Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000 Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.3 to support Claro SIP Trunking Services - Issue 1.0

Abstract

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Communication Server 1000 Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.3 to support Claro SIP Trunking Services.

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.

Claro SIP Trunking services provides PSTN access via SIP trunks between the enterprise and Claro as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Communication Server 1000 Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.3 to support Claro SIP Trunking Services.

During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure interoperability between Claro and the Avaya Communication Server 1000.

In the sample configuration, the Avaya enterprise solution consists of a Communication Server 1000 Rel. 7.6 (hereafter referred to as CS1000), Avaya Session Border Controller for Enterprise Rel. 6.3 (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 SIP trunks. The Avaya SBCE was connected to Claro's network via SIP trunks. Various call types were made from the CS1000 to Claro and vice versa to verify interoperability between the CS1000 and Claro.

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 for 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 Avaya Communication Server 1000 Release 7.6 and the Avaya Session Border Controller for Enterprise Release 6.3 can interoperate with the Claro's network. The following interoperability areas were covered:

- Incoming calls from the PSTN were routed to DID numbers assigned by Claro. 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 Claro'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 to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two way speech-path. Testing was performed with codecs: G.711MU, G.711A and G.729A, Claro's preferred codec order.
- No matching codecs.

- 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, interacting with Interactive Voice Response systems (IVR).
- Calling number and calling name blocking (Privacy).
- Call Hold/Resume.
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call transfers.
- Station Conference.
- T.38 fax.
- Long duration calls (one hour).
- Early Media transmission.
- Mobility: Mobil X and Personal Call Assistance (PCA).

Items not supported or not tested included the following:

- Inbound toll-free calls, Outbound Toll-Free calls, 911 calls (emergency), "0" calls (Operator), 0+10 digits calls (Operator Assisted), and 411 calls (Local Directory Assistance) were not tested.
- G.711 fax pass-through was not tested.

2.2. Test Results

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

- **DTMF digits not recognized on calls to voice mail systems involving international carriers**: When calls were made from CS1000 phones to a voice mail system based in the U.S., the digits entered to identify the voice mail subscriber were not recognized. The issue is that with a particular carrier handling international calls, Claro negotiates a value of **16000**, as the clock rate in the Media Attribute of the SDP, and includes this value (**16000**) in the Media Attribute of the SDP in the 183 message it sends to the CS1000. With other carriers the value of **8000** is negotiated. With the value of **8000** there is no issue (digits are recognized by the voice mail system). The same test was performed using a voice mail system in the Dominican Republic local PSTN network (as opposed to a voice mail system in the U.S.), with no issues found; the value of **8000**, as the clock rate, was always negotiated using the local PSTN voice mail system. Claro is investigating this issue with the international carrier.
- **No ring back tone after execution of Blind Transfers to the PSTN**: Ring back tone is not heard (only silence) on PSTN phones after the execution of Blind Transfers to the PSTN from CS1000 phones (PSTN_1→CS1000_IP_Phone →Blind Transfer →PSTN_2). **Plug-in 501** has to be enabled in order for Blind Transfers to the PSTN to function properly. If **Plug-in 501** is not enabled, the CS1000 will prevent the execution of Blind Transfers from one PSTN endpoint to another PSTN endpoint by disabling the **Trans** key on the CS1000 phone doing the transfer. This is a known CS1000 limitation when **Plug-in 501** is enabled.

- **Blind Call Transfer to the PSTN using SIP phones do not complete until after the transferee answers the call:** When Blind Transfers to the PSTN are executed from CS1000 SIP phones the transfer does not complete until after the end user (transferee) answers the call. **Scenario**: A PSTN user calls an enterprise SIP extension (**CS1000 SIP phone**), the call is answered. The enterprise user then proceeds to do a Blind Transfer to another PSTN endpoint. **Result**: The expected behavior on the enterprise SIP phone is to display "**transfer completed**" after answering "**No**" to the question "**Consultative transfer with party?**" which implies a Blind Transfer. Instead, the SIP phone continues to display "**transferring**" until the transferee (PSTN user) answers the call. The work around is to hang up the SIP phone. There is no user impact, the transfer completes successfully. This issue is only seen with SIP phones. UniStim phones do not display this behavior.
- **No matching codec on outbound calls:** If an unsupported audio codec is received by Claro on the SIP Trunk (e.g., G.728), Claro will respond with "500 Server Internal Error" instead of the more common "488 Not Acceptable Here" response, the user will hear re-order. This issue does not have any user impact, it is listed here simply as an observation.
- **SIP Header Optimization**: SIP header rules were implemented in the Avaya SBCE to streamline the SIP header and remove any unnecessary parts. These particular headers and MIME have no real use in the service provider network.

2.3. Support

For support and information on Claro systems, please visit the corporate Web page at: http://www.claro.com.do/wps/portal/do/sc/empresas

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 below illustrates the test configuration used. The test configuration simulates an enterprise site with the Avaya components connected to Claro SIP Trunking Services through the public Internet.

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

- Avaya Communication Server 1000 (CS1000).
- Dell R210 V2 Server running Avaya Session Border Controller for Enterprise.
- Avaya 1100-Series IP Deskphones (UniStim).
- Avaya 1100-Series Deskphones (SIP).
- Avaya 2050 IP Softphone.
- Avaya M3904 Digital Deskphones.
- Analog Deskphones.
- Fax machines.
- Desktop with administration interfaces.

Located at the edge of the enterprise is a VPN Firewall, followed by the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **B1** is used to connect to the public network, interface **A1** is used to connect to the private network. Since a VPN connection was used with this solution to connect Claro's network to the enterprise networks, the **A1** interface was used for access to the private enterprise network and to route calls to Claro's network across the VPN tunnel. In this solution, the **B1** interface was not used.

When a VPN connection is not used, the **B1** interface is normally used to route calls to the service provider across the public Internet.

All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE and through the VPN Firewall. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Claro, through the VPN tunnel, and across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and the CS1000, across the enterprise private IP network, is also SIP over 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 Claro to the Avaya SBCE through the VPN tunnel, then to the CS1000. Once the call arrived at the CS1000, further 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 Claro's network through the VPN tunnel.

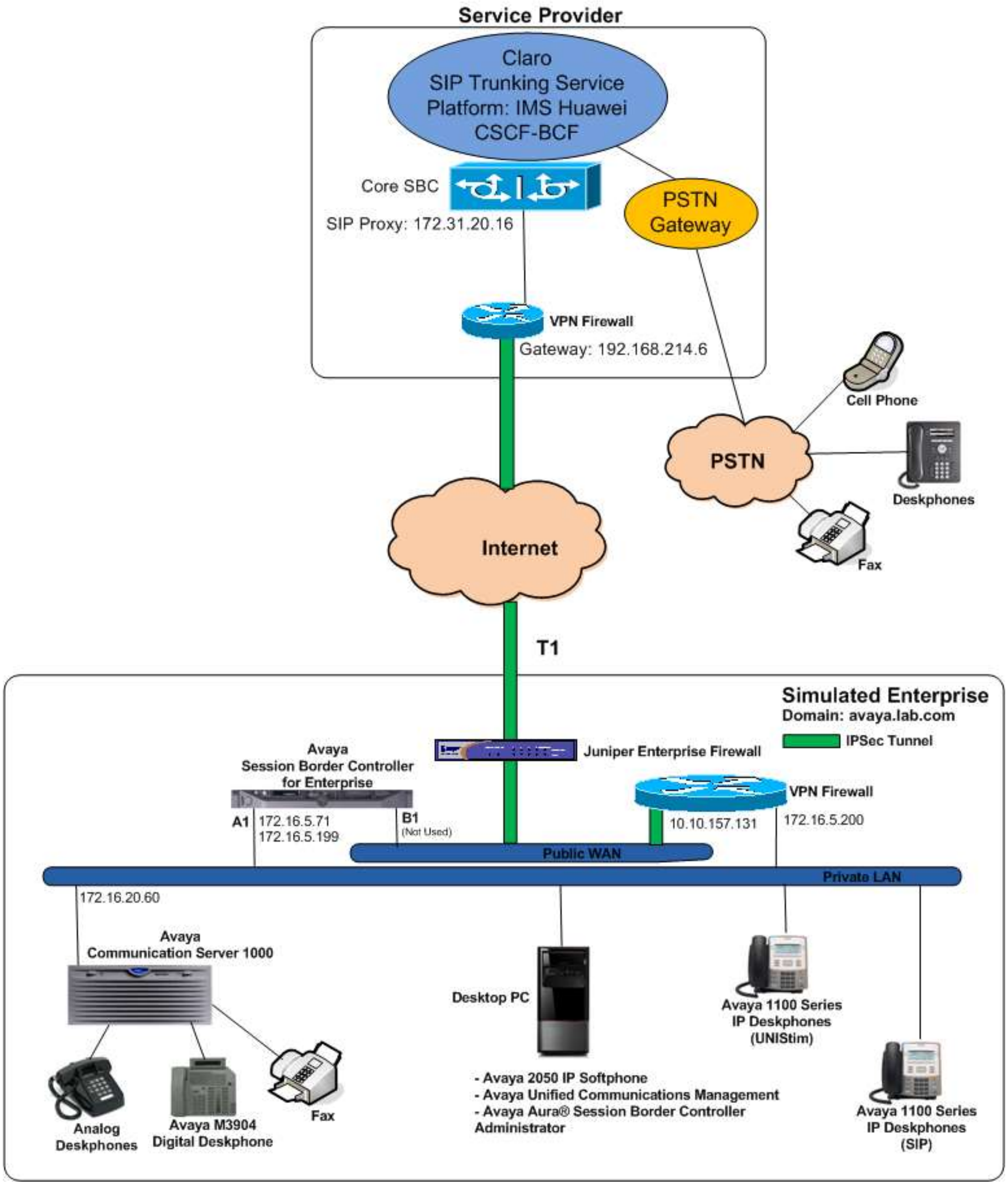


Figure 1: Claro SIP Trunk Service with Avaya CS1000

4. Equipment and Software Validated

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

Avaya	
Equipment	**Release/Version**
Avaya Communication Server 1000 running Co-resident Call Server, Signaling Server and Media Gateway in a single CP-MGS card.	RELEASE 7 ISSUE 65 P + **Call Server:** DepList 1: core Issue: 01(created: 2015-03-19 12:06:06 (est)) **Signaling Server:** 7.65.16.00 **(Service Pack 6)**
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	6.3.1-22-4653
Avaya Deskphones	1110: 0623C8Y (UniStim) 1120: 0624C8Y (UniStim) 1150: 0627C8Y (UniStim) 1165: 0626C8Y (UniStim) 1120E: 04.04.18.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.04.0106
Lucent Analog Phone	N/A
Fax Machines	N/A
Claro	
Equipment	**Release/Version**
IMS Huawei CSCF-BCF	V100R010C00SPC100
SBC Huawei SessionEngine2600	V200R009ENGC30SPC100

Signaling Server Service Updates (SU) and Patches:
(CS1000 Linux Service Updates (SU) and patches included in Release 7.6 Service Pack 6):
cs1000-csmWeb-7.65.16.22-2.i386.000
cs1000-Jboss-Quantum-7.65.16.23-3.i386.000
cs1000-dmWeb-7.65.16.23-1.i386.000
cs1000-patchWeb-7.65.16.22-4.i386.000
cs1000-cs1000WebService_6-0-7.65.16.21-00.i386.000
cs1000-sps-7.65.16.23-1.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-csoneksvrmgr-7.65.16.22-5.i386.000
cs1000-dbcom-7.65.16.21-00.i386.000
cs1000-baseWeb-7.65.16.22-4.i386.000
cs1000-linuxbase-7.65.16.23-3.i386.000
jdk-1.6.0_81-fcs.i586.000
cs1000-emWeb_6-0-7.65.16.23-2.i386.000
cs1000-cs-7.65.P.100-03.i386.000
bash-3.2-33.el5_11.4.i386.000
tzdata-2014g-1.el5.i386.000
cs1000-bcc-7.65.16.23-4.i386.000
cs1000-tps-7.65.16.23-7.i386.000
cs1000-shared-omm-7.65.16.21-2.i386.000
cs1000-vtrk-7.65.16.23-24.i386.000
cs1000-ftrpkg-7.65.16.22-2.i386.000
cs1000-snmp-7.65.16.21-00.i686.000
cs1000-oam-logging-7.65.16.22-4.i386.000
cs1000-csv-7.65.16.22-2.i386.000
cs1000-mscTone-7.65.16.22-2.i386.000
cs1000-mscMusc-7.65.16.22-4.i386.000
cs1000-mscConf-7.65.16.22-2.i386.000
cs1000-emWebLocal_6-0-7.65.16.22-1.i386.000
cs1000-ipsec-7.65.16.22-1.i386.000
cs1000-cppmUtil-7.65.16.22-1.i686.000
cs1000-mscAnnc-7.65.16.22-2.i386.000
cs1000-mscAttn-7.65.16.22-2.i386.000
cs1000-gk-7.65.16.22-1.i386.000
cs1000-shared-pbx-7.65.16.22-3.i386.000
cs1000-shared-xmsg-7.65.16.22-1.i386.000

Patches:
p33331_1
p33384_1
p31484_1
p33125_1
p33274_1

MGC Loadware:
DSP1AB07.LW
DSP2AB07.LW
DSP3AB07.LW
DSP4AB07.LW
DSP5AB07.LW
udtcab25.lw
MGCCDC05.LW

In addition to applying the latest Call Server patches, Signaling Server Service updates and patches listed above, the following procedure should be followed to ensure proper operation of Call Transfers from the CS1000 to the PSTN.

Enable Plug-In **501** as follows:
Login to the **Unified Communications Management (UCM) and Element Manager** as described in **Section 5.1.1**, go to **System → Software → Plug-ins,** select **plug-in 501** and click the **Enable** button, the status will change to **Enabled**.

ENABLED PLUGINS:

PLUGIN STATUS PRS/CR_NUM MPLR_NUM DESCRIPTION
----
501 **ENABLED** Q02138637 MPLR30070 Enables Blind Transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end

5. Configure Avaya Communication Server 1000

These Application Notes assume that the basic Avaya Communications Server 1000 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 used on the CS1000.

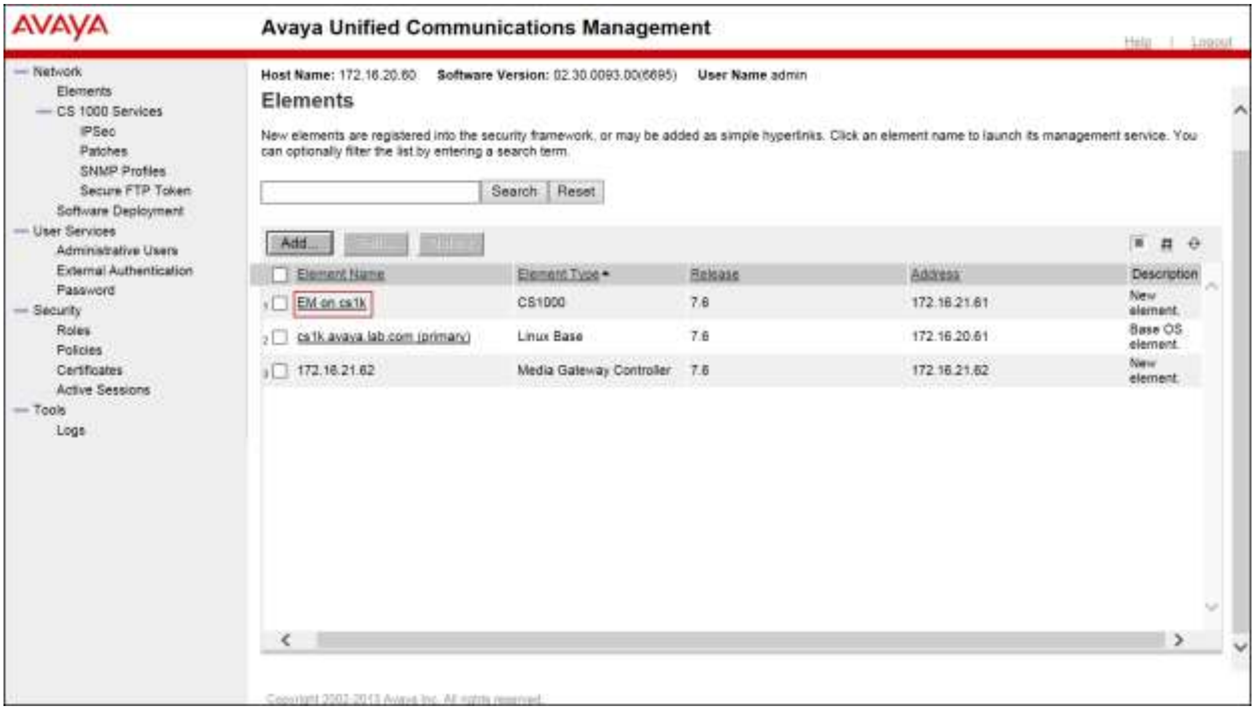
Note: Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

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, log in 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:

               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.

     @172.16.20.60's password:
Last login: Fri Feb 27 13:19:36 2015 from 172.16.5.250
[     @cs1k ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without aut
hentica
ting
logi
USERID?
PASS?
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only to
authorized users for approved purposes. Unauthorized access to
any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.

.
TTY #15 LOGGED IN       14:14  27/2/2015

>
```

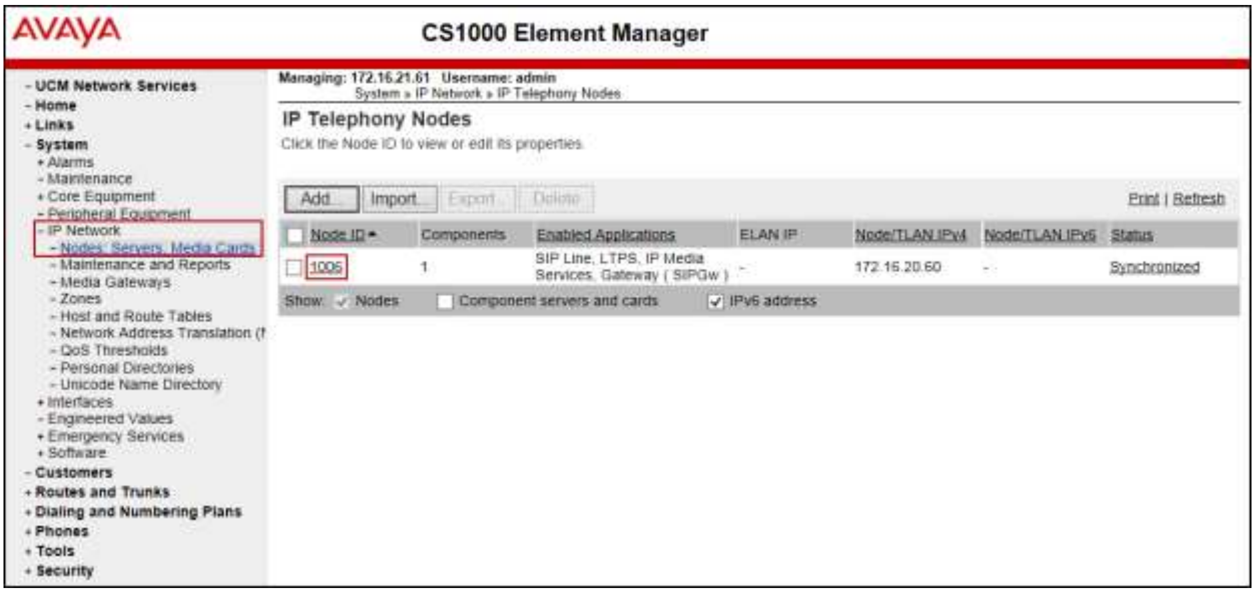
5.2. Administer an IP Telephony Node

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

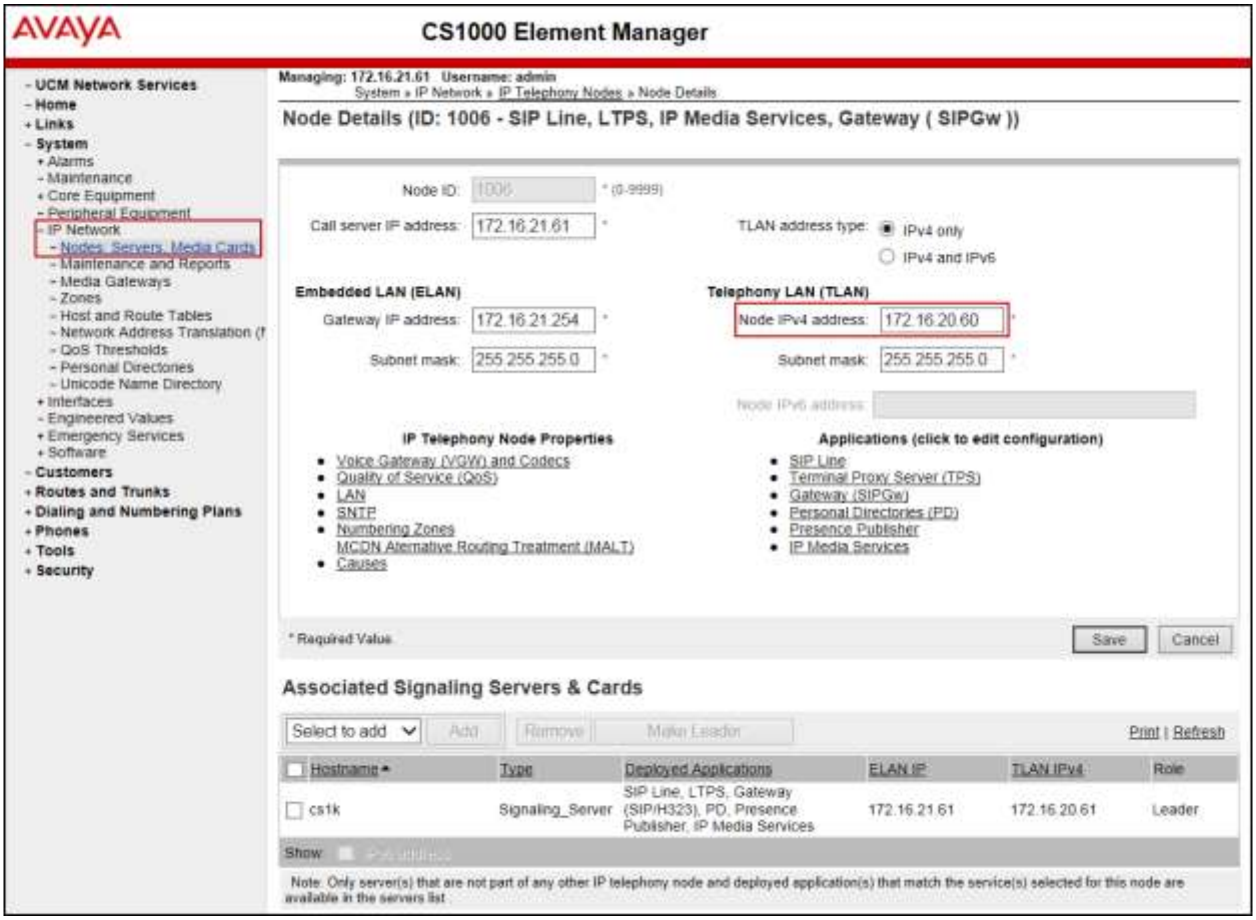
5.2.1. Obtain Node IP address

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 Claro.

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

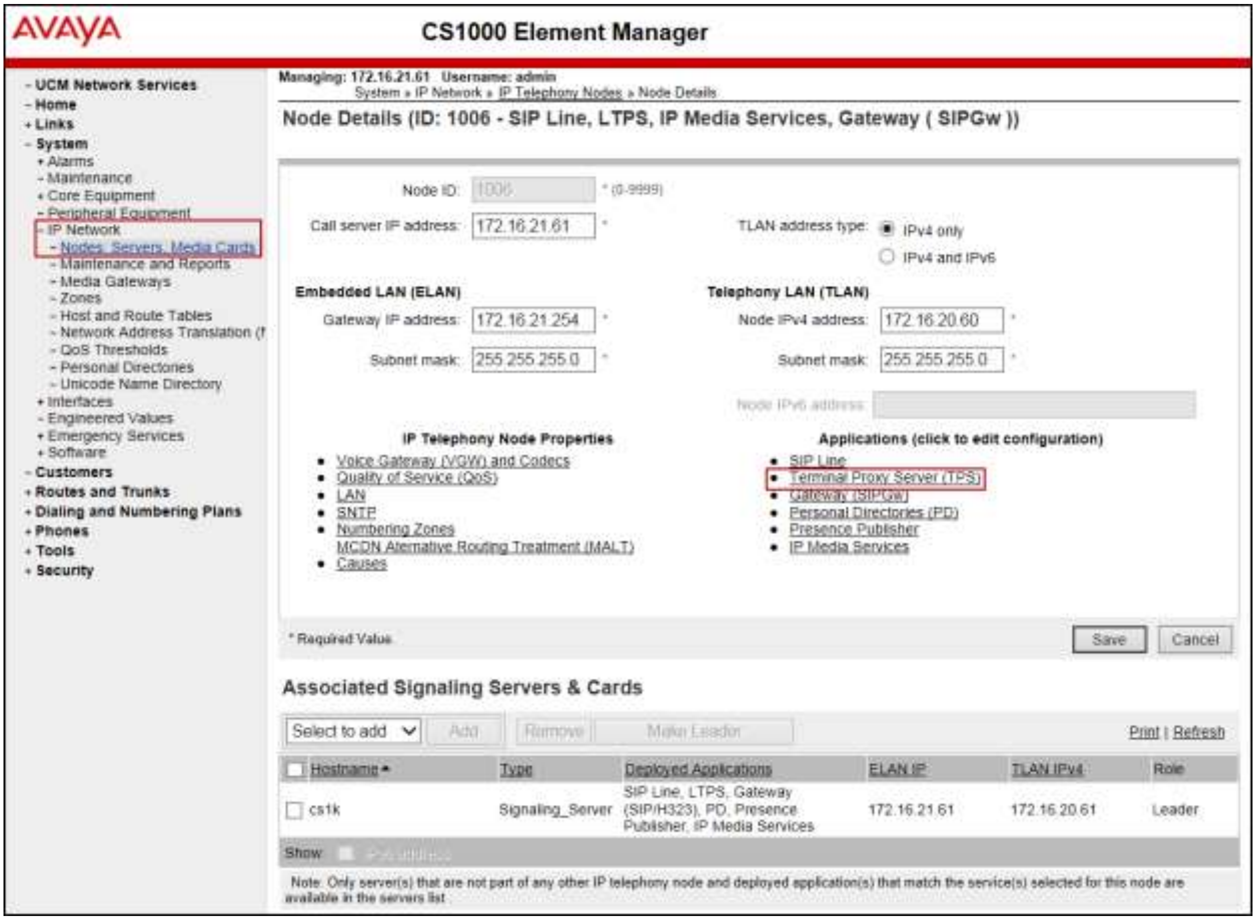


The **Node Details** screen is displayed below with the IP address of the CS1000 node. The **Node IPv4 Address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IPv4 Address** to communicate with other components for call processing.

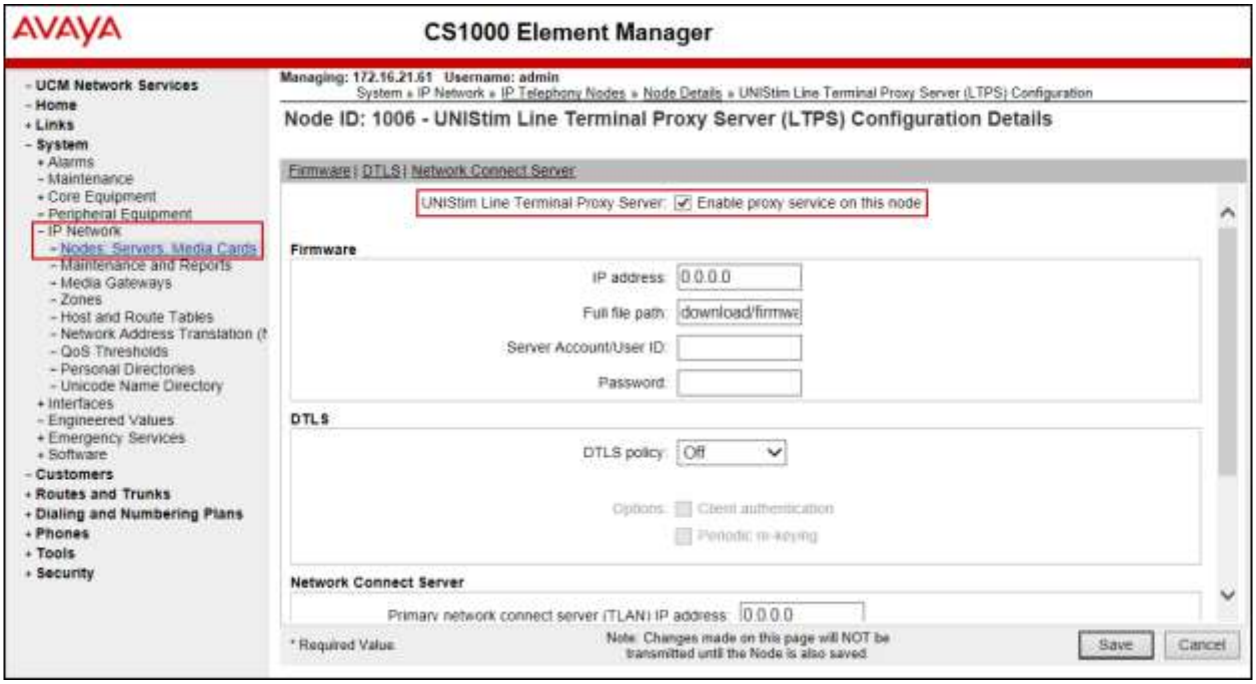


5.2.2. Administer Terminal Proxy Server

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

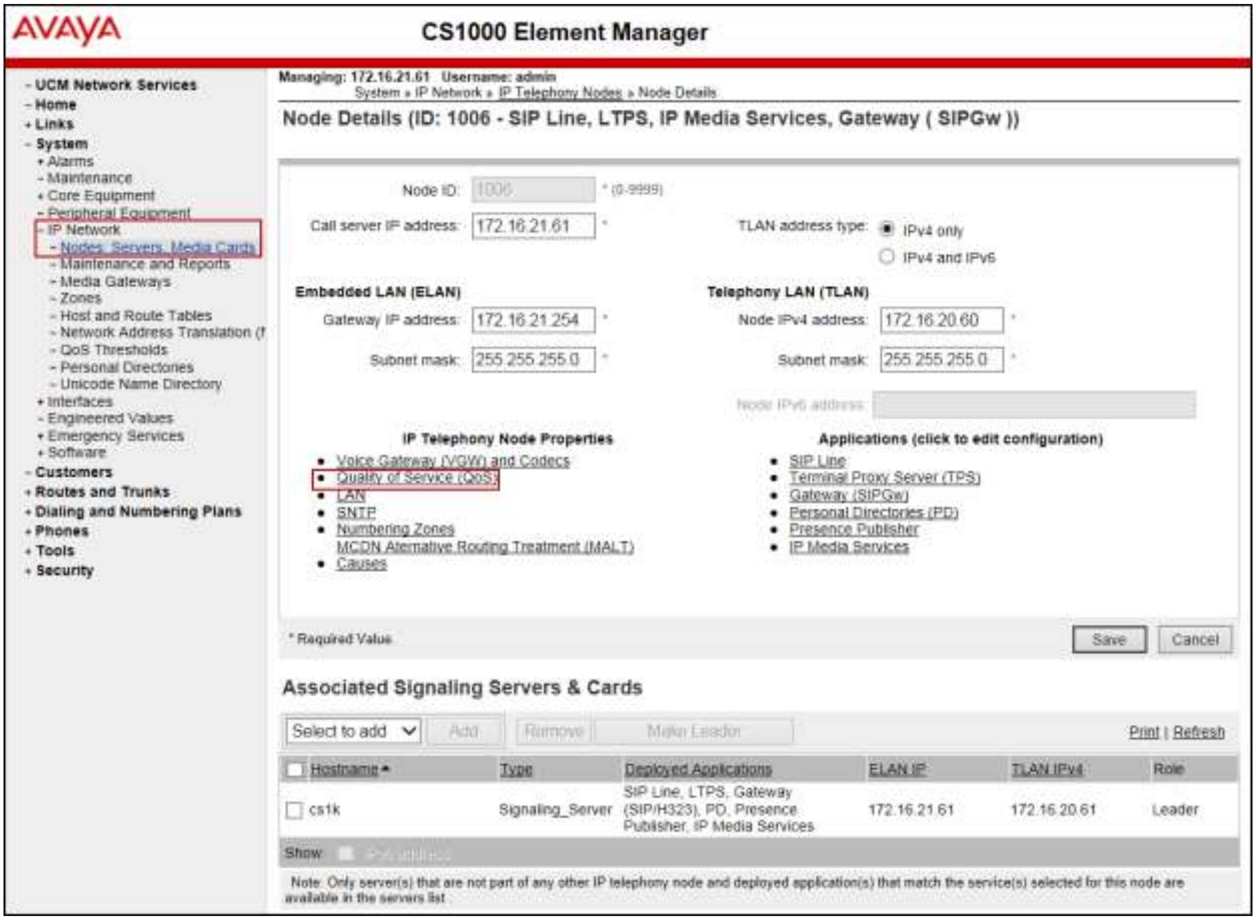


The **UNIStim Line Terminal Proxy Server (LTPS) Configuration Details** screen is displayed as shown below. Check the **Enable proxy service on this node** check box and then click **Save**.

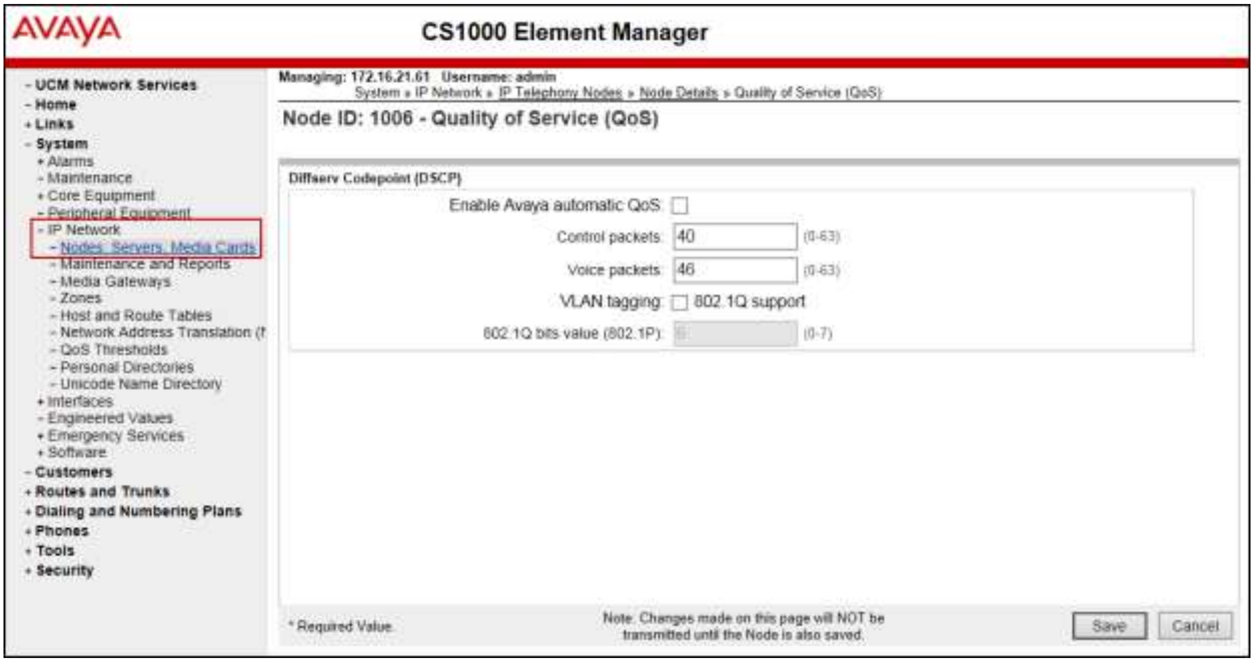


5.2.3. Administer Quality of Service (QoS)

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.

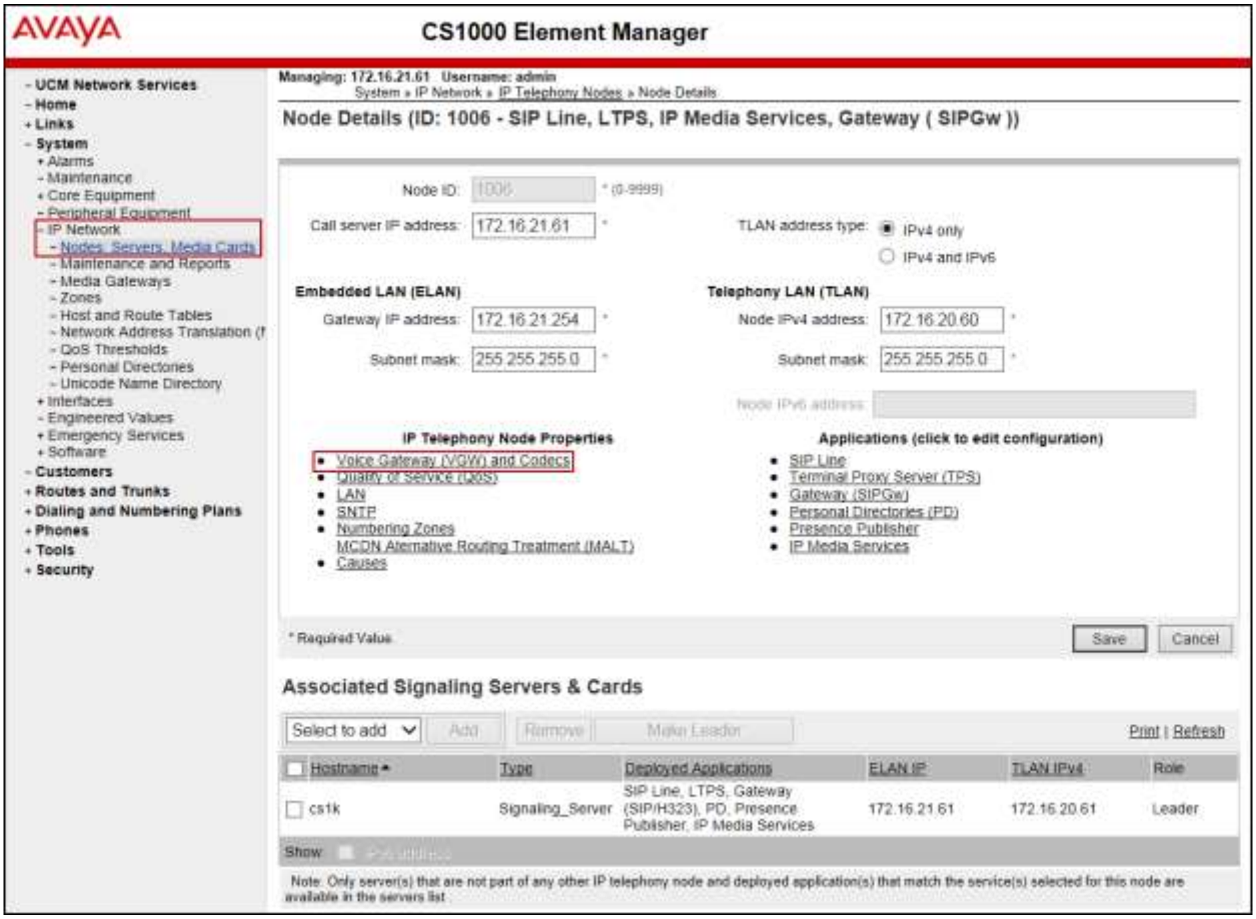


5.3. Administer Voice Codec

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

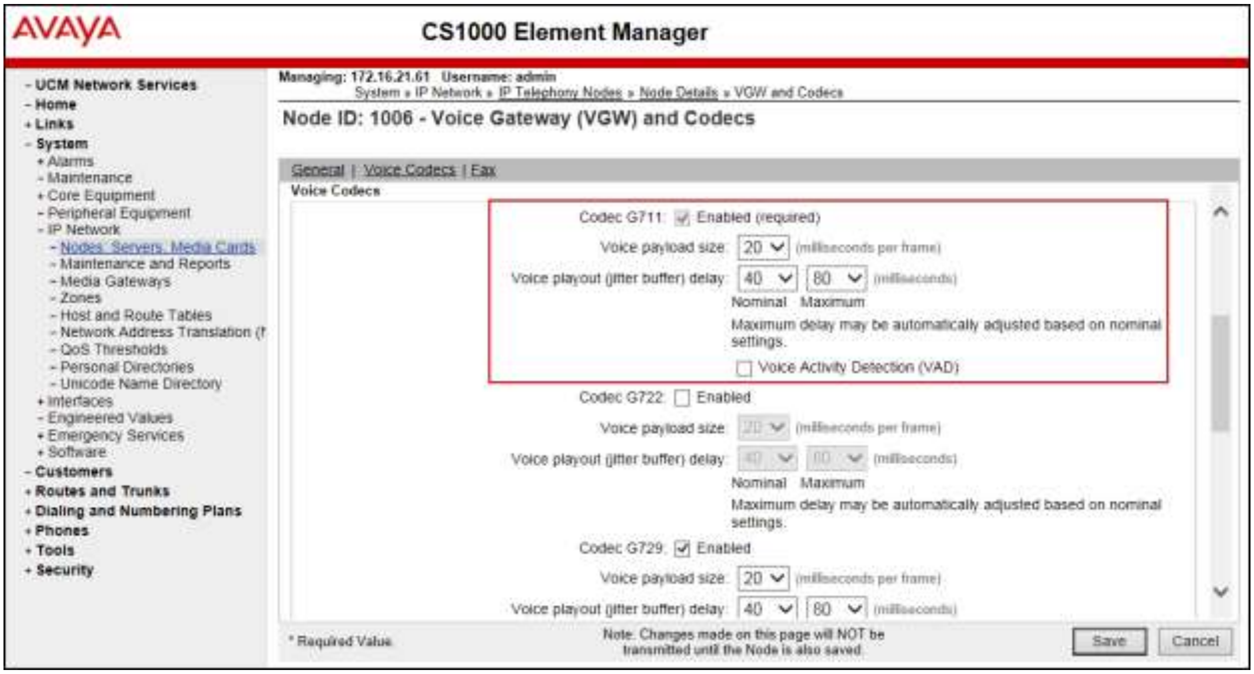
5.3.1. Enable Voice Codec, Node IP Telephony

Select **System→ 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**.

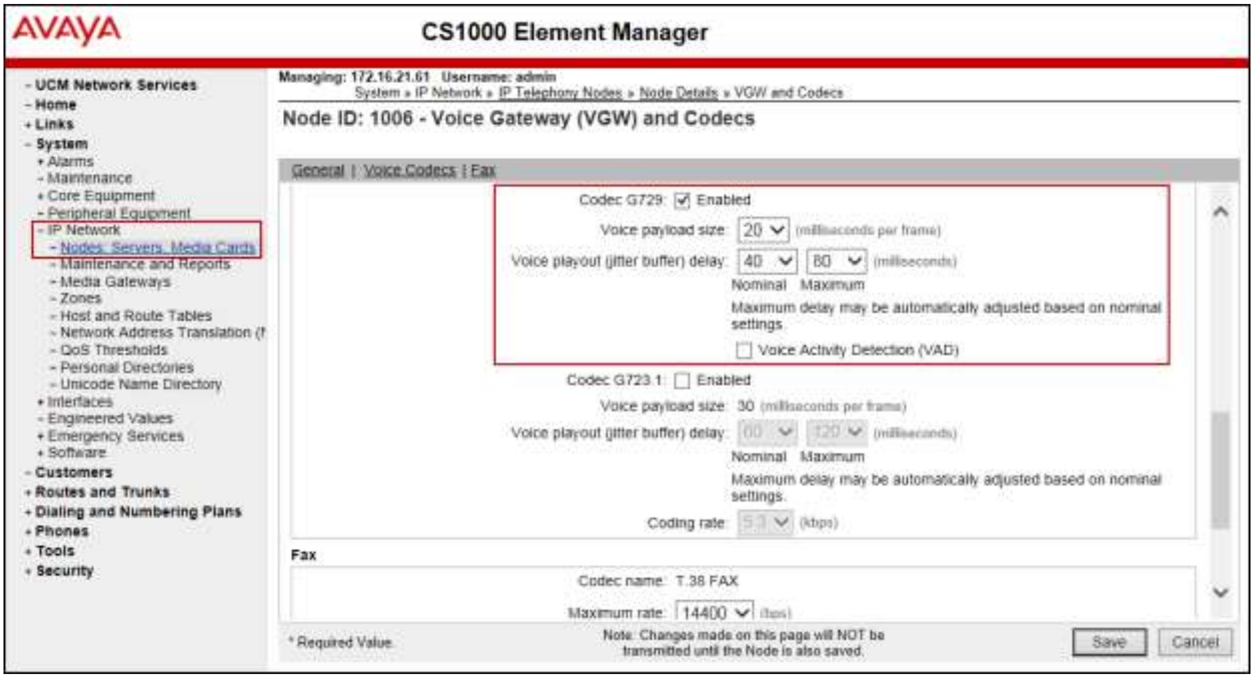


The **Voice Gateway (VGW) and Codecs** screen is displayed as shown below. Claro supports codecs **G.711MU, G.711A** and **G.729A** with **Voice Activity Detection** **(VAD)** disabled**.**

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



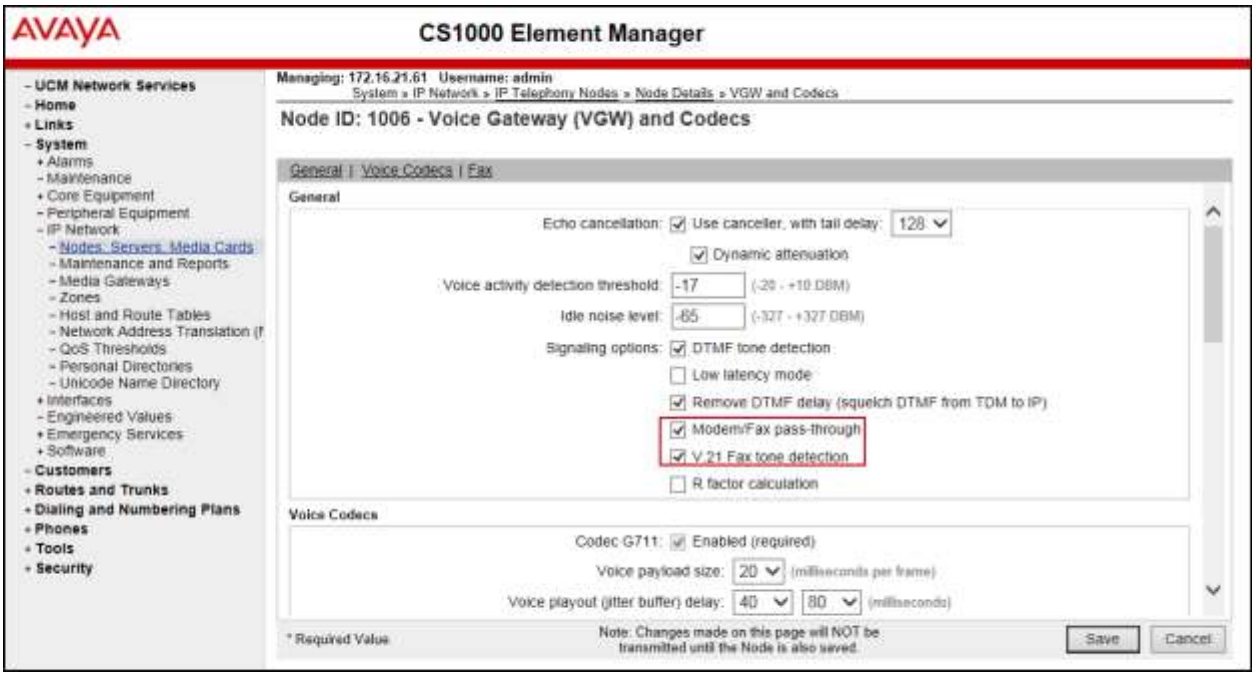
The values for the **G729** Voice Codec are shown below, ensure that **Codec G729 Enabled** is checked and **Voice Activity Detection (VAD)** is unchecked.



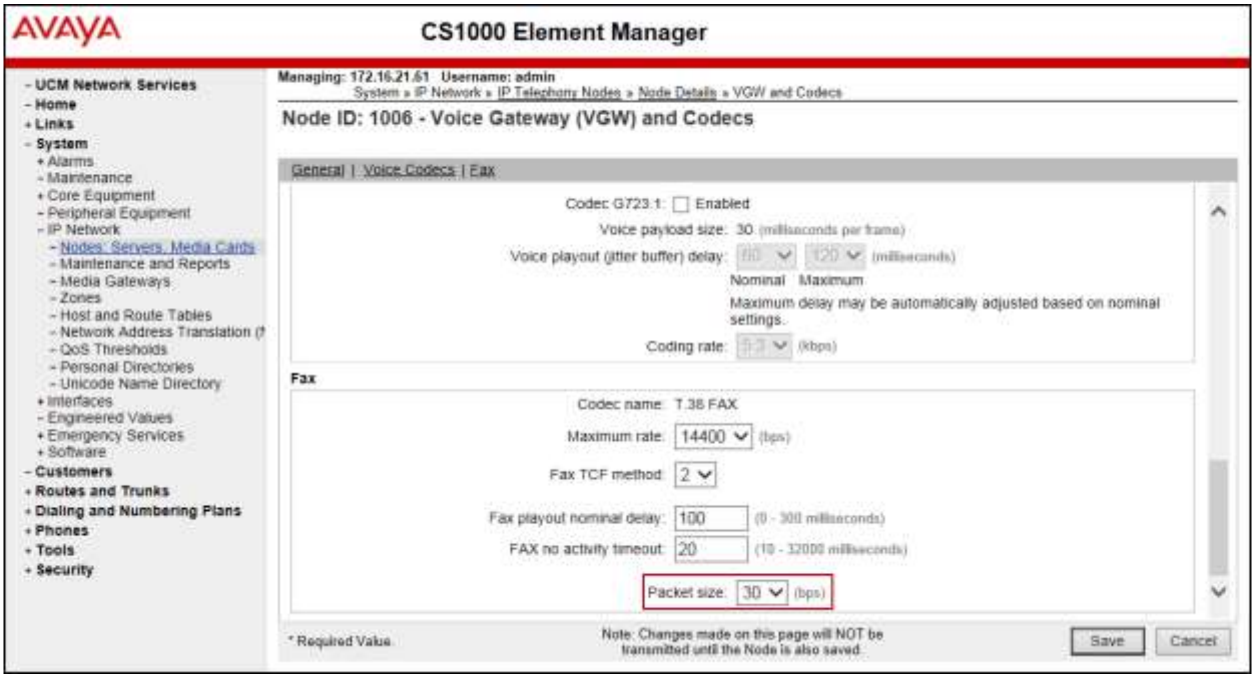
For Fax over IP, **T.38** was used as default. During the testing, **T.38** fax transport was tested successfully, **G.711MU fax pass-through** was not tested.

For CS1000 FAX over IP Support recommendation refer to **Section 5.7.1** for analog station provisioning and the Avaya Product Support Notice (PSN) referred to in **Section 10** [7], including the "**Analog Station provisioning for T.38** section" and "**Minimum Vintage Loadware Recommendation"** for MGC.

The following screenshot shows the General settings. **Modem/Fax pass-through** is selected for Node 1006; this enables the G.711MU codec to be used for fax calls between the CS1000 and Claro. The **V.21 Fax tone detection** is also selected to enable T.38 fax capability on the SIP Trunk. Click the **Save** button.

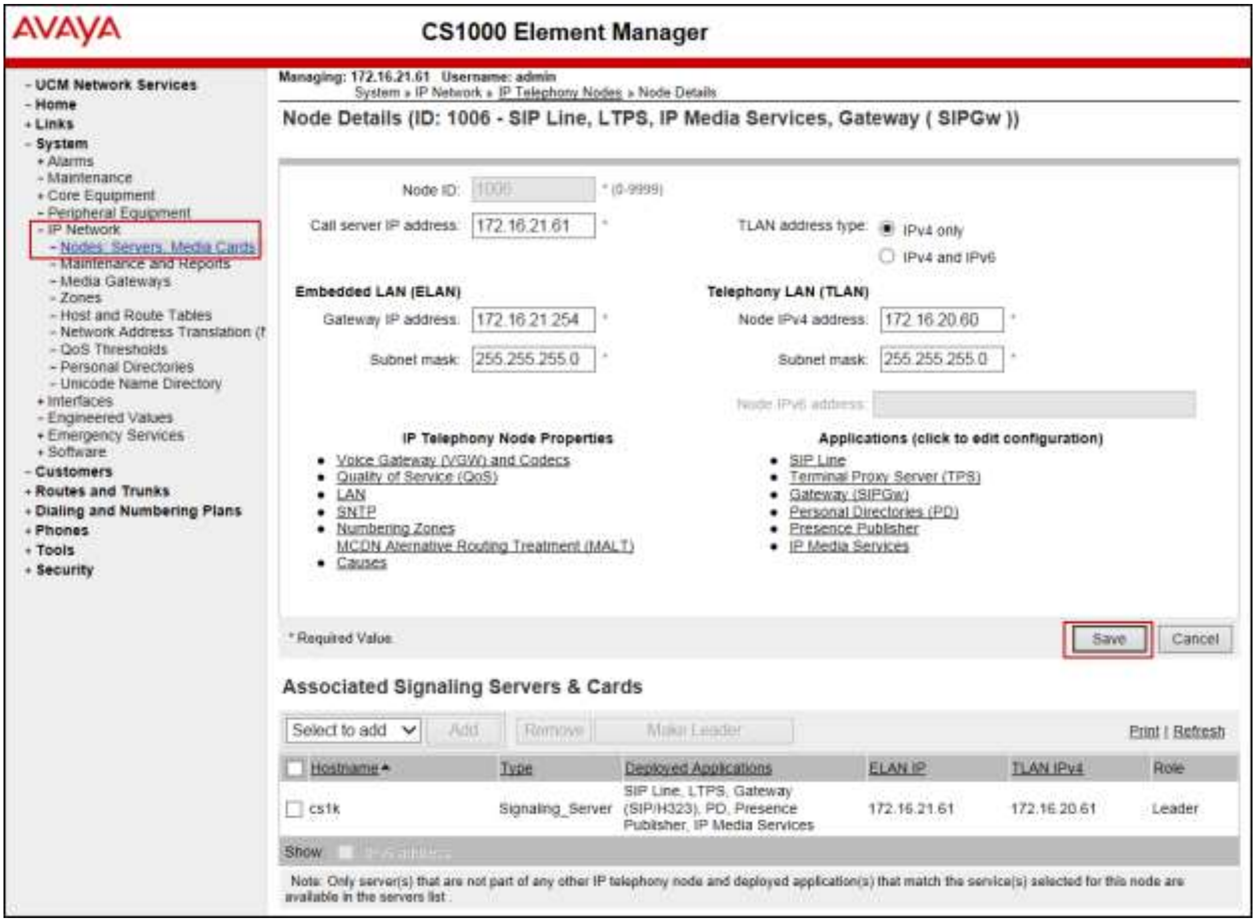


T.38 with payload size **30ms** was chosen for fax. Clicking on the **Save** button.

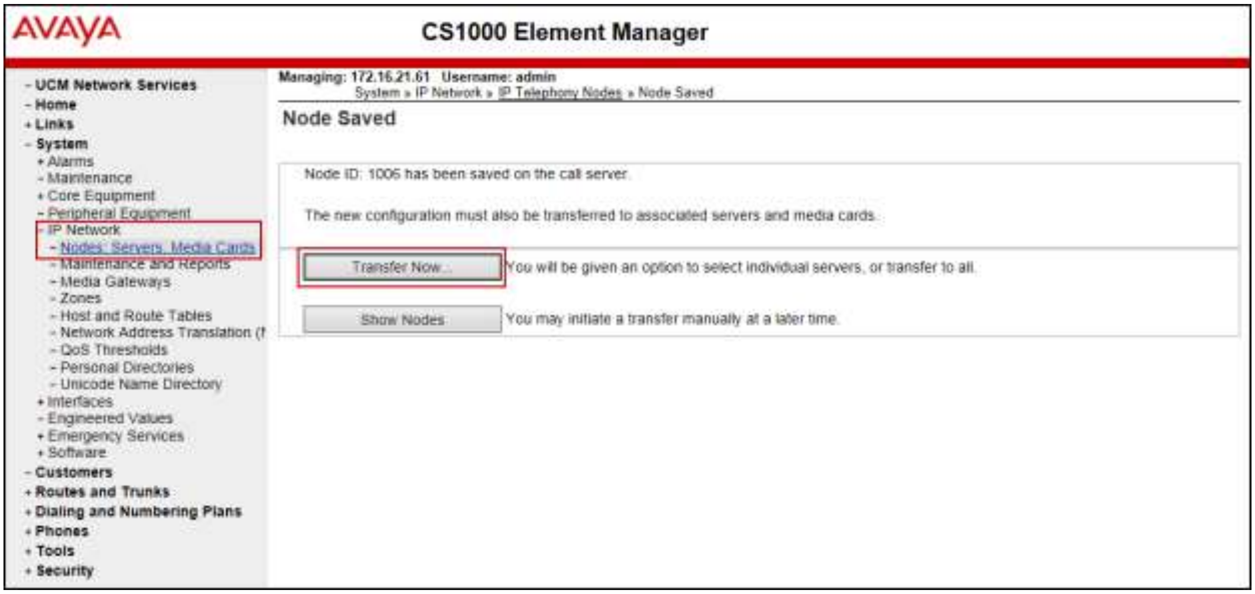


5.3.2. Synchronize the New Configuration

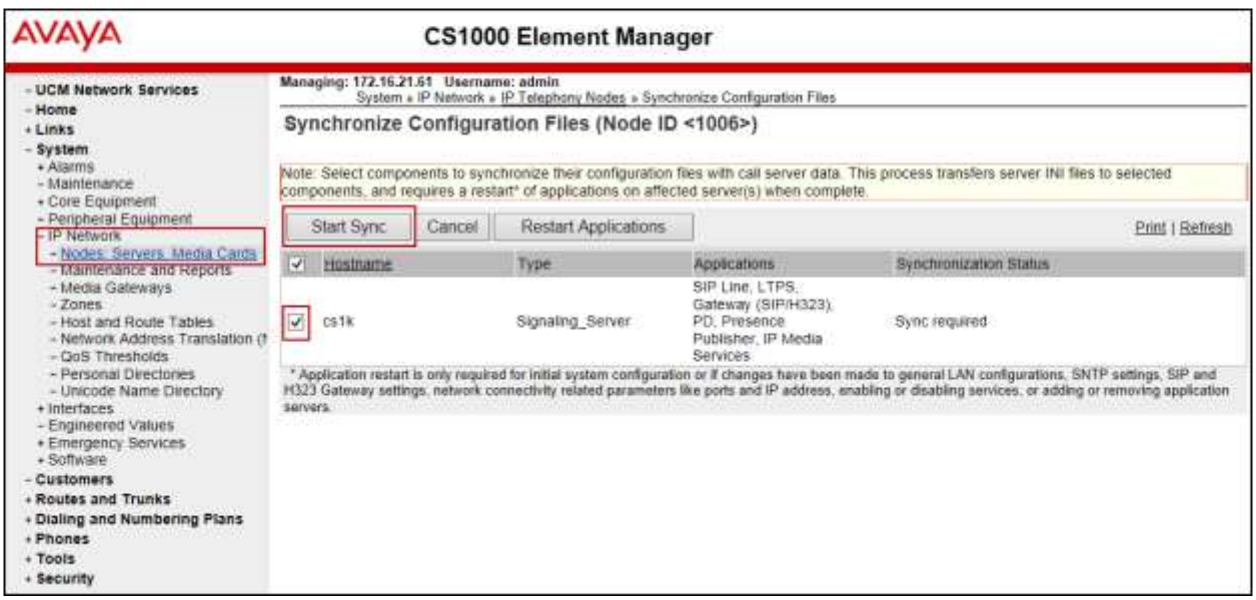
Continue from **Section 5.3.1**. Clicking on the Save button shown above will return to the **Node Details** page shown below, click on the **Save** button shown below.



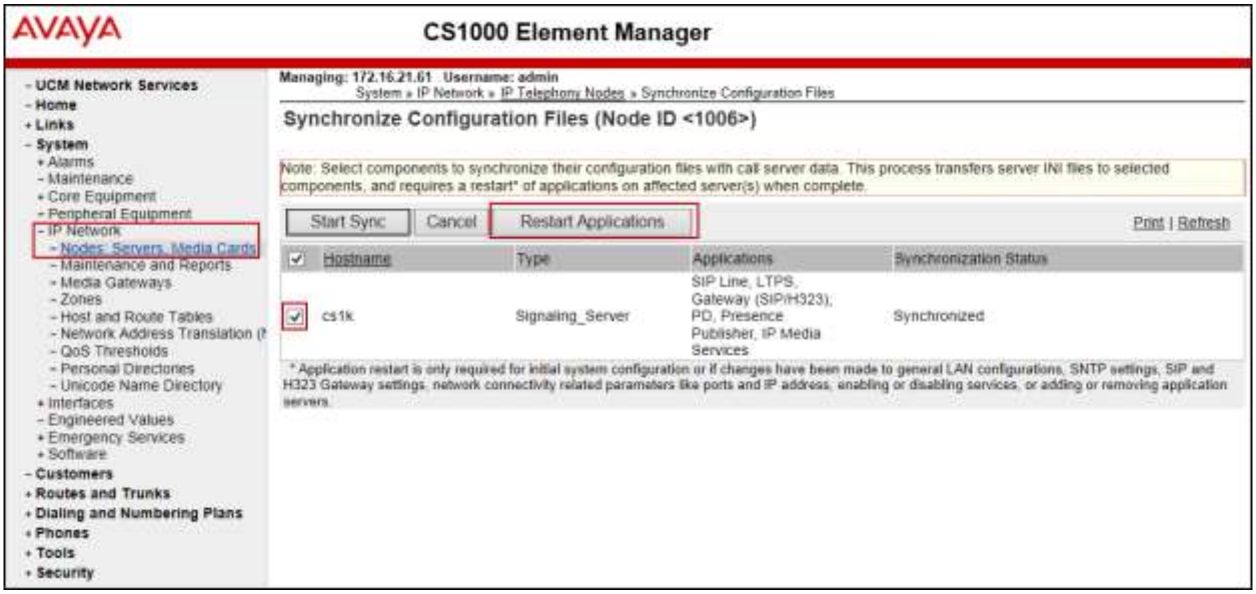
The **Node Saved** screen is displayed. Click on **Transfer Now**…



The **Synchronize Configuration Files** screen is displayed. Check the Signaling Server check box (**cs1k**), and click on the **Start Sync** button.

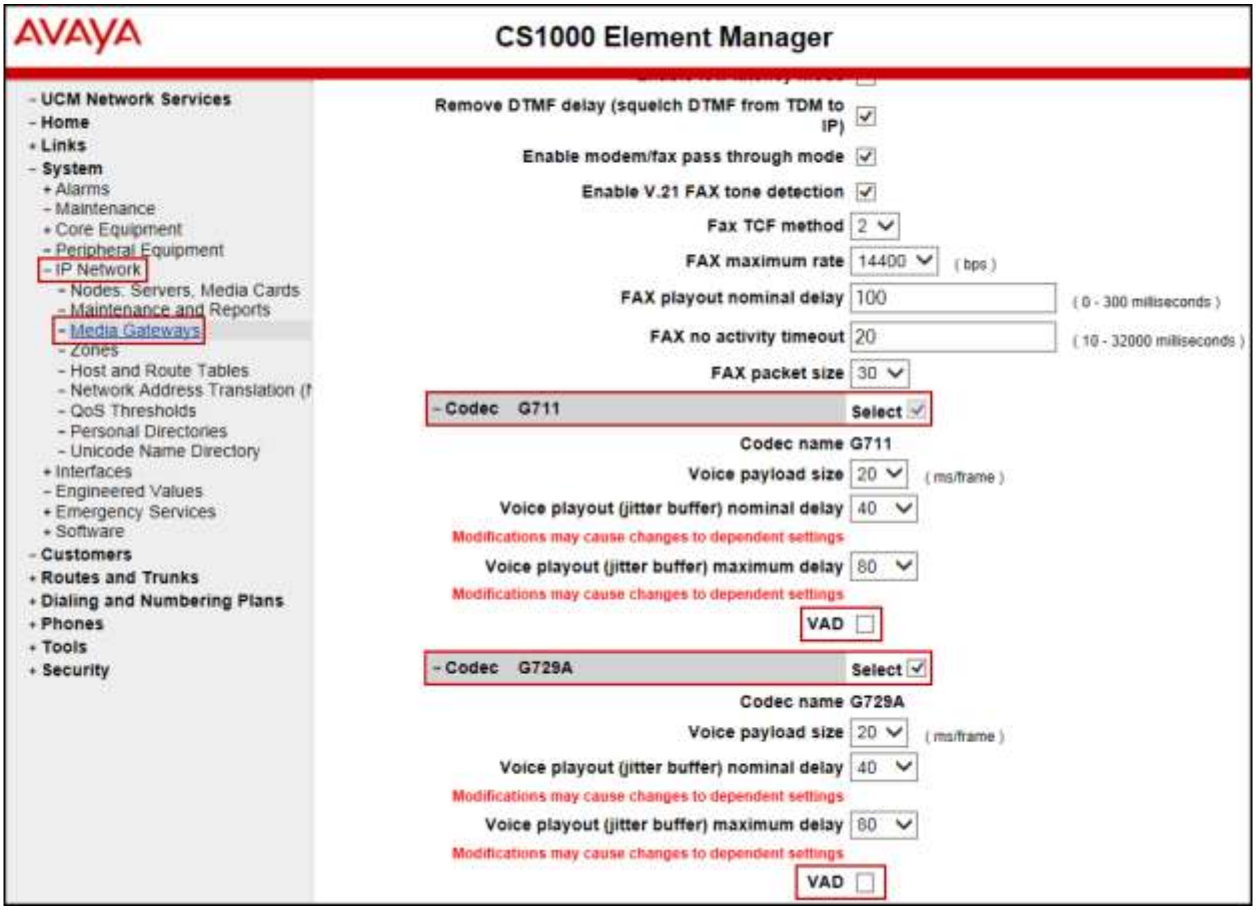


When the synchronization completes, check the Signaling Server (**cs1k**) check box again and click on the **Restart Applications** button, wait a couple of minutes for the Application restart to complete. Note that Application Restart is service affecting, it should be done off hours.



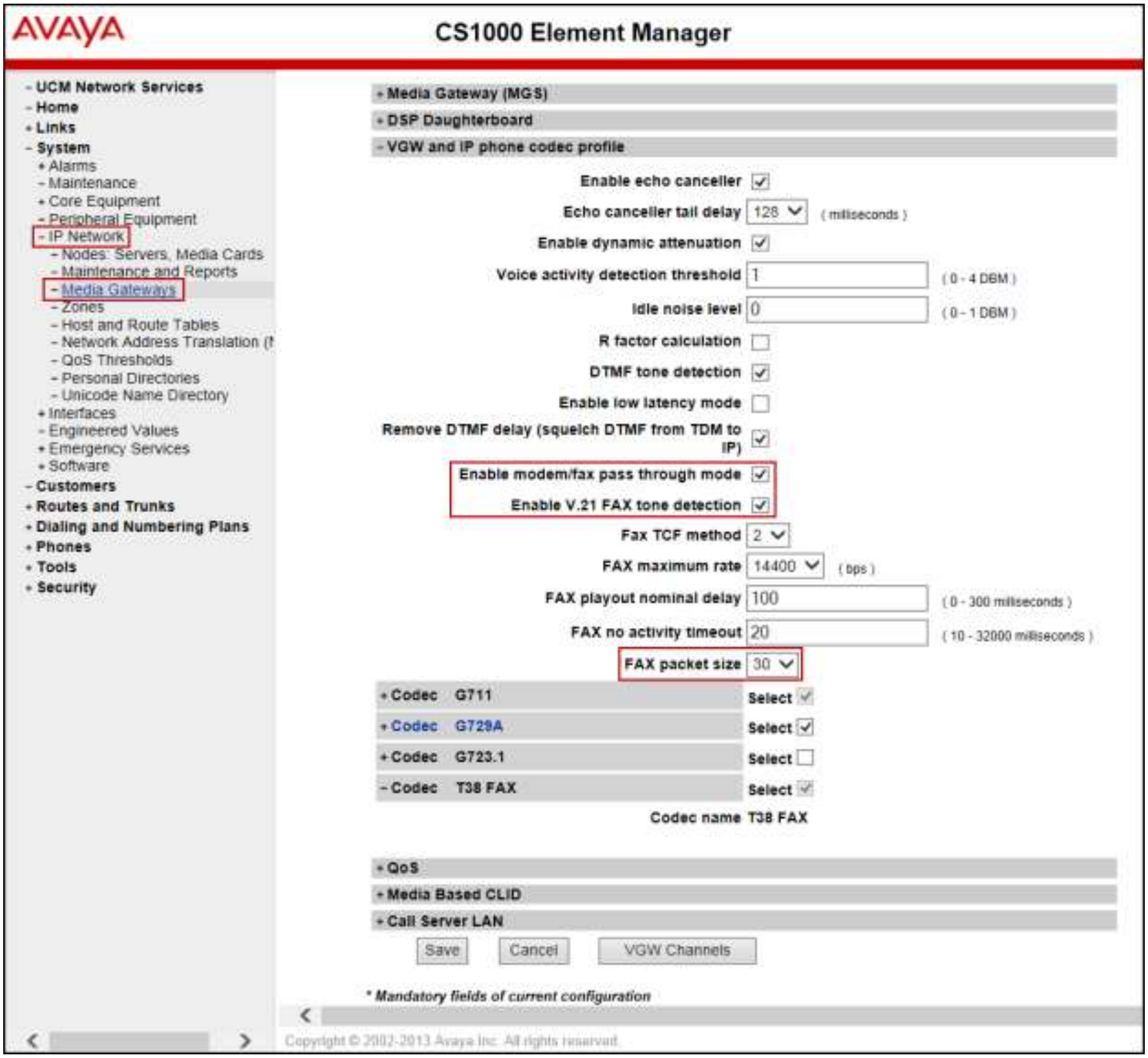
5.3.3. Enable Voice Codec on Media Gateways

From the left menu of the **Element Manager** page, select the **System→ 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** and 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. During the testing, **T.38** fax transport was tested successfully, **G.711MU fax pass-through** was not tested.

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. Click on the **Save** button.

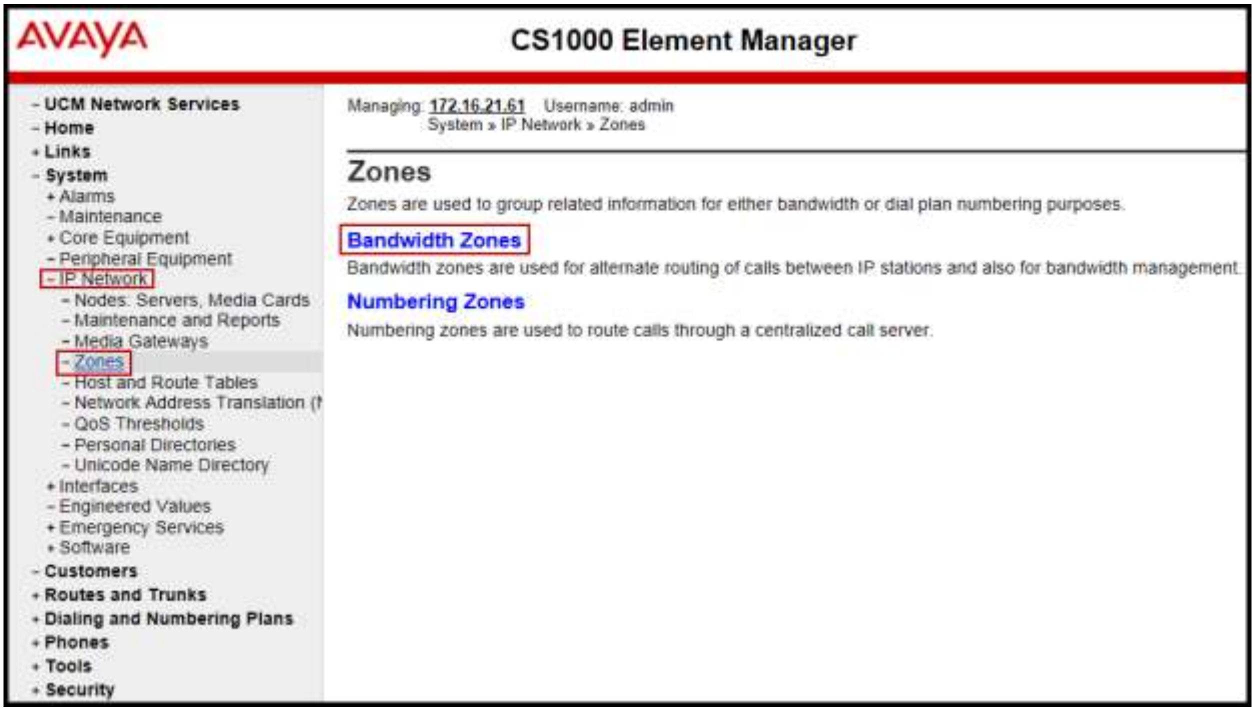


5.4. Administer Zones and Bandwidth

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 (zone 5)

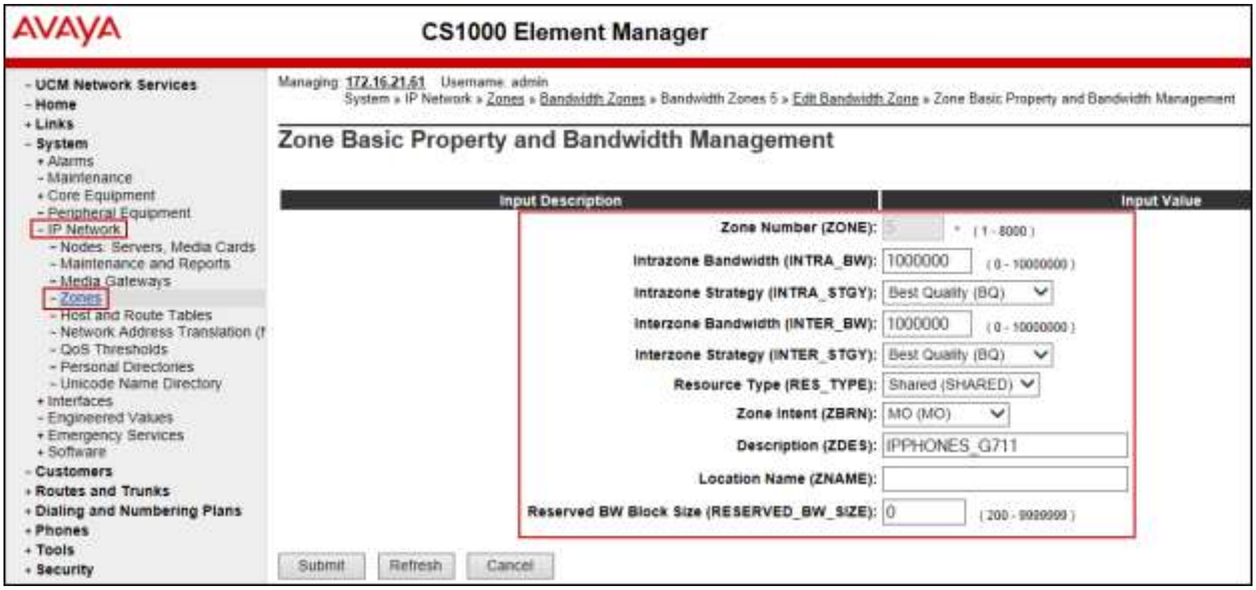
The following figures show how to configure a zone for IP sets for bandwidth management purposes. The bandwidth strategy can be adjusted to preference. Select **System→ IP Network → Zones** from the left pane, click on the **Bandwidth Zones** as shown below.



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

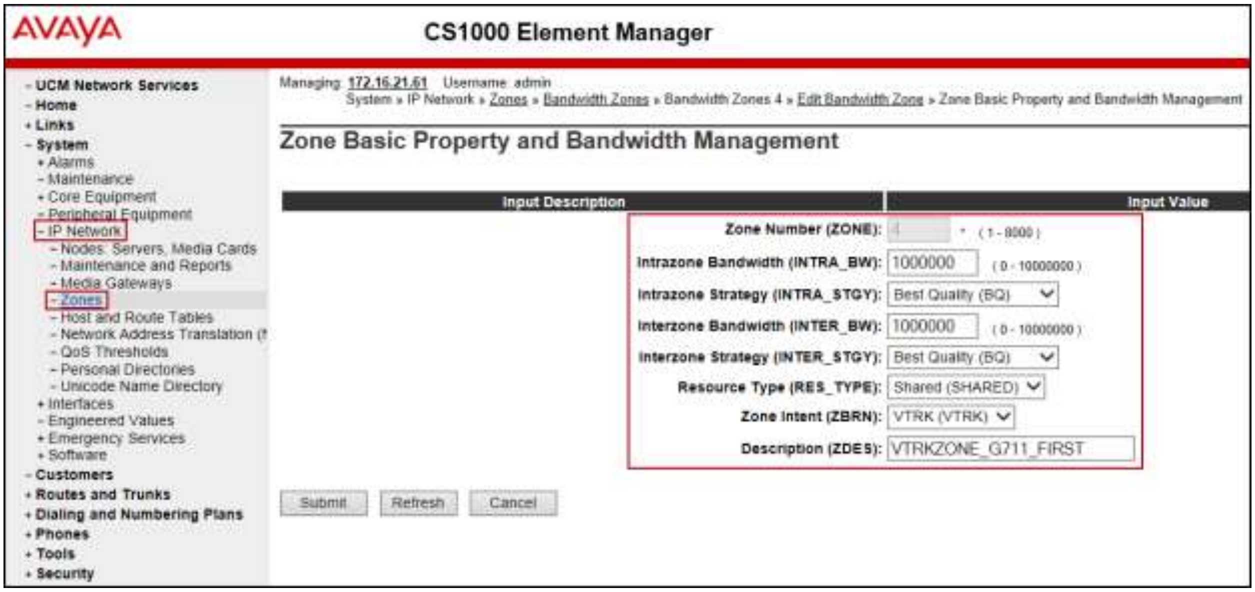
- **INTRA_STGY**: Bandwidth configuration for local calls, select **Best Quality (BQ).**
- **INTER_STGY**: Bandwidth configuration for the calls over trunk, select **Best Quality (BQ).**
- **ZBRN:** Select **MO** (**MO** is used for IP phones).

The values for **Zone 5** are shown below.



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 then select **Best Quality (BQ)** for both **INTRA_STGY** and **INTER_STGY**, as shown below. Click on the **Submit** button. For Claro, **Zone 4** was created for the Virtual SIP Trunks.

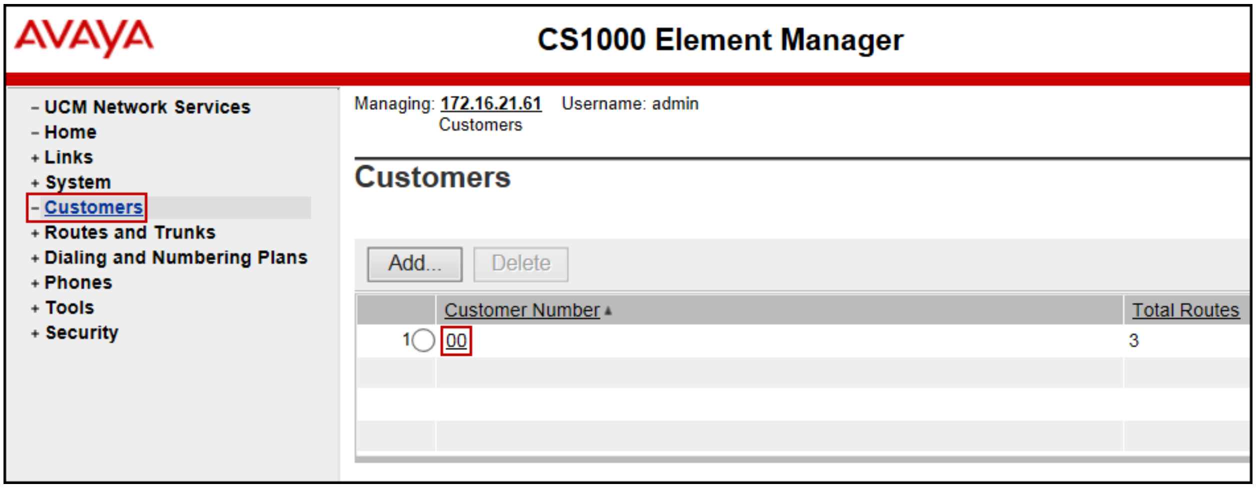


Note: Claro supports codec order G.711MU, G.711A and G.729A, with G.711MU being the preferred codec.

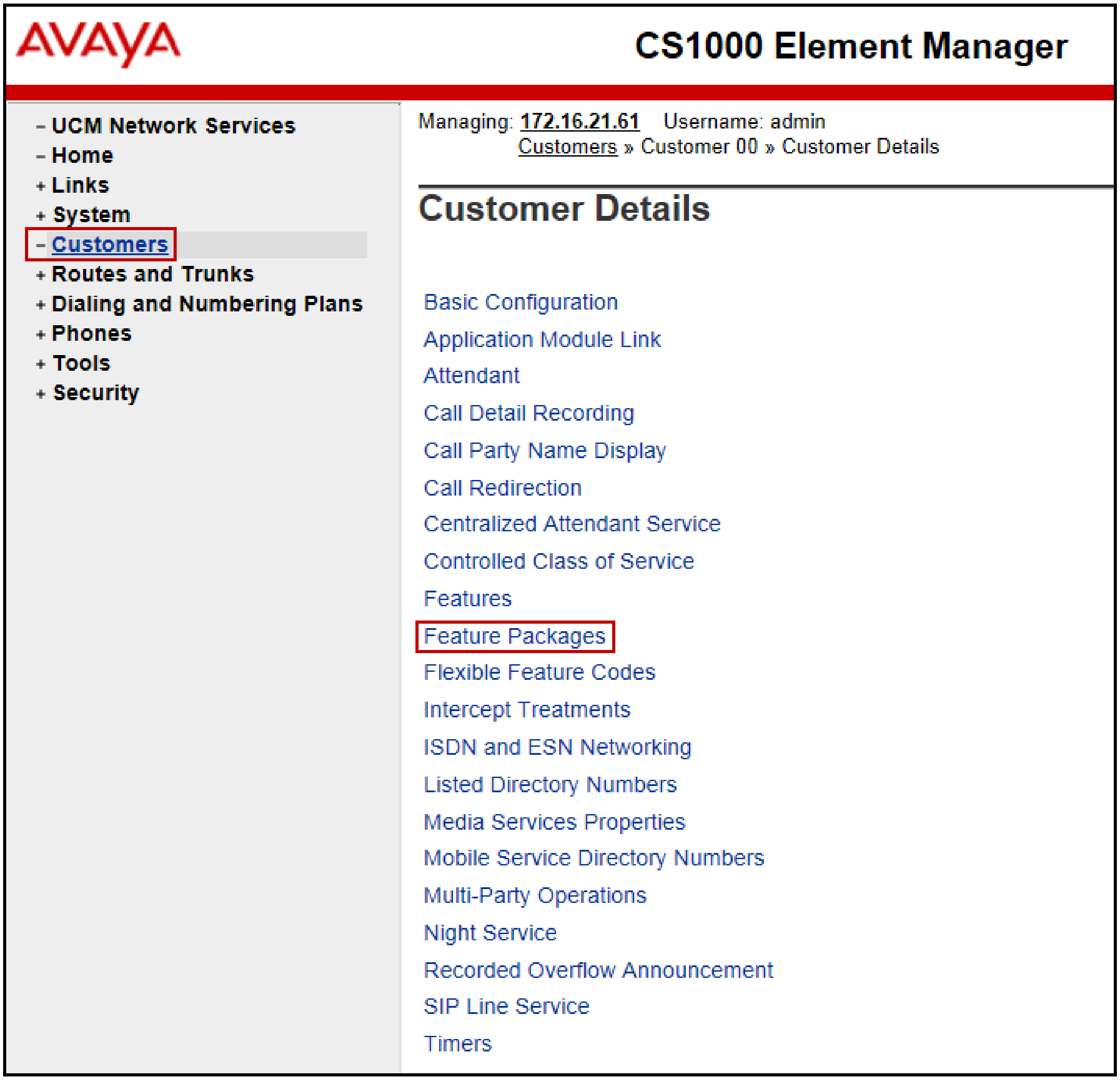
5.5. Administer SIP Trunk Gateway

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

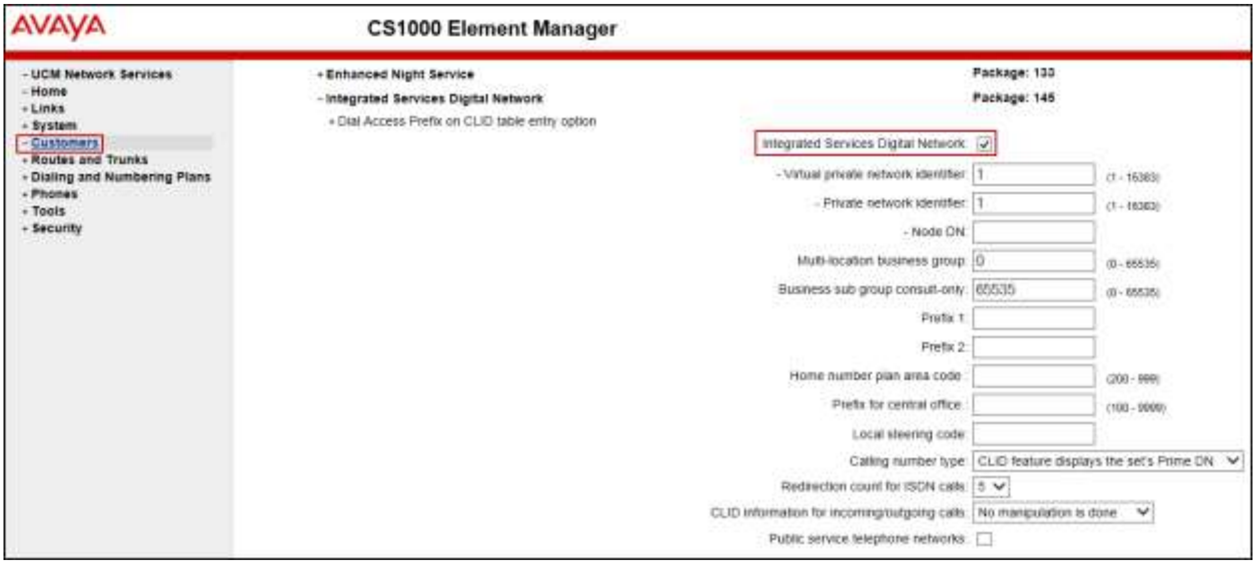
Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options.



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



The screen is updated with a list of **Feature 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 **Save** (not shown).



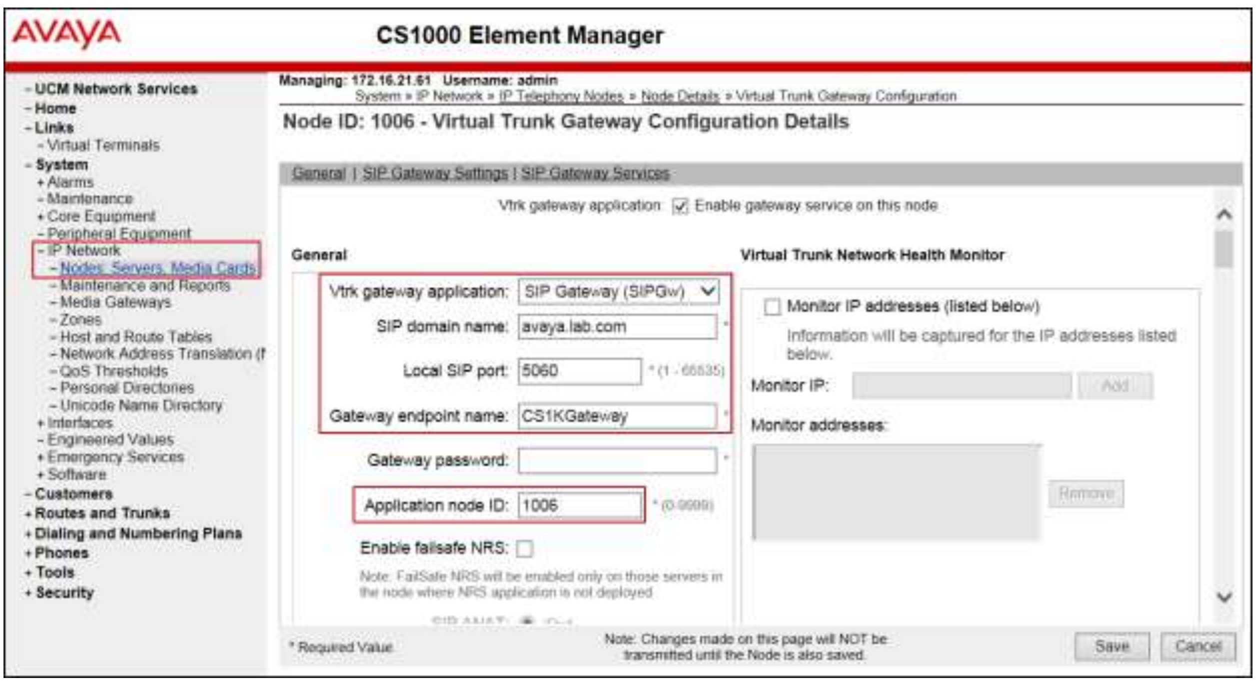
5.5.1. Administer the SIP Trunk Gateway to the Avaya SBCE

Select **System→ 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 as shown in **Section 5.2.1.**

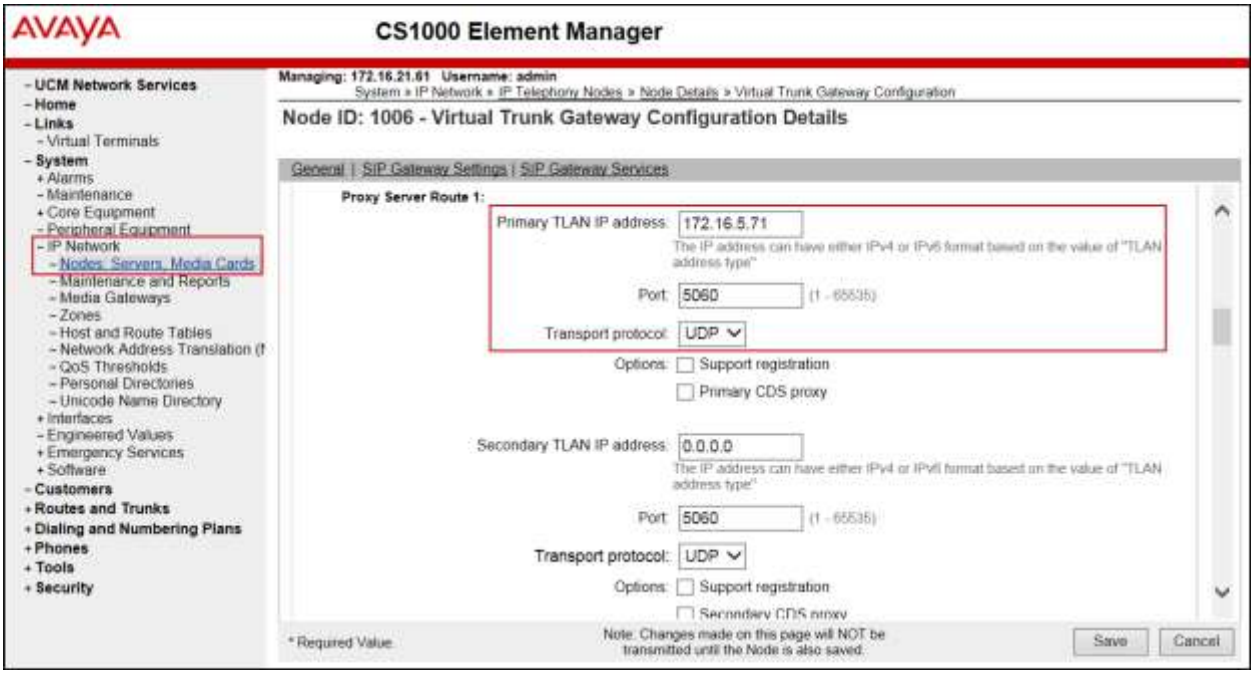
On the **Node Details** screen, select **Gateway (SIPGw)** (not shown).

Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown below. The parameters (highlighted in red boxes) are filled in to match values entered under the Server Configuration section of the Avaya SBCE (these are shown in **Section 6.2.3**).

- **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 exists, and 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, entries shown below were used during the compliance testing:

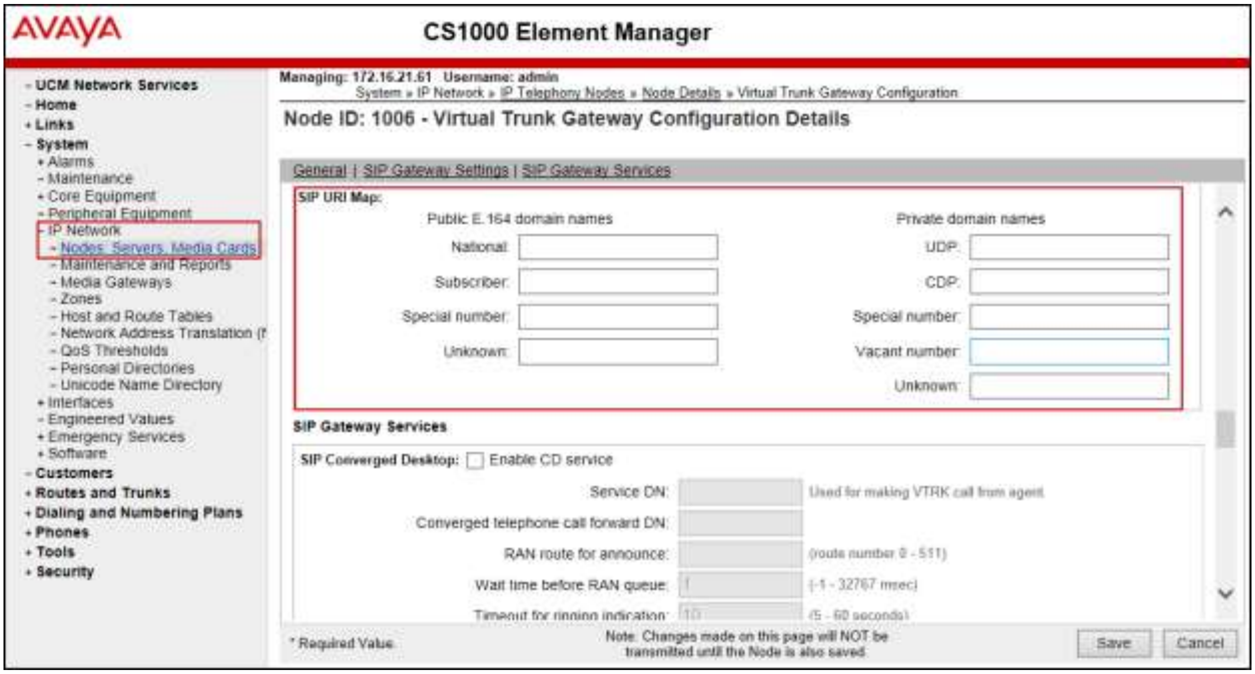
Under the **Public E.164 Domain Names**, for:

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

- Under the **Private Domain Names**, for:
- **UDP**: blank.
- **CDP**: blank.
- **Special Number**: blank.
- **Vacant number**: blank.
- **Unknown**: blank.

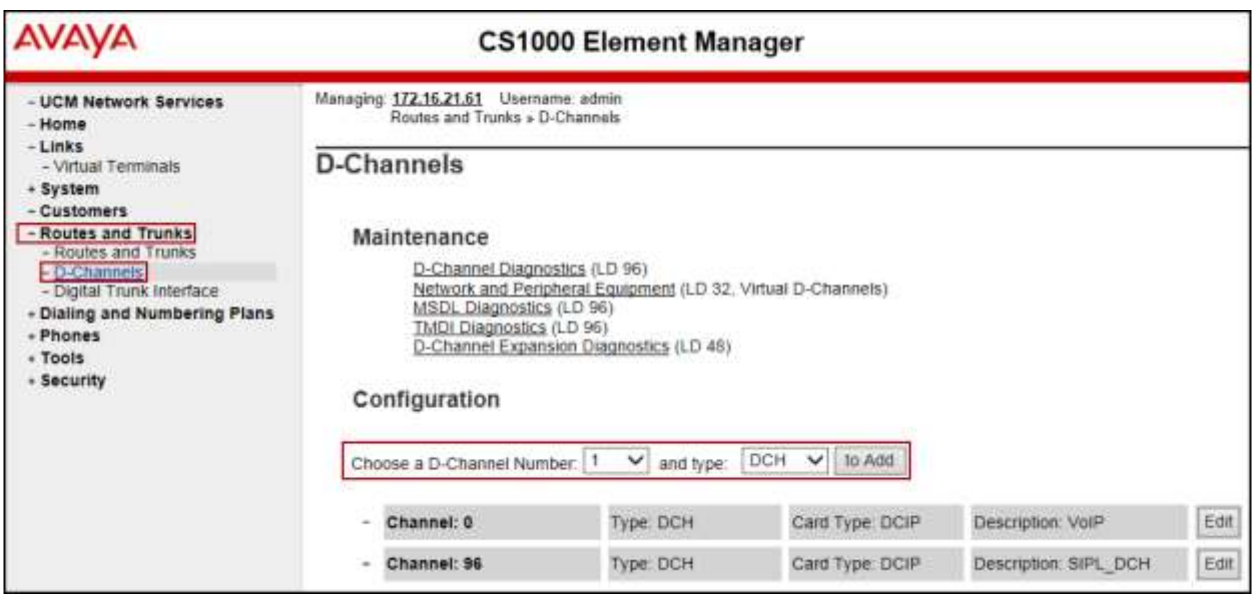
Note: The SIP URI Map entries shown above were used during the compliance testing; it is possible that in a customer environment other values are used.

Click on the **Save** button and synchronize the new configuration as shown under **Section 5.3.2**.



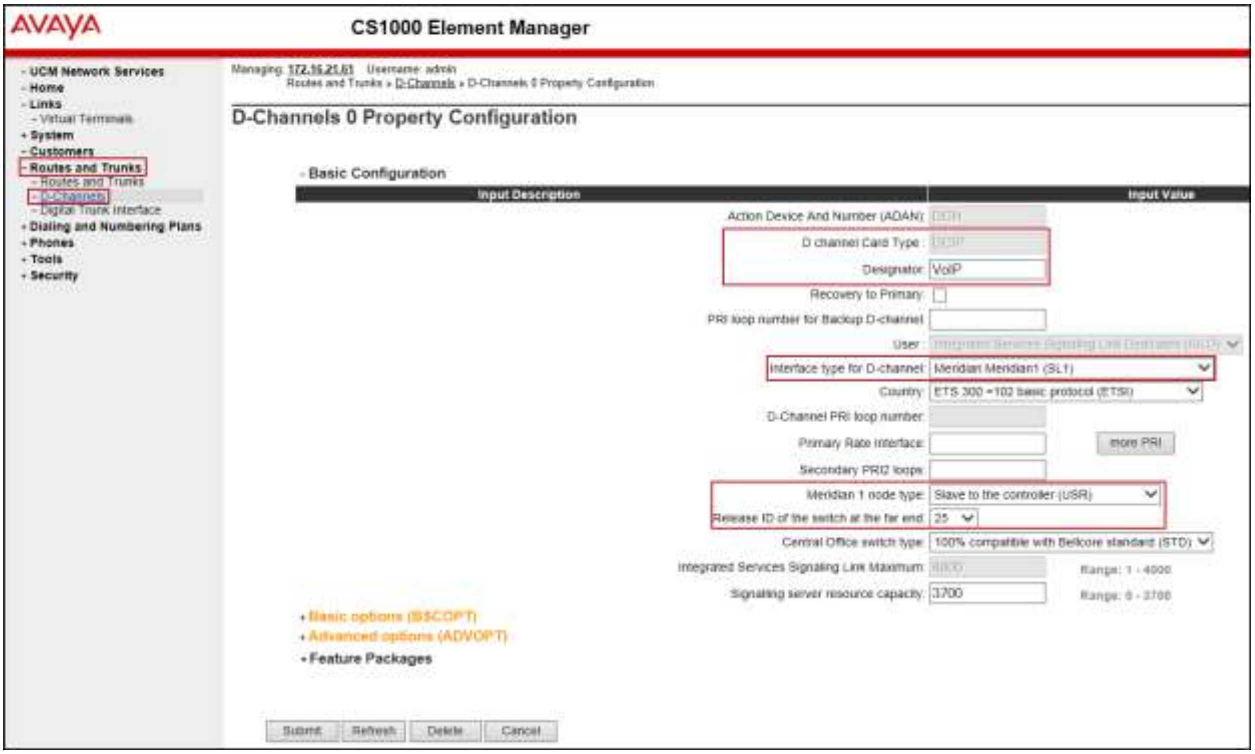
5.5.2. Administer Virtual D-Channel

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 the **to Add** button**.**



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

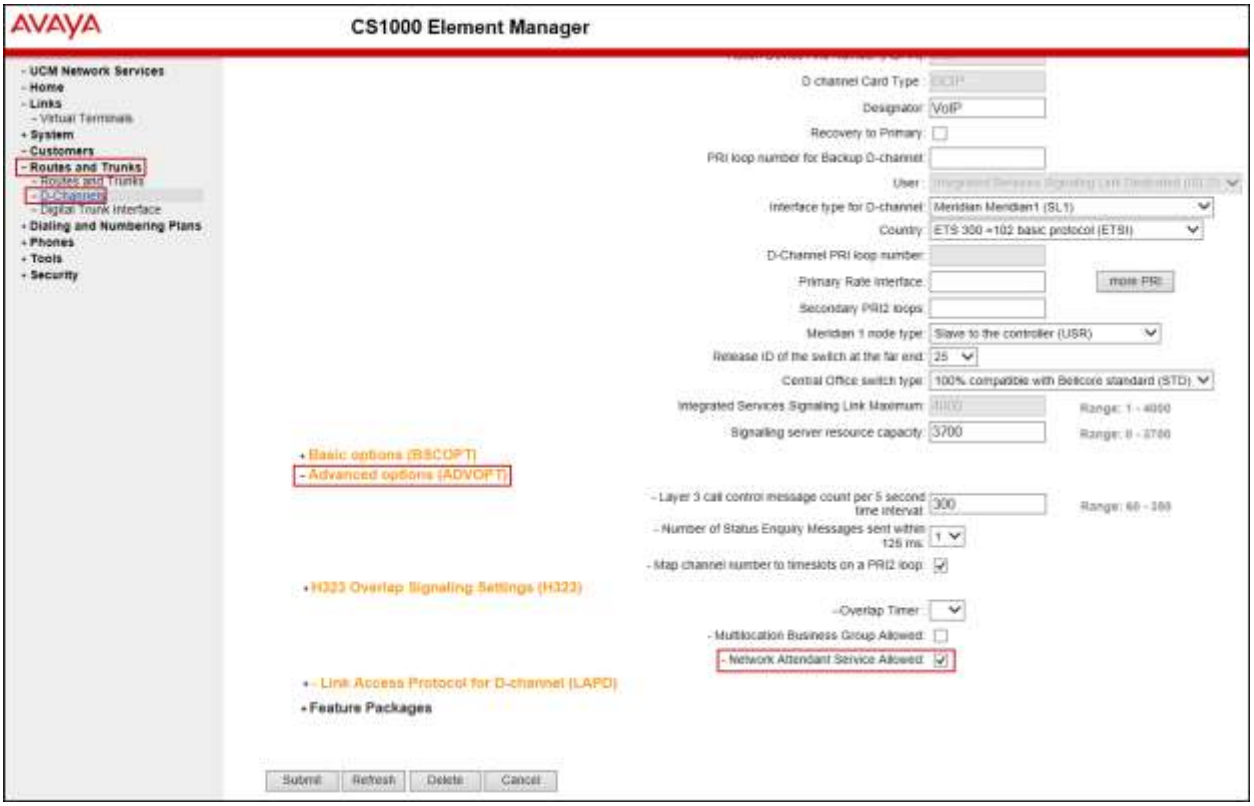
- **D channel Card Type (CTYP): D-Channel is over IP (DCIP)**.
- **Designator (DES)**: A descriptive name.
- **Interface type for D-channel (IFC): Meridian Meridian1 (SL1)**.
- **Meridian 1 node type: Slave to the controller (USR)**.
- **Release ID of the switch at the far end (RLS): 25**.



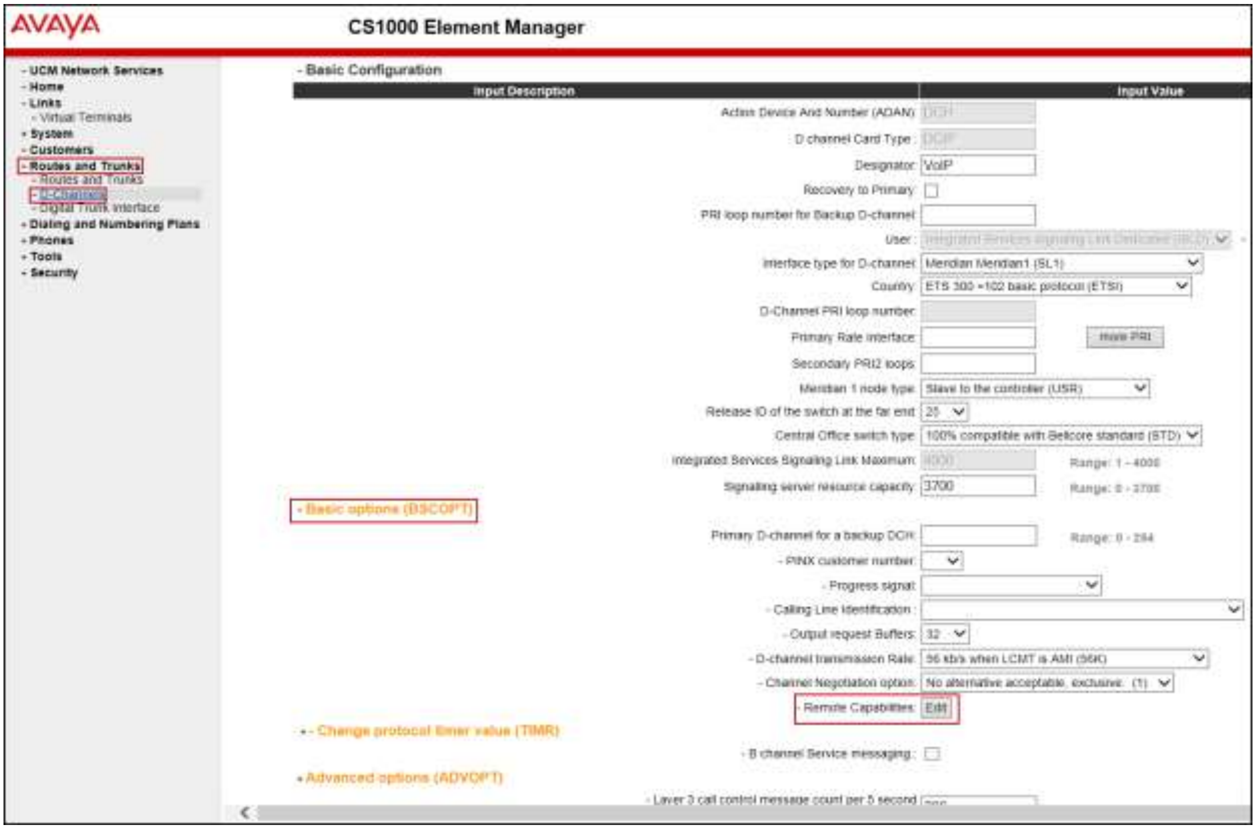
On the same page scroll down and enter the following values for the specified fields:

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

Retain the default values for the remaining fields.

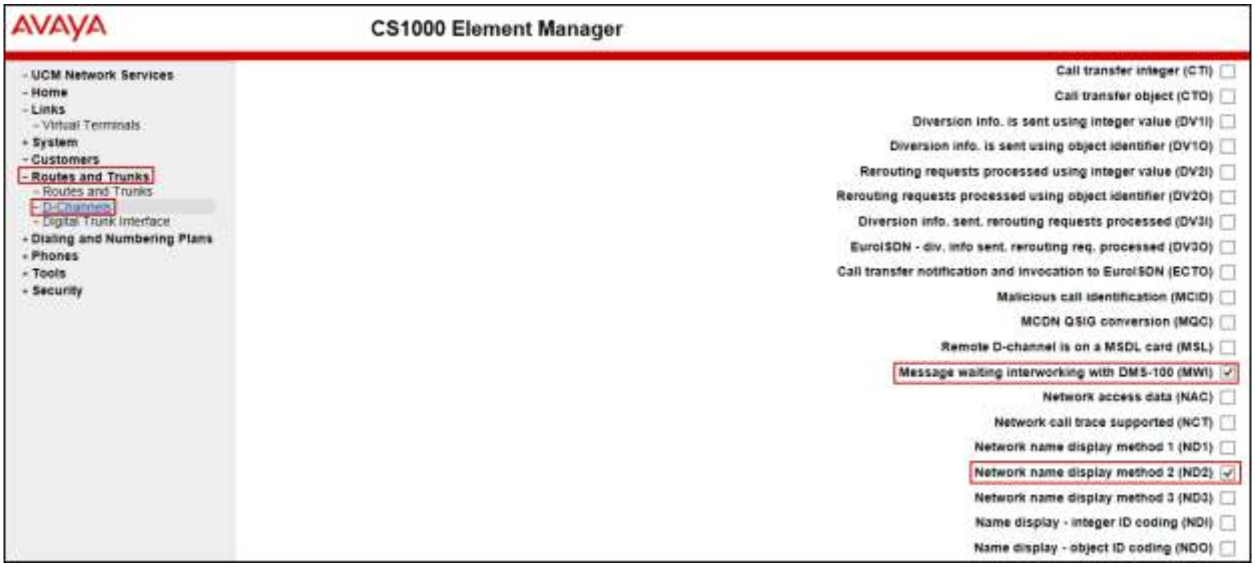


Click on the **Basic Options (BSCOPT)** link and click on the **Edit** button for the **Remote Capabilities** attribute, as shown below.



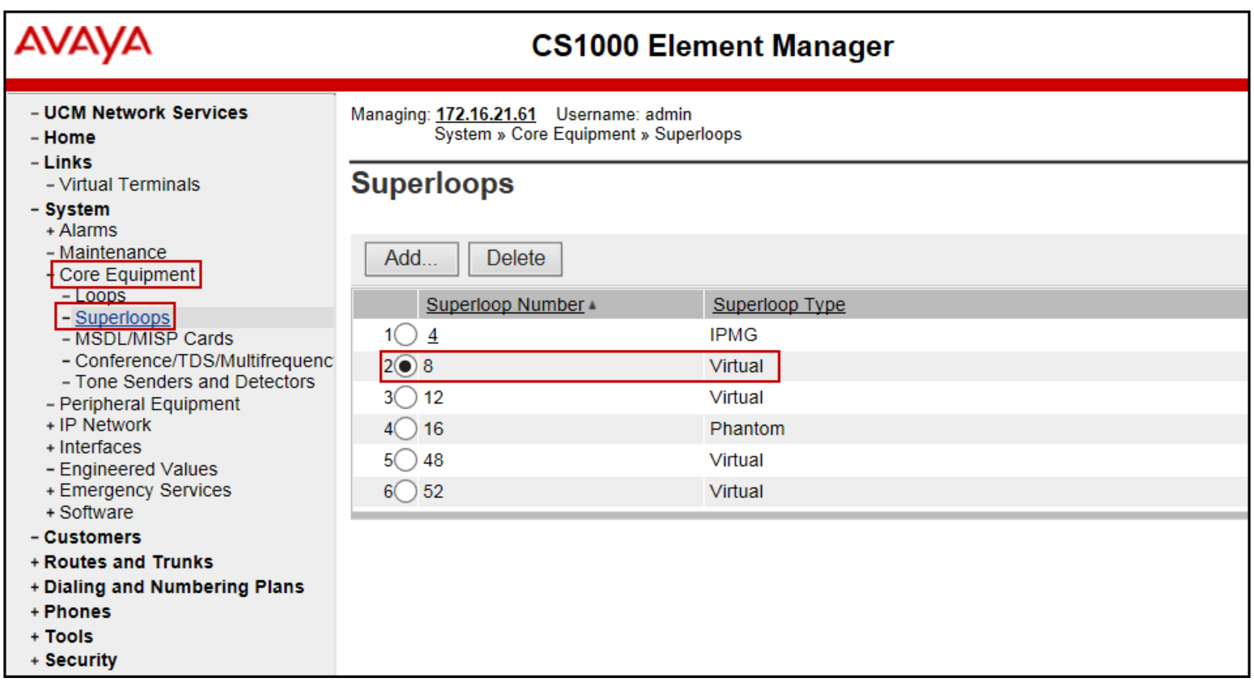
The **Remote Capabilities Configuration** page will appear. Check **ND2** and **MWI** (if mailboxes are present on the CS1000 Call Pilot) checkboxes as shown below.

Click on **Return – Remote Capabilities** button (not shown).
Click on the **Submit** button at the bottom of the previous screen (not shown).



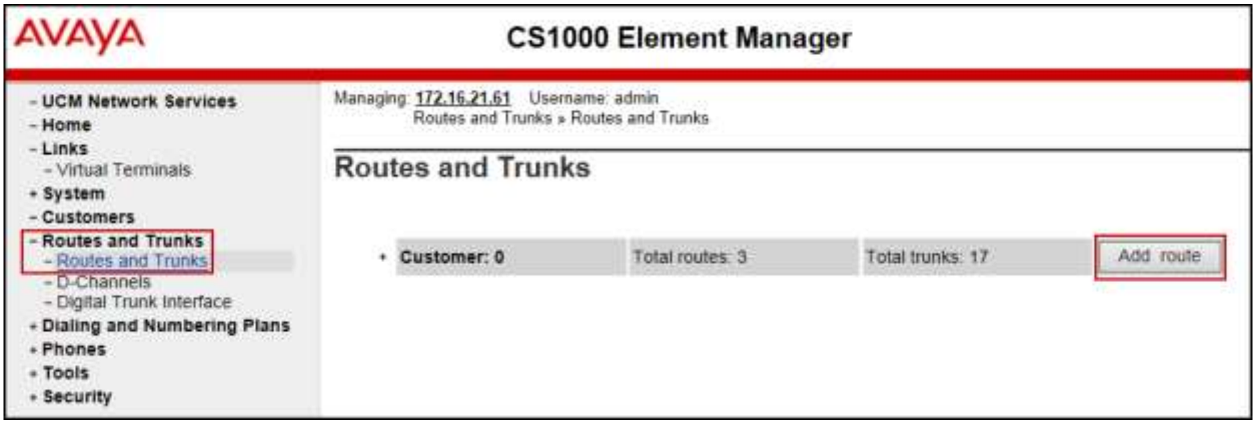
5.5.3. Administer Virtual Superloop

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



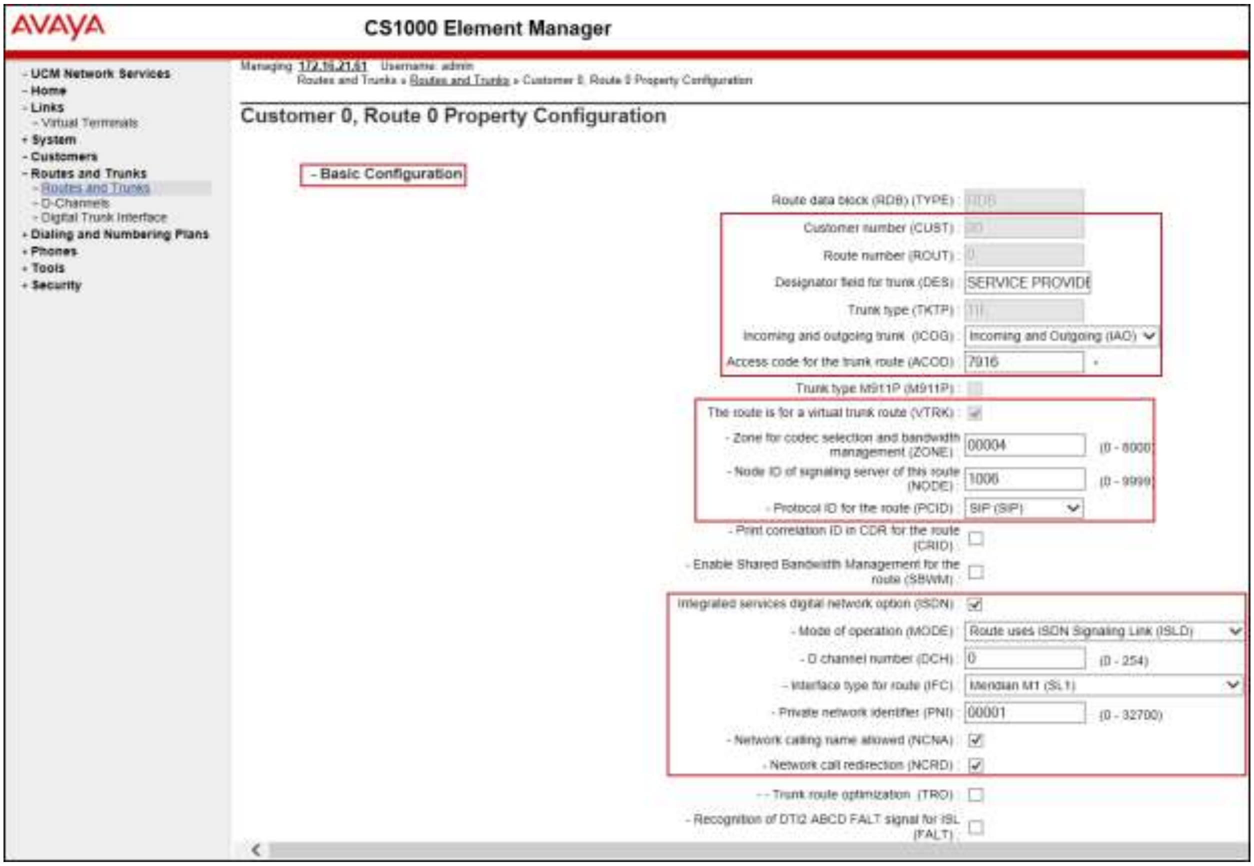
5.5.4. Administer Virtual SIP Routes

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.

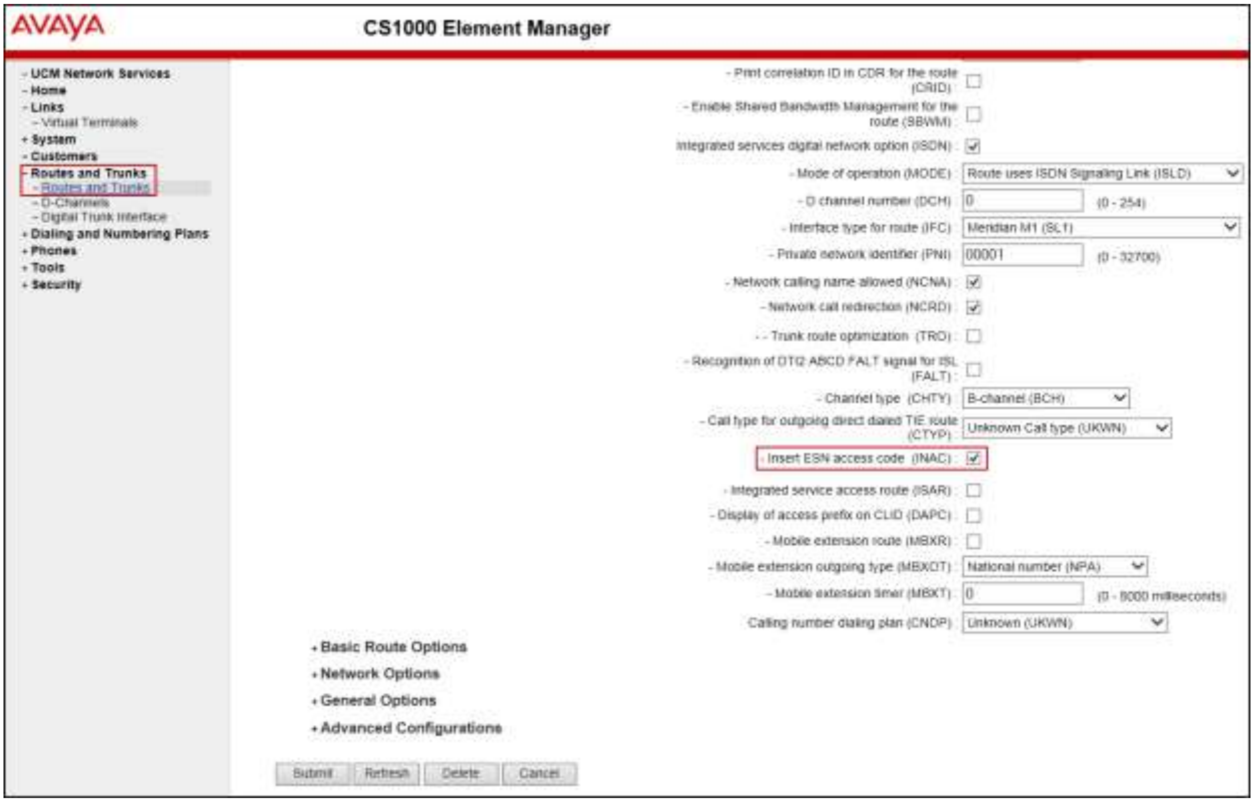


The **Customer 0**, **Route 0 Property Configuration** screen is displayed next. Scroll down until the **Basic Configuration** Section is displayed and enter the following values for the specified fields. Retain the default values for the remaining fields as shown below.

- **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.

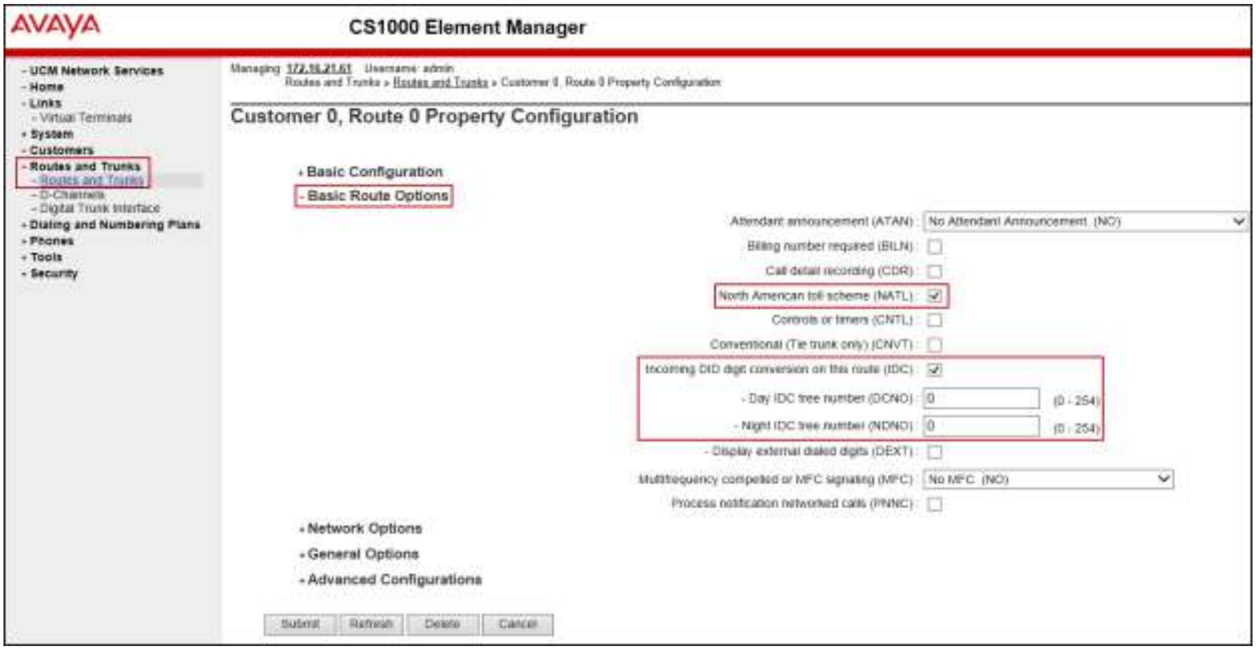

AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
+ System
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
+ Dialing and Numbering Plans
+ Phones
+ Tools
+ Security
Managing: 172.16.21.61 Username: admin
Routes and Trunks » Routes and Trunks » Customer 0, Route 0 Property Configuration
Customer 0, Route 0 Property Configuration
- Basic Configuration
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 00
Route number (ROUT) : 0
Designator field for trunk (DES) : SERVICE PROVIDE
Trunk type (TKTP) : TIE
Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD) : 7916
Trunk type M911P (M911P) :
The route is for a virtual trunk route (VTRK) :
- Zone for codec selection and bandwidth management (ZONE) : 00004 (0 - 8000)
- Node ID of signaling server of this route (NODE) : 1006 (0 - 9999)
- Protocol ID for the route (PCID) : SIP (SIP)
- Print correlation ID in CDR for the route (CRID) :
- Enable Shared Bandwidth Management for the route (SBWM) :
Integrated services digital network option (ISDN) :
- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) : 0 (0 - 254)
- Interface type for route (IFC) : Meridian M1 (SL1)
- Private network identifier (PNI) : 00001 (0 - 32700)
- Network calling name allowed (NCNA) :
- Network call redirection (NCRD) :
- - Trunk route optimization (TRO) :
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :

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



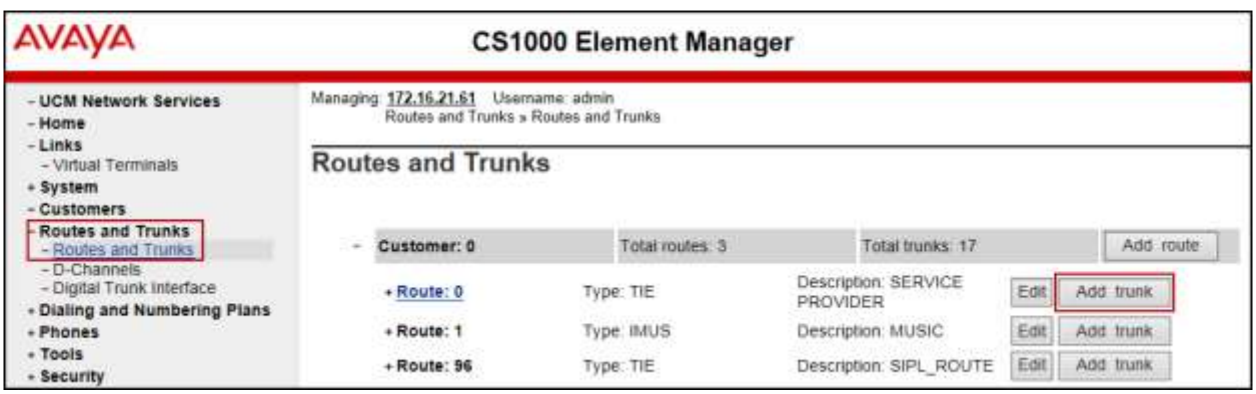
Click on **Basic Route Options**,

- Check **North American toll scheme (NATL)**.
- Check **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** Error! Reference source not found..
- Click on the **Submit** button shown at the bottom of the screen.



5.5.5. Administer Virtual Trunks

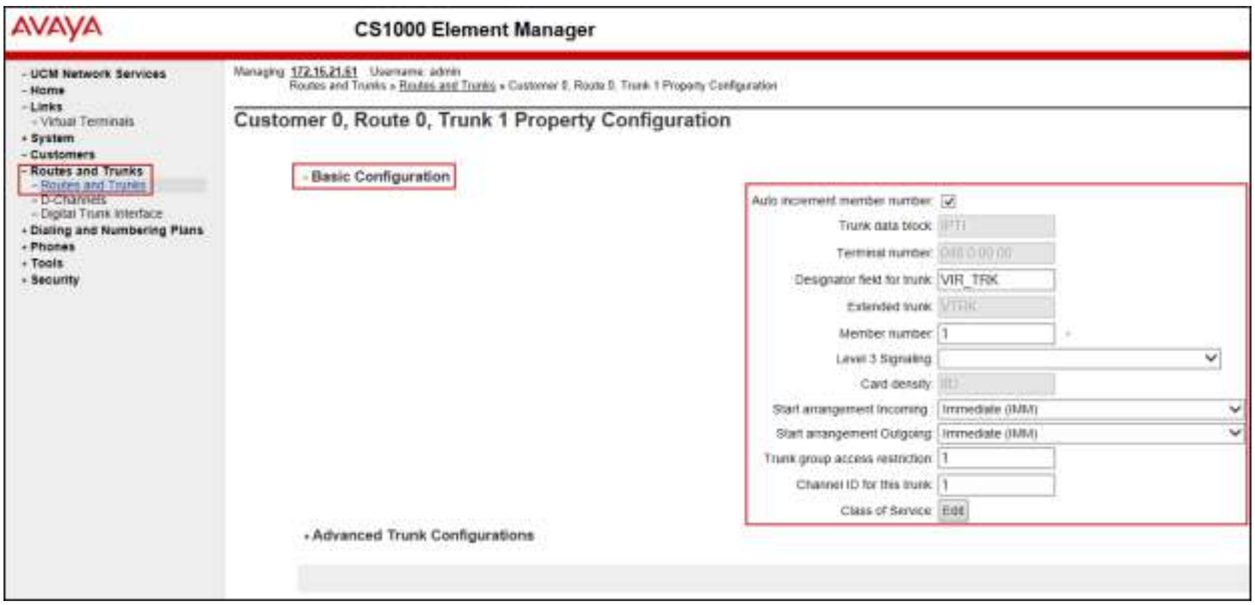
Continue from **Section 5.5.4**, after clicking on **Submit**, the **Routes and Trunks** screen is displayed and updated with the newly added route. In the example, **Route 0** was added. Click on the **Add trunk** button next to the newly added route 0 as shown below.



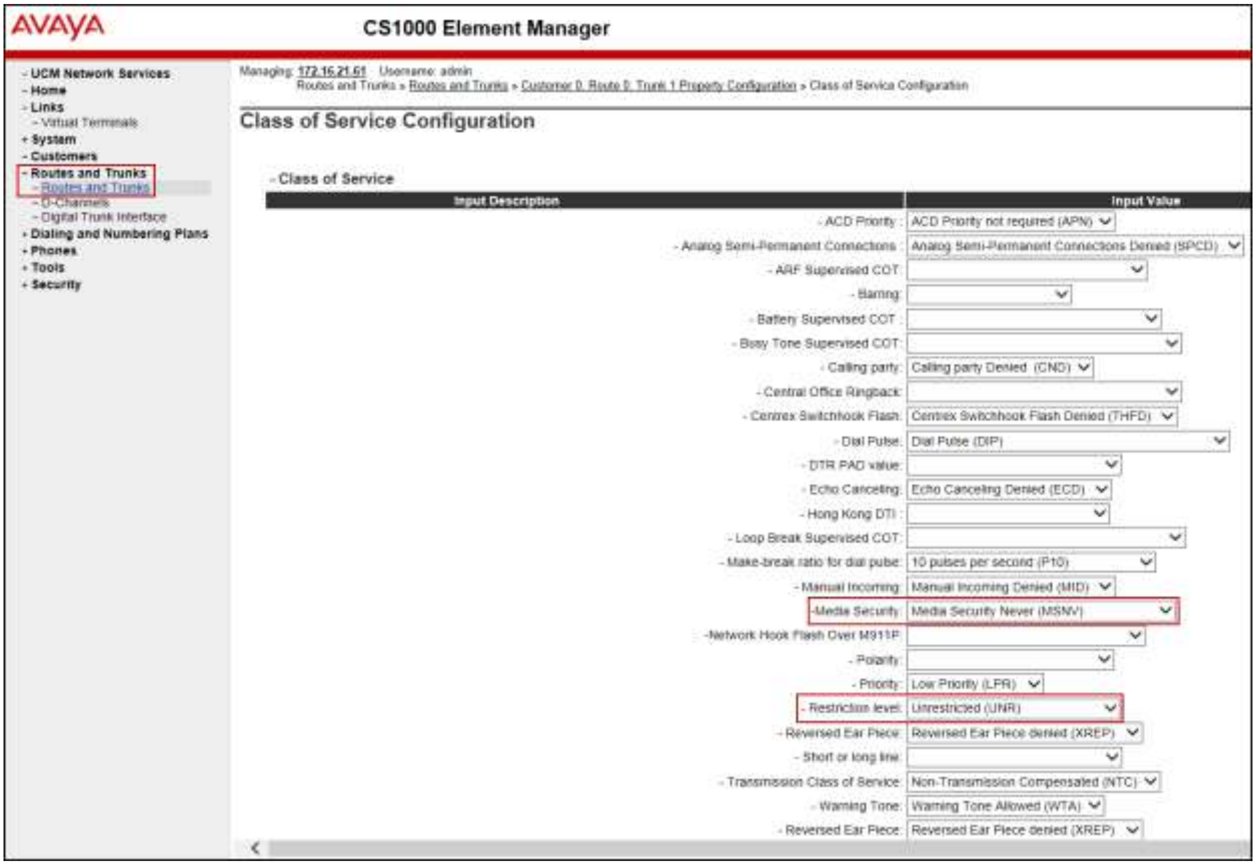
The **Customer 0, Route 0, Trunk 1 Property Configuration** screen is displayed as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields.

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 superloop created in **Section 5.5.3**).
- **Designator field for trunk** (**DES**): A descriptive text.
- **Extended Trunk (XTRK): Virtual trunk (VTRK)**.
- **Member number** (**RTMB**): 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.

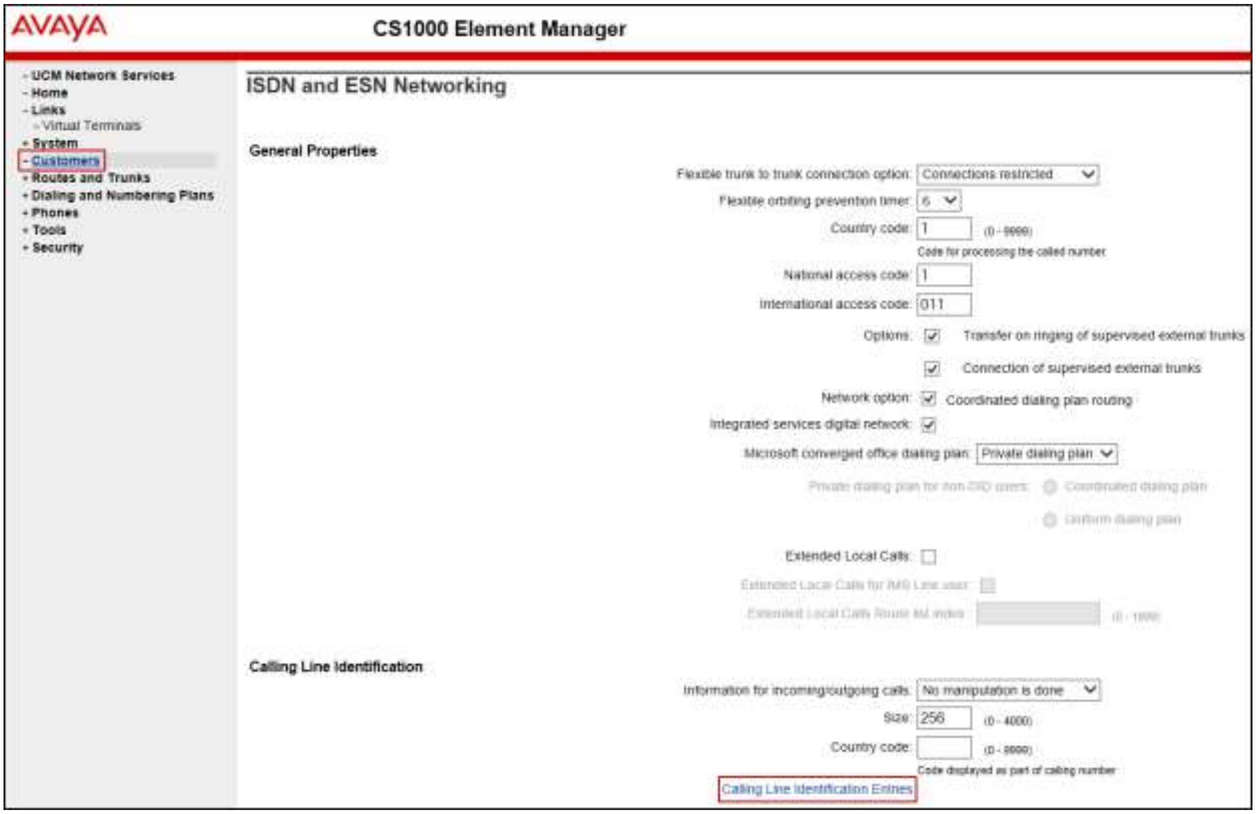


Click on **Edit Class of Service** (shown on previous screen). For **Media Security**, select **Media Security Never** (**MSNV),** for **Restriction Level**, select **Unrestricted (UNR)**. Use defaults for remaining values. Scroll down to the bottom of the screen and click **Return Class of Service**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

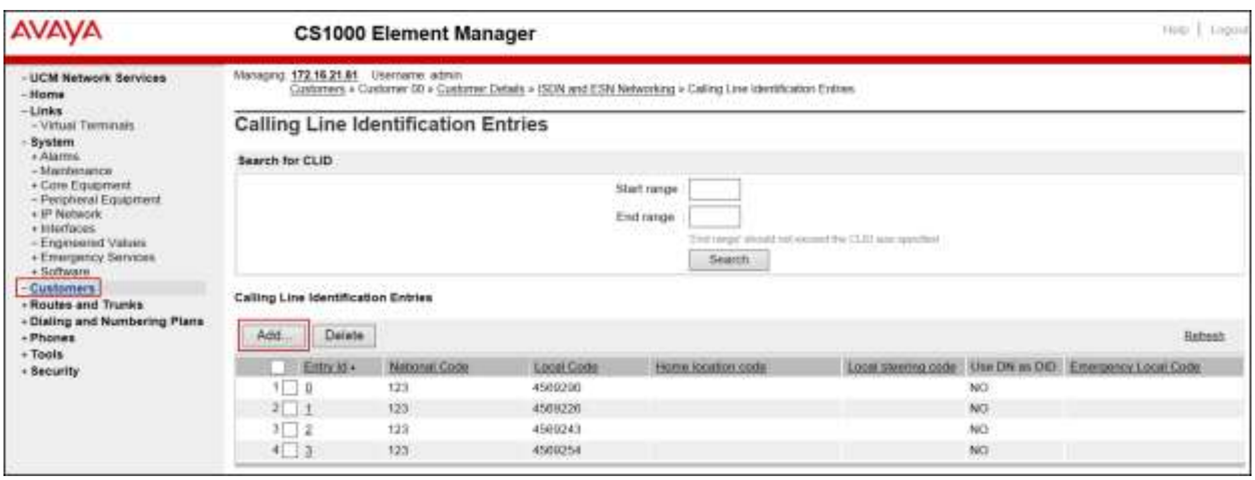


5.5.6. Administer Calling Line Identification Entries

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



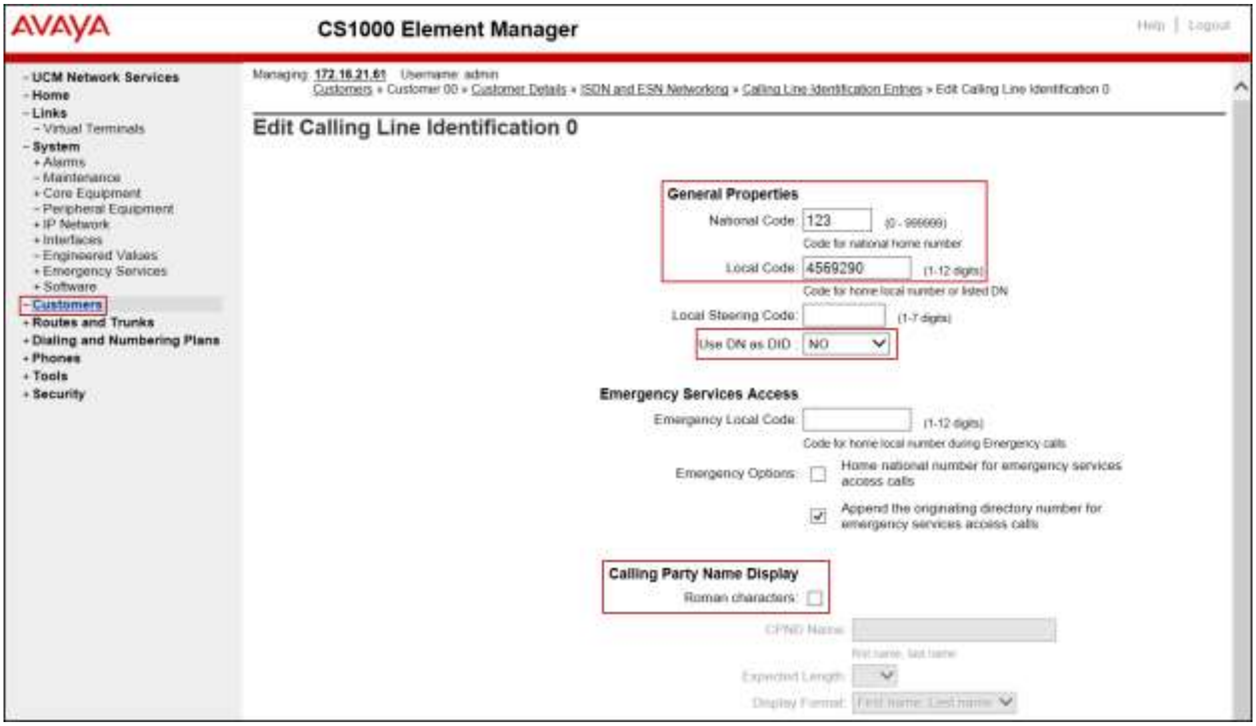
Click on **Add** as shown below.



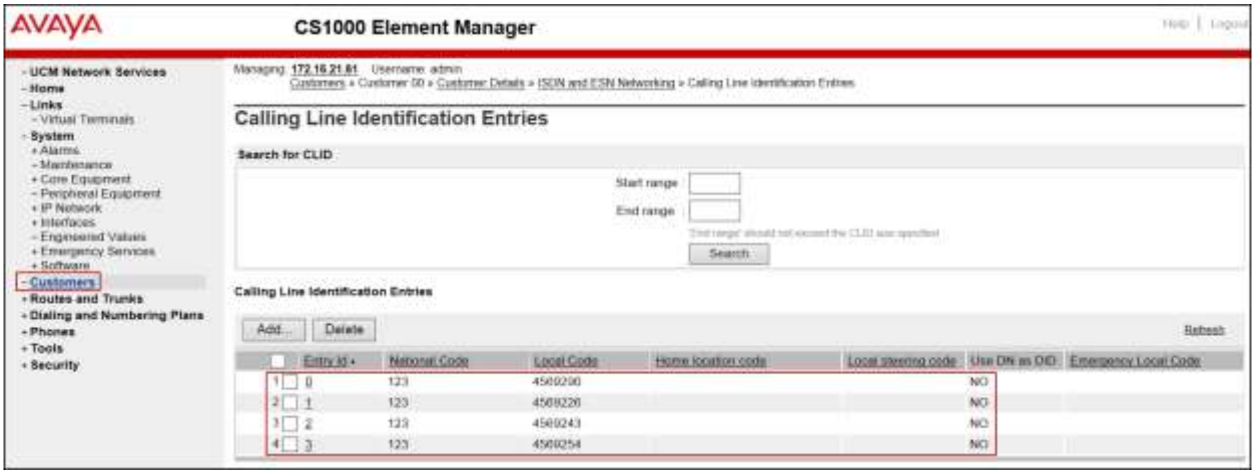
Add entry **0** as shown below, click on the **Save** button (not shown) after adding each entry.

- **National Code**: Input the three digit area code prefix of the DID number assigned by the service provider, in this case **123** (Note that digits have been masked for security reasons).
- **Local Code**: Input the seven digit number of the DID assigned by the service provider, in this case it is **4569290** (Note that digits have been masked for security reasons).
- **Use DN as DID**: Select **NO**.
- **Calling Party Name Display**: Uncheck for **Roman characters**.

Repeat for each of the DID numbers to be assigned to extensions in the CS1000 using **Entry Id 1, 2, 3, 4**, **etc**.



The following screen shows the **Calling Line Identification Entries** used for the compliance testing.



Enable External Trunk to Trunk Transfer:

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

- Login to the 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**.

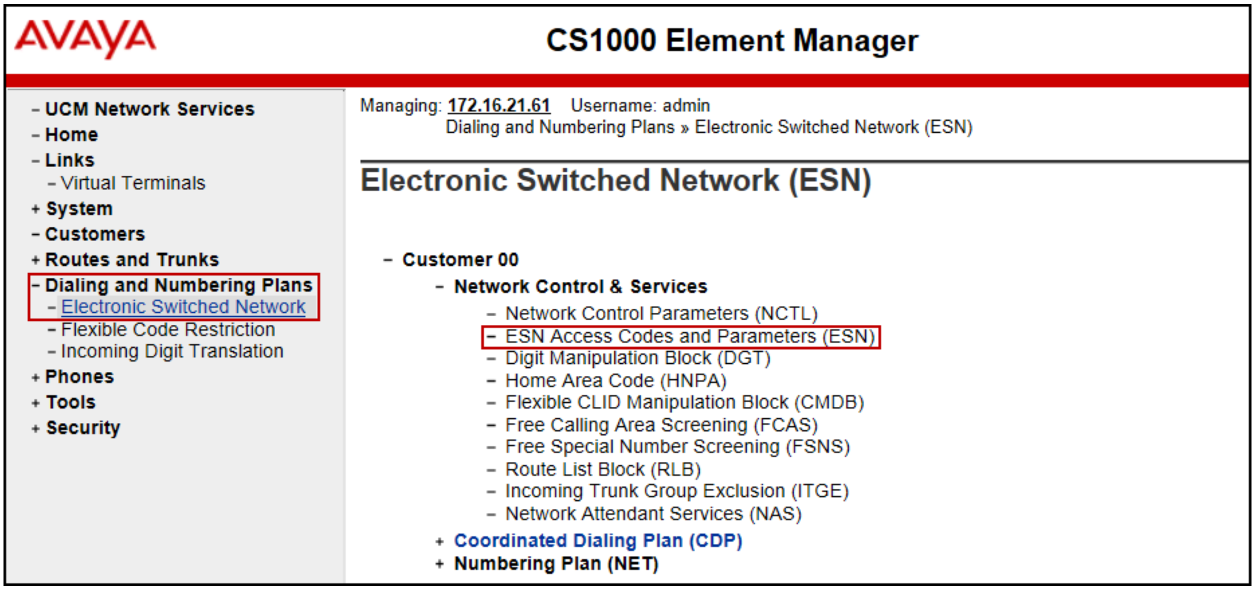
```
>ld 15 CDB000
MEM AVAIL: (U/P): 43552101    USED U P: 371282 939078    TOT: 44862461
DISK SPACE NEEDED: 1713 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
....
TRNX yes
EXTT yes
....
```

5.6. Administer Dialing Plans

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

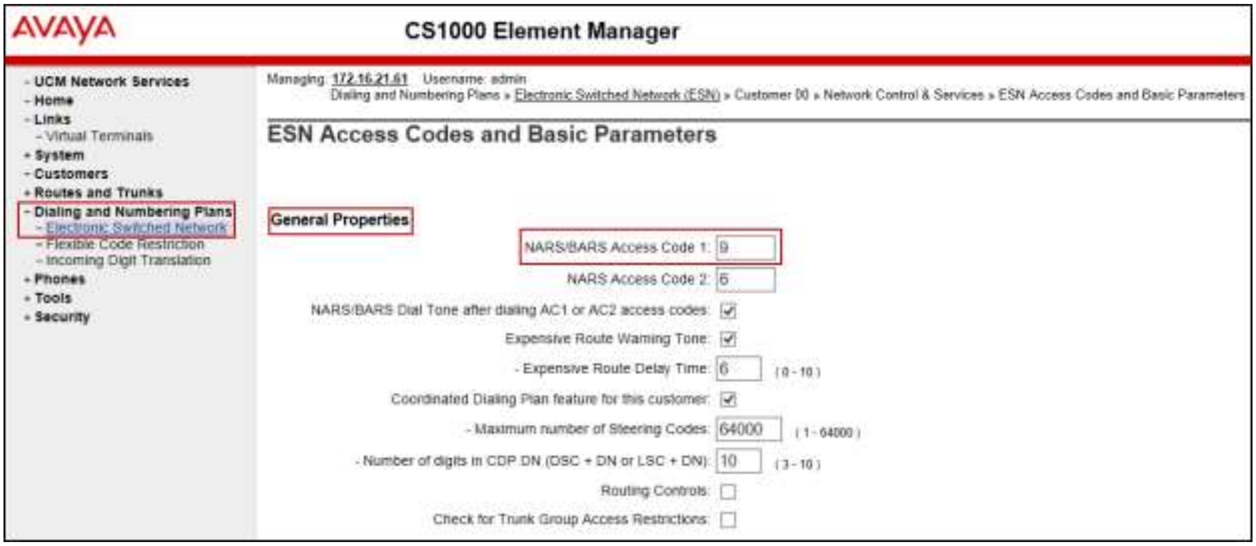
5.6.1. Define ESN Access Codes and Parameters (ESN)

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 from being 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
…
```

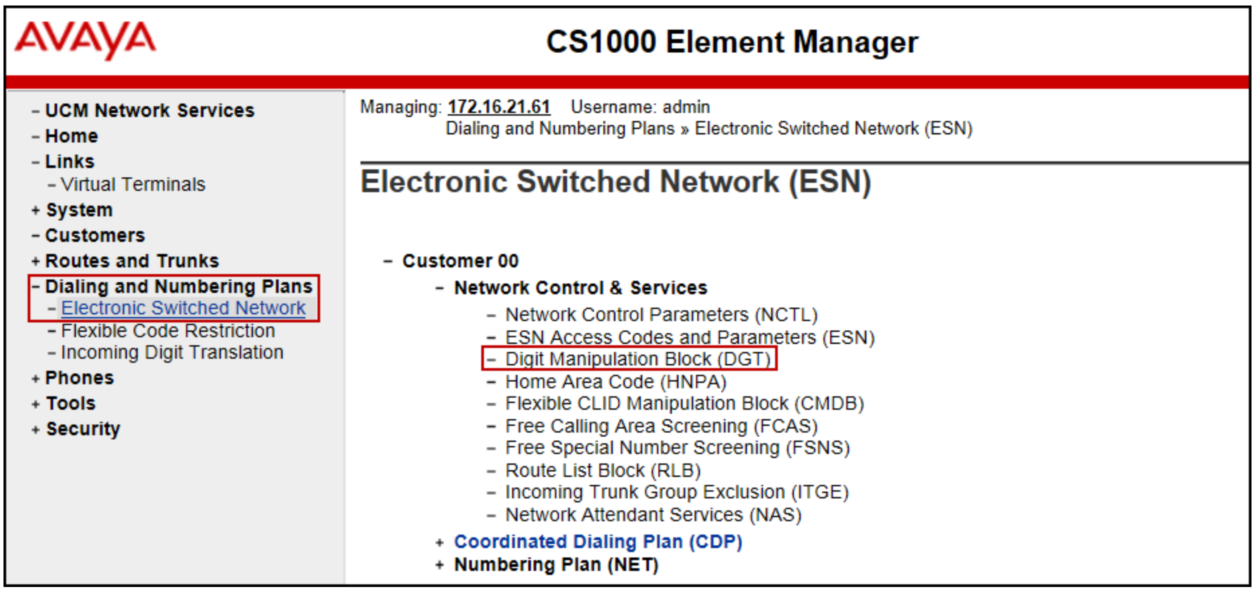
Verify Customer **Net_Data** block by using **LD 21**.

```
>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
…
```

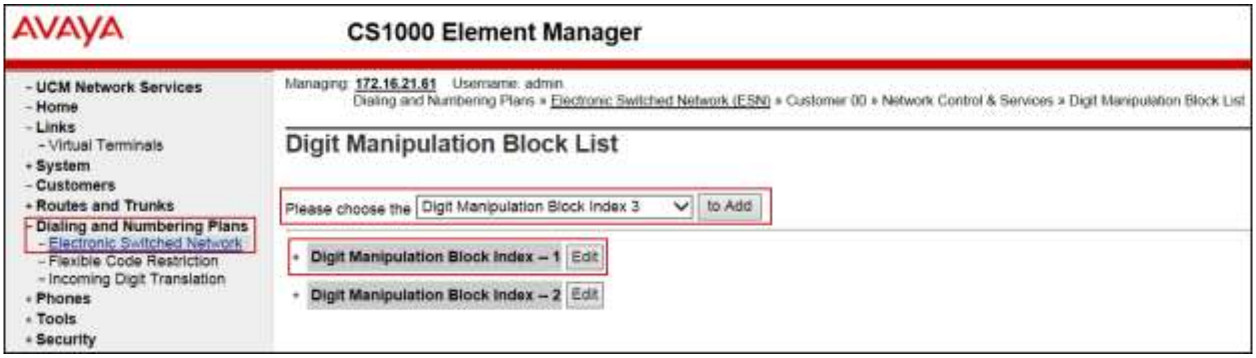
5.6.3. Digit Manipulation Block Index (DMI)

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.

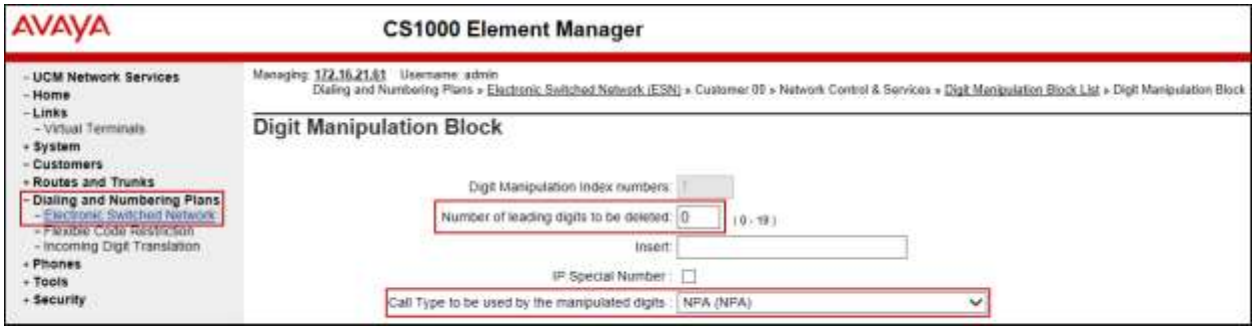


In the **Please choose the Digit Manipulation Block Index** drop-down field, select an available DMI from the list and click **to Add** as shown below.

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

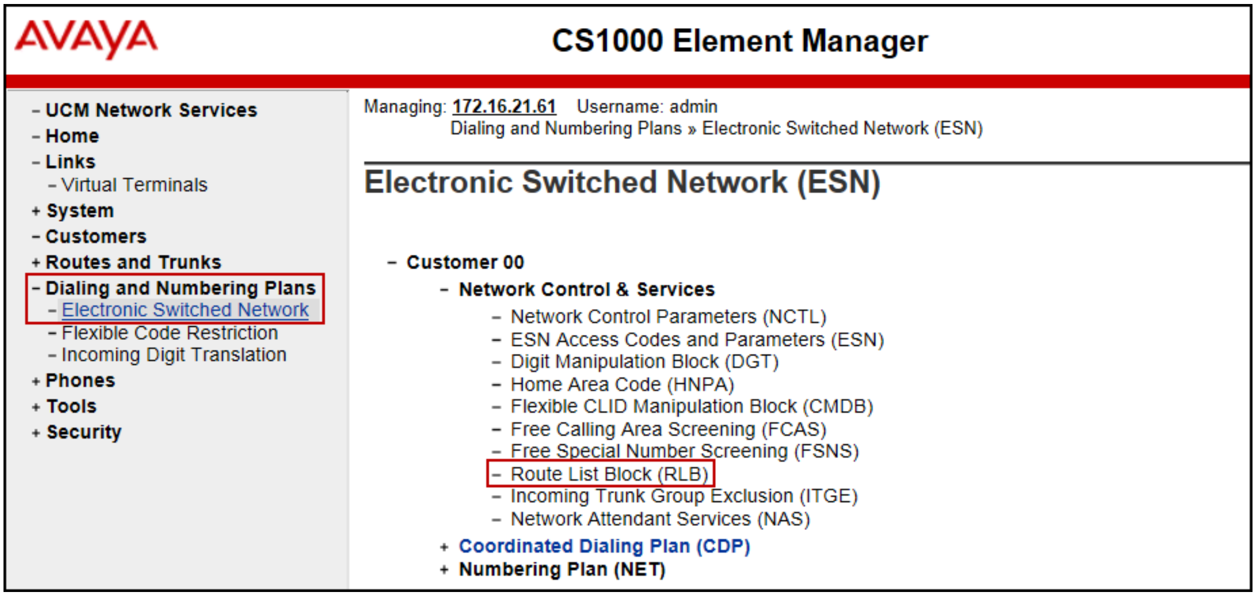


Enter **0** for the **Number of leading digits to be deleted** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits**, then click **Submit** (not shown).



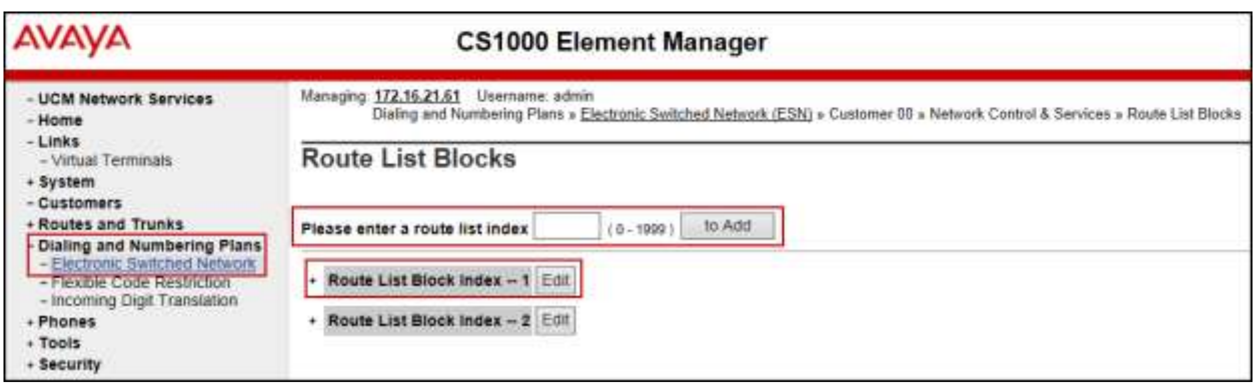
5.6.4. Route List Block (RLB)

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.



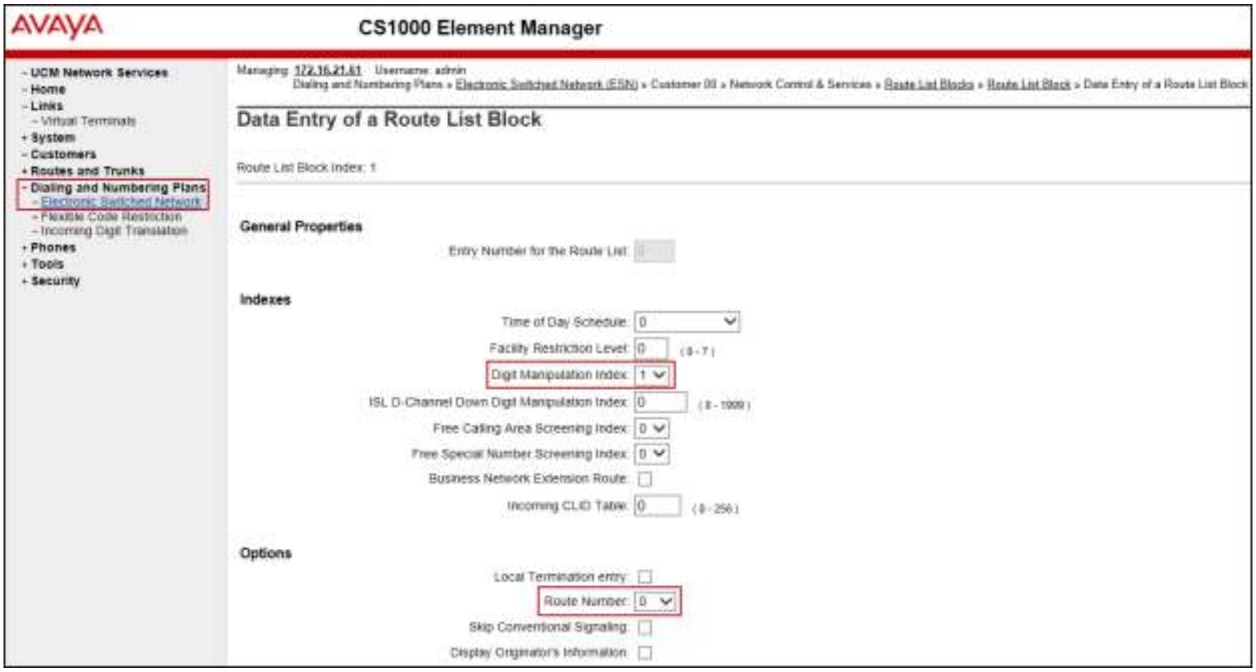
Enter an available value in the **Please enter a route list index** and click on the "**to Add"** button as shown below.

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** buttons (not shown).

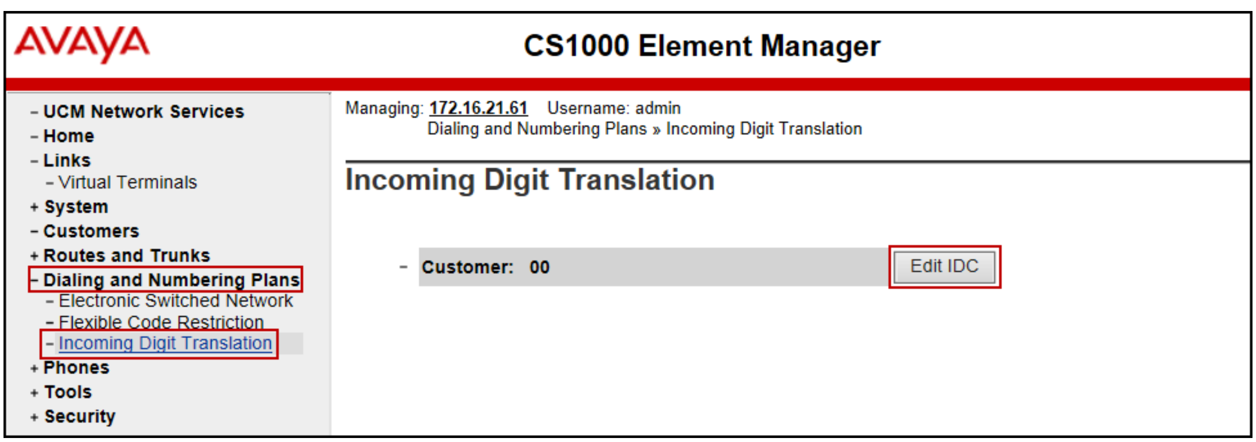
- **Digit Manipulation Index** (DMI): **1** (created in **Section 5.6.3**).
- **Route number** (ROUT): **0** (created in **Section 5.5.4**).



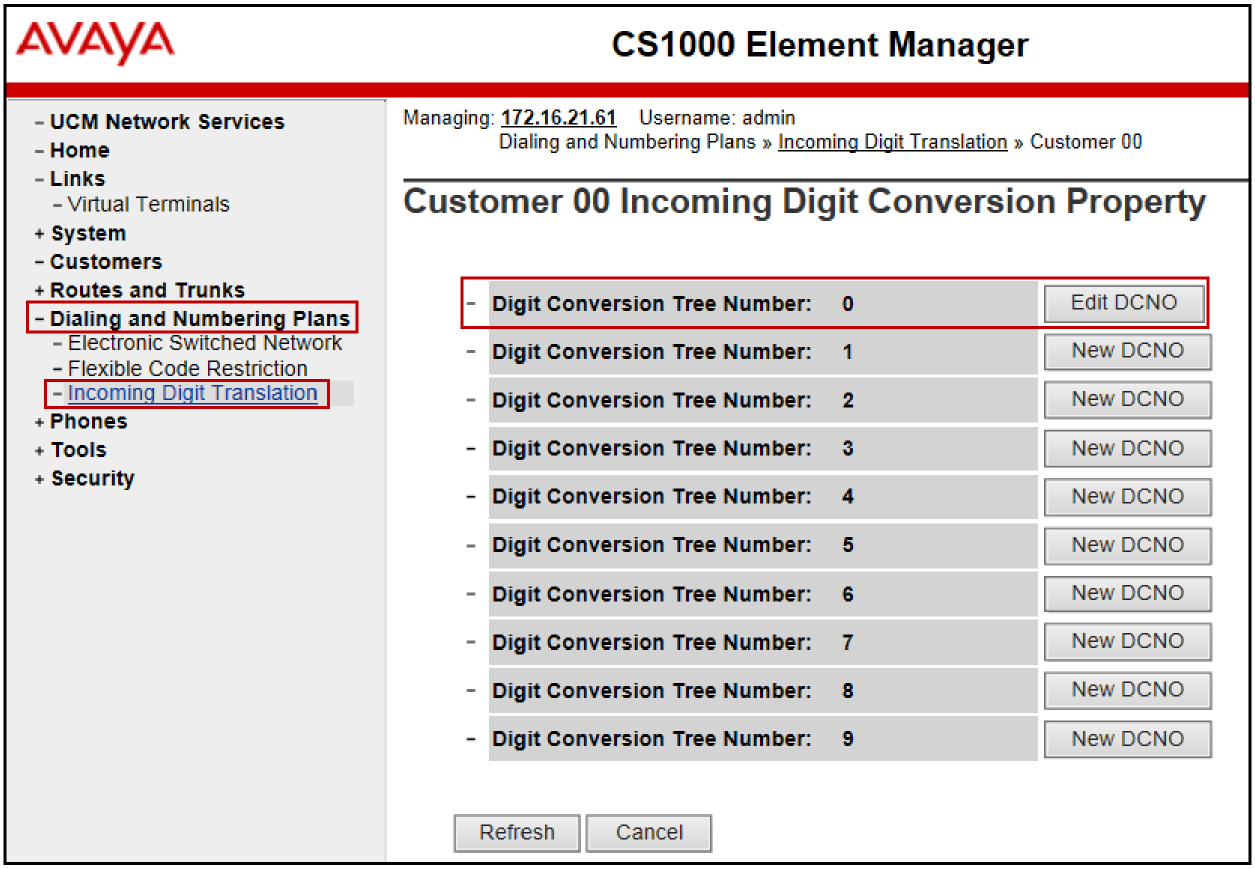
5.6.5. Inbound Digit Translation

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 the **Edit IDC** button as shown below.

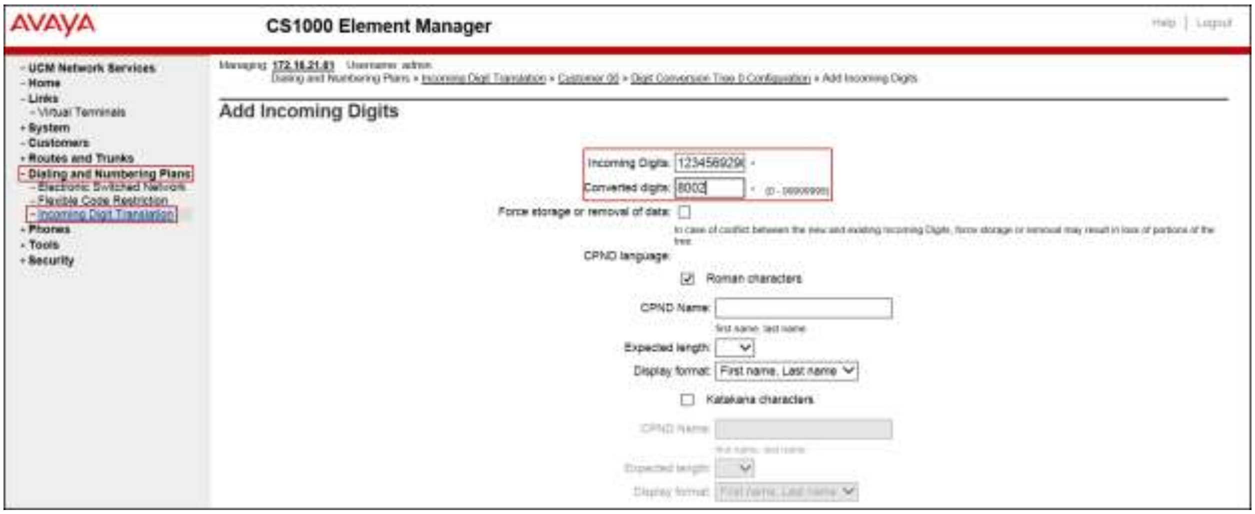


Click on **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number (DCN0) 0** was created as shown below.



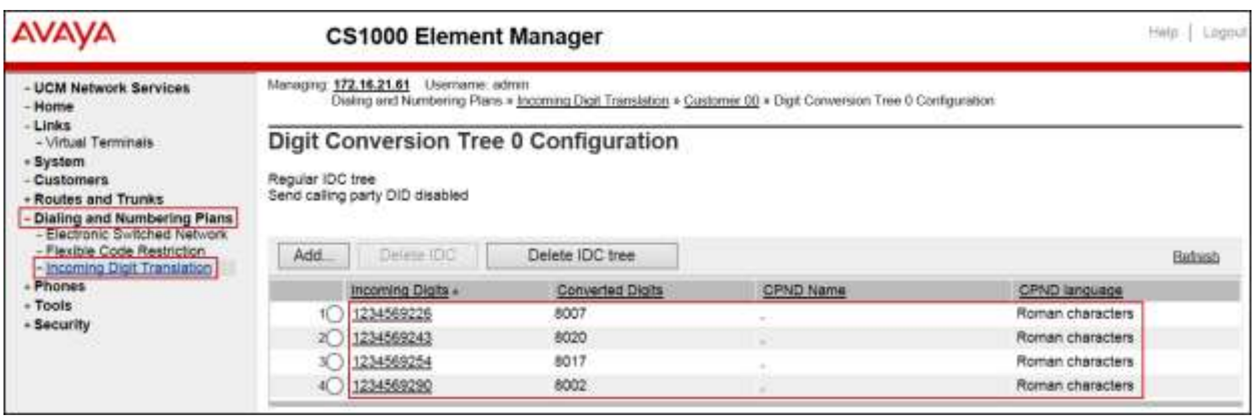
Detailed configuration of the **DCNO** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 system extension number. This **DCN0** has been assigned to route 0 as shown in **Section 5.5.4**.

In the following configuration, the incoming call from the PSTN with the prefix 1234569290 will be translated to the CS1000 extension number 8002 (note that digits have been masked for security reasons).



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

The following screen shows the Incoming Digit Translations used during the compliance testing (note one of the digits have been masked for security reasons).

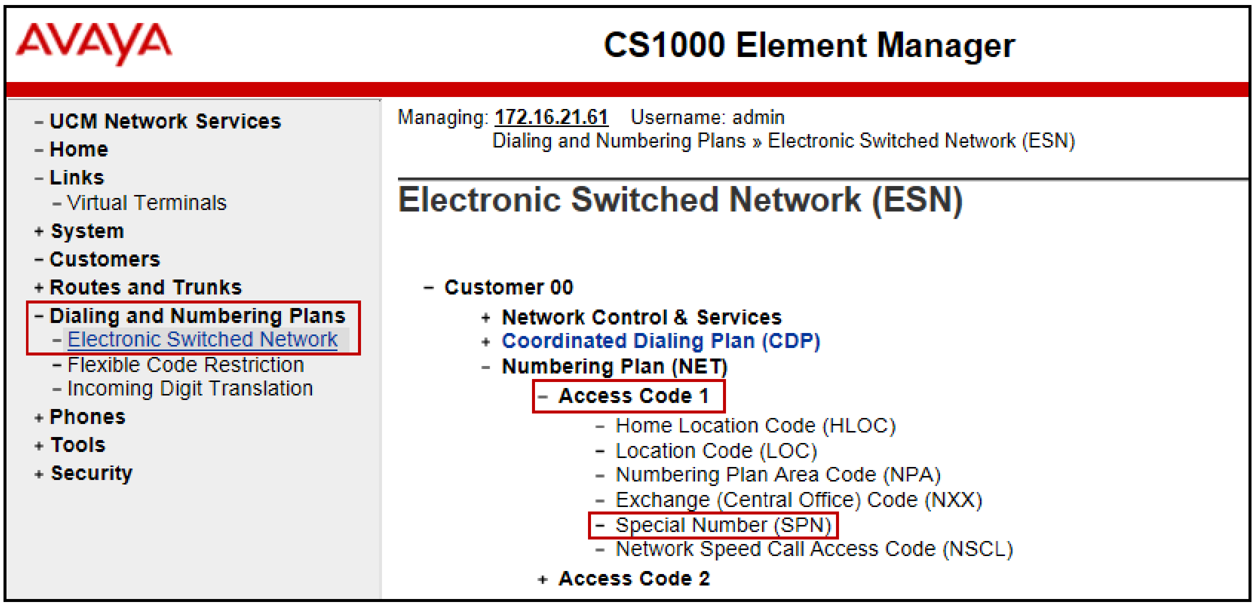


5.6.6. Outbound Call - Special Number Configuration

There are special numbers which are configured to be used for this testing, such as **0** to reach the service provider operator, **0+10** digits to reach the service provider operator assistant, **011** prefix for international calls, **1** for national long distance calls, **411** for directory assistant, **911** for emergency, and so on. Calls to special numbers shown here are for reference only and may not have been used during the testing.

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

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Under **Access Code 1**, select **Special Number (SPN)** as shown below.



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:** 11.
- **CallType**: NATL.
- **Route list index**: 1, created in **Section 5.6.4**.

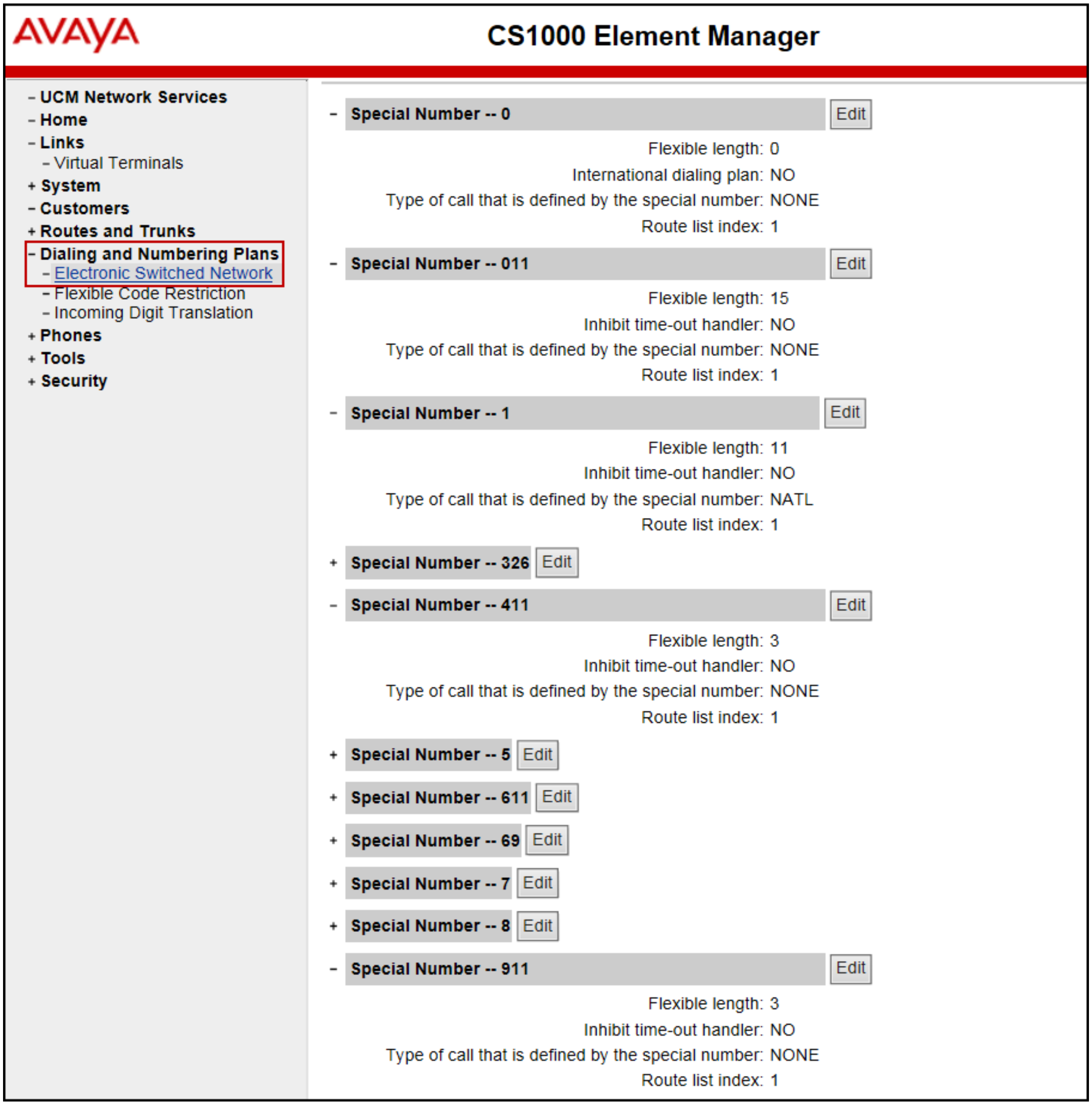
Special Number: 411

- **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**.

Add any other special numbers as required.


AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
+ System
- Customers
+ Routes and Trunks
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
+ Phones
+ Tools
+ Security
- Special Number -- 0 Edit
Flexible length: 0
International dialing plan: NO
Type of call that is defined by the special number: NONE
Route list index: 1
- Special Number -- 011 Edit
Flexible length: 15
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 1
- Special Number -- 1 Edit
Flexible length: 11
Inhibit time-out handler: NO
Type of call that is defined by the special number: NATL
Route list index: 1
+ Special Number -- 326 Edit
- Special Number -- 411 Edit
Flexible length: 3
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 1
+ Special Number -- 5 Edit
+ Special Number -- 611 Edit
+ Special Number -- 69 Edit
+ Special Number -- 7 Edit
+ Special Number -- 8 Edit
- Special Number -- 911 Edit
Flexible length: 3
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 1

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 superloop **- 8** used for IP phone.
Refer to **Section 5.4.1** to create a bandwidth zone - **5** for IP phone.

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
```

Note: For CS1000 FAX over IP Support recommendation, refer to the Avaya Product Support Notice (PSN) referred to in **Section 10** [7], including the "**Analog Station Provisioning for V.34 Fax and Modem**" and "**Minimum Vintage Loadware Recommendation"** for MGC.

The analog station used for fax was provisioned as follows:

Analog Station Provisioning (this setting is required for **T.38** fax):
TYPE 500 ....Analog Station Type
DN 3500..Extension Number
CLS DTN ....Digitone (DTMF)
CLS FAX**A** ....Fax Class of Service
CLS MPT**D**…………………………Will force T.38 codec selection when FAX V.21 preamble is detected.

5.7.2. Enable Privacy for the 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 the SIP message header before sending to the 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 the SIP message header before sending to the service provider.

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

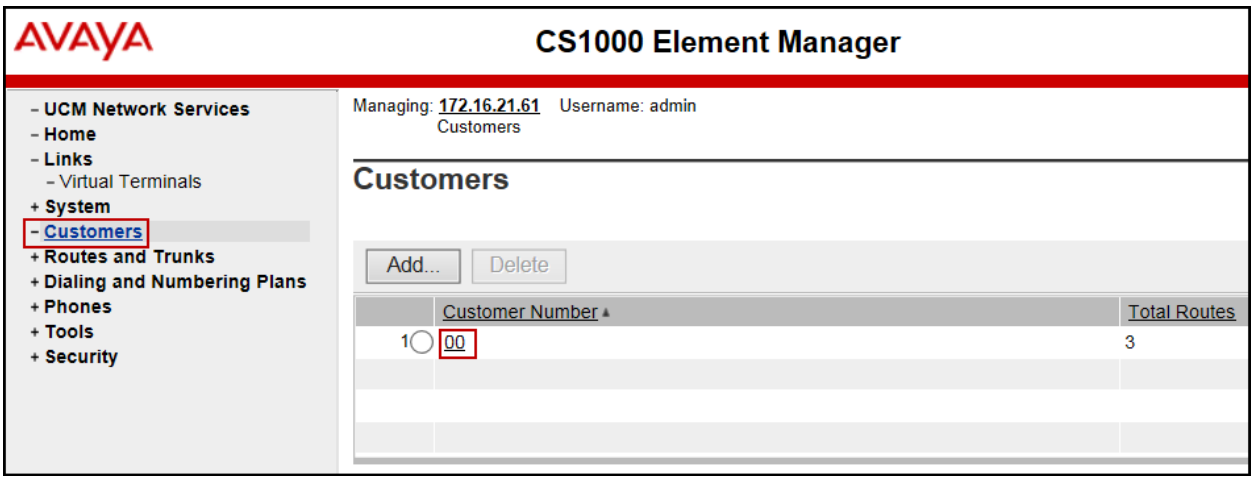
To allow display name and number, set CLS to **nama, ddga**. The CS1000 will send header “Privacy:none” to the service provider.

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

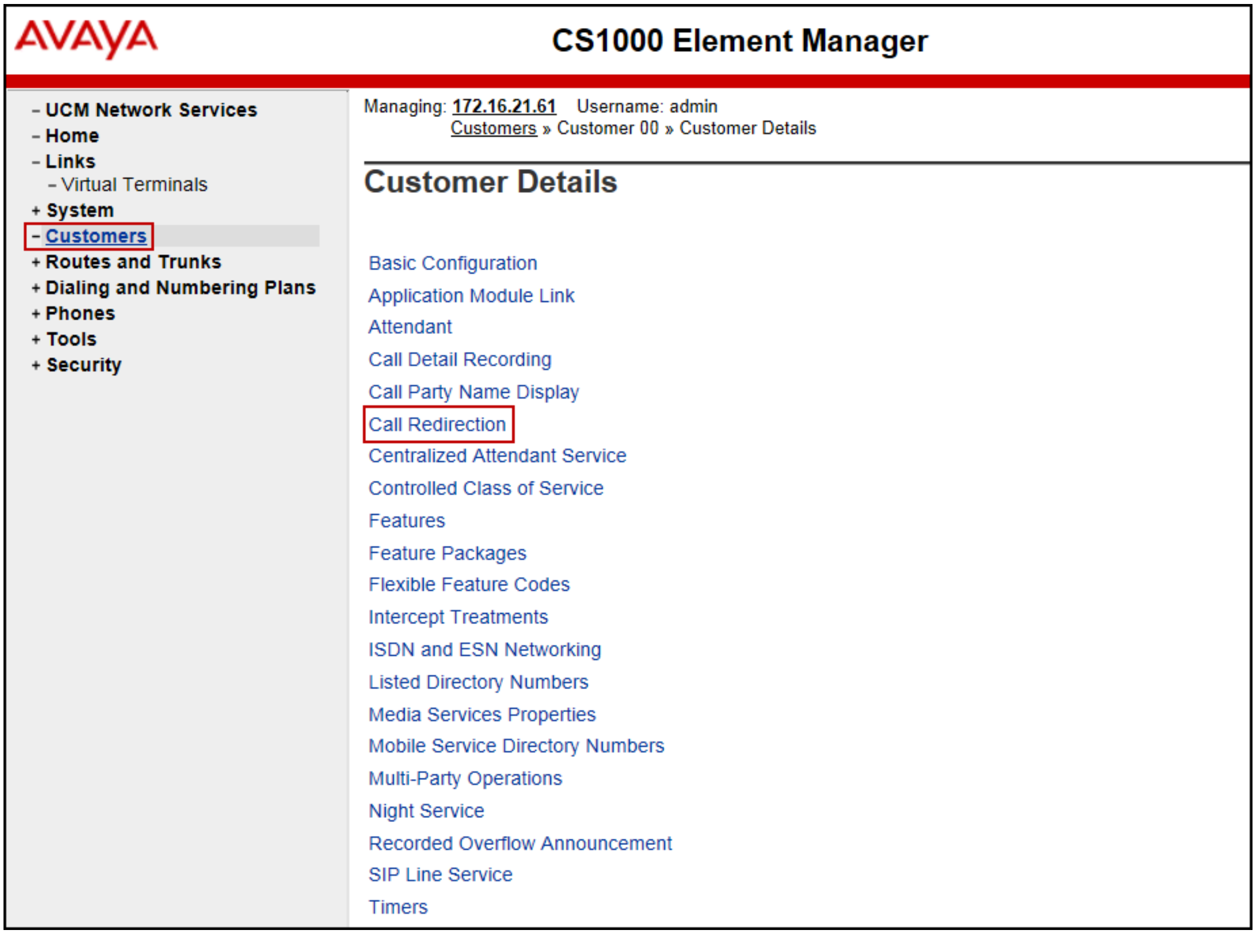
5.7.3. Enable Call Forward for the Phone

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.



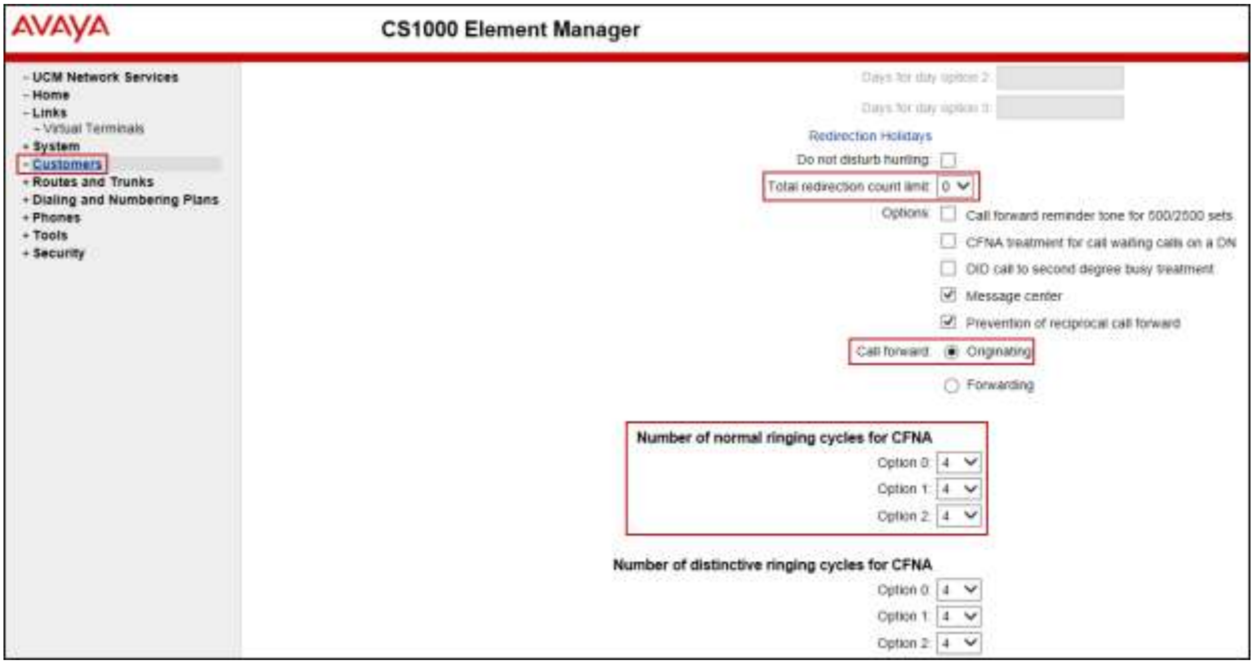
Select **Call Redirection** as shown below.



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

Set the following fields:

- **Total redirection count limit**: **0** (unlimited).
- **Call Forward:** Check **Originating**.
- **Number of normal ring cycles of CFNA: 4**.
- Click on **Save** (not shown).



To enable **Call Forward All Calls** (**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. The following is the configuration of a phone that has CFAC enabled; the phone was 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**, and then program the forward number as **HUNT**. The following is the configuration of a phone that has CFB enabled; the phone was 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 the SIP trunk by using **LD 11**, change CLS to **FNA, SFA**, then program the forward number as **FDN**. The following is the configuration of a phone that has CFNA enabled; the phone was 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 the **Call Waiting** feature at the phone level.

To configure the 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 Avaya Session Border Controller for Enterprise (Avaya SBCE).

This section describes the required configuration of the Avaya SBCE to connect to Claro's SIP Trunk service.

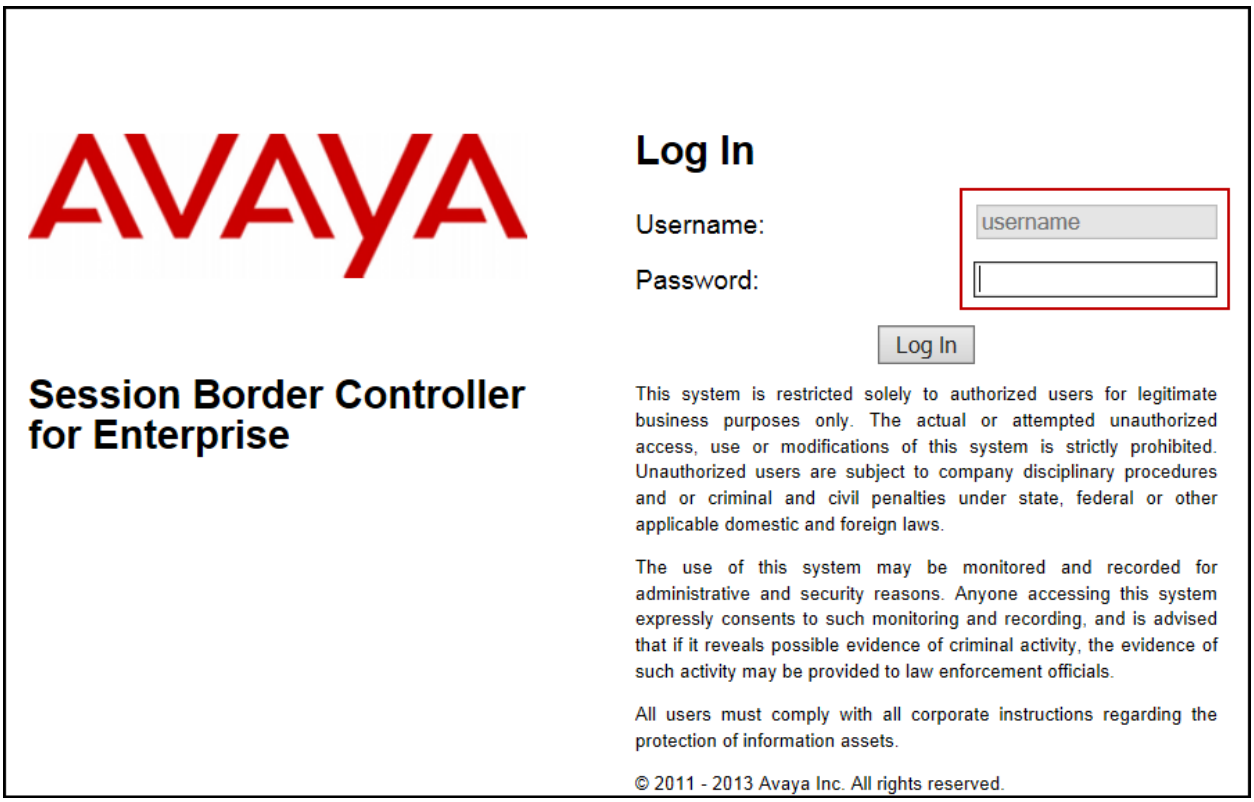
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

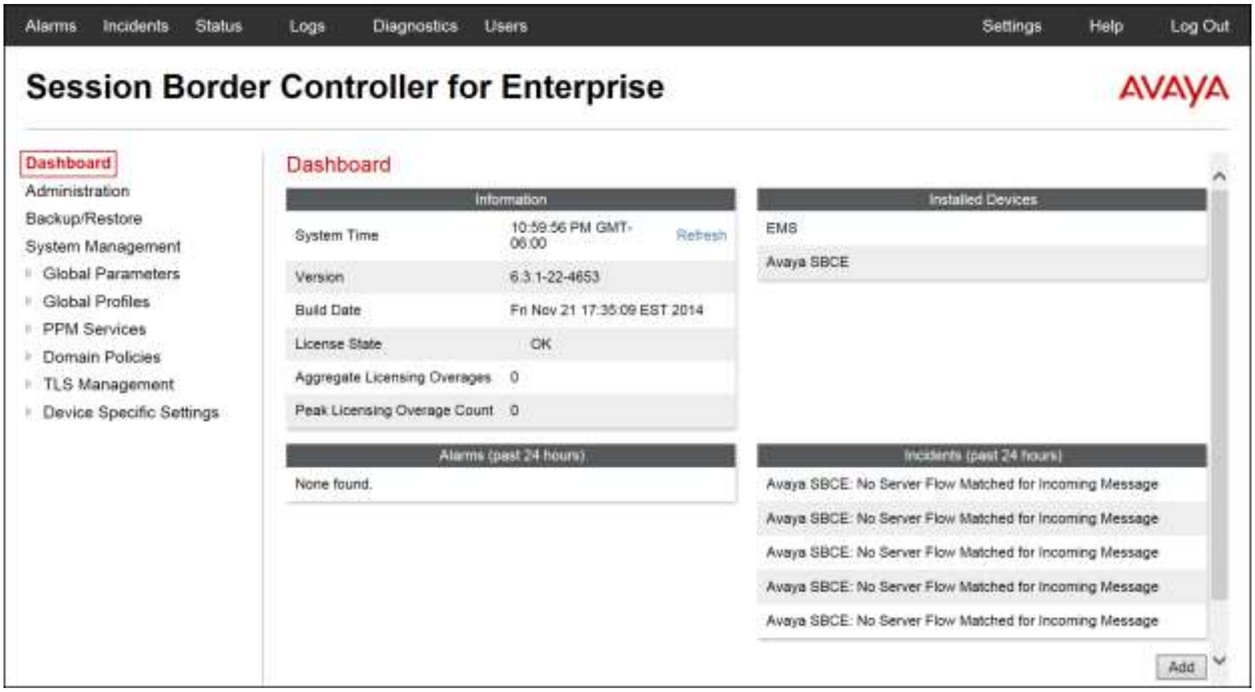
6.1. Log in Avaya SBCE

Use a Web browser to access the Avaya SBCE Web interface. Enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the Avaya SBCE management IP address.

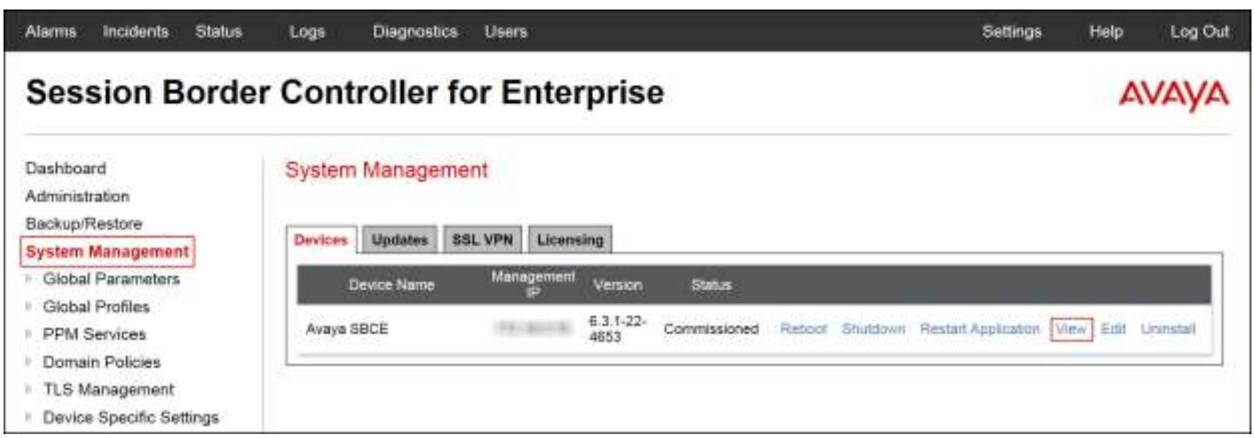
Enter the appropriate credentials and click **Log In**.



The **Dashboard** main page will appear as shown below.

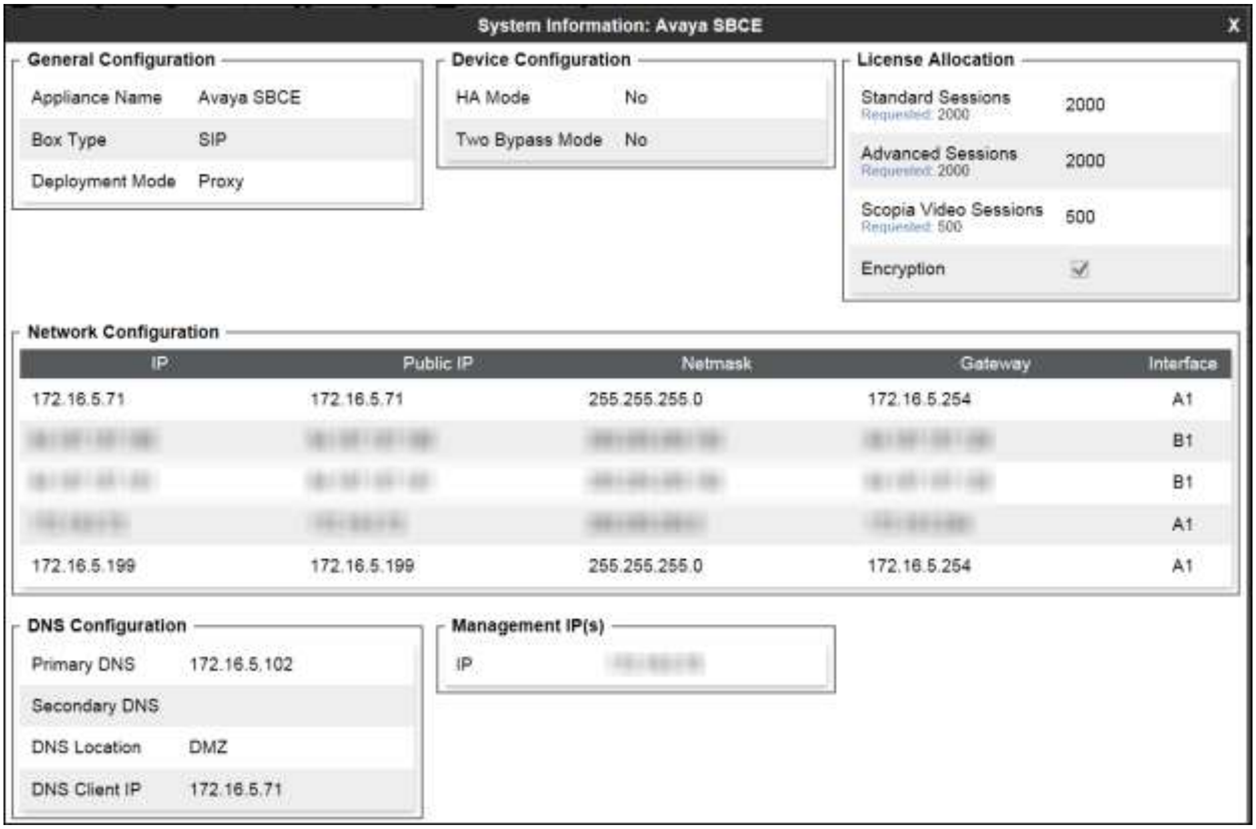


To view the system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya SBCE** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.



To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



On the previous screen, note that the **A1** interface corresponds to the inside interface (Private Network side) and **B1** interface corresponds to the outside interface (Public Network side) of the Avaya SBCE. Since a VPN connection was used with this solution to connect Claro's network to the enterprise network, the **A1** interface was used for access to the private enterprise network and to route calls to Claro's network across the VPN tunnel. In this solution, the **B1** interface was not used. Refer to **Figure 1** for the IP addresses assigned on the Avaya SBCE.

When a VPN connection is not used, the **B1** interface is normally used to route calls to the service provider across the public Internet.

The management IP was blurred out for security reasons.

IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled "M1") of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private or public network interfaces (e.g., A1 and B1).

6.2. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows for 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 in 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.

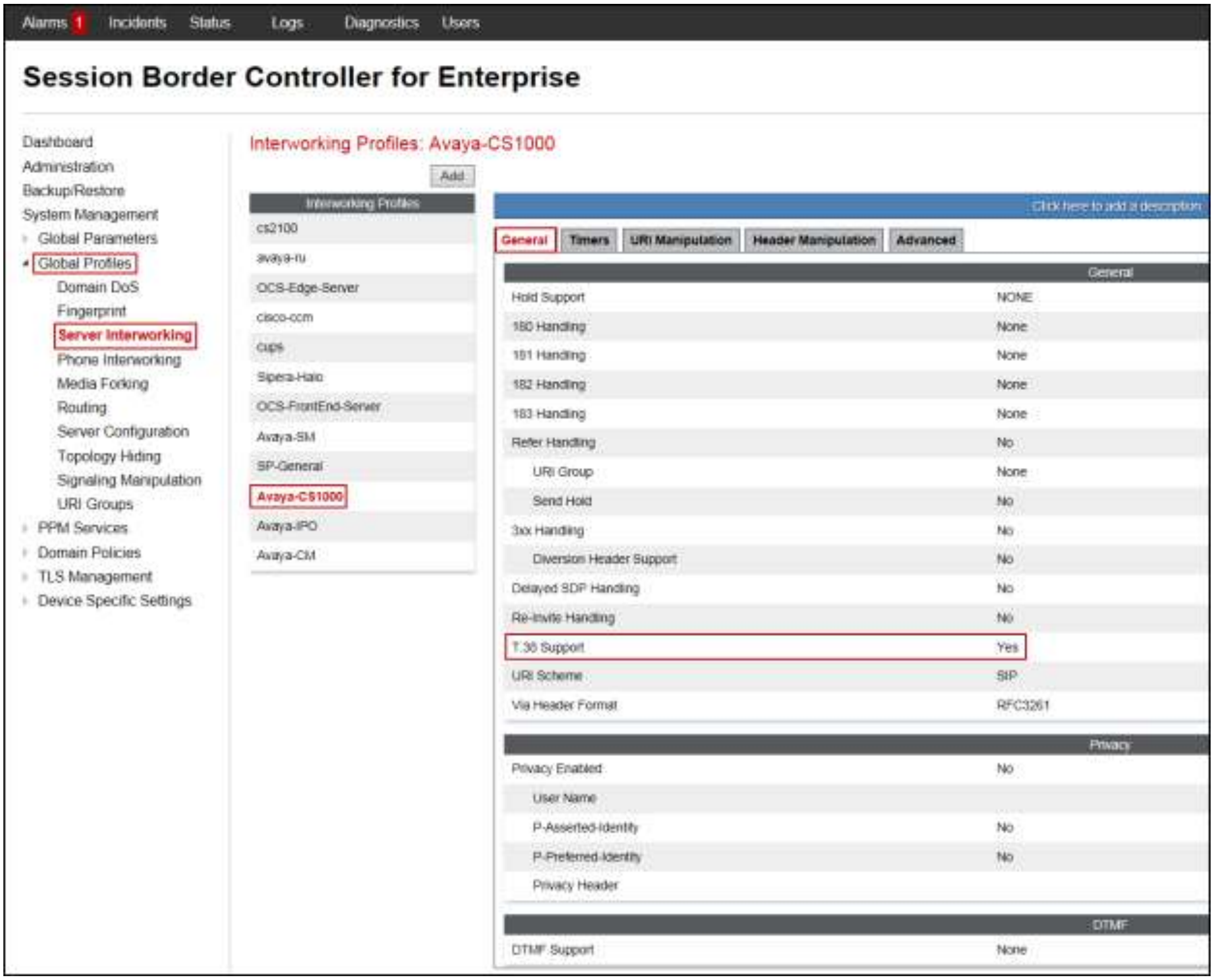
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone Profile.**

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

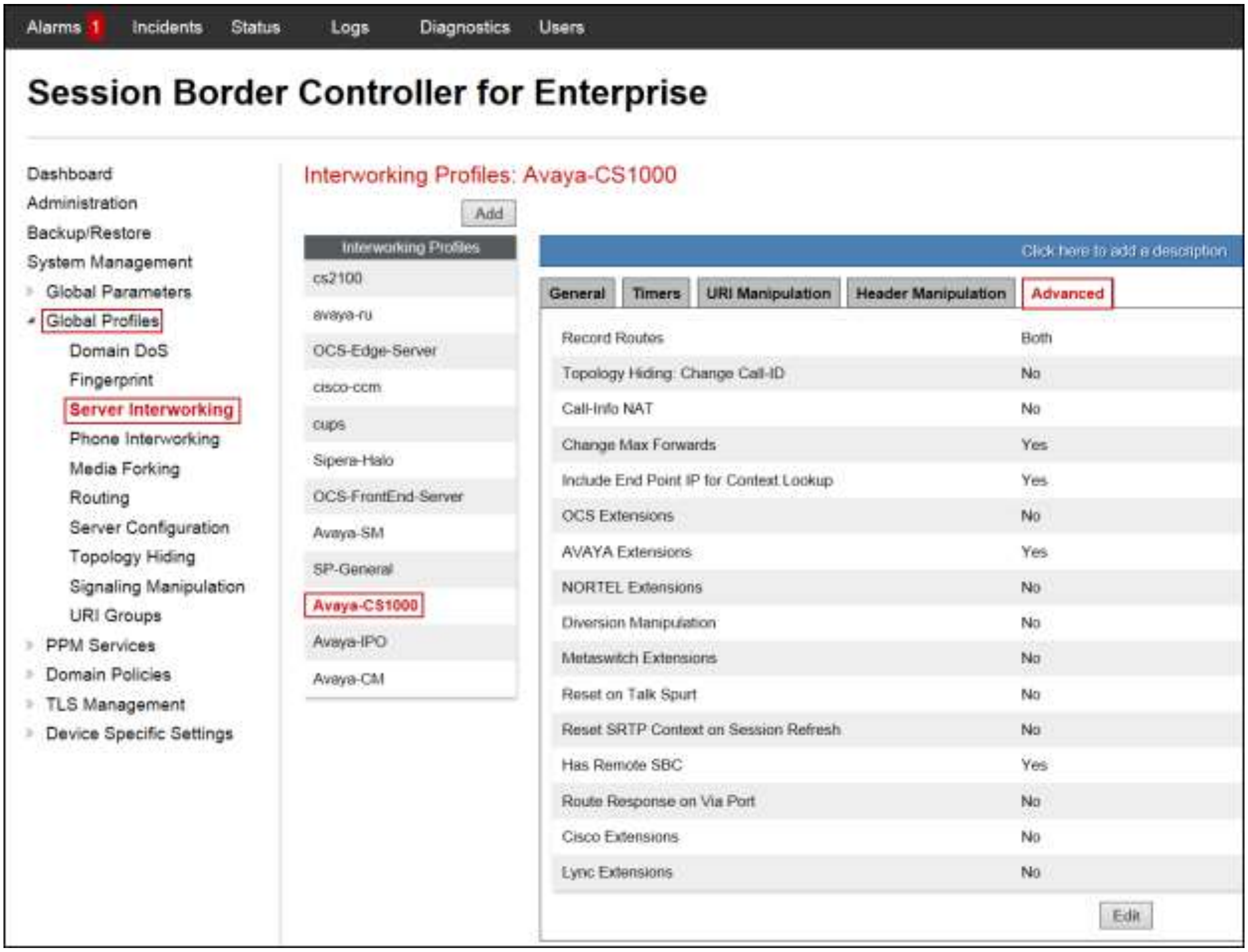
For the newly created **Avaya-CS1000** profile, click **Edit** (not shown) at the bottom of the **General** tab:

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

The following screen capture shows the **General** tab of the newly created **Avaya-CS1000** Profile.



The following screen capture shows the **Advanced** tab of the newly created **Avaya-CS1000** Profile.



6.2.2. Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the service provider.

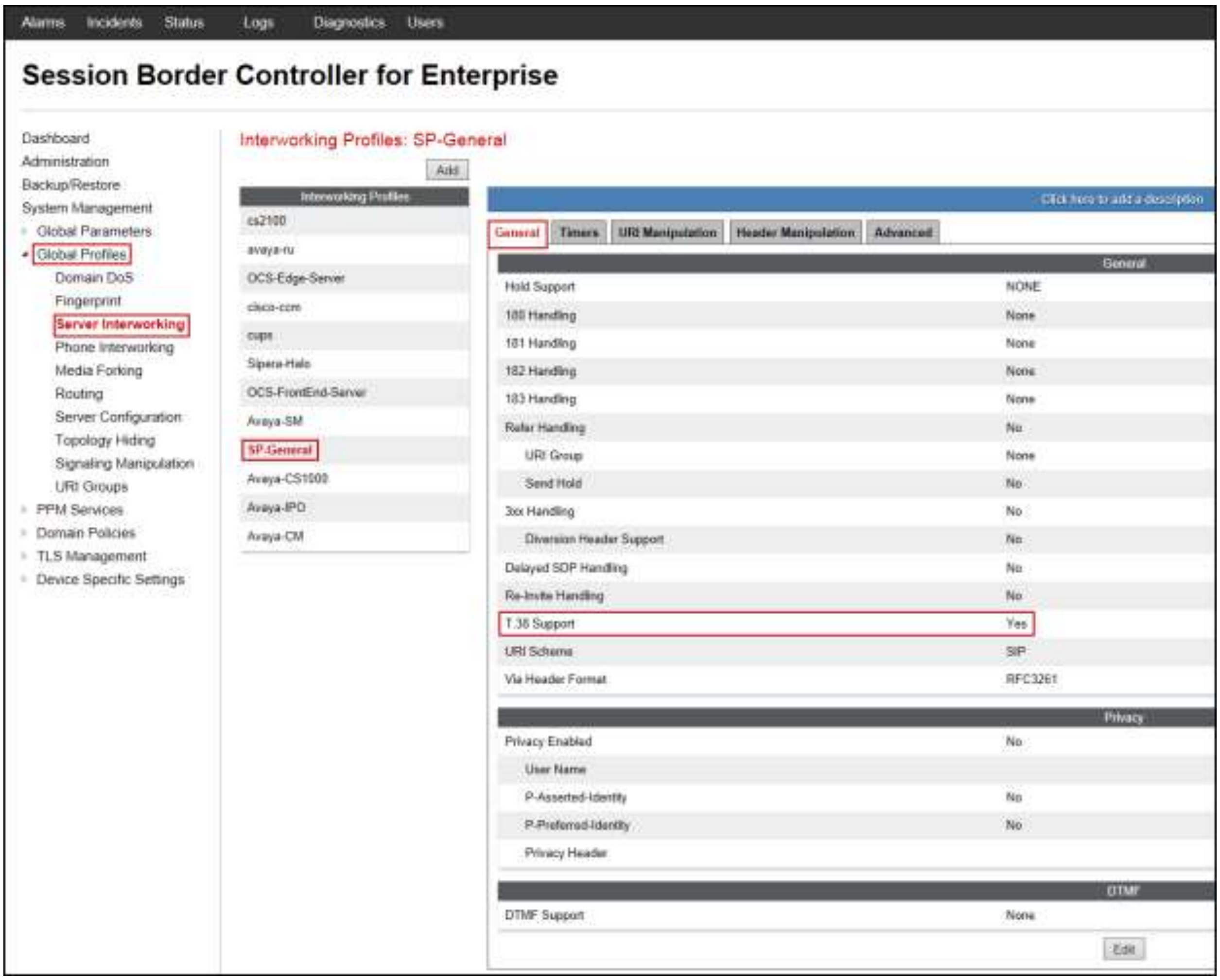
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add.**

Enter the new profile name (not shown), the name of **SP-General** was chosen in this example, clicking **Next**:

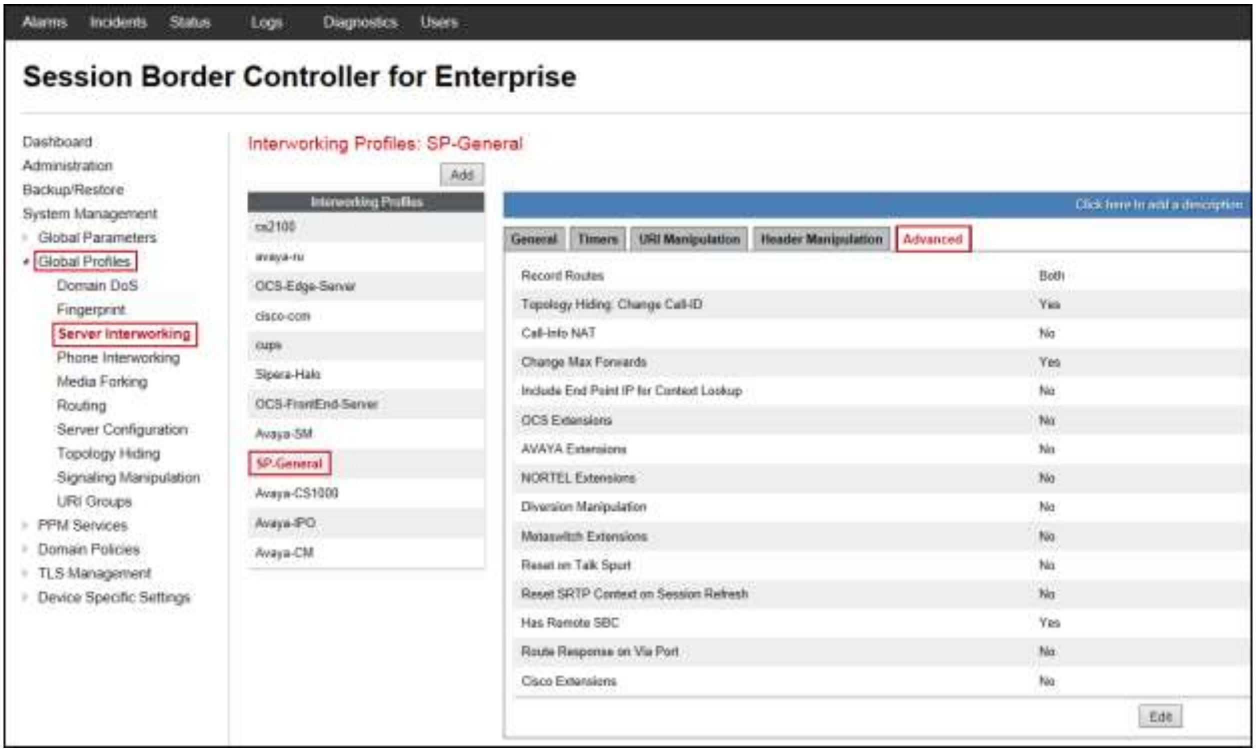
On the **General** tab:

- Check **T.38 Support**.
- Leave other fields with their default values.
- Click **Next** until the **Advanced** tab is reached, then click **Finish** on the Advanced tab.

The following screen capture shows the **General** tab of the newly created **SP-General** profile.



The following screen capture shows the **Advanced** tab of the newly created **SP-General** profile.



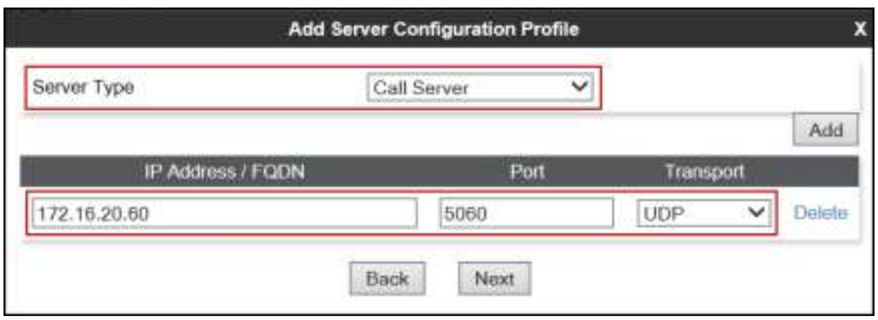
6.2.3. Server Configuration

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 - General** window:

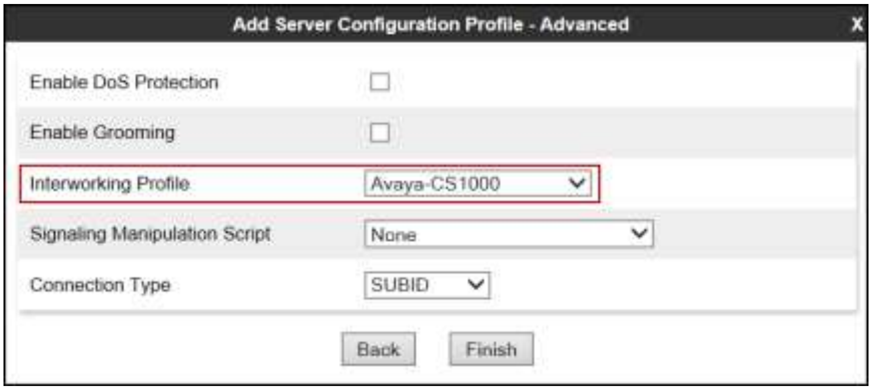
- **Server Type:** Select **Call Server.**
- **IP Address / FQDN**: **172.16.20.60** (Node IP address of the CS1000).
- **Port: 5060** (This port must match the far end (CS1000) local port number defined in **Section 5.5.1)**.
- **Transport**: Select **UDP**.
- Click **Next**.



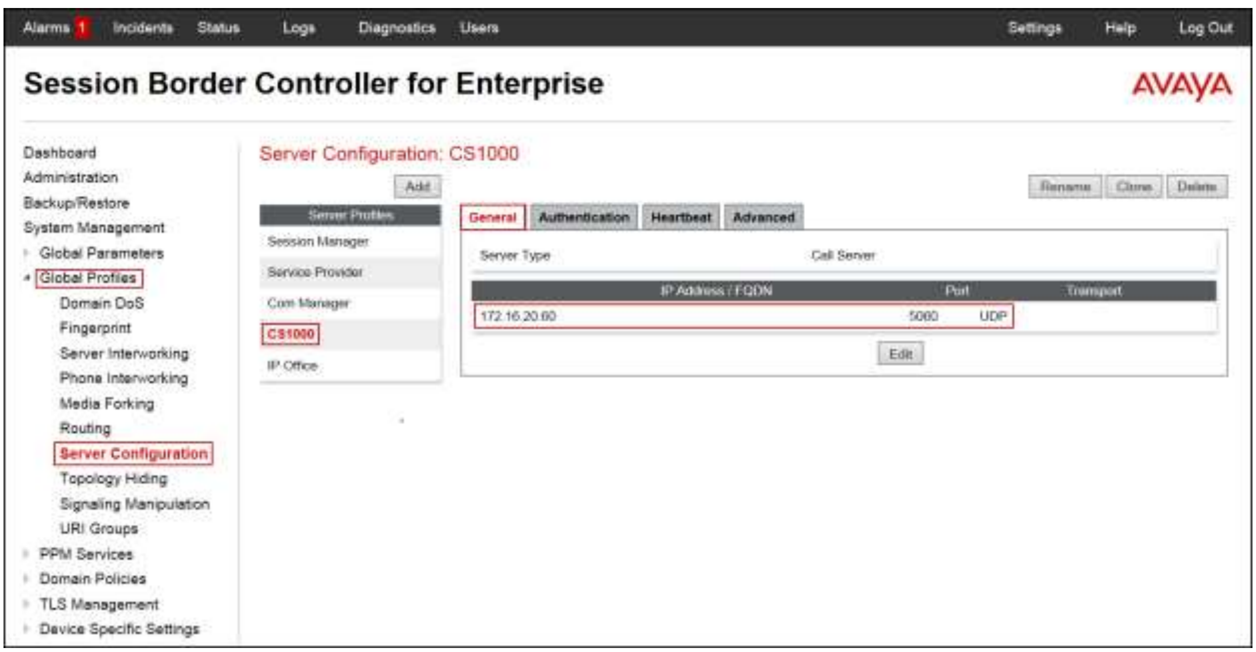
- Click **Next** on the **Authentication** window.
- Click **Next** on the **Heartbeat** window.

On the **Advanced** tab:

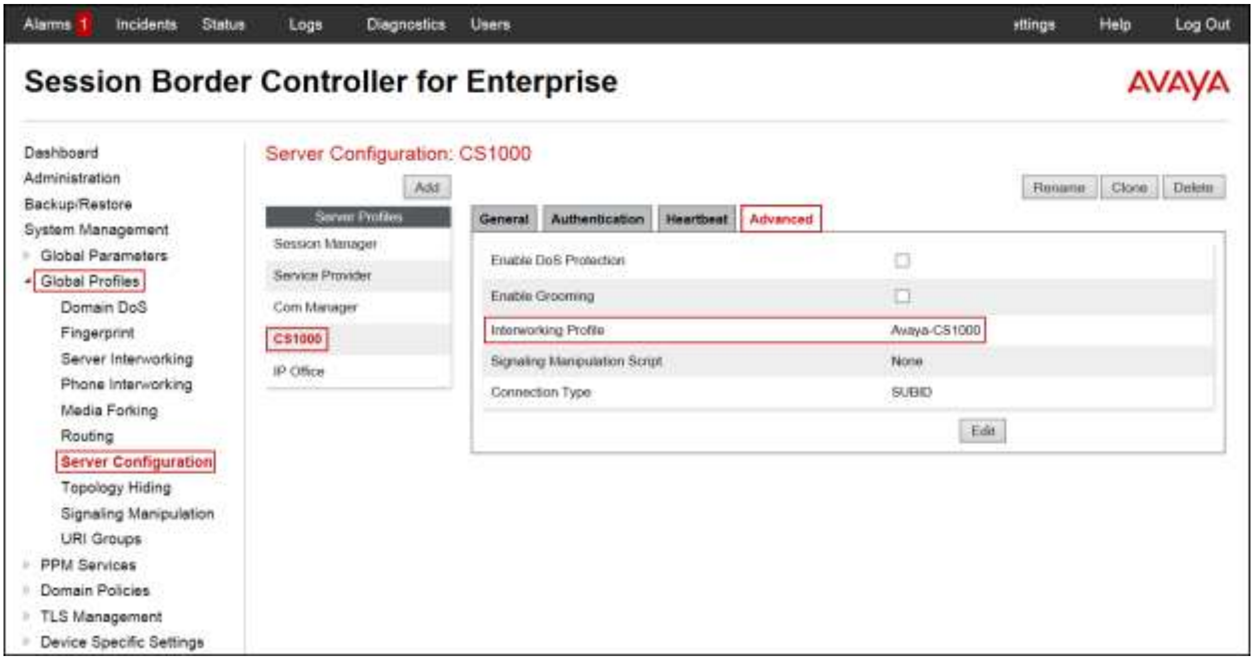
- Select **Avaya-CS1000** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **CS1000** profile.



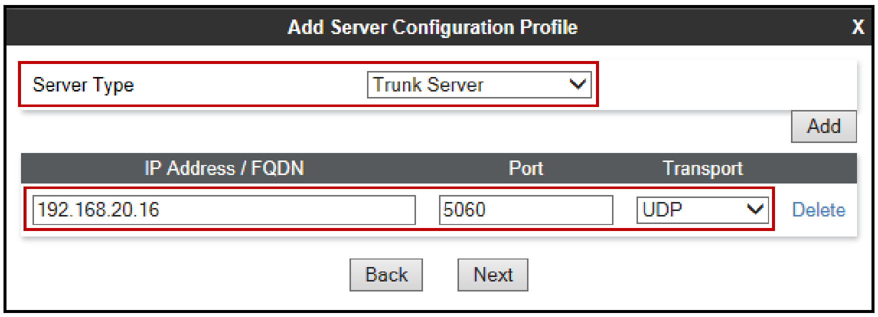
The following screen capture shows the **Advanced** tab of the newly created **CS1000** profile.



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

On the **Add Server Configuration Profile - General** window:

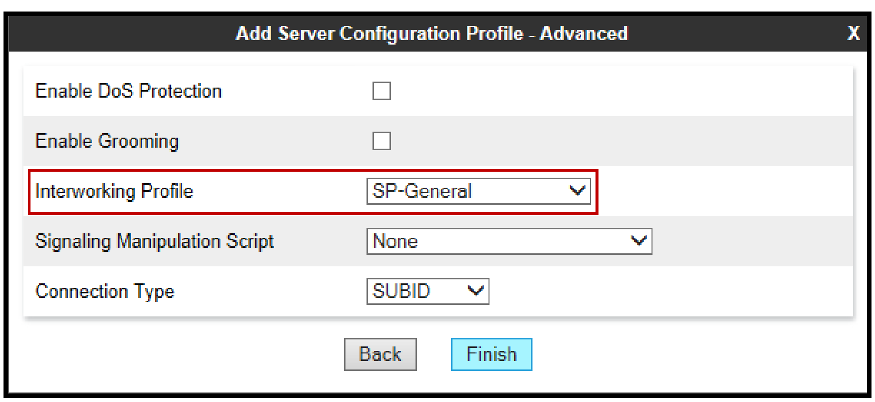
- **Server Type:** Select **Trunk Server.**
- **IP Address / FQDN**: **192.168.20.16** (IP Address of the service provider SIP Proxy).
- **Port: 5060**.
- **Transport**: Select **UDP**.
- Click **Next**.



- Click **Next** on the **Authentication** window.
- Click **Next** on the **Heartbeat** window.

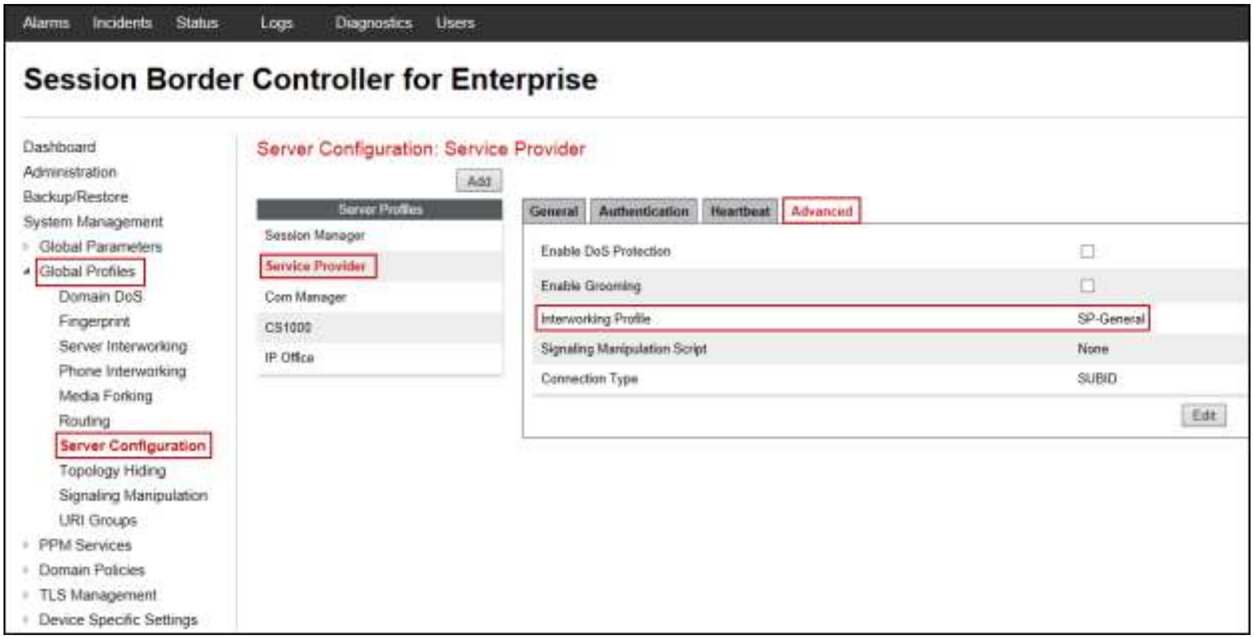
On the **Advanced** tab:

- 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 later.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **Service Provider** profile.

The following screen capture shows the **Advanced** tab of the newly created **Service Provider** profile.



6.2.4. 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.

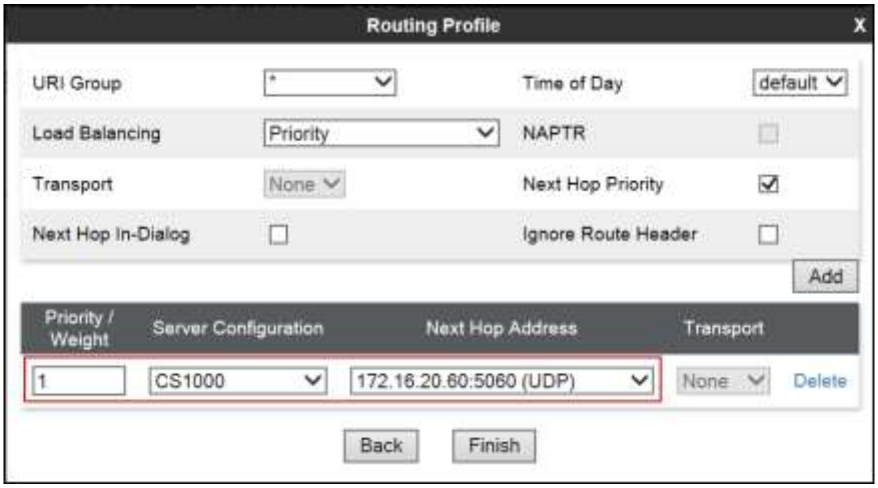
Two Routing profiles were created, one for inbound calls, with the CS1000 as the destination, and the second one for outbound calls, which are sent to the service provider SIP trunk.

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

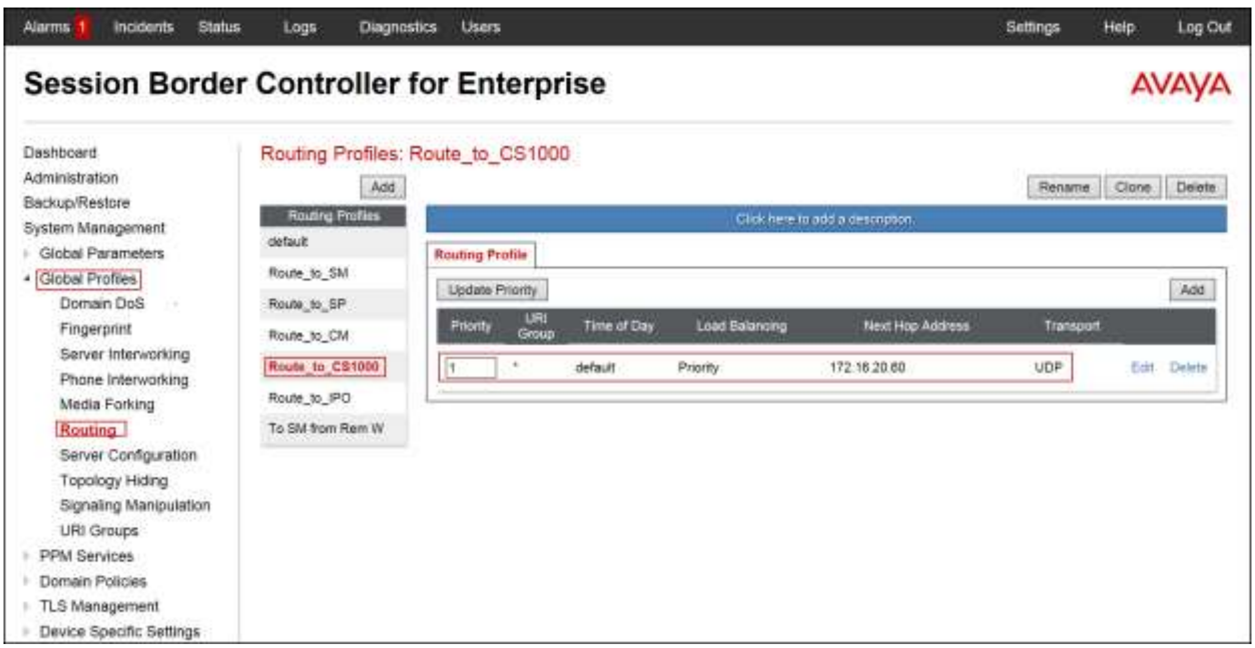
- Select **Routing**.
- Click **Add** in the **Routing Profiles** section**.**
- Enter Profile Name: **Route_to_CS1000**.
- Click **Next**.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: **1**
- **Server Configuration**: Select **CS1000**.
- **Next Hop Address**: Select **172.16.20.60:5060 (UDP)** ((Node IP address of the CS1000, Port and Transport).
- Click **Finish**.



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

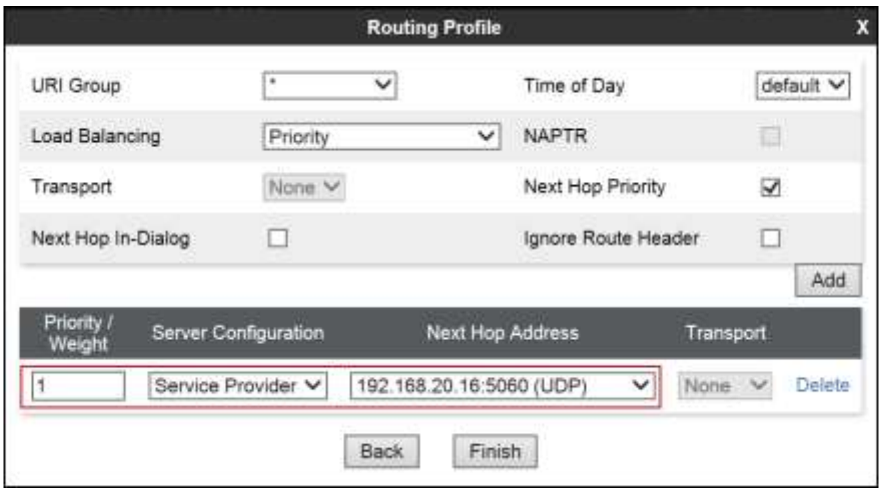


Similarly, for the outbound route:

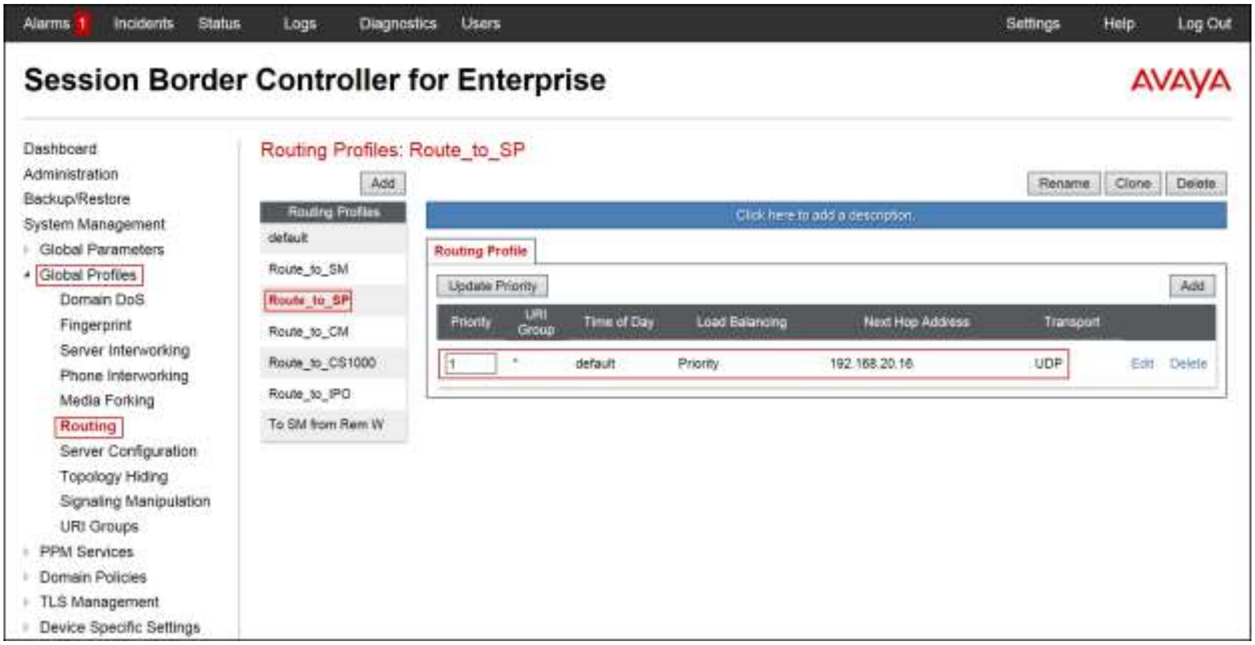
- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SP**.
- Click **Next**.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: **1**
- **Server Configuration**: Select **Service Provider**.
- **Next Hop Address**: Select **192.168.20.16:5060 (UDP)** (service provider SIP Proxy IP address, Port and Transport).
- Click **Finish**.



The following screen capture shows the newly created **Route_to_SP** 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.

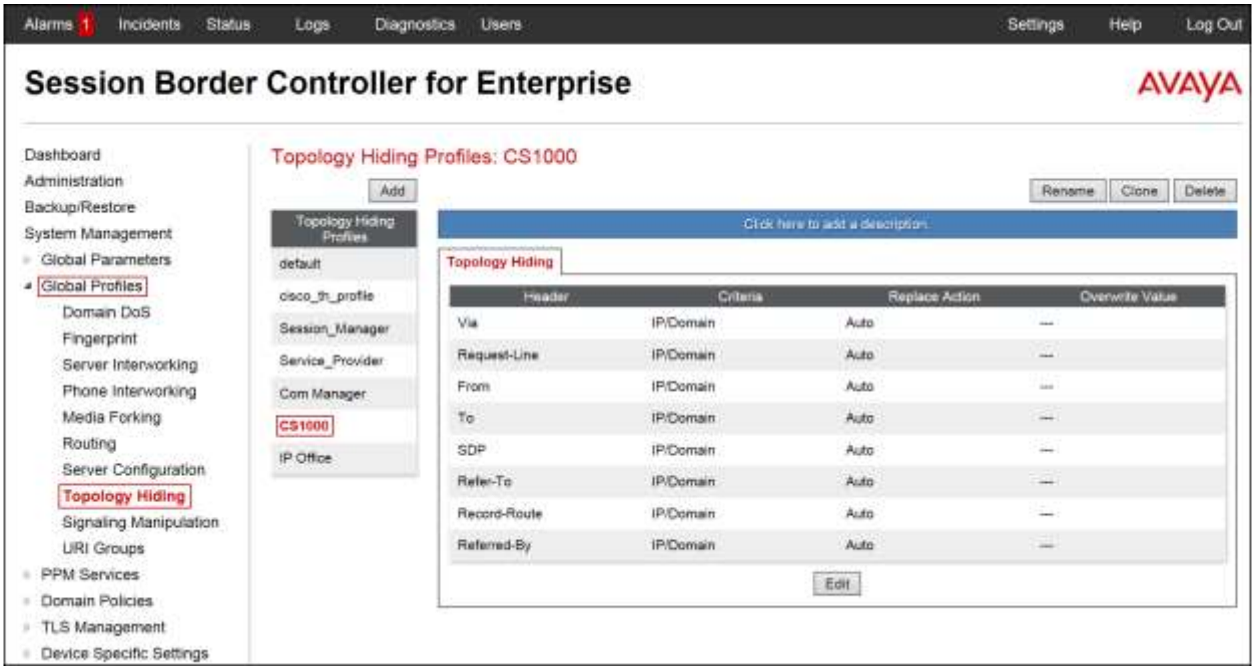
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains, allowing the call to be accepted in each case.

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**.

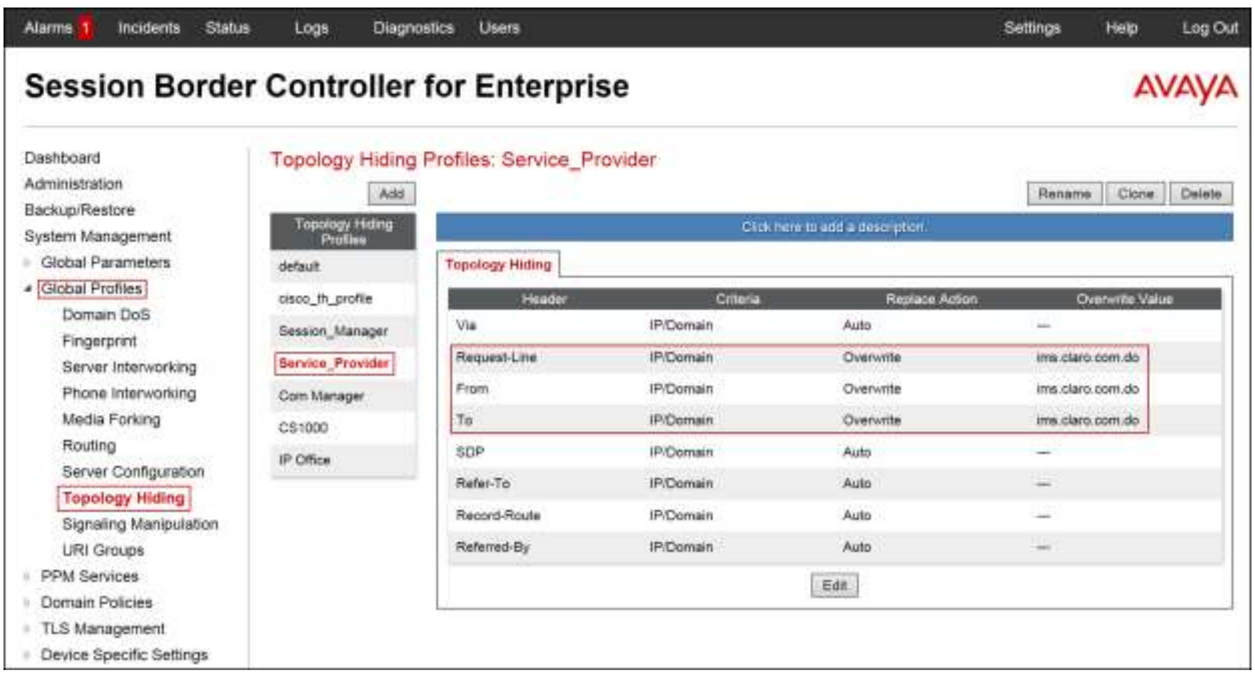
The following screen capture shows the newly added **CS1000** Profile. Note that for the CS1000, no values were overwritten (default).



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**.
- Click **Edit** on the newly added **Service_Provider** Topology Hiding profile.
- For **Request-Line** under **Header**, choose ***Overwrite*** from the pull-down menu under **Replace Action;** enter the domain name for the service provider **(*ims.claro.com.do*)** under **Overwrite Value**.
- For **From** under **Header**, choose ***Overwrite*** from the pull-down menu under **Replace Action,** enter the domain name for the service provider **(*ims.claro.com.do*)** under **Overwrite Value**.
- For **To** under **Header**, choose ***Overwrite*** from the pull-down menu under **Replace Action,** enter the domain name for the service provider **(*ims.claro.com.do*)** under **Overwrite Value**.

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



6.2.6. Signaling Manipulation

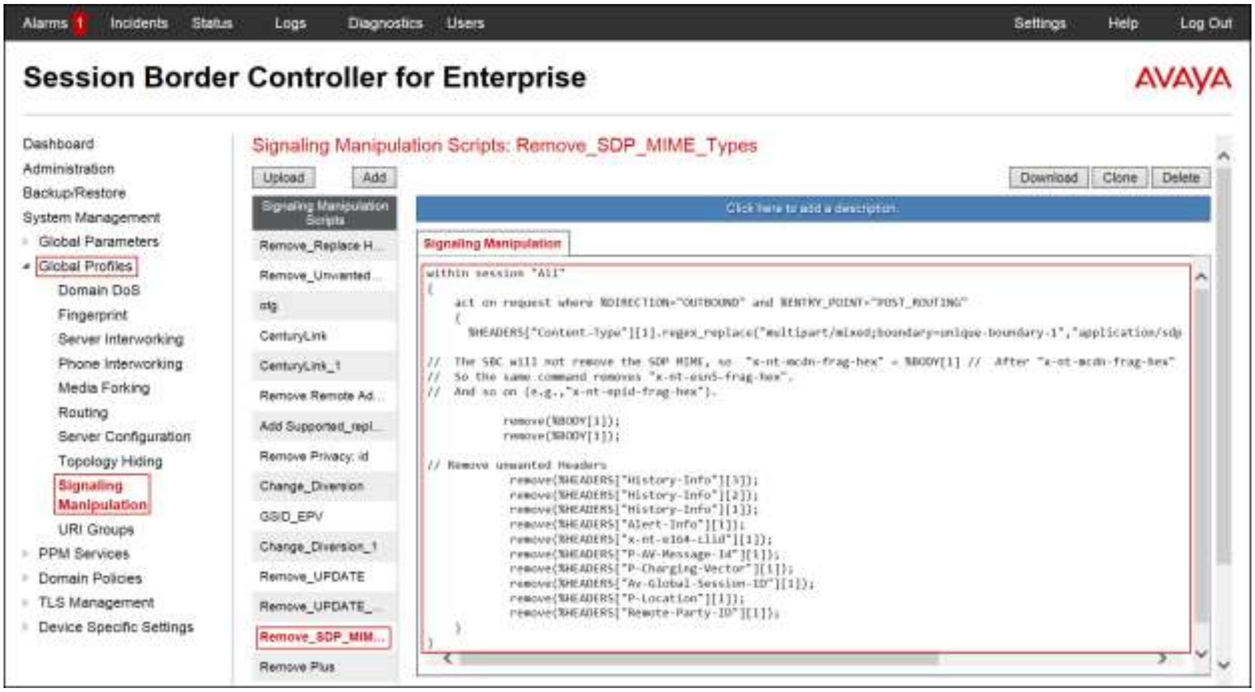
The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For 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 remove unwanted headers from being sent to the service provider. This is in addition to the Signaling Rules created to remove headers under **Section 6.3.3**.

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.

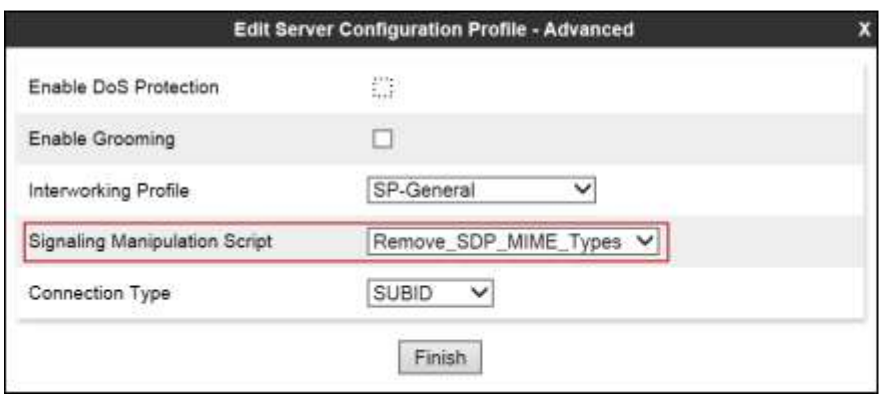
- For the **Title,** enter a name. The name of **Remove_SDP_MIME_Types** was chosen in this example.
- Enter the script as shown on the screen below (**Note**: The script can be copied from **Appendix A**).
- Click **Save**.

The following screen shows the newly added Signaling Manipulation script.

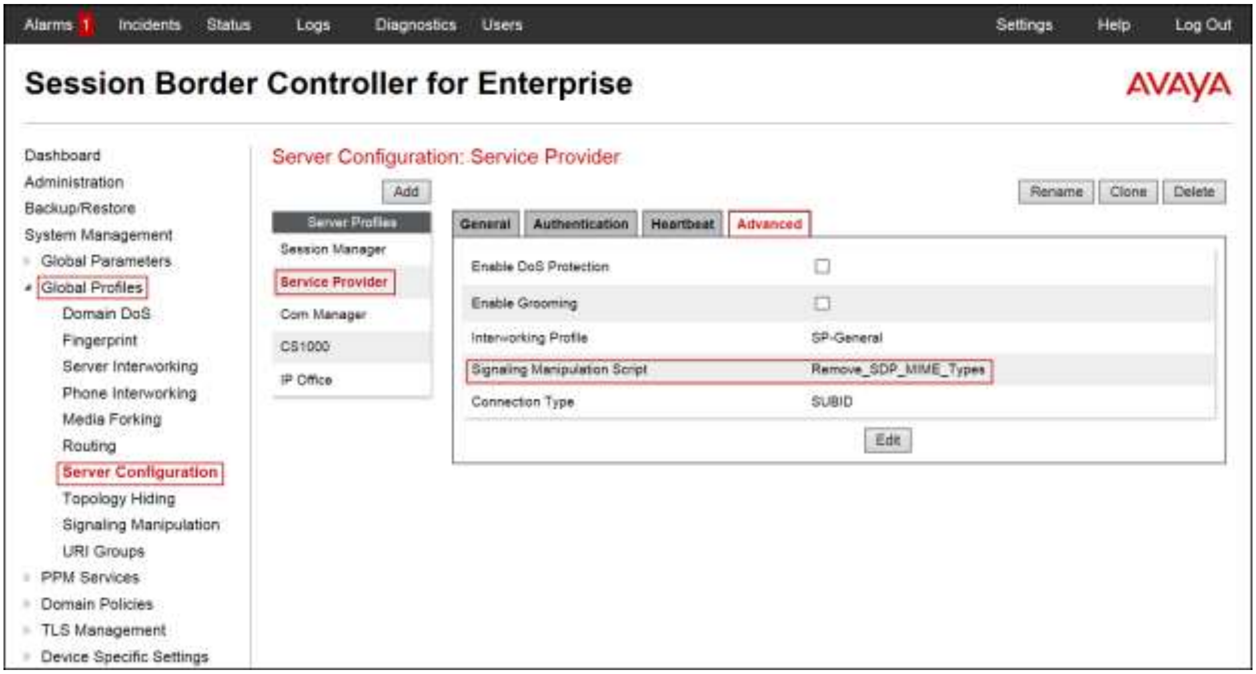


After the Signaling Manipulation Script is created, it should be applied to the **Service Provider Server Configuration Profile** previously created in **Section 6.2.3.**

Go to **Global Profiles** → **Server Configuration** → **Service Provider** → **Advanced** tab → **Edit**. Select **Remove_SDP_MIME_Types** 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.



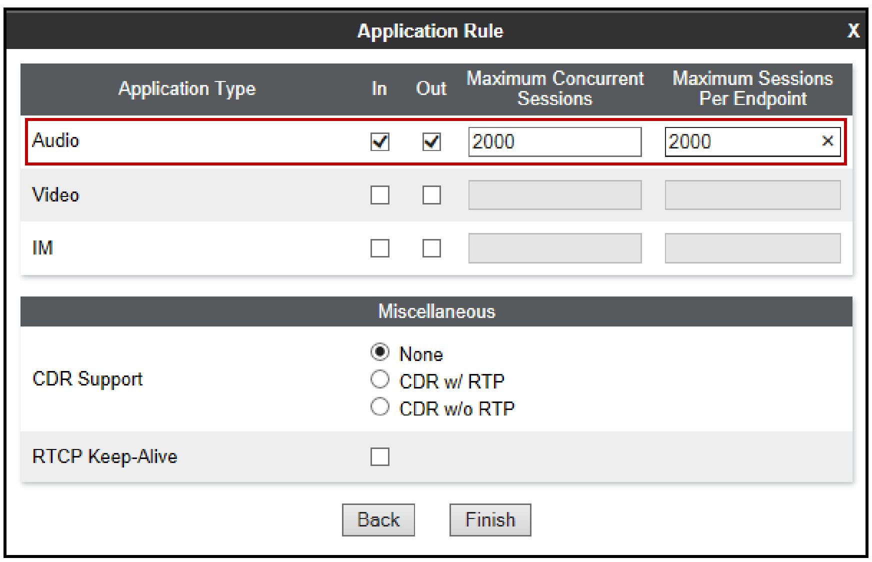
6.3. Domain Policies

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.

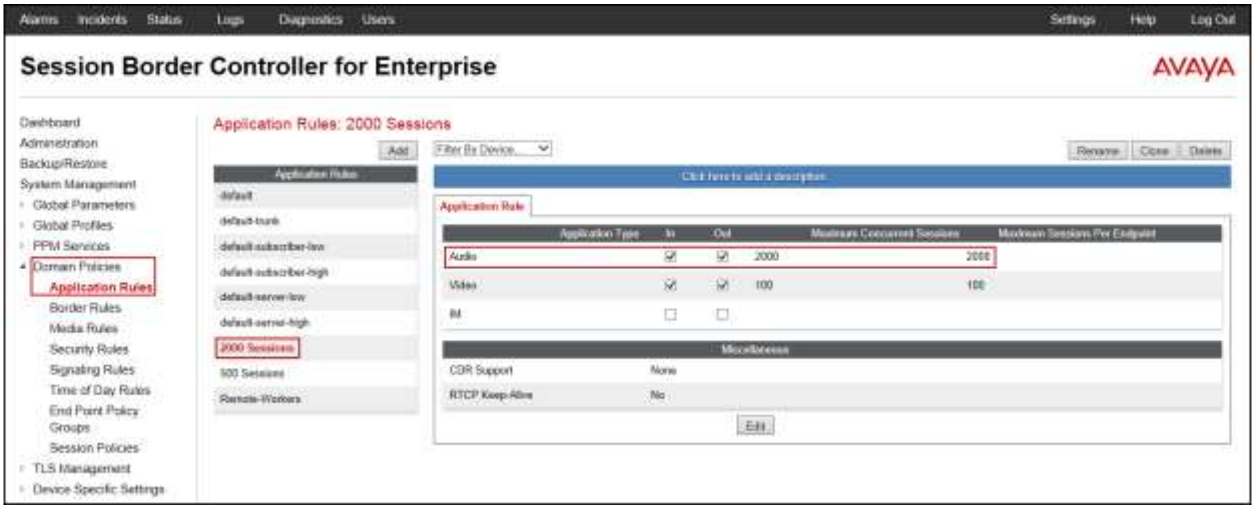
6.3.1. Create Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define 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**.

- Click on the **Add** button to add a new rule.
- **Rule Name:** enter the name of the profile, e.g., **2000 Sessions**.
- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **2000** was used in the sample configuration.
- Click **Finish**.

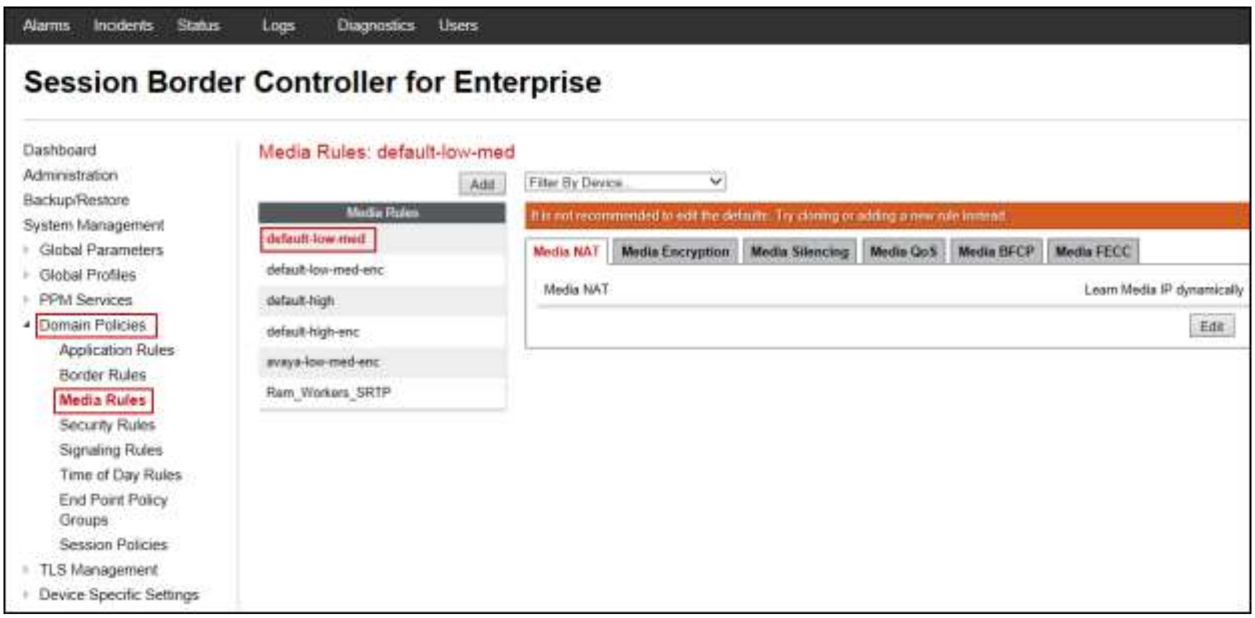


The following screen capture shows the newly created **2000 Sessions** application rule.



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.

Headers such as Alert-Info, P-Location, P-Charging-Vector and others are sent in SIP messages from the CS1000 to the Avaya SBCE for egress to the service provider's network. These headers should not be exposed external to the enterprise. For simplicity, these headers were simply removed (blocked) from both requests and responses for both inbound and outbound calls.

A Signaling Rule was created, to later be applied in the direction of the Enterprise to block unwanted headers coming from the CS1000 from being propagated to the Claro network. To add this header, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on **default** in the **Signaling Rules** list.
- Click on **Clone** on top right of the screen.
- Enter a name: **CS1K_SigRule**. Click **Finish**.

Select the **Request Headers** tab of the newly created **CS1K_SigRule** signaling rule.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name: AV-Global-Session-ID**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **Alert-Info** header:

- Select **Add in Header Control**
- **Header Name: Alert-Info**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish.**

To add the **Endpoint-View** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: Endpoint-View**
- **Method Name: ALL**
- **Header Criteria: Forbidden**

- **Presence Action: Remove Header**
- Click **Finish.**

To add the **History-Info** header:

- Select **Add in Header Control**
- **Header Name: History-Info**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box
- **Header Name: P-AV-Message-ID**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **P-Charging-Vector** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-Charging-Vector**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **P-Location** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-Location**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **x-nt-ocn-id** header:

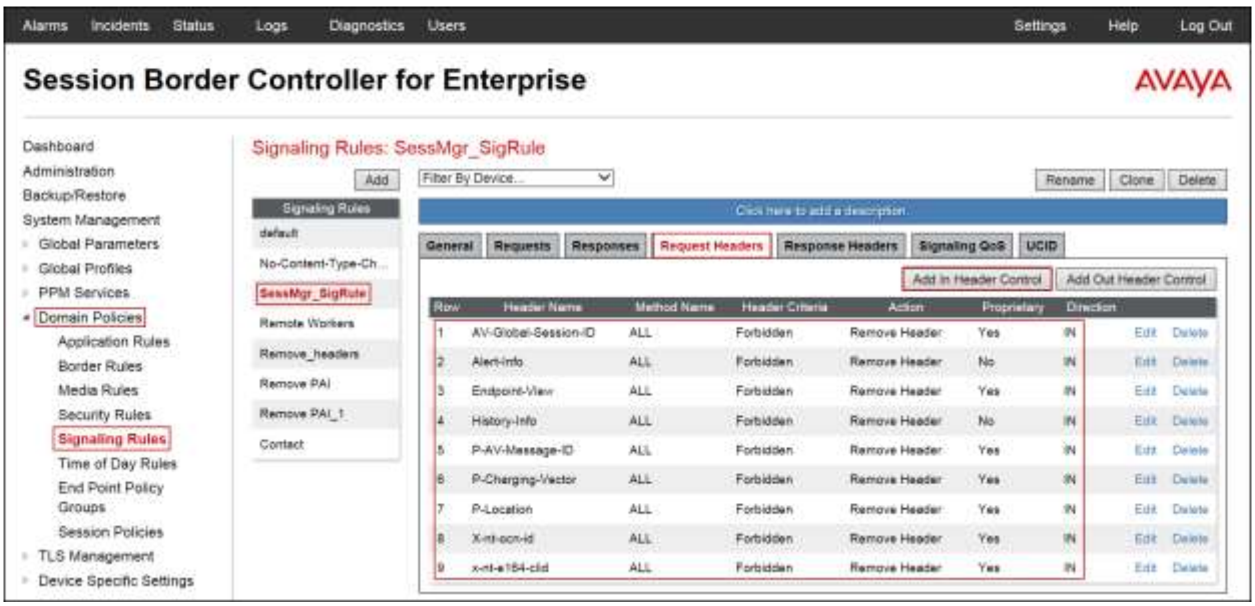
- Select **Add in Header Control**
- Check the **Proprietary Request Header** box

- **Header Name: x-nt-ocn-id**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **x-nt-e164-clid** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: x-nt-e164-clid**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

The following screen capture shows the **Request Headers** tab of the **CS1K_SigRule** signaling rule.



Select the **Response Headers** tab of the newly created **CS1K_SigRule** signaling rule.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: AV-Global-Session-ID**
- **Response Code: 1XX**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: AV-Global-Session-ID**
- **Response Code: 200**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: AV-Global-Session-ID**
- **Response Code: 4XX**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **Alert-Info** header:

- Select **Add in Header Control**
- **Header Name: Alert-Info**
- **Response Code: 200**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-AV-Message-ID**
- **Response Code: 1XX**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-AV-Message-ID**
- **Response Code: 200**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **P-Charging-Vector** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-Charging-Vector**
- **Response Code: 200**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **P-Location** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-Location**
- **Response Code: 1XX**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

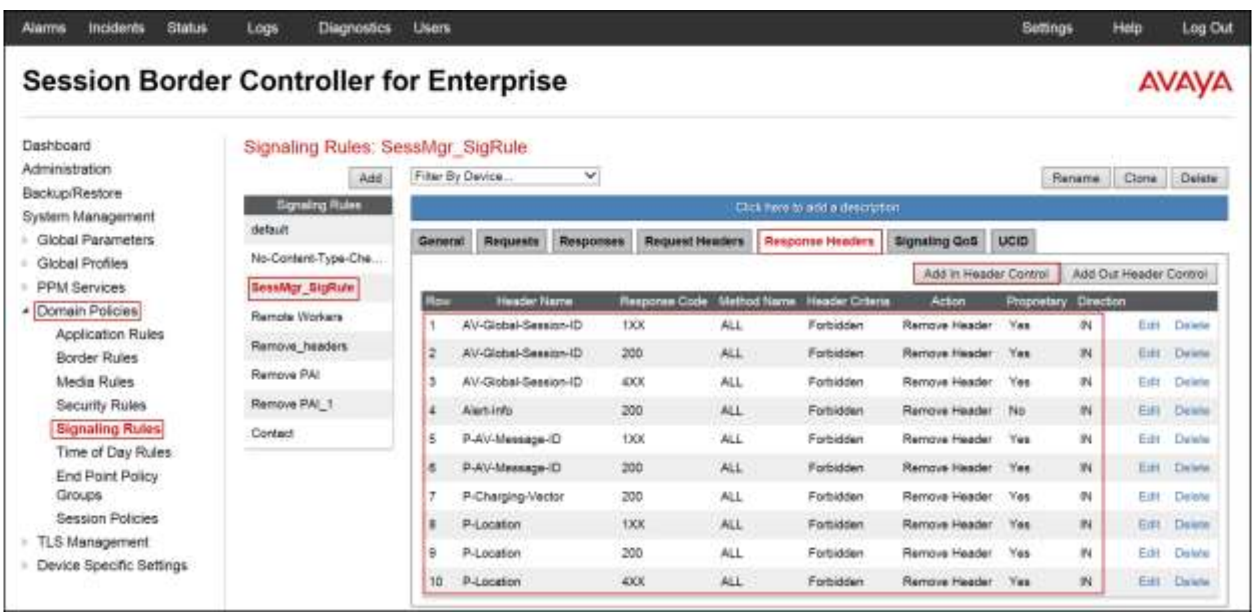
To add the **P-Location** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-Location**
- **Response Code: 200**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **P-Location** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-Location**
- **Response Code: 4XX**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

The following screen capture shows the **Response Headers** tab of the **CS1K_SigRule** signaling rule.



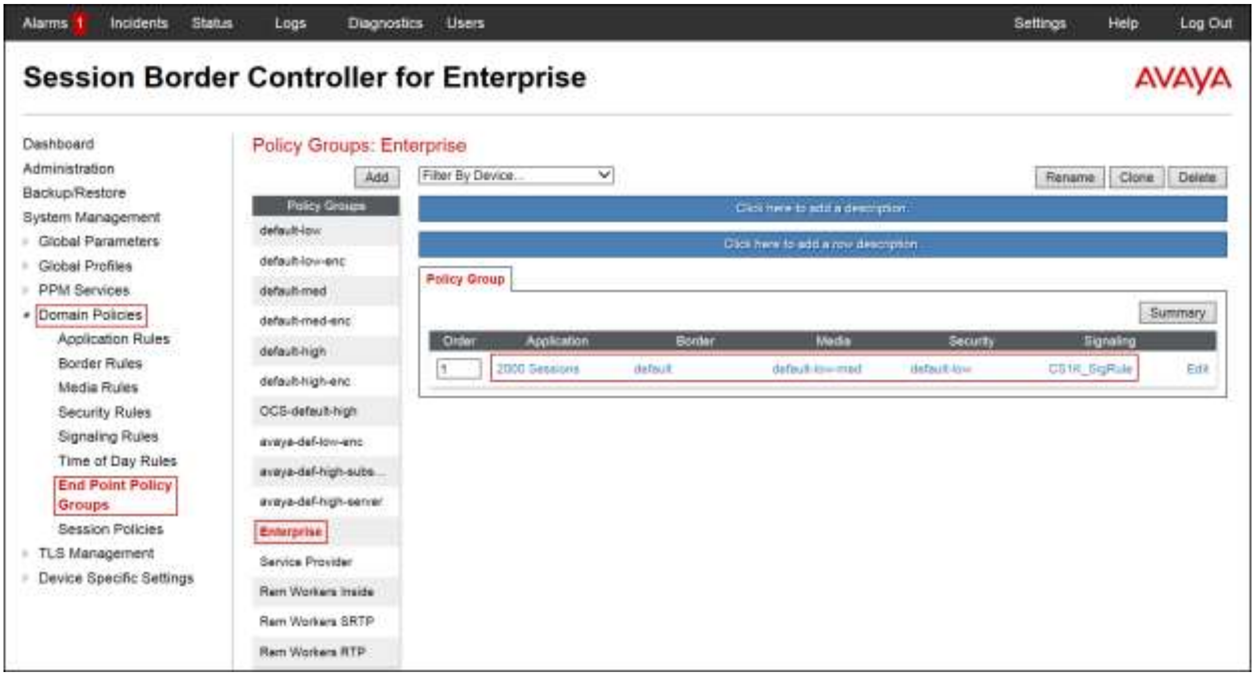
6.3.4. End Point Policy Groups

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**.

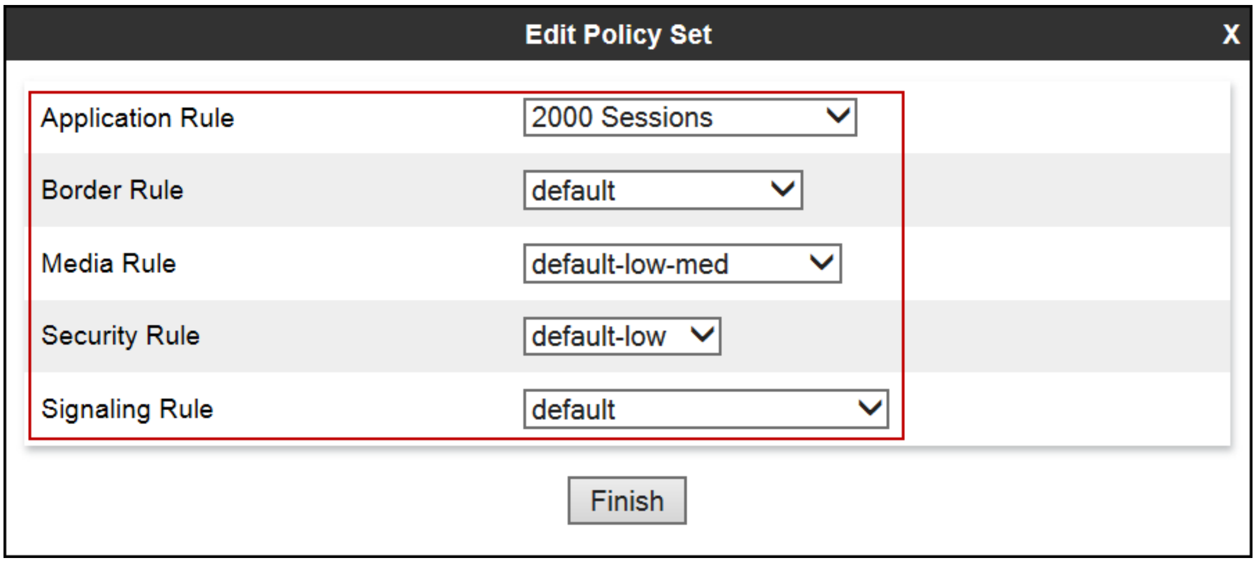
- **Group Name: Enterprise**.
- **Application Rule: 2000 Sessions.**
- **Border Rule: default**.
- **Media Rule: default-low-med**.
- **Security Rule: default-low**.
- **Signaling Rule: CS1K_SigRule**.
- Click **Finish**.

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

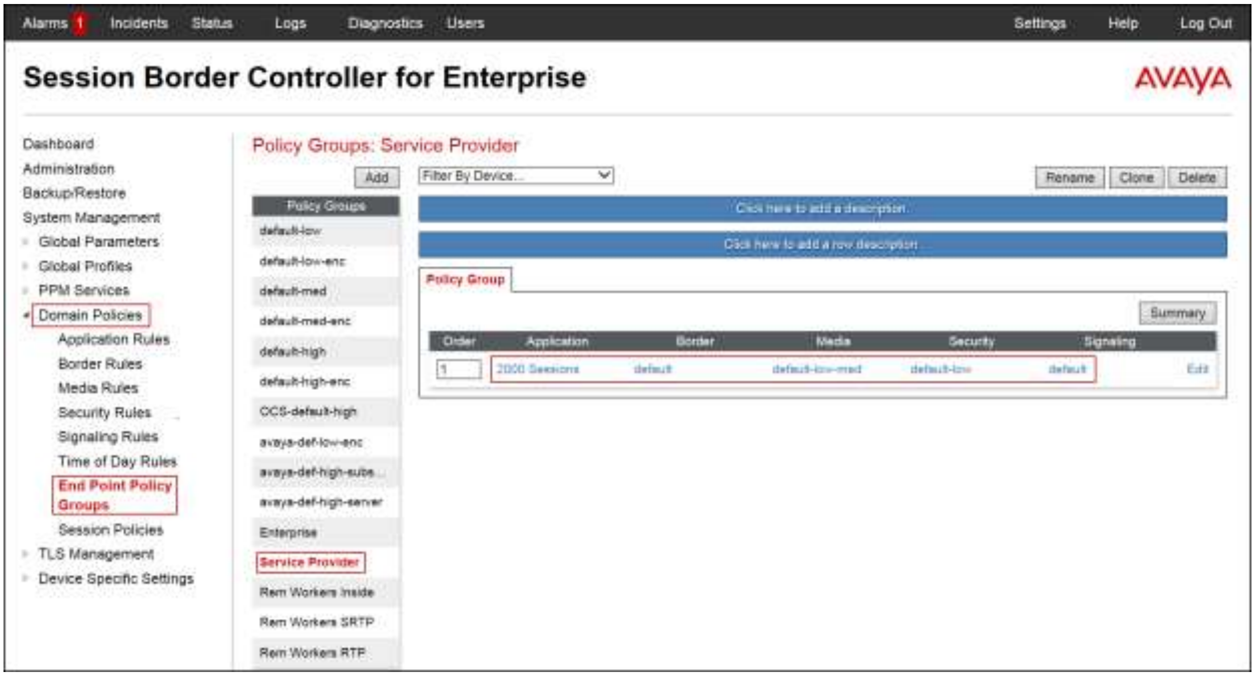


Similarly, to create an End Point Policy Group for the service provider SIP Trunk, select **Add Group**.

- **Group Name: Service Provider**.
- **Application Rule: 2000 Sessions**.
- **Border Rule: default**.
- **Media Rule: default-low-med**.
- **Security Rule: default-low**.
- **Signaling Rule: default**.
- Click **Finish**.



The following screen capture shows the newly created **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 Settings** menu on the left-hand side, select **Network Management**. Select the **Networks** tab.

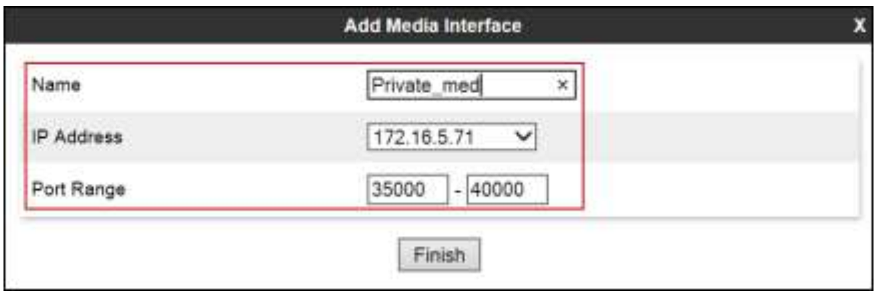
On the **Interface** tab, click the **Disabled** control for interface **A1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **Disabled**, so it is important to perform this step, or the Avaya SBCE will not be able to communicate on any of its interfaces.

6.4.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, port range 35000 to 40000 was used.

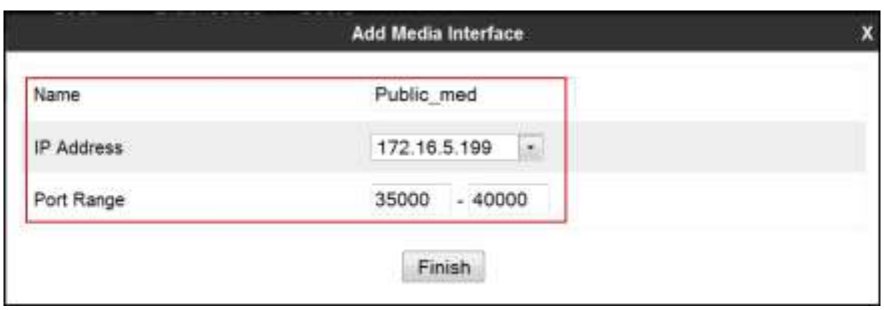
From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**. Below is the configuration of the inside, private Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area (not shown).
- **Name: Private_med**.
- **IP Address: 172.16.5.71** (Inside or Private IP Address of the Avaya SBCE, toward the CS1000).
- **Port Range: 35000-40000**.
- Click **Finish**.



Below is the configuration of the outside, public Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area.
- **Name: Public_med**.
- **IP Address: 172.16.5.199** (IP Address of the Avaya SBCE toward the service provider via the VPN tunnel).
- **Port Range: 35000-40000**.
- Click **Finish**.



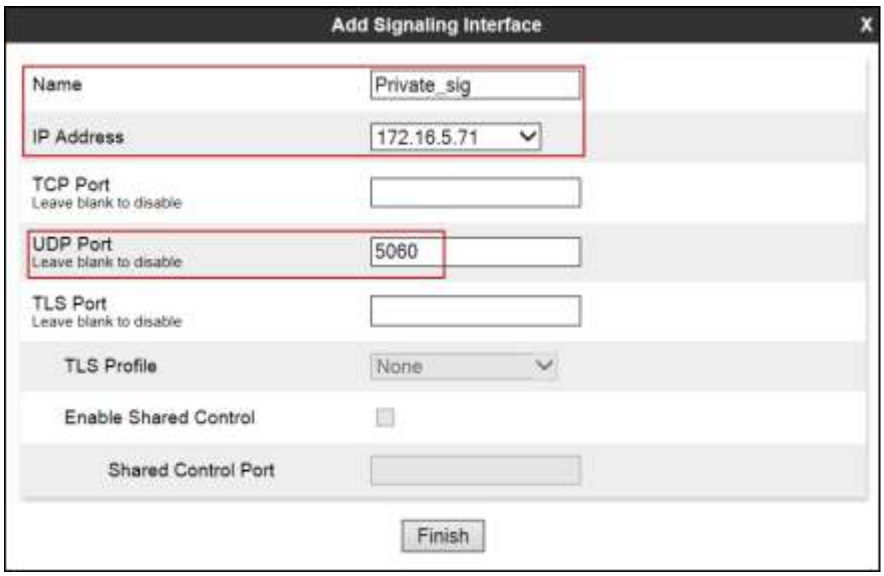
The following screen capture shows the newly created media interfaces.

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**.

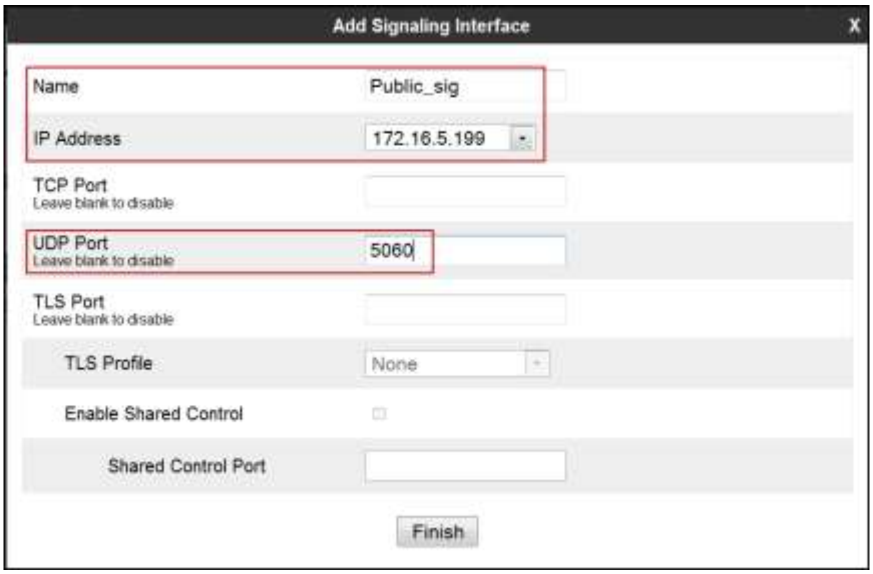
Below is the configuration of the inside, private Signaling Interface of the Avaya SBCE.

- Select **Add** in the **Signaling Interface** area.
- **Name: Private_sig**.
- Select **IP Address: 172.16.5.71** (Inside or Private IP Address of the Avaya SBCE, toward the CS1000).
- **UDP Port: 5060**.
- Click **Finish**.



Below is the configuration of the outside, public signaling Interface of the Avaya SBCE.

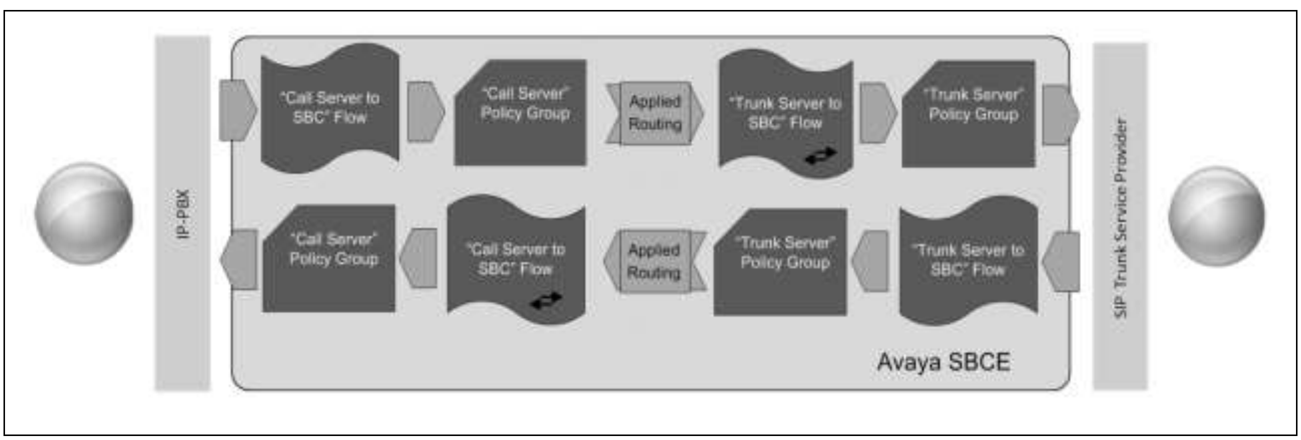
- Select **Add** in the **Signaling Interface** area.
- **Name: Public_sig**.
- **IP Address: 172.16.5.199** (IP Address of the Avaya SBCE toward the service provider via the VPN tunnel).
- **UDP Port: 5060**.
- Click **Finish**.



The following screen capture shows the newly created signaling interfaces.

6.4.4. End Point Flows

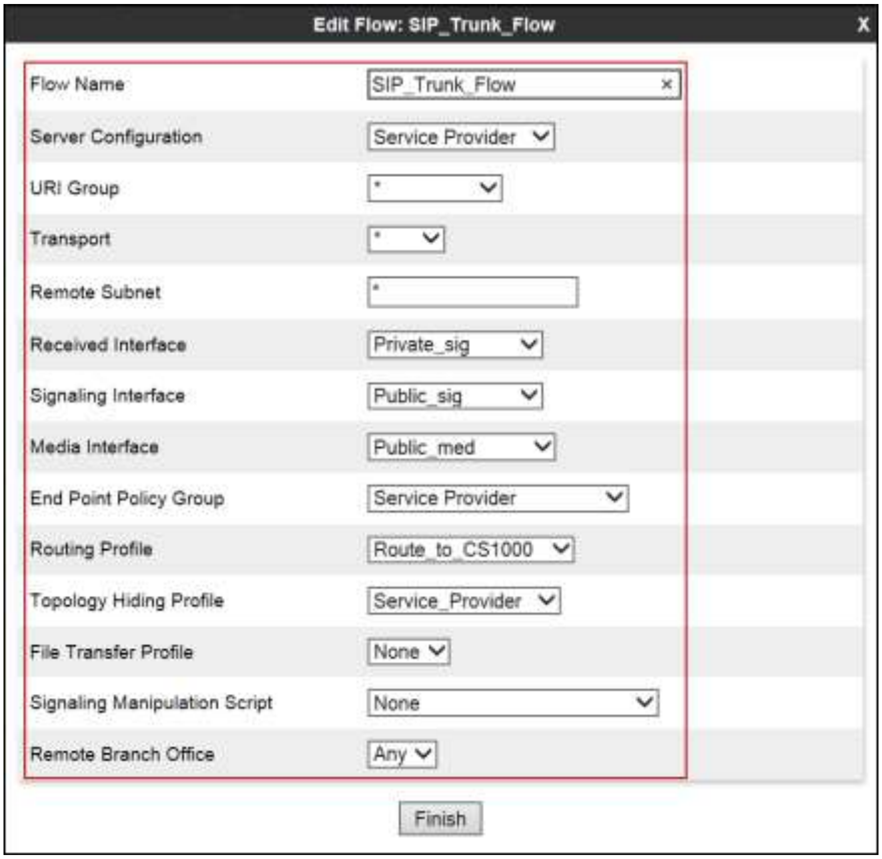
When a packet is received by the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing 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 **End-Point Flows** define 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.

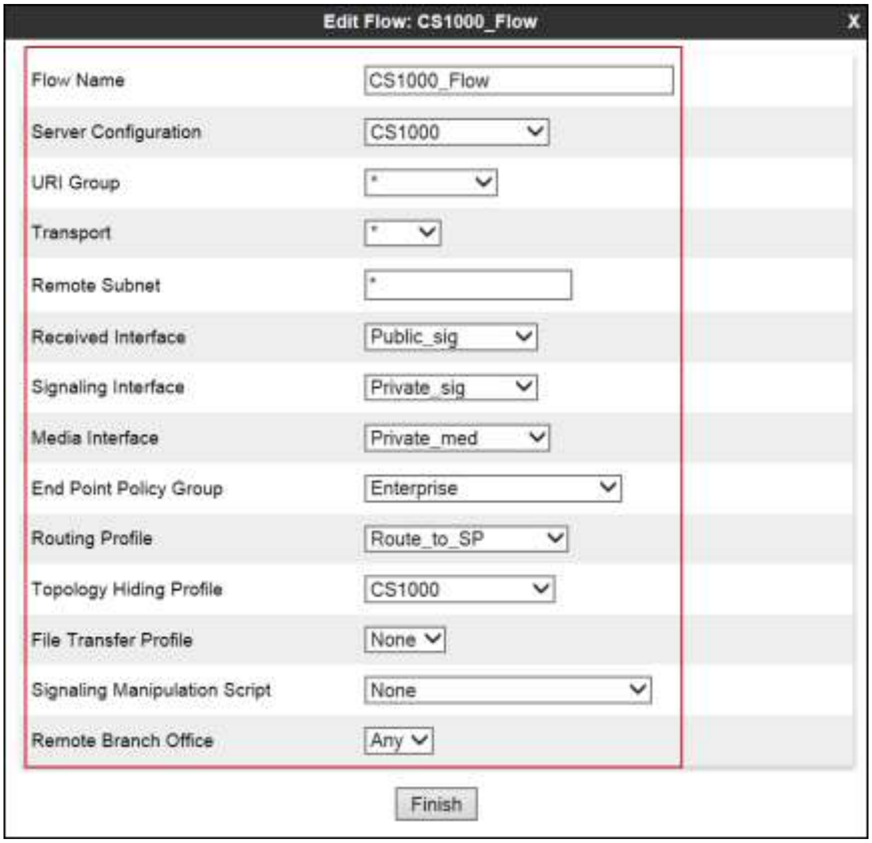
To create the call flow toward the service provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, and then the **Server Flows** tab. Click **Add Flow** (not shown).

- **Name: SIP_Trunk_Flow**.
- **Server Configuration**: **Service Provider**.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private_sig**.
- **Signaling Interface: Public_sig**.
- **Media Interface**: **Public_med**.
- **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**.
- **Signaling Manipulation Script**: **None**
- **Remote Brach Office: Any**.
- Click **Finish.**

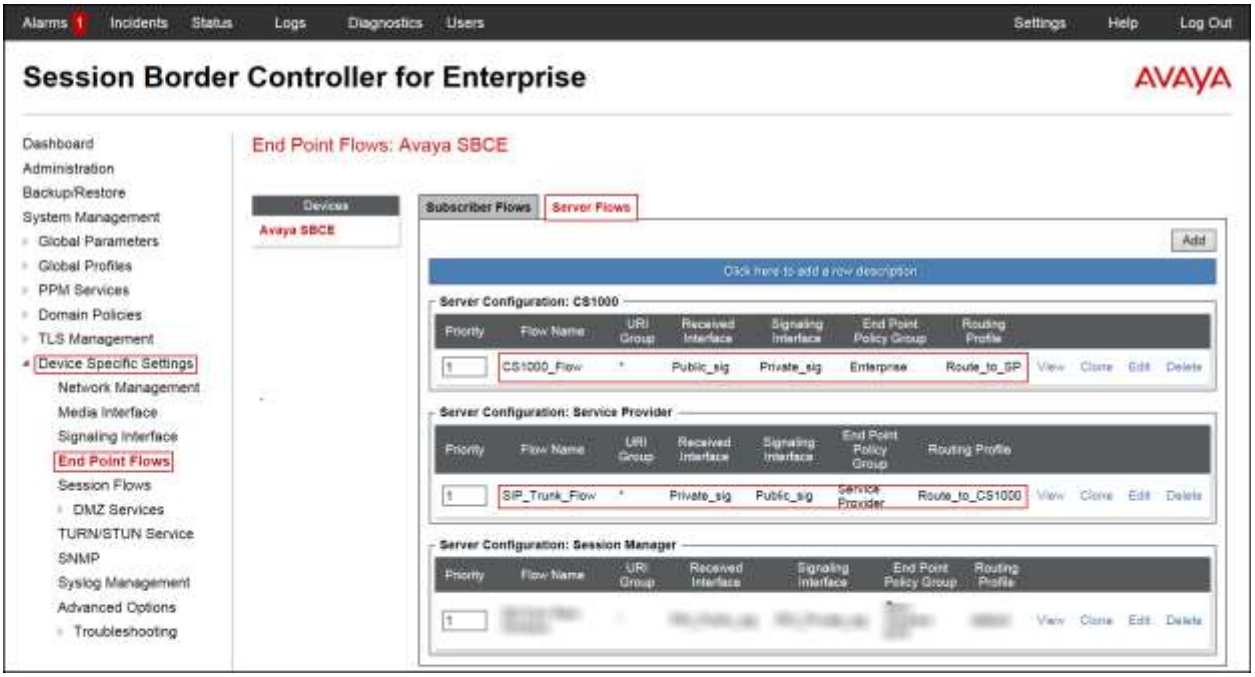


To create the call flow toward the CS1000, click **Add Flow**.

- **Name: CS1000_Flow**.
- **Server Configuration**: **CS1000**.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Public_sig**.
- **Signaling Interface: Private_sig**.
- **Media Interface**: **Private_med**.
- **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**.
- **Signaling Manipulation Script**: **None**
- **Remote Brach Office: Any**.
- Click **Finish**.


Edit Flow: CS1000_Flow
Flow Name
CS1000_Flow
Server Configuration
CS1000
URI Group
*
Transport
*
Remote Subnet
*
Received Interface
Public_sig
Signaling Interface
Private_sig
Media Interface
Private_med
End Point Policy Group
Enterprise
Routing Profile
Route_to_SP
Topology Hiding Profile
CS1000
File Transfer Profile
None
Signaling Manipulation Script
None
Remote Branch Office
Any
Finish

The following screen capture shows the newly created **End Point Flows.**



7. Claro SIP Trunking Service Configuration

To use Claro SIP Trunking service, a customer must request the service from Claro using the established sales processes. The process can be started by contacting Claro via the corporate web site at: http://www.claro.com.do/wps/portal/do/sc/empresas

During the signup process, Claro will require that the customer provide the public IP address used to reach Avaya SBCE at the edge of the enterprise. Claro 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 Avaya Communication Server 1000 and the Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

During the interoperability testing, a VPN connection was used to connect the simulated enterprise site to Claro's network via the public Internet. The connection could also be done without the use of a VPN connection, by directly connecting the Avaya SBCE to a public facing SBC located in Claro's network. This is accomplished by assigning public IP addresses, capable of being reached across the public Internet, to the Avaya SBCE (interface **B1**) and to the Claro's SBC.

8. Verification Steps

The following steps may be used to verify the configuration.

8.1. General

Place an inbound/outbound call from/to a PSTN phone and 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 disconnects properly.

Verify Call Establishment on the CS1000 Call Server.

Active Call Trace (LD 80).

The 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 (786331xxxx).

- 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 the call is released, issue command **trac 0 8000** 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 extension 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[redacted]
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[redacted]  NUM_PLAN:E164    TON:NATIONAL  ESN:NPA
```

The following screen shows an example after the call on extension 8000 was been 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
```

8.2. Protocol Traces

Wireshark was used to verify SIP message information for each call. Wireshark traces were captured on the outside or public network side of the Avaya SBCE, in between the simulated enterprise and Claro.

9. Conclusion

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Communication Server 1000 Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.3 to support Claro SIP Trunking Services, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

10. References

This section references the documentation relevant to these Application Notes.

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

[1] *Avaya Communication Server 1000 Network Routing Service Fundamentals*, Release 7.6, Document Number NN43001-130, Issue 04.04, June 2014.
[2] *Avaya Communication Server 1000 IP Peer Networking Installation and Commissioning*, Release 7.6, Document Number NN43001-313, Issue 06.04, September 2014.
[3] *Avaya Communication Server 1000 Overview*, Release 7.6, Document Number NN43041-110, Issue 06.02, June 2014.
[4] *Unified Communications Management Common Services Fundamentals Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013.
[5] *Avaya Communication Server 1000 Dialing Plans Reference*, Release 7.6, Document Number NN43001-283, Issue 06.02, July 2014.
[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 Release 7.6: An Overview*. Document Number PSN003460u, Issue 02, April 05, 2013.
[8] *Communication Server 1000 Release 7.6 & Service Pack 6 Release Notes*, Issue 1.0 December 2014.

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 6.3, Issue 4, October 2014.
[10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014.

Other resources:

[11] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[12] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

11. Appendix A: SigMa Script

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

Title: Remove_SDP_MIME_Types

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