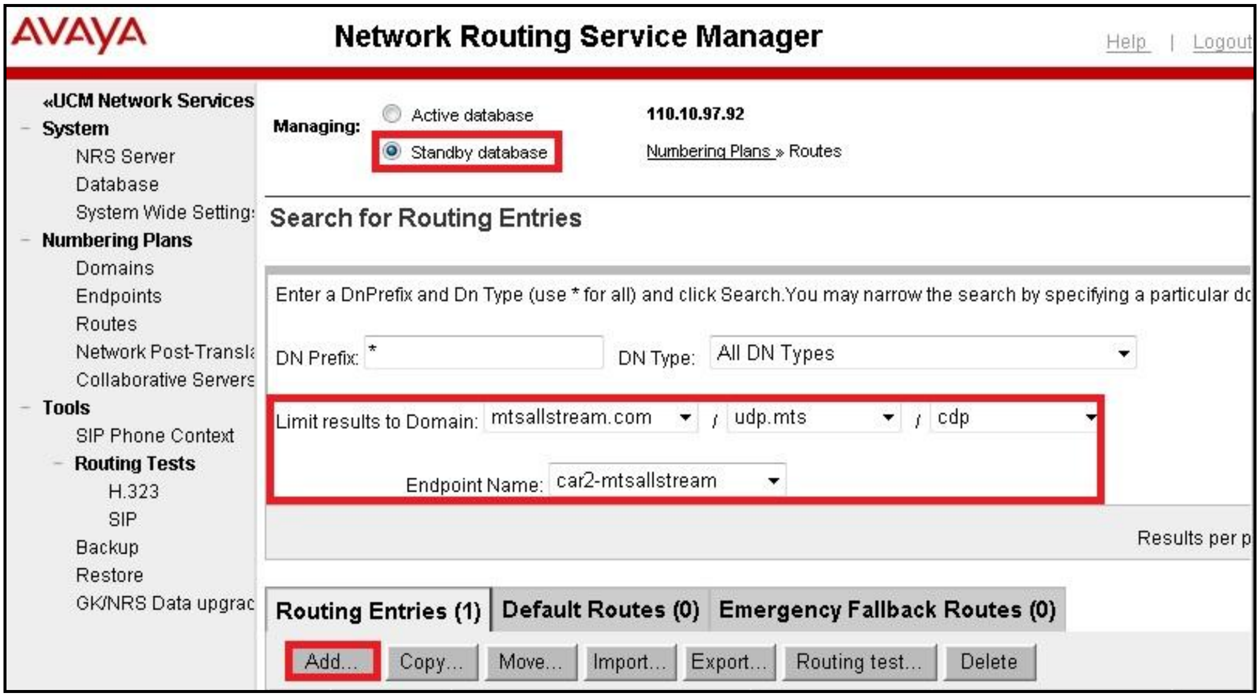


5.7.5. Creating Inbound Route for the SSG

In this section, it describes how to create a routing entry on the NRS for inbound call from PSTN via the Avaya SBCE to the SSG. In the test configuration, routing entry 647776 is added to match DID range of 64777612XX assigned by MTS Allstream for inbound call.

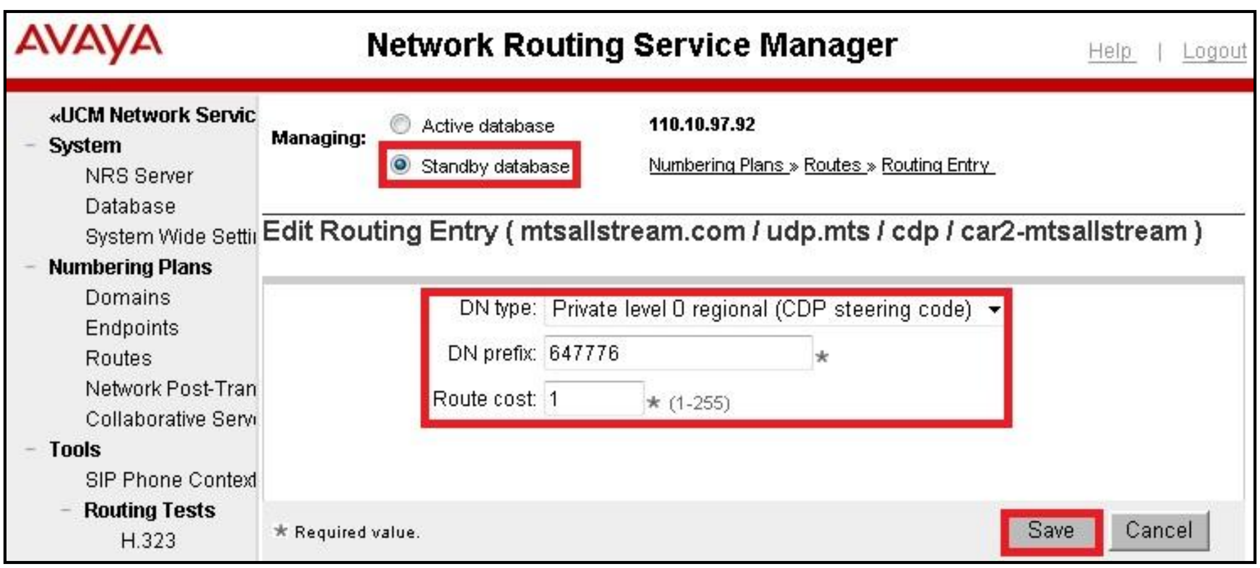
a) To add a route, in **Network Routing Service Manager** page select **Numbering Plans → Routes** then click on the radio button of the **Standby database**.

b) On the **Routing Entries** page, under **Limit results to Domain** list select **All service domains** as **mtsallstream.com**, **All L1 domains** as **udp.mts**, **All L0 domains** as **cdp**, **Endpoint Name** as **car2-mtsallstream**. Then click **Add** button.



b) **Add Routing Entry** page appears as shown the screenshot below. Fill in the textboxes with:

- **DN Type**: Private level 0 regional (CDP steering code)
- **DN Prefix**: 647776
- **Route cost**: 1



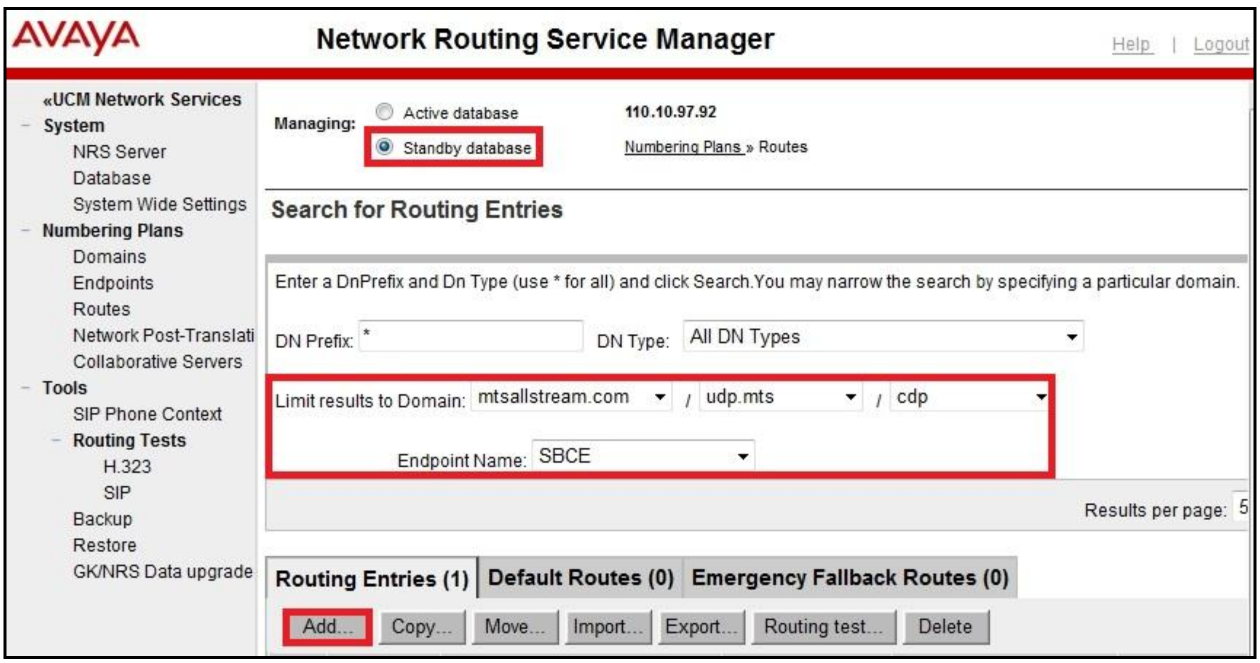
Note: **DN Type** has to be selected as CDP to make the NRS to route the call without phone-context. The NRS natively bases on predefined phone-context to retrieve associated call type by comparing with its internal routing entries. In the compliance testing, the CS1000 was configured not to send phone-context on the SIP trunk because it is not supported by MTS Allstream.

c) Click **Save** button.
d) From the left menu column, select **System** -> **Database.** Then click on the **Cut Over** button to transfer the configured data to save to the **Active Database.** Click on the **Commit** button (not shown).

5.7.6. Creating Outbound Route for the Avaya SBCE

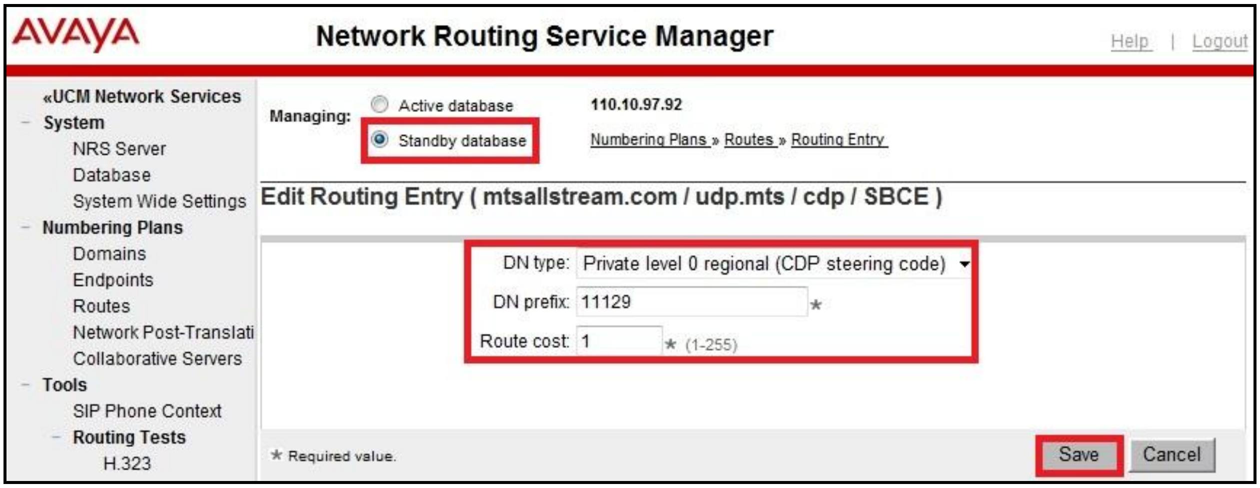
In this section, it describes how to create a routing entry on the NRS for outbound call from the SSG to PSTN via the Avaya SBCE. In the test configuration, routing entry 11129 is added to match outbound call prefix sent by the CS1000. The prefix is required by MTS Allstream to access to all different dialing plan at service provider side. For more information, refer to **Section 5.6.3**.

Use the procedure in **Section 5.7.5** to create an outbound route for the Avaya SBCE.
a) To add a route, in **Network Routing Service Manager** page select **Numbering Plans → Routes** then click on the radio button of the **Standby database**.
b) On the **Routing Entries** page, under **Limit results to Domain** list select **All service domains** as **mtsallstream.com**, **All L1 domains** as **udp.mts**, **All L0 domains** as **cdp**, **Endpoint Name** as **SBCE**. Then click **Add** button.



b) **Add Routing Entry** page appears as shown the screenshot below. Fill in the textboxes with:

- **DN Type**: Private level 0 regional (CDP steering code)
- **DN Prefix**: 11129
- **Route cost**: 1



Note: **DN Type** has to be selected as CDP to make the NRS routes the call without phone-context. The NRS natively bases on predefined phone-context to retrieve associated call type by comparing with its internal routing entries. In the compliance testing, the CS1000 was configured not to send phone-context on the SIP trunk because it is not supported by MTS Allstream.

c) Click **Save** button.
d) From the left menu column, select **System → Database.** Then click on the **Cut Over** button to transfer the configured data to save to the **Active Database.** Click on the **Commit** button (not shown).

6. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Reference** [**9**] and [**10**].

The compliance testing comprises of configuration for two major components; trunk server for service provider and call server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration is performed using the Avaya SBCE web user interface as described in the following sections.

Trunk server configuration elements for service provider MTS Allstream:

- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Signaling Manipulation
  - Server Configuration
- Domain Policies:
  - Application Rules
  - Media Rules
  - Signaling Rules
  - Endpoint Policy Group
  - Session Policy
- Device Specific Settings:
  - Network Management
  - Media Interface
  - Signaling Interface
  - End Point Flows → Server Flows
  - Session Flows

Call server configuration elements at the enterprise for the NRS:

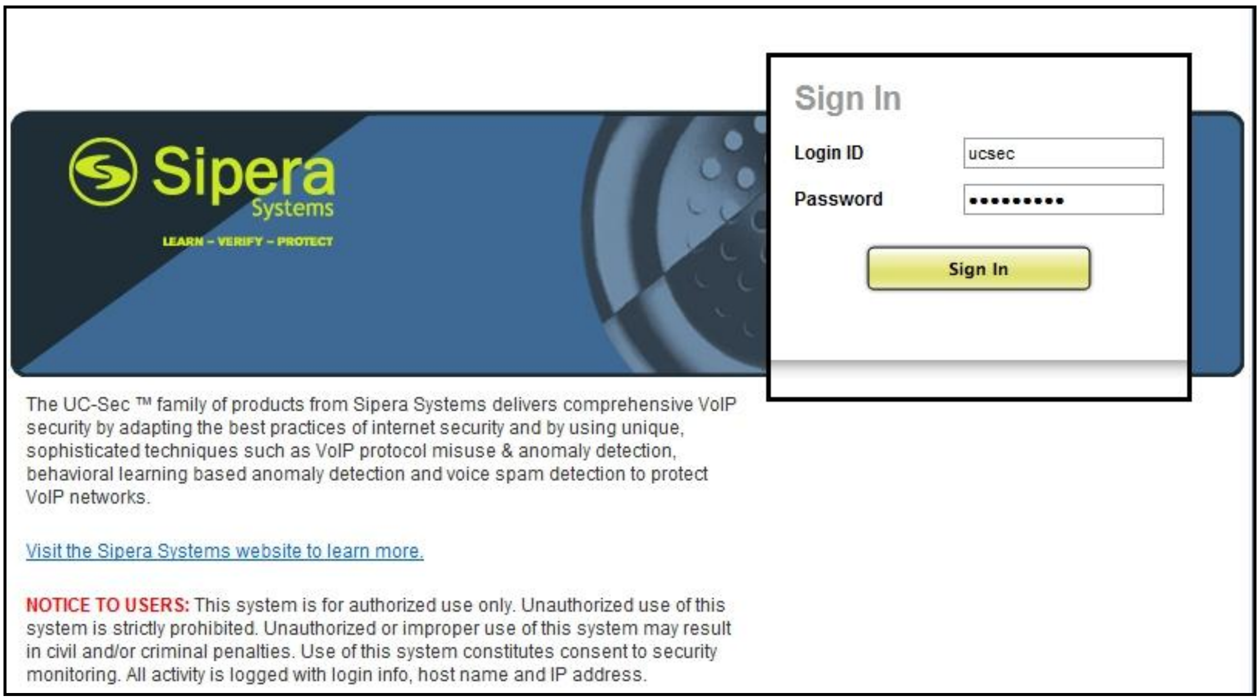
- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Server Configuration
- Domain Policies:
  - Application Rules
  - Media Rules
  - Signaling Rules
  - Endpoint Policy Group

    - Session Policy
- Device Specific Settings:
    - Network Management
    - Media Interface
    - Signaling Interface
    - End Point Flows → Server Flows
    - Session Flows

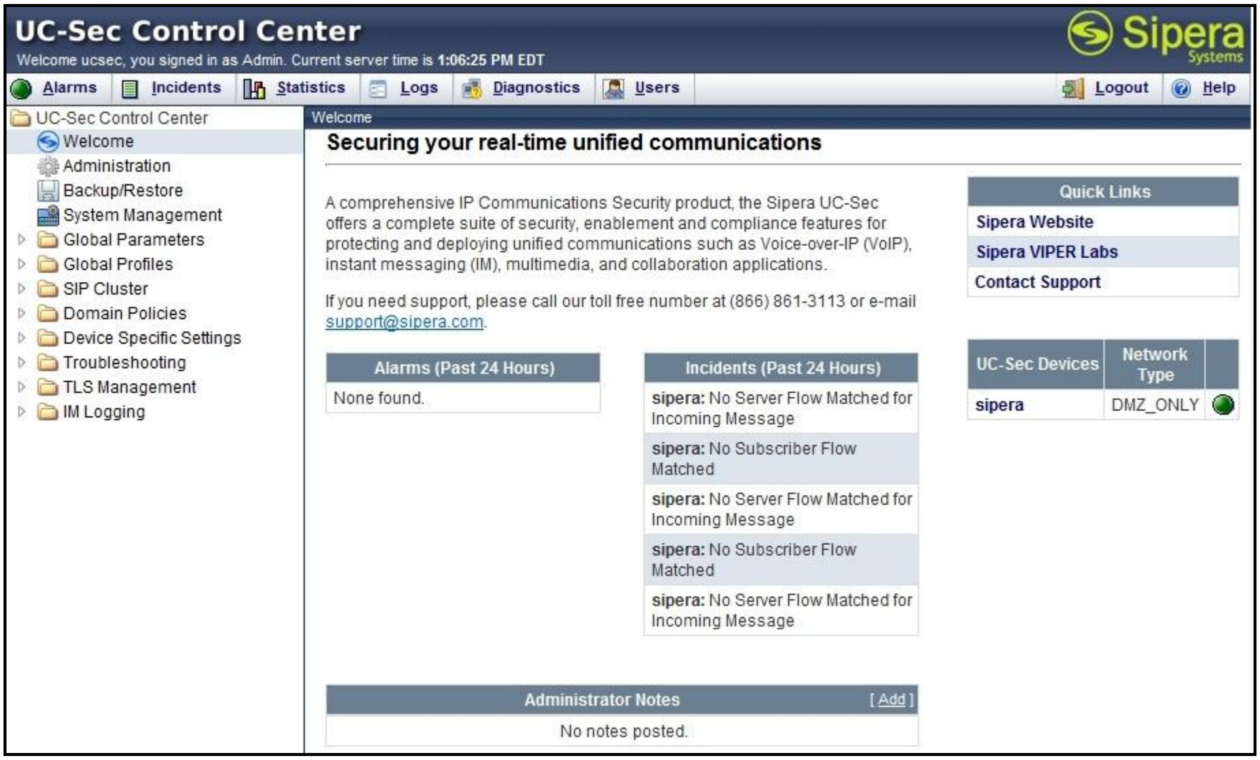
6.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Unify Communication Security (UC-Sec) web interface, enter **https://<ip-addr>/ucsec** in the address field of the web browser (not shown), where <ip-addr> is the management LAN IP address of UC-Sec.

Enter appropriate credentials and click ***Sign In***.

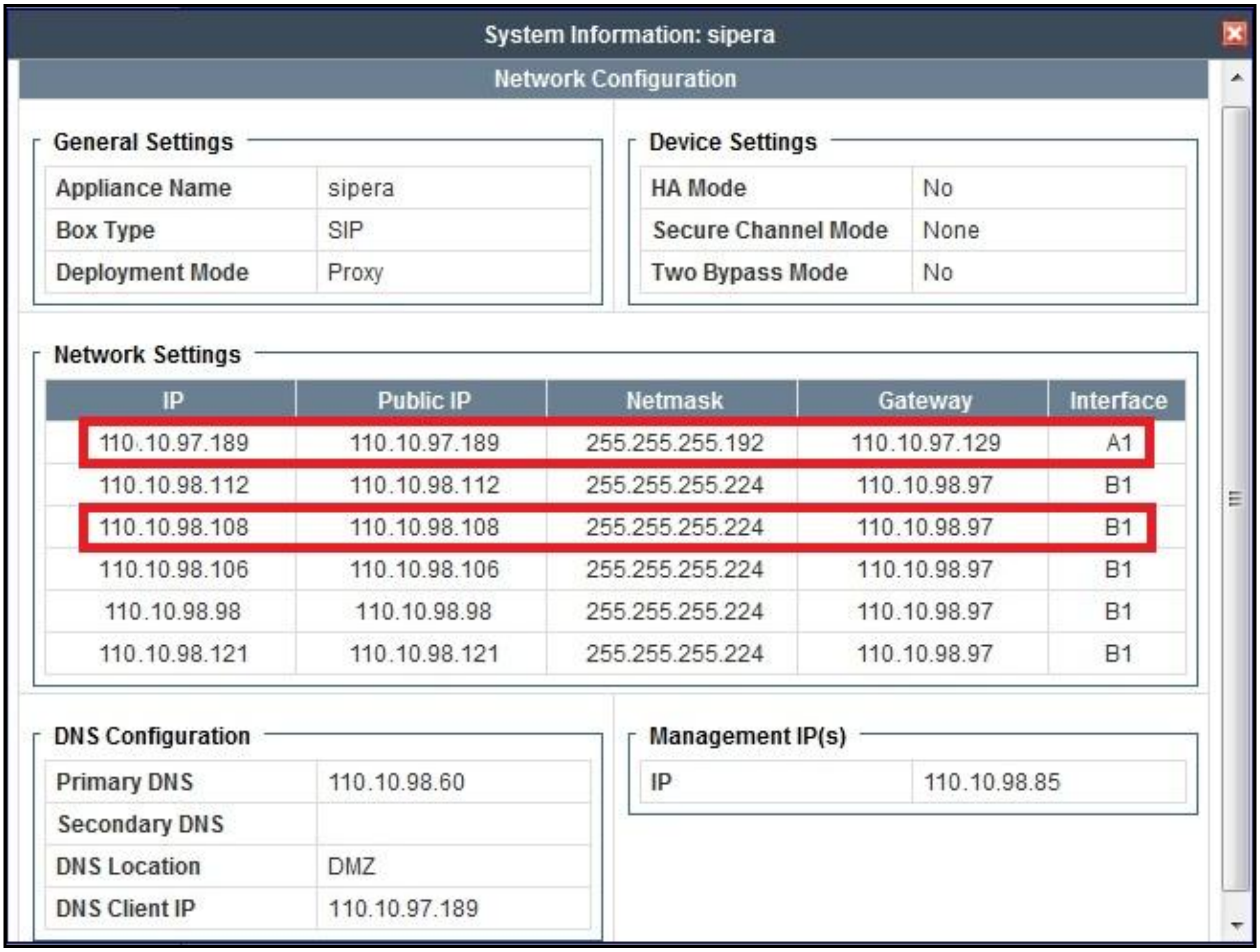


The main page of the **UC-Sec Control Center** will appear as shown below.



To view system information that has been configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single device named **sipera** was added. To view the configuration of this device, click the **View Config** icon (the third icon from the right) as shown below.

The **System Information** screen shows **Network Settings, DNS Configuration** and **Management IP** information provided during installation and corresponds to the screen shot on the next page. The **Box Type** is set to **SIP** and the **Deployment Mode** is set to **Proxy**. Default values are used for all other fields.



6.2. Global Profiles

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

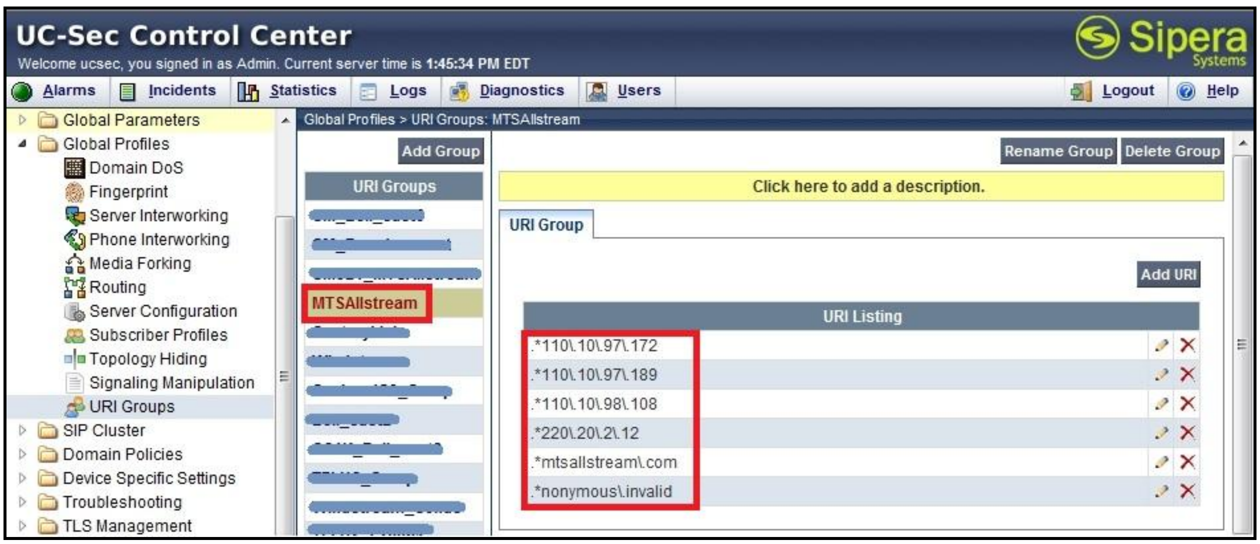
6.2.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

To add an URI Group, select **UC-Sec Control Center → Global Profiles → URI Groups** and click on the **Add Group** button (not shown).

In the compliance testing, a URI Group named **MTSAllstream** was added with URI type **Regular Expression** (not shown) and consists of four domain .*@\.nonymous\.invalid, .*@mtsalllstream\.com, .*@110\.10\.98\.108, .*@220\.20\.2\.12, .*@110\.10\.97\.172 and .*@110\.10\.97.\189. The URI .*@\.nonymous\.invalid is defined to match private calls received either from call server or trunk server had URI-Host masked by **anonymous.invalid**. The enterprise domain name **mtsallstream.com** is for SIP trunk domain defined in **Section 5.5.2** step c) between the CS1000 and the Avaya SBCE via the NRS. For the public SIP trunk between the Avaya SBCE and MTS Allstream, the Avaya SBCE public IP address 110.10.98.108 is set as URI-Host of “From”, “PAI” and “Diversion” headers while the public IP address of MTS Allstream 220.20.2.12 is set as URI-Host of “Request-URI” and “To” headers. URI .*@110\.10\.97\.172 and .*@110\.10\.97\.189 are defined to match outbound OPTIONS heartbeat received from the NRS to make the Avaya SBCE forward to MTS Allstream to query for the status of SIP trunk.

This URI-Group is used to match the “From” and “To” headers in a SIP call dialog received from both the NRS and MTS Allstream. If there is a match, the Avaya SBCE will apply the appropriate Routing Profile and Server Flow to route the inbound or outbound call to the right destinations. The Routing Profile and Server Flow are configured in **Section 6.2.2** and **Section 6.4.4** appropriately. The screenshot below illustrates the URI listing for URI Group **MTSAllstream**.



6.2.2. Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by **Routing Profiles** include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

To create a Routing Profile, select **UC-Sec Control Center → Global Profiles → Routing** and click on the **Add Profile** button (not shown).

In the compliance testing, a Routing Profile named **To_MTSAllstream** was created to be used in conjunction with the server flow defined for the NRS. This entry is to route the outbound call from the enterprise to MTS Allstream.

In the opposite direction, a Routing Profile named **To_NRS** is created to be used in conjunction with the server flow defined for MTS Allstream. This entry is to route the inbound call from MTS Allstream to the enterprise.

6.2.2.1 Routing Profile for MTS Allstream

The screenshot below illustrates the **UC-Sec Control Center → Global Profiles → Routing**: **To_MTSAllstream**. As shown below, MTS Allstream SIP trunk is connected with transportation protocol **UDP**. If there is a match of the "To" header with the **MTSAllstream** URI Group defined in **Section 6.2.1**, the outbound call will be routed to the **Next Hop Server 1** which is the IP address of MTS Allstream trunk server on port 5060.

6.2.2.2 Routing Profile for the NRS

The routing profile **To_NRS** is defined to route inbound call where the "To" header matches the URI-Group **MTSAllstream** defined in **Section 6.2.1** to **Next Hop Server 1** which is the IP address of the NRS, on port 5060 as a destination. As shown in below, the SIP trunk between the NRS and the Avaya SBCE is connected with transportation protocol **TCP**.

6.2.3. Topology Hiding

Topology Hiding is a security feature of the Avaya SBCE which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

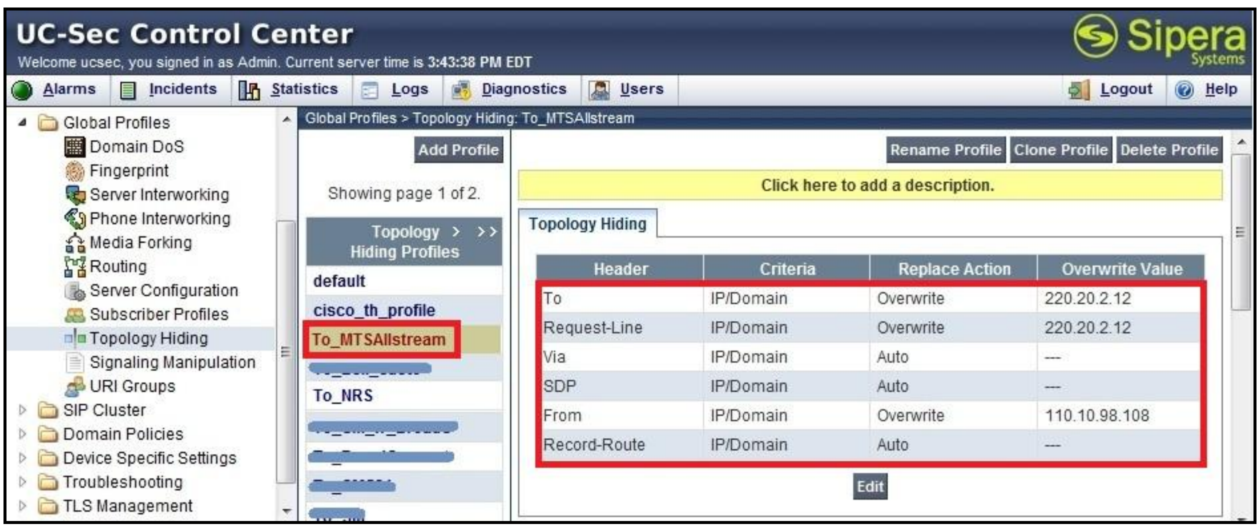
To create a Topology Hiding profile, select **UC-Sec Control Center → Global Profiles → Topology Hiding** and click on the **Add Profile** button (not shown).

In the compliance testing, two Topology Hiding profiles **To_MTSAllstream** and **To_CS1K** were created.

6.2.3.1 Topology Hiding Profile for MTS Allstream

Profile **To_MTSAllstream** is defined to mask the enterprise SIP domain "avaya.com**"** in "Request-URI" and "To" headers to IP **220.20.2.12** (the IP address MTS Allstream uses as URI-Host portion for "Request-URI" and "To" headers to meet the SIP specification requirement of MTS Allstream); mask the enterprise SIP domain "avaya.com" in "From" header to IP **110.10.98.108** (the Avaya SBCE public IP address); and replace "Record-Route", "Via" headers and Session Description Protocol (SDP) added by the CS1000 by external IP address known to MTS Allstream. It is to secure the enterprise network topology and also to meet the SIP requirement from service provider.

The screenshots below illustrate the Topology Hiding profile **To_MTSAllstream**.



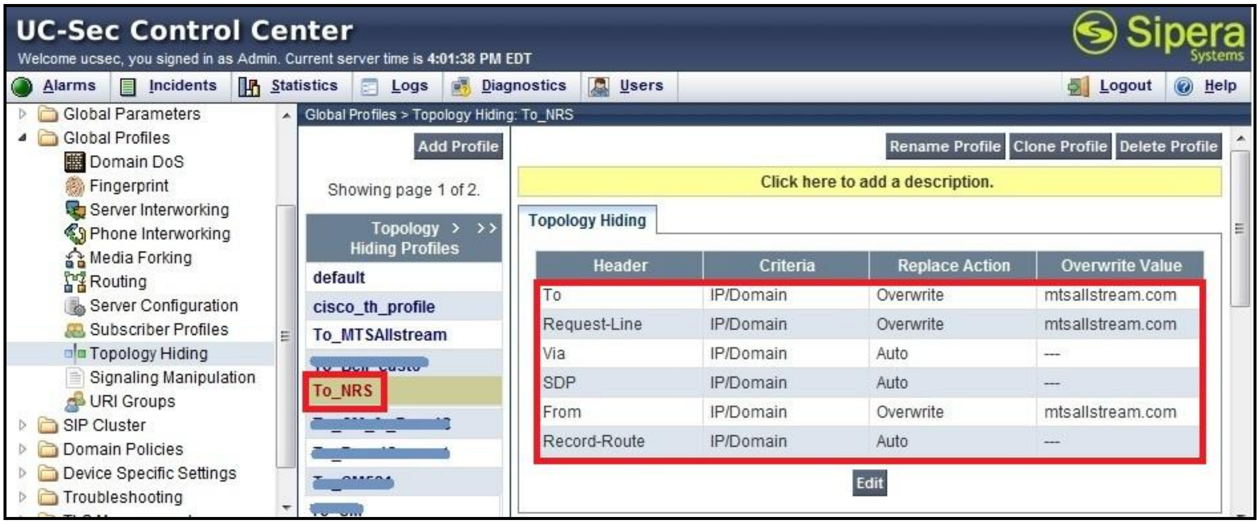
Notes:

- The Criteria should be selected as IP/Domain to give the Avaya SBCE the capability to mask both domain name and IP address present in SIP URI-Host.
- The masking applied on "From" header also applies to "Referred-By" and "P-Asserted-Identity" headers.
- The masking applied on "To" header also applies to "Refer-To" header.

6.2.3.2 Topology Hiding Profile for the NRS

Profile **To_NRS** is also needed to mask MTS Allstream URI-Host in "Request-URI", "From", "To" headers to the enterprise SIP domain "mtsallstream.com"; replace "Record-Route", "Via" headers and SDP added by MTS Allstream by internal IP address known to the CS1000.

The screenshots below illustrate the Topology Hiding profile **To_NRS**.



Notes:

- The Criteria should be IP/Domain to give the Avaya SBCE the capability to mask both domain name and IP address present in SIP URI-Host.
- The masking applied on "From" header also applies to "Referred-By" and "P-Asserted-Identity" headers.
- The masking applied on "To" header also applies to "Refer-To" header.

6.2.4. Server Interworking

Interworking Profile features are configured differently for call and trunk servers.

To create a Server Interworking profile, select **UC-Sec Control Center → Global Profiles → Server Interworking** and click on the **Add Profile** button (not shown).

In the compliance testing, two profiles **MTSAllstream** and **NRS** were created for MTS Allstream and the NRS.

6.2.4.1 Server Interworking profile for MTS Allstream

Profile **MTS Allstream** is defined to match the specification of MTS Allstream. The **General** and **Advanced** settings are configured with following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

General settings:

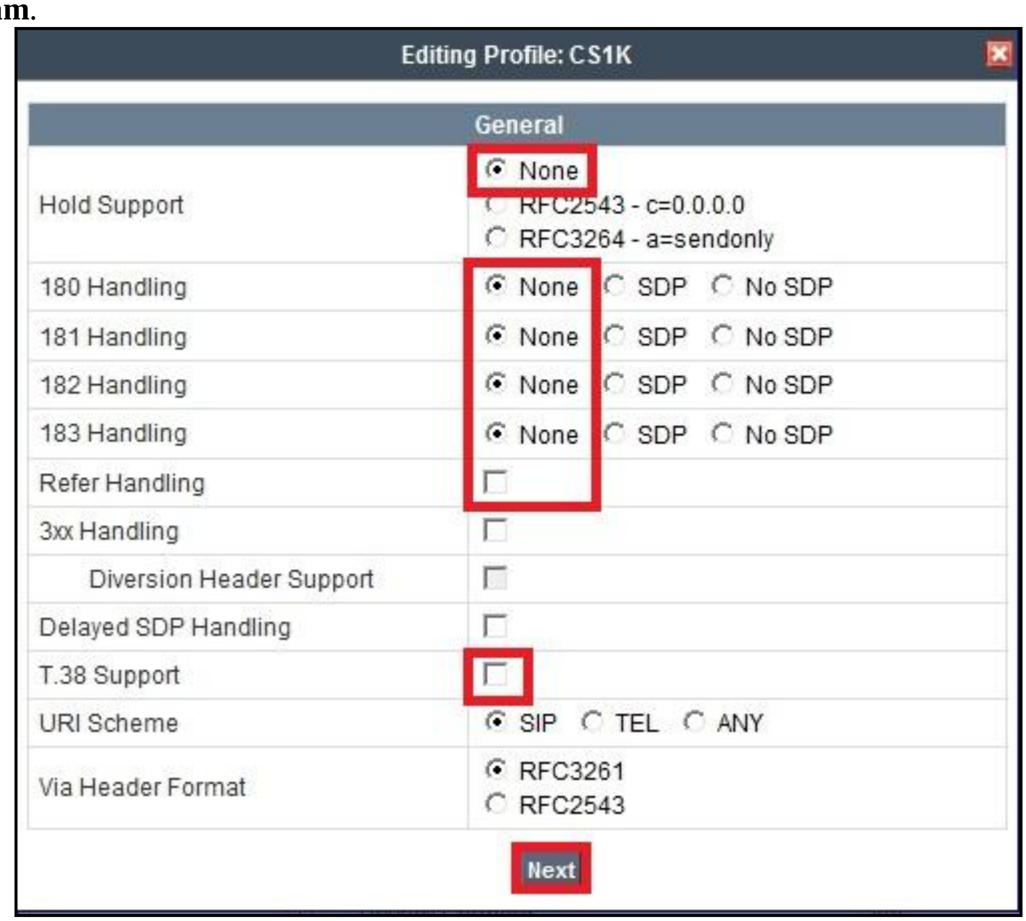
- **Hold Support** = None. The Avaya SBCE will not modify hold/ resume signaling from the CS1000 to MTS Allstream.
- **18X Handling** = None. The Avaya SBCE will not handle 18X responses. It keeps 18X responses unchanged from the CS1000 to MTS Allstream.
- **Refer Handling** = Unchecked. The Avaya SBCE will not handle REFER request. It keeps REFER request unchanged from the CS1000 to MTS Allstream.

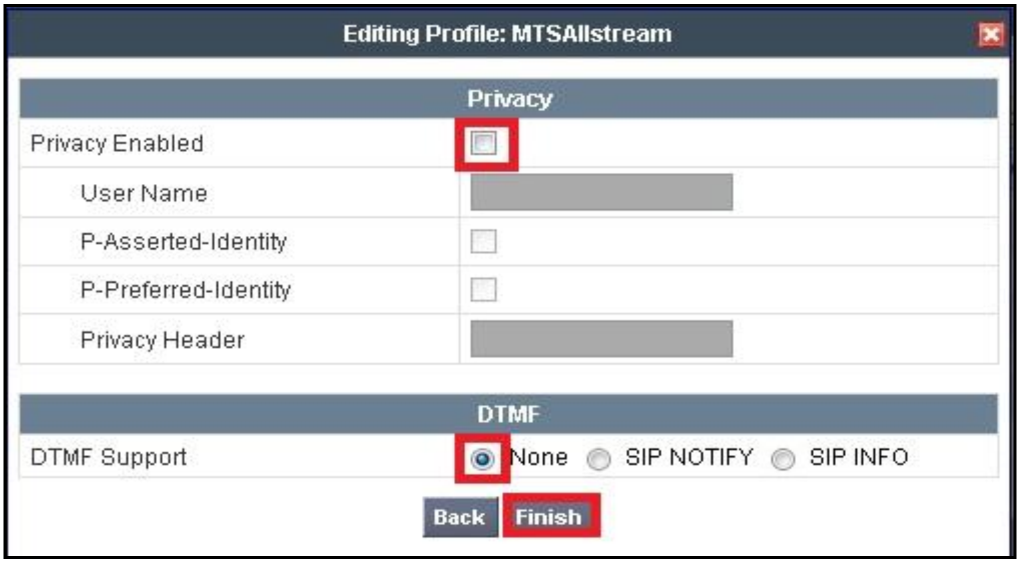
- **T.38 Support** = Unchecked. MTS Allstream does not support T.38 fax in the compliance testing.
- **Privacy Enabled** = Unchecked. The Avaya SBCE will not mask “From” header with anonymous for outbound call to MTS Allstream. It depends on the CS1000 to enable/ disable privacy on individual call basis.
- **DTMF Support** = None. The Avaya SBCE will send original DTMF supported by the CS1000 to MTS Allstream.

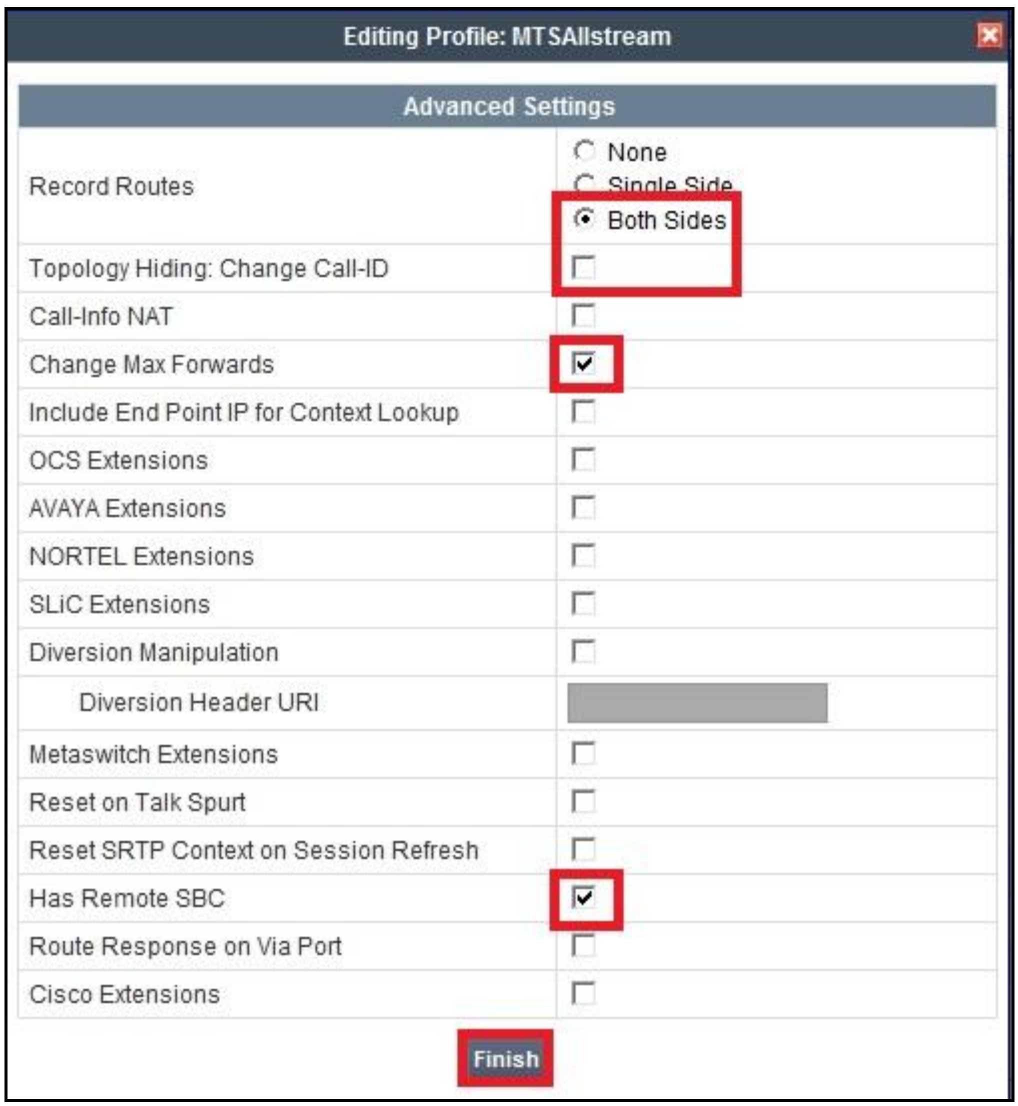
Advanced settings:

- **Record Routes** = Both Sides. The Avaya SBCE will send “Record-Route” header to both call and trunk servers.
- **Topology Hiding**: Change Call-ID = Unchecked. The Avaya SBCE will not modify “Call-ID” header. It keeps original Call-ID unchanged from the CS1000 to MTS Allstream.
- **Change Max Forwards**: Checked. The Avaya SBCE will adjust the original Max-Forwards value from the CS1000 to MTS Allstream by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC**: Checked. MTS Allstream has SBC which interfaces its Central Office (CO) with enterprise SIP trunk.

The screenshots below and on the next page illustrate the Server Interworking profile **MTS Allstream**.




Editing Profile: MTSAllstream
Privacy
Privacy Enabled
User Name
P-Asserted-Identity
P-Preferred-Identity
Privacy Header
DTMF
DTMF Support
None
SIP NOTIFY
SIP INFO
Back
Finish


Editing Profile: MTSAllstream
Advanced Settings
Record Routes
None
Single Side
Both Sides
Topology Hiding: Change Call-ID
Call-Info NAT
Change Max Forwards
Include End Point IP for Context Lookup
OCS Extensions
AVAYA Extensions
NORTEL Extensions
SLiC Extensions
Diversion Manipulation
Diversion Header URI
Metaswitch Extensions
Reset on Talk Spurt
Reset SRTP Context on Session Refresh
Has Remote SBC
Route Response on Via Port
Cisco Extensions
Finish

6.2.4.2 Server Interworking profile for the NRS

Profile **NRS** is defined to match the specification of the CS1000. The **General** and **Advanced** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

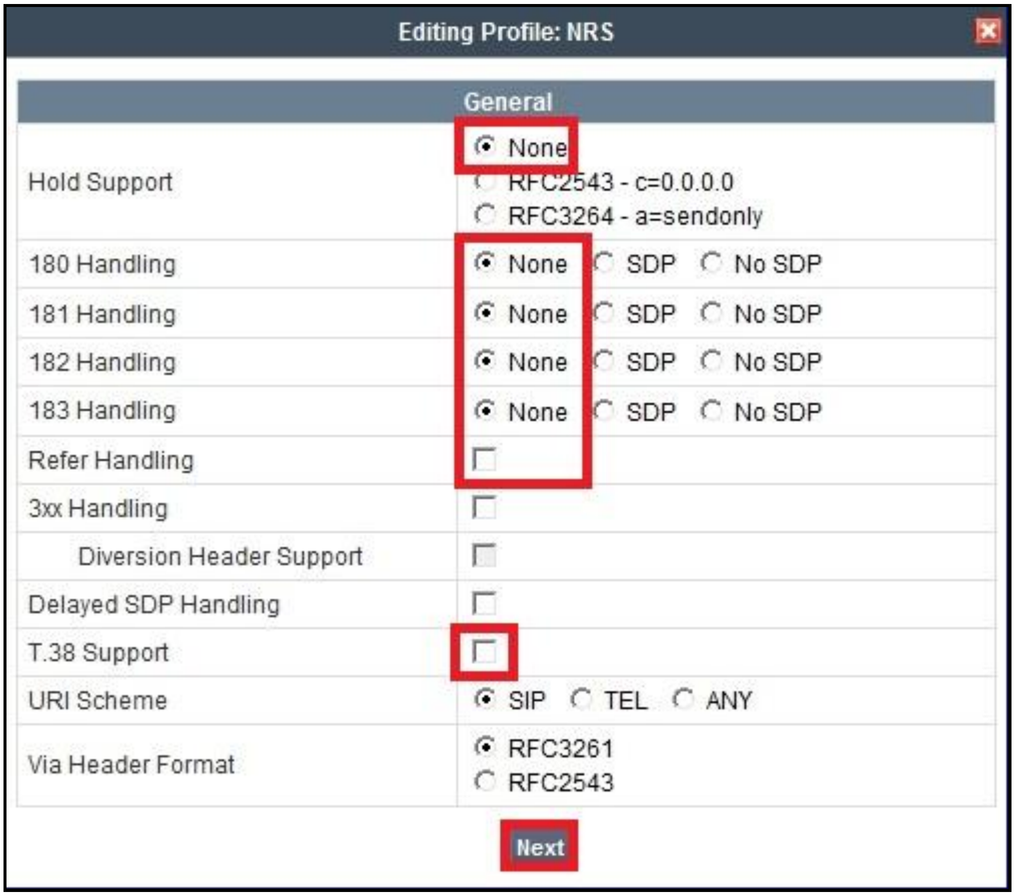
General settings:

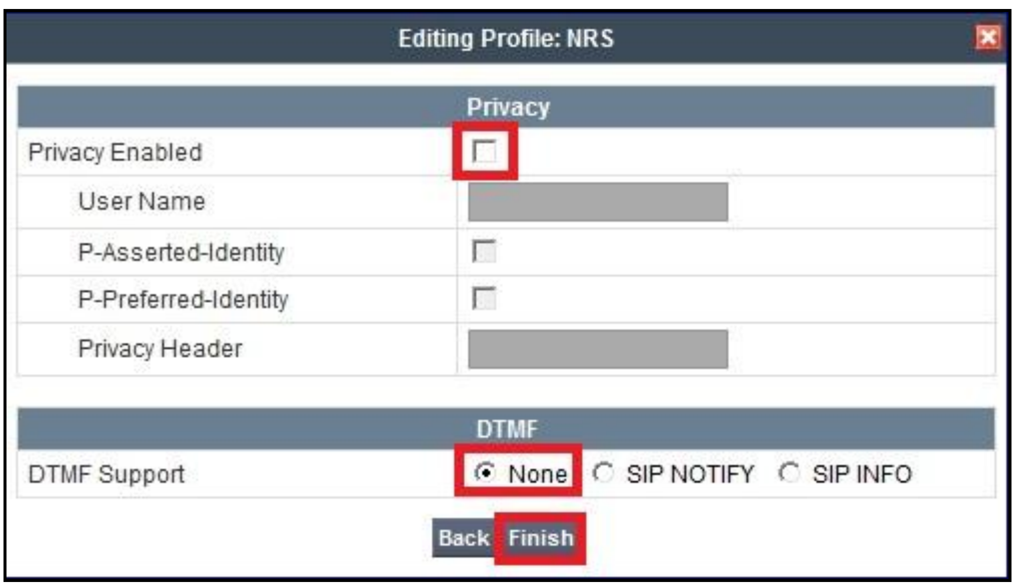
- **Hold Support** = None. The Avaya SBCE will not modify hold/ resume signaling from MTS Allstream to the CS1000.
- **18X Handling** = None. The Avaya SBCE will not handle 18X responses. It keeps 18X responses unchanged from MTS Allstream to the CS1000.
- **Refer Handling** = Unchecked. The Avaya SBCE will not handle REFER request. It keeps REFER request unchanged from MTS Allstream to the CS1000.
- **T.38 Support** = Unchecked. MTS Allstream does not support T.38 fax in the compliance testing.
- **Privacy Enabled** = Unchecked. The Avaya SBCE will not mask “From” header with anonymous for inbound call to the CS1000. It depends on the MTS Allstream to enable/ disable privacy on individual call basis.
- **DTMF Support** = None. The Avaya SBCE will send original DTMF supported by MTS Allstream to the CS1000.

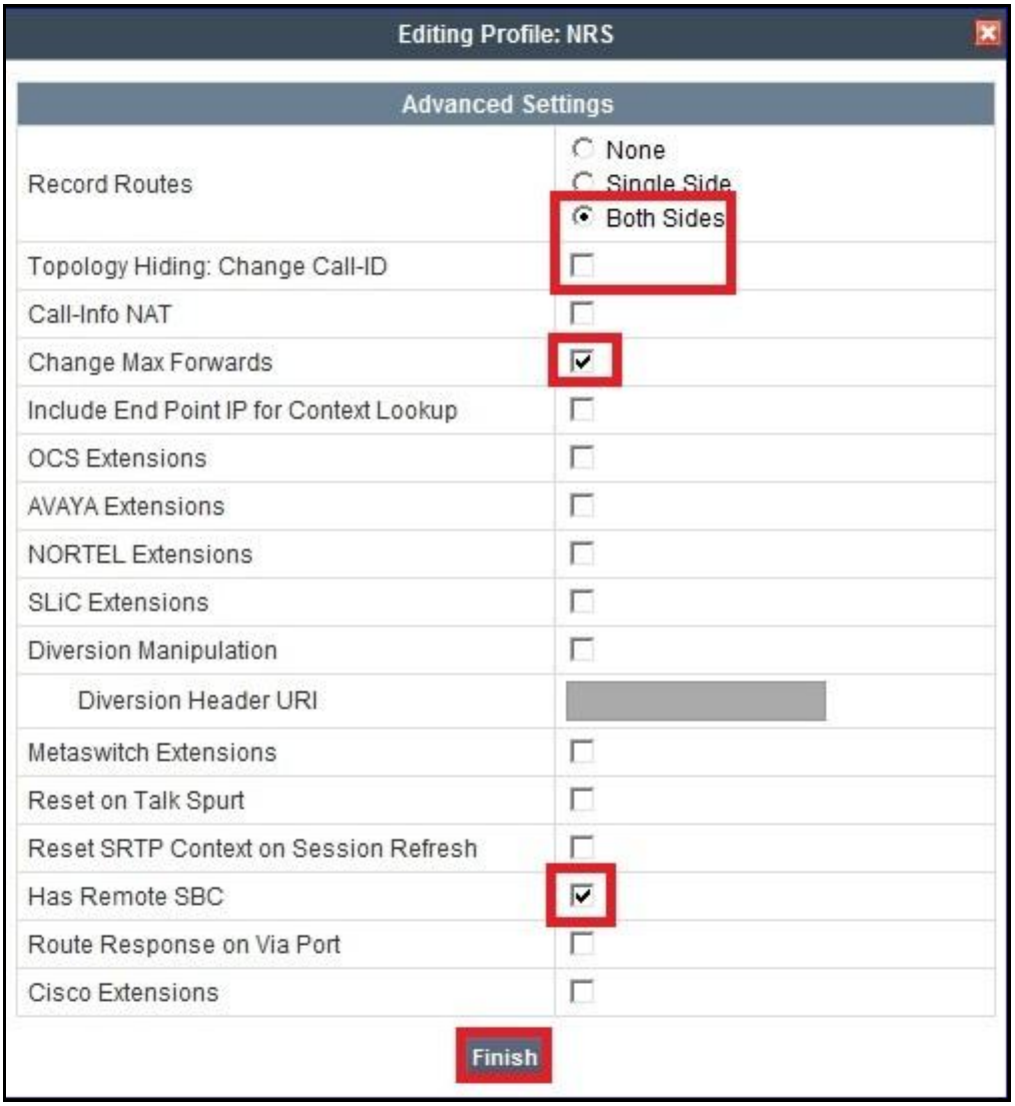
Advanced settings:

- **Record Routes** = Both Sides. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Topology Hiding**: Change Call-ID = Unchecked. The Avaya SBCE will not modify Call-ID. It keeps original Call-ID unchanged from MTS Allstream to the CS1000.
- **Change Max Forwards**: Checked. The Avaya SBCE will adjust the original Max-Forwards value from MTS Allstream to the CS1000 by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC**: Checked.
-

The screenshots on the next two pages illustrate the Server Interworking profile **NRS**.


Editing Profile: NRS
General
Hold Support
None
RFC2543 - c=0.0.0.0
RFC3264 - a=sendonly
180 Handling
181 Handling
182 Handling
183 Handling
None
SDP
No SDP
Refer Handling
3xx Handling
Diversion Header Support
Delayed SDP Handling
T.38 Support
URI Scheme
SIP
TEL
ANY
Via Header Format
RFC3261
RFC2543
Next


Editing Profile: NRS
Privacy
Privacy Enabled
User Name
P-Asserted-Identity
P-Preferred-Identity
Privacy Header
DTMF
DTMF Support
None
SIP NOTIFY
SIP INFO
Back
Finish



6.2.5. Signaling Manipulation

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

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given Server Configuration which is configured in the next steps through the EMS GUI. The Avaya SBCE appliance then interprets this script at the given entry point or "hook point".

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in Topology Hiding.

To create a Signaling Manipulation script, select **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on the **Add Script** button (not shown). Separate SigMa scripts are created for call server and trunk server.

In the compliance testing, a SigMa script named **MTSAllstream_To_NRS** was created for server configuration of MTS Allstream as described below.

```
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 {
  if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("64777612")) then
   {
    %var="this does nothing, match for DID number passed";
   }
  else
   {
    if (%HEADERS["History-Info"][1].regex_match("reason")) then
     {
      %var="this does nothing, match for DID number passed";
     }
    else
     {
      %HEADERS["History-Info"][1].URI.USER="6477761232";
     }
    %HEADERS["Diversion"][1] = "sip:dummy@dummy.com";
    %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-Info"][1].URI.SCHEME;
    %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-Info"][1].URI.USER;
    %HEADERS["Diversion"][1].URI.HOST = "110.10.98.108";
    %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-Info"][1].URI.PORT;
    %HEADERS["Diversion"][1].URI.PARAMS["reason"] = "unconditional";
    %HEADERS["Diversion"][1].URI.PARAMS["counter"] = "1";
    %HEADERS["Diversion"][1].URI.PARAMS["privacy"] = "off";
   }
  remove(%HEADERS["History-Info"][2]);
  remove(%HEADERS["History-Info"][1]);
  %HEADERS["P-Asserted-Identity"][1].URI.HOST="110.10.98.108";
 }
}
```

The statement `act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"` is to specify the script will take effect on all type of SIP messages for outbound calls to MTS Allstream and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

A set of rules as shown in the screenshot below are added in the "if" statement to check P-Asserted-Header if a DID number does not exist in URI-User to match the scenario of either call forward off-net or mobility extension. In case of call forward off-net, the URI-User of History-Info header will present a DID number known to MTS Allstream for call authentication purpose. Then the followed rules will apply to construct Diversion header based on the information of History-Info header. However, in case of mobility extension calls, URI-User of History-Info header presents original PSTN number which is not known to MTS Allstream. Therefore, before constructing the Diversion header, the URI-User of History-Info needs to be re-defined as a DID number known to MTS Allstream (as known as a pilot number). Without the pilot number, the outbound call to mobility extension will fail to be authenticated, it then results a call drop.

```
if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("64777612")) then
   {
    %var="this does nothing, match for DID number passed";
   }
  else
   {
    if (%HEADERS["History-Info"][1].regex_match("reason")) then
     {
      %var="this does nothing, match for DID number passed";
     }
    else
     {
      %HEADERS["History-Info"][1].URI.USER="6477761232";
     }
    %HEADERS["Diversion"][1] = "sip:dummy@dummy.com";
    %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-Info"][1].URI.SCHEME;
    %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-Info"][1].URI.USER;
    %HEADERS["Diversion"][1].URI.HOST = "110.10.98.108";
    %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-Info"][1].URI.PORT;
    %HEADERS["Diversion"][1].URI.PARAMS["reason"] = "unconditional";
    %HEADERS["Diversion"][1].URI.PARAMS["counter"] = "1";
    %HEADERS["Diversion"][1].URI.PARAMS["privacy"] = "off";
   }
```

After the Diversion has been created, two rules are also added as shown in the screenshot below to delete index 1 and 2 of History-Info header because they are not required by MTS Allstream.

```
  remove(%HEADERS["History-Info"][2]);
  remove(%HEADERS["History-Info"][1]);
```

The **Topology-Hiding** profile **MTSAllstream** could successfully mask URI-Host of P-Asserted-Identity header in “request” signaling. However, as a limitation, the P-Asserted-Identity header in “response” signaling still have the private enterprise SIP domain. Therefore, a SigMa rule is used to correct the URI-Host of P-Asserted-Identity header, it is shown in the screenshot below.

```
  %HEADERS["P-Asserted-Identity"][1].URI.HOST="110.10.98.108";
```

Note: The SigMa script for the CS1000 is not required as all the necessary signaling modification has been applied to server configuration of MTS Allstream.

6.2.6. Server Configuration

Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, **Advanced**, **DoS Whitelist** and **DoS Protection** These tabs are used to configure and manage various SIP call server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

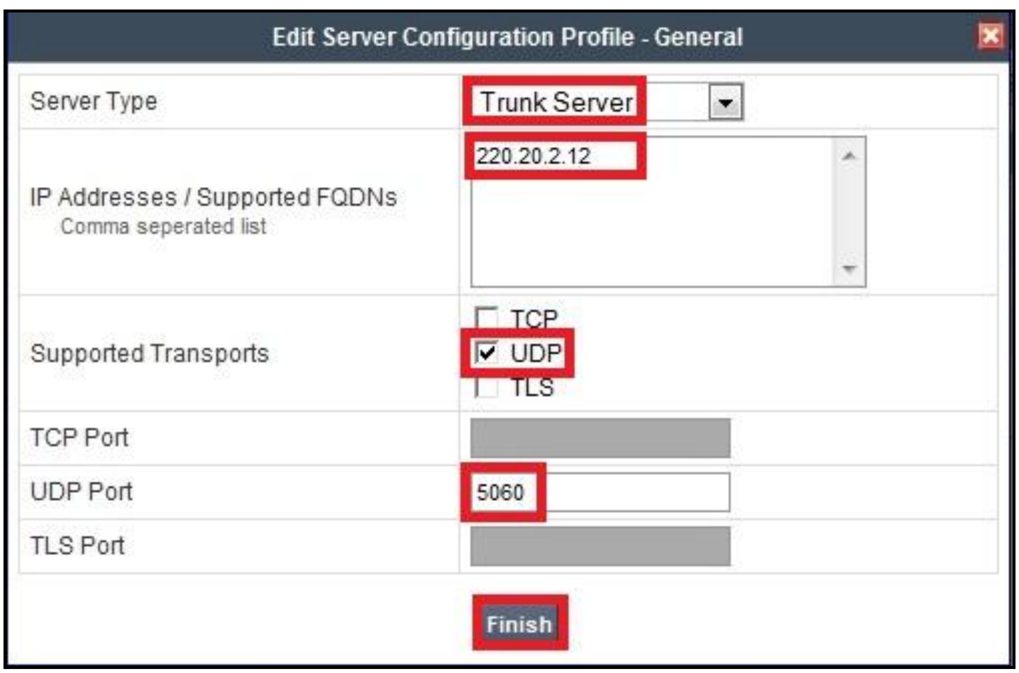
To create a Server Configuration entry, select **UC-Sec Control Center →Global Profiles →Server Configuration** and click on the **Add Profile** button (not shown).

In the compliance testing, two separate Server Configurations were created, entry **MTSAllsream** for MTS Allstream and entry **NRS** for the NRS.

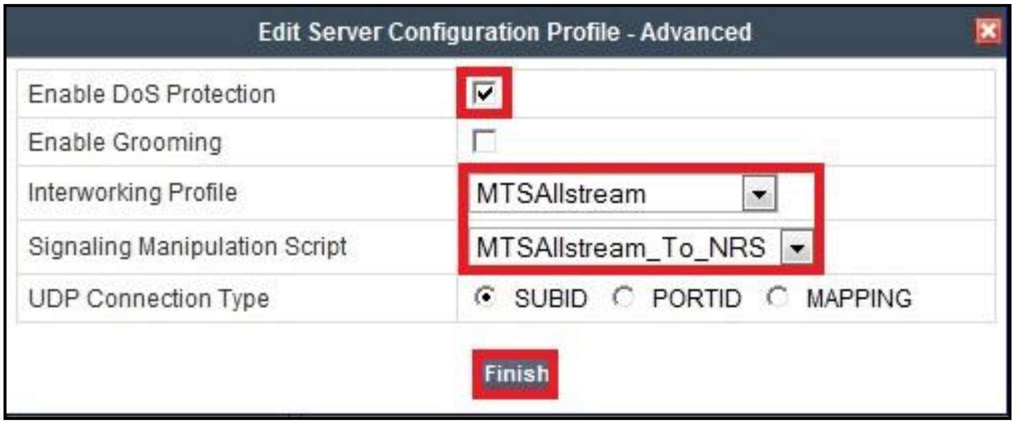
6.2.6.1 Server Configuration for MTS Allstream

The Server Configuration named **MTSAllstream** is added for MTS Allstream, it will be discussed in detail as below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab as MTS Allstream does not implement Authentication on a SIP trunk. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from the NRS to MTS Allstream to query the status of the SIP trunk. The **DoS Whitelist** and **DoS Protection** tabs are displayed after DoS Protection is enabled under **Advanced** tab, the settings for them are kept as default.

In the **General** tab, set **Server Type** for MTS Allstream to **Trunk Server**. During the compliance testing, MTS Allstream supported UDP and listened on port 5060.

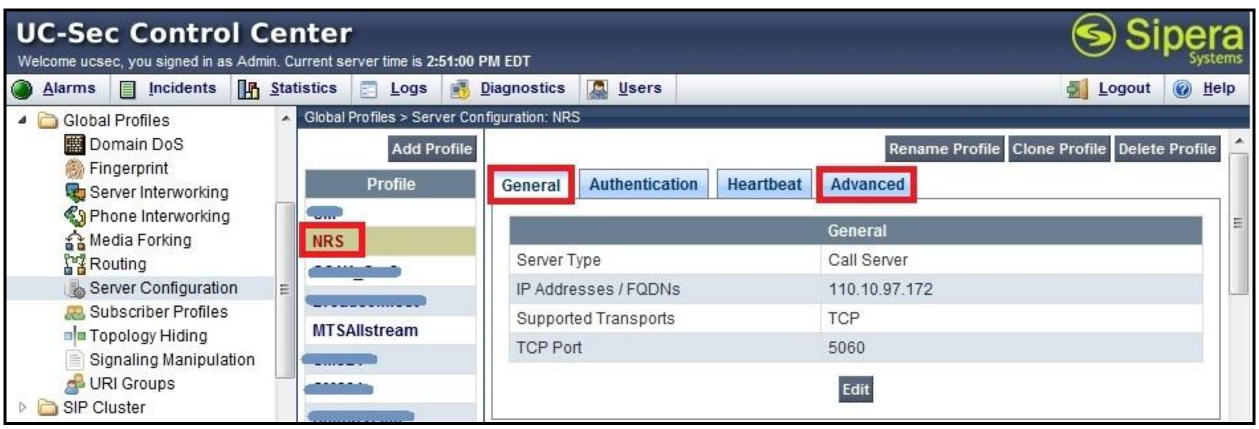


Under **Advanced** tab, check to activate **Enable DoS Protection**. For **Interworking Profile** drop down list, select **MTSAllstream** as defined in **Section 6.2.4** and for **Signaling Manipulation Script** drop down list select **MTSAllsteram_To_NRS** as defined in **Section 6.2.5**. These configurations are applied the specific SIP profile and SigMa rules to the MTS Allstream traffic. The other settings are kept as default.

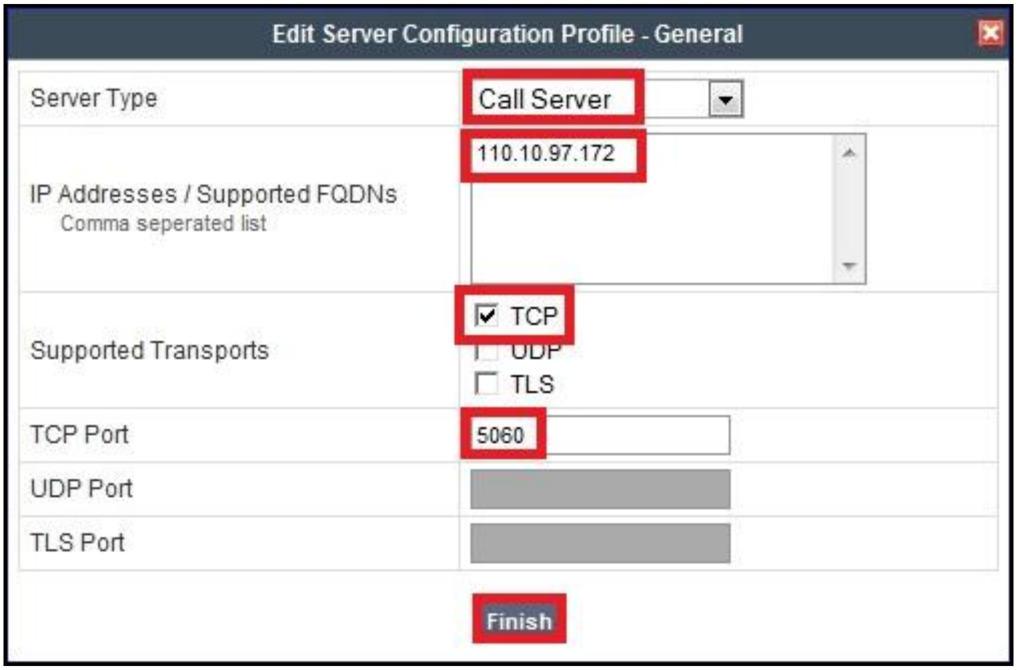


6.2.6.2 Server Configuration for the NRS

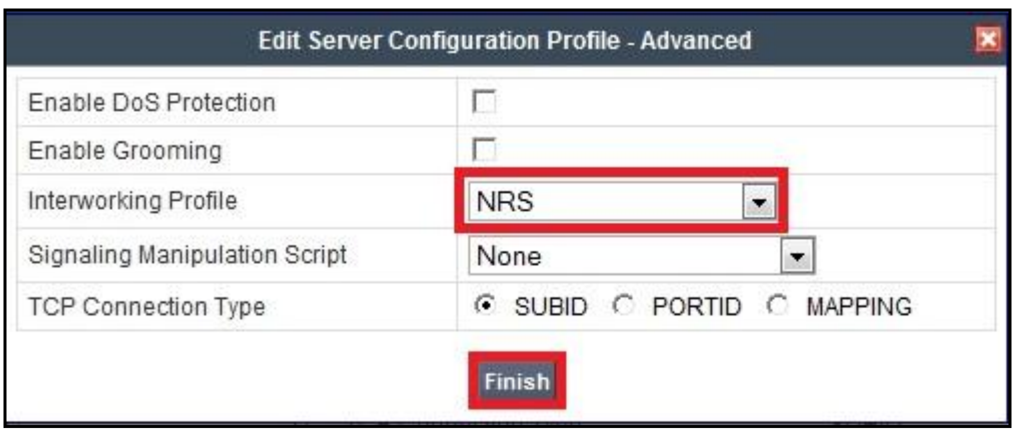
The Server Configuration named **NRS** is added for the CS1000 is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from MTS Allstream to the NRS to query the status of the SIP trunk.



In the **General** tab, specify **Server Type** as **Call Server**. During the compliance testing, the link between the Avaya SBCE and the NRS was TCP and the NRS listened on port 5060.



Under **Advanced** tab, for **Interworking Profile** drop down list select **NRS** as defined in **Section 6.2.4**. The other settings are kept as default.



6.3. Domain Policies

Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the UC-Sec security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

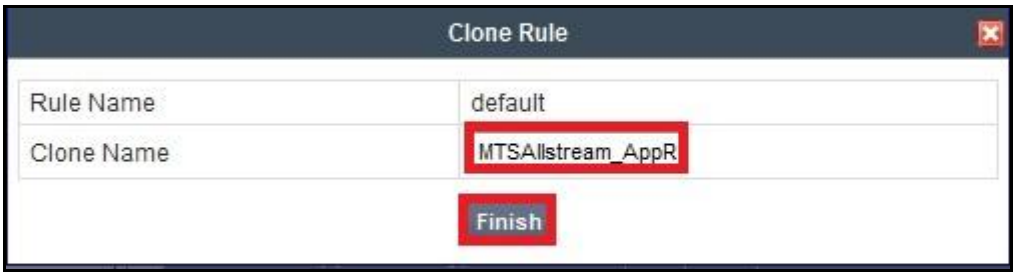
6.3.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, it is possible to configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

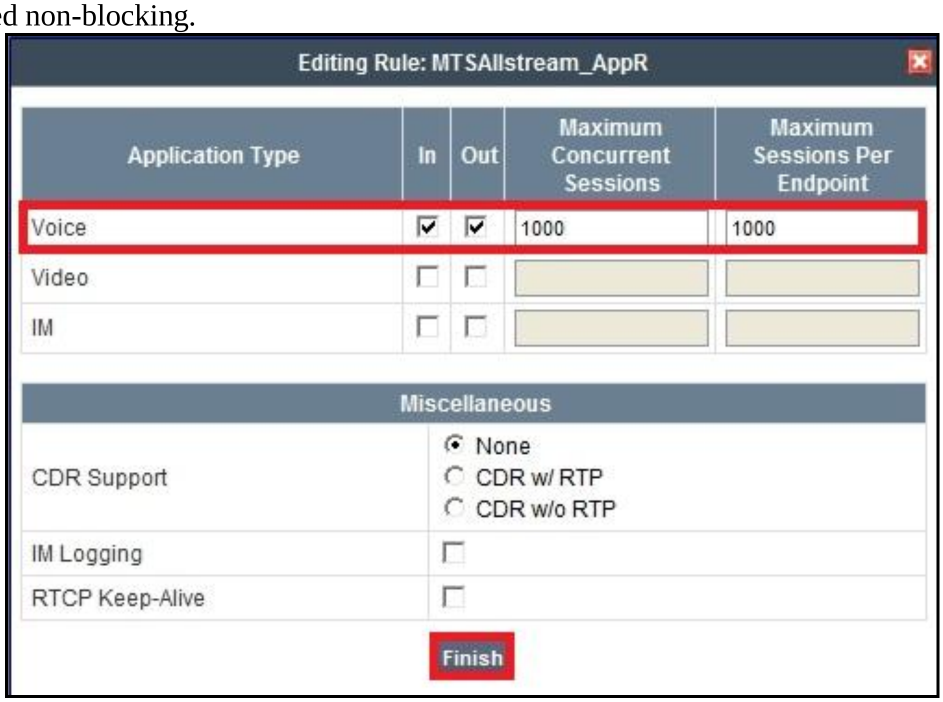
An Application Rule is created to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules** and select the default rule then click on the **Clone Rule** button (not shown).

Enter a rule with a descriptive name **MTSAllstream_AppR** and click on the **Finish** button.



Click **Edit** button (not shown) to modify the rule. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to 1000. In the compliance testing, the CS1000 was programmed to control the concurrent sessions by setting the number of Virtual Trunks (**Section 5.5.7**) to the allotted number. Therefore, the values in the Application Rule named **MTSAllstream_AppR** are set high enough to be considered non-blocking.



6.3.2. Media Rules

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

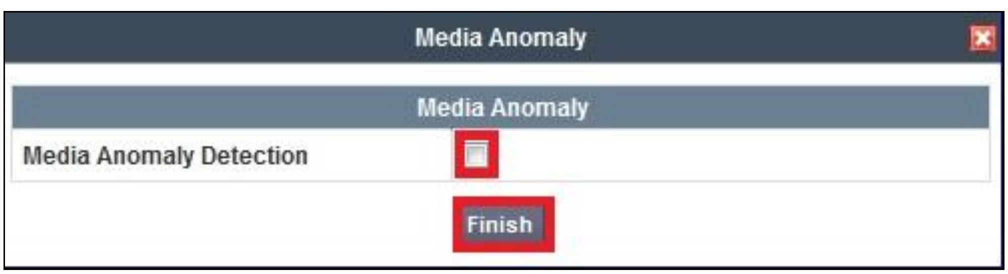
A custom Media Rule is created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration shows Media Rule **MTSAllstream_MediaR** used for both the CS1000 and MTS Allstream.

To create a Media Rule, navigate to **UC-Sec Control Center → Domain Policies → Media Rules** and select the **default-low-med** rule then click on the **Clone Rule** button (not shown).

Enter a Media Rule with a descriptive name **MTSAllstream_MediaR** and on the click **Finish** button.

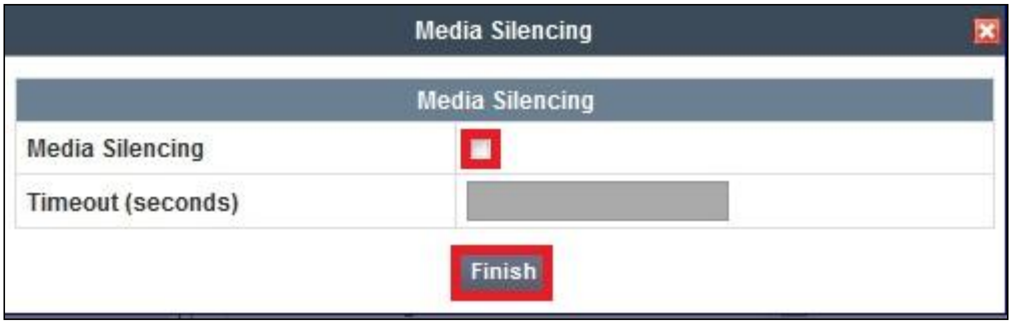
When the RTP of a call is changed when an active call is in progress, the Avaya SBCE will interpret this as an anomaly and an alert will be created in the **Incidents Log**. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created in the log during a modification to audio stream.

To modify the Media Rule, select the **Media Anomaly** tab and click on the **Edit** button (not shown), uncheck **Media Anomaly Detection** and click on the **Finish** button.

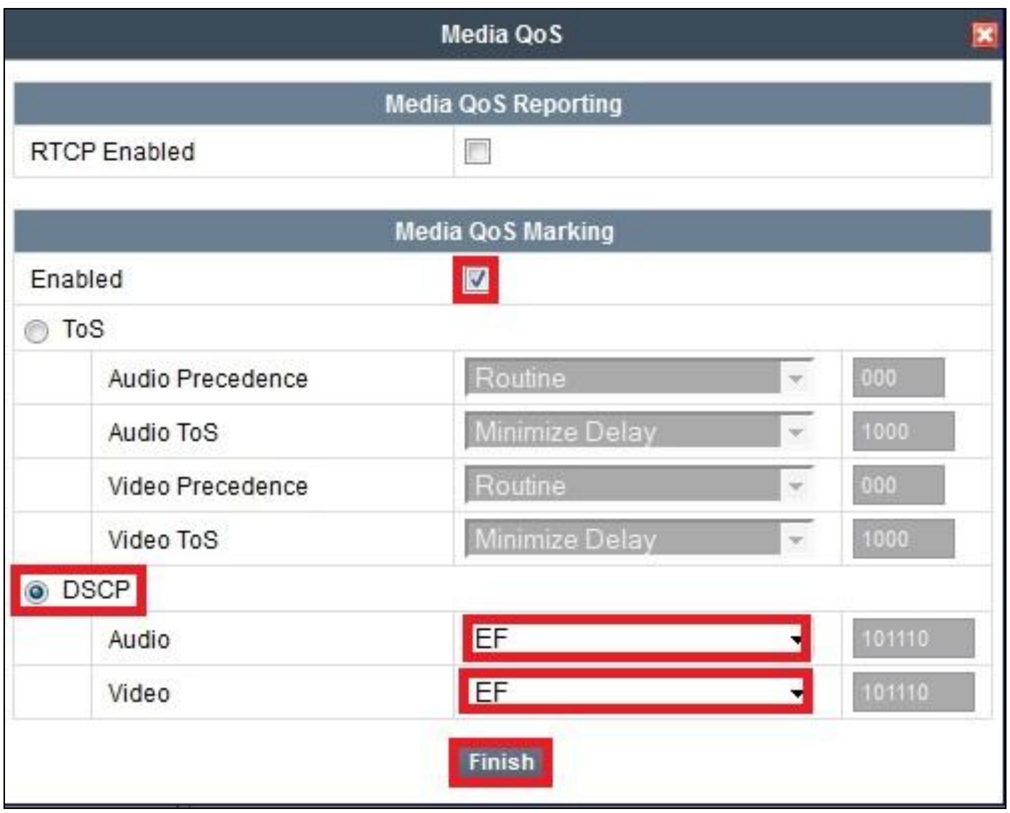


Media Silencing feature detects silence when the call is in progress. If the silence is detected and exceeds the allowed duration, the Avaya SBCE generates alert in the **Incidents Log**. In the compliance testing, the Media Silencing detection was disabled to prevent the call from unexpectedly disconnected due to a RTP packet lost maybe happen temporarily on public Internet.

To modify the Media Rule, select the **Media Silencing** tab and click on the **Edit** button (not shown), uncheck **Media Silencing** and click on the **Finish** button.



Next, select the **Media QoS** tab and click **Edit** to configure the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in header of IP packet with specific values to support Quality of Services policies for the media. The following screen shot on the next page shows the QoS values used for the compliance testing.



6.3.3. Signaling Rules

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

To clone a Signaling Rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules** and select the **default** rule then click on the **Clone Rule** button (not shown).

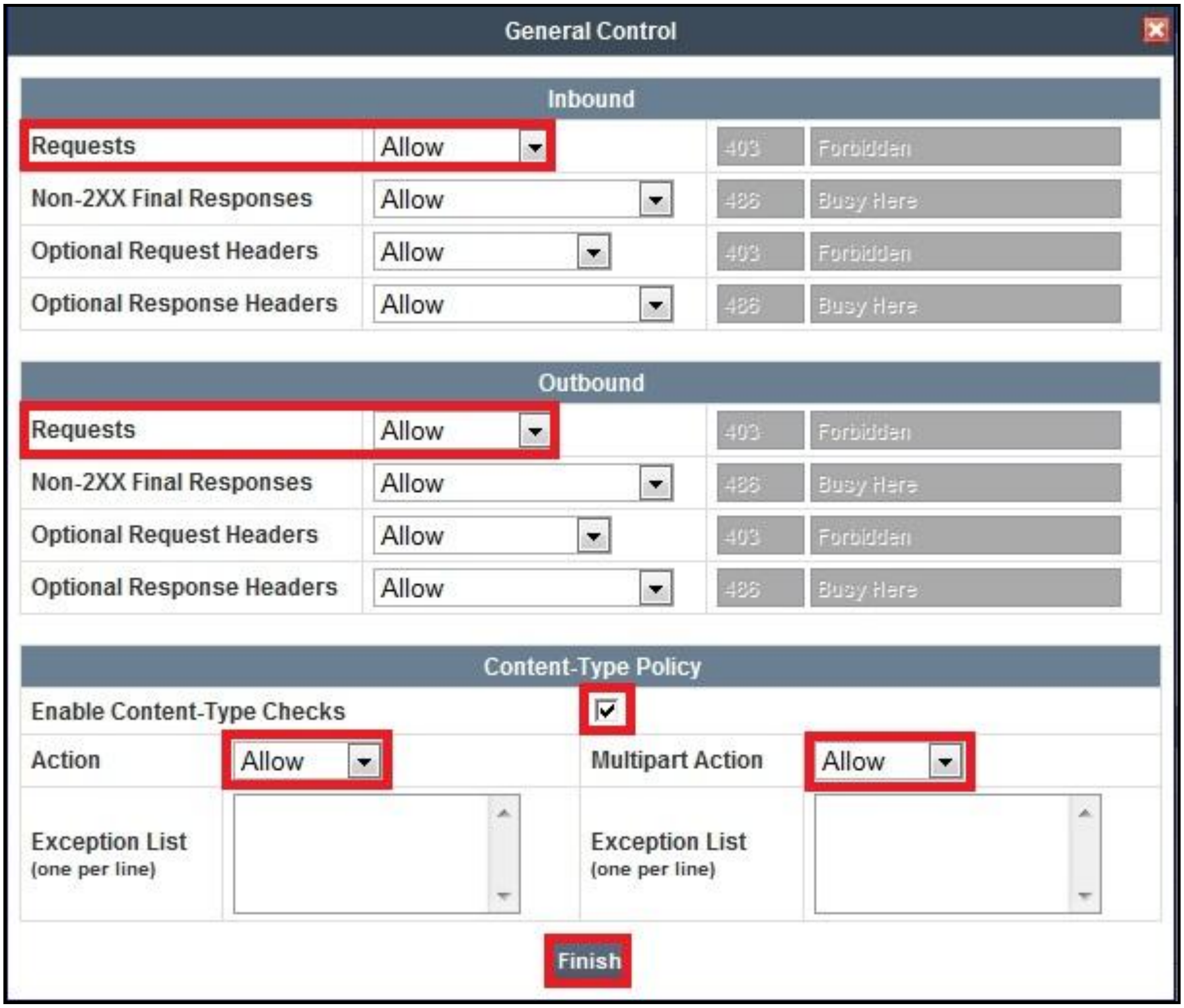
In the compliance testing, two Signaling Rules were created for MTS Allstream and the NRS.

6.3.3.1 Signaling Rule for MTS Allstream

Clone a Signaling Rule with a descriptive name **MTSAllstream_SigR** and click on the **Finish** button.

The **MTSAllstream_SigR** is configured to allow the Avaya SBCE to accept inbound and outbound call requests from MTS Allstream. It also blocks Alert-Info, x-nt-e164-clid and x-nt-ocn-id headers from the CS1000 because these headers are not required by MTS Allstream.

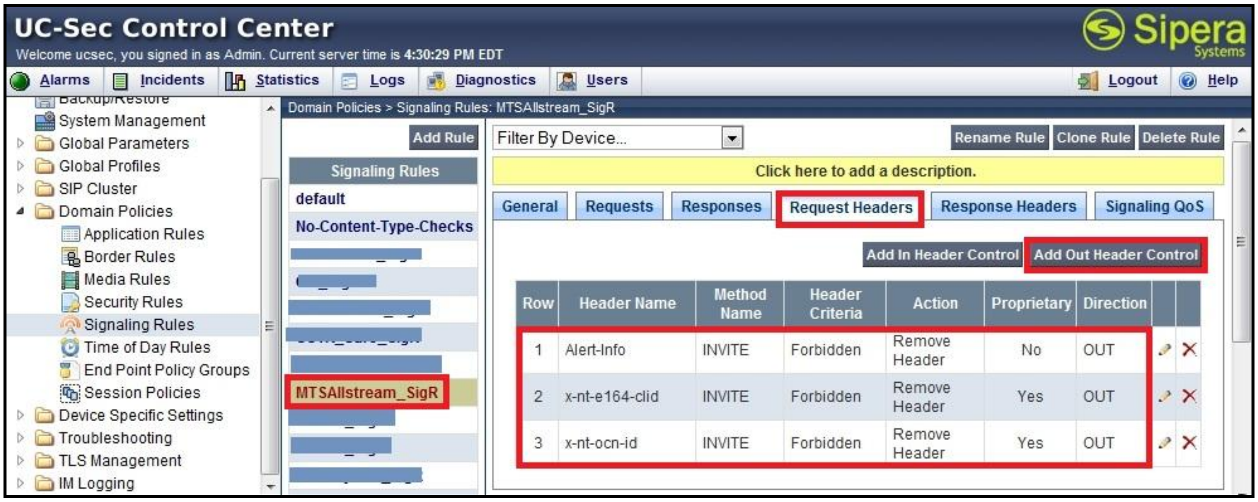
Being cloned from the **Signaling Rule default**, the **MTSAllstream_SigR** blocks all requests with 403 Forbidden. To start accepting calls, go to **General** tab, click on **Edit** (not shown). Then change **Inbound** and **Outbound Request** to **Allow**. **Content-Type Policy** is also configured to allow Multipart Content-Type from the CS1000 as shown in the screenshot below.



Request Headers setting is to allow or block a header in particular direction for request method. The buttons "**Add In Header Control**" and "**Add Out Header Control**" are used to define the inbound and outbound Request Header rules. The signaling rule **MTSAllstream_SigR** will be assigned to server configure of MTS Allstream as discussed in **Section 6.2.6.1**.

The following screenshot shows three rules added to block the Alert-Info, nt-e164-clid and x-nt-ocn-id headers.

- **Header Name**: Select or enter a header to be manipulated
- **Method Name**: Select **INVITE**
- **Header Criteria**: Click on **Forbidden**
- **Action**: Select **Remove Header**



Note: The pre-defined list does not include nt-e164-clid and x-nt-ocn-id headers, but the Avaya SBCE provides an option to define these as proprietary headers.

Response Headers setting is to allow or block a header in particular direction for response method. The buttons "**Add In Header Control**" and "**Add Out Header Control**" are used to define inbound and outbound Response Header rules. The Signaling Rule **MTSAllstream_SigR** will be assigned to Server Configure for MTS Allstream as discussed in **Section 6.2.6.1**.

The following screenshots show three rules added to block the Alert-Info, nt-e164-clid and x-nt-ocn-id headers.

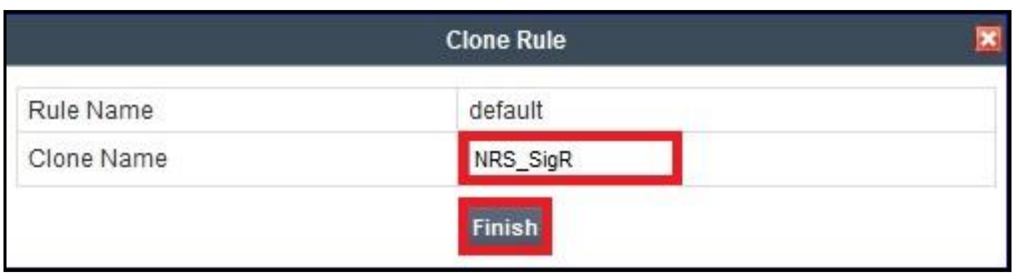
- **Header Name**: Select the header to be manipulated
- **Response Code**: Select **2XX**
- **Method Name**: Select **INVITE**
- **Header Criteria**: Click on **Forbidden**
- **Action**: Select **Remove Header**

Note: The pre-defined list does not include nt-e164-clid and x-nt-ocn-id headers, but the Avaya SBCE provides an option to define these as proprietary headers.

Under **Signaling QoS** tab, select proper value for Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in header of IP packet with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance testing.

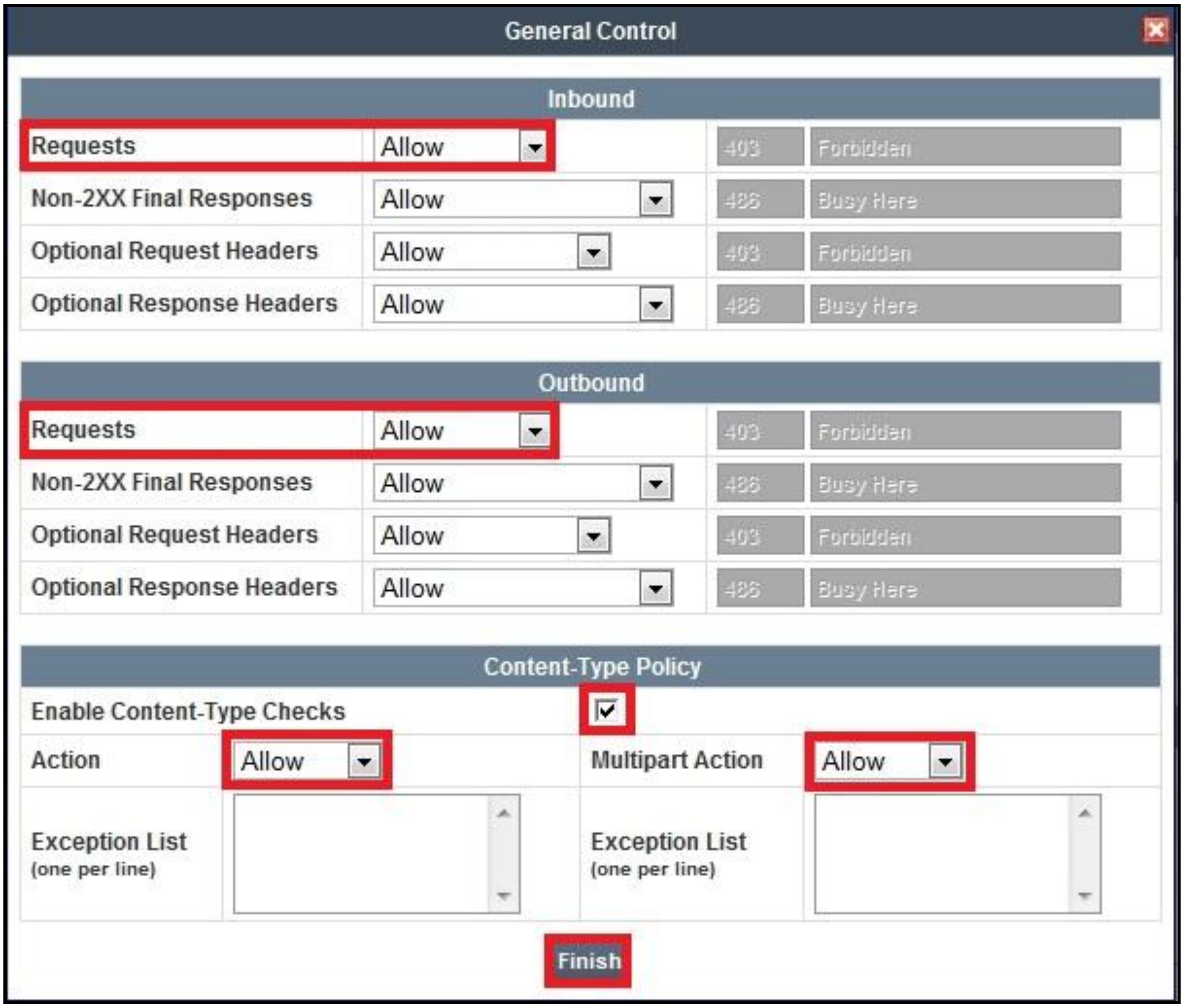
6.3.3.2 Signaling Rule for the NRS

Clone a Signaling Rule with a descriptive name **NRS_SigR** and click on the **Finish** button.



The **NRS_SigR** is configured to allow the Avaya SBCE to accept inbound and outbound call requests from the CS1000.

Being cloned from the Signaling Rule **default**, the **NRS_SigR** blocks all requests with 403 Forbidden. To start accepting calls, select **NRS_SigR** then go to **General** tab, click on **Edit** (not shown) then change **Inbound-Requests** and **Outbound-Requests** to **Allow**. **Content-Type Policy** is also configured to allow Multipart Content-Type from the CS1000 as shown in the screen shot on the next page.



Under **Signaling QoS** tab, select proper values for Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in header of IP packets with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance testing.

6.3.4. Endpoint Policy Groups

The rules created within the **Domain Policy** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section**.**

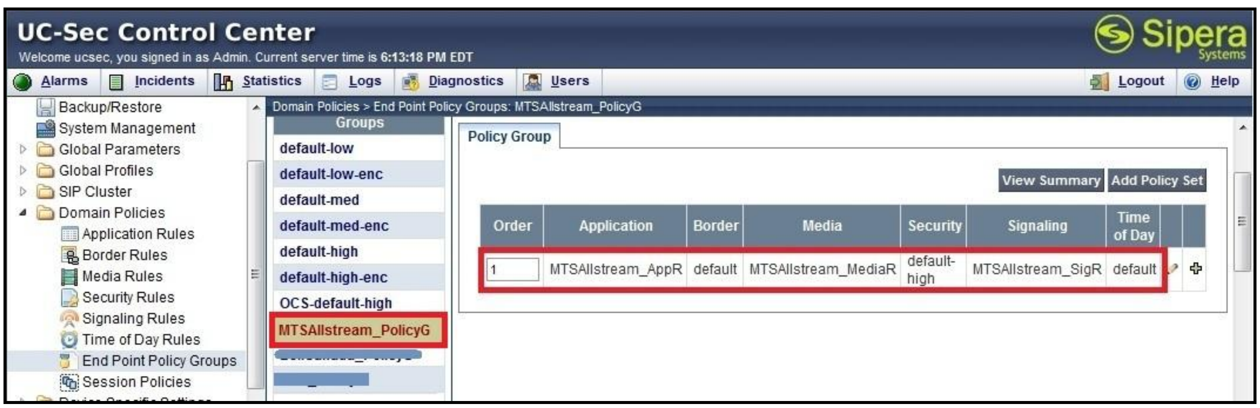
Endpoint Policy Groups are created for MTS Allstream and the NRS.

To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on the **Add Group** button (not shown)**.**

6.3.4.1 Endpoint Policy Group for MTS Allstream

The following screen shows **MTSAllstream_PolicyG** created for MTS Allstream.

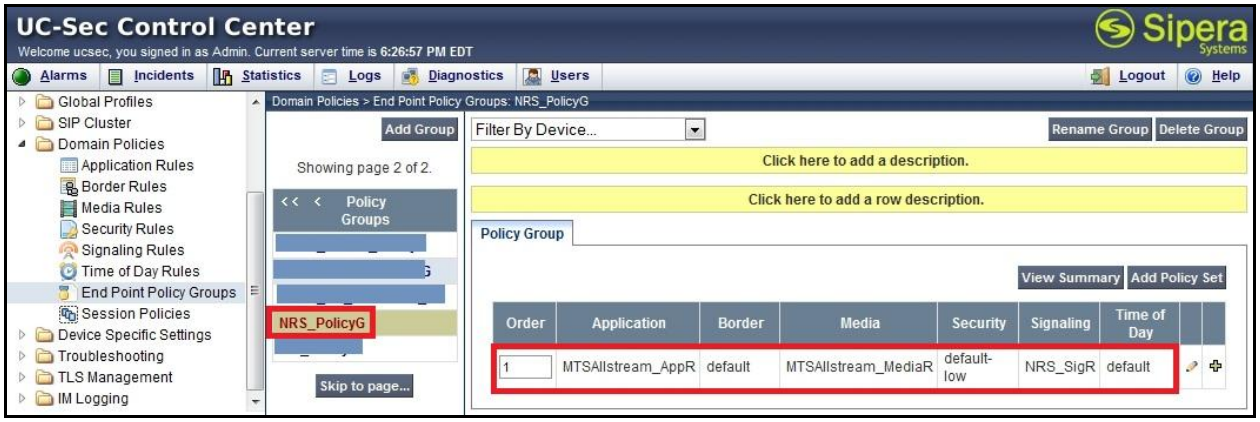
- Select Application Rule created in **Section 6.3.1**
- Select Media Rule created in **Section 6.3.2**
- Select Signaling Rule **MTSAllstream_SigR** created in **Section 6.3.3.1**
- Select Border Rule and Time of Day Rule to **default**.
- Select Security Rule to **default-high**.



6.3.4.2 Endpoint Policy Group for the NRS

The following screen shows **NRS_PolicyG** created for the NRS.

- Select Application Rule created in **Section 6.3.1**
- Select Media Rule created in **Section 6.3.2**
- Select Signaling Rule **NRS_SigR** created in **Section 6.3.3.2**
- Select the Border Rule and Time of Day Rule to **default**
- Select the Security Rule to **default-low**



6.3.5. Session Policy

Session Policy is applied based on the source and destination of a media session i.e., which codec is to be applied to the media session between its source and destination. The source and destination are defined in URI Group in **Section 6.2.1**.

In the compliance testing, the Session Policy named **MTSAllstream** was created to match the codec configuration of MTS Allstream. The policy also allows the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.

To clone a **Session Policy**, navigate to **UC-Sec Control Center → Domain Policies e→ Session Policies** select the **default** rule then click on the **Clone Rule** button (not shown).

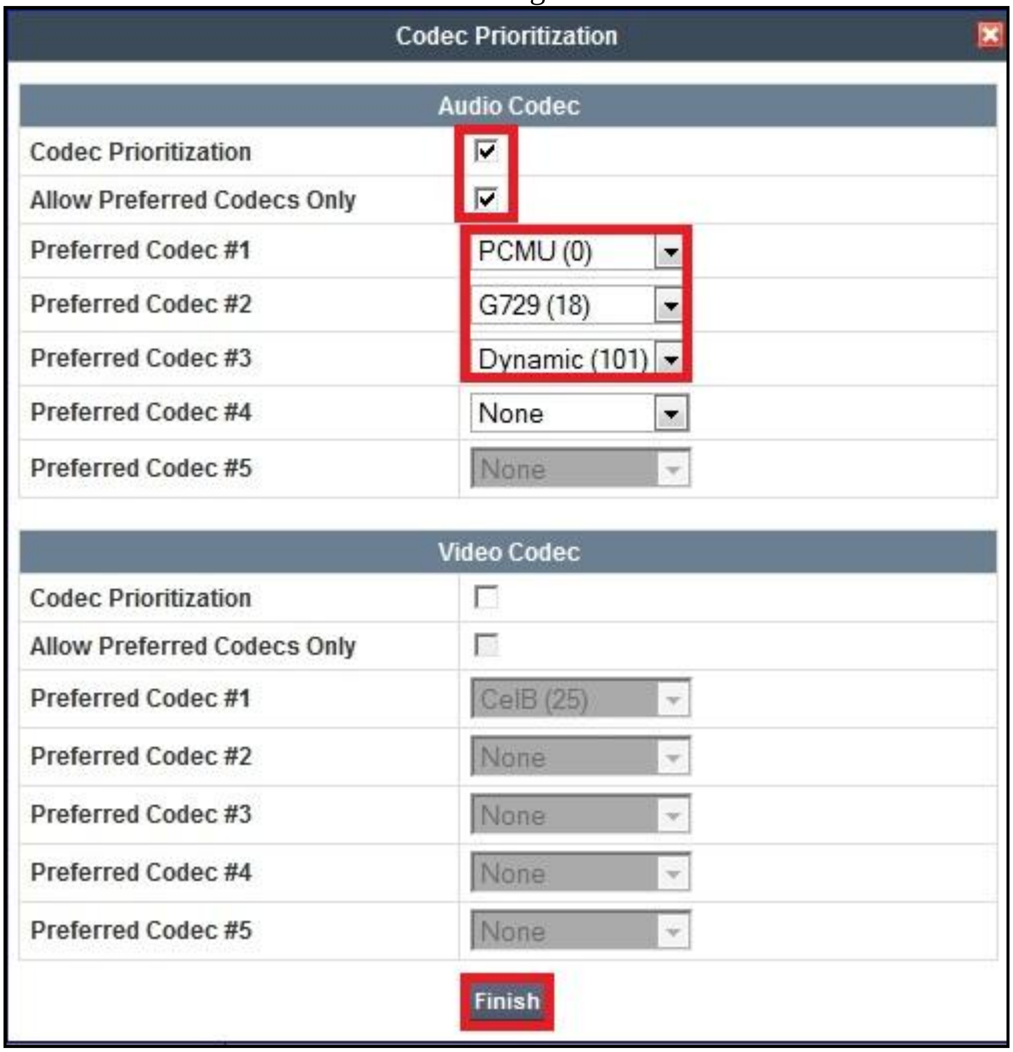
Enter a descriptive name **MTSAllstream** for the new policy and click on the **Finish** button.

MTS Allstream supports voice codec G.729 and G.711MU in prioritized order with payload 101 for RFC2833/ DTMF. To define **Codec Prioritization** for Audio Codec, select the profile **MTSAllstream** created above, click on **Edit** (not shown). Select **Preferred Codec #1** as G.711MU, **Preferred Codec #2** as G.729 and **Preferred Codec #3** as Dynamic (101) for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent the unsupported codec from being sent to both ends.

Notes:

- The T.38 fax is not yet supported by MTS Allsteream SIP trunking Service.

- The Session Policy prioritizes voice codec G.711MU to establish the voice call. It is mandatory for a G.711MU fax call to be successful because both the CS1000 and MTS Allstream cannot switch the voice call using different codec to G.711MU for fax.



To enable Media Anchoring on the Avaya SBCE, select Session Policy **MTSAllstream** created above then select tab **Media**, click on the **Edit** button (not shown). Check on **Media Anchoring**.

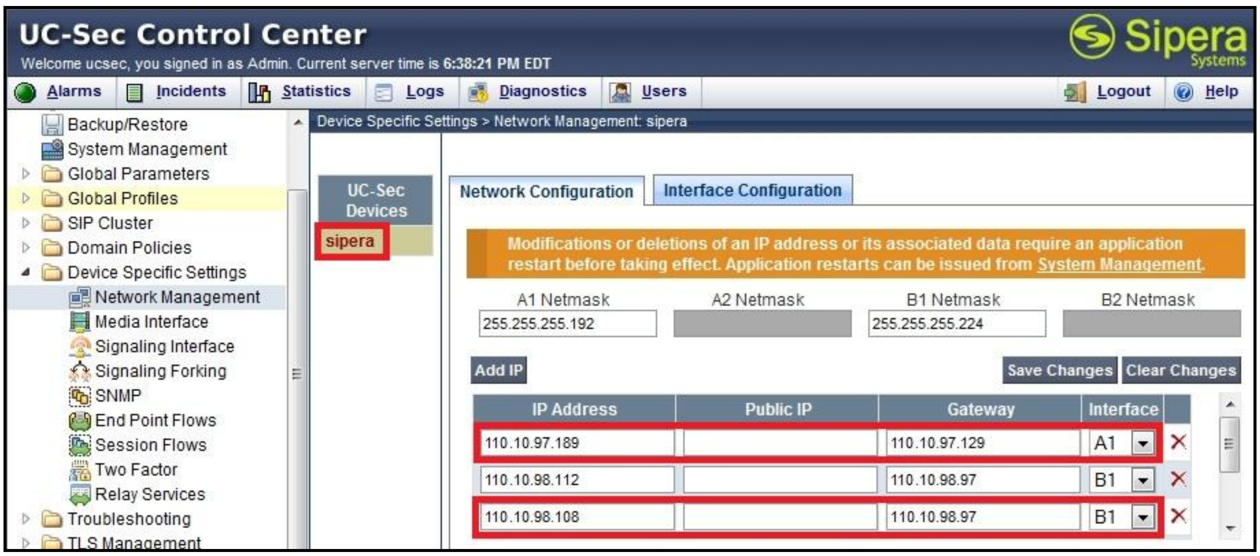
6.4. Device Specific Settings

Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network.

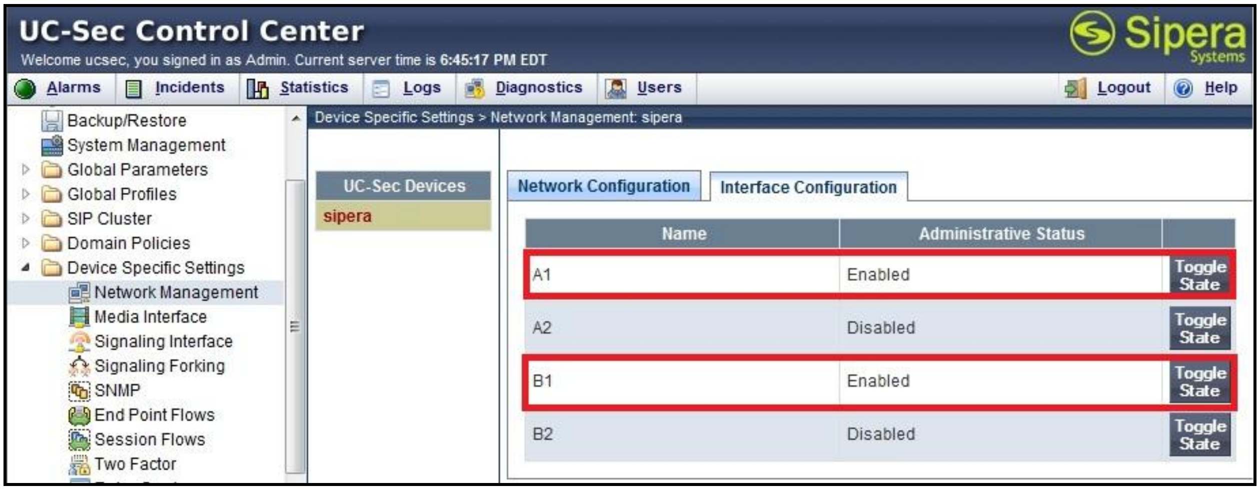
6.4.1. Network Management

Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP addresses, public IP addresses, Netmask, gateway, etc. to interface the device to the network. This information populates the various **Network Management** tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and under **Network Configuration** tab verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.



Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click it's **Toggle State** button.

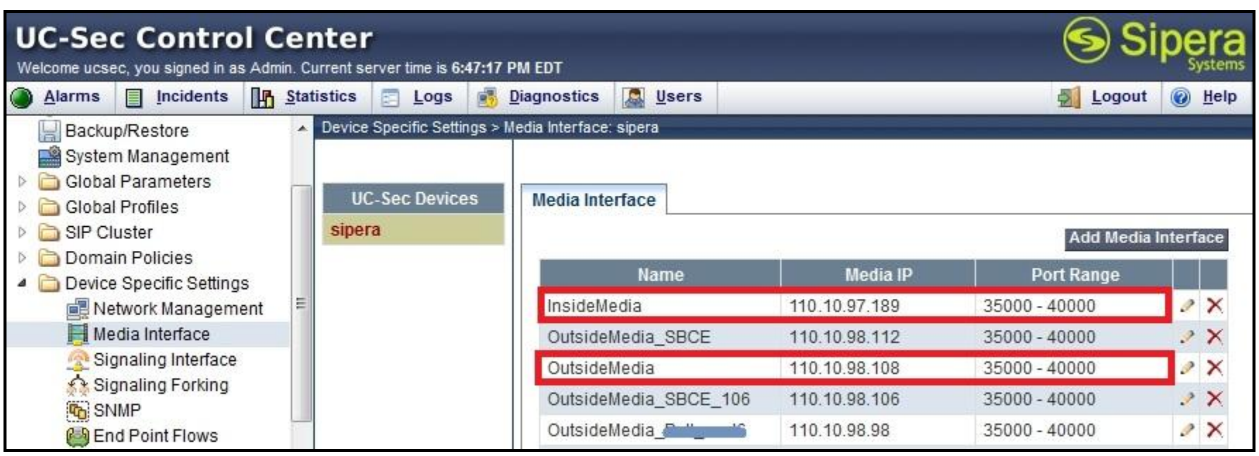


6.4.2. Media Interface

The **Media Interface** screen is where the media ports are defined. The Avaya SBCE will open connection for RTP on the defined ports.

To create a new **Media Interface**, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface** (not shown).

Media Interfaces are created for both the inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.



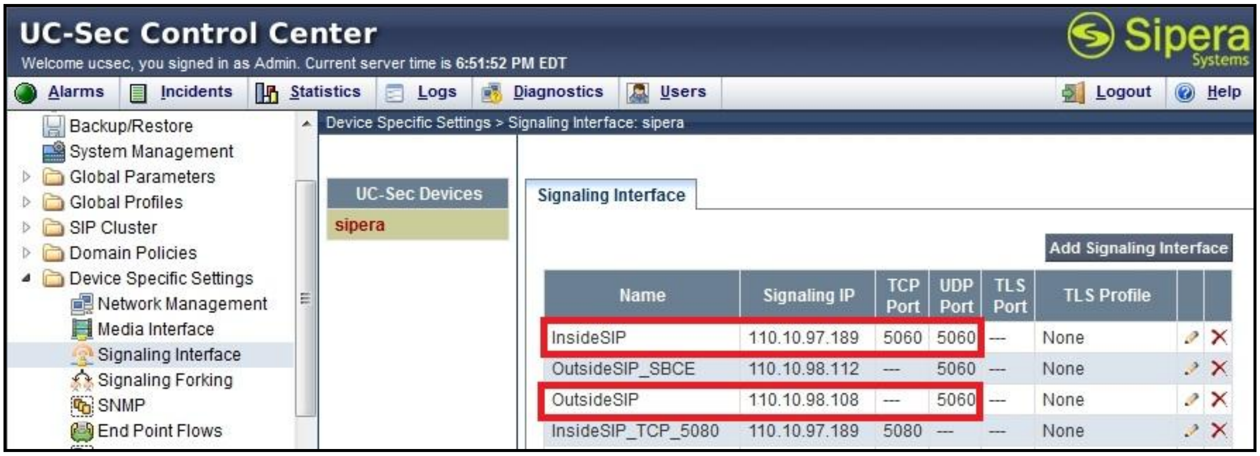
Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.

6.4.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

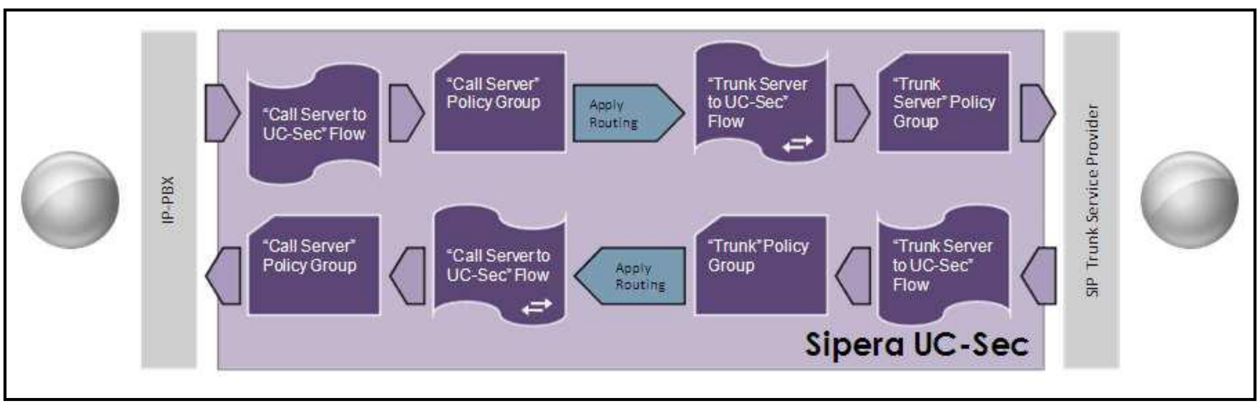
To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific → Settings → Signaling Interface** and click on the **Add Signaling Interface** button (not shown).

Signaling Interface is created for both inside and outside interfaces. The following screen shows the Signaling Interfaces created in the compliance testing with TCP/5060 and UDP/5060 used respectively for the inside and outside IP interface.



6.4.4. End Point Flows - Server Flow

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP trunk call.

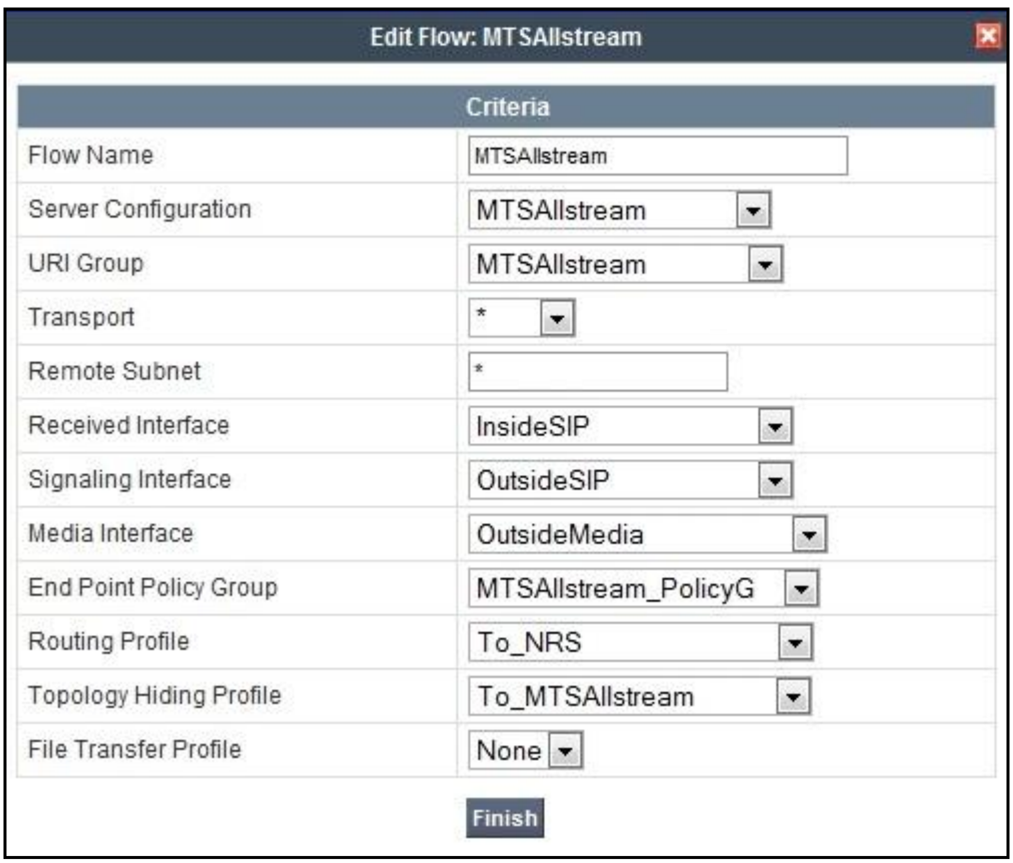


In the compliance testing, separate Server Flow was created for MTS Allstream and the NRS. To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown). In the pop up window, enter the following values.

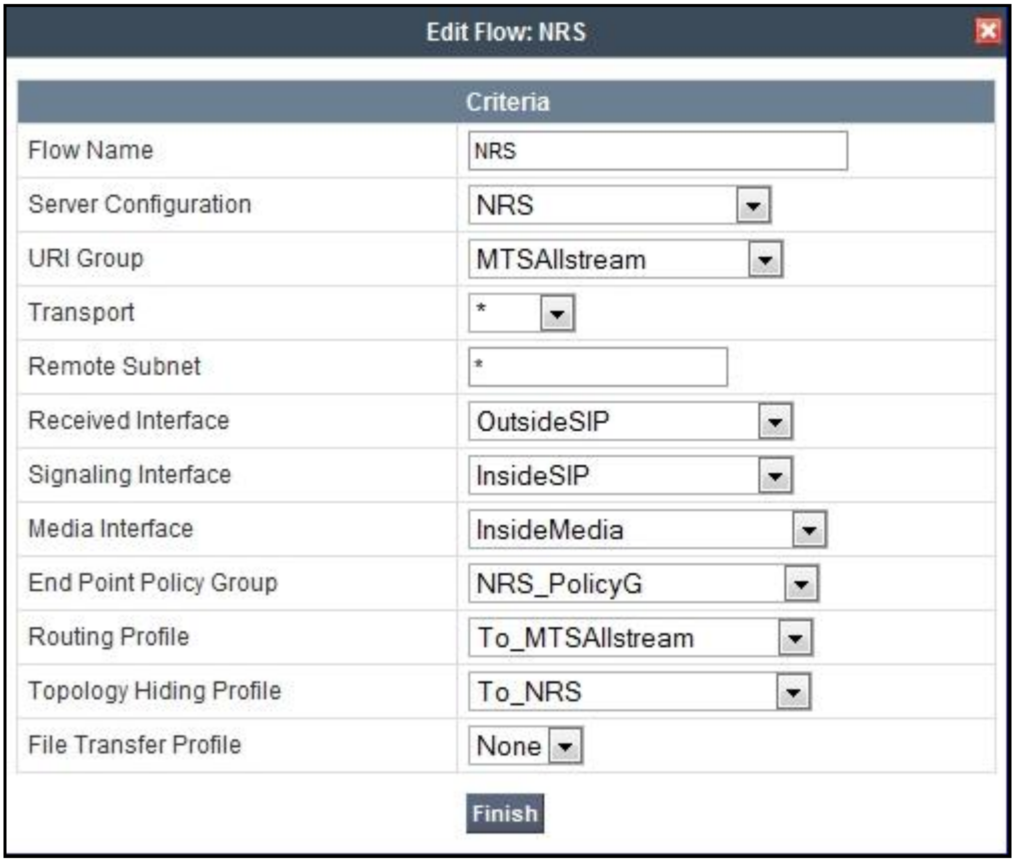
- **Flow Name**: Enter a descriptive name.

• **Server Configuration**: Select a Server Configuration created in **Section 6.2.6**.
• **URI Group**: Select the URI Group created in **Section 6.2.1**.
• **Received Interface**: Select a Signaling Interface created in **Section 6.4.3**, on which SIP traffic enters to the server flow.
• **Signaling Interface**: Select a Signaling Interface created in **Section 6.4.3**, on which SIP traffic exits from the server flow.
• **Media Interface**: Select a Media Interface created in **Section 6.4.2**, on which RTP traffic exits from the server flow.
• **End Point Policy Group**: Select an associate End Point Policy Group created in **Section 6.3.4**.
• **Routing Profile**: Select an associate Routing Profile created in **Section 6.2.2** to determine the destination of the SIP traffic.
• **Topology Hiding Profile**: Select an associate Topology-Hiding profile created in **Section 6.2.3** to apply masking to required SIP headers.
• Click on the **Finish** button.

The following screen shows the Server Flow **MTSAllstream** configured for MTS Allstream.



The following screen shows the Server Flow **NRS** configured for the NRS.



6.4.5. Session Flows

Session Flows feature allows defining certain parameters that pertain to the media portions of a call, whether it originates from the enterprise or outside the enterprise. This feature provides the complete and unparalleled flexibility to monitor, identify and control very specific types of calls based upon these user-definable parameters. Session Flows profiles SDP media parameters, to completely identify and characterize a call placed through the network.

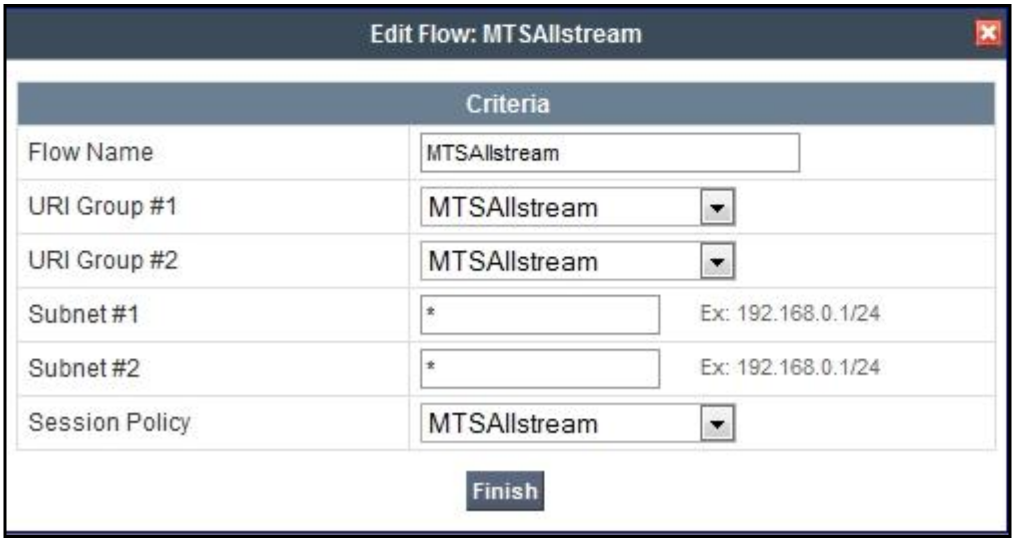
To create a session flow, navigate to **UC-Sec Control Center → Device Specific Settings → Session Flows** and click on the **Add Flow** button (not shown).

A common Session Flow is created for both MTS Allstream and the NRS. In the pop up window, enter the following values.

- **Flow Name**: Enter a descriptive name
- **URI Group #1**: Select the URI Group created in **Section 6.2.1** for the Session Flow as the source URI Group
- **URI Group #2**: Select the URI Group created in **Section 6.2.1** for the Session Flow as the destination URI Group
- **Session Policy**: Select the Session Policy created in **Section 6.3.5** for the Session Flow
- Click on the **Finish** button.

Note: A unique **URI Group** is used for source and destination as it contains multiple URIs defined for the source as well as for the destination.

The following screen shows the Session Flow named **MTSAllstream** is created.



7. MTS Allstream SIP Trunking Service Configuration

MTS Allstream is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at enterprise side. MTS Allstream will provide the customer with the necessary information to configure the SIP connection from enterprise to the MTS Allstream. The information provided by MTS Allstream includes:

- IP address of the MTS Allstream Session Border Controller
- MTS Allstream SIP domain. In the compliance testing, MTS Allstream preferred to use IP address as a URI-Host
- Enterprise SIP domain. In the compliance testing, MTS Allstream preferred to use IP address of the Avaya SBCE as a URI-Host
- Supported codecs
- DID numbers
- IP addresses and port range for media traffic

The sample configuration for the SIP trunk between MTS Allstream and the CS1000 uses static IP address. There is no SIP registration is implemented.

8. Verification and Troubleshooting

8.1. Verification Steps

The following activities are made to each test scenario.

1. Calls are checked for the correct call progress tones and cadences.
2. During the ringing state, the ring back tone and destination ringing are checked.
3. Calls are checked in both hands-free and handset mode due to internal Avaya requirement.
4. Calls are checked for speech path in both directions using spoken words to ensure clarity of speech.
5. The display(s) of the sets/clients involved are checked for consistent and expected calling party name and number and redirection information both prior to answer and after call establishment.
6. The speech path and messaging system are observed for timely and quality End to End tone audio path generation and application responses.
7. The call server maintenance terminal window is used for the monitoring of BUG(s), ERR and AUD messages.
8. Speech path and display checked before and after calls are put on/off hold from each end.
9. Applicable files are screened on an hourly basis during the testing for messages that may indicate technical issues. This refers to Avaya PBX files.
10. Calls are checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs are released when a call scenario ends.

8.2. Protocol Traces

The following SIP headers are inspected using sniffer traces:

- Request-URI: Verify the request number and SIP domain
- From: Verify the display name and display number
- To: Verify the display name and display number
- P-Asserted-Identity: Verify the display name and display number
- Privacy: Verify privacy masking with “user, id”
- Diversion: Verify DID number
- Authorization: Verify Digest Authentication implementation

The following attributes in the SIP message body are inspected using sniffer traces:

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

8.3. Troubleshooting

8.3.1. The Avaya SBCE

Using a network sniffing tool (e.g., WireShark) to monitor the SIP signaling messages between MTS Allstream and the Avaya SBCE.

Following is an example inbound call from MTS Allstream to the enterprise.

- Inbound INVITE request from MTS Allstream:

```
INVITE sip:6477761226@110.10.98.108;user=phone SIP/2.0
Max-Forwards: 139
Session-Expires: 3600;refresher=uac
Min-SE: 600
Supported: timer, 100rel
To: <sip:6477761226@110.10.98.108;user=phone>
From: "Bell Demo12345" <sip:4167751882@220.20.2.12>;tag=3552660863-170682
Call-ID: 22103-3552660863-170674@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Allow: CANCEL, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bKdc0152a612ccddb5f6d6a0289b4dc233
Contact: <sip:4167751882@220.20.2.12:5060;tgrp=TOROONSBCIOT1>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 512559100 512559100 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 16840 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
```

- 200OK/SDP response by the enterprise:

```
SIP/2.0 200 OK
From: "Bell Demo12345" <sip:4167751882@220.20.2.12>;tag=3552660863-170682
To: <sip:6477761226@110.10.98.108;user=phone>;tag=5d3a368-be610a87-13c4-55013-
1a6de2-4bea57da-1a6de2
CSeq: 1 INVITE
Call-ID: 22103-3552660863-170674@nextone-msw-lab-3.mtsallstream.com
Contact: <sip:6477761226@110.10.98.108:5060;transport=udp;user=phone>
Record-Route: <sip:110.10.98.108:5060;ipcs-line=3521;lr;transport=udp>
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO,
SUBSCRIBE, UPDATE
Supported: 100rel,x-nortel-sipvc,replaces
User-agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bKdc0152a612ccddb5f6d6a0289b4dc233
Require: timer
Privacy: none
P-Asserted-Identity: "MTS x1226" <sip:6477761226@110.10.98.108;user=phone>
Content-Type: application/sdp
Content-Length: 252
```

```
v=0
o=- 37 1 IN IP4 110.10.98.108
s=-
c=IN IP4 110.10.98.108
t=0 0
m=audio 35014 RTP/AVP 0 101 111
c=IN IP4 110.10.98.108
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=maxptime:20
a=sendrecv
```

Following is an example outbound call from the enterprise to MTS Allstream.

- Outbound INVITE request from the enterprise:

```
INVITE sip:1112916139675258@220.20.2.12;user=phone SIP/2.0
From: "MTS x1226" <sip:6477761226@110.10.98.108;user=phone>;tag=5d551e8-be610a87-
13c4-55013-1a7d33-2828d1fb-1a7d33
To: <sip:1112916139675258@220.20.2.12;user=phone>
CSeq: 1 INVITE
Call-ID: 0a343f1f5d80e50d78424333bc533f1f
Contact: <sip:6477761226@110.10.98.108:5060;transport=udp;user=phone>
Record-Route: <sip:110.10.98.108:5060;ipcs-line=4867;lr;transport=udp>
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO,
SUBSCRIBE, UPDATE
Supported: 100rel,x-nortel-sipvc,replaces
User-agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
Max-Forwards: 68
Via: SIP/2.0/UDP 110.10.98.108:5060;branch=z9hG4bK-s1632-001920367336-1--s1632-
Privacy: none
P-Asserted-Identity: "MTS x1226" <sip:6477761226@110.10.98.108;user=phone>
Content-Type: multipart/mixed ;boundary=unique-boundary-1
Content-Length: 921

--unique-boundary-1
Content-Type: application/sdp

v=0
o=- 51 1 IN IP4 110.10.98.108
s=-
c=IN IP4 110.10.98.108
t=0 0
m=audio 35032 RTP/AVP 0 18 101
c=IN IP4 110.10.98.108
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv

--unique-boundary-1
Content-Type: application/x-nt-mcdn-frag-hex;version=ssLinux-7.50.17;base=x2611
Content-Disposition: signal;handling=optional

0500a201
0107130081900000a200
09090f00e9a0830001002200
```

```
131e070011fd1800a1160201010201a1300e8102010582010184020000850104
1315070011fa0f00a10d02010102020100cc0400005b8400
1e0403008183
460e01000a00010004000a0000000000
4a1c010018000100000000000000004677670000000500000000000021620000

--unique-boundary-1
Content-Type: application/x-nt-epid-frag-hex;version=ssLinux-7.50.17;base=x2611
Content-Disposition: signal;handling=optional

011201
00:1a:64:20:2b:c8

--unique-boundary-1--
```

- 200OK/SDP response by MTS Allstream:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 110.10.98.108:5060;received=110.10.98.108;branch=z9hG4bK-s1632-
001920367336-1--s1632-
Record-Route: <sip:110.10.98.108:5060;ipcs-line=4867;lr;transport=udp>
To: <sip:1112916139675258@220.20.2.12;user=phone>;tag=3552664786-110918
From: "MTS x1226" <sip:6477761226@110.10.98.108;user=phone>;tag=5d551e8-be610a87-
13c4-55013-1a7d33-2828d1fb-1a7d33
Call-ID: 0a343f1f5d80e50d78424333bc533f1f
CSeq: 1 INVITE
Allow: CANCEL, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:1112916139675258@220.20.2.12:5060>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 551784282 551784282 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 16904 RTP/AVP 0 18 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
    a=fmtp:101 0-15
```

8.3.2. The CS1000 Verification Steps

8.3.2.1 Verify Patch Installation

Verify that the patches mentioned in **Section 4**, **Table 1** are properly installed on the CS1000.

Following screen shows the output of “dstat” command on Call Server. This command can be issued in “pdt” mode. To log into “pdt” mode, from the Call Server CLI as shown in **Section 5.1.2**, enter combination keys of Ctrl + pdt

```
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 :  2012-07-16 17:52:47 (est)
        Number of patches: 246
        Patches Loaded: 246
        Patches In-service: 246
pdt>
```

Following screen shows the output of “spstat” command on SSG Server. This command can be issued in SSH session of the SSG Server.

```
[admin@car2-mas ~]$ spstat
There is no SP in loaded status.
The last applied SP: Service_Pack_Linux_7.50_17_20120713.ntl
It is a STANDARD SP.
Has been applied by user nortel on Sun Aug  5 18:02:20 2012.
spins command completed with no errors detected.
```

8.3.2.2 Active Call Trace (LD 80)

The following is an example of one of the commands available on the CS1000 to trace the DN when the call is in progress. The call scenario involved the PSTN phone number 6139675258 calling 6477761230 on the 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
TRA000
.trac 4 1230

NON ACTIVE  VTN 108 0 00 31

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: 110.10.97.189
  FAR-END MEDIA ENDPOINT IP: 110.10.97.189  PORT: 35648
  FAR-END VendorID: Not available
TERM   VTN 108 0 00 18  KEY 0  SCR MARP  CUST 4  DN 1230  TYPE 2007
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 110.10.98.62  PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 1230
MAIN_PM  ESTD
TALKSLOT  ORIG  94   TERM  35
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 34898
```

```
----  ISDN ISL CALL (ORIG) ----
CALL REF # =  387
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  16139675258  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
CALLED NO  =  6477761230  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
```

Following is an example after the call on 1205 is completed.

```
.trac 4 1230

IDLE VTN 108 0 00 18   MARP
```

8.3.2.3 SIP Trunk Monitoring (LD 32)

Place an inbound call from PSTN (6139675258) to the CS1000 (6477761230). 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
```

Following is an 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
```

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000 7.5 and Avaya Session Border Controller for Enterprise 4.0.5 to MTS Allstream SIP Trunking Service. MTS Allstream SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large the enterprises. MTS Allstream SIP Trunking Service provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The MTS Allstream SIP Trunking Service is considered **compliant** with Avaya Communication Server 1000 7.5 and Avaya Session Border Controller for Enterprise 4.0.5.

10. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[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.
[7] *Administering Avaya one-X® Communicator*, April 2011.
[8] *Using Avaya one-X® Communicator*, April 2011.
[9] *UC-Sec Install Guide (*102-5224-400v1.01*)*
[10] *UC-Sec Administration Guide (*010-5423-400v106*)*
[11] *RFC3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[12] *RFC2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,* http://www.ietf.org/

Product documentation for MTS Allstream SIP Trunking Service is available from MTS Allstream.

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.