Avaya Solution & Interoperability Test Lab

Application Notes for Configuring CenturyLink SIP Trunk service with Avaya Communication Server 1000E Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring CenturyLink SIP Trunk service with Avaya Communication Server 1000E Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.2.

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

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

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

Table of Contents

1. Introduction

These Application Notes provide the procedure for configuring CenturyLink SIP Trunk service with Avaya Communication Server 1000E Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.2. During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure the interoperability between CenturyLink and Avaya Communication Server 1000E.

In the sample configuration, the Avaya solution consists of a Communication Server 1000E Rel. 7.6 (hereafter referred to as CS1000), Avaya Session Border Controller for Enterprise Rel. 6.2 (hereafter referred to as the Avaya SBCE), and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya SBCE.

2. General Test Approach and Test Results

The CS1000 system was connected to the Avaya SBCE via the Local Area Network (LAN). The Avaya SBCE was connected to CenturyLink's network via the public internet. Various call types were made from the CS1000 to CenturyLink and vice versa to verify interoperability between the CS1000 and CenturyLink.

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

2.1. Interoperability Compliance Testing

The focus of this test was to verify that the CS1000 can interoperate with CenturyLink. The following interoperability areas were covered:

- Incoming calls from the PSTN were routed to DID numbers assigned by CenturyLink. Incoming PSTN calls were terminated to the following Avaya Endpoints: Avaya 1100 Series IP Telephones (SIP), Avaya 1100 Series IP Telephones (UniStim), Avaya M3904 Digital Telephones, Avaya 2050 IP Softphone, Analog Telephones and Fax machines.
- Outgoing calls to the PSTN were routed via CenturyLink's network.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect during normal active call termination by the caller or the callee.
- Proper disconnect by the network for calls that are not answered (with voice mail off).
- Proper response when calling busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codec G.711 u-law/20ms, G.711 a-law/20ms and G.729/20ms with Voice Activity Detection (VAD) disabled.
- Voice mail and DTMF tone support in both directions (RFC2833) (Leaving voice mail, retrieving voice mail, etc.).
- Call Pilot Voice Mail Server (Hosted in the CS1000).

- Outbound Toll-Free calls to Interactive Voice Response systems (IVR).
- Inbound Toll-Free.
- Local Calls and long distance calls.
- Operator assisted calls (0 and 0+10).
- Emergency calls (911).
- Directory Assistance calls (411).
- Calling number and calling name blocking (Privacy).
- Call Hold/Resume.
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Call Park.
- Consultative Call transfers.
- Station Conference.
- T.38 fax support.
- G.711u fax pass-through support.
- Long duration calls (one hour).
- Early Media transmission.

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunk Service with the CS1000 solution was completed successfully with the following observations/limitations.

- **Caller-ID on re-directed calls to PSTN:** Caller ID works properly between the CS1000 and CenturyLink when there is no call re-direction involved. However, when calls are re-directed to the PSTN at the CS1000 extension, the Caller ID will not properly reflect the true originator of the call. If a call is re-directed at the CS1000 to a PSTN extension, the Caller ID displayed at the PSTN extension will be of the extension doing the re-direction (i.e., transferee) and not the Caller ID of the extension that originated the call. The CS1000 is not sending UPDATE or re-INVITE to update the true connected Calling Party. This is a CS1000 known issue.
- **CS1000 phone holds/retrieves an outbound call**: If a CS1000 phone holds/retrieves an outbound call, the dialed digits are no longer displayed; instead the access code of the trunk route (ACOD) is displayed. Also, the trunk route (ACOD), instead of the Caller ID of the extension that originated the call, is displayed during some call transfer scenarios. These are CS1000 known issues.
- **PSTN to CS1000 calls with Privacy enabled:** Calls from the PSTN to the CS1000 with Privacy enabled (Calling Party Name/Number Block) will display the access code of the trunk route (ACOD) instead of **Anonymous**. This is a CS1000 known issue.
- **Conversion of History-Info to Diversion Header:** CenturyLink supports Diversion Header for call re-direction, Signaling Manipulation rules (SigMa script) were added to the Avaya SBCE to convert History-Info messages sent by the CS1000 to Diversion Header. Refer to **Section 6.2.6**.
- **SIP Header Optimization:** SIP header rules were implemented in the Avaya SBCE to streamline the SIP header and remove any unnecessary parts. The following headers were

removed: X_nt_e164_clid, Alert-Info if they were present in the INVITE. Also the multipart MIME SDP, which included the x-nt-mcdn-frag-hex, x-nt-esn5-frag-hex, and x-nt-epid-frag were stripped out. These particular headers and MIME have no real use in the service provider network. If an issue is being investigated on the service provider network, the presence of these headers may add unnecessary confusion.

- Items not supported or not tested included the following:
    - International calls were not tested.

2.3. Support

For support on CenturyLink systems, visit the corporate web page at:
http://www.CenturyLink.com/

3. Reference Configuration

Figure 1 below illustrates the test configuration used. The test configuration simulates an enterprise site with the Avaya components connected to CenturyLink SIP Trunk Service through the Public Internet.

The Avaya components used to create the simulated customer site included:

- Avaya Communication Server 1000E (CS1000E).
- DELL R210 V2 Server running Avaya Session Border Controller for Enterprise.
- Avaya 1100-Series IP Deskphones (UniStim).
- Avaya 1100-Series Deskphones (SIP).
- 2050 Avaya IP Softphone.
- Avaya M3904 Digital Deskphones.
- Analog Deskphones.
- Fax machines.
- Desktop with administration interfaces.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any 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 CenturyLink across the public IP network is UDP. The transport protocol between the Avaya SBCE and the CS1000 across the enterprise IP network is UDP.

For security reasons, any actual public IP addresses used in the configuration have been masked. Similarly, any references to real routable DIDs and PSTN numbers have also been masked to numbers that cannot be routed by the PSTN.

For inbound calls, the calls flowed from CenturyLink to the Avaya SBCE, then to the CS1000. Once the call arrived at the CS1000, incoming call treatment, such as incoming digit translations and class of service restrictions were performed. Outbound calls to the PSTN were first processed by the CS1000 for outbound treatment through the Electronic Switched Network and class of service restrictions. Once the CS1000 selected the proper SIP trunk; the call was routed to the Avaya SBCE for egress to CenturyLink.

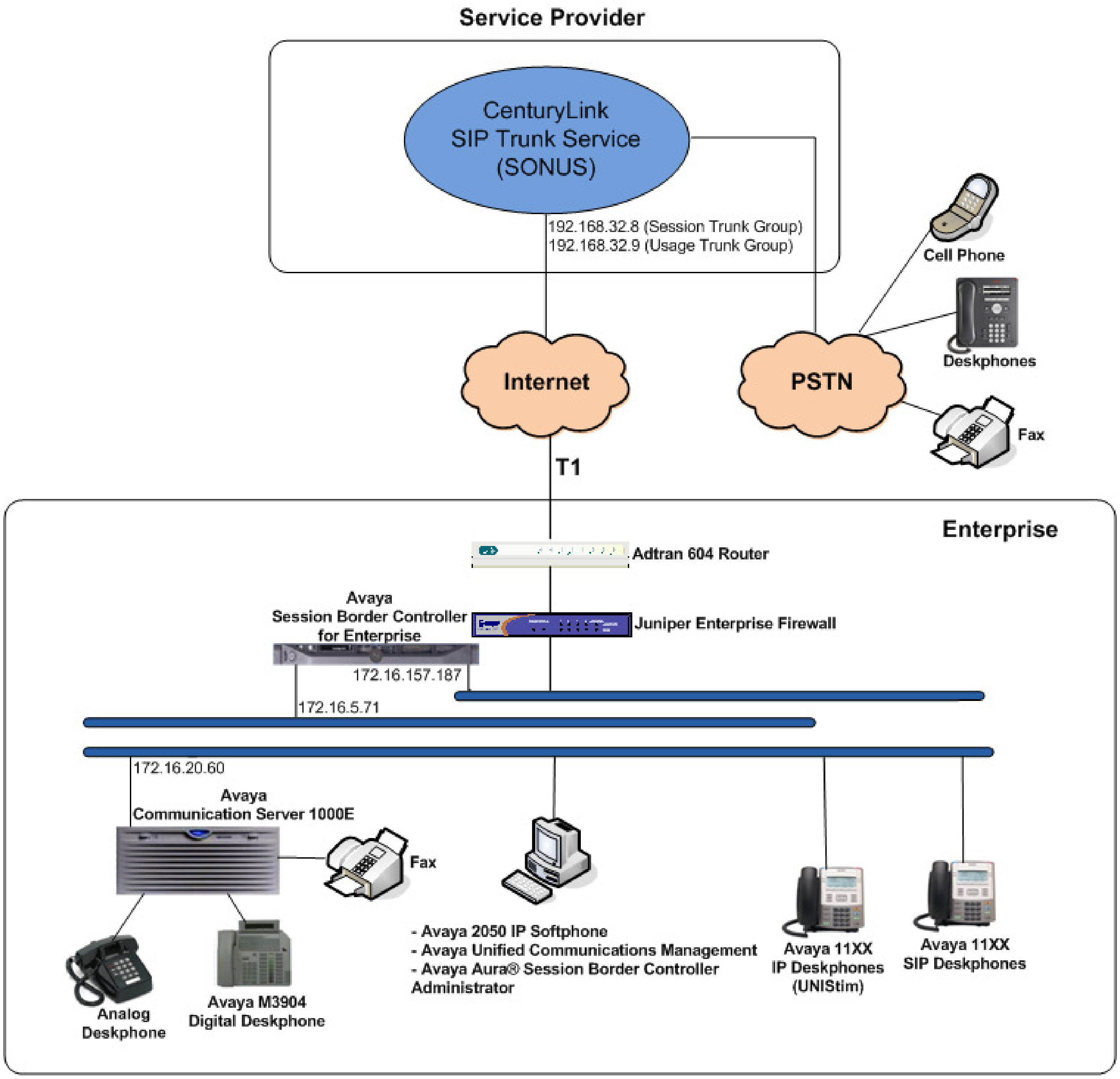


Figure 1: CenturyLink SIP Trunk service with Avaya CS1000E

4. Equipment and Software Validated

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

Avaya:	
Equipment	**Release/Version**
Avaya Communication Server 1000E running Co-resident Call Server, Signaling Server and Media Gateway in a single CP-MGS card.	RELEASE 7 ISSUE 65 P + DepList 1: core Issue: 01(created: 2013-05-28 04:19:50 (est)) Signaling Server: 7.65.16.00 **(Service Pack 2)** **See Service Updates & Patches below**
Avaya Call Pilot 202i	Call Pilot Manager Version: 05.00.41.156
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.0.Q48
Avaya Deskphones	1110: 0623C8G (UniStim) 1120: 0624C8G (UniStim) 1165: 0626C8G (UniStim) 1120: 04.01.15.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.4 Service Pack 1 (Build 067)
Lucent Analog Phone	N/A
Fax Machines	N/A
CenturyLink:	
Equipment	**Release/Version**
SONUS SBC9000	V07.03.07F017

Signaling Server Service Updates & Patches:

CS1000 Linux SU's included in Service Pack 2:
cs1000-linuxbase-7.65.16.21-04.i386.000
cs1000-patchWeb-7.65.16.21-04.i386.000
cs1000-dmWeb-7.65.16.21-01.i386.000|
cs1000-snmp-7.65.16.00-01.i686.000
cs1000-oam-logging-7.65.16.01-01.i386.000
cs1000-cs1000WebService_6-0-7.65.16.21-00.i386.000
cs1000-sps-7.65.16.21-01.i386.000
cs1000-pd-7.65.16.21-00.i386.000
cs1000-shared-carrdtct-7.65.16.21-01.i386.000
cs1000-shared-tpselect-7.65.16.21-01.i386.000
cs1000-emWebLocal_6-0-7.65.16.21-01.i386.000
cs1000-dbcom-7.65.16.21-00.i386.000
cs1000-csmWeb-7.65.16.21-05.i386.000
cs1000-shared-xmsg-7.65.16.21-00.i386.000
cs1000-vtrk-7.65.16.21-29.i386.000
cs1000-tps-7.65.16.21-05.i386.000
cs1000-mscAnnc-7.65.16.21-02.i386.001
cs1000-mscAttn-7.65.16.21-04.i386.001
cs1000-mscConf-7.65.16.21-02.i386.001
cs1000-mscMusc-7.65.16.21-02.i386.001
cs1000-mscTone-7.65.16.21-03.i386.001
cs1000-bcc-7.65.16.21-21.i386.000
cs1000-Jboss-Quantum-7.65.16.21-3.i386.000
cs1000-emWeb_6-0-7.65.16.21-06.i386.000
cs1000-cs-7.65.P.100-01.i386.001
####################
Patches:
####################

Loadware:

INSTALLED LOADWARE PEPS : 5

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME
00	wi01057886	ISS1:1OF1	DSP1AB07	09/08/2013	DSP1AB07.LW
01	wi01057886	ISS1:1OF1	DSP2AB07	09/08/2013	DSP2AB07.LW
02	wi01057886	ISS1:1OF1	DSP3AB07	09/08/2013	DSP3AB07.LW
03	wi01057886	ISS1:1OF1	DSP4AB07	09/08/2013	DSP4AB07.LW
04	wi01057886	ISS1:1OF1	DSP5AB07	09/08/2013	DSP5AB07.LW

5. Configure Avaya Communication Server 1000E

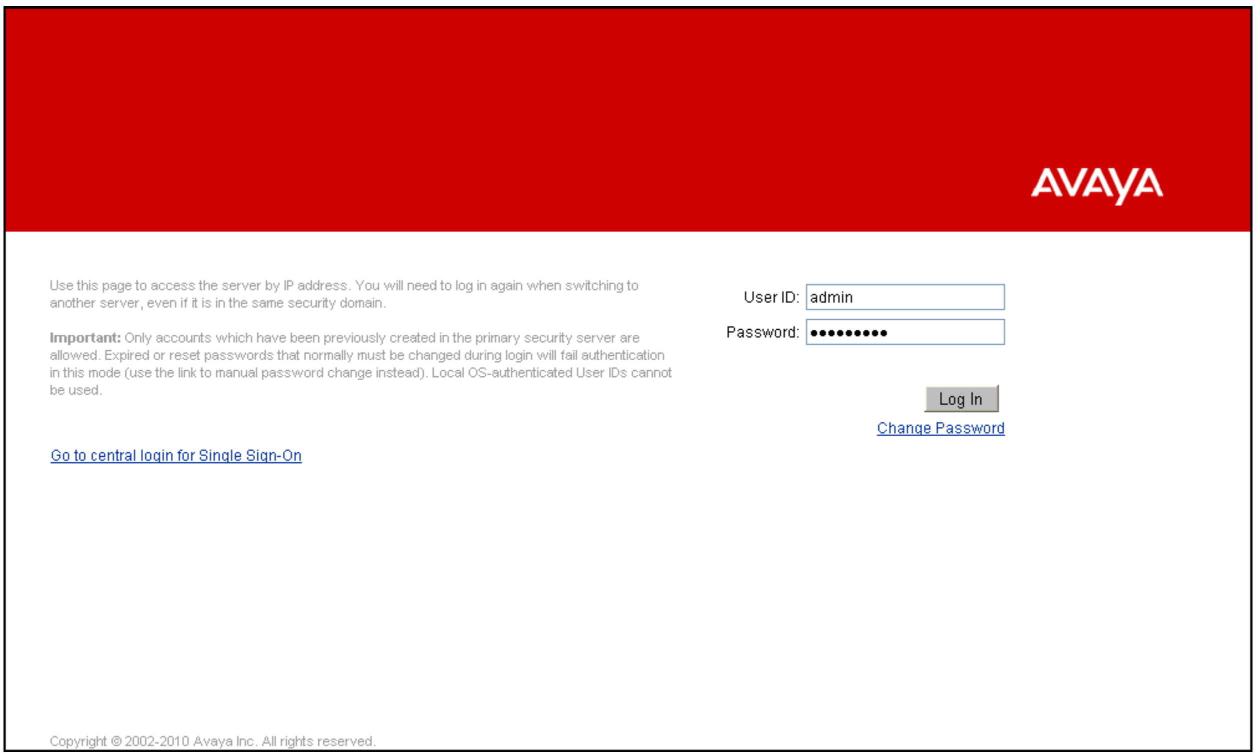
These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 10.**

The procedures shown below describe the configuration details of the CS1000 with SIP trunks to the CenturyLink's network.

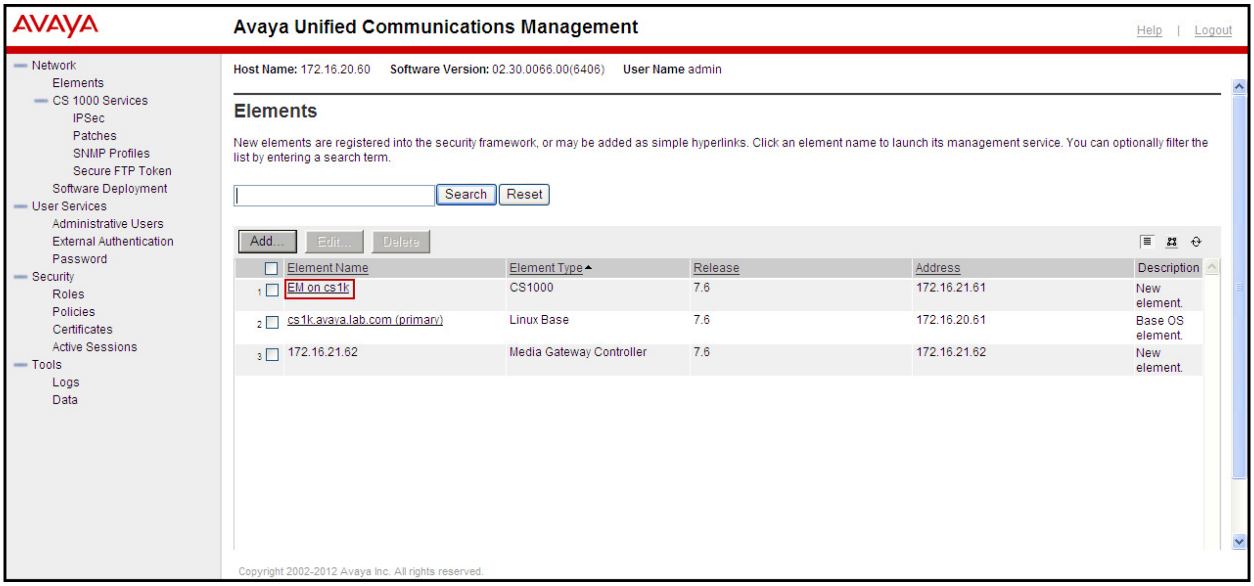
5.1. Login to the CS1000 System

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

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



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



The CS1000 Element Manager **System Overview** page is displayed as shown below.

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

Using Putty, login to the Signaling Server with the admin account. Run the command “cslogin” and “logi” with the appropriate admin account and password, as shown below.

```
login as: admin

               Avaya Inc. Linux Base  7.65
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.

admin@172.16.20.60's password:
Last login: Wed Aug 28 15:59:22 2013 from 172.16.5.250
[admin@cs1k ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without aut
hentica
ting

TTY 14 SCH MTC BUG OSN   10:44
OVL111 IDLE   0
>logi
USERID? admin
PASS?
.
TTY #14 LOGGED IN ADMIN 10:44  29/8/2
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.
013

>
```

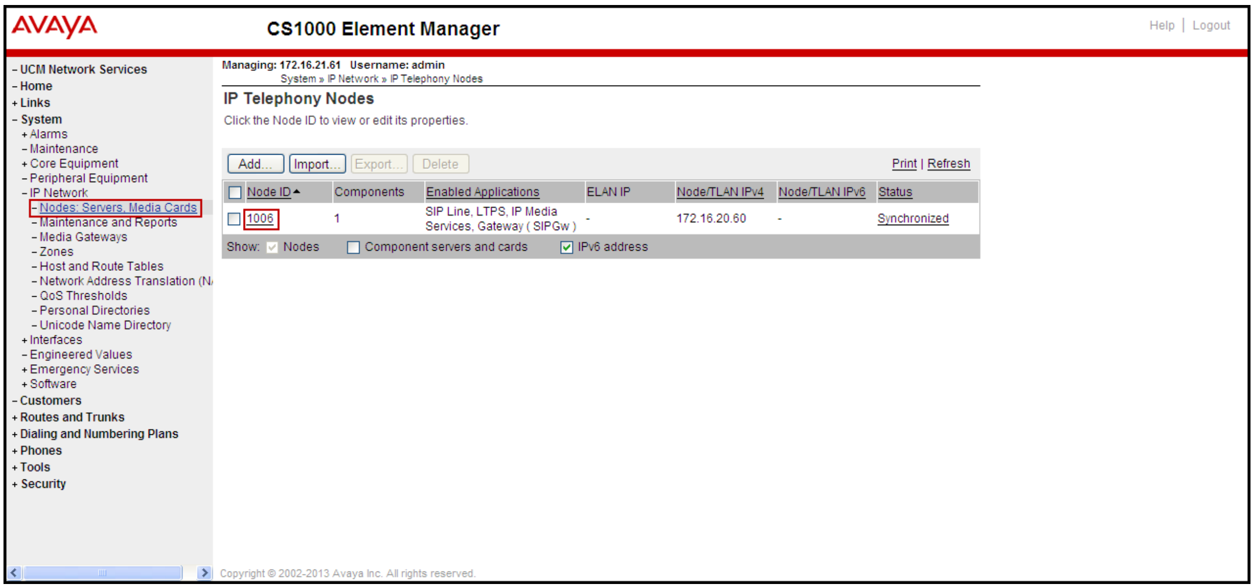
5.2. Administer an IP Telephony Node

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

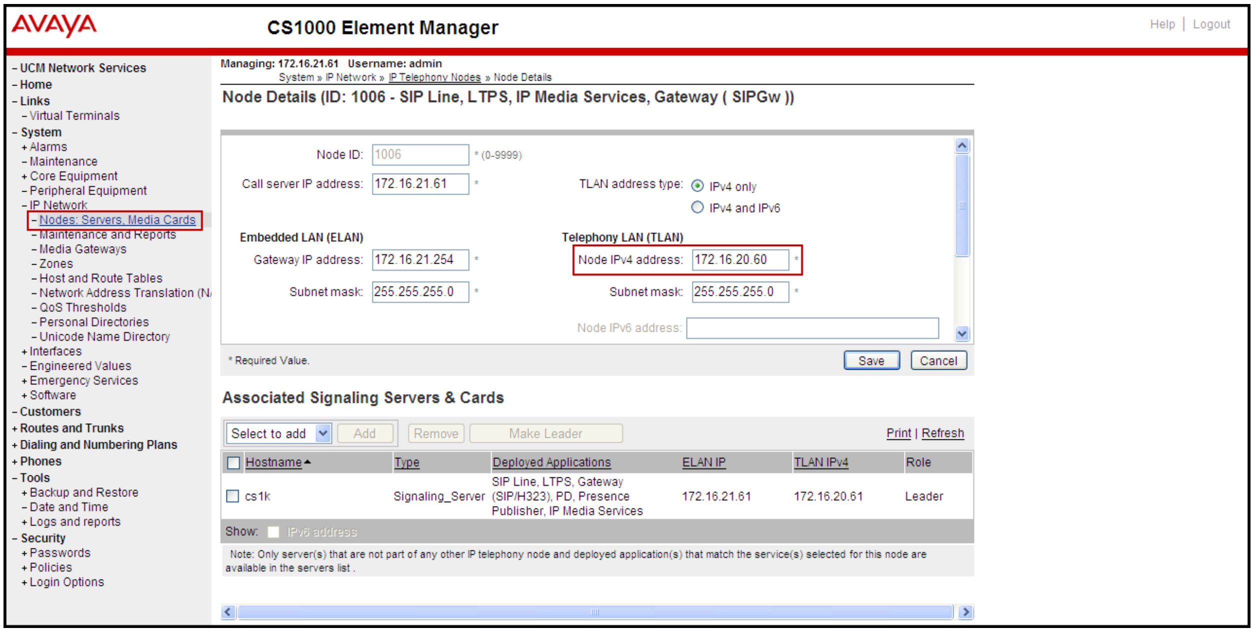
5.2.1. Obtain Node IP address

These Application Notes assume that the basic configuration has already been done and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 1006) in the CS1000 IP network to work with CenturyLink.

Select **System → IP Network → Nodes: Servers, Media Cards**. Following is the display of the **IP Telephony Nodes** page. Then click on the **Node ID** of the CS1000 Element (i.e., 1006).

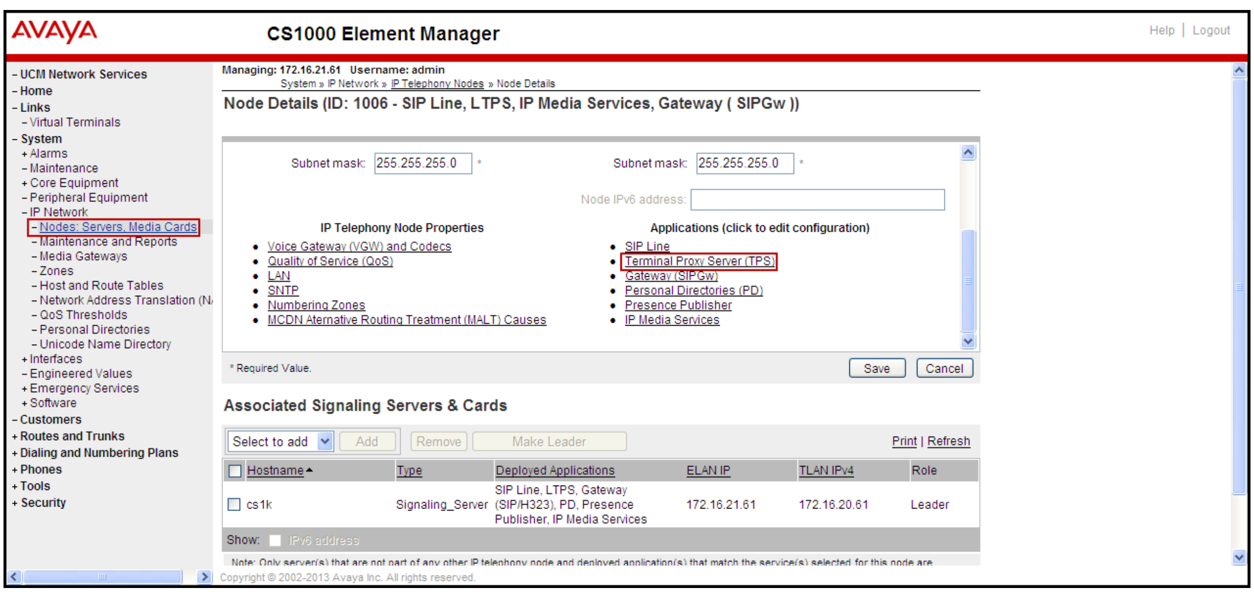


The **Node Details** screen is displayed below with the IP address of the CS1000 node. The **Node IP Address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IP Address** to communicate with other components for call processing.

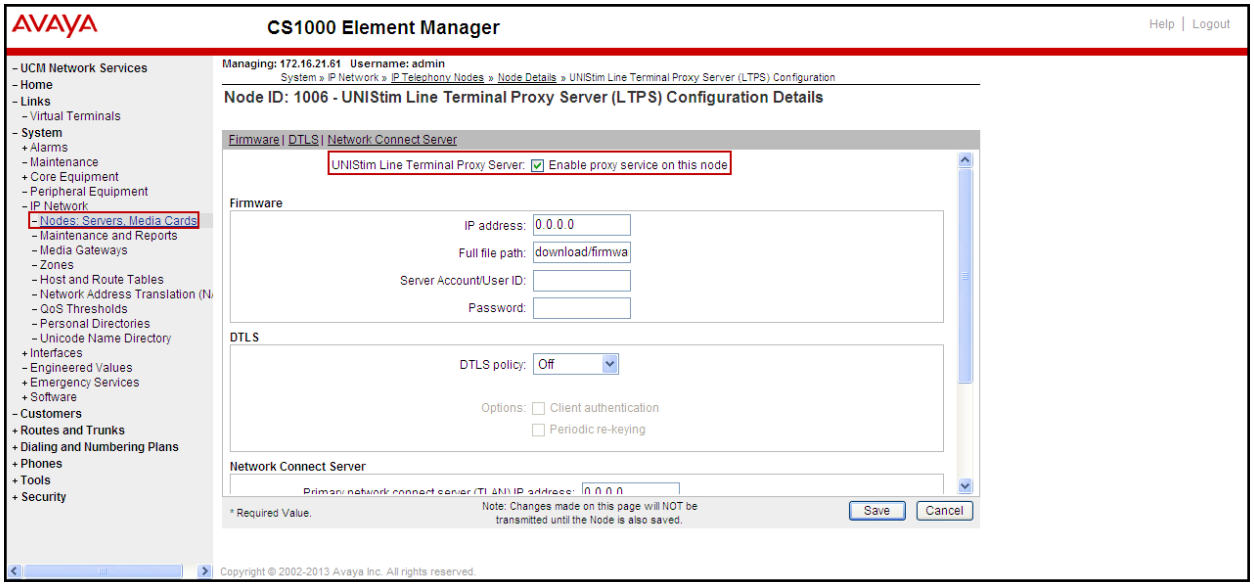


5.2.2. Administer Terminal Proxy Server

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

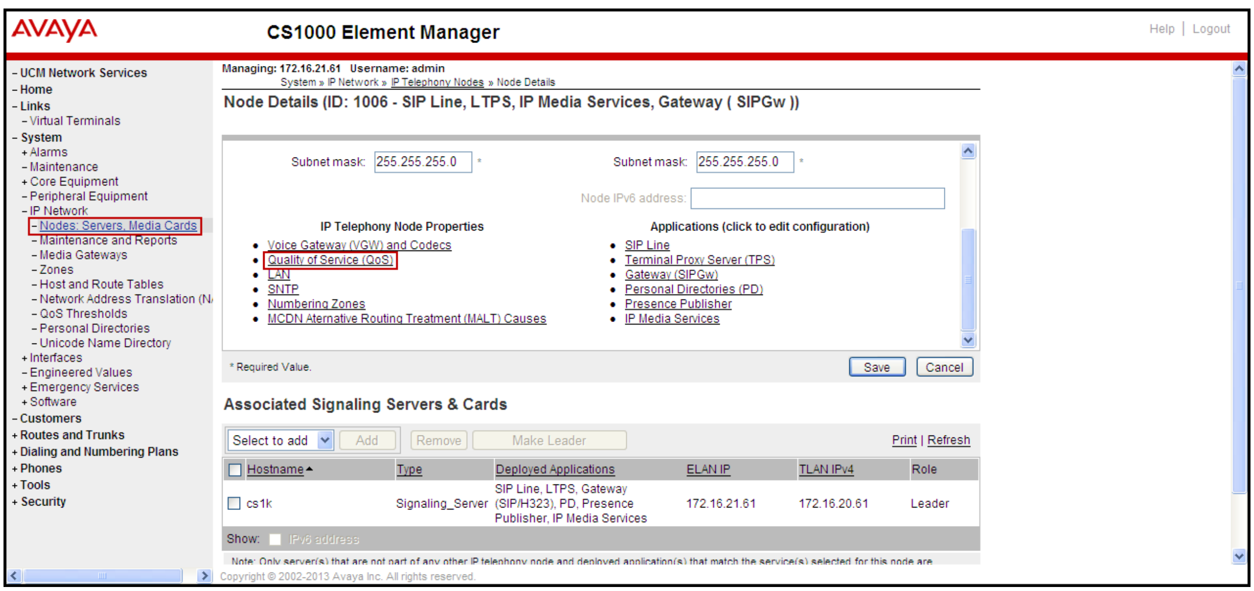


The **UNIStim Line Terminal Proxy Server (LTPS) Configuration Details** screen is displayed below. Check the **Enable proxy service on this node** check box and then click **Save**.

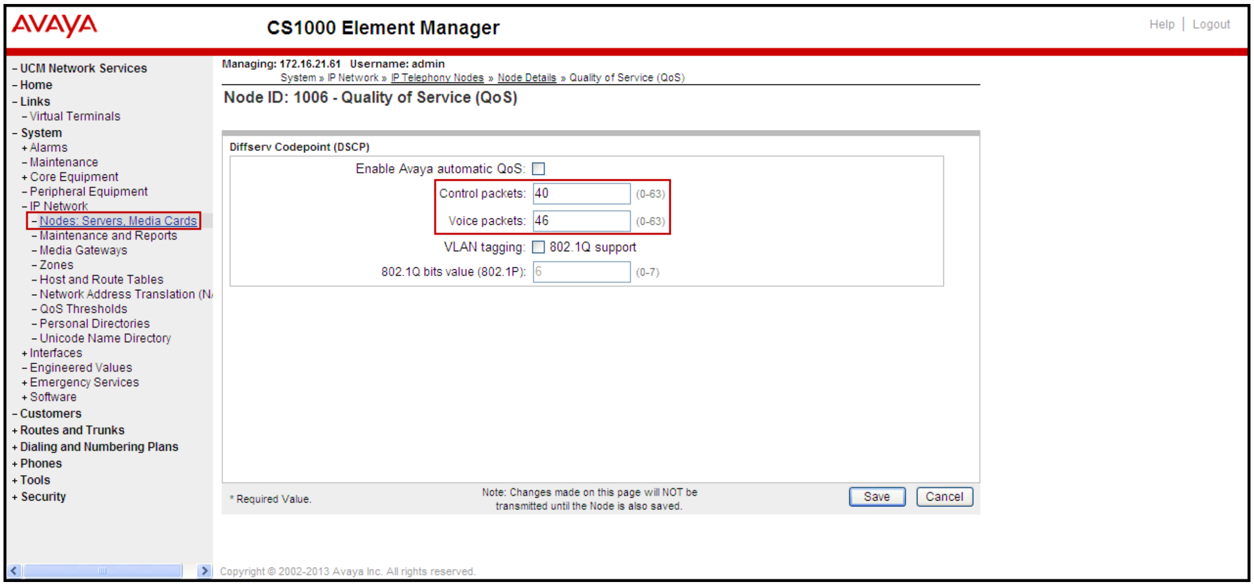


5.2.3. Administer Quality of Service (QoS)

Continue from **Section 5.2.2**. On the **Node Details** page, select the **Quality of Service (QoS)** link as shown below.

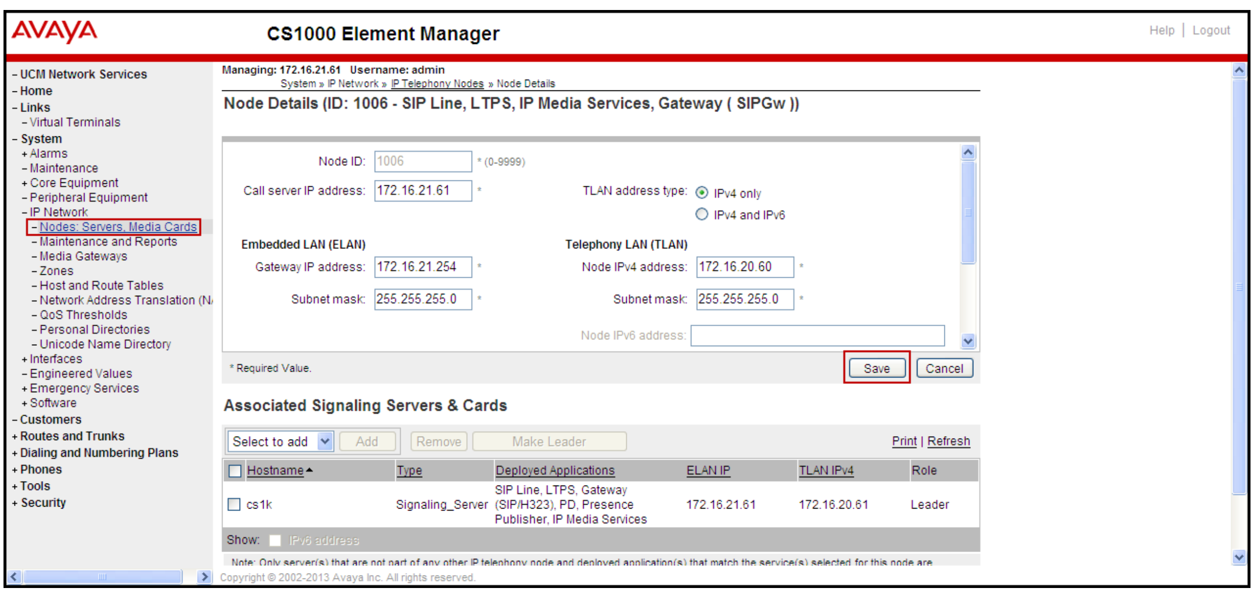


The **Quality of Service (QoS)** screen shown below will be displayed. Accept the default Diffserv values. Click the **Save** button.



5.2.4. Synchronize the New Configuration

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

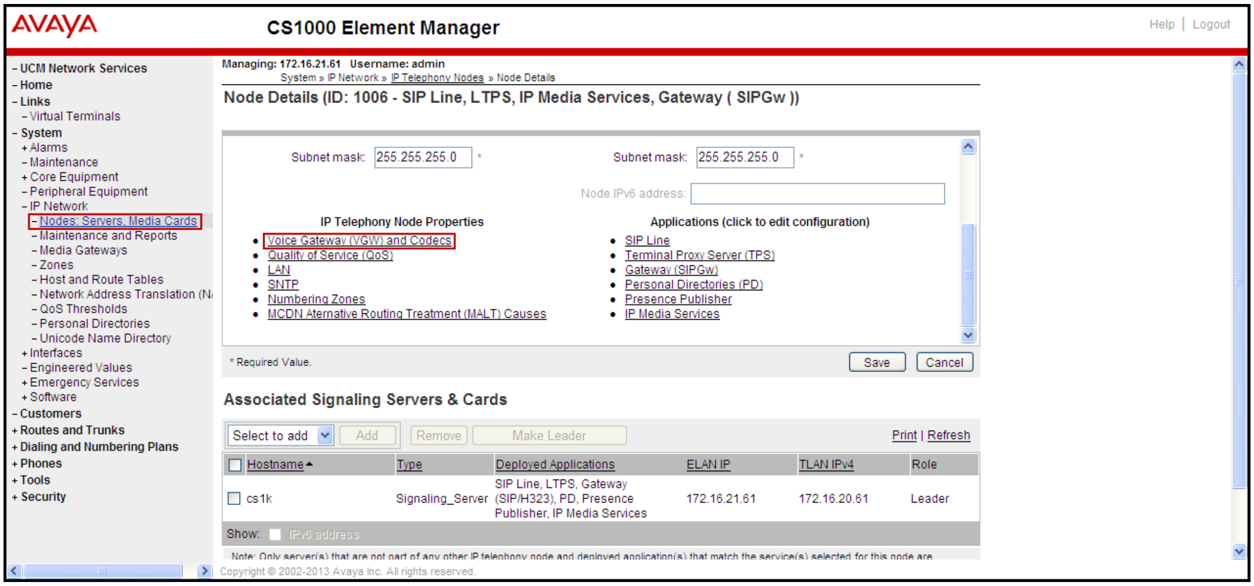


5.3. Administer Voice Codec

This section describes how to configure Voice Codecs on the CS1000.

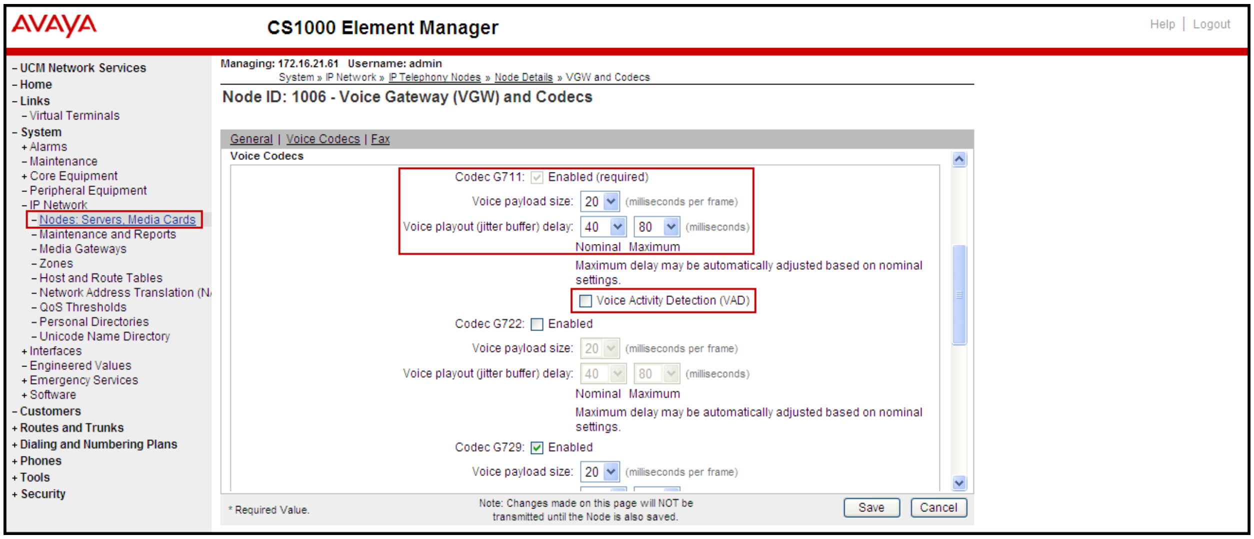
5.3.1. Enable Voice Codec, Node IP Telephony.

Select **IP Network → Nodes: Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of the CS1000 system (not shown). The **Node Details** screen is displayed. On the **Node Details** page shown below, click on **Voice Gateway (VGW) and Codecs**.

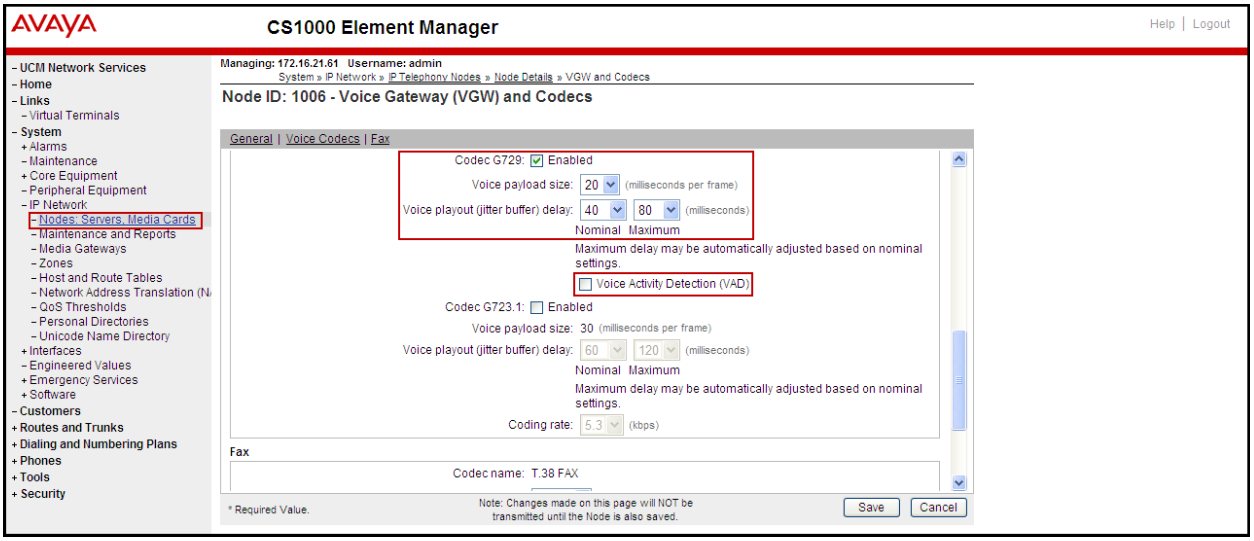


The **Voice Gateway (VGW) and Codec** screen is displayed below. CenturyLink supports codecs **G711u, G.711a** and **G.729** with **Voice Activity Detection** (**VAD**) disabled**.** Enable **codec G.729** by checking the box.

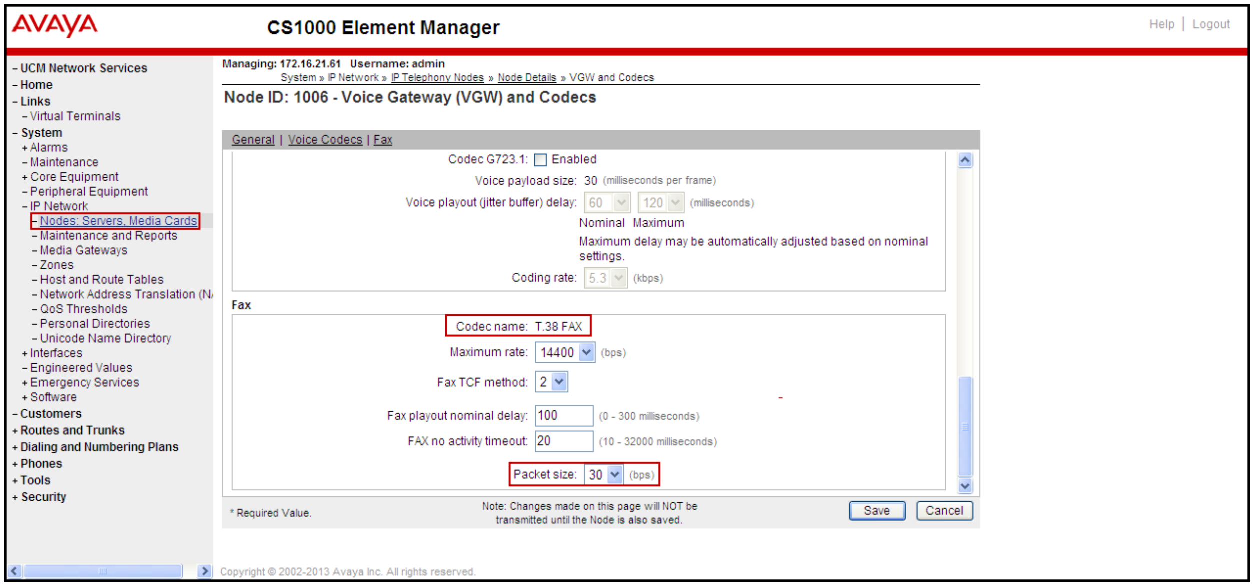
The values for the **G711** Voice Codec are shown below. Ensure that **Voice Activity Detection (VAD)** is unchecked.



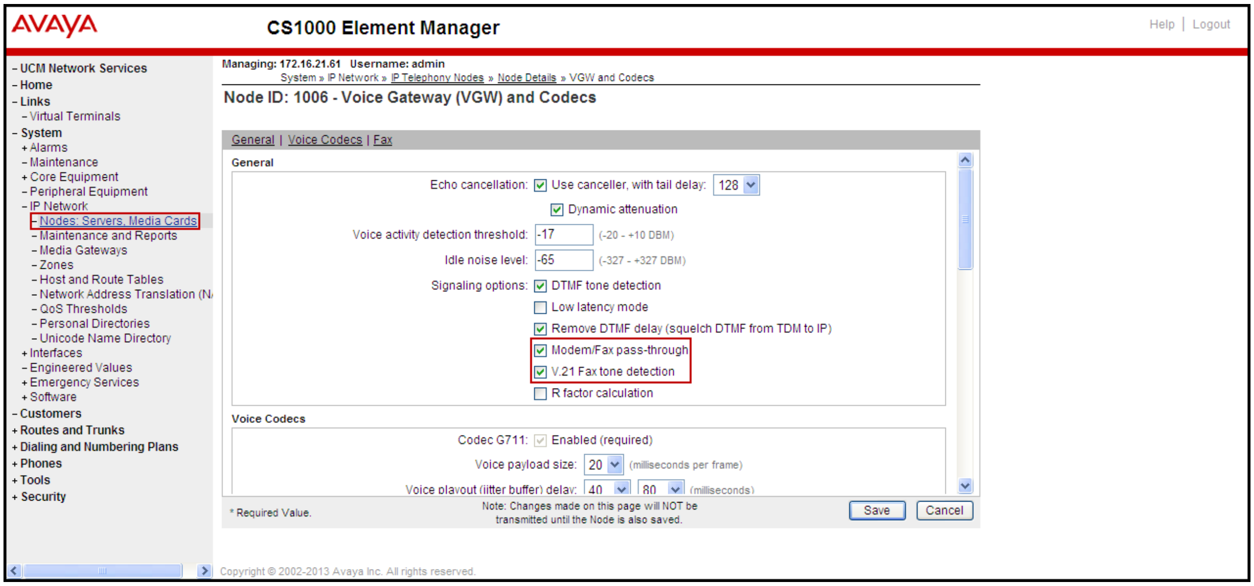
The values for the **G729** Voice Codec are shown below. Ensure that **Voice Activity Detection (VAD)** is unchecked.



For Fax over IP, **T.38** was used as default and **G.711u pass-through** as fallback. **T.38** with payload size **30ms** was chosen as default codec for fax. During the testing, **T.38** fax transport worked successfully for fax calls made from the PSTN to the CS1000 (inbound) and for CS1000 to the PSTN (outbound). **G.711u fax pass-through** was also tested successfully.



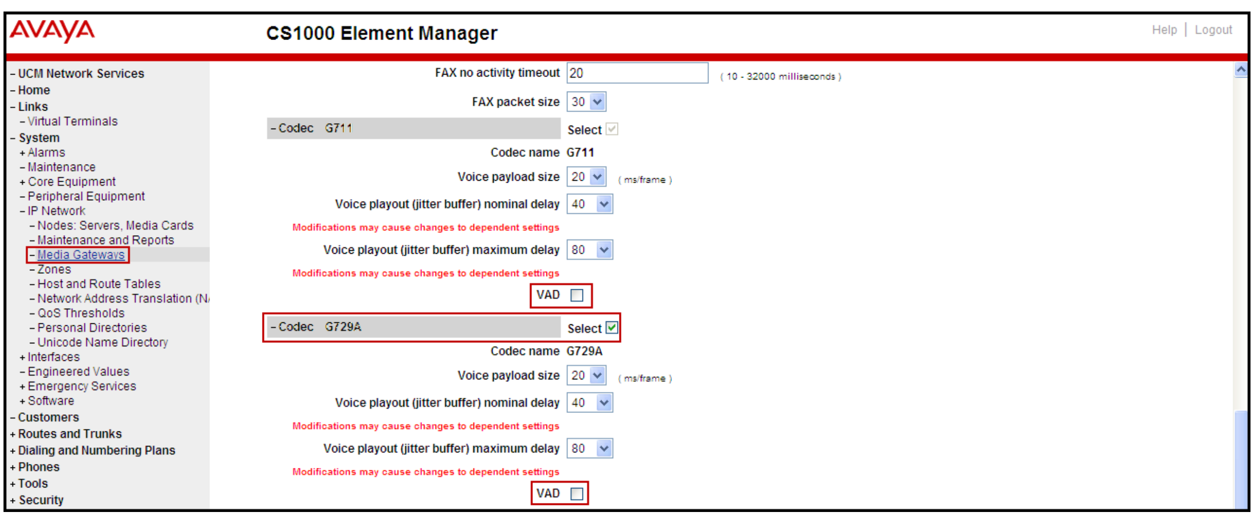
Ensure that **Modem/Fax Pass Through** and **V.21 Fax tone detection** are checked.



Click on **Save** and Synchronize the new configuration as described in **Section 5.2.4**.

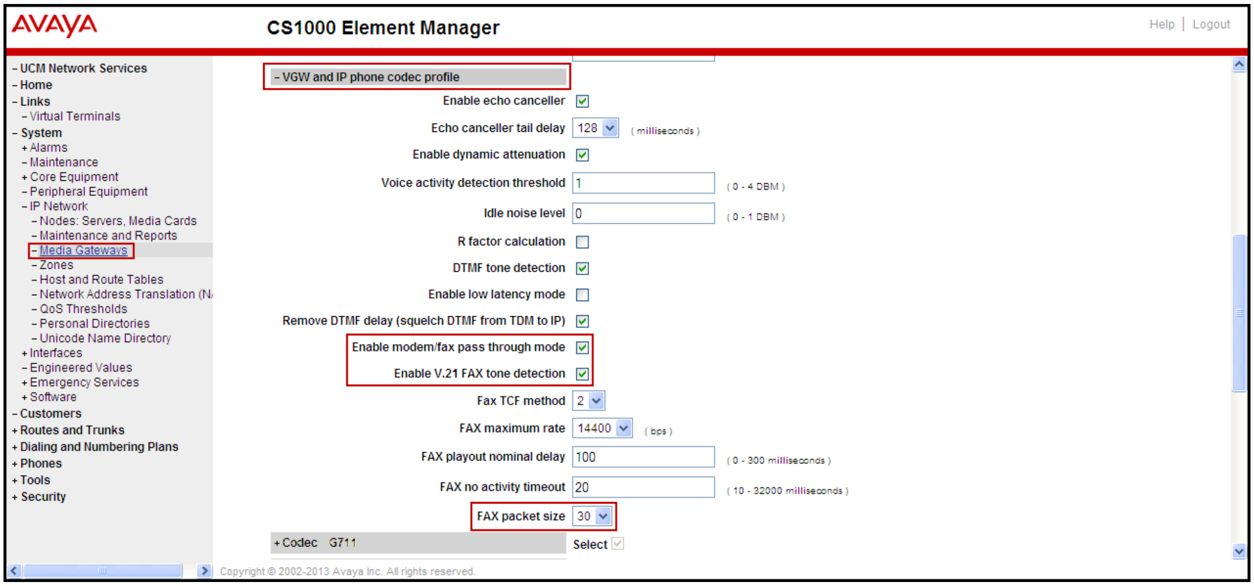
5.3.2. Enable Voice Codec on Media Gateways

From the left menu of the Element Manager page, select **IP Network → Media Gateways** menu item. The Media Gateways page will appear (not shown). Click on the **IPMG** (not shown) and the IPMG Property Configuration page is displayed (not shown), click **next** (not shown), scroll down to the Codec **G711**, uncheck **VAD** for codec **G711**, check Codec **G729A**, and uncheck **VAD** for codec **G729A**, as shown below. Scroll down to the bottom of the page and click **Save** (not shown).



For Fax over IP, **T.38** was used as default and **G.711u pass-through** as fallback. During the testing, **T.38** fax transport worked successfully for fax calls made from the PSTN to the CS1000 (inbound) and from the CS1000 to the PSTN (outbound). **G.711u fax pass-through** was also tested successfully.

Under **VGW and IP phone codec profile** ensure that **Enable V.21 FAX tone detection** and **Enable modem fax pass through mode** are checked. T.38 with payload size 30ms was chosen.

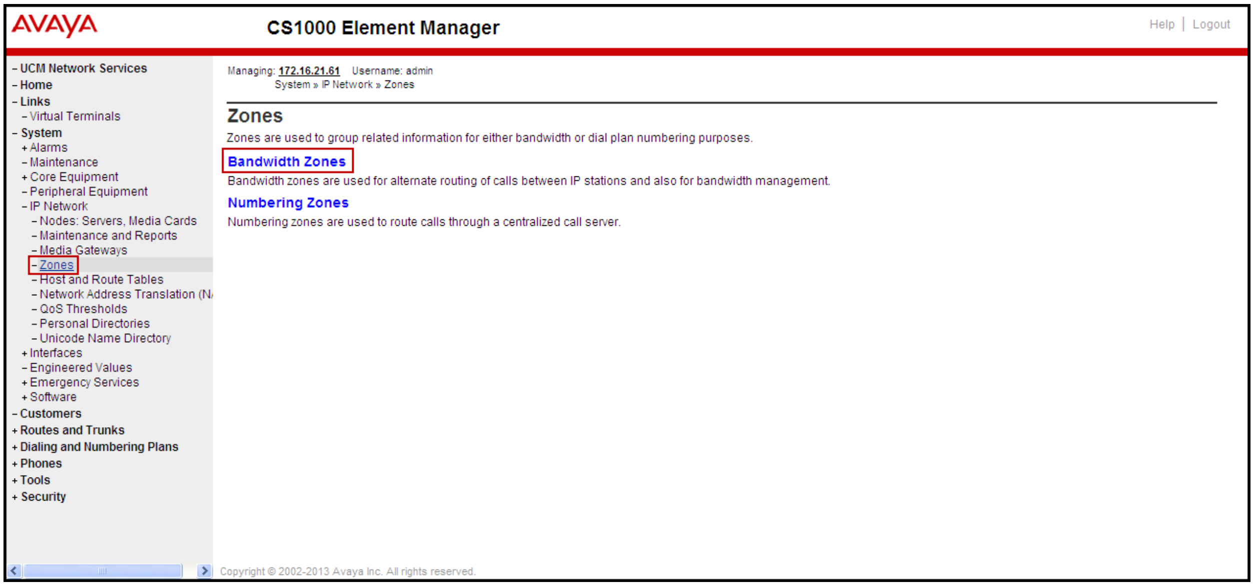


5.4. Administer Zones and Bandwidth

This section describes the steps to create bandwidth zones to be used by IP sets and SIP Trunks: **zone 5** is used by IP sets and **zone 4** is used by SIP Trunks.

5.4.1. Create a zone for IP phones (zones 5)

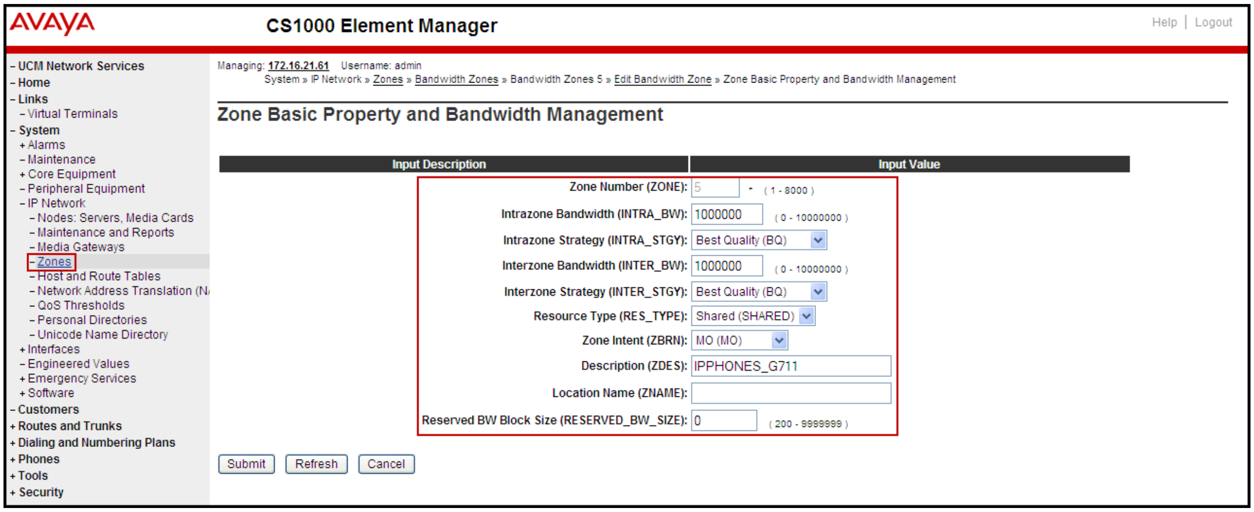
The following figures show how to configure a zone for IP sets for bandwidth management purposes. The bandwidth strategy can be adjusted to preference. Select **IP Network → Zones** from the left pane, click on the **Bandwidth Zones** as shown below.



Click **Add** (not shown), select the values shown below and click on the **Save** button.

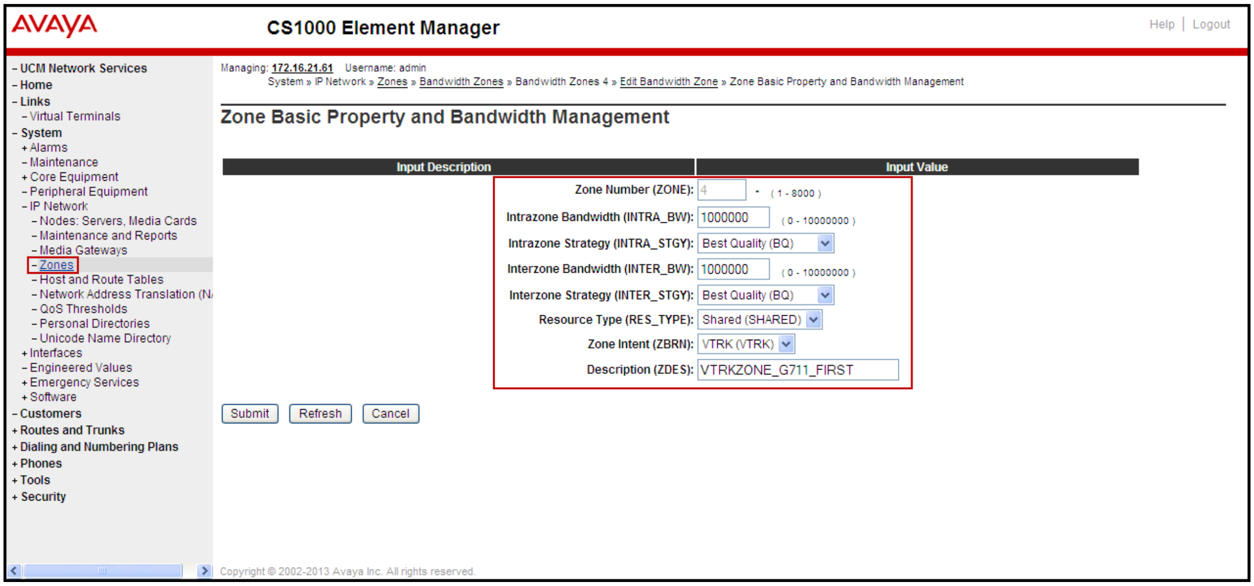
- **INTRA_STGY**: Bandwidth configuration for local calls, select **Best Quality (BQ).**
- **INTER_STGY**: Bandwidth configuration for the calls over trunk, select **Best Quality (BQ).**
- **ZBRN: Select MO** (**MO** is used for IP phones).

The values for Zone 5 are shown below; **G711** will be used for local and for calls over the trunk.



5.4.2. Create a zone for virtual SIP trunks (zone 4)

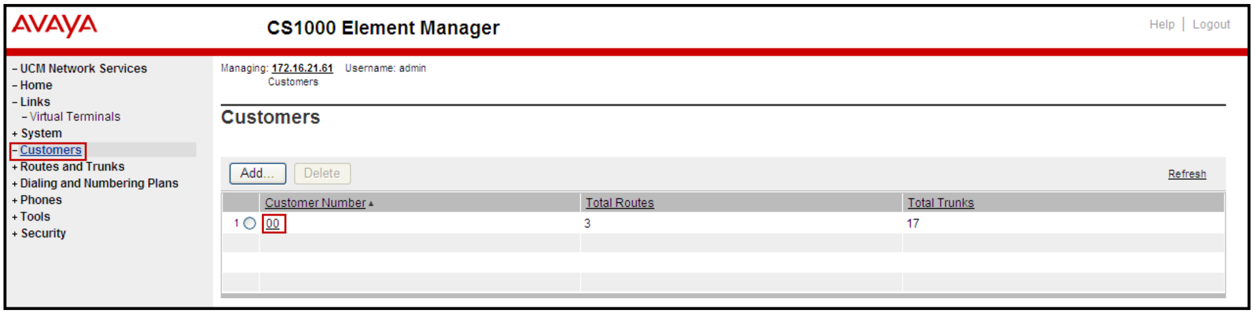
Follow Section **5.4.1** to create a zone for the Virtual SIP Trunks. The difference is in the **Zone Intent** (**ZBRN**) field, For **ZBRN** select **VTRK** for virtual trunk and **Best Quality (BQ)** for both, **INTRA_STGY** and **INTER_STGY** as shown below and then click on the **Save** button. For CenturyLink, Zone 4 was created for the Virtual SIP Trunks.



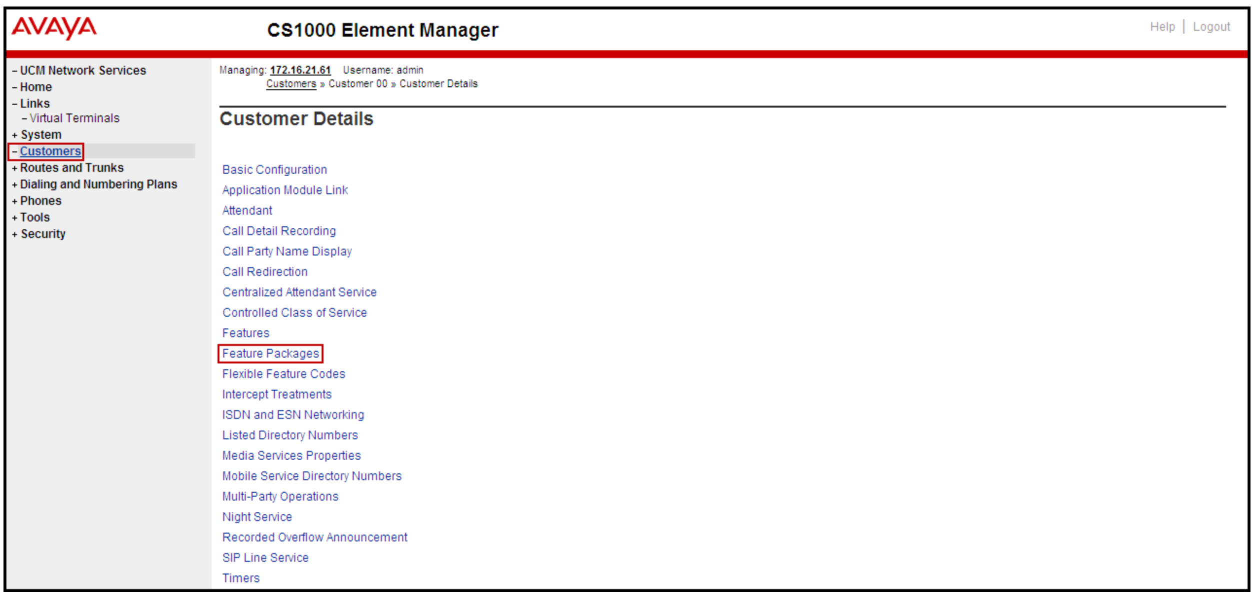
5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP IP connection between the SIP Signaling Gateway (SSG) and the Avaya SBCE.

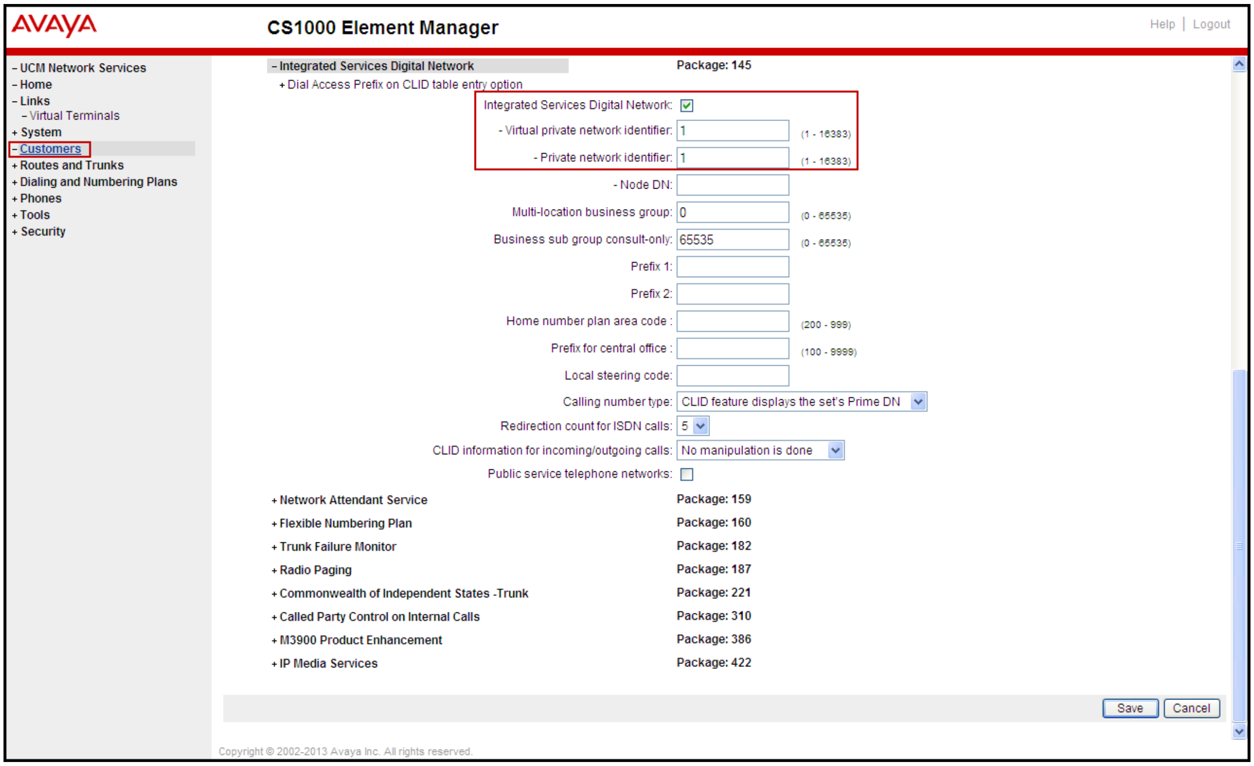
Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options.



The **Customer 00** Edit page will appear. Select the **Feature Packages** option from this page.



The screen is updated with a list of F**eature Packages** populated. Select **Integrated Services Digital Network** to edit its parameters (not shown). The screen is updated with parameters populated below **Integrated Services Digital Network**. Check the **Integrated Services Digital Network** (ISDN) check box, and retain the default values for all remaining fields as shown below. Scroll down to the bottom of the screen, and click on the **Save** (not shown).



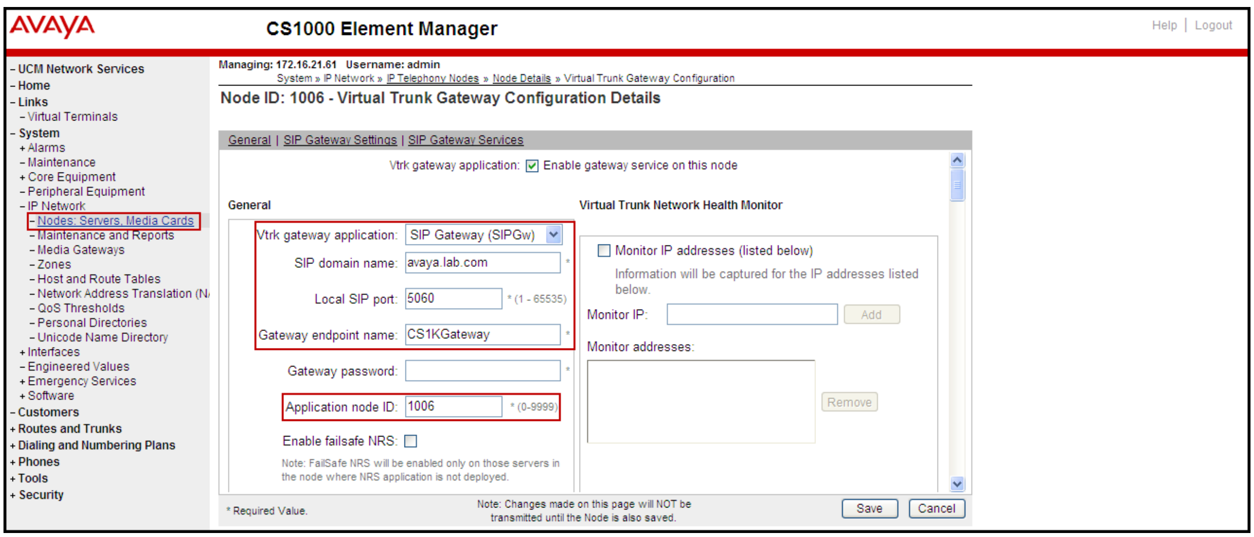
5.5.1. Administer the SIP Trunk Gateway to the Avaya SBCE

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

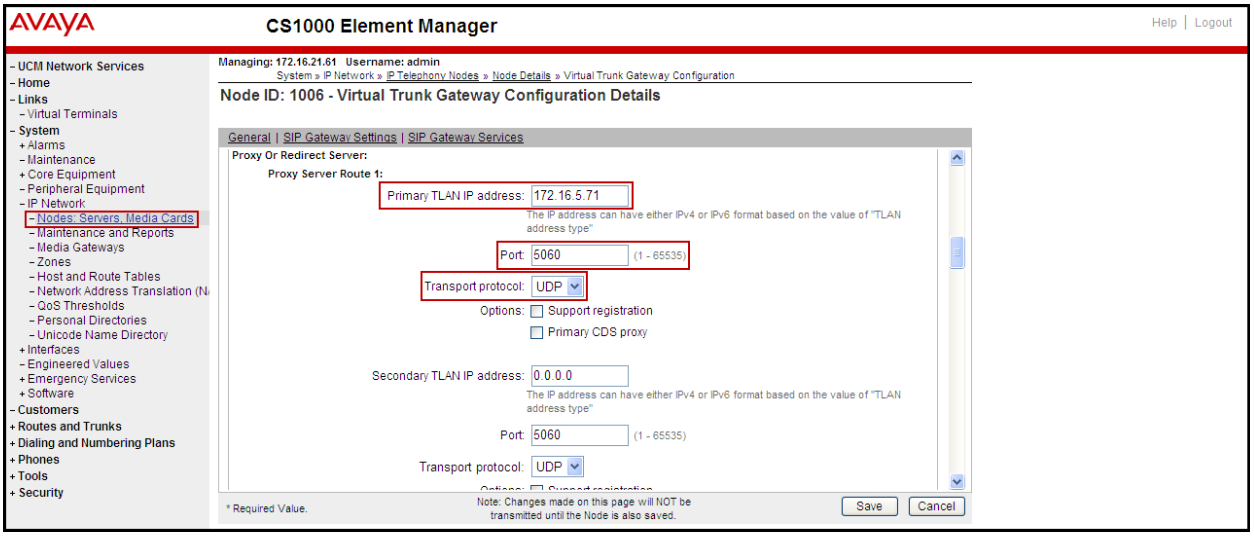
On the **Node Details** screen, select **Gateway (SIPGw)** (not shown).

Under **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown below.

- **Vtrk gateway application**: **SIP Gateway (SIPGw).**
- **SIP domain name**: avaya.lab.com
- **Local SIP port**: 5060.
- **Gateway endpoint name**: CS1KGateway.
- **Application node ID**: 1006.



Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the values highlighted in red boxes for the Primary TLAN, and Secondary TLAN if one exist, retain the default values for the remaining fields as shown below. For the compliance testing only the Primary TLAN was configured, values shown correspond to the IP address, Port, and Transport of the inside (private side) IP address of the Avaya SBCE.



On the same page shown above, scroll down to the **SIP URI Map** section. The entries shown below were used during the compliance testing:

Under the **Public E.164 Domain Names**, for:

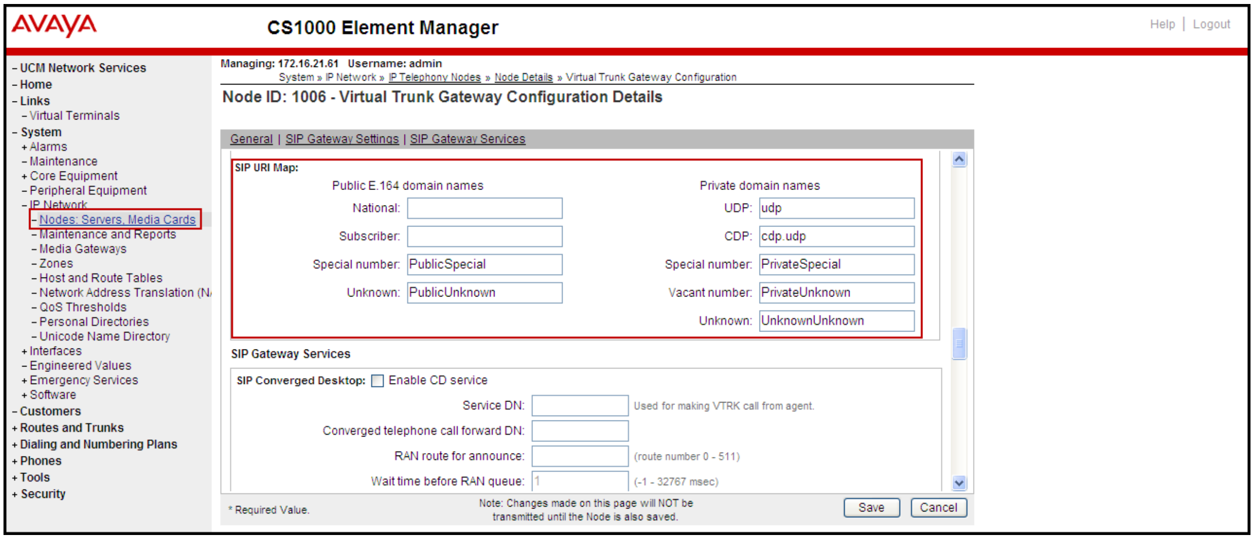
- **National**: blank.
- **Subscriber**: blank.
- **Special Number**: **PublicSpecial.**
- **Unknown**: **PublicUnknown.**

Under the **Private Domain Names**, for:

- **UDP**: **udp**.
- **CDP**: **cdp.udp**.
- **Special Number**: **PrivateSpecial**.
- **Vacant number**: **PrivateUnknown**.
- **Unknown**: **UnknowUnknown**.

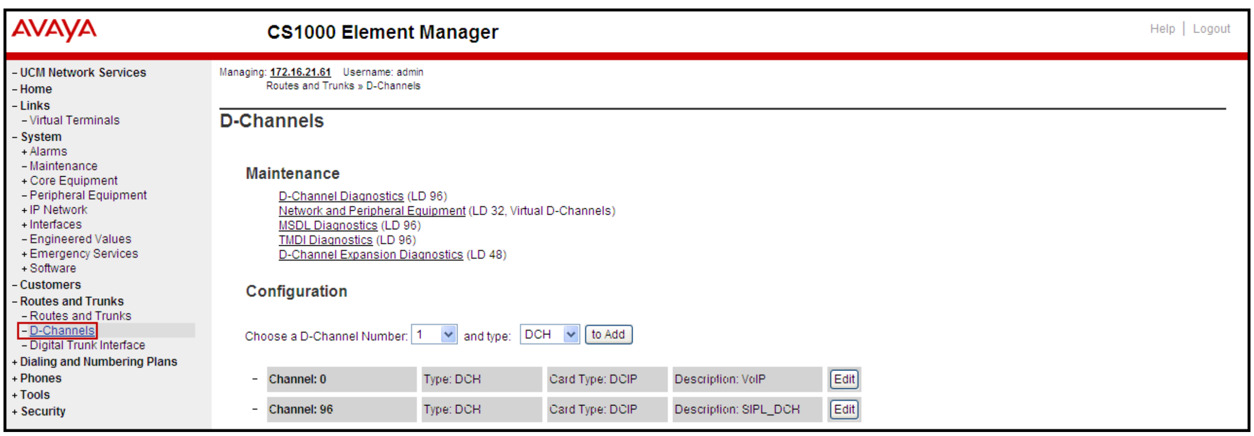
Note: The SIP URI Map entries shown above were used during the compliance testing; the values shown are default values.

Click on the **Save** button.



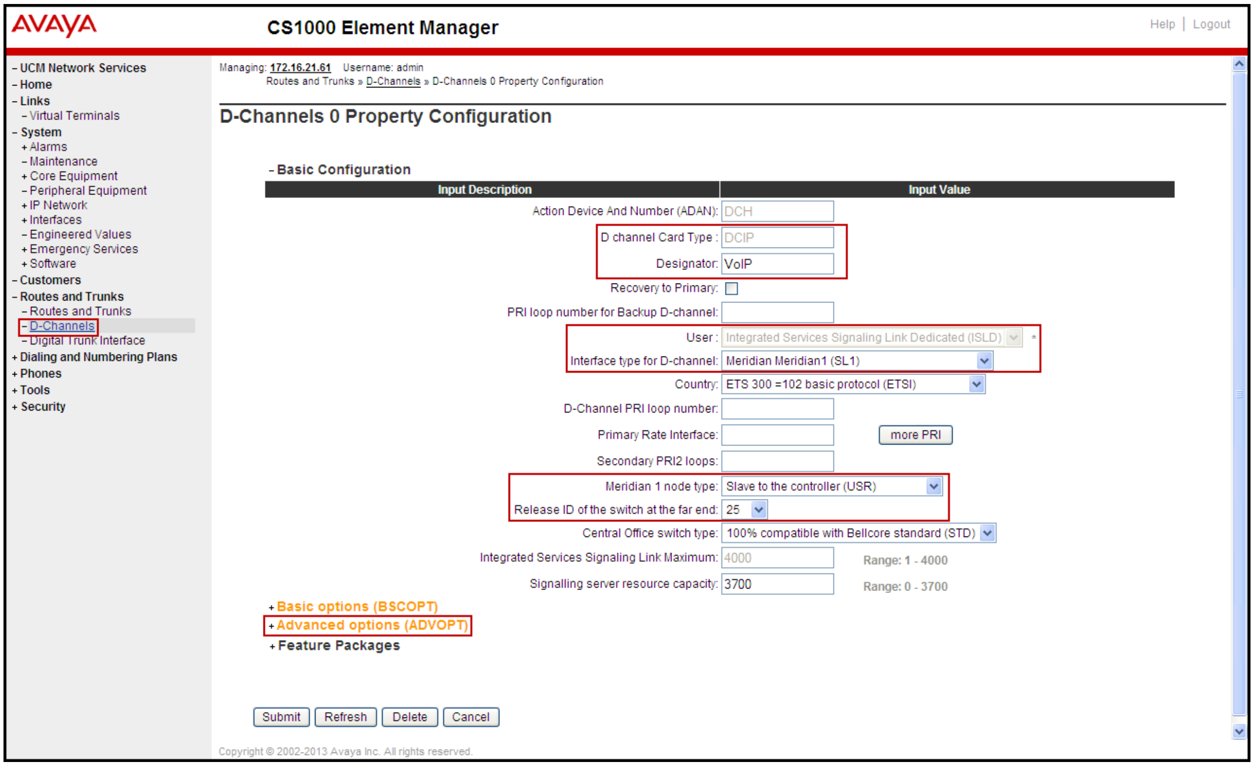
5.5.2. Administer Virtual D-Channel

Select **Routes and Trunks → D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list as shown below. Click on **to Add** button**.**



The **D-Channels 0 Property Configuration** screen is displayed next as shown below (D-Channel 0 was added for testing). Enter the following values for the specified fields:

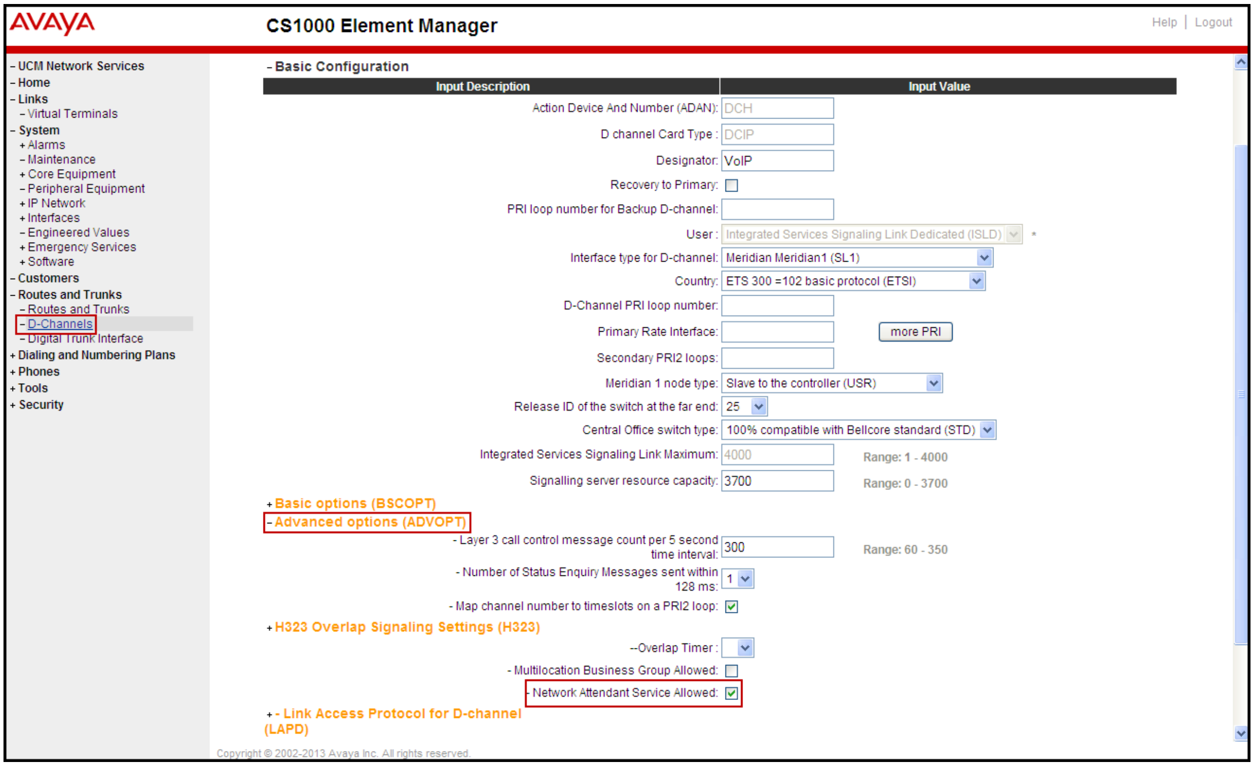
- **D channel Card Type (CTYP):** D-Channel is over IP (DCIP).
- **Designator (DES)**: A descriptive name.
- **Interface type for D-channel (IFC):** Meridian Meridian1 (SL1).
- **Meridian 1 node type:** Slave to the controller (USR).
- **Release ID of the switch at the far end (RLS):** 25.



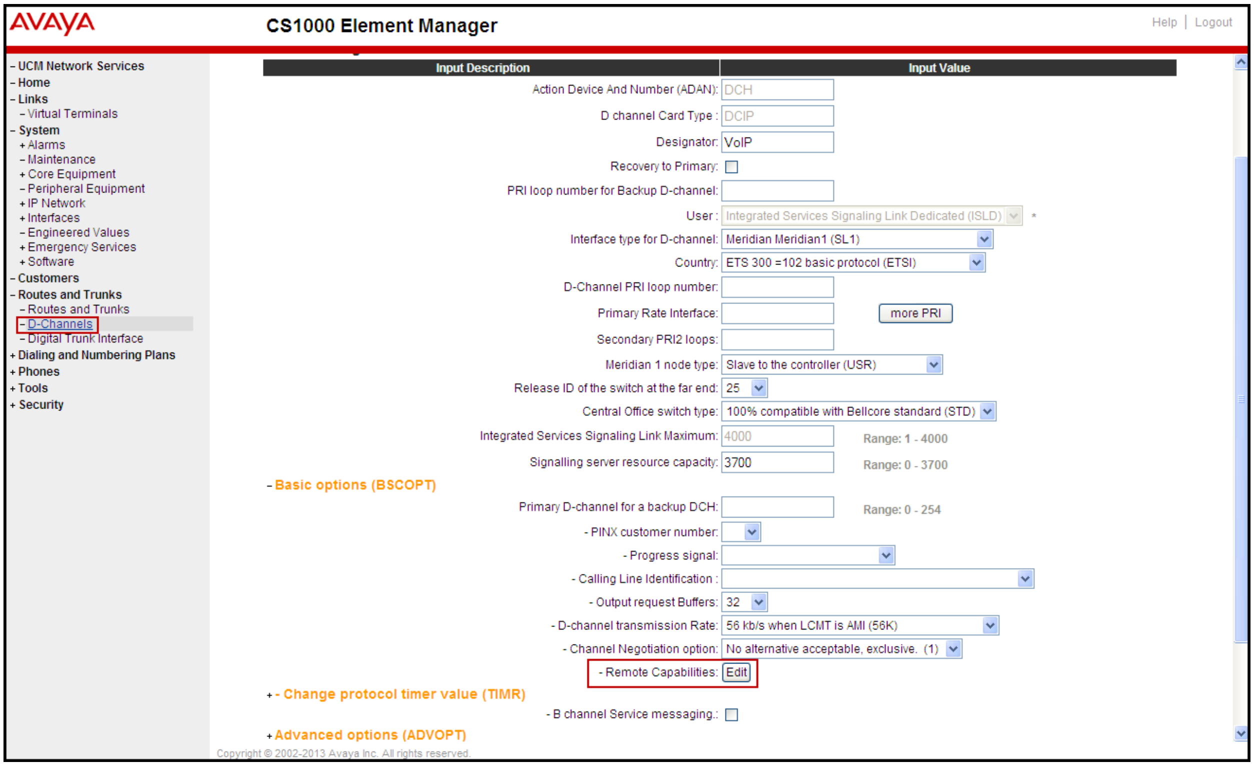
On the same page scroll down and enter the following values for the specified fields:

- **Advanced options (ADVOPT):** check **Network Attendant Service Allowed.**

Retain the default values for the remaining fields.

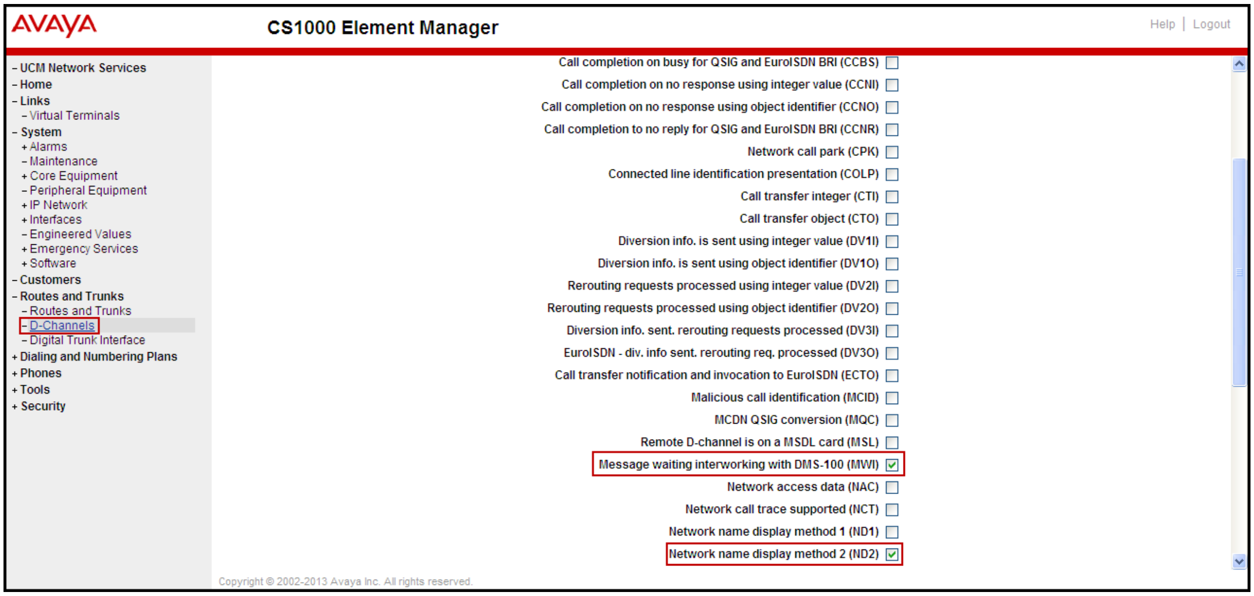


Click on the **Basic Options (BSCOPT)** and click on the **Edit** button for the **Remote Capabilities** attribute as shown below.



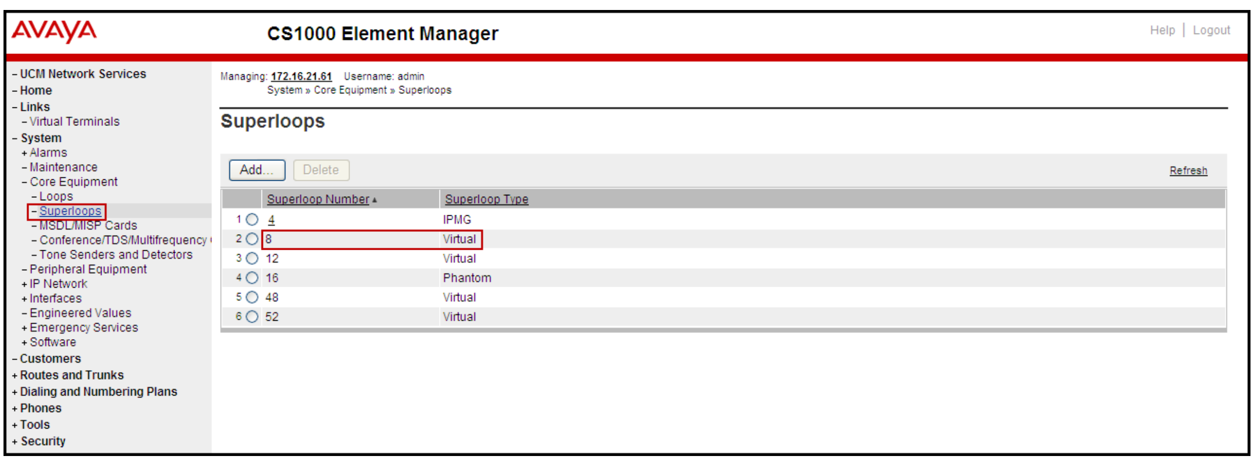
The **Remote Capabilities Configuration** page will appear, check **MWI** and **ND2** (if mailboxes are present on the CS1K Call Pilot) checkboxes as shown below.

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



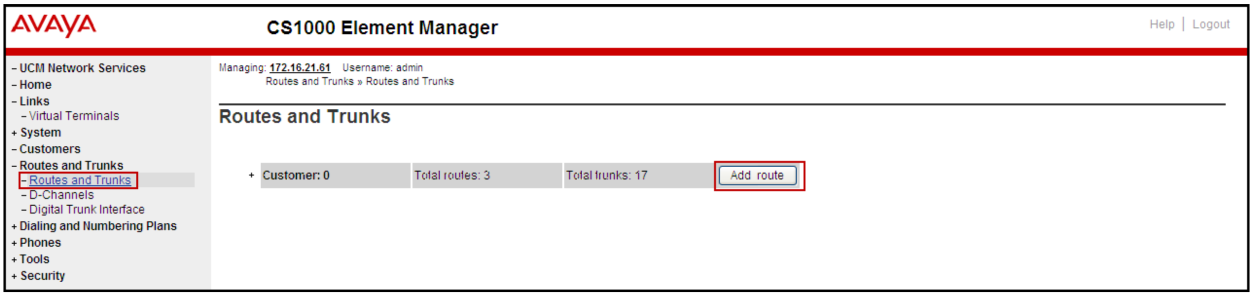
5.5.3. Administer Virtual Super-Loop

Select **System → Core Equipments → Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, click "**Add**" button to create a new one. In this example, Superloop 8 is one of the Super-loops that was added and used for the testing.



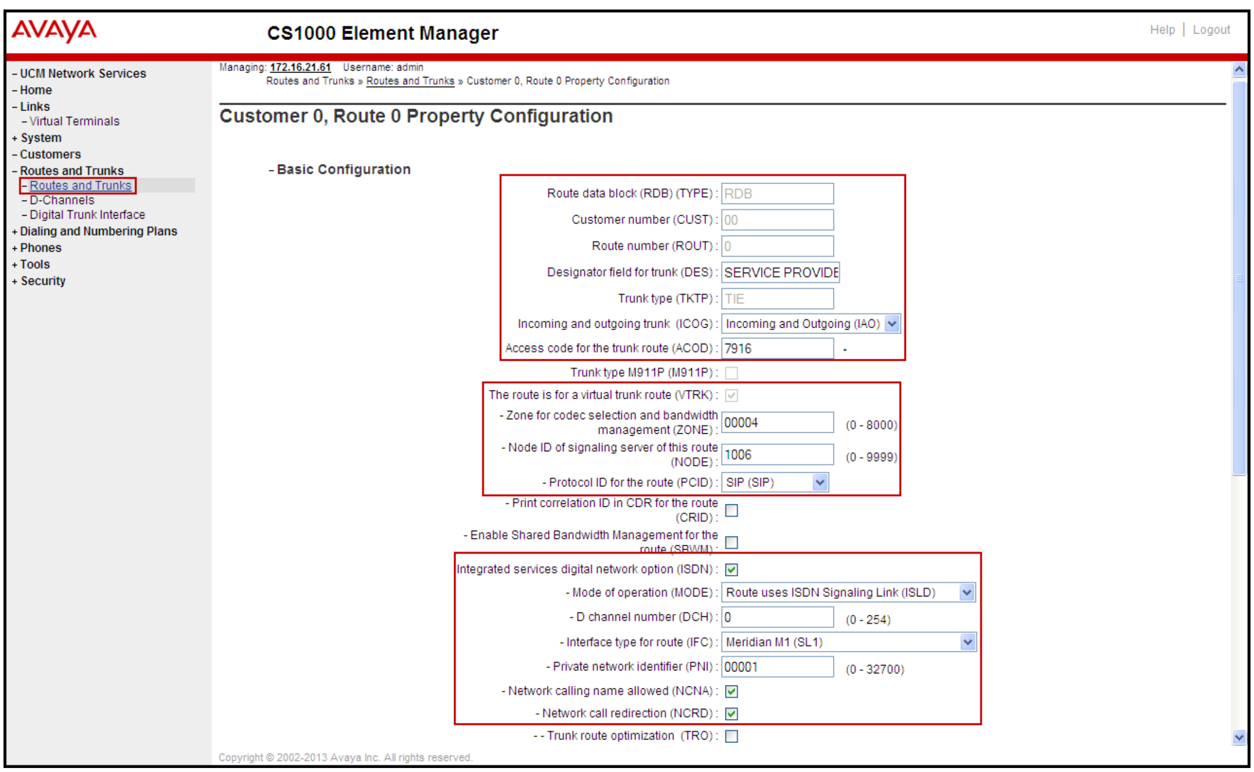
5.5.4. Administer Virtual SIP Routes

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

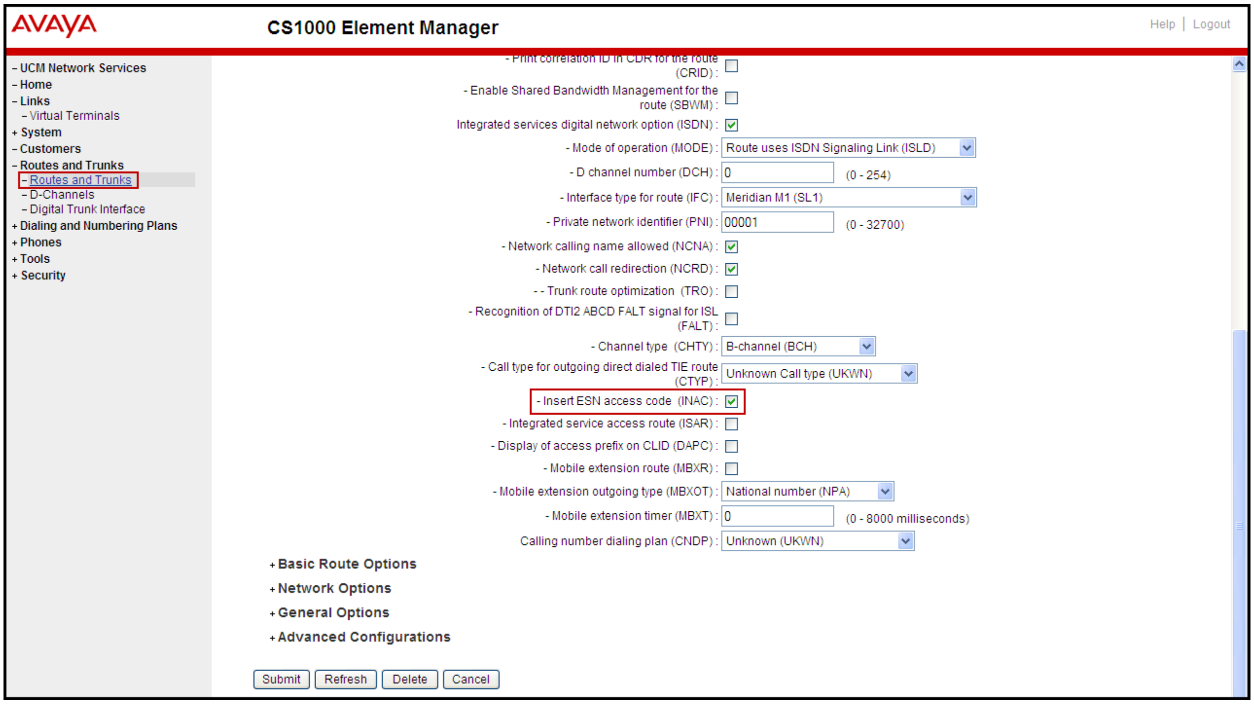


The **Customer 0**, New **Route Configuration** screen is displayed next. Scroll down until the **Basic Configuration** Section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown below.

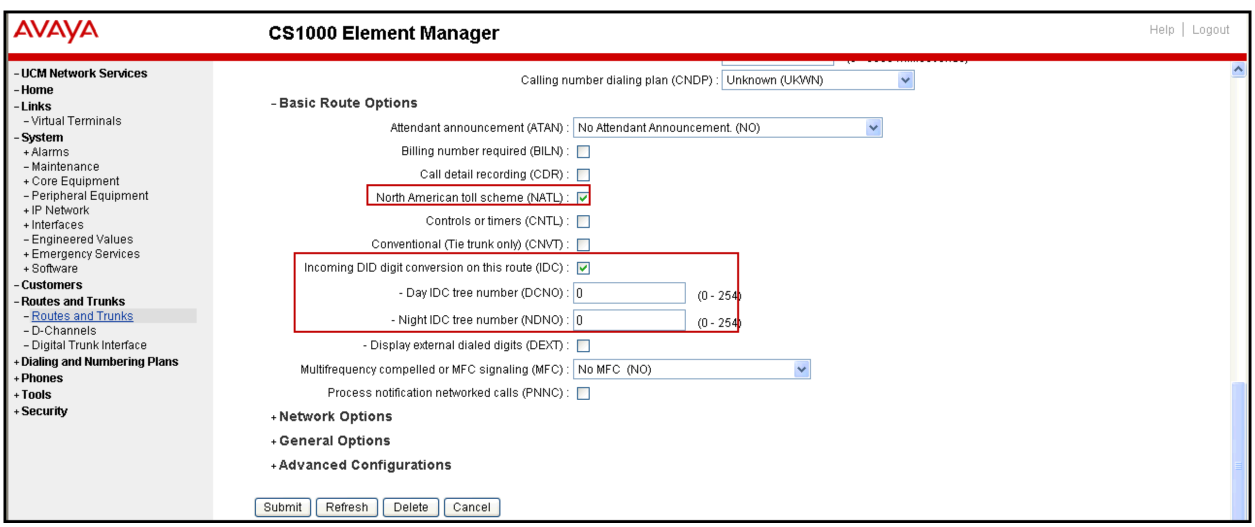
- **Route Number (ROUT)**: Select an available route number.
- **Designator field for trunk (DES)**: A descriptive text.
- **Trunk Type (TKTP)**: **TIE trunk data block (TIE).**
- **Incoming and Outgoing trunk (ICOG)**: **Incoming and Outgoing (IAO).**
- **Access Code for the trunk route (ACOD)**: An available access code.
- Check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter 4 (created in **Section 5.4.2**).
- For the **Node ID of signalling server of this route (NODE)** field, enter the node number 1006 (created in **Section 5.2.1**).
- Select **SIP** (SIP) from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen.
- **Mode of operation (MODE)**: Route uses **ISDN Signalling Link (ISLD).**
- **D channel number (DCH)**: D-Channel number 0 (created in **Section 5.5.2**).
- **Interface type for route (IFC)**: Meridian M1 (SL1).
- **Network calling name allowed (NCNA)**: Check box.
- **Network call redirection (NCRD)**: Check box.



- **Insert ESN access code (INAC):** Check box.

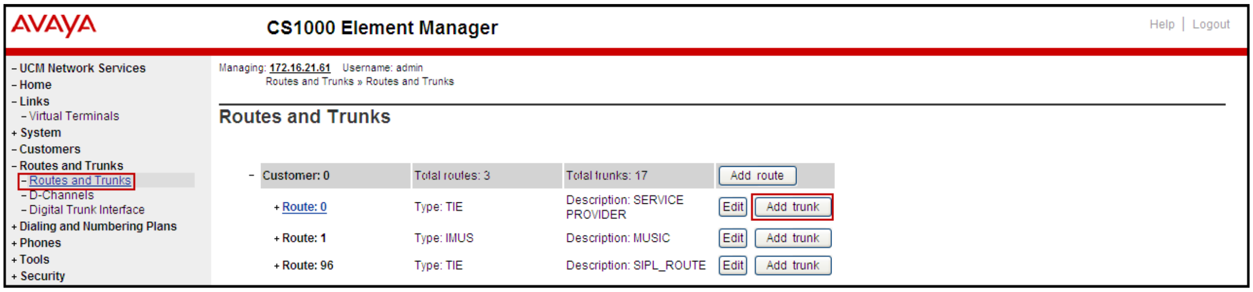


- Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 0** (created in **Section 5.6.5**) for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown below.



5.5.5. Administer Virtual Trunks

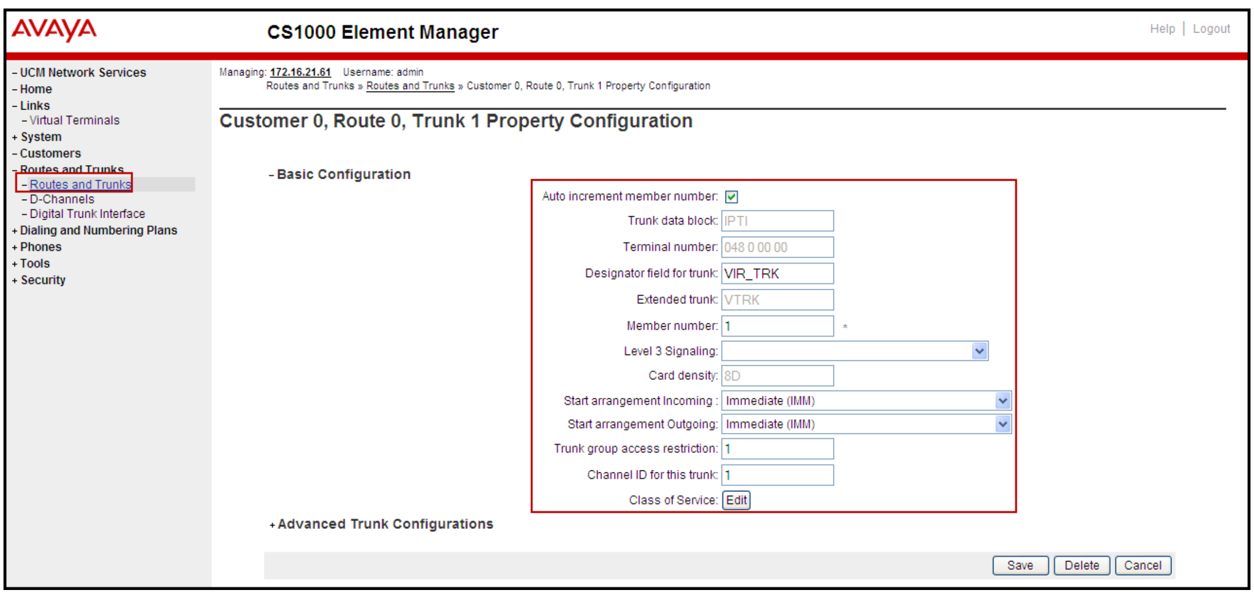
Continue from **Section 5.5.4**, after clicking on **Submit**, the **Routes and Trunks** screen is displayed and updated with the newly added route. In the example, Route 0 has being added. Click on **Add trunk** button next to the newly added route 0 as shown below.



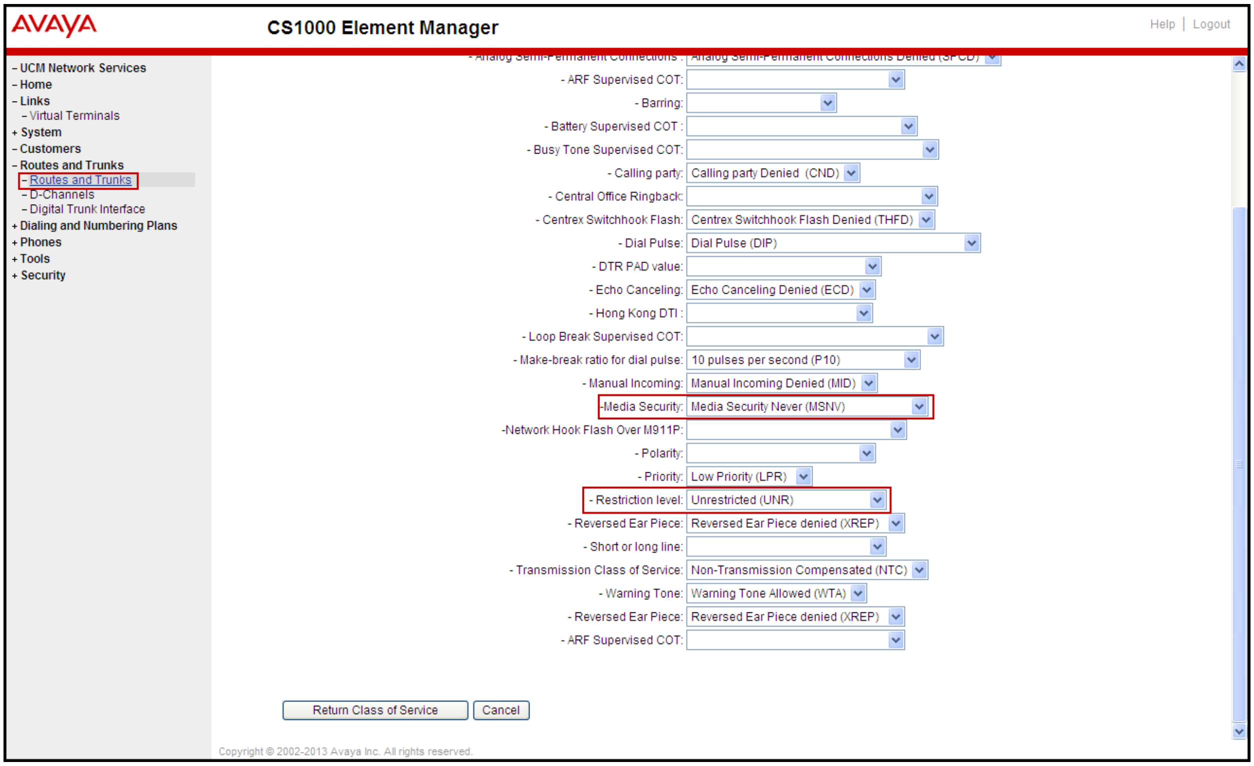
The **Customer 0, Route 0, Trunk 1 Property Configuration** screen is displayed as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields. The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service**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

Note: The **Multiple trunk input number** (**MTINPUT**) field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 11 trunks were created.

- **Trunk data block** (**TYPE**): **IP Trunk (IPTI).**
- **Terminal Number** (**TN**): Available terminal number (use virtual super-loop created in **Section 5.5.3**).
- **Designator field for trunk** (**DES**): A descriptive text.
- **Extended Trunk (XTRK): Virtual trunk (VTRK).**
- **Member number** (**RTMB**): Current route number and starting member.
- **Start arrangement Incoming** (**STRI**): **Immediate (IMM).**
- **Start arrangement Outgoing** (**STRO**): **Immediate (IMM).**
- **Trunk Group Access Restriction** (**TGAR**): Desired trunk group access restriction level.
- **Channel ID for this trunk** (**CHID**): An available starting channel ID.

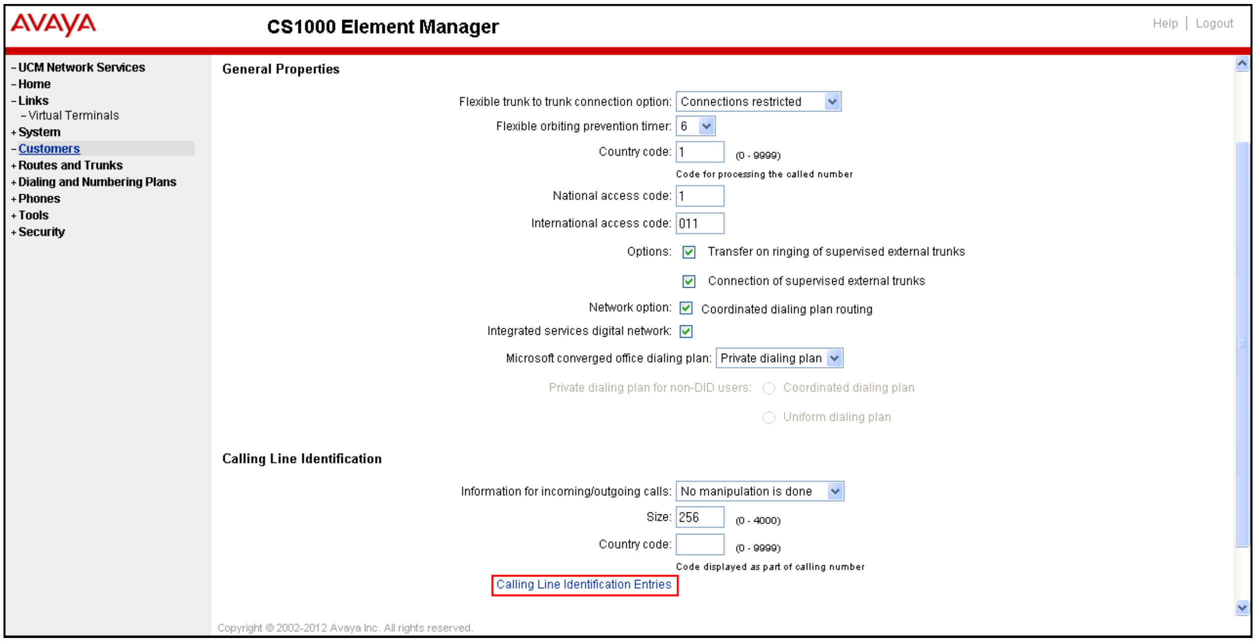


Click on **Edit Class of Service** (shown on previous screen), For **Media Security**, select **Media Security Never** (**MSNV**)**,** for **Restriction Level**, select **Unrestricted (UNR)**. Use default for remaining values. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the **Save** button (not shown).

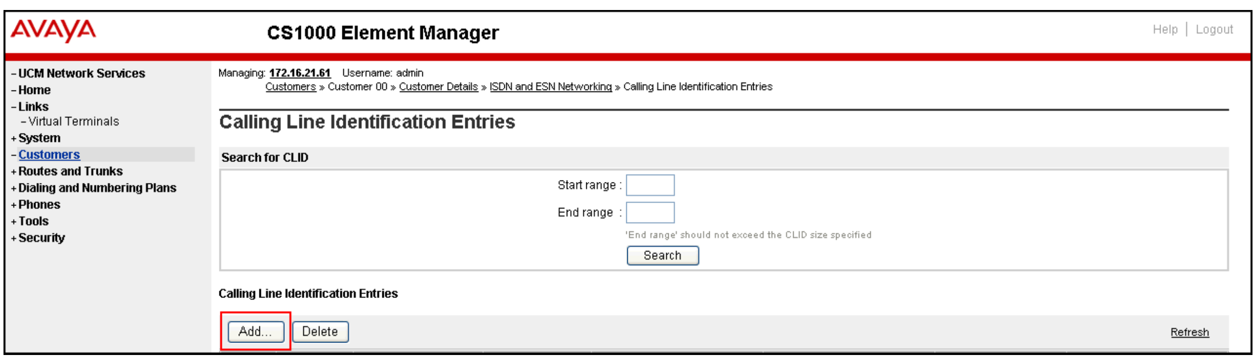


5.5.6. Administer Calling Line Identification Entries

Select **Customers → 00 → ISDN and ESN Networking** (Not shown). Click on **Calling Line Identification Entries** as shown below.



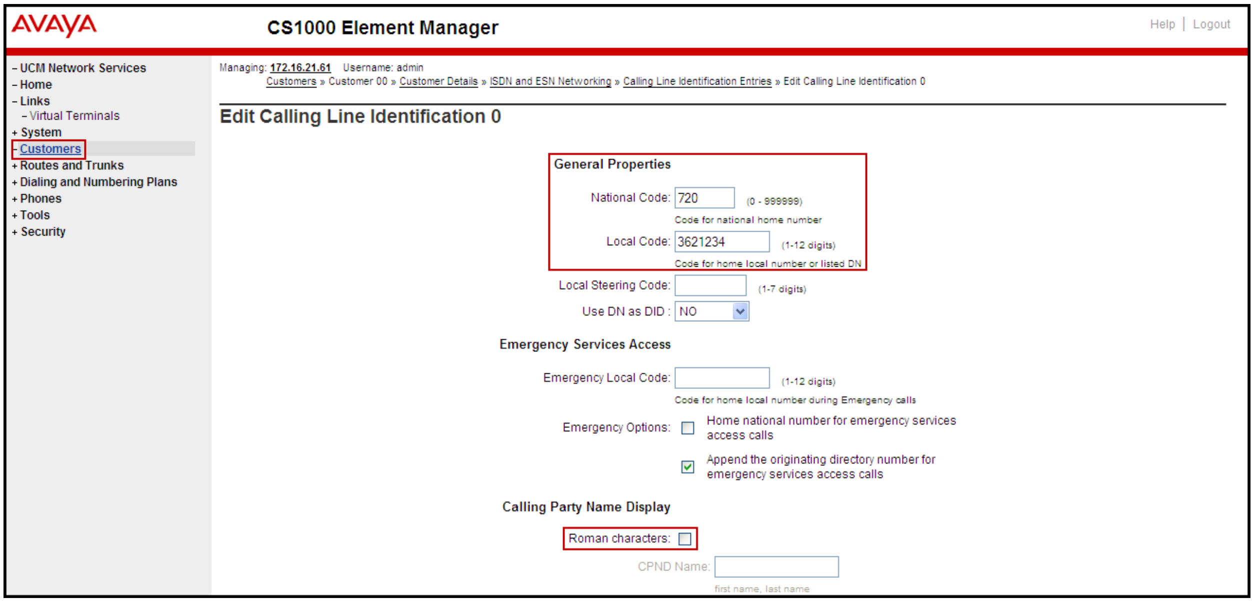
Click on **Add** as shown below.



Add entry **0** as shown below.

- **National Code**: Input the three digit area code prefix of the DID number assigned by the service provider, in this case 720.
- **Local Code**: input the seven digit number of the DID assigned by Service Provider, in this case it is 3621234.
- **Calling Party Name Display**: Uncheck for **Roman characters**.

Repeat for each of the DID numbers to be assigned to extensions in the CS1000.


AVAYA
CS1000 Element Manager
Help | Logout
- UCM Network Services
- Home
- Links
- Virtual Terminals
+ System
- Customers
+ Routes and Trunks
+ Dialing and Numbering Plans
+ Phones
+ Tools
+ Security
Managing: 172.16.21.61 Username: admin
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries » Edit Calling Line Identification 0
Edit Calling Line Identification 0
General Properties
National Code: 720 (0 - 999999)
Code for national home number
Local Code: 3621234 (1-12 digits)
Code for home local number or listed DN
Local Steering Code: (1-7 digits)
Use DN as DID : NO
Emergency Services Access
Emergency Local Code: (1-12 digits)
Code for home local number during Emergency calls
Emergency Options:
Home national number for emergency services access calls
Append the originating directory number for emergency services access calls
Calling Party Name Display
Roman characters:
CPND Name:
first name, last name

5.5.7. Enable External Trunk to Trunk Transfer

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 trunk.

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

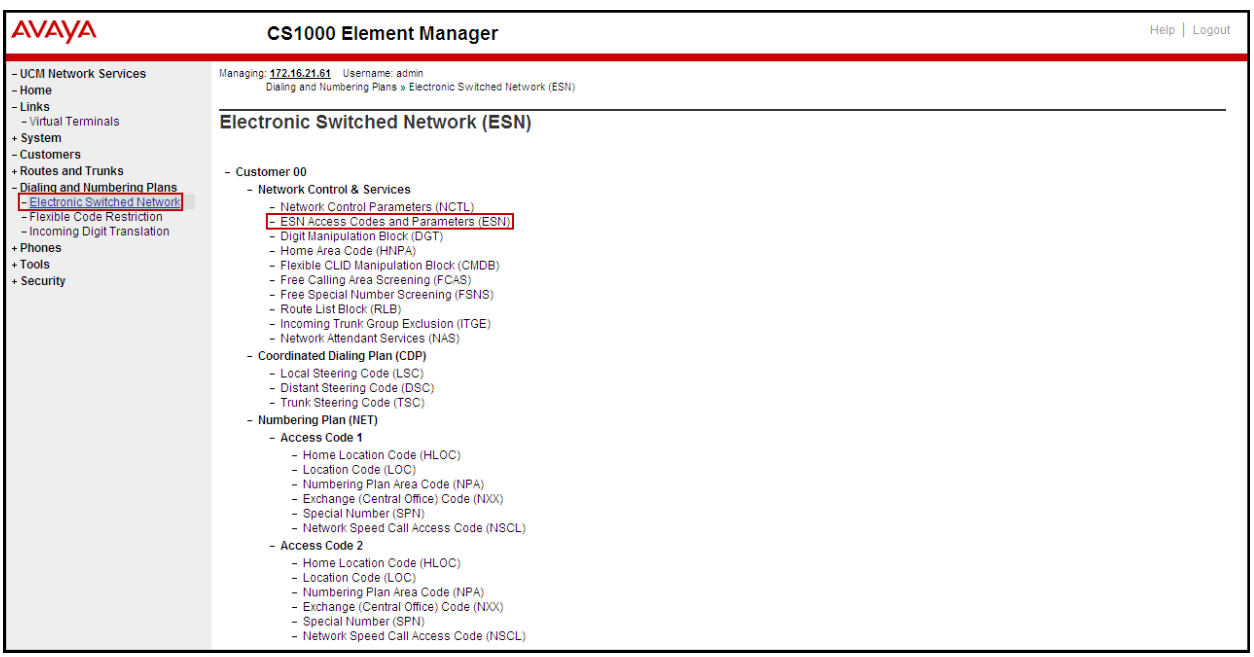
```
>ld 15 CDB000
MEM AVAIL: (U/P): 43552101    USED U P: 371282 939078    TOT: 44862461
DISK SPACE NEEDED: 1713 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
....
TRNX yes
EXTT yes
....
```

5.6. Administer Dialing Plans

This section describes how to administer dialing plans on the CS1000.

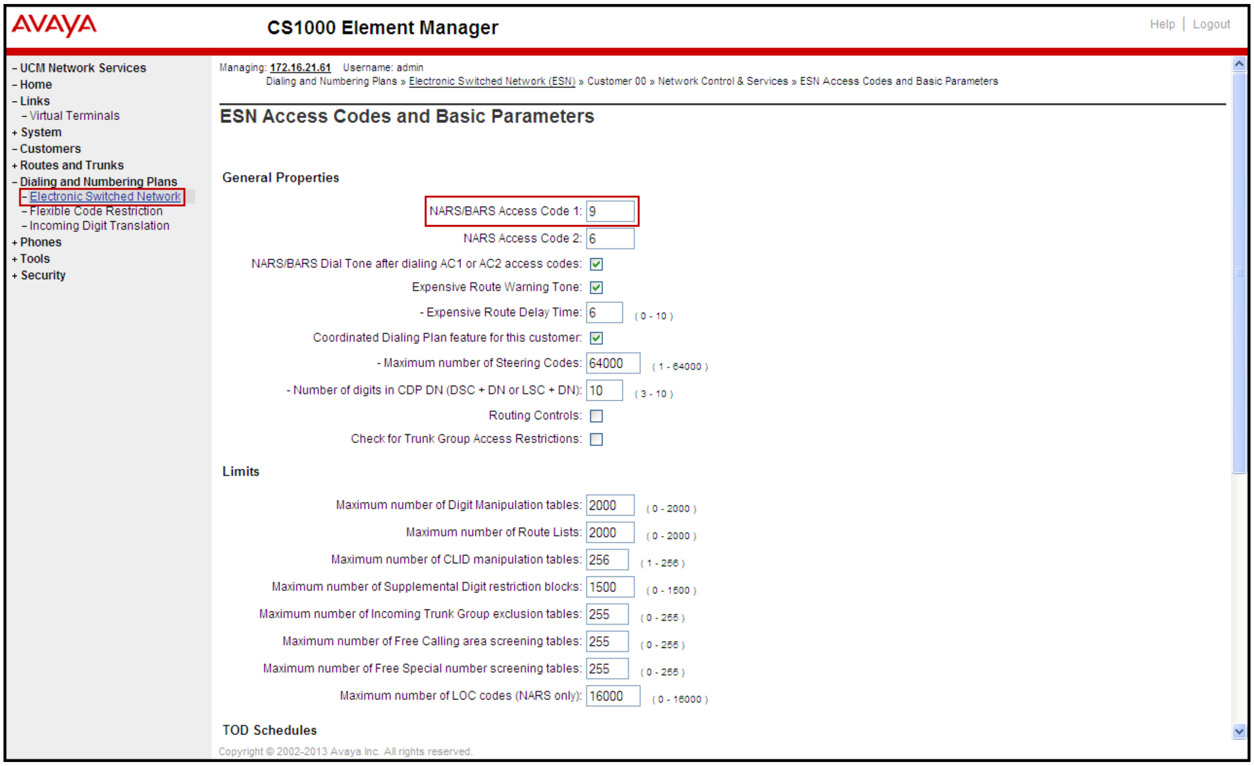
5.6.1. Define ESN Access Codes and Parameters (ESN)

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen. Select **ESN Access Code and Parameters (ESN)** as shown below.



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

Note: BARS and NARS access codes are customer defined; any one or two digit code can be used, provided there is no conflict with any other part of the dial plan.



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

Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail)
In LD 15, change Customer Net_Data block by disabling NPA and SPN to be associated to Access Code 2 (AC2). It means Access Code 1 will be used for NPA and SPN calls.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35717857    USED U P: 8241949 920063    TOT: 44879869
DISK SPACE NEEDED: 1697 KBYTES
REQ: chg
TYPE: net_data
CUST 0
OPT
AC2 xnpa xspn
FNP
CLID
ISDN
…
```

Verify Customer Net_Data block by using LD 21

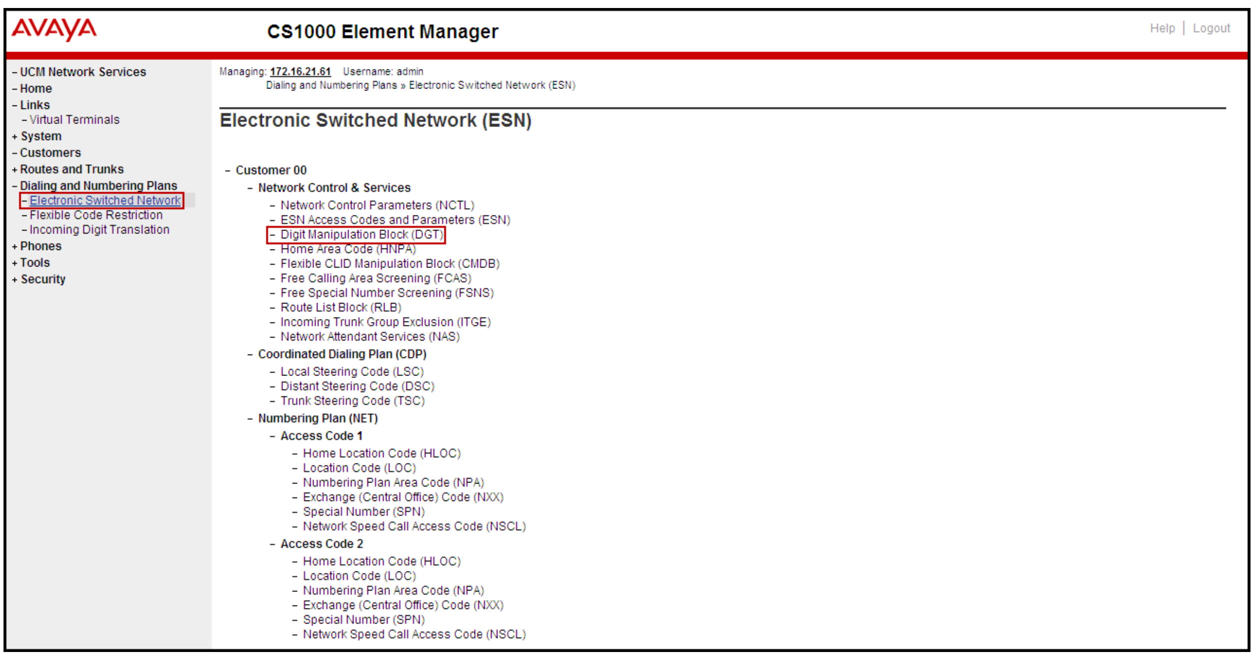
```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

TYPE NET_DATA
CUST 00
OPT RTA
AC1 INTL NPA SPN NXX LOC
AC2
FNP YES
…
```

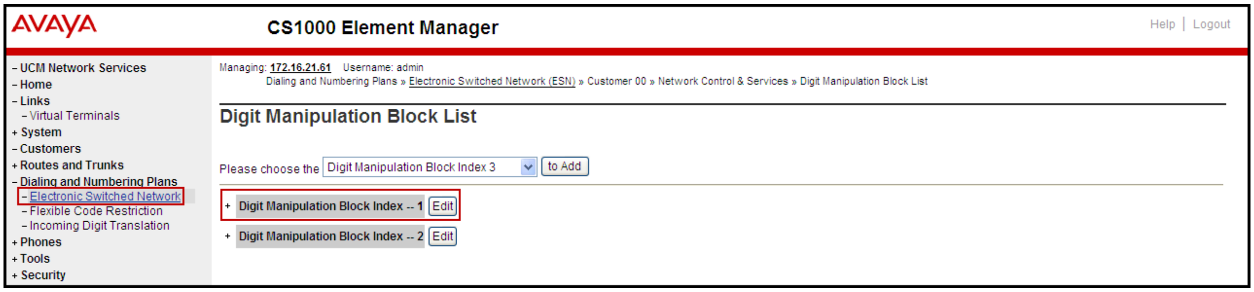
5.6.3. Digit Manipulation Block Index (DMI)

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Digit Manipulation Block (DGT)** as shown below.

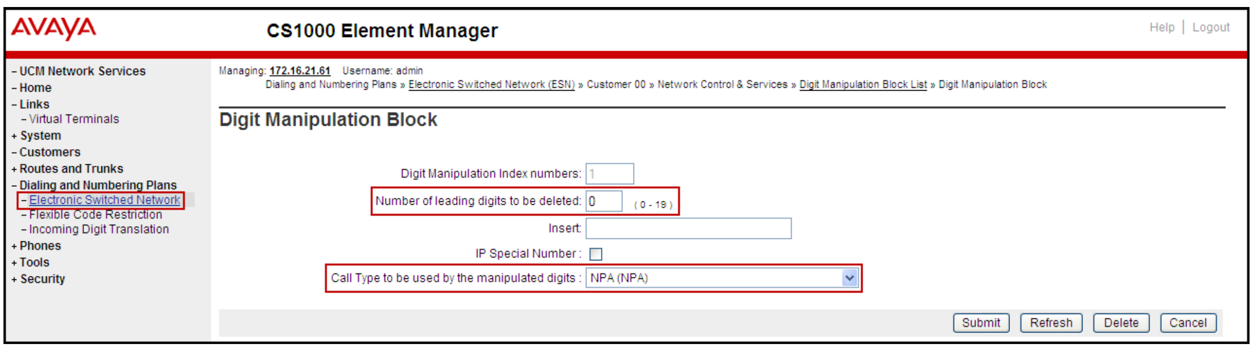


In the **Please choose the Digit Manipulation Block Index** drop-down field, select an available DMI from the list and click **to Add** as shown below.

In the example shown below Digit manipulation Block Index 1 was previously added.

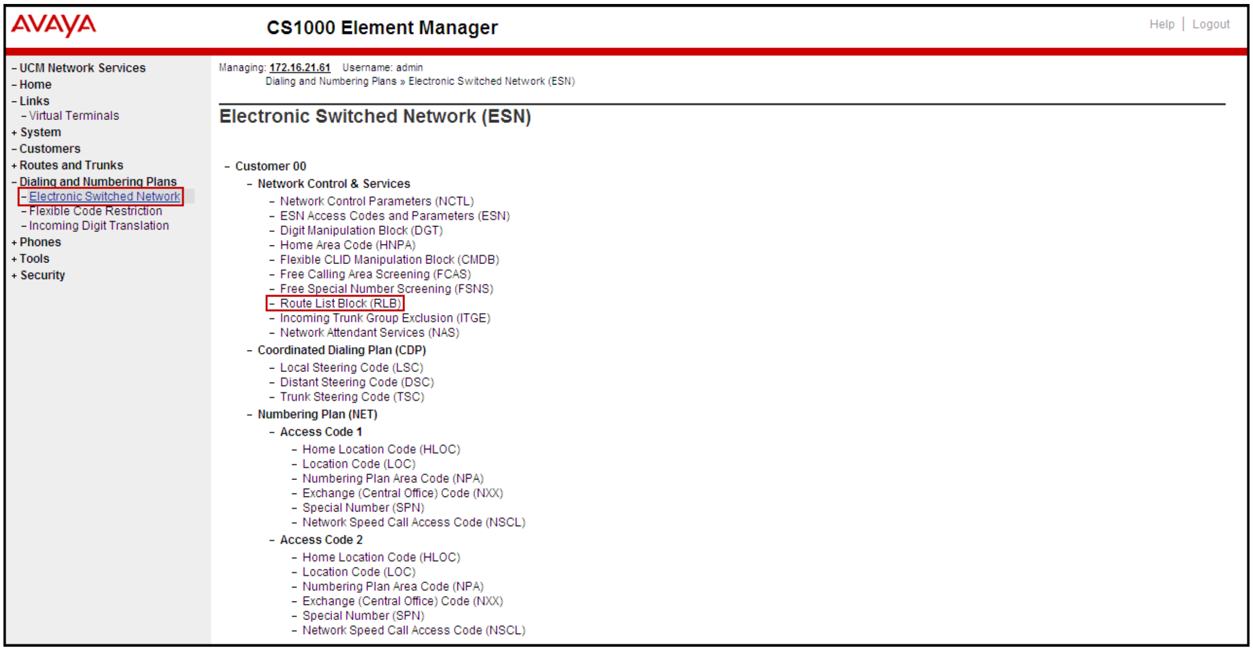


Enter **0** for the **Number of leading digits to be deleted** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits** and then click **Submit** as shown below.



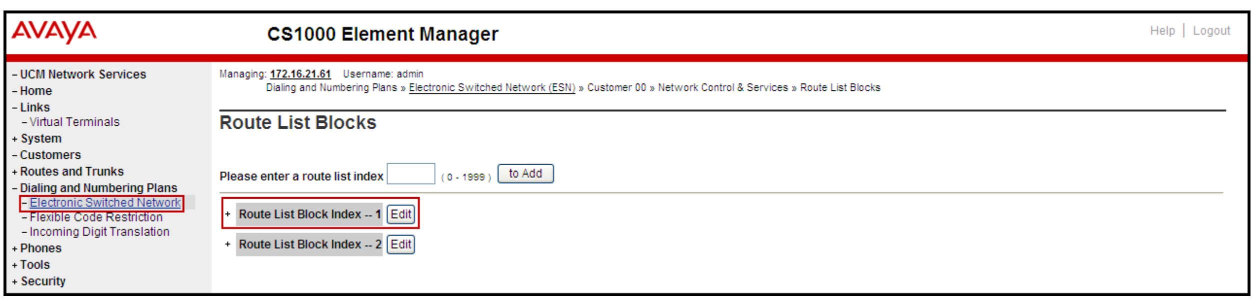
5.6.4. Route List Block (RLB)

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



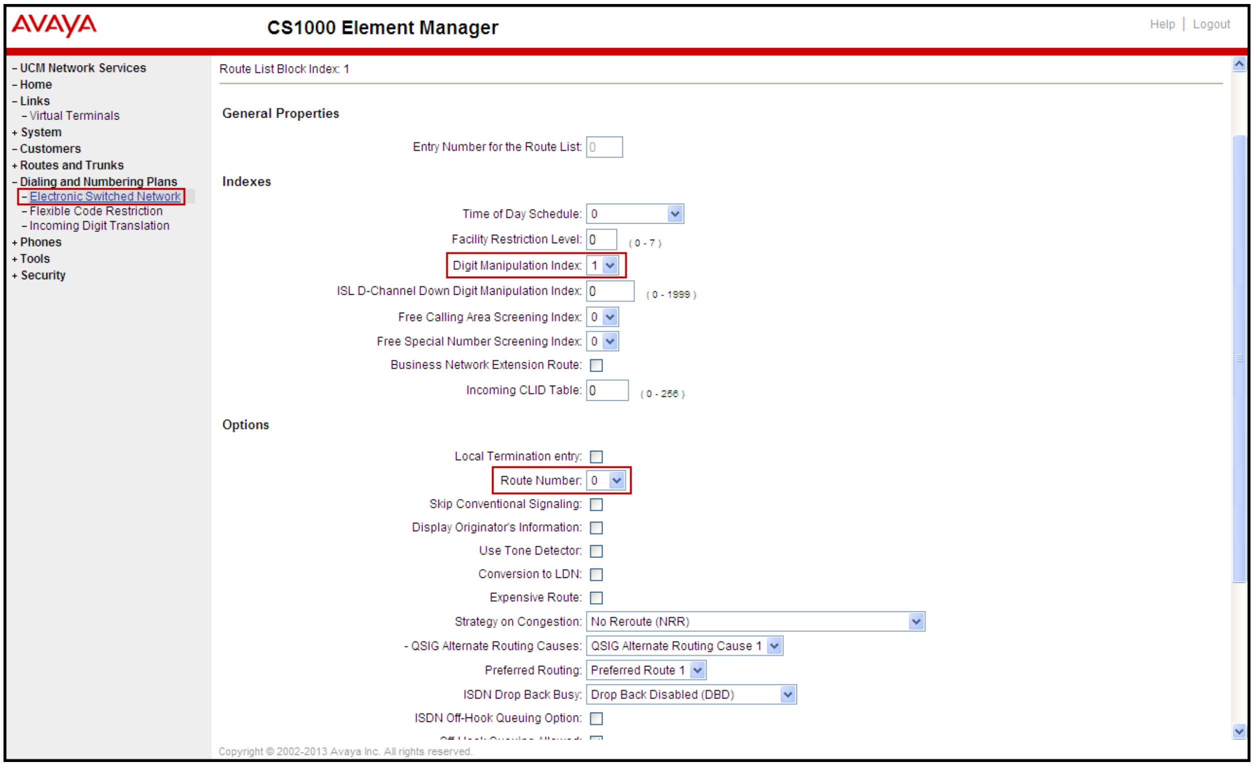
Enter an available value in the **Please enter a route list index** and click on the "**to Add"** button as shown below.

In the example shown below Route List Block Index 1 was previously added.



Enter the following values for the specified fields, and retain the default values for the remaining fields as shown below. Scroll down to the bottom of the screen, and click on the **Submit** button.

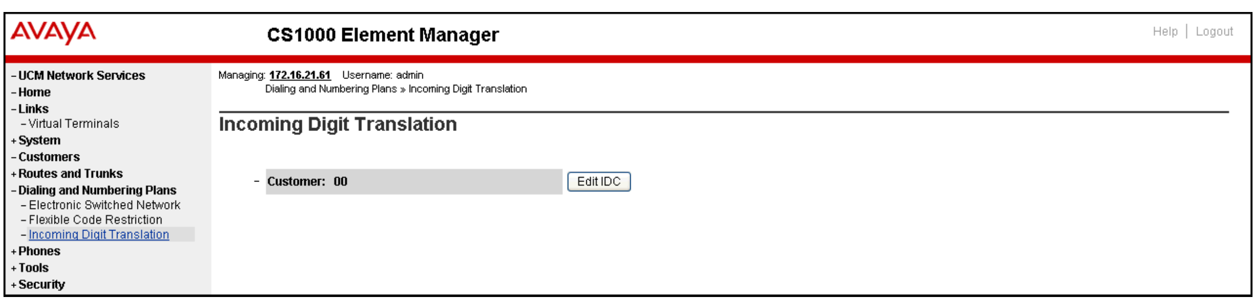
- **Digit Manipulation Index** (DMI): 1 (created in **Section 5.6.3**).
- **Route number** (ROUT): 0 (created in **Section 5.5.4**).



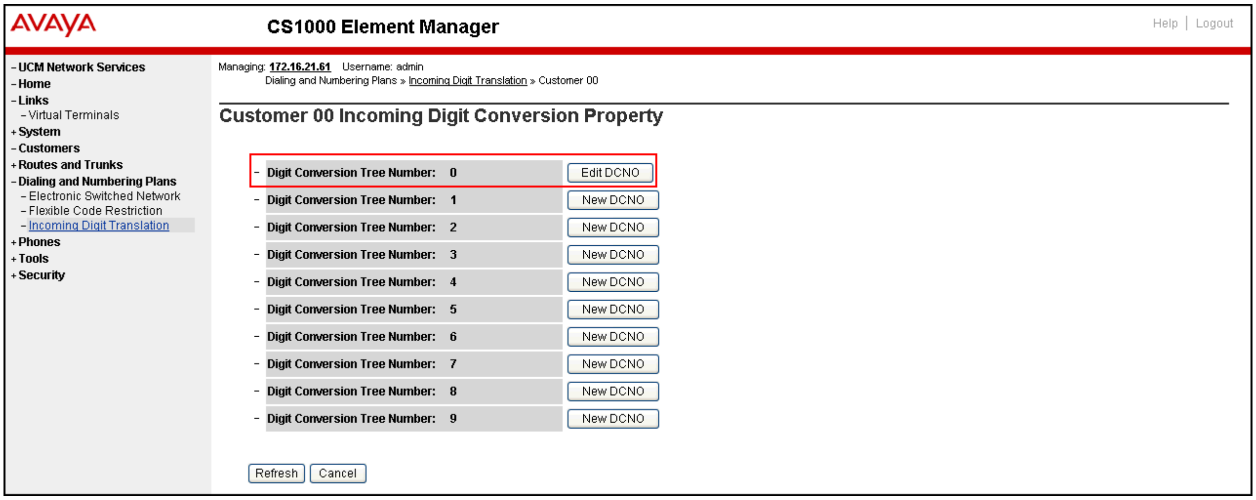
5.6.5. Inbound Digit Translation

This section describes the steps for mapping DID numbers to extensions in the CS1000.

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

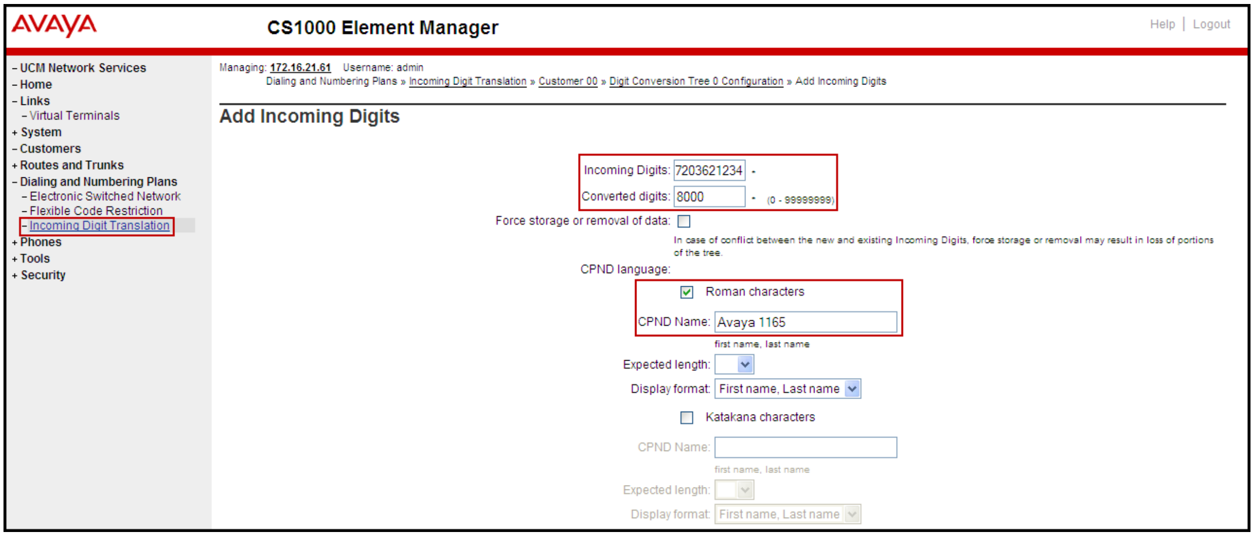


Click on **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number (DCN0) 0** was created as shown below.



Detail configuration of the **DCNO** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 system extension number. This **DCN0** has been assigned to route 0 as shown in **Section 5.5.4**

In the following configuration, the incoming call from PSTN with the prefix 7203621234 will be translated to the CS1000 extension number 8000.

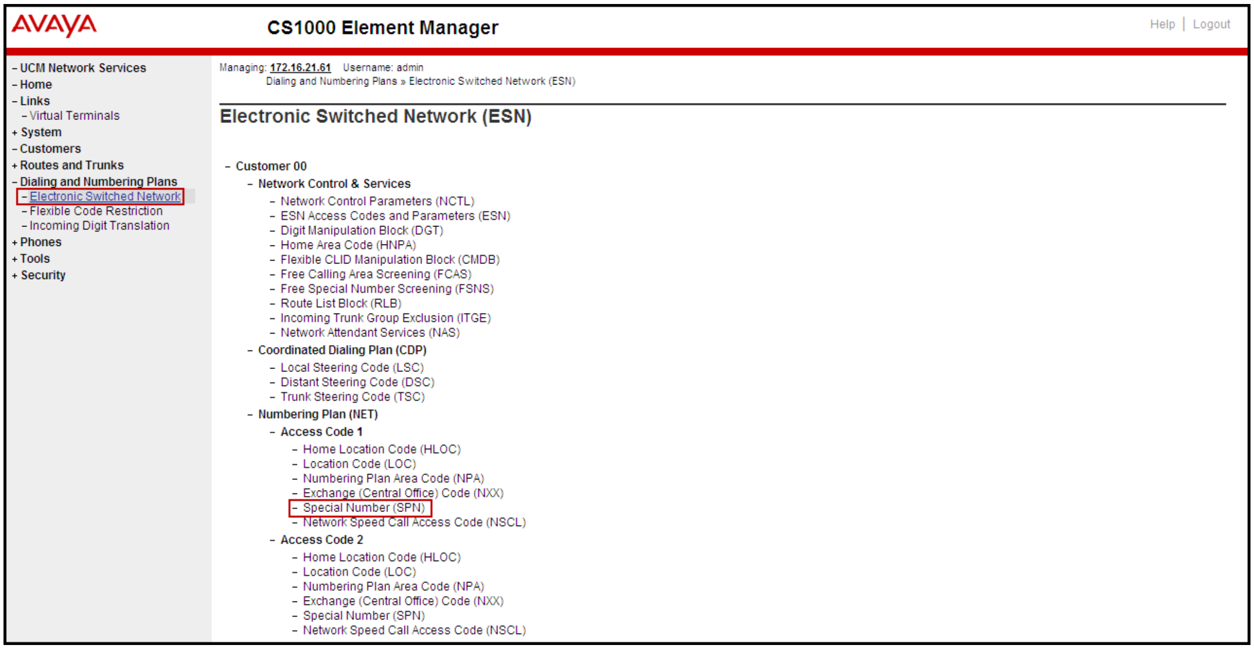


5.6.6. Outbound Call - Special Number Configuration.

There are special numbers which are configured to be used for this testing such as **0** to reach Service Provider operator, **0+10** digits to reach Service Provider operator assistant, **011** prefix for international call, **1** for national long distance call, **411**, **911** and so on. Calls to special numbers shown here are for reference only and may not have been tested for various reasons. Refer to section **Items not supported or not tested** in **Section 2.2.**

Note that for the compliance testing, "1" was added to the Special Number list and was used for national long distance, if the customer prefers, the **Numbering Plan Area Code (NPA)** could be use instead.

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Special Number (SPN)** as shown on the next screen.



Enter **SPN** and then click on the "**to Add**" button.

Special Number: 0

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number).
- **CallType:** NONE.
- **Route list index:** 1, created in **Section 5.6.4.**

Special Number: 011

- **Flexible length:** 15.
- **CallType:** NONE.
- **Route list index:** 1, created in **Section 5.6.4.**

Special Number: 1

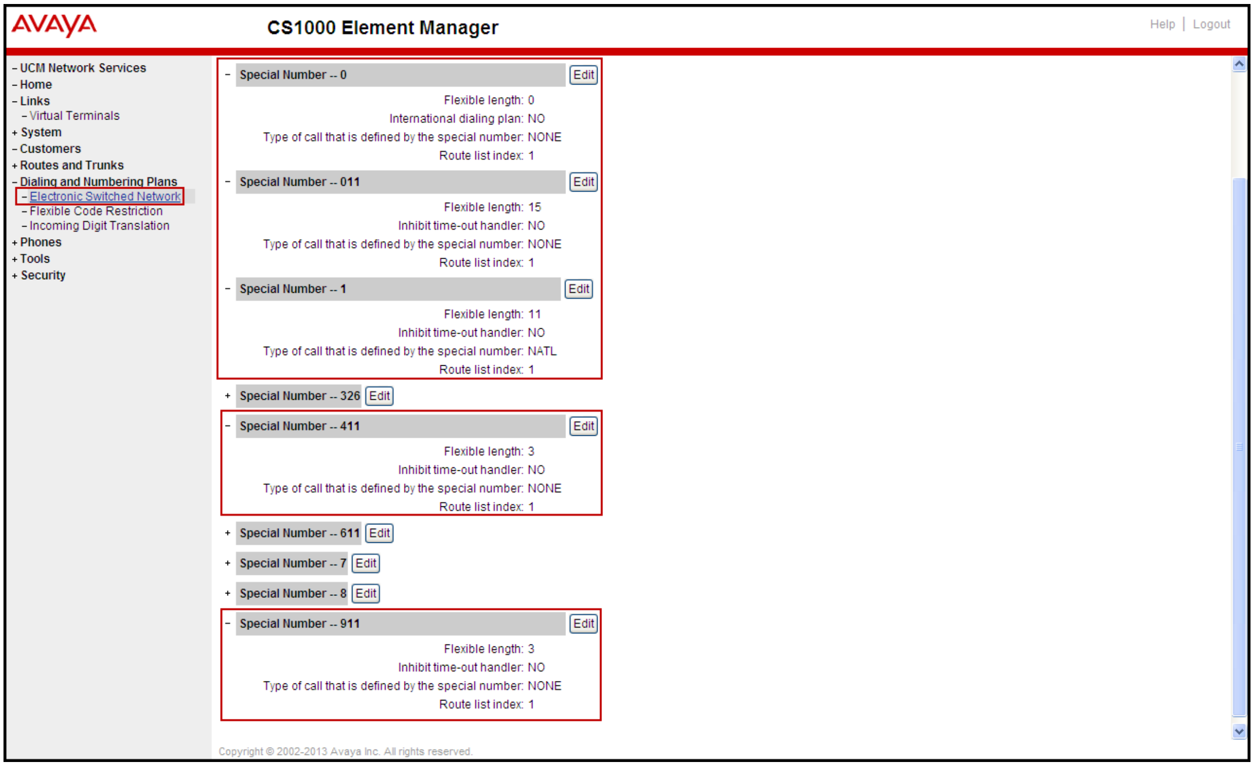
- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number).
- **CallType**: NATL.
- **Route list index**: 1, created in **Section 5.6.4.**

Special Number: 411

- **Flexible length**: 3.
- **CallType**: None.
- **Route list index**: 1, created in **Section 5.6.4.**

Special Number: 911

- **Flexible length**: 3.
- **CallType**: None.
- **Route list index**: 1, created in **Section 5.6.4.**



5.6.7. Outbound Call - Numbering Plan Area Code (NPA)

The **Numbering Plan Area Code (NPA)** was not used for Outbound Calls. The **Special Number 1** defined above in **Section 5.6.6** allows the user to dial any Numbering Plan Area Code (NPA) when dialing **9+1.**

5.7. Administer Phone

This section describes the addition of the CS1000 extension used during the testing.

5.7.1. Phone creation

Refer to **Section 5.5.3** to create a virtual super-loop - **8** used for IP phone.
Refer to **Section 5.4.1** to create a bandwidth zone - **5** for IP phone.

For CS1000 FAX over IP Support recommendation, refer to the Avaya Product Support Notice (PSN) listed in **Section 10** [7], including the "**Analog Station provisioning for T.38** section" and "**Minimum Vintage Loadware Recommendation"** for MGC.

Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail).
Create an IP phone using **Unified Communications Management (UCM) or LD 11**.

Not all fields are shown in the example below; some of the fields have been cut out for brevity.

```
>ld 11
REQ: prt
TYPE: 1165
DES  8000
TN   008 0 00 00  VIRTUAL
TYPE 1165
CDEN 8D
CTYP XDLC
CUST 0
CFG_ZONE 00005
CUR_ZONE 00005
TGAR 0
LDN  NO
NCOS 5
CAC_MFC 0
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDD
     CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBD
     ICDA CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDD CFXA ARHD CLTD ASCD
     CPFA CPTA ABDD CFHA FICD NAID DNAA BUZZ
     UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
     KEM3 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD VMSA
CPND_LANG ENG
RCO  0
EFD  91786331[illegible]
HUNT 91786331[illegible]
EHT  91786331[illegible]
DNDR 0
KEY  00 SCR 8000 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Avaya, 1165_Uni
            XPLN 14
            DISPLAY_FMT FIRST,LAST
        ANIE 0
     01 CWT
     02
     31
```

5.7.2. Enable Privacy for Phone

This section shows how to enable or disable Privacy for a phone by changing its class of service (CLS); changes can be made by using **Unified Communications Management (UCM)** or **LD 11**. By modifying the configuration of the phone created in **Section 5.7.1**, the display of the outbound call will be changed appropriately. The privacy for a single call can be done by configuring per-call blocking and a corresponding dialing sequence, for example *67. The resulting SIP privacy setting will be the same in either case.

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

```
REQ: chg
TYPE: 1110
TN   8 0 0 1
ECHG yes
ITEM cls namd
ITEM
```

To hide display number, set CLS to **ddgd**. The CS1000 will include "Privacy:id" in SIP message header before sending to Service Provider.

```
REQ: chg
TYPE: 1110
TN   8 0 0 1
ECHG yes
ITEM cls ddgd
ITEM
```

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

```
REQ: chg
TYPE: 1110
TN   8 0 0 1
ECHG yes
ITEM cls namd ddgd
ITEM
```

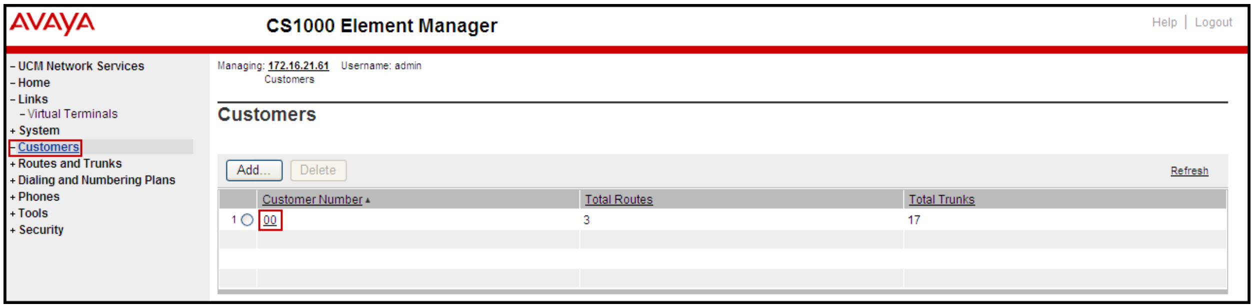
To allow display name and number, set CLS to **nama, ddga**. The CS1000 will send header "Privacy:none" to Service Provider.

```
REQ: chg
TYPE: 1110
TN   8 0 0 1
ECHG yes
ITEM cls nama ddga
ITEM
```

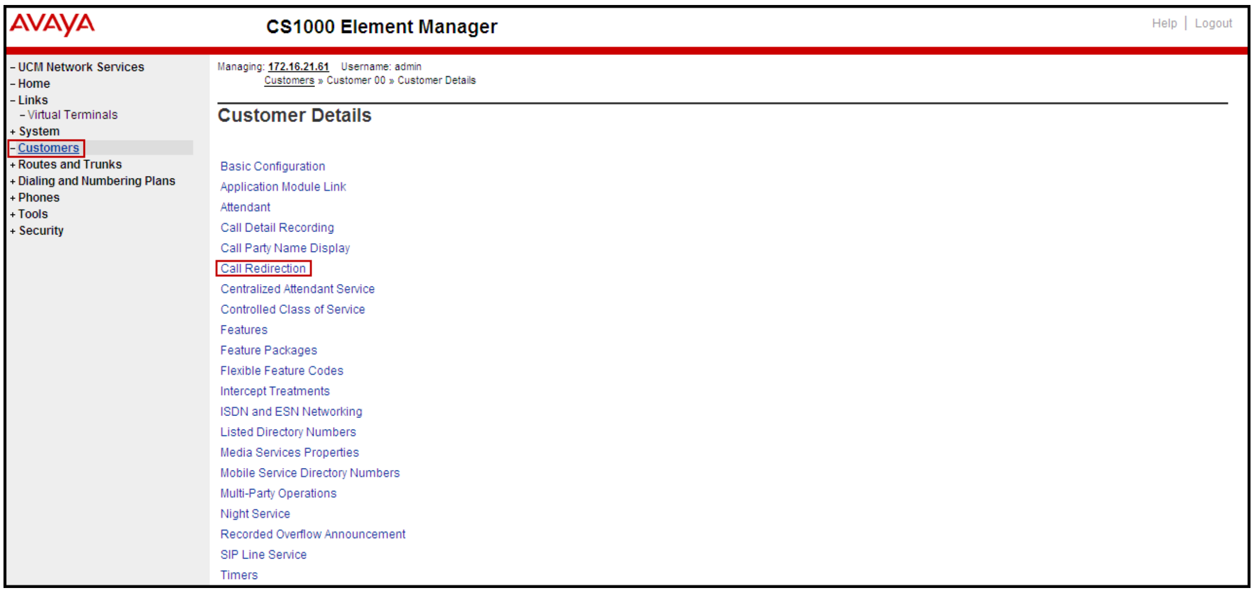
5.7.3. Enable Call Forward for the Phone

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

Select **Customers** from the left pane to display the **Customers** screen as shown below. Select **Customer 00** as shown below.



Select **Call Redirection** as shown below.

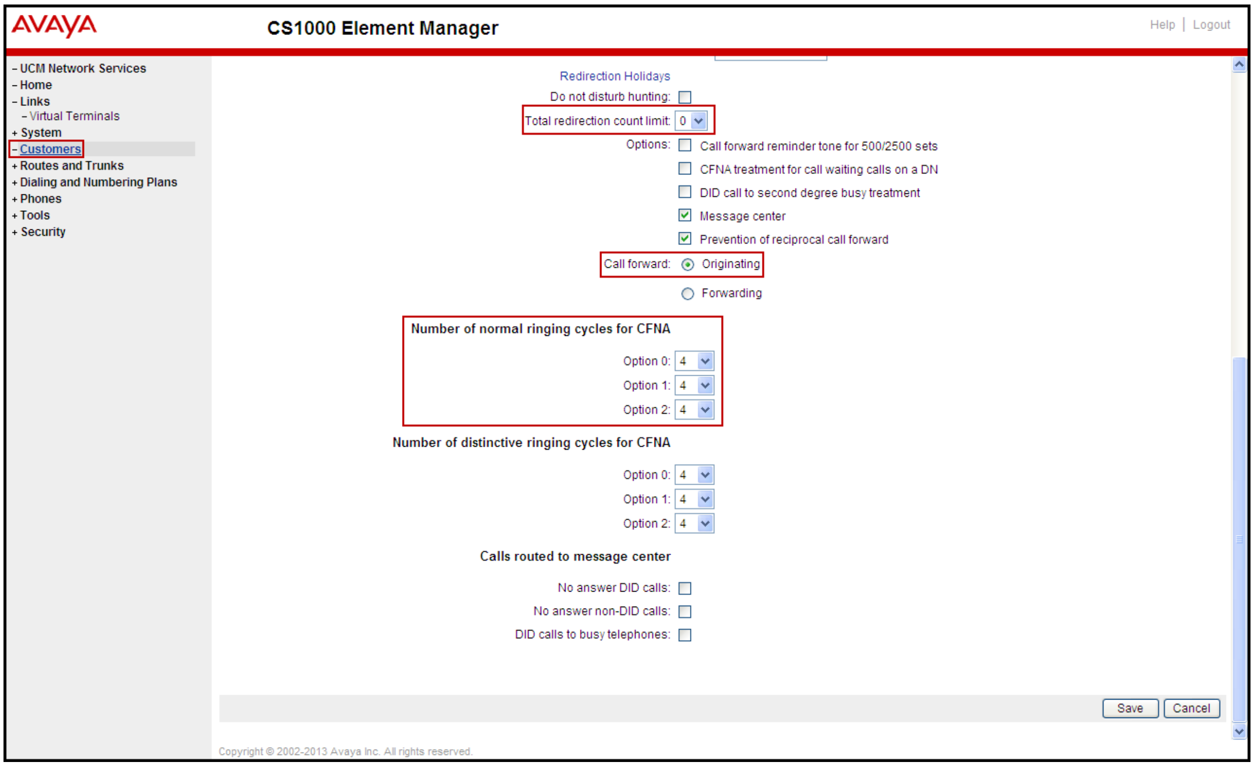


The **Call Redirection** page is displayed as shown below.

Set the following fields:

- **Total redirection count limit**: **0** (unlimited).
- **Call Forward: Originating.**
- **Number of normal ring cycle of CFNA: 4.**

Click on **Save** (not shown)



To enable **Call Forward All Call** (**CFAC**) for the phone over the SIP trunk by using **LD 11**, change its CLS to **CFXA** then program the forward number on the phone set. Following is the configuration of a phone that has CFAC enabled, the phone forwarded to the PSTN number **919195551212**.

```
REQ: prt
TYPE: 2050pc
TN   8 0 0 3
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTA SFD MRD DDV CNIA CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
     UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
     KEM3 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD
......
19 CFW 12  919195551212
```

To enable **Call Forward Busy (CFB)** for the phone over the SIP trunk by using **LD 11**, change its CLS to **FBA, HTA** then program the forward number as **HUNT**. Following is the configuration of a phone that has CFB enabled; the phone is CFB to the PSTN number **919195551212**.

```
REQ: prt
TYPE: 2050pc
TN   8 0 0 3
.....
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTA SFD MRD DDV CNIA CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
     UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
     KEM3 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD
CPND_LANG ENG
RCO  0
EFD  8004
HUNT 919195551212
....
```

To enable **Call Forward No Answer (CFNA)** for the phone over SIP trunk by using **LD 11**, change CLS to **FNA, SFA** then program the forward number as **FDN**. Following is the configuration of a phone that has CFNA enabled; the phone is CFNA to the PSTN number **919195551234**.

```
REQ: prt
TYPE: 2050pc
TN   8 0 0 3
....
FDN  919195551234
....
CLS  UNR FBA WTA LPR MTD FNA HTA TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
     UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
     KEM3 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD
....
```

5.7.4. Enable Call Waiting for the Phone

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

To configure Call Waiting feature for the phone by using **LD 11**, change the CLS to **HTD**, **SWA** and add **CWT** to a key as shown below.

```
REQ: prt
TYPE: 2050pc
TN   8 0 0 3
....
CLS  UNR FBA WTA LPR MTD FNA HTD TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWA LND CNDA
     CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
     UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
     KEM3 MSNV FRA  PKCH MUTA MWTD DVLD CROD ELCD
....
     02 CWT
....
```

6. Configure the Avaya Session Border Controller for Enterprise.

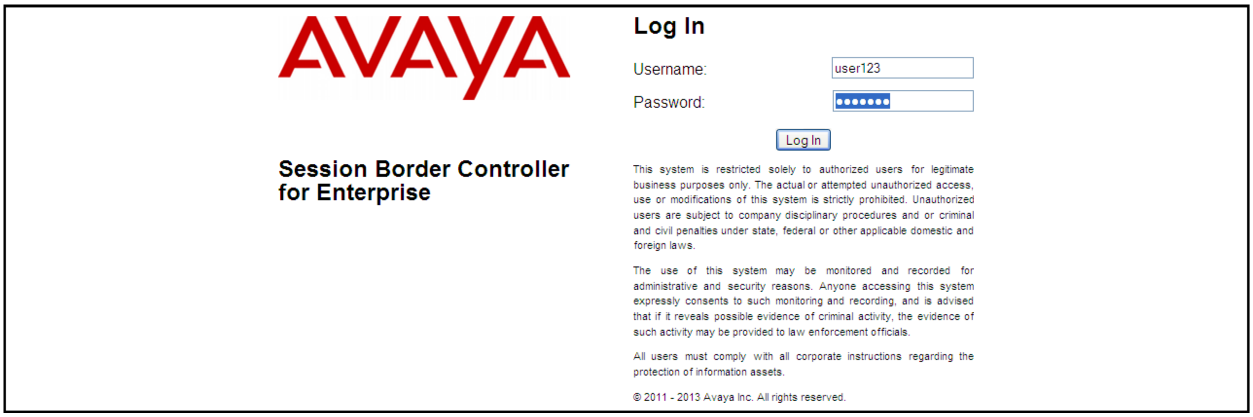
This section describes the required configuration of the Avaya SBCE to connect to CenturyLink SIP Trunk service.

It is assumed that the Avaya SBCE is provisioned and ready to be used on the IP network; the configuration shown here is accomplished using the Avaya SBCE web interface.

6.1. Log in the Avaya SBCE

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

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



6.2. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all devices.

6.2.1. Server Interworking Avaya-CS1000

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned", and then modified to meet specific requirements for the enterprise SIP-enabled solution.

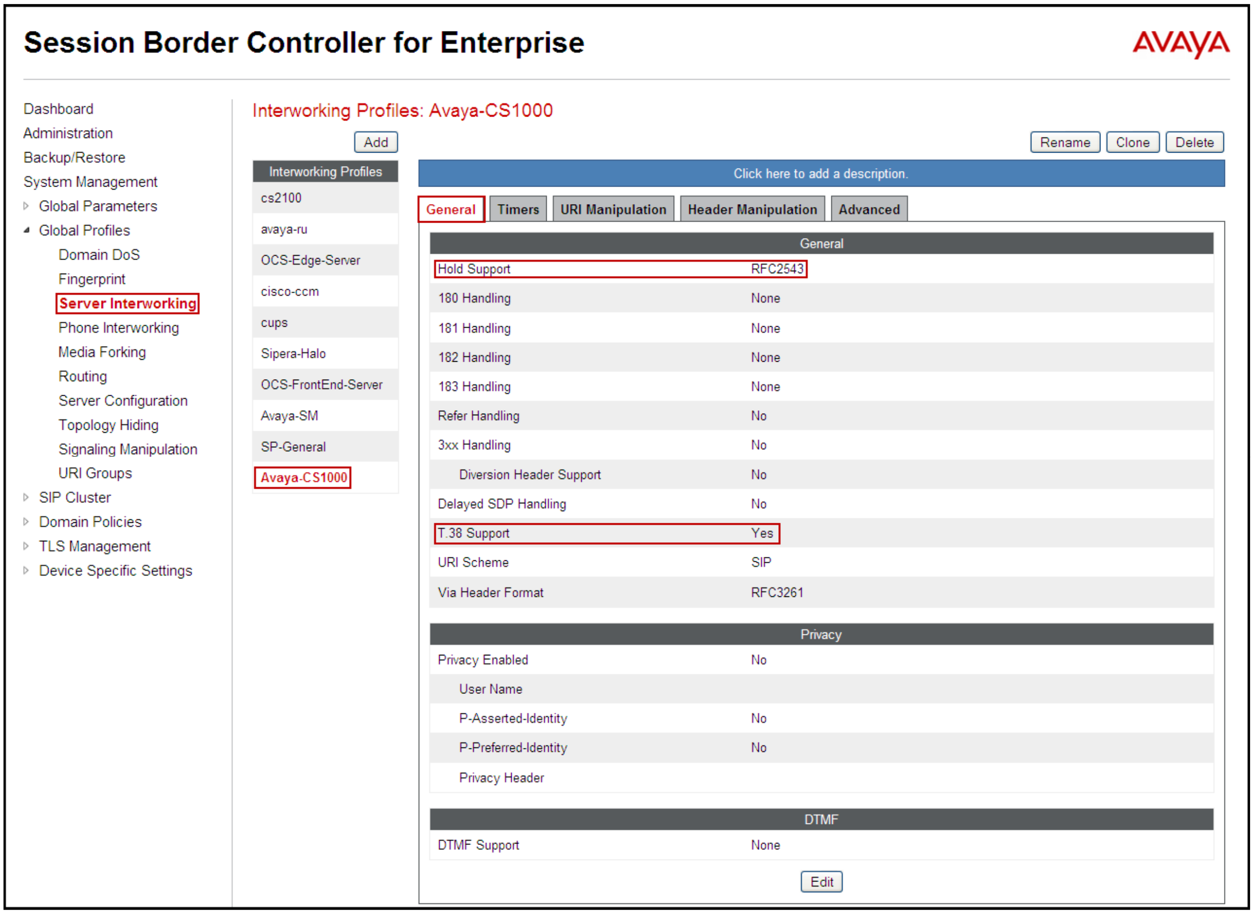
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone Profile.**

Enter the new profile name in the **Clone Name** field, the name of **Avaya-CS1000** was chosen in this example. Click **Finish**.

For the newly created **Avaya-CS1000** profile, click **Edit** (not shown) at the bottom of the General tab

- Verify that for **Hold Support**, **RFC2543** is selected.
- Check **T.38 Support**.
- Click **Next**.
- Click **Finish** on the **Privacy and DTMF** tab.
- Leave other fields with their default values.

The following screen capture shows the newly added **Avaya-CS1000** Profile.



6.2.2. Server Interworking SP-General

A second Server Interworking profile named **SP-General** was created for the Service Provider.

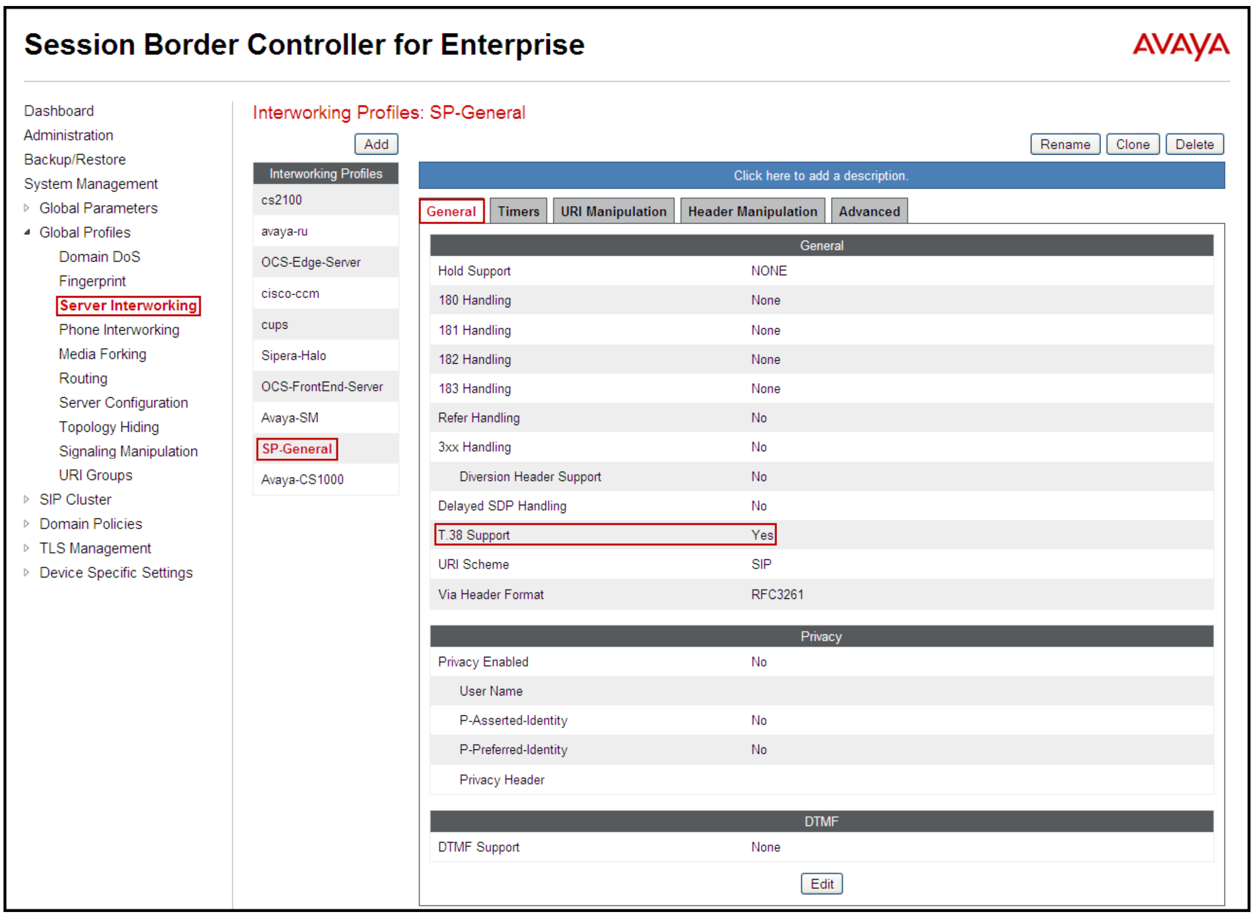
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add.**

Enter the new profile name (not shown), the name of **SP-General** was chosen in this example. Accept the default values for all fields by clicking **Next** and then Click **Finish.**

For the newly created **SP-General** profile, click **Edit** (not shown) at the bottom of the General tab.

- Check **T.38 Support**.
- Click **Next**.
- Click **Finish** on the **Privacy** tab.
- Leave other fields with their default values.

The following screen capture shows the newly added **SP-General** Profile.



6.2.3. Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing Profiles were created in the test configuration, one for inbound calls, with the CS1000 as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

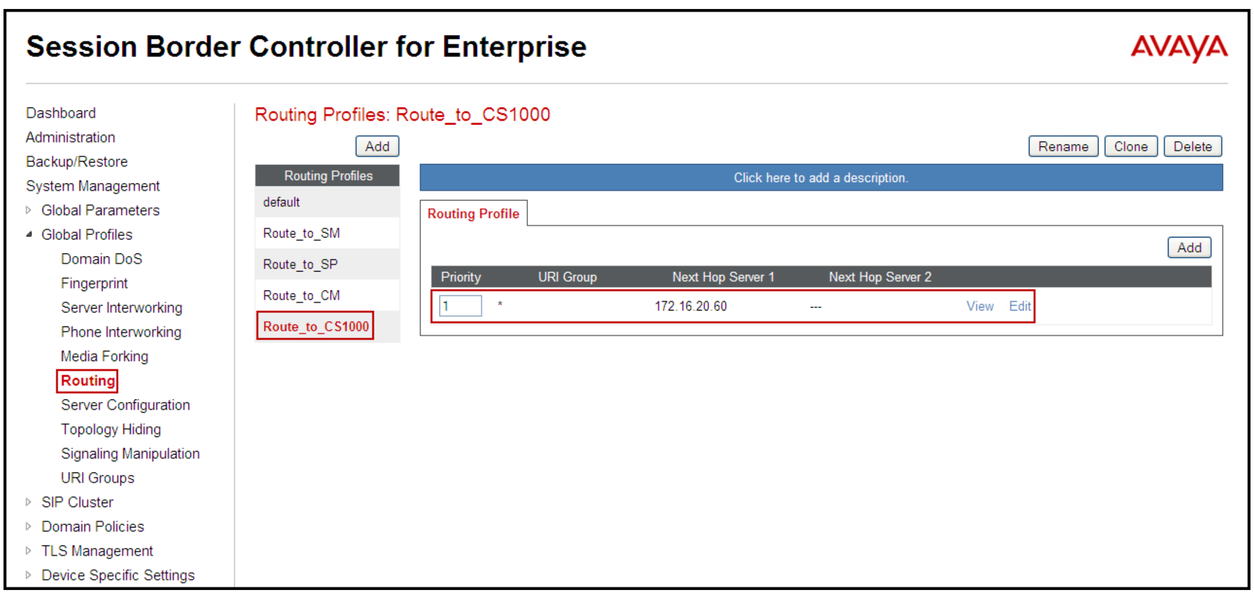
To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select the **Routing** tab.
- Select **Add Profile.**
- Enter Profile Name: **Route_to_CS1000.**
- Click **Next.**

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.20.60** (Node IP address of the CS1000).
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish.**

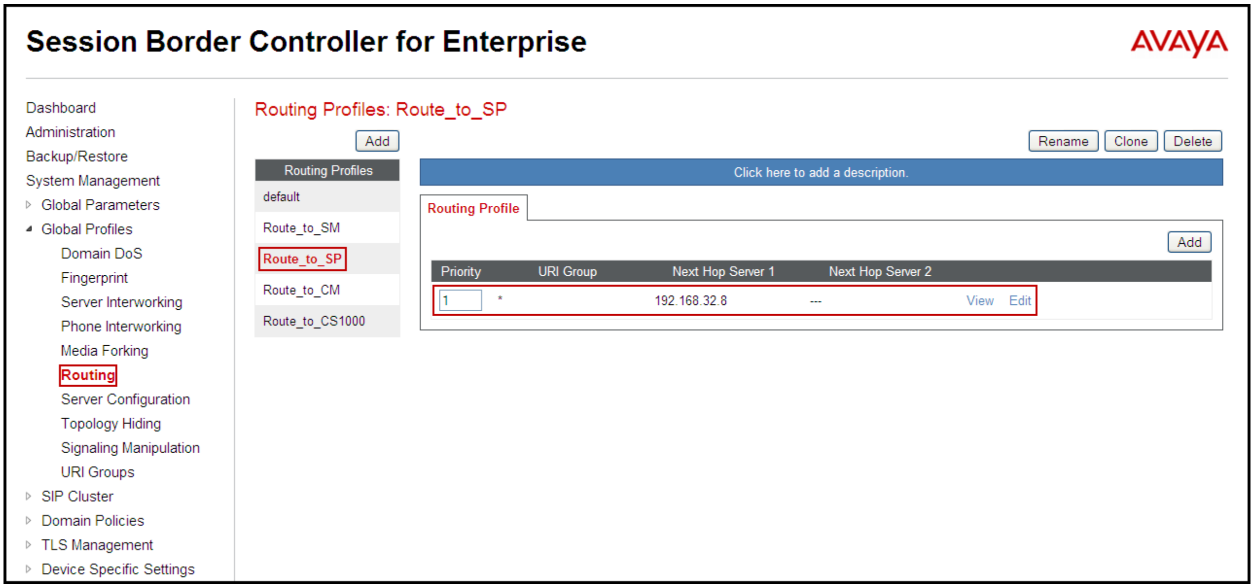
The following screen shows the newly added **Route_to_CS1000** Profile.



Similarly, for the outbound route:

- Select **Add Profile.**
- Enter Profile Name: **Route_to_SP**
- Click **Next.**
- **Next Hop Server 1: 192.168.32.8** (IP address for CenturyLink **SESSION** Trunk Group).
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish.**

The following screen capture shows the newly added **Route_to_SP** Profile.



6.2.4. Server Configuration

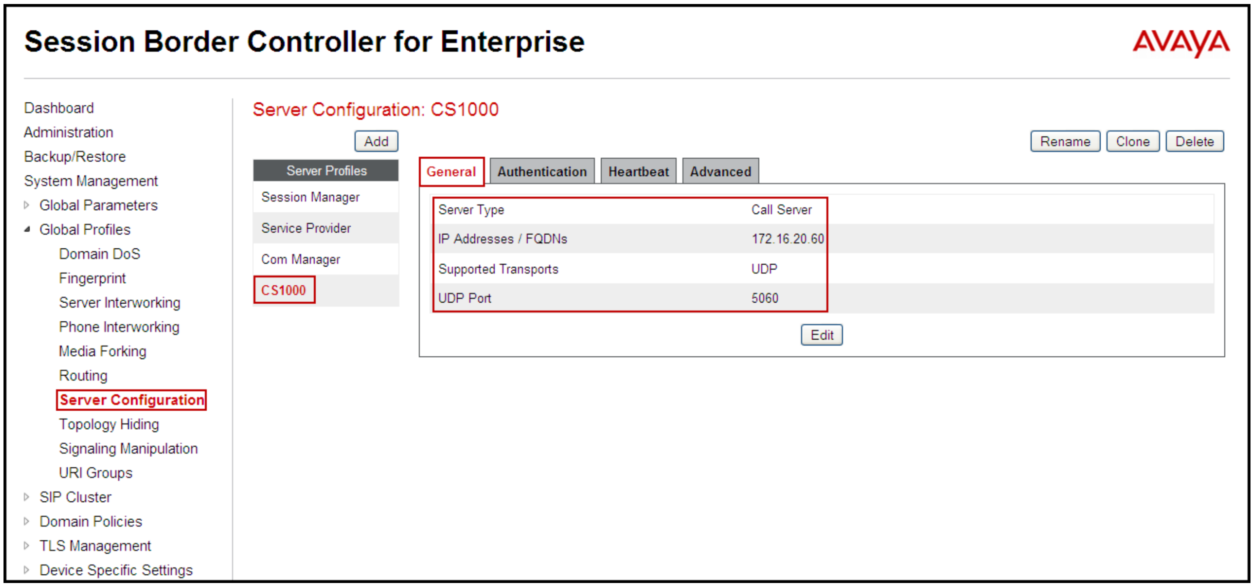
Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (CS1000) and the Trunk Server or SIP Proxy at the service provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add Profile** and enter the profile name: **CS1000**.
On the **Add Server Configuration Profile** Tab:

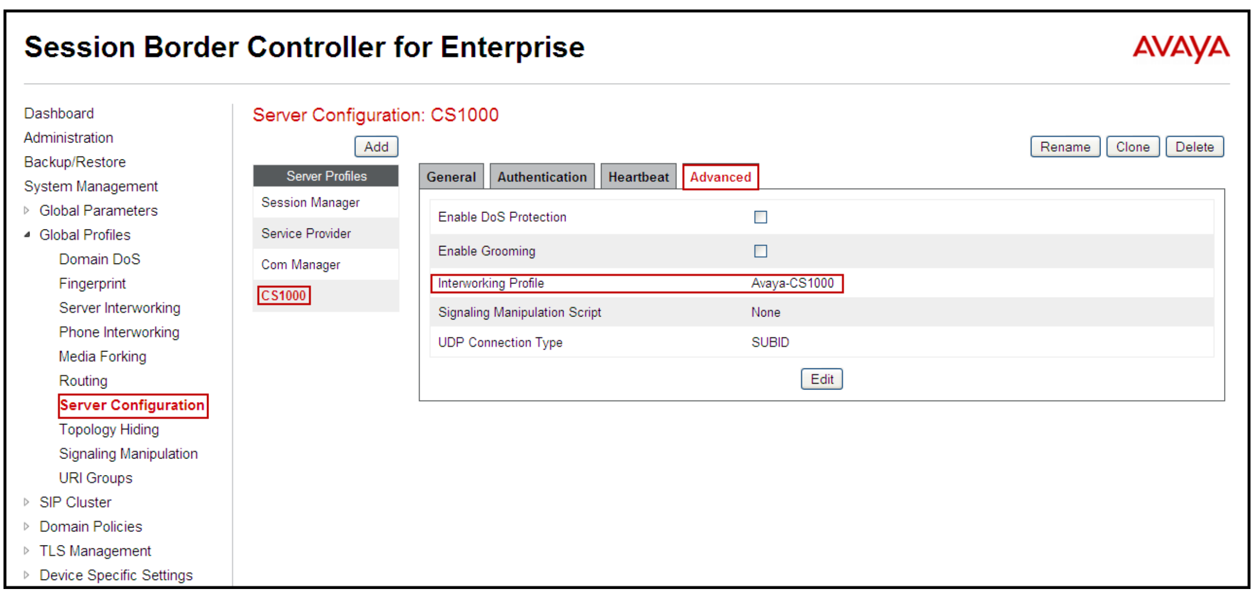
- Select Server Type**: Call Server.**
- **IP Address: 172.16.20.60** (Node IP address of the CS1000).
- **Supported Transports**: Check **UDP**.
- **UDP Port: 5060** (This port must match the far end (CS1000) local port number defined in **Section 5.5.1**).
- Click **Next.**
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.

- On the **Advanced** tab, select **Avaya-CS1000** from the **Interworking Profile** drop down menu.
  Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish.**

The following screen capture shows the **General** tab of the newly added **CS1000** Profile.



The following screen capture shows the **Advanced** tab of the added **CS1000** Profile.

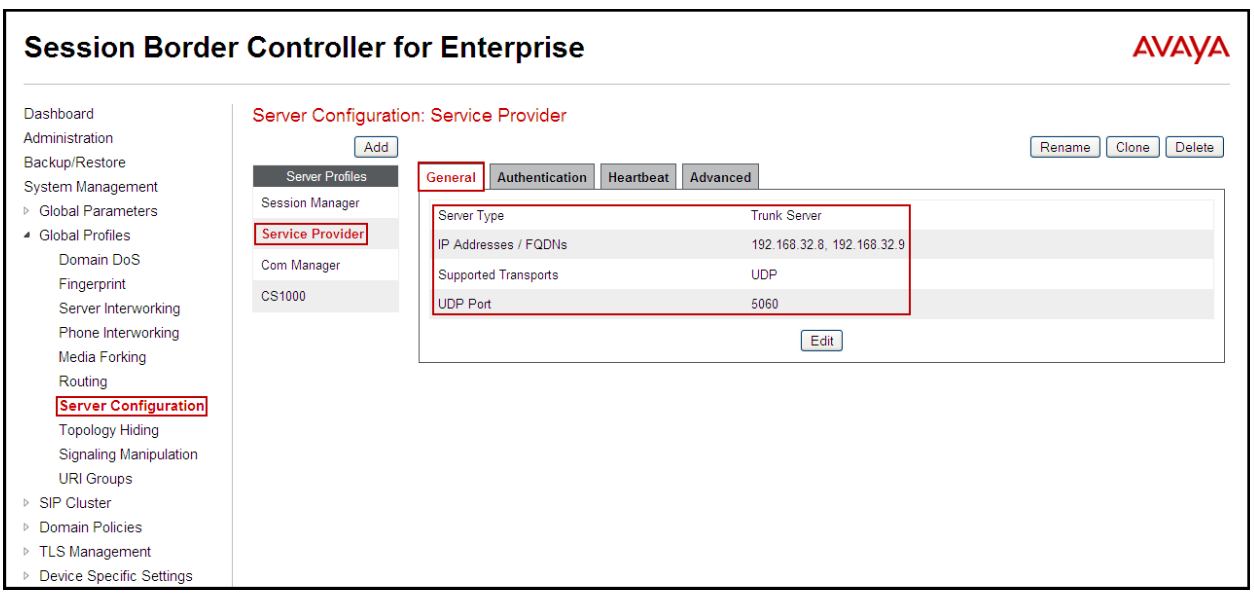


To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add Profile** and enter the profile name: **Service Provider.**

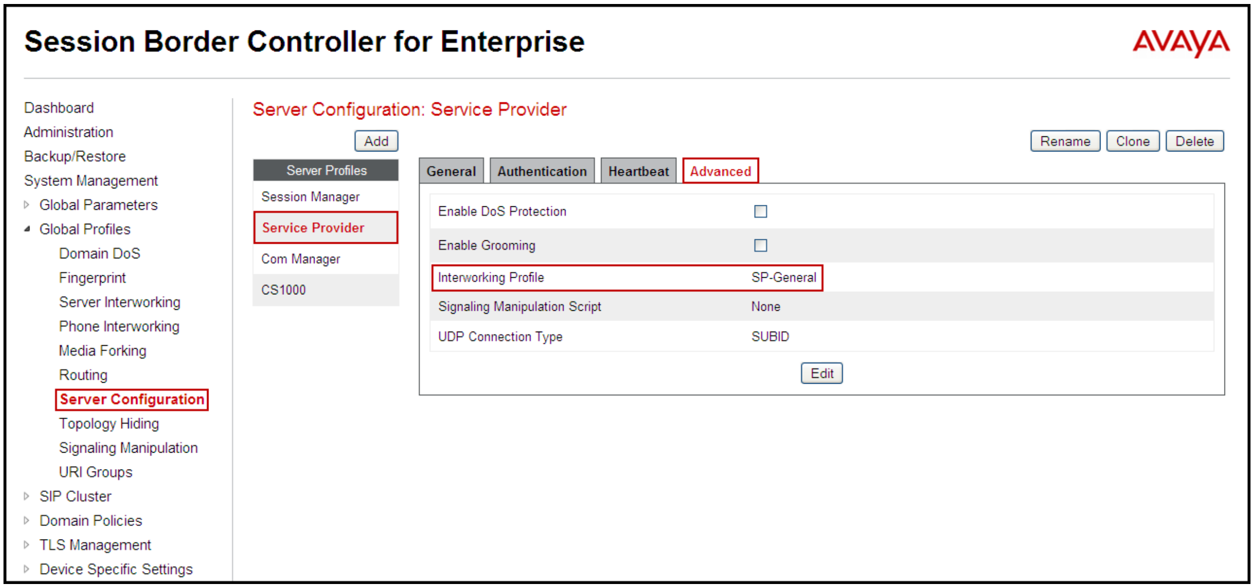
On the **Add Server Configuration Profile** Tab:

- Select Server Type**: Trunk Server.**
- **IP Addresses: 192.168.32.8, 192.168.32.9**
    - **192.168.32.8** (IP address for CenturyLink **SESSION** Trunk Group).
    - **192.168.32.9** (IP address for CenturyLink **USAGE** Trunk Group).
- **Supported Transports**: Check **UDP**.
- **UDP Port: 5060.**
- Click **Next.**
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **SP-General** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**, a Signaling Manipulation Script will be assigned latter.
- Click **Finish.**

The following screen capture shows the **General** tab of the **Service Provider** Profile.



The following screen capture shows the **Advanced** tab of the **Service Provider** Profile.



6.2.5. Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

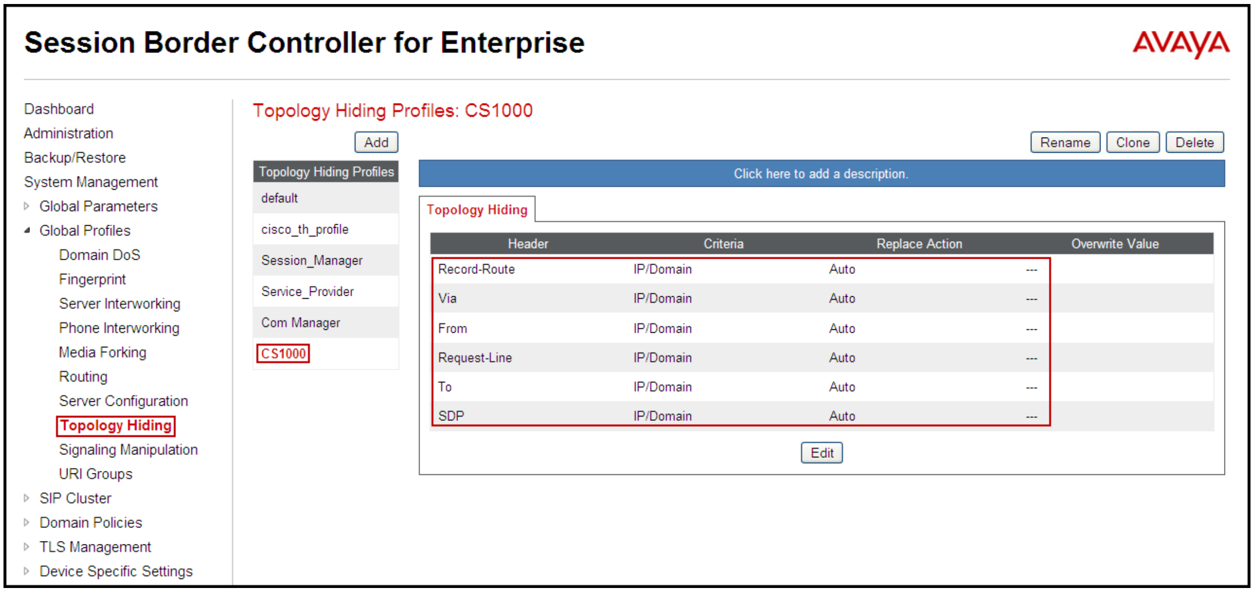
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains names.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile.**
- Enter the **Profile Name**: **CS1000**.
- Click **Finish**.

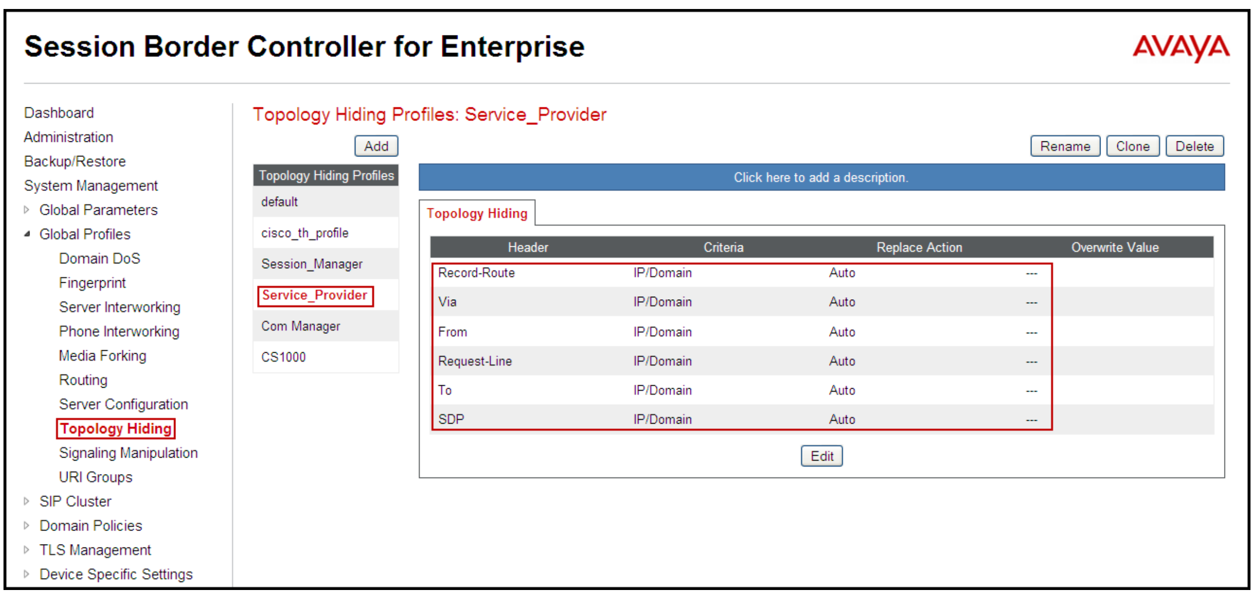
The following screen capture shows the newly added **CS1000** Profile. Note that for the CS1000 profile no values were overwritten (default).



To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**
- Enter the **Profile Name**: **Service_Provider.**
- Click **Finish**.

The following screen capture shows the newly added **Service_Provider** Profile. Note that for the Service Provider no values were overwritten (default).



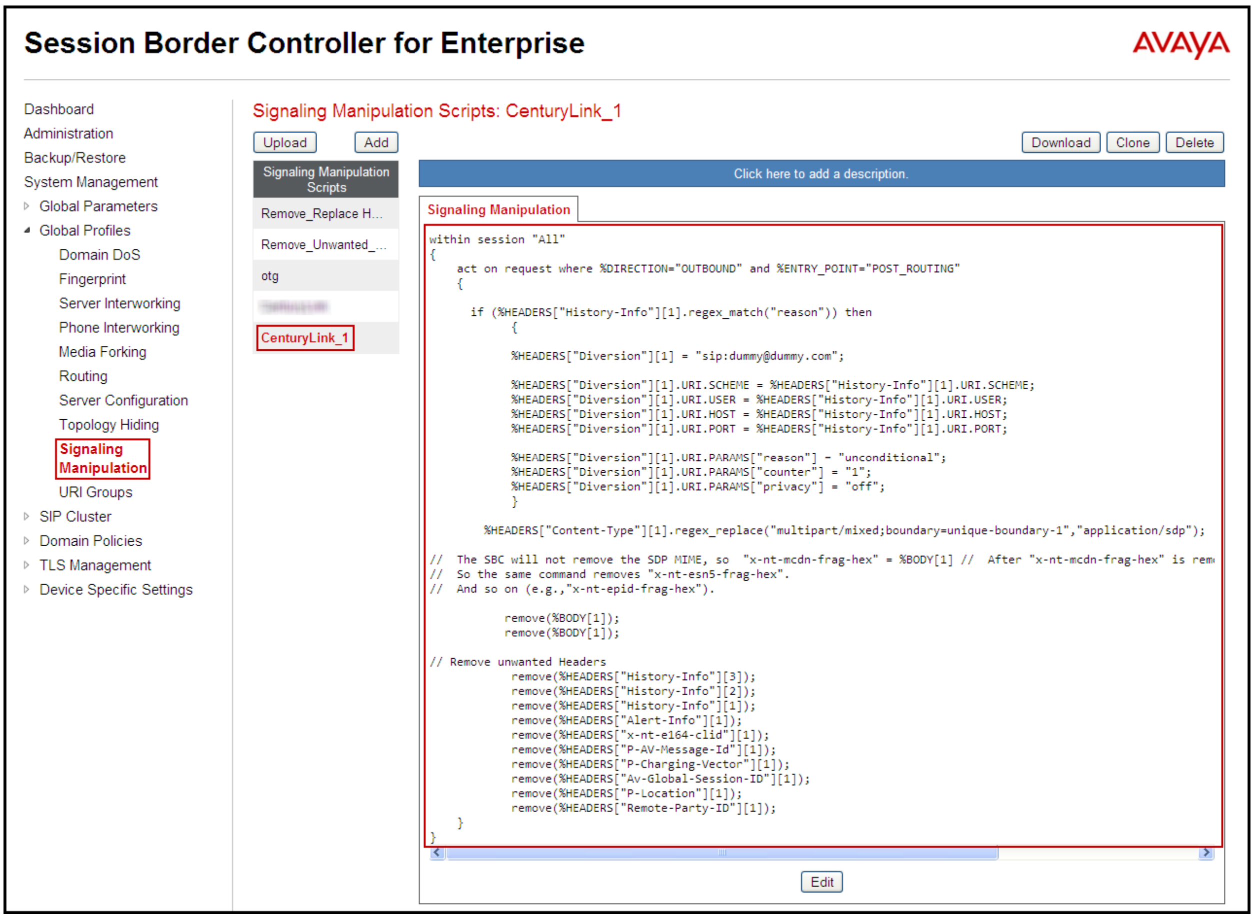
6.2.6. Signaling Manipulation

The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For the test configuration, the Editor was used to create the script needed to handle the header manipulation described below.

The Signaling Manipulation Script shown below is needed to convert History Info to Diversion Header, also to remove unwanted headers and MIME types.

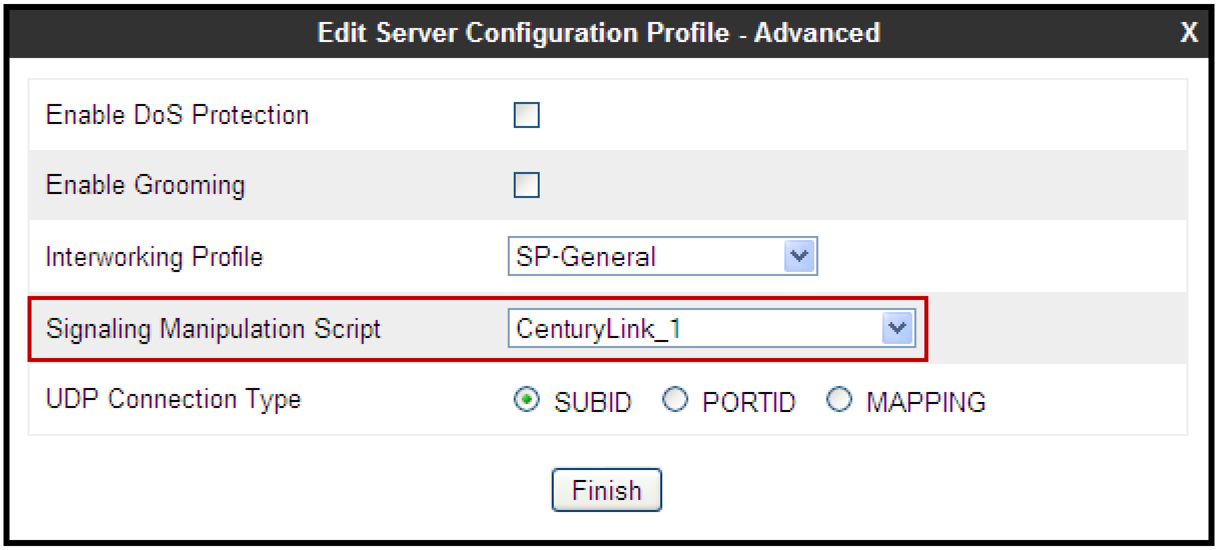
From the **Global Profiles** menu on the left panel (not shown), select **Signaling Manipulation** (not shown). Click on **Add Script** (not shown) to open the SigMa Editor screen (not shown).

- On the **Title** enter a name, the name of **CenturyLink_1** was chosen in this example.
- Enter the script as shown on the screen below (The script can be copied from Appendix A).
- Click **Save**.

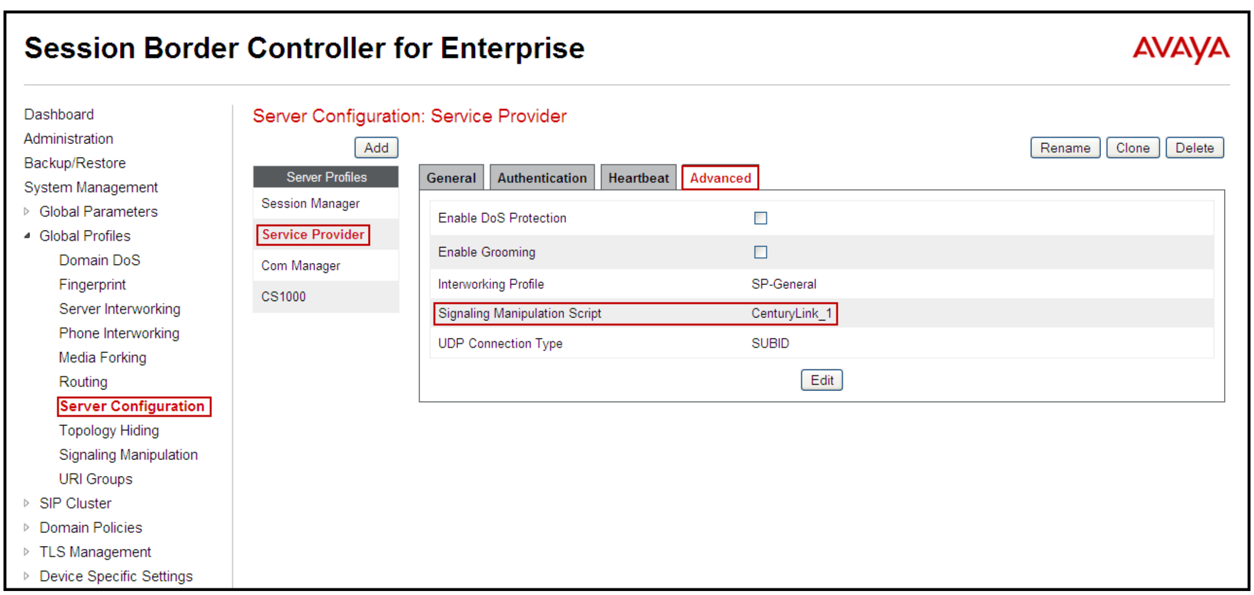


After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 6.2.4.**

Go to **Global Profiles** → **Server Configuration** → **Service Provider** → **Advanced** tab → **Edit**. Select **CenturyLink_1** from the drop down menu on the **Signaling Manipulation Script** field. Click **Finish** to save and exit.



The following screen capture shows the **Advanced** tab of the previously added **Service Provider** Profile with the **Signaling Manipulation Script** assigned.



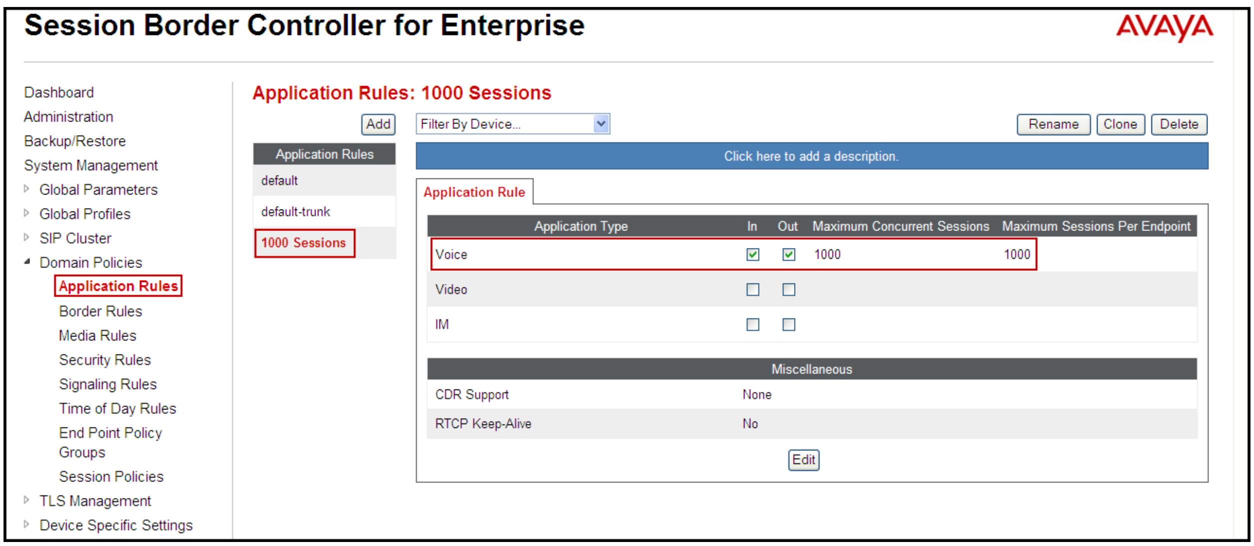
6.3. Domain Policies

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.3.1. Create Application Rules

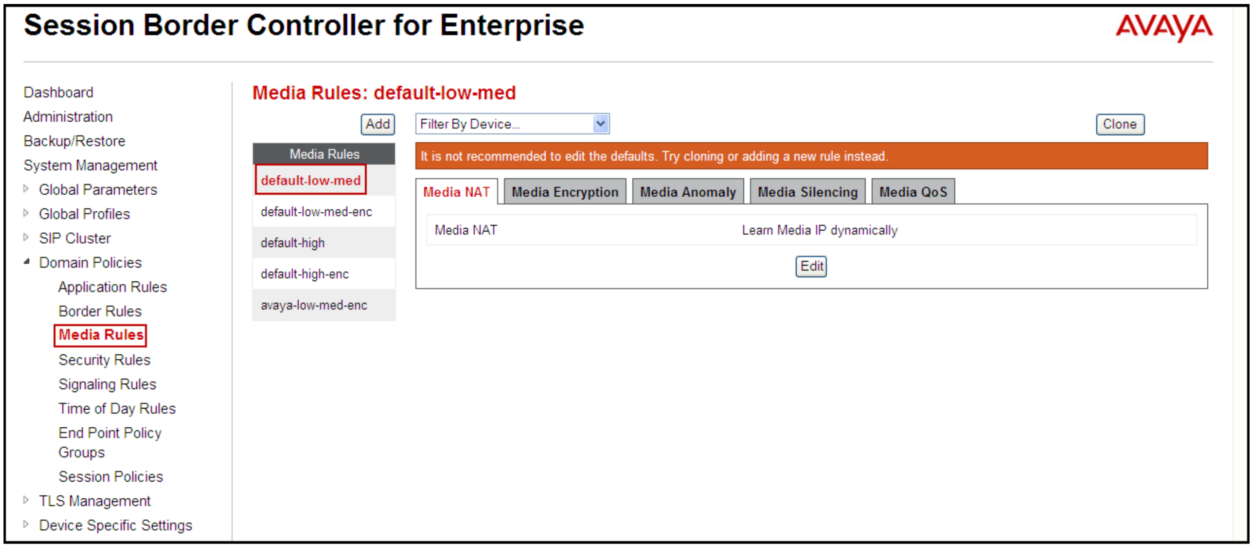
Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies → Application Rules**.

- Select **default** Rule (not shown)
- Select **Clone Rule** button (not shown)
- Name**: 1000 Sessions**
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **1000** was used in the sample configuration.
- Click Finish (not shown).



6.3.2. Media Rules

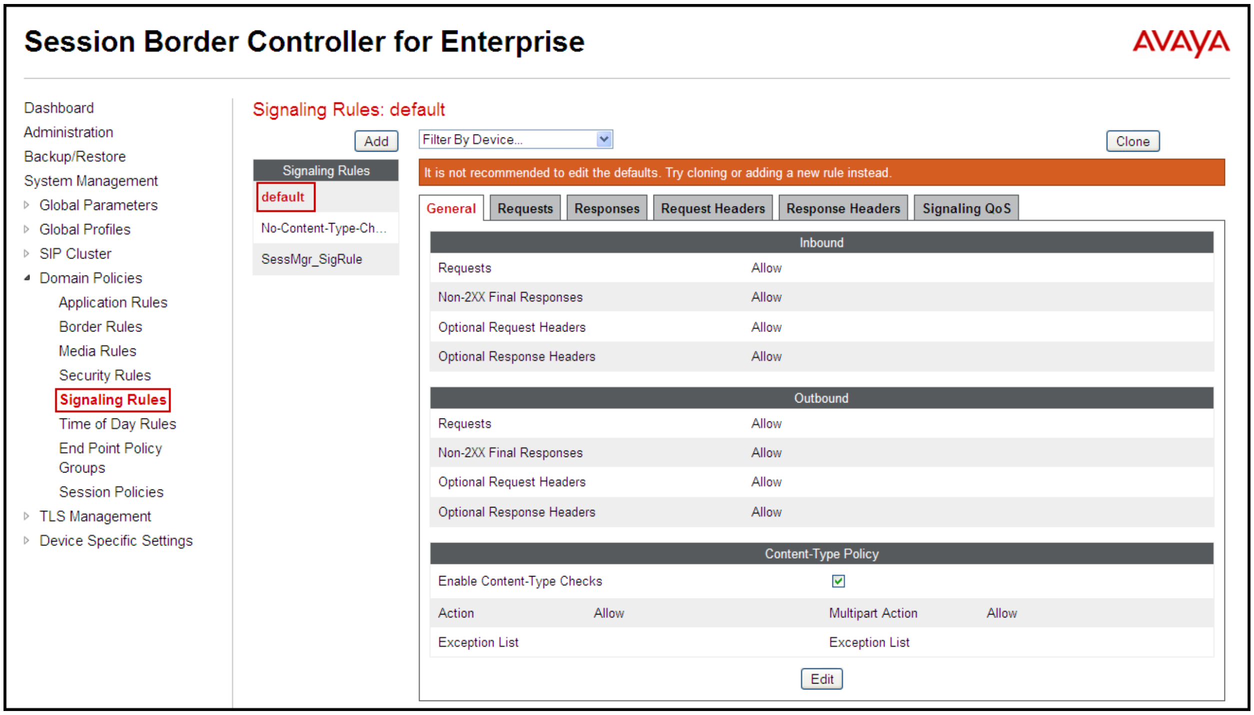
For the compliance test, the **default-low-med** Media Rule was used.



6.3.3. Signaling Rules

Signaling Rules define the actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. They also allow the control of the Quality of Service of the signaling packets.

For the compliance test **default** Signaling Rule was used. The removal of unwanted headers is accomplished by Signaling Manipulation rules defined in **Section 6.2.6**.



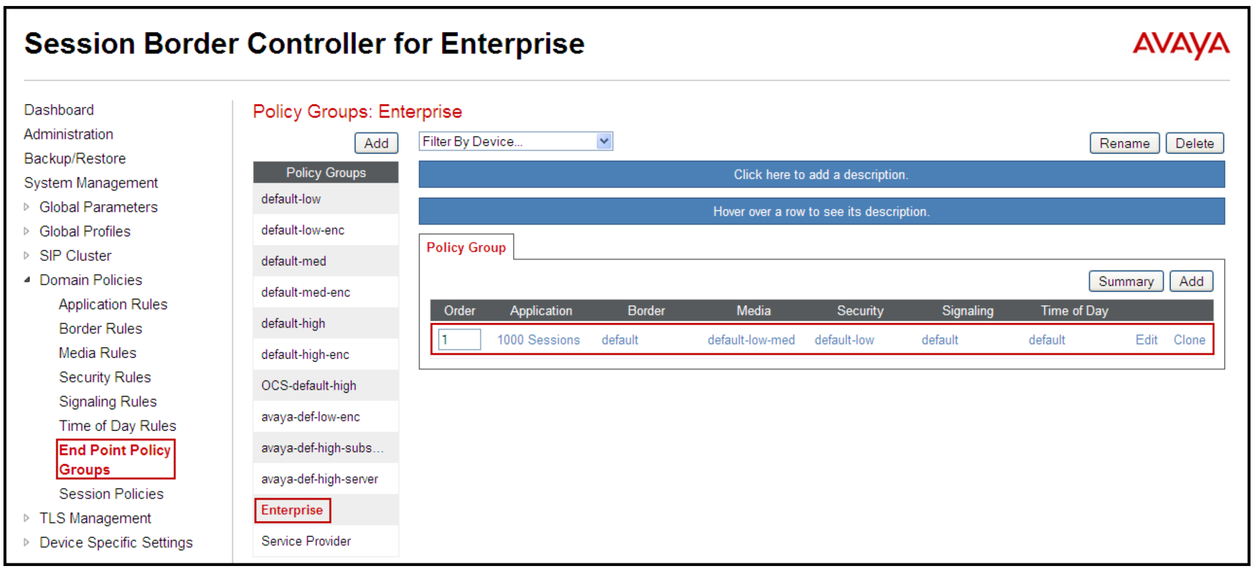
6.3.4. End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add Group**.

- **Group Name: Enterprise**.
- **Application Rule: 1000 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Time of Day: default.**
- Click **Finish**.

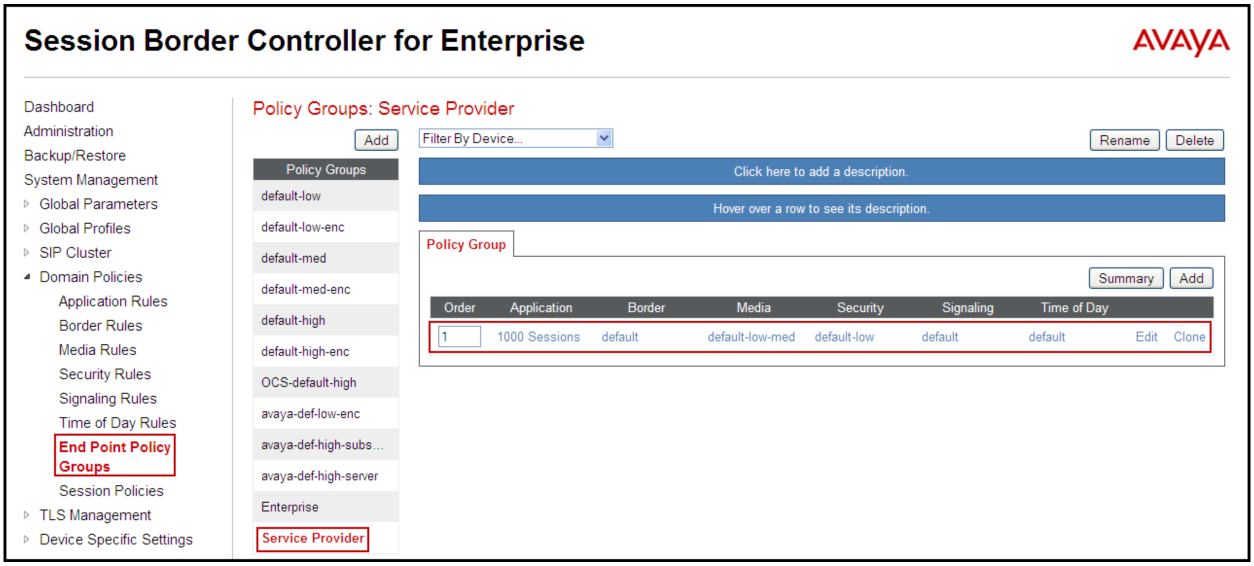
The following screen capture shows the newly added **Enterprise** End Point Policy Group.



Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add Group**.

- **Group Name: Service Provider**.
- **Application Rule: 1000 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Time of Day: default.**
- Click **Finish**.

The following screen capture shows the newly added **Service Provider** End Point Policy Group.



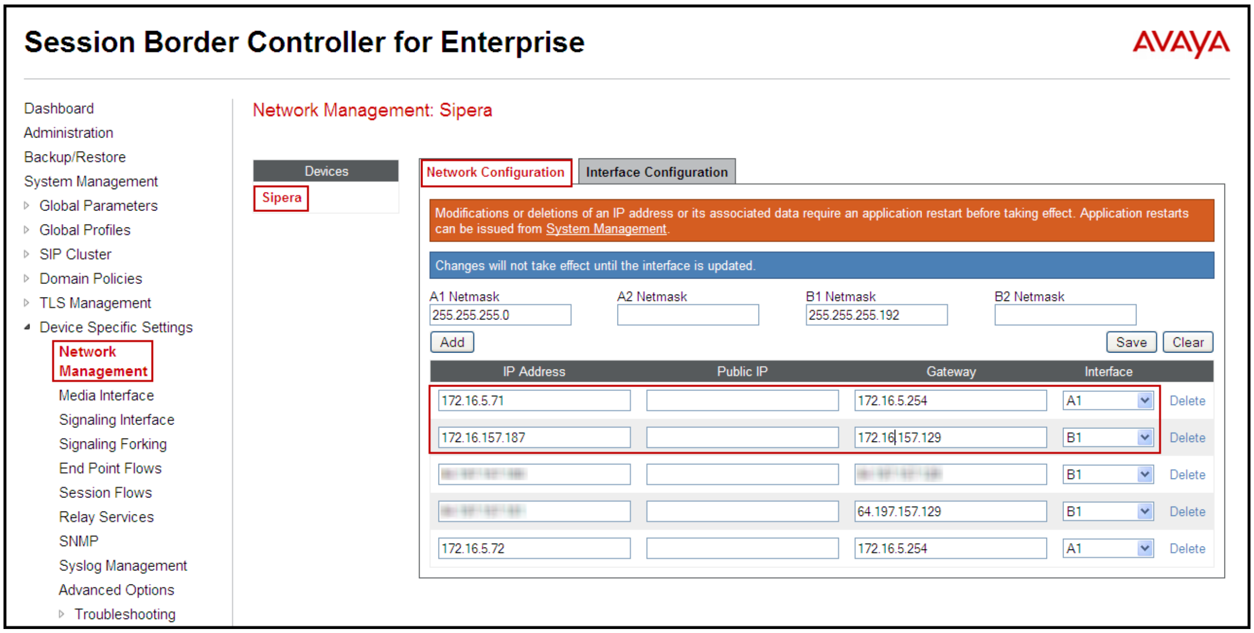
6.4. Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

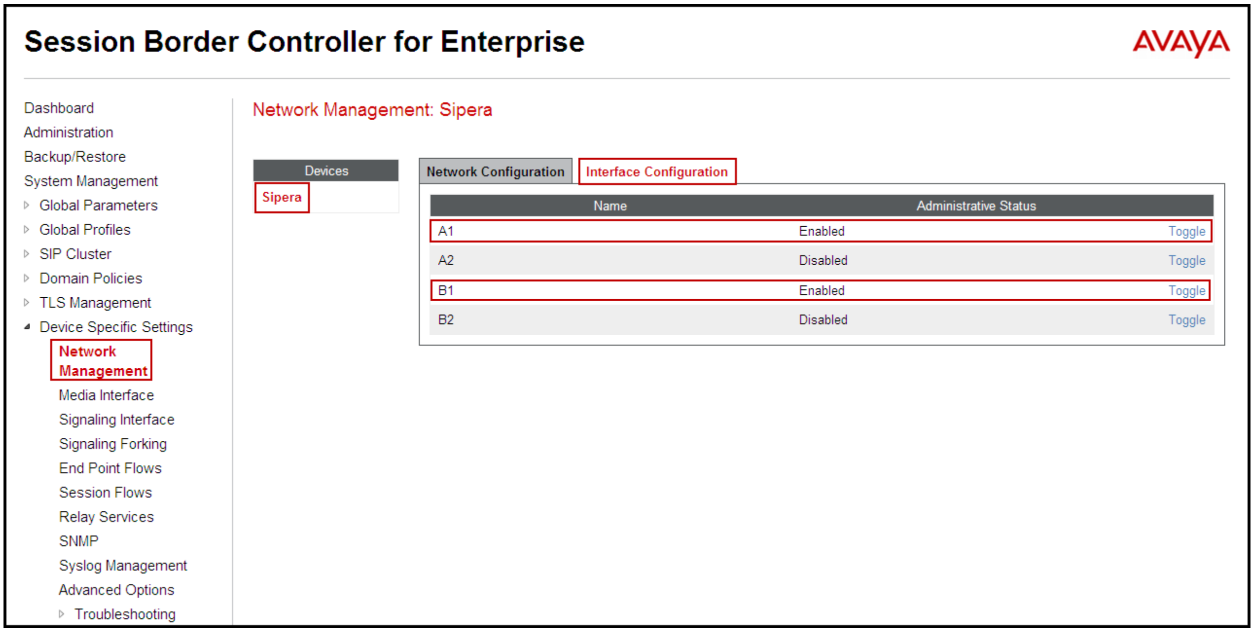
6.4.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Menu** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

In the event that changes need to be made to the network configuration information, they could be entered here.



On the Interface Configuration tab, click the **Toggle State** control for interfaces **A1** and **B1 to** change the status to **Enabled**. It should be noted that the default state for all interfaces is **disabled**, so it is important to perform this step, or the Avaya SBCE will not be able to communicate on any of its interfaces.



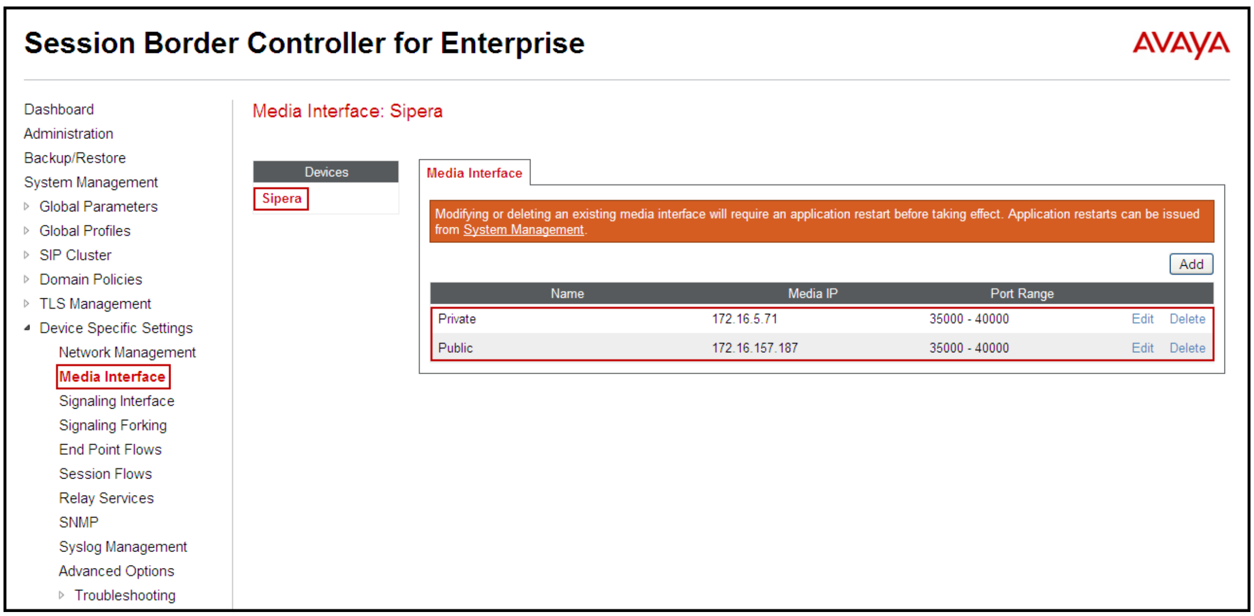
6.4.2. Media Interface

Media Interfaces were created to adjust the port range that the Avaya SBCE will advertise as the listening ports. On the Private and Public interfaces of the Avaya SBCE ports range 35000 to 40000 was used.

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

- Select **Add Media Interface.**
- **Name: Private.**
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward the CS1000).
- **Port Range: 35000-40000.**
- Click **Finish.**
- Select **Add Media Interface.**
- **Name: Public.**
- Select **IP Address: 172.16.157.187** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish.**

The following screen capture shows the added **Media Interfaces**.



6.4.3. Signaling Interface

To create the Signaling Interface toward the CS1000, from the **Device Specific** menu on the left hand side, select **Signaling Interface**

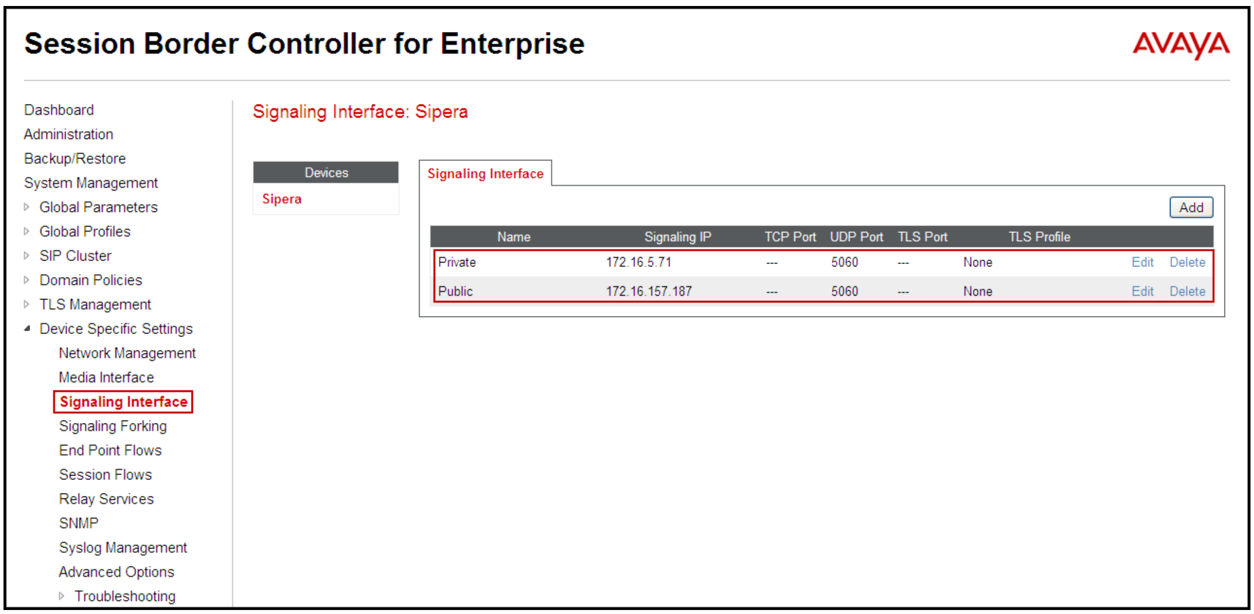
- Select **Add Signaling Interface**:
- **Name: Private.**

- Select **IP Address: 172.16.5.71** (Inside or private IP Address of the Avaya SBCE , toward the CS1000)
- **UDP Port: 5060.**
- **Click Finish.**

To create the Signaling Interface toward the Service Provider, from the **Device Specific** menu on the left hand side, select **Signaling Interface**

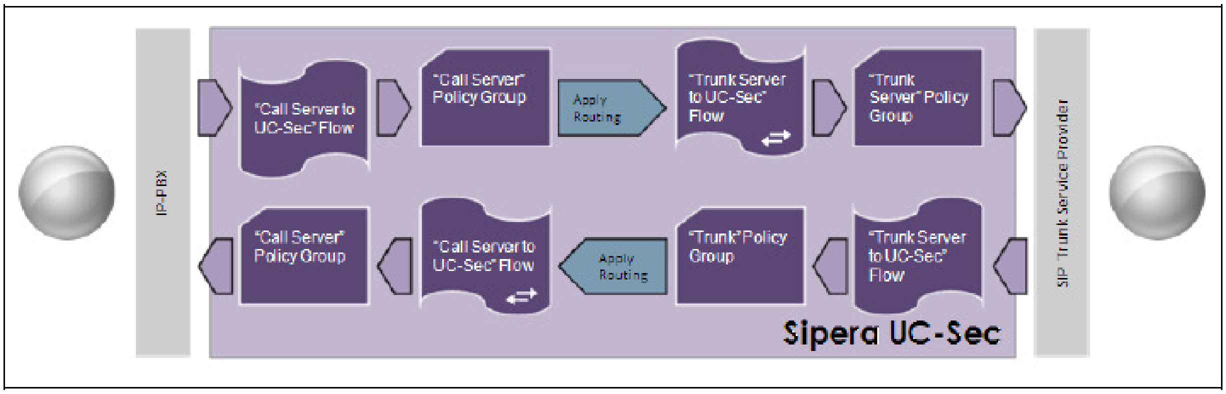
- Select **Add Signaling Interface**:
- **Name: Public**
- Select **IP Address: 172.16.157.187** (Outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- **Click Finish.**

The following screen capture shows the newly added **Signaling Interfaces**.



6.4.4. End Point Flows

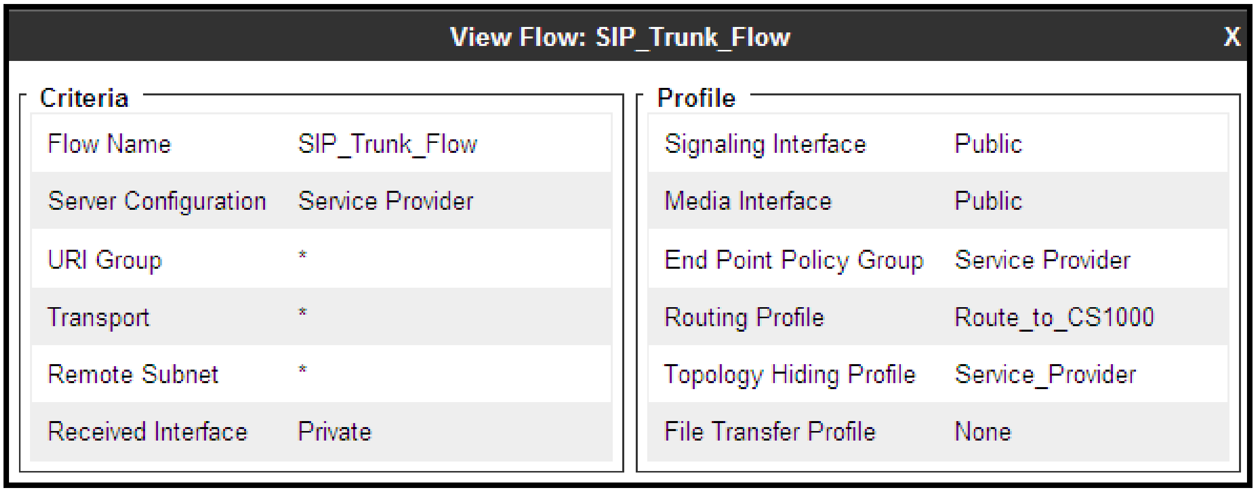
When a packet is received by the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing 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 to secure a SIP Trunk call.



The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, tab **Server Flows**. Click **Add Flow**.

- **Name: SIP_Trunk_Flow.**
- **Server Configuration**: **Service Provider.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private.**
- **Signaling Interface: Public.**
- **Media Interface**: **Public.**
- **End Point Policy Group: Service Provider.**
- **Routing Profile: Route_to_CS1000** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service_Provider.**
- **File Transfer Profile: None.**
- Click **Finish.**



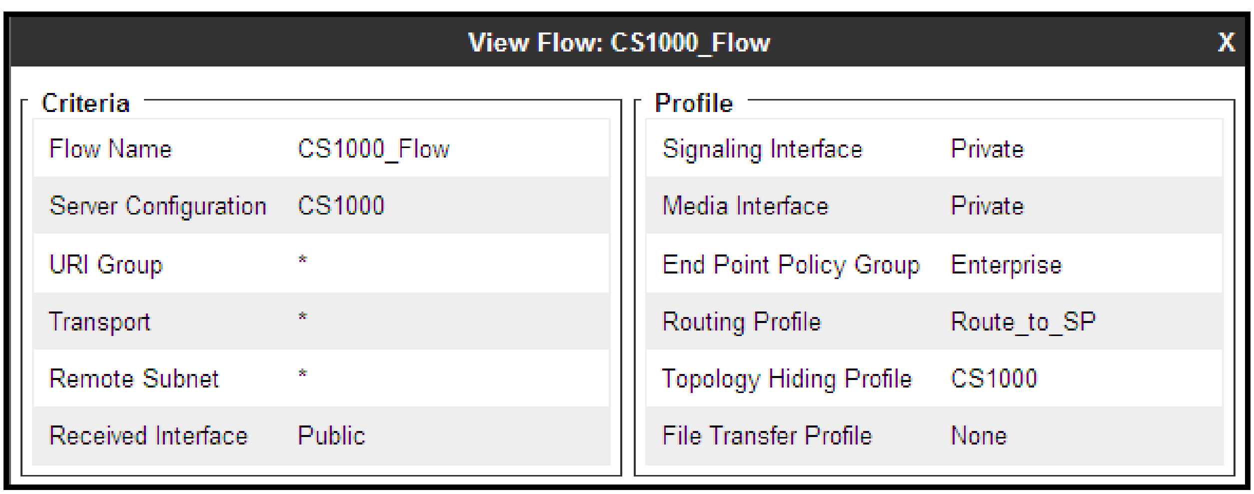
View Flow: SIP_Trunk_Flow

Criteria	
Flow Name	SIP_Trunk_Flow
Server Configuration	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private

Profile	
Signaling Interface	Public
Media Interface	Public
End Point Policy Group	Service Provider
Routing Profile	Route_to_CS1000
Topology Hiding Profile	Service_Provider
File Transfer Profile	None

To create the call flow toward the CS1000, click **Add Flow**.

- **Name: CS1000_Flow.**
- **Server Configuration**: **CS1000.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Public**
- **Signaling Interface: Private.**
- **Media Interface**: **Private.**
- **End Point Policy Group: Enterprise.**
- **Routing Profile: Route_to_SP** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: CS1000.**
- **File Transfer Profile: None.**
- Click **Finish.**

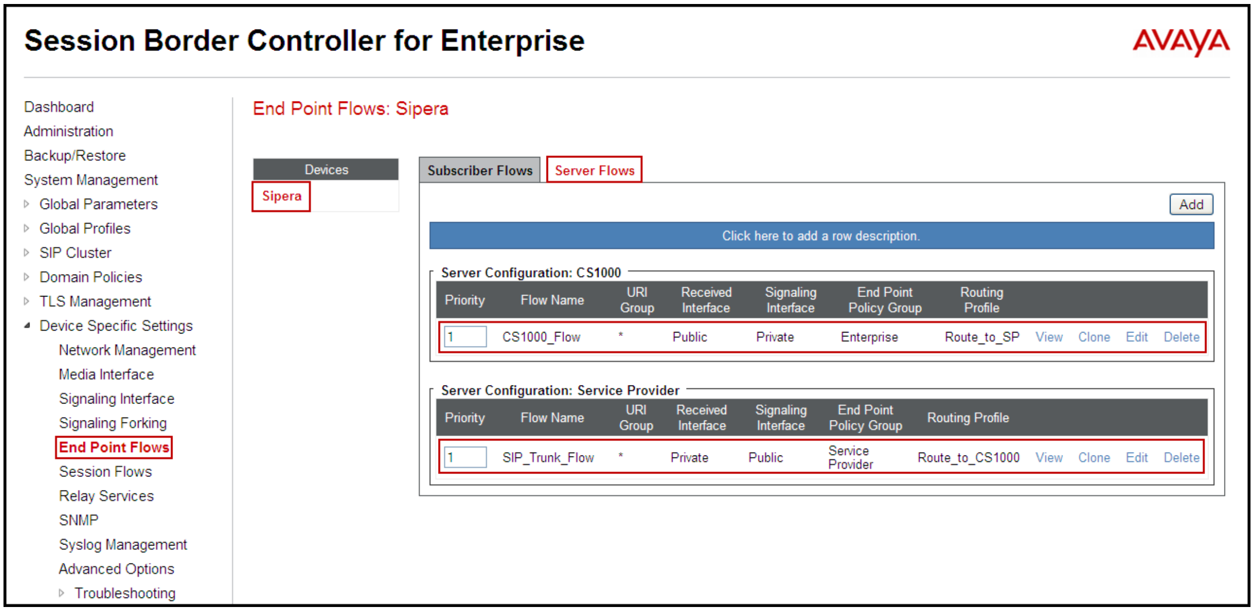


View Flow: CS1000_Flow

Criteria	
Flow Name	CS1000_Flow
Server Configuration	CS1000
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public

Profile	
Signaling Interface	Private
Media Interface	Private
End Point Policy Group	Enterprise
Routing Profile	Route_to_SP
Topology Hiding Profile	CS1000
File Transfer Profile	None

The following screen capture shows the added **End Point Flows.**



7. CenturyLink SIP Trunk Service Configuration

To use CenturyLink SIP Trunk service, a customer must request the service from CenturyLink using their sales processes. The process can be started by contacting CenturyLink via the corporate web site at: http://www.CenturyLink.com/

During the signup process, CenturyLink will require that the customer provide the public IP address used to reach the Avaya SBCE at the edge of the enterprise. CenturyLink will provide the IP address of the SIP proxy/SBC, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the CS1000 and the Avaya SBCE configuration discussed in the previous sections.

8. Verification Steps

The following steps may be used to verify the configuration.

8.1. General

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

8.2. Verify Call Establishment on the CS1000 Call Server

Active Call Trace (LD 80).

Following is an example of one of the commands available on the CS1000 to trace the extension (DN) when the call is active or idle. The call scenario involved the CS1000 extension 8000 calling a PSTN phone number (7863311234).

- Login to the 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 **trac 0 8000** while the call is active.
- After call is released, issue command **trac 0 8000** again to see if the DN is released back to idle state.

The screen on the next page shows the actual output of the Call Server Command Line mode when the 8000 is in an active call:

Note that IP addresses and telephone numbers have been masked for security reasons.

The following screen shows an example of an active call on extension 8000.

```
>ld 80
TRA000
.trac 0 8000

ACTIVE  VTN 008 0 00 00

ORIG   VTN 008 0 00 00  KEY 0  SCR MARP  CUST 0  DN 8000  TYPE 1165
  SIGNALLING ENCRYPTION: INSEC
  FAR-END SIP SIGNALLING IP: 172.16.21.61
  FAR-END MEDIA ENDPOINT IP: 172.16.20.154  PORT: 5200
  FAR-END SIP SIGNALLING IP: 172.16.21.61
  FAR-END MEDIA ENDPOINT IP: 172.16.20.154  PORT: 5200
TERM   VTN 048 0 00 10   VTRK IPTI  RMBR  0 11 OUTGOING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 172.16.5.71
  FAR-END MEDIA ENDPOINT IP: 172.16.5.71  PORT: 35010
  FAR-END VendorID: AVAYA-SM-6.3.2.0.632023
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 91786331
MAIN_PM  ESTD
TALKSLOT  ORIG  10   TERM  15    JUNCTOR  ORIG0   TERM0
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 489


----  ISDN ISL CALL (TERM) ----
CALL REF # =  395
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  8000  NUM_PLAN:E164    TON:NATIONAL  ESN:NPA
CALLED NO  =  1786331  NUM_PLAN:E164    TON:NATIONAL  ESN:NPA
```

The following screen shows an example after the call on extension 8000 was released.

```
.trac 0 8000

IDLE VTN 008 0 00 00   MARP
```

The following screen shows an example after the call was released, it shows that there are no trunks busy.

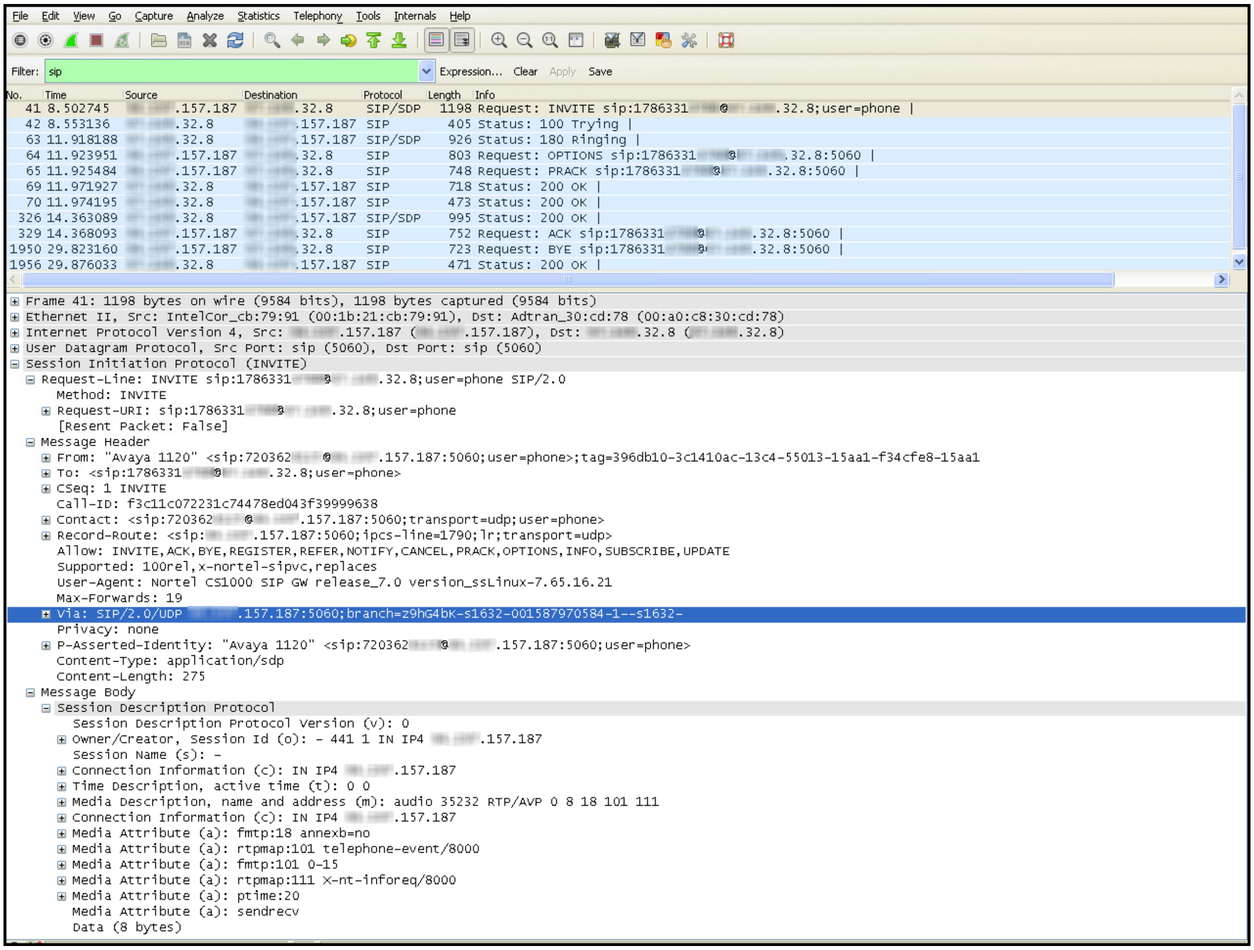
```
>ld 32
NPR000
.stat 48 0
012 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

8.3. Protocol Traces

Wireshark was used to verify the following information for each call:

- RequestURI: verify the request number and SIP domain.
- From: verify the display name and display number.
- To: verify the display name and display number.
- Diversion: verify the name and number and reason code.
- P-Asserted-Identity: verify the display name and display number.
- Privacy: verify the "user, id" masking.
- Connection Information: verify IP addresses.
- Time Description: verify session timeout of far end endpoint.
- Media Description: verify audio port, codec, DTMF event description.
- Media Attribute: verify specific audio port, codec, ptime, send/ receive ability.
- DTMF event and fax attributes.

The following screen shows an example of a typical capture for a call made from an 1165 Deskphone (DID: 7203621234) on the CS1000 to a PSTN number (7863311234).



9. Conclusion

These Application Notes describe the procedures necessary to Configuring CenturyLink SIP Trunk service with Avaya Communication Server 1000E Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.2 as shown in **Figure 1**.

CenturyLink SIP Trunk service passed compliance testing with the observation/limitations noted in **Section 2.2**.

10. References

This section references the documentation relevant to these Application Notes.

Product documentation for the Avaya Communication Server 1000E, including the following, is available at:
http://support.avaya.com/

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

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

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

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

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

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

[7] Avaya Product Support Notice – PSN003460u – Configuring FAX over IP in CS 1000: An Overview.

[8] Communication Server 1000 Release 7.6 & Service Pack 2 Release Notes, Issue 1.1 July 2013.

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

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

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

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

Other resources:

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

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

Appendix A: SigMa Script

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

```
within session "All"
{
   act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
   {

      if (%HEADERS["History-Info"][1].regex_match("reason")) then
          {

          %HEADERS["Diversion"][1] = "sip:dummy@dummy.com";

          %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-
Info"][1].URI.SCHEME;
          %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-
Info"][1].URI.USER;
          %HEADERS["Diversion"][1].URI.HOST = %HEADERS["History-
Info"][1].URI.HOST;
          %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-
Info"][1].URI.PORT;

          %HEADERS["Diversion"][1].URI.PARAMS["reason"] = "unconditional";
          %HEADERS["Diversion"][1].URI.PARAMS["counter"] = "1";
          %HEADERS["Diversion"][1].URI.PARAMS["privacy"] = "off";
          }

       %HEADERS["Content-Type"][1].regex_replace("multipart/mixed;boundary=unique-
boundary-1","application/sdp");

//  The SBC will not remove the SDP MIME, so  "x-nt-mcdn-frag-hex" = %BODY[1] //  After
"x-nt-mcdn-frag-hex" is removed, "x-nt-esn5-frag-hex" moves up one...
//  So the same command removes "x-nt-esn5-frag-hex".
//  And so on (e.g.,"x-nt-epid-frag-hex").

         remove(%BODY[1]);
         remove(%BODY[1]);

// Remove unwanted Headers
          remove(%HEADERS["History-Info"][3]);
          remove(%HEADERS["History-Info"][2]);
          remove(%HEADERS["History-Info"][1]);
```

```
        remove(%HEADERS["Alert-Info"][1]);
        remove(%HEADERS["x-nt-e164-clid"][1]);
        remove(%HEADERS["P-AV-Message-Id"][1]);
        remove(%HEADERS["P-Charging-Vector"][1]);
        remove(%HEADERS["Av-Global-Session-ID"][1]);
        remove(%HEADERS["P-Location"][1]);
        remove(%HEADERS["Remote-Party-ID"][1]);
    }
}
```

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.