Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Hawaiian Telecom SIP Trunk service with Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring Hawaiian Telecom SIP Trunk service with Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2.

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

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

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

Table of Contents

1. Introduction

These Application Notes provide the procedure for configuring Hawaiian Telecom SIP Trunk service with Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2. During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure the interoperability between the Hawaiian Telecom network and Avaya Communication Server 1000E.

In the sample configuration, the Avaya solution consists of a Communication Server 1000E Rel. 7.5 (hereafter referred to as CS1000), Avaya Aura® Session Manager Rel. 6.3 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Rel. 6.2 (hereafter referred to as Avaya SBCE), and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya SBCE or Session Manager.

2. General Test Approach and Test Results

The CS1000 system was connected to the Avaya SBCE via SIP trunks to Session Manager. The Avaya SBCE was connected to the Hawaiian Telecom network via SIP trunks. Various call types were made from the CS1000 to Hawaiian Telecom's network and vice versa to verify interoperability between the CS1000 and the Hawaiian Telecom network.

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 CS1000 can interoperate with the Hawaiian Telecom network. The following interoperability areas were covered:

- SIP trunk registration with the service provider
- Incoming calls from the PSTN were routed to DID numbers assigned by Hawaiian Telecom. 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 Hawaiian Telecom'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 voicemail off).
- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codecs G.711u, G.711a and G.729 with Voice Activity Detection (VAD) disabled.

- Voicemail and DTMF tone support in both directions (RFC2833) (Leaving voicemail, retrieving voicemail, etc.).
- CallPilot Voicemail Server (Hosted in the CS1000).
- Outbound Toll-Free calls, interacting with Interactive Voice Response systems (IVR).
- International calls.
- Calling number and calling name blocking (Privacy).
- Call Hold/Resume.
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Call Park.
- Consultative Call transfers.
- Station Conference.
- T.38 fax support.
- G.711u fax pass-through support.
- Long duration calls (one hour).
- Early Media transmission.

2.2. Test Results

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

- **Calling Name and Calling Number Delivery to PSTN:** On outbound calls from the CS1000 to the PSTN the "Calling Name" is not delivered to the PSTN phone (is not displayed), only the "Calling Number" is delivered (is displayed).
- **Caller-ID on re-directed calls to PSTN:** Caller ID works properly between the CS1000 and the Hawaiian Telecom network when there is no call re-direction involved. However, when a call is re-directed to the PSTN at the CS1000 extension, the Caller ID will not properly reflect the true originator of the call. In normal conditions if a call is re-directed at the CS1000 to a PSTN extension, the Caller ID displayed at the PSTN extension will be of the extension doing the re-direction (i.e., transferee) and not the Caller ID of the extension that originated the call.
- **T.38 Fax:** T.38 fax from the CS1000 to the PSTN (outbound) is not supported by Hawaiian Telecom; Hawaiian Telecom only supports T.38 fax from the PSTN to the CS1000 (inbound). Fax calls from the CS1000 to the PSTN (outbound) defaulted to G.711 pass-through. G.711 pass-through for fax was successfully tested in both directions (CS1000 → PSTN and PSTN → CS1000).
- **SIP Header Optimization:** SIP header rules were implemented in Avaya SBCE and in Session Manager to streamline the SIP header and remove any unnecessary parts. The following headers were removed: X_nt_e164_clid, Alert-Info if they were present in the INVITE. Also the multipart MIME SDP, which included the x-nt-mcdn-frag-hex, x-nt-esn5-frag-hex, and x-nt-epid-frag were stripped out. These particular headers and MIME have no real use in the service provider network. If an issue is being investigated on the service provider network, the presence of these headers may add unnecessary confusion.

- **Calls to Busy Numbers:** Hawaiian Telecom's network is not sending "486 Busy Here" for calls from the CS1000 to Busy PSTN numbers. Since Busy Tone is heard by the user this observation is considered non critical.
- **Displays on Held Calls:** If a CS1000 phone holds/retrieves an outbound call, the dialed digits are no longer displayed, instead the access code for the trunk route (ACOD) is displayed. This is a Communication Server 1000 known issue.
- **Items not supported or not tested included the following**:
  - Off-net call forwarding was not tested with the History-Info method. Testing was done with an Adaptation in Session Manager to convert History-Info to Diversion header.
  - Inbound toll-free calls.
  - 0, 0+10, 911

2.3. Support

For support on Hawaiian Telecom systems, call:
Toll Free at: 1-808-643-0944 or visit the corporate Web page at:
https://www.hawaiiantel.com/business/Business.aspx

3. Reference Configuration

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

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

- Avaya Communication Server 1000E (CS1000E).
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® Session Manager.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya 1100-Series IP Telephones (UniStim).
- Avaya 1100-Series Telephones (SIP).
- 2050 Avaya IP Softphone.
- Avaya M3904 Digital telephones.
- Analog Telephones.
- Fax machines.
- Desktop with administration interfaces.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Hawaiian Telecom across the public IP network is SIP over UDP. The transport protocol between the Avaya SBCE and Session Manager across the enterprise IP network is SIP over TCP. The transport protocol between Session Manager and the CS1000 across the enterprise IP network is SIP over TLS. For ease of troubleshooting during testing, the compliance test was conducted with the Transport Method set to UDP between Session Manager and the CS1000.

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.

One SIP trunk group was created between the CS1000 and Session Manager to carry the traffic to and from the service provider (two-way trunk group).

For inbound calls, the calls flowed from Hawaiian Telecom's network to the Avaya SBCE and then to Session Manager. Session Manager used the configured dial patterns and routing policies to determine the recipient (in this case the CS1000) and on which link to send the call. 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 Session Manager. Session Manager once again used the configured dial patterns, adaptations, and routing policies to determine the route to the Avaya SBCE for egress to Hawaiian Telecom's network.

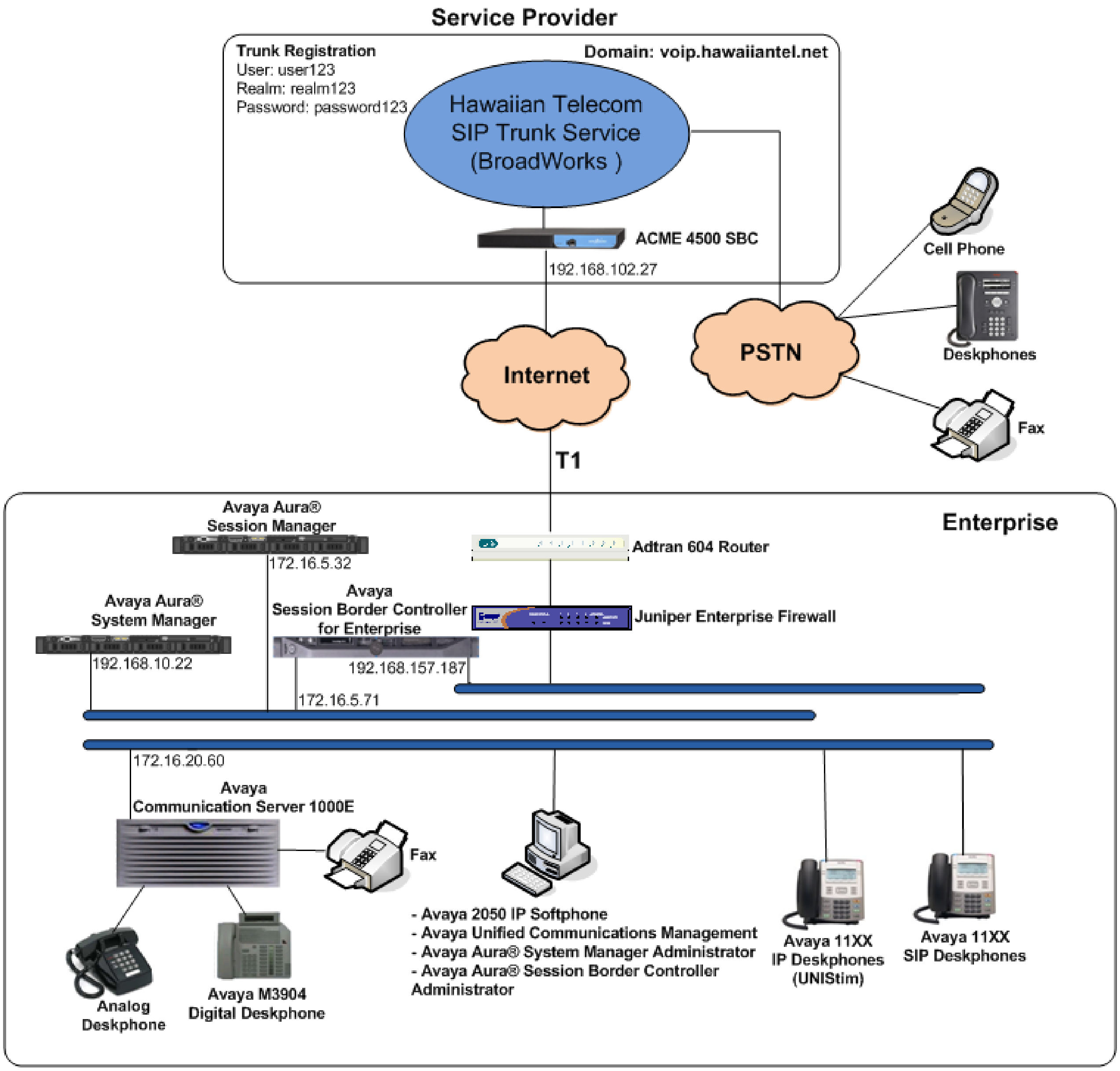


Figure 1: Hawaiian Telecom SIP Trunk service with Avaya CS1000E

4. Equipment and Software Validated

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

Avaya:	
Equipment	**Release/Version**
Avaya Communication Server 1000E running Co-resident Call Server, Signaling Server and Media Gateway in a single CP-MGS card.	Call Server: 7.50 Q + DepList 1: core Issue: 01 **(created: 2013-03-19 16:44:12 (est))** Signaling Server: 7.50.17.00 **See Service Updates & Patches below**
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3 Service Pack 1 (6.3.1.0.631004)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3 Service Pack 1 Build No. 6.3.0.8.5682-6.3.8.859 Software Update Rev. No. 6.3.1.9.1212
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.0.Q36
Avaya Deskphones	1110: 0623C8G (UniStim) 1120: 0624C8G (UniStim) 1165: 0626C8G (UniStim) 1120: 04.01.15.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.02.0062
Lucent Analog Phone	N/A
Fax Machines	N/A
Hawaiian Telecom:	
Equipment	**Release/Version**
BroadWorks	17 SP3
ACME Session Border Controller (4500)	SCX 6.2.0 MR11

Signaling Server Service Updates & Patches:

Note: The **VTRK** SU version should be "cs1000-vtrk-7.50.17.16-**20**.i386.000.ntl" or higher on all Signaling Servers to ensure proper operation of blind transfer feature. Patch **p30224_1** is required if problems with SIP **UPDATE** are observed during Call Redirection scenarios. Patch **p27159_1** is required for T.38 fax support.

SUs:
avaya-cs1000-cnd-4.0.20-00.i386.000
cs1000-dbcom-7.50.17.16-1.i386.000

ipsec-tools-0.6.5-14.el5.3_avaya_1.i386.000
cs1000-shared-pbx-7.50.17.16-1.i386.000
cs1000-kcv-7.50.17.16-1.i386.000
cs1000-baseWeb-7.50.17.16-2.i386.000
cs1000-ipsec-7.50.17.16-1.i386.000
cs1000-linuxbase-7.50.17.16-15.i386.000
cs1000-patchWeb-7.50.17.16-11.i386.000
cs1000-ncs-7.50.17.16-1.i386.000|Start:ncs
spiritAgent-6.1-1.0.0.108.208.i386.000
cs1000-dmWeb-7.50.17.16-7.i386.000
cs1000-Jboss-Quantum-7.50.17.16-33.i386.000
cs1000-sps-7.50.17.16-12.i386.000
cs1000-cs1000WebService_6-0-7.50.17.16-1.i386.000
tzdata-2011h-2.el5.i386.000
cs1000-csoneksvrmgr-7.50.17.16-1.i386.000
cs1000-csmWeb-7.50.17.16-6.i386.000
cs1000-emWeb_6-0-7.50.17.16-34.i386.000
cs1000-tps-7.50.17.16-29.i386.000
cs1000-ftrpkg-7.50.17.16-12.i386.000
cs1000-pd-7.50.17.16-2.i386.000
cs1000-EmCentralLogic-7.50.17.16-2.i386.000
cs1000-bcc-7.50.17.16-87.i386.000
cs1000-mscAttn-7.50.17.16-6.i386.000
cs1000-mscAnnc-7.50.17.16-16.i386.000
cs1000-emWebLocal_6-0-7.50.17.16-3.i386.000
cs1000-mscConf-7.50.17.16-4.i386.000
cs1000-mscMusc-7.50.17.16-17.i386.000
cs1000-mscTone-7.50.17.16-4.i386.000
cs1000-vtrk-7.50.17.16-168.i386.000
####################
Patches:
p30224_1
p27159_1
p31484_1
####################

Loadware:

LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 11

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME
00	Q01981776	ISS1:1OF1	udtcab17	09/04/2013	udtcab17.lw
01	Q01820502	ISS1:1OF1	MGCMAB01	13/02/2012	MGCMAB01.LW
02	WI00998702	ISS1:1OF1	MGCCCD03	09/04/2013	MGCCCD03.LW
05	wi00839337	ISS1:1OF1	DSP1AB06	08/02/2012	DSP1AB06.LW
06	wi00839337	ISS1:1OF1	DSP2AB06	08/02/2012	DSP2AB06.LW
07	wi00839337	ISS1:1OF1	DSP3AB06	08/02/2012	DSP3AB06.LW
08	wi00839337	ISS1:1OF1	DSP4AB06	08/02/2012	DSP4AB06.LW
09	wi00839337	ISS1:1OF1	DSP5AB06	08/02/2012	DSP5AB06.LW
10	wi00946113	ISS1:1OF1	MGCBBA15	08/02/2012	MGCBBA15.LW
11			mgcfaa19	08/02/2012	MGCFAA19.LD
12	wi00946109	ISS1:1OF1	MGCABA15	08/02/2012	MGCABA15.L

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-Ins **201** and **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 201** and click the **Enable** button, the status will change to **Enabled**; do the same for **plug-in 501**.

ENABLED PLUGINS : 2

PLUGIN	STATUS	PRS/CR_NUM	MPLR_NUM	DESCRIPTION
201	**ENABLED**	Q00424053	MPLR08139	PI:Cant XFER OUTG TRK TO OUTG TRK
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 1000E

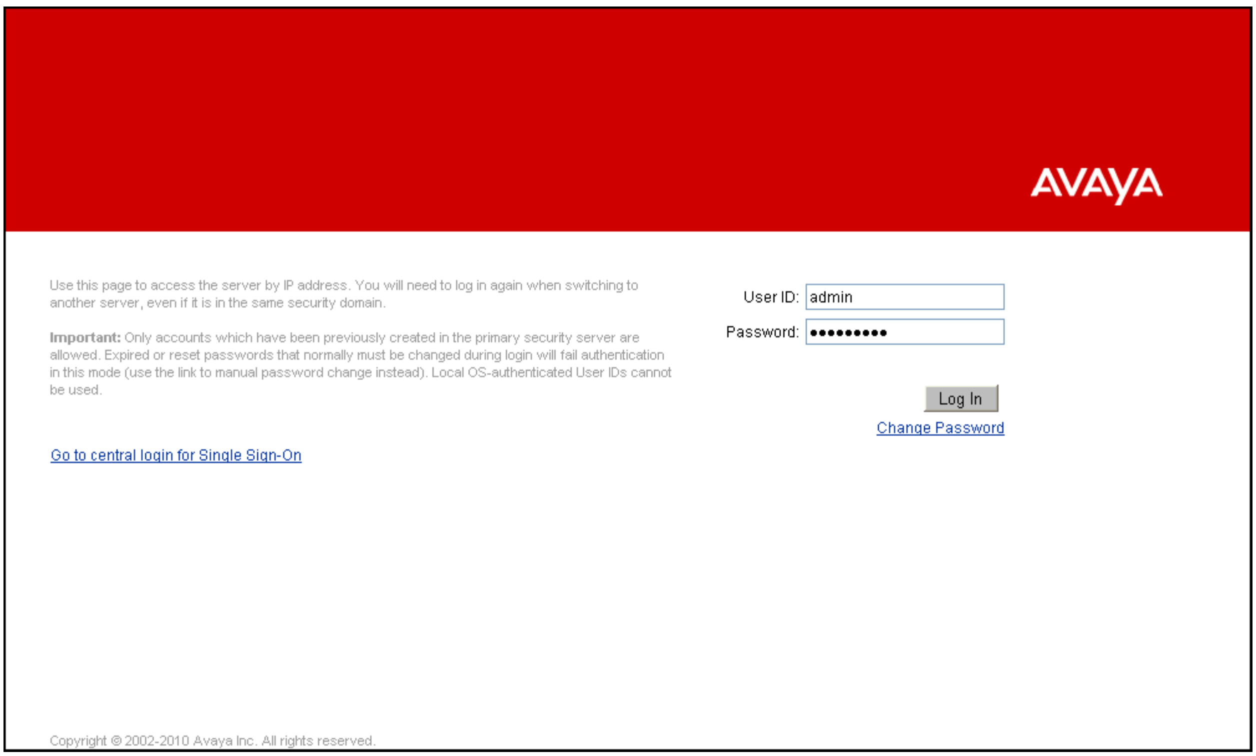
These Application Notes assume that the basic configuration of the CS1000 has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 11.**

The procedures shown below describe the configuration details of the CS1000 with SIP trunks to the Hawaiian Telecom network.

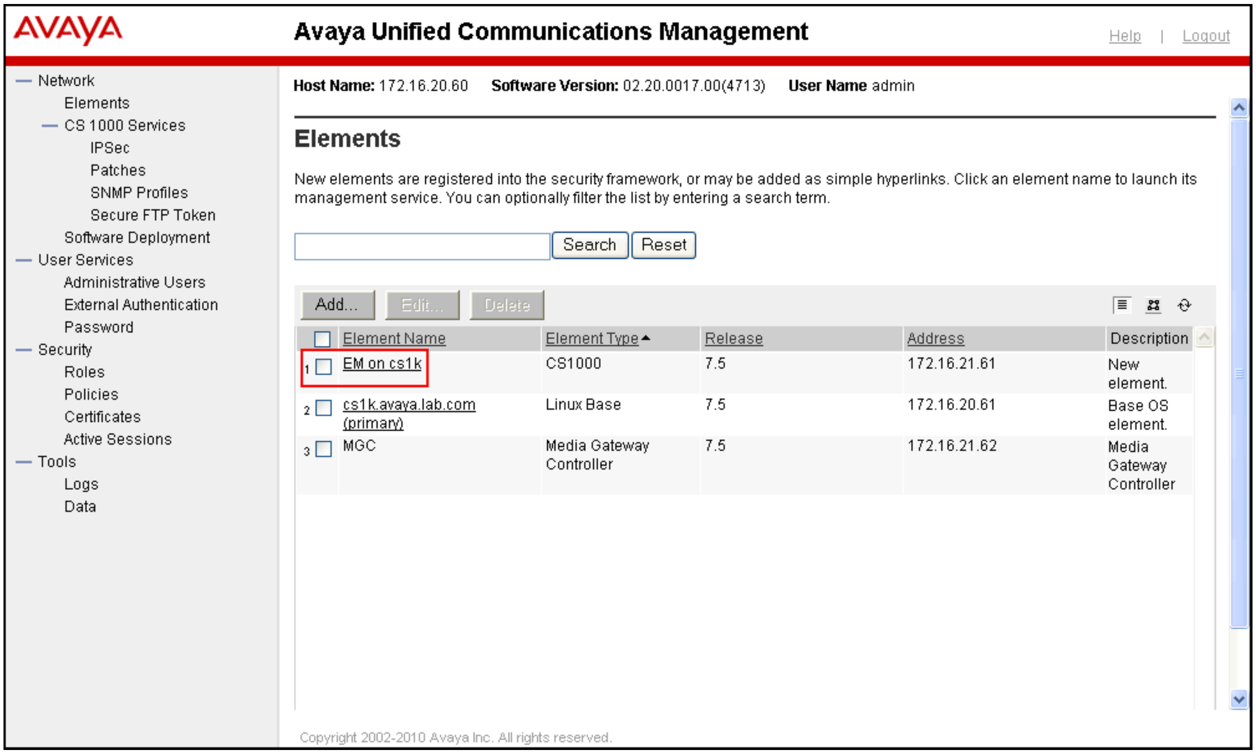
5.1. Login to the CS1000 System

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

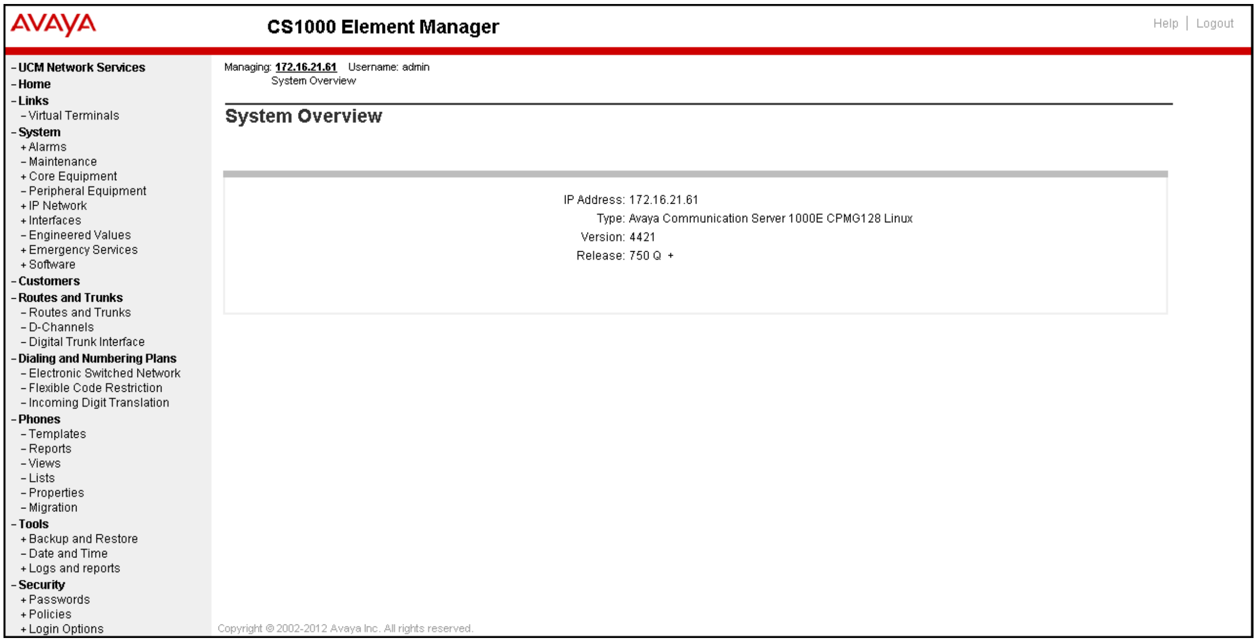
Open an instance of a web browser and connect to the UCM GUI at the following address: http://<UCM IP address> Log in using an appropriate Username and Password.



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



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



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

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

```
=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2012.03.26 11:44:22 =~=~=~=~=~=~=~=~=~=~=~=
login as: admin

               Avaya Inc. Linux Base  7.50
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.

admin@172.16.20.60's password:
Last login: Mon Mar 26 12:15:09 2012 from 172.16.5.250
]0;admin@cs1k:~[admin@cs1k ~]$ cslogin

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

TTY 15 SCH MTC BUG OSN   12:18
OVL111 IDLE   0
>logi
USERID? admin
PASS?
.
TTY #15 LOGGED IN ADMIN 12:18  26/3/2012

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

OVL000
>
```

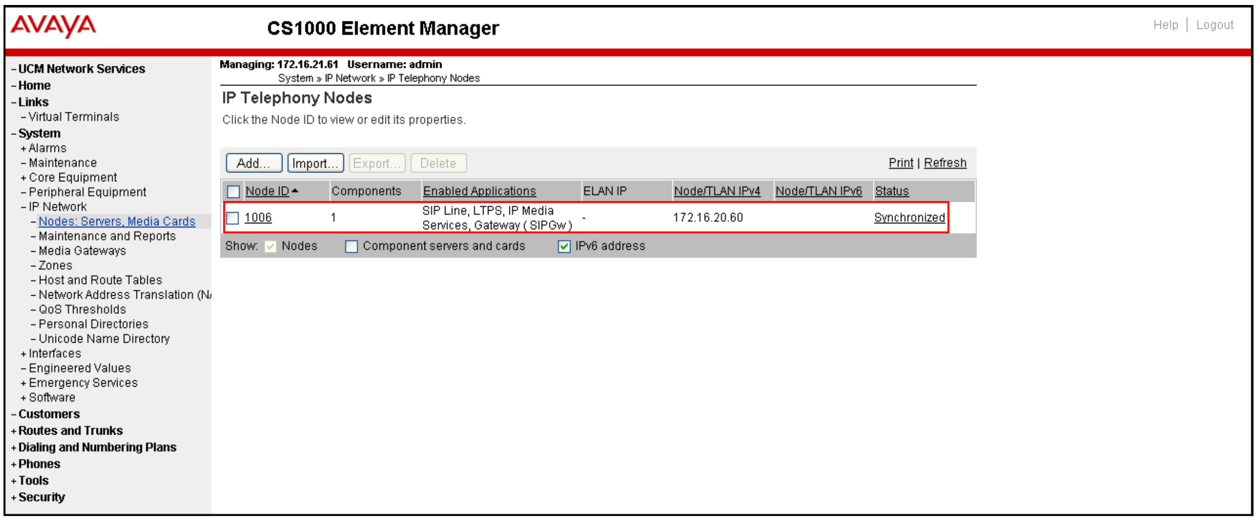
5.2. Administer a Node IP Telephony

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

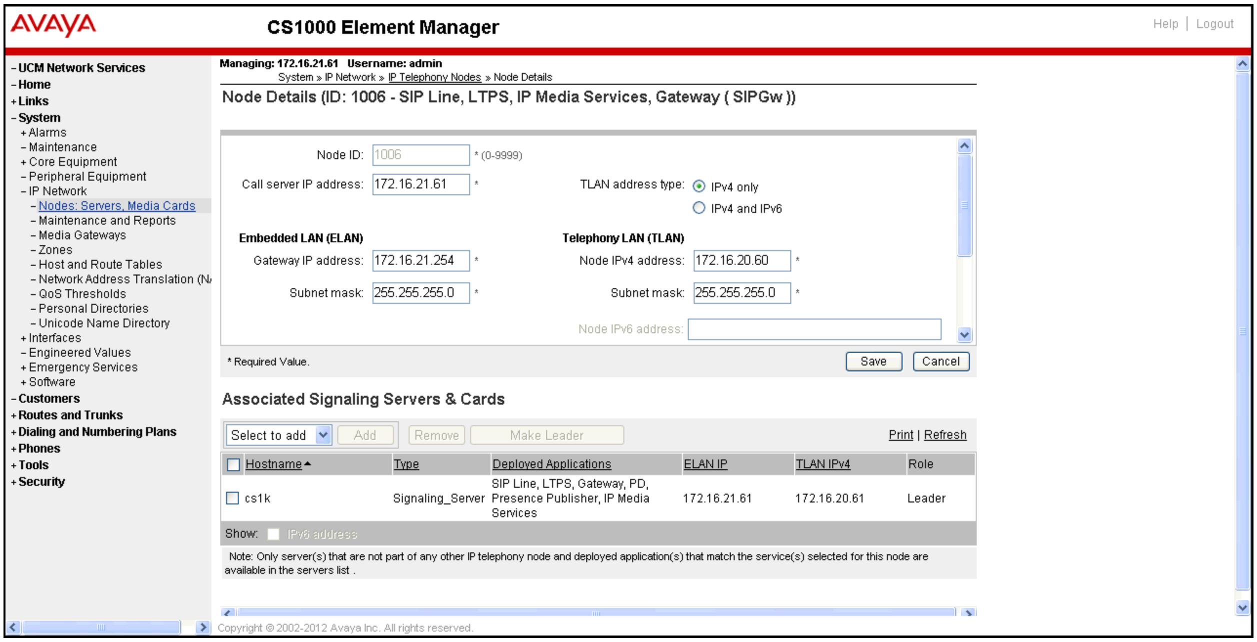
5.2.1. Obtain Node IP address

These Application Notes assume 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 the Hawaiian Telecom network.

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

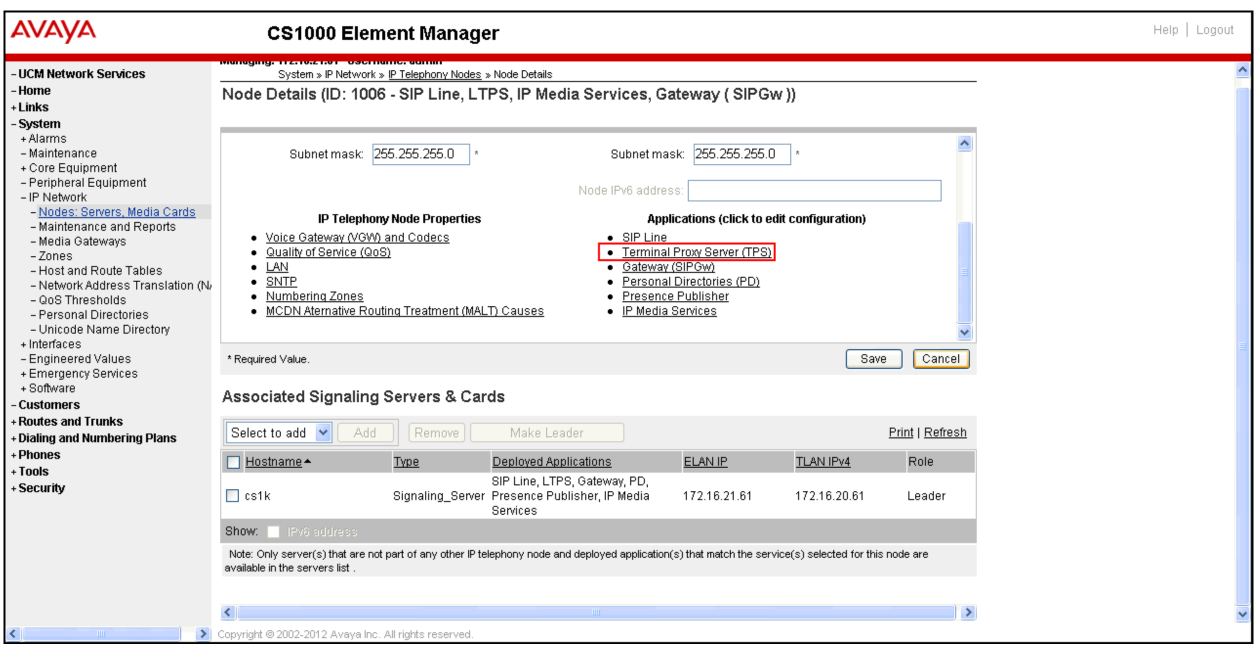


The **Node Details** screen is displayed below with the IP address of the CS1000 node. Under the **Node Details** heading at the top of the screen, make a note of the **TLAN Node IPV4 address**. In the sample screen below, the **Node IPV4 address** is "**172.16.20.60**". This IP address will be needed when configuring Session Manager with a SIP Entity for the Avaya CS1000 in **Section 6.5.**

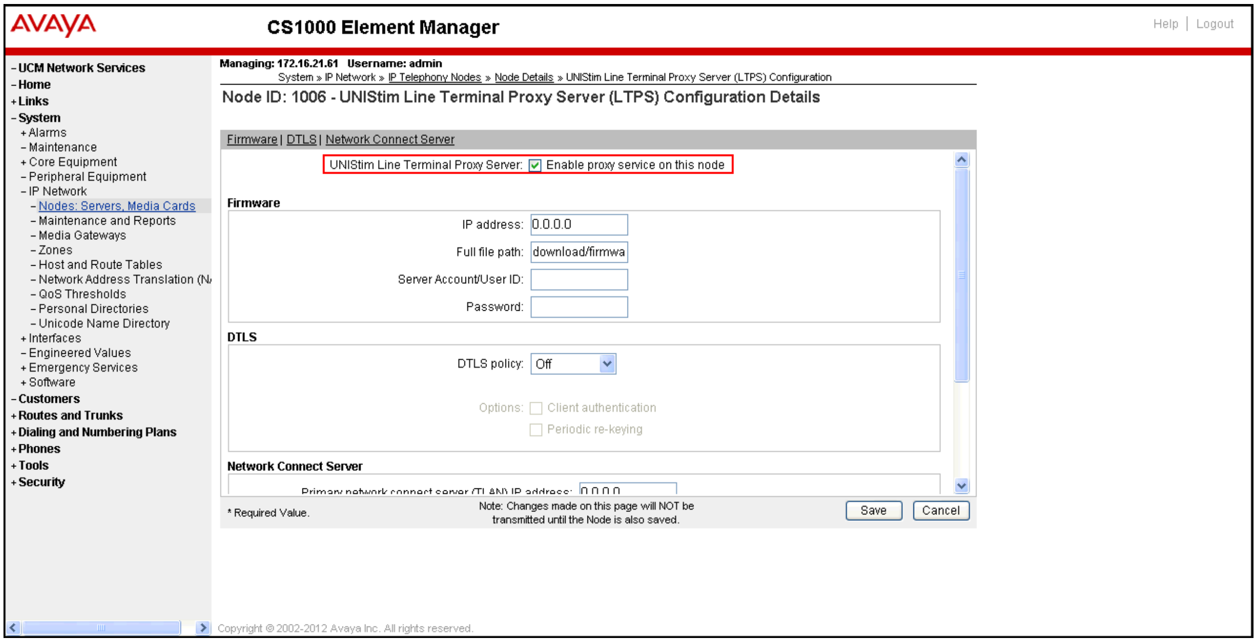


5.2.2. Administer Terminal Proxy Server

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

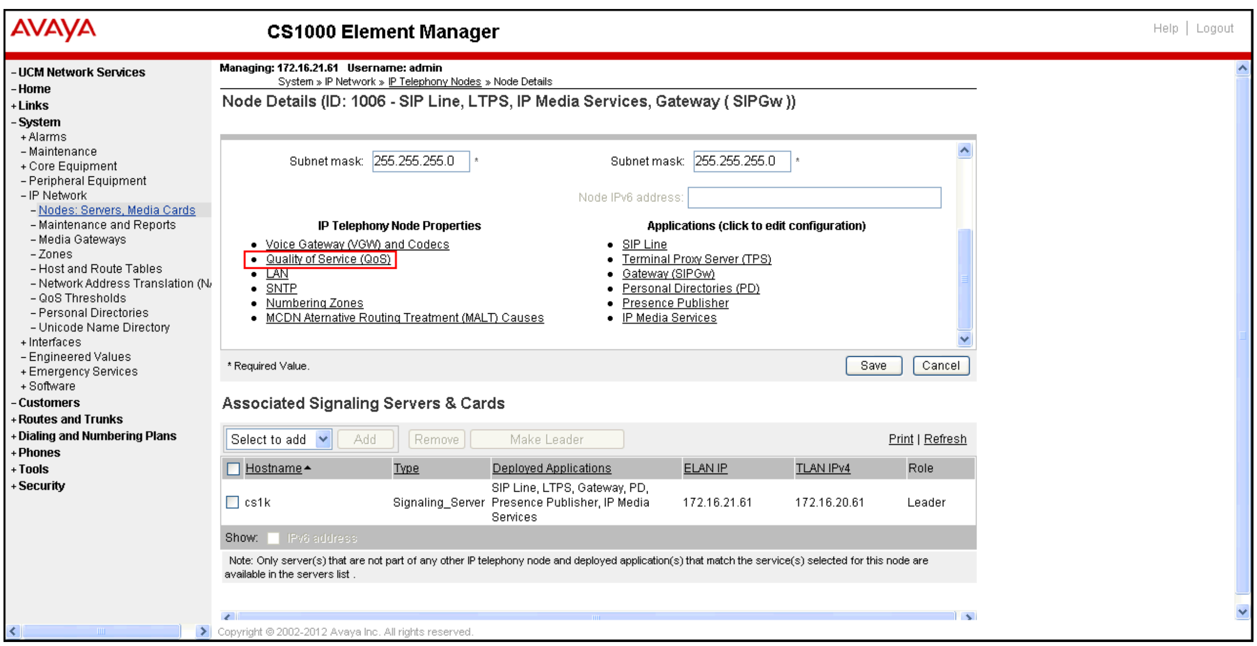


The **UNIStim Line Terminal Proxy Server (LTPS) Configuration Details** screen is displayed below. Check the **Enable proxy service on this node** check box and then click **Save**.

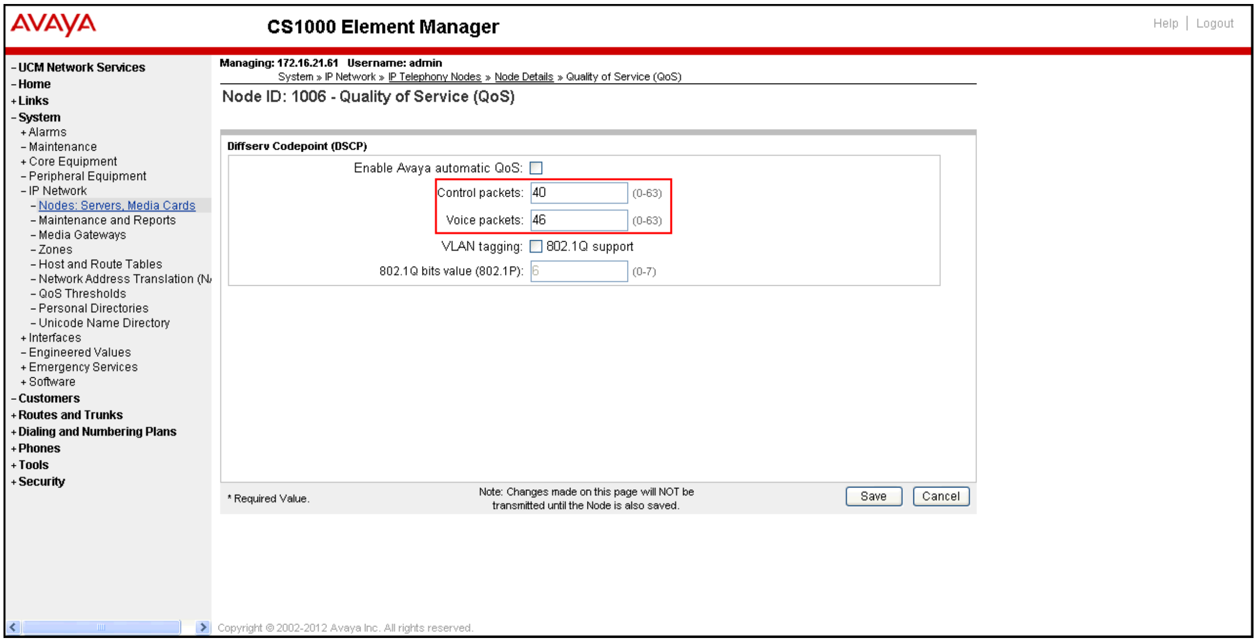


5.2.3. Administer Quality of Service (QoS)

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

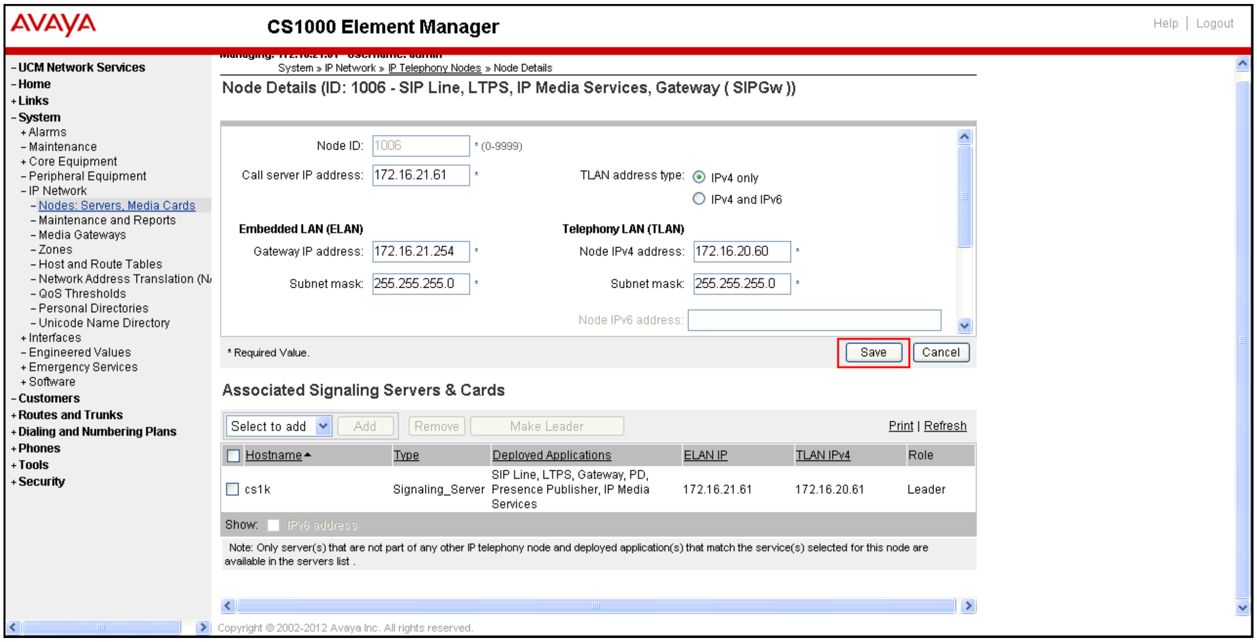


The **Quality of Service (QoS)** screen shown below will be displayed. Accept the default Diffserv values. Click the **Save** button.



5.2.4. Synchronize the New Configuration

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

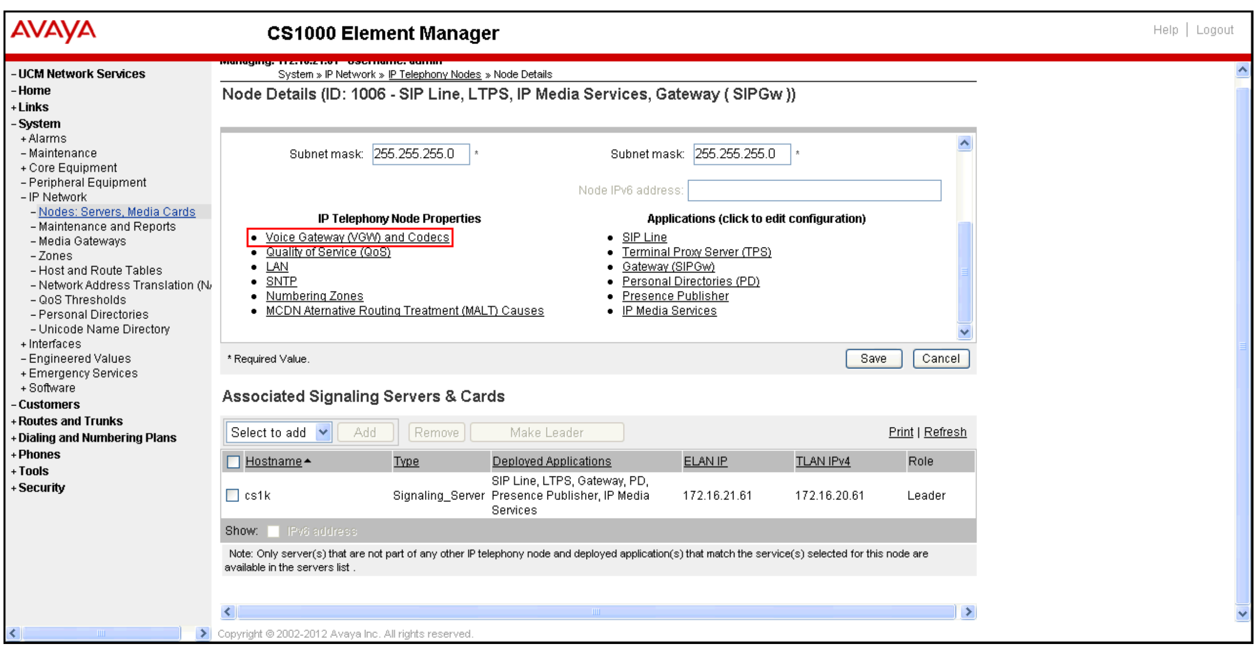


5.3. Administer Voice Codec

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

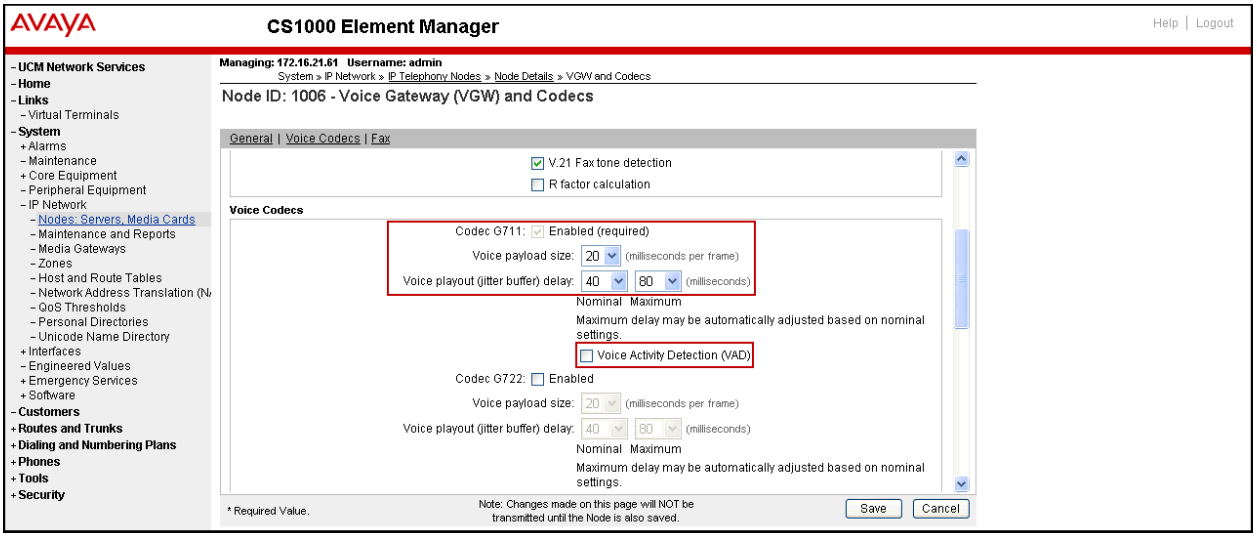
5.3.1. Enable Voice Codec, Node IP Telephony.

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

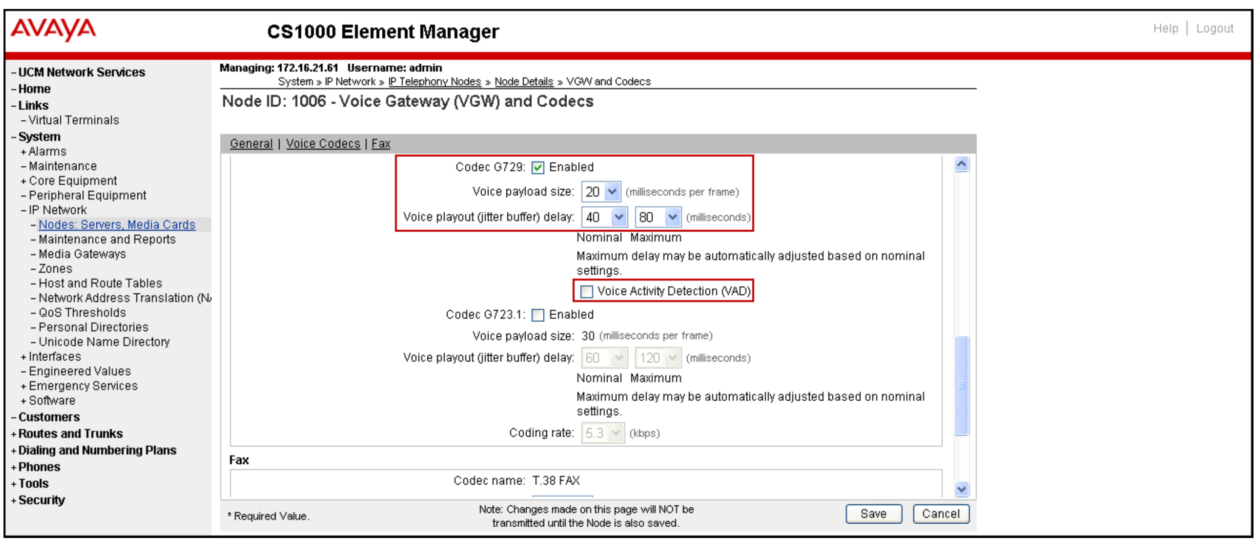


The **Voice Gateway (VGW) and Codec** screen is displayed below. Hawaiian Telecom supports **G711u, G.711a** and **G.729** Codecs with **Voice Activity Detection** **(VAD)** disabled.

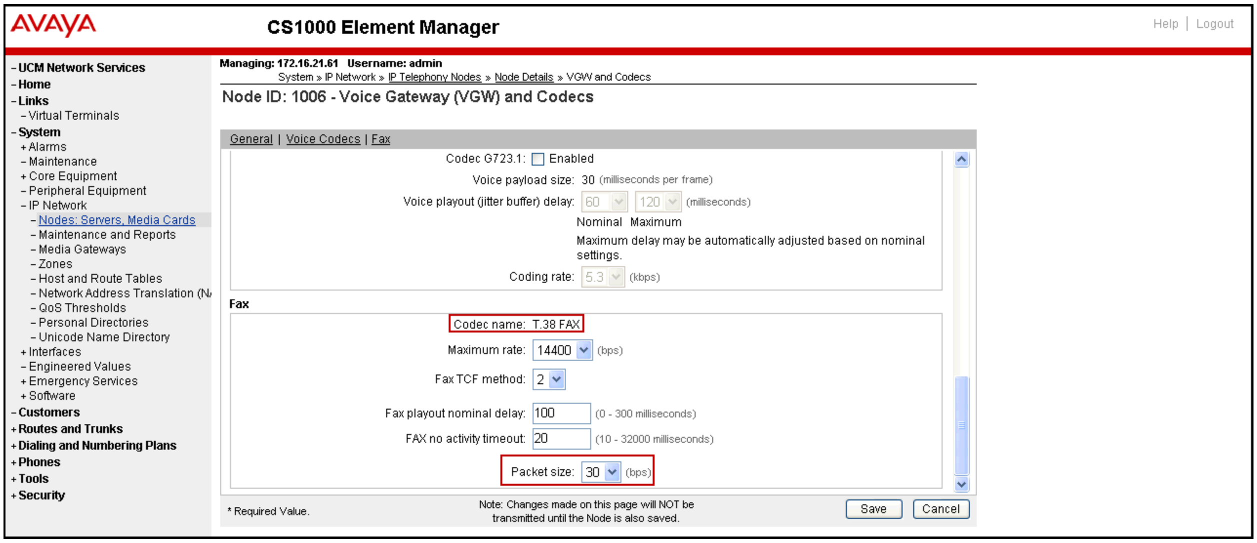
The values for the **G711** Voice Codec is shown below, ensure that **Voice Activity Detection (VAD)** is unchecked.



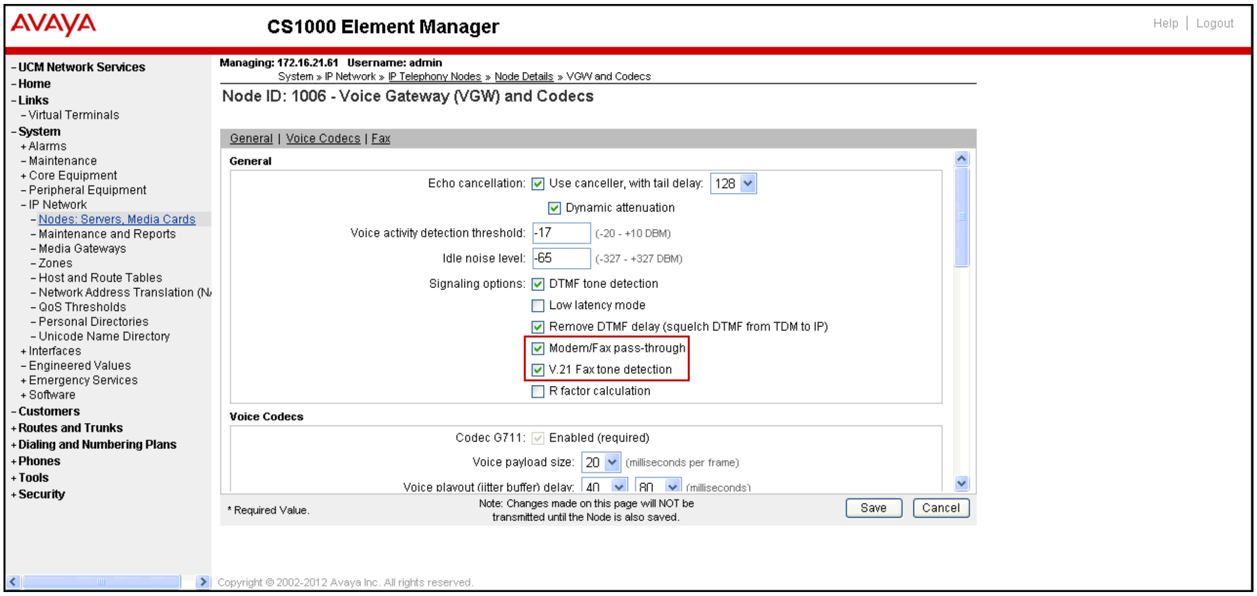
The values for the **G729** Voice Codec are shown below; ensure that **Codec G729** is checked and **Voice Activity Detection (VAD)** is unchecked as shown below.



For Fax over IP, **T.38** was used as the default and **G.711u pass-through** was set as fallback. **T.38** with payload size **30ms** was chosen as the default codec for fax. During the testing **T.38** fax transport worked successfully for fax calls from the PSTN to the CS1000 (inbound), for fax calls from the CS1000 to the PSTN (outbound), calls defaulted to **G.711u pass-through** (Refer to **Section 2.2**).



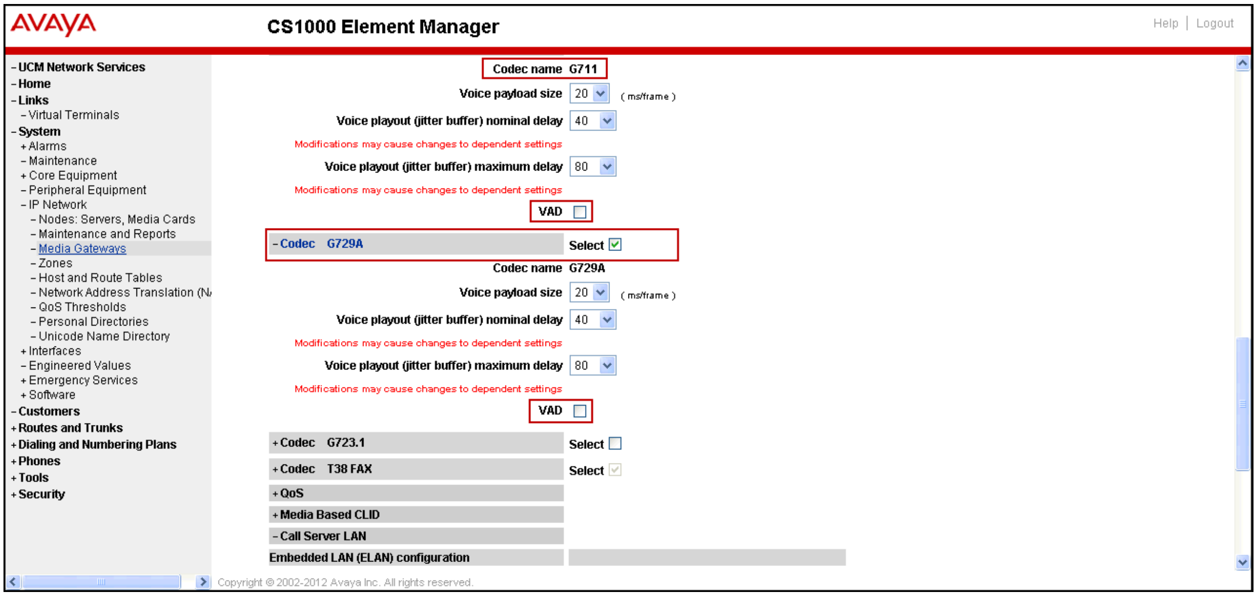
Scroll to the top of the page and ensure that **Modem/Fax Pass Through** and **V.21** are checked.



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

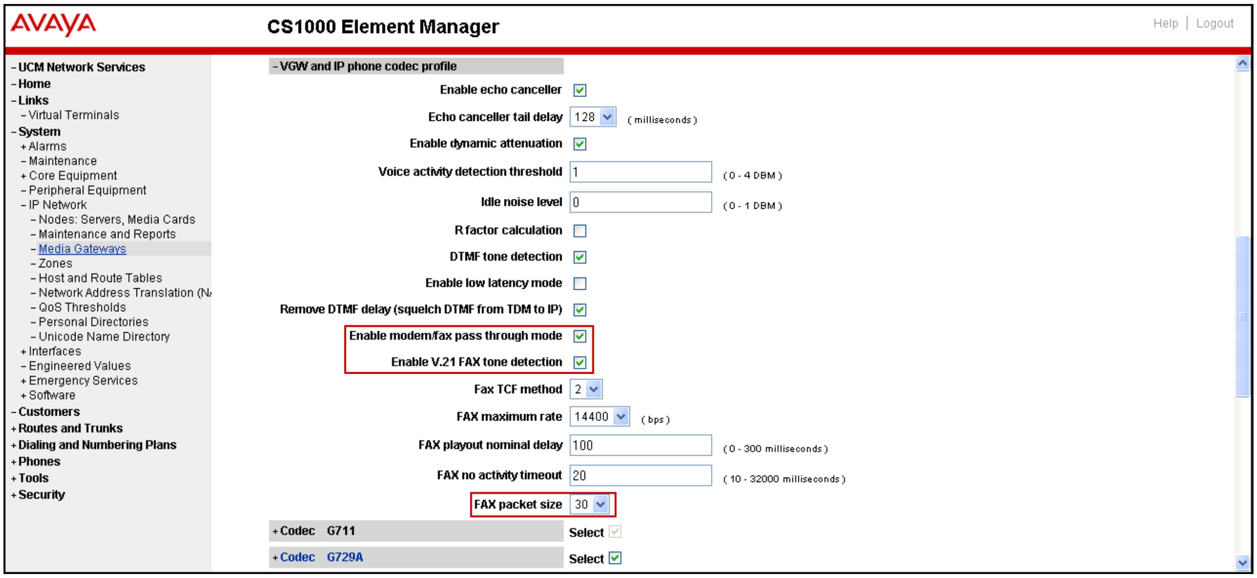
5.3.2. Enable Voice Codec on Media Gateways.

From the left menu of the Element Manager page, select the **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) and scroll down to the Codec **G711**, uncheck **VAD** for codec **G711**. Check Codec **G729A** and uncheck **VAD** for codec **G729A** as shown below. Scroll down to the bottom of the page and click **Save** (not shown).



For Fax over IP, **T.38** was used as the default and **G.711u pass-through** was set as fallback. During the testing, **T.38** fax transport worked successfully for fax calls from the PSTN to the CS1000 (inbound), but for fax calls from the CS1000 to the PSTN (outbound), calls defaulted to **G.711u pass-through** (Refer to **Section 2.2**).

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

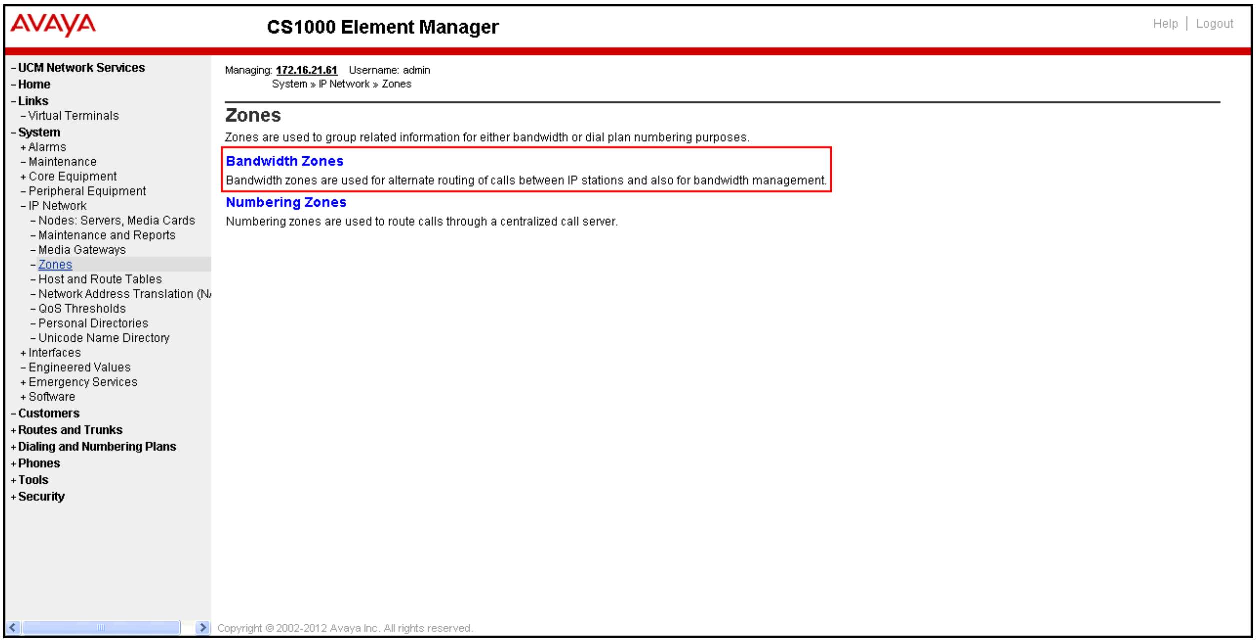


5.4. Administer Zones and Bandwidth

This section describes the steps to create bandwidth zones to be used by IP sets and SIP Trunks: **zones 1** and **5** are used by IP sets and **zone 4** is used by SIP Trunks.

5.4.1. Create a zone for IP phones (zones 1 and 5)

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

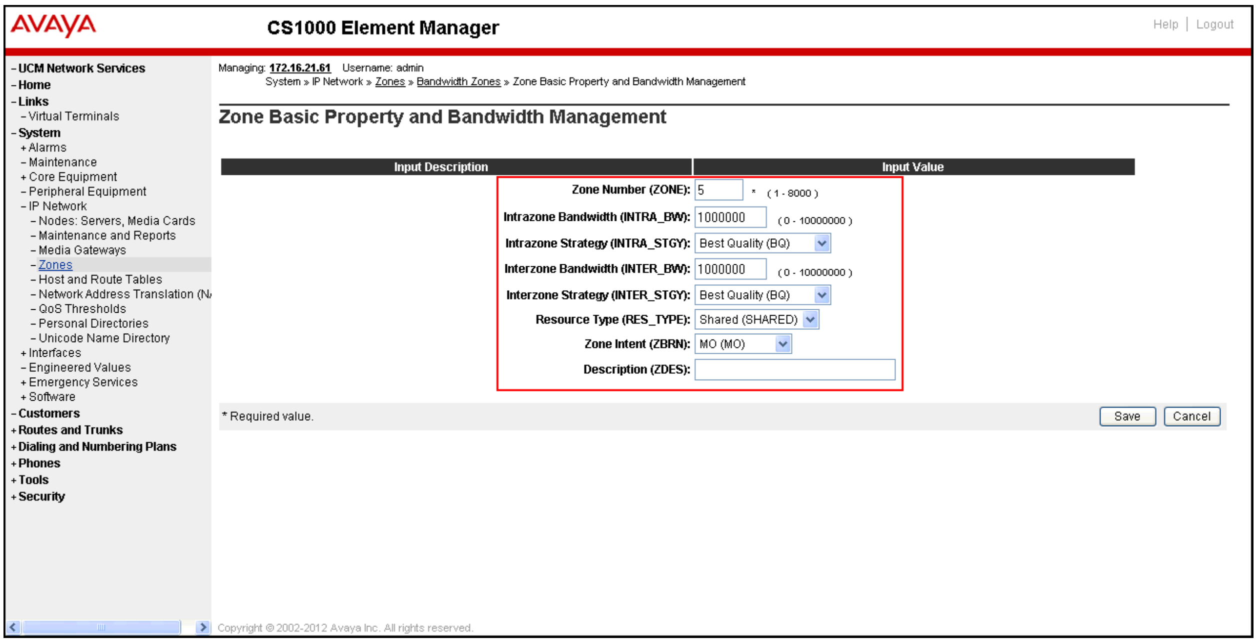


Click **Add** (not shown), select the values shown below and click on the **Save** button.

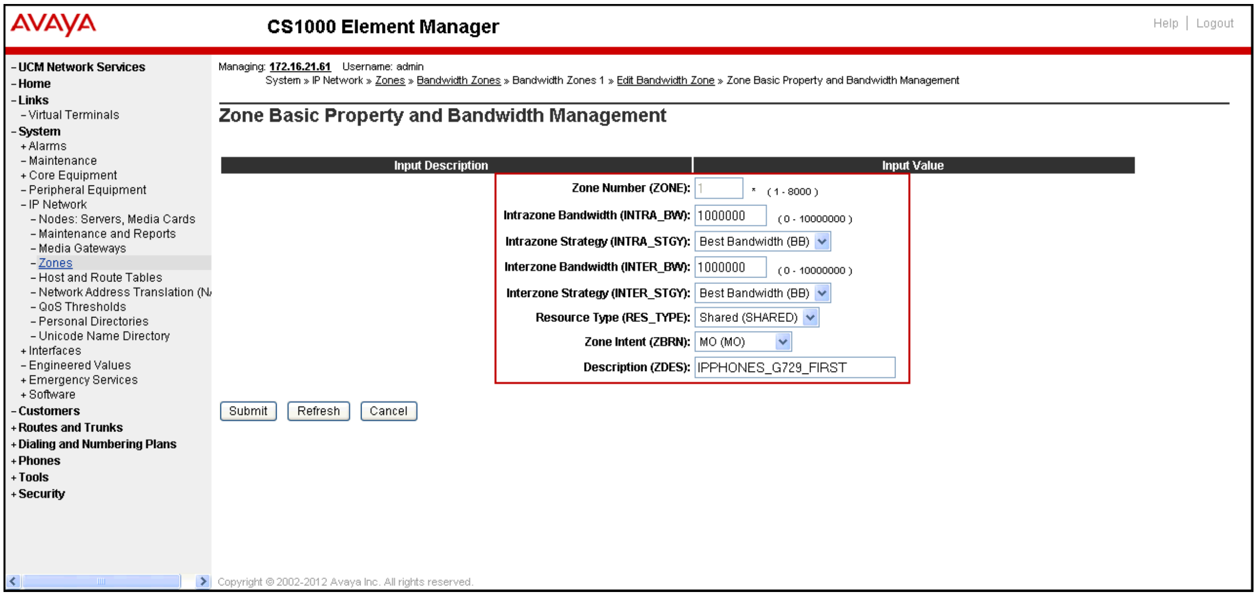
- **INTRA_STGY**: Bandwidth configuration for local calls, select **Best Quality (BQ).**
- **INTER_STGY**: Bandwidth configuration for calls over the trunk, select **Best Quality (BQ).**
- **ZBRN: Select MO** (**MO** is used for IP phones).

Note: BQ will use **G711** as first choice and **G729** as second choice. **BB**, or **Best Bandwidth**, will use **G729** as first choice and G711 as second choice.

The values for **Zone 5** are shown below; **G711** will be used as first choice and **G729** as second choice.

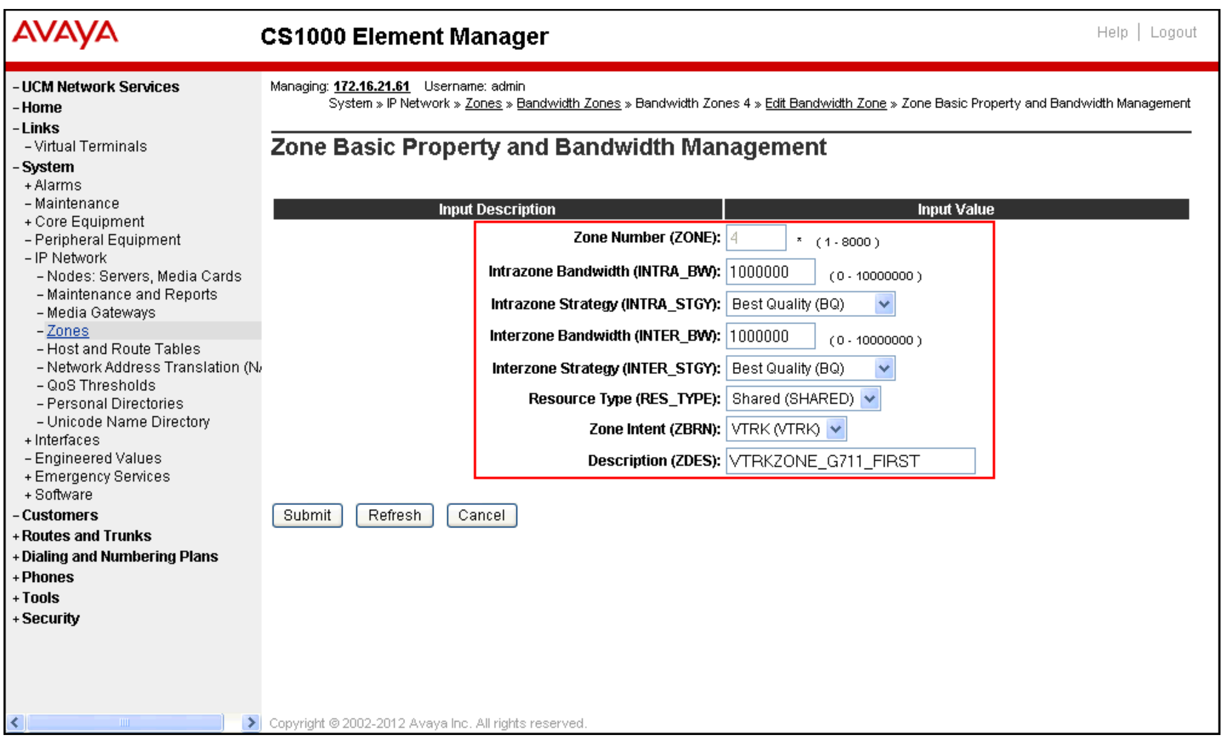


The values for **Zone 1** are shown below; **G729** will be used as first choice and **G711** as second choice.



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

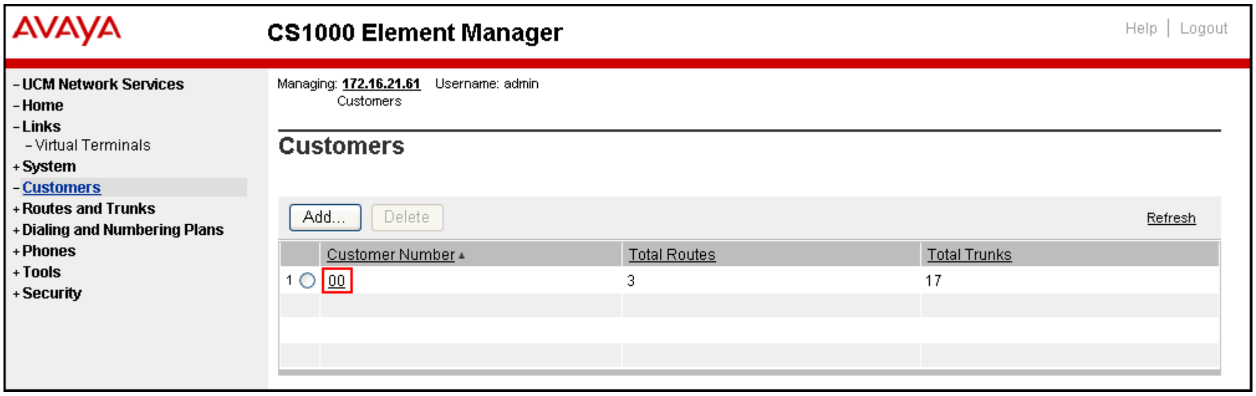
This section describes how to create a zone for the Virtual SIP Trunks. The difference is in the **Zone Intent (ZBRN)** field. For **ZBRN** select **VTRK** for virtual trunk and **Best Quality (BQ)** for both **INTRA_STGY** and **INTER_STGY** as shown below, and then click on the **Save** button. For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



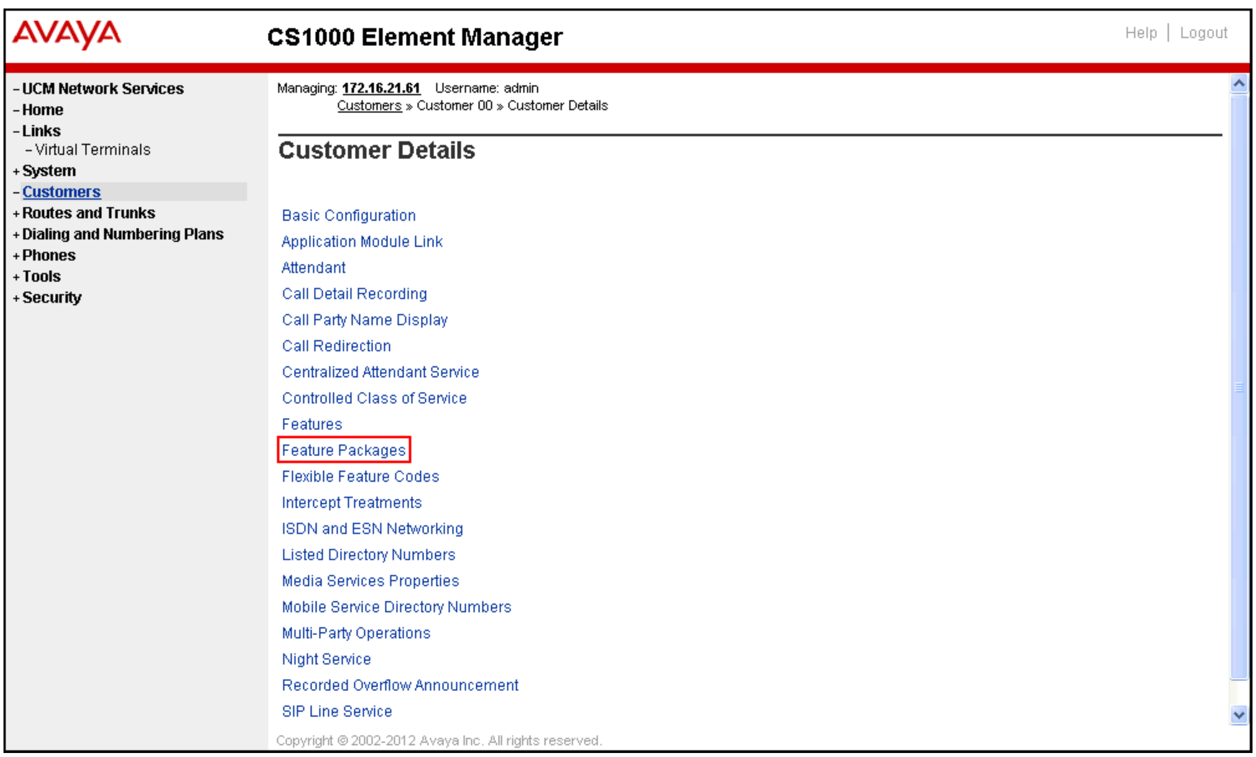
5.5. Administer SIP Trunk Gateway

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

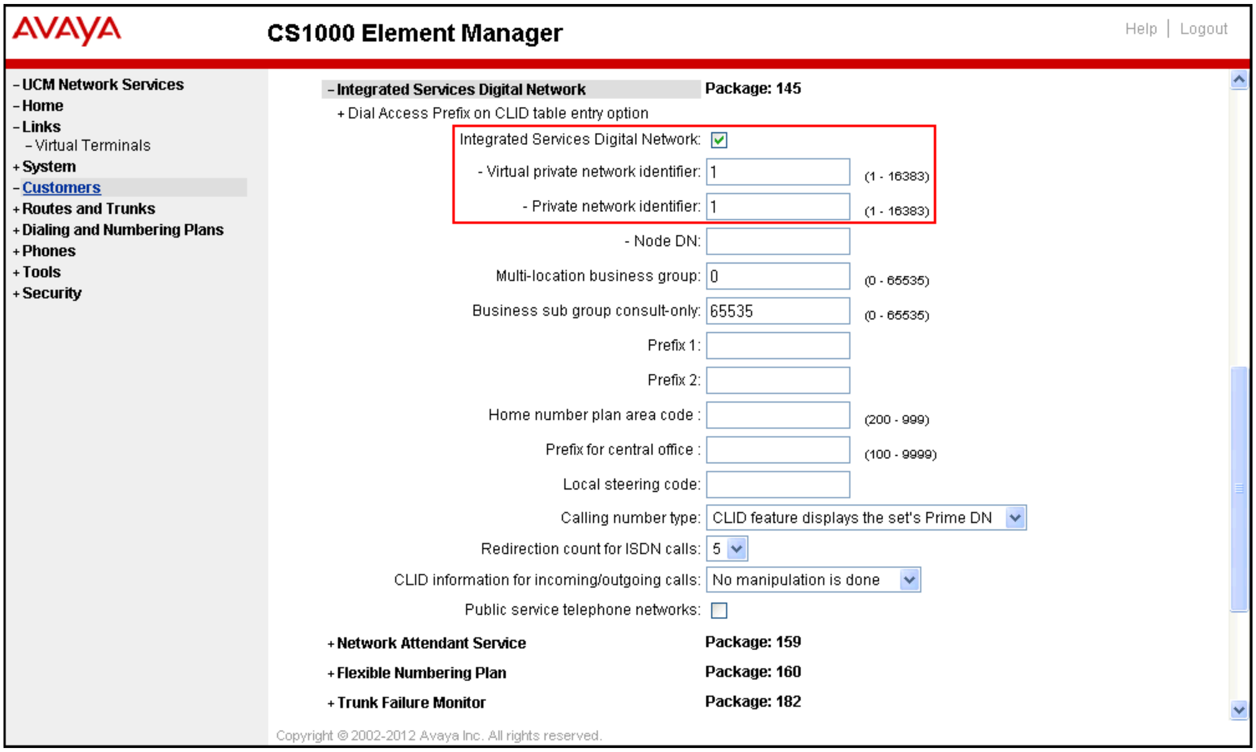
Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options.



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



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



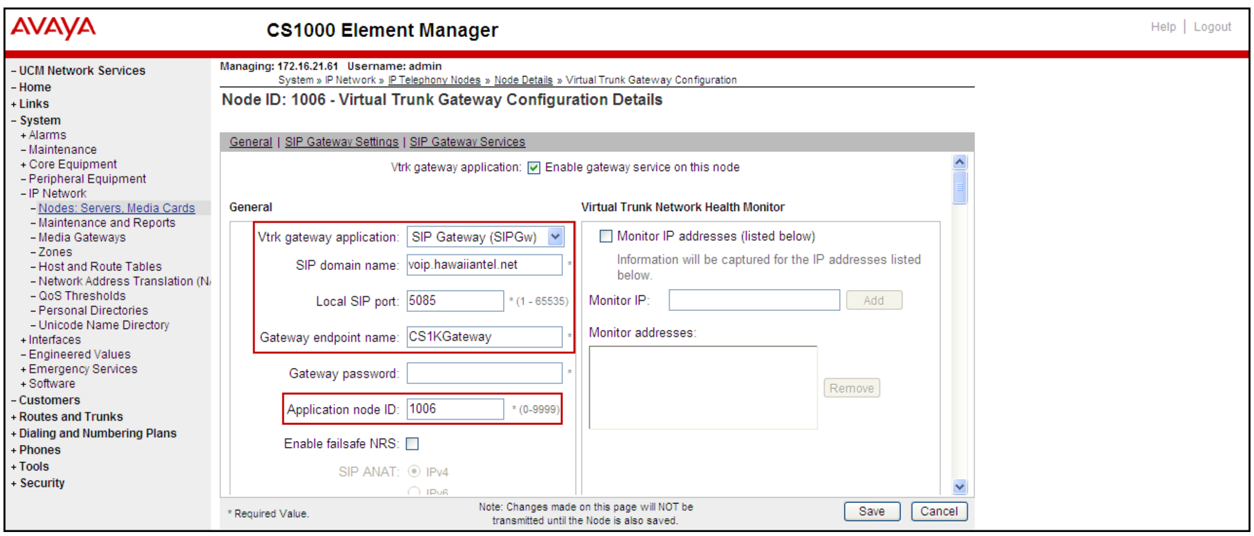
5.5.1. Administer the SIP Trunk Gateway to Session Manager

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

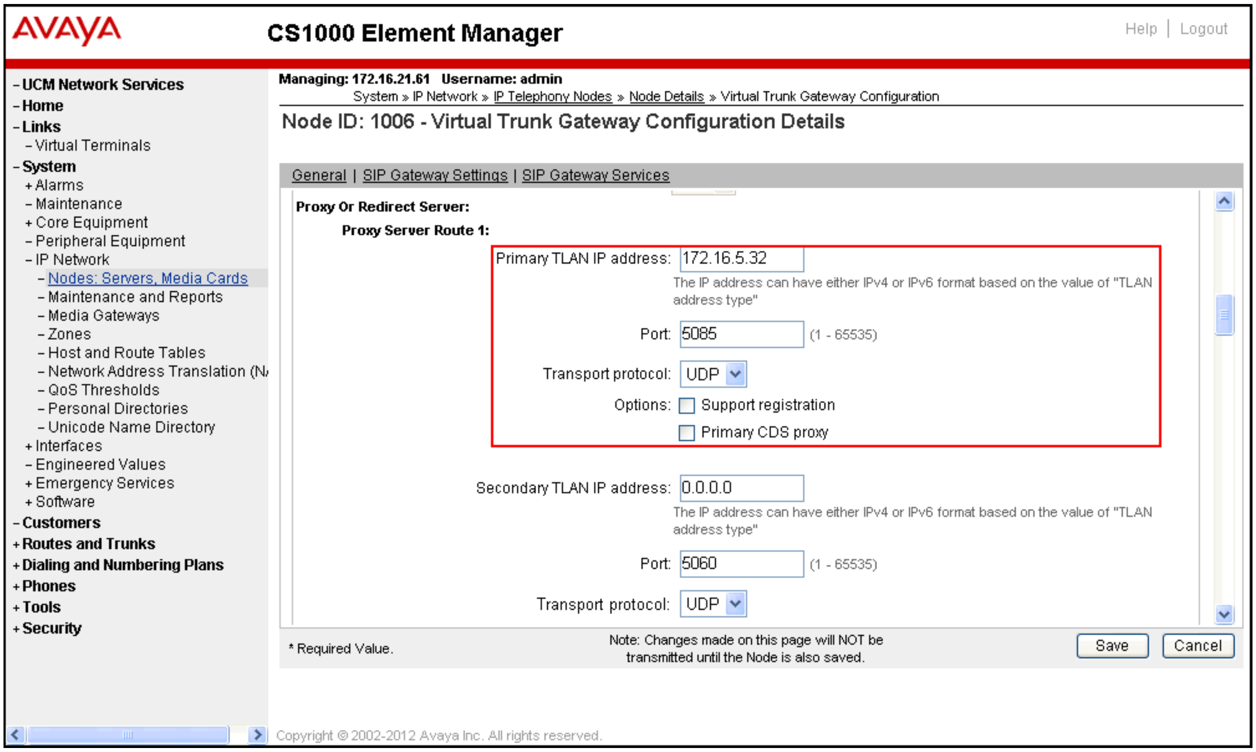
On the **Node Details** screen, select **Gateway (SIPGw)** (not shown).

Under 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 for the SIP Entity Link in Session Manager (these are shown in **Section 6.6**).

- **Vtrk gateway application**: SIP Gateway (SIPGw).
- **SIP domain name**: voip.hawaiiantel.net
- **Local SIP port**: 5085.
- **Gateway endpoint name**: CS1KGateway.
- **Application node ID**: 1006.



Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in the red box) for the specified fields, and retain the default values for the remaining fields as shown below.



On the same page shown above, scroll down to the **SIP URI Map** section.
Under the **Public E.164 Domain Names**, for:

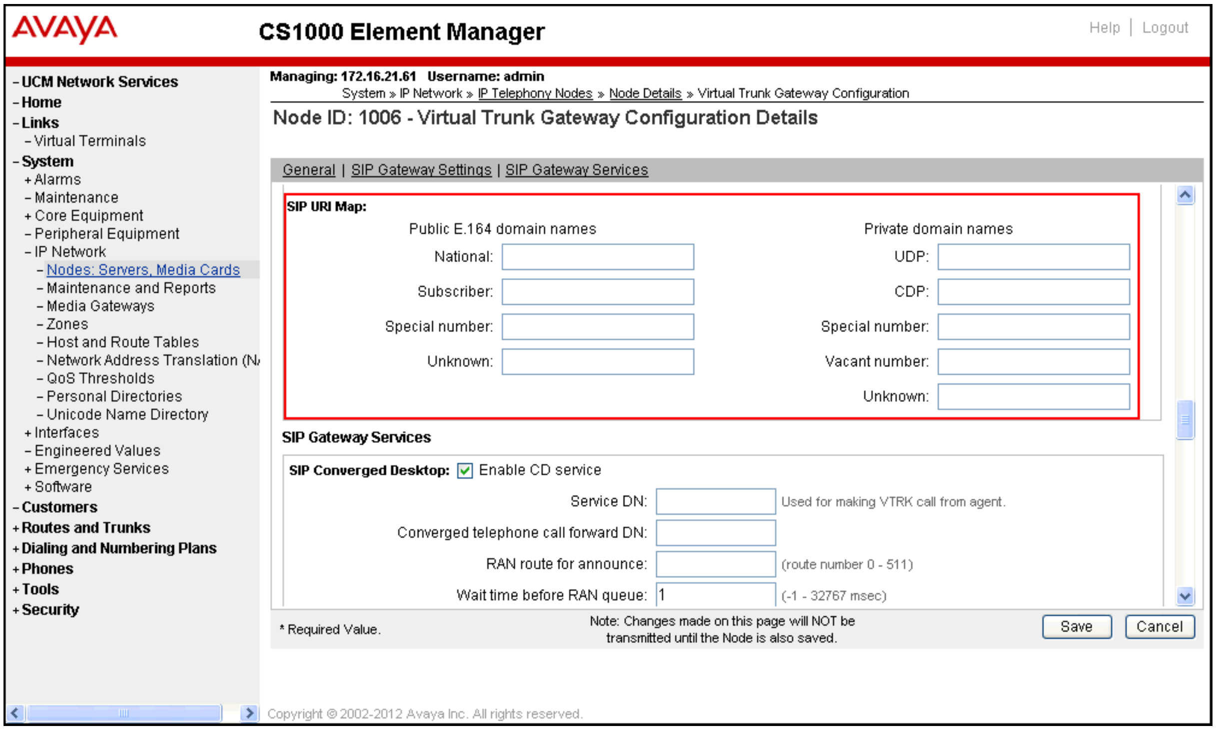
- **National**: leave this SIP URI field as blank.
- **Subscriber**: leave this SIP URI field as blank.
- **Special Number**: leave this SIP URI field as blank.
- **Unknown**: leave this SIP URI field as blank.

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

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

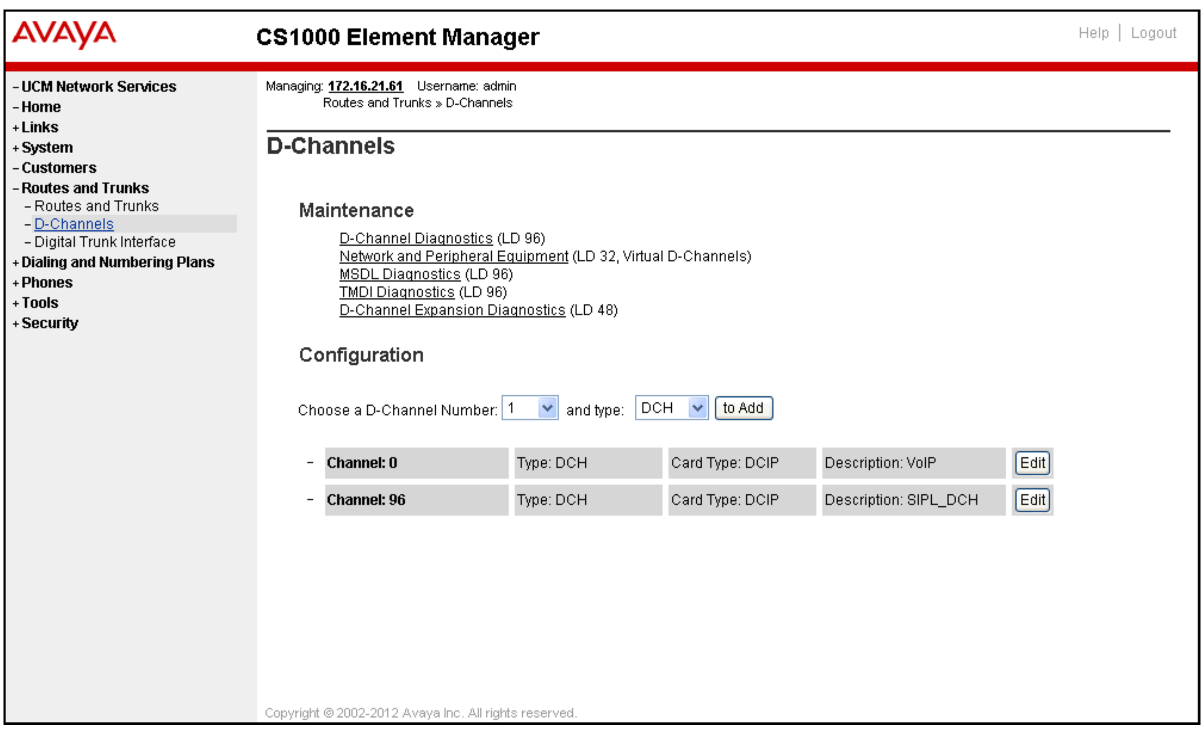
Note: These fields are shown with no entries (blank) for the Avaya DevConnect lab configuration; it is possible that customer installations may have domain names configured here.

Then click on the **Save** button.



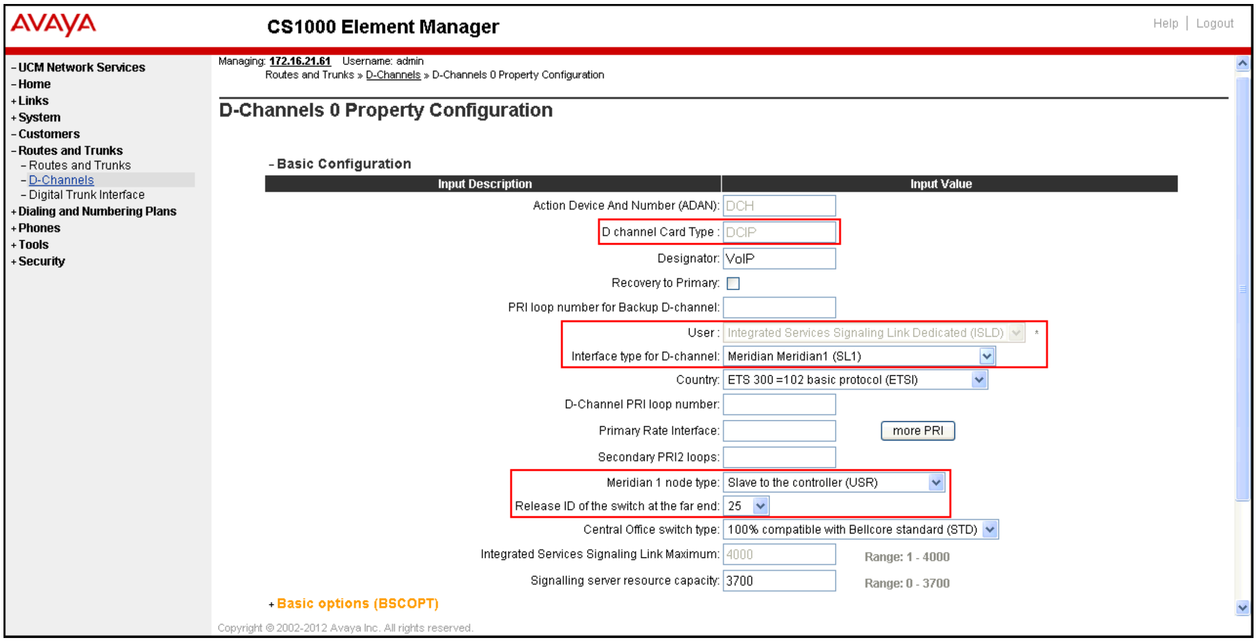
5.5.2. Administer Virtual D-Channel

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



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

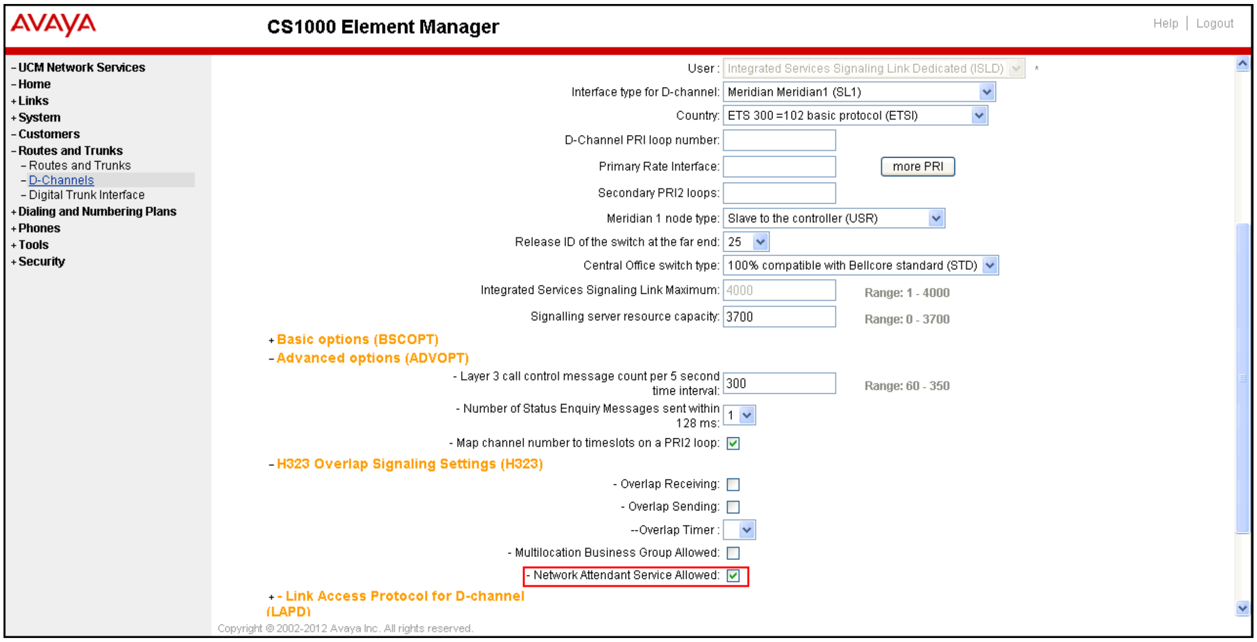
- **D channel Card Type (CTYP):** D-Channel is over IP (DCIP).
- **Designator (DES)**: A descriptive name.
- **Interface type for D-channel (IFC):** Meridian Meridian1 (SL1).
- **Meridian 1 node type:** Slave to the controller (USR).
- **Release ID of the switch at the far end (RLS):** 25.



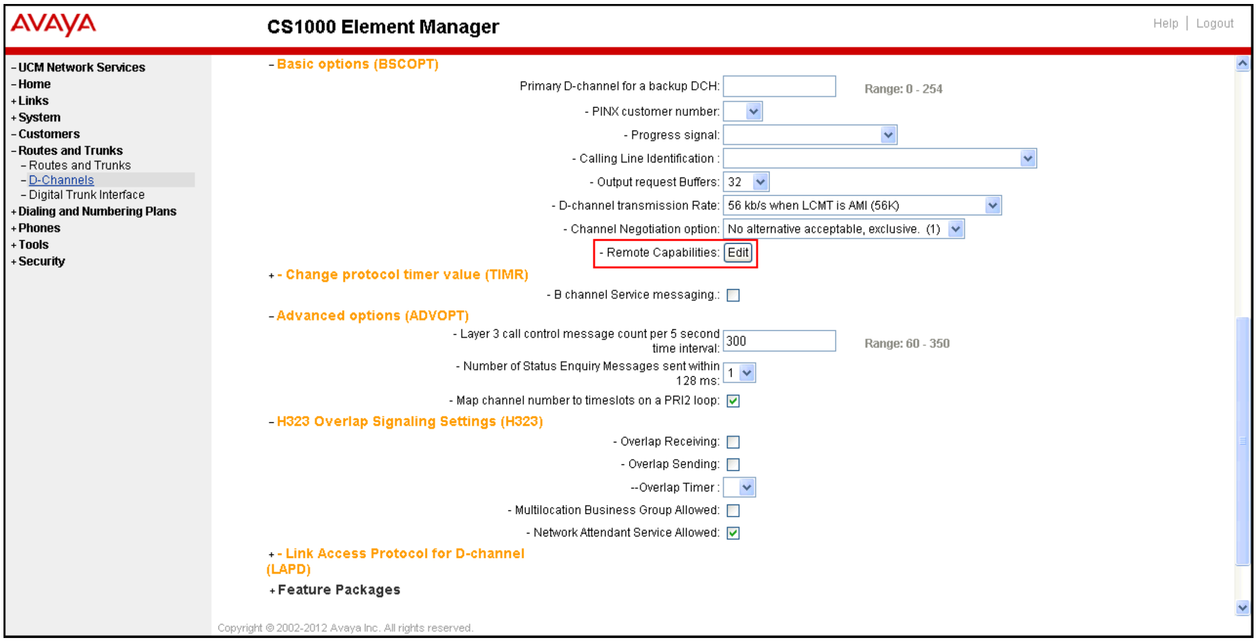
On the same page scroll down and enter the following values for the specified fields:

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

Retain the default values for the remaining fields.

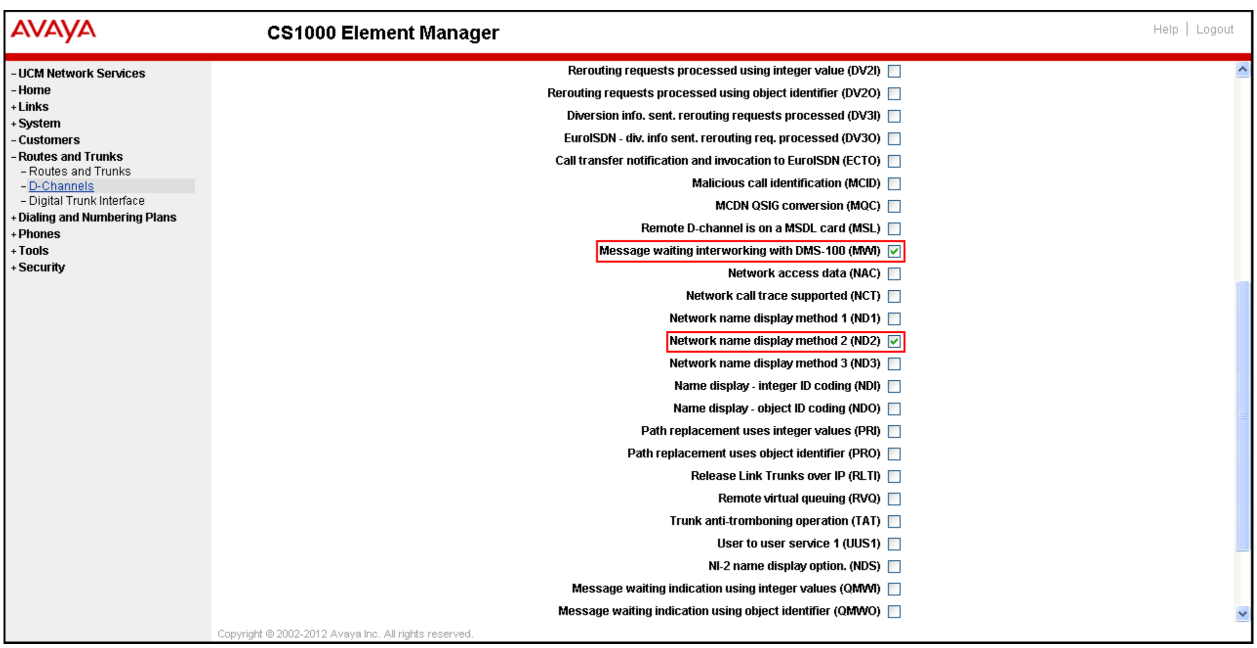


Click on **Basic Options (BSCOPT)** and click on the **Edit** button for the **Remote Capabilities** attribute as shown below.



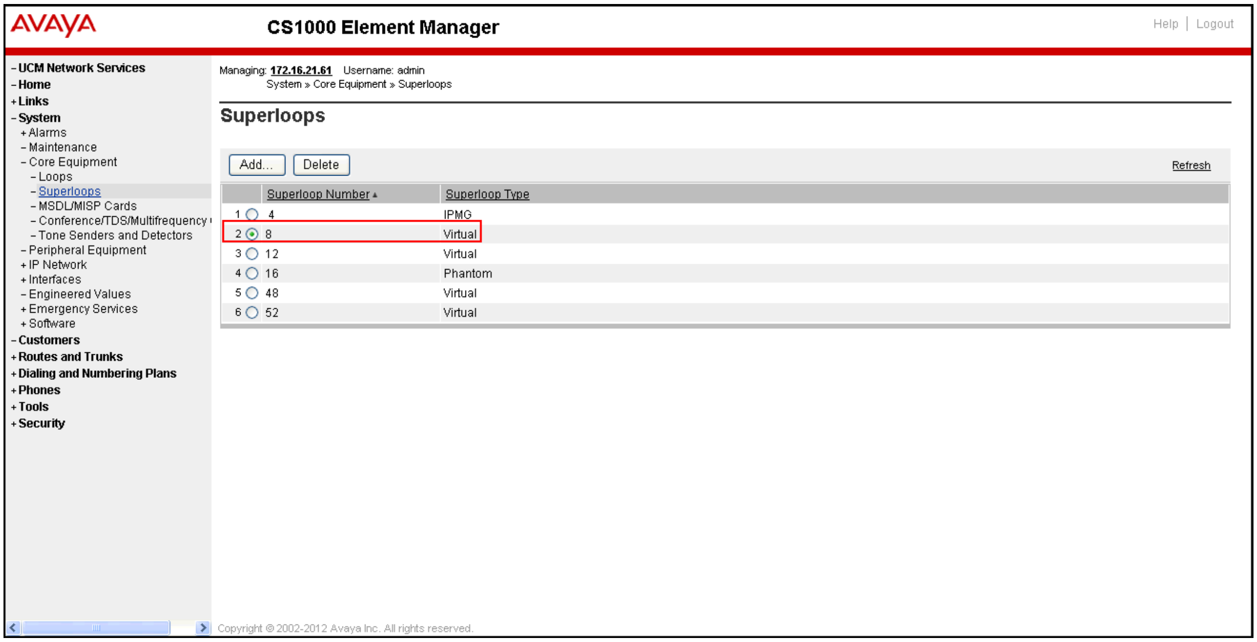
The **Remote Capabilities Configuration** page will appear. Then check **ND2** and **MWI** (if mailboxes are present on the CS1K Call Pilot) checkboxes as shown below.

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



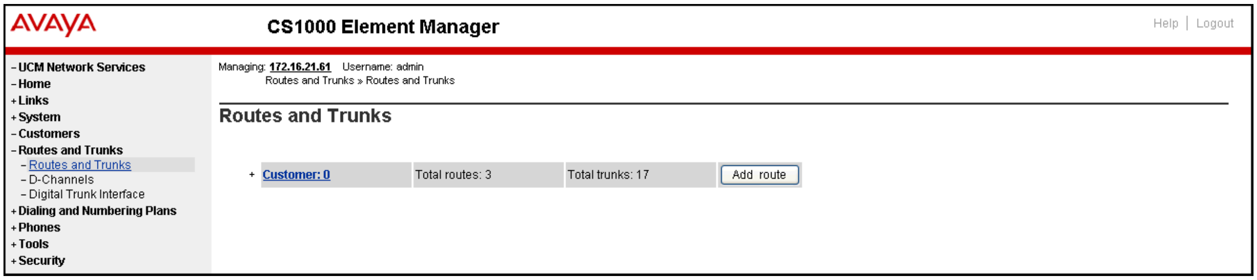
5.5.3. Administer Virtual Super-Loop

Select **System → Core 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.



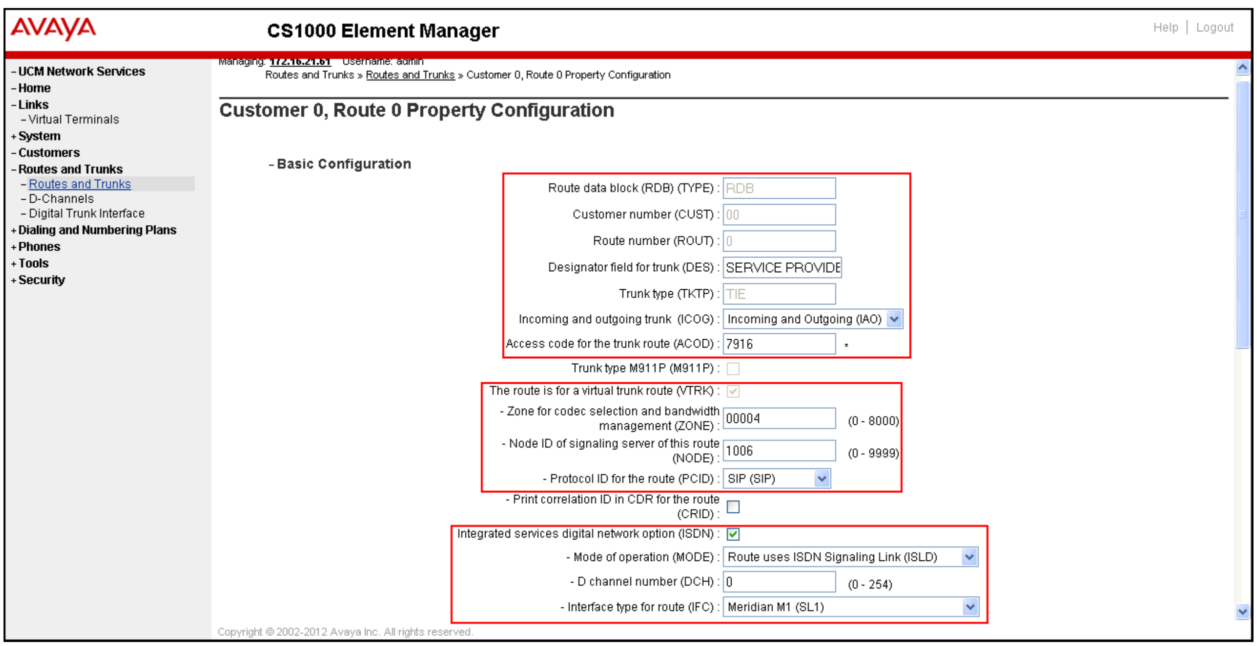
5.5.4. Administer Virtual SIP Routes

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.

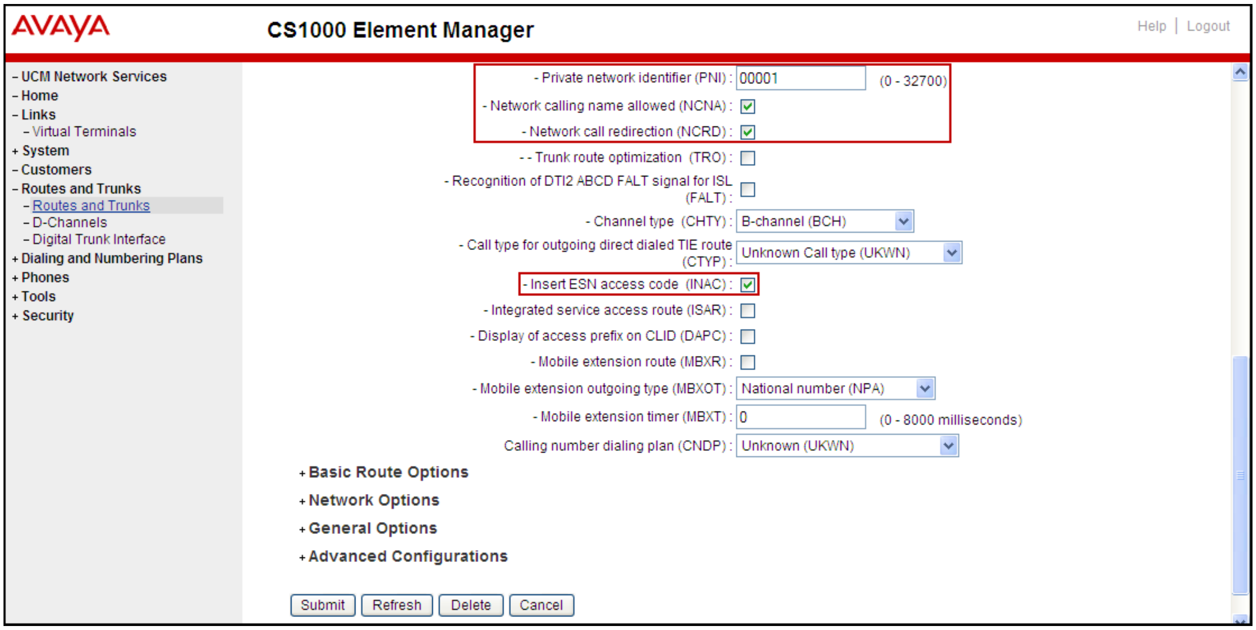


The **Customer 0**, **Route 0 Property Configuration** screen is displayed next. Scroll down until the **Basic Configuration** Section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown below.

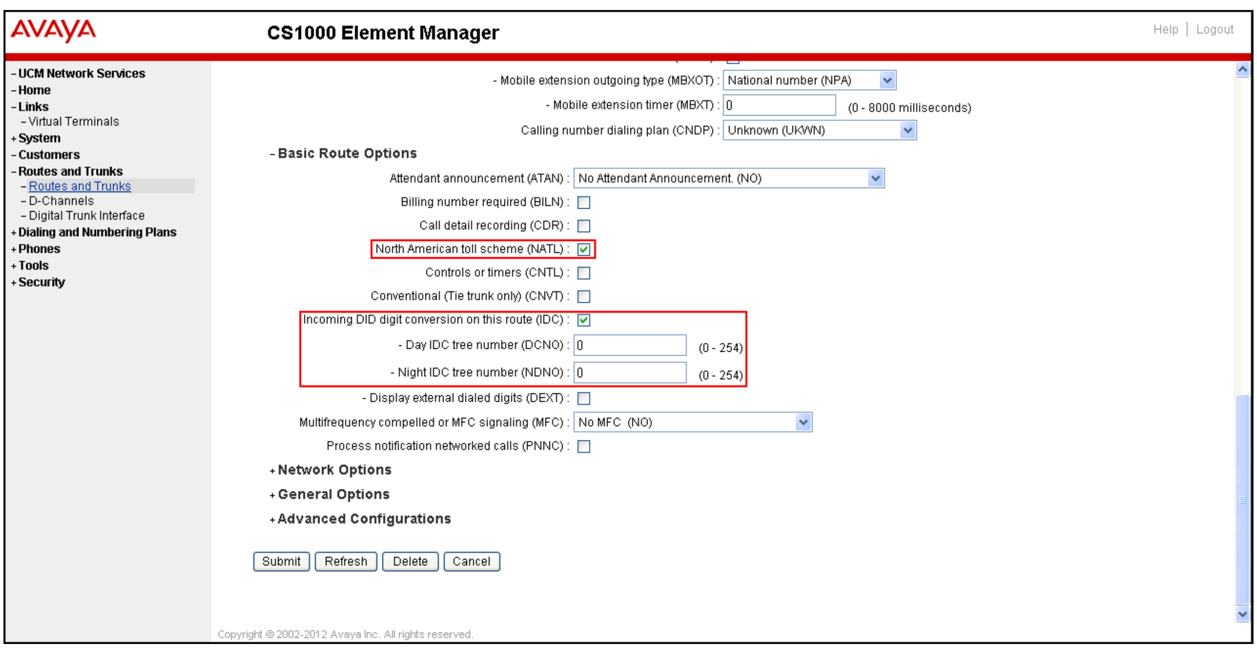
- **Route Number (ROUT)**: Select an available route number.
- **Designator field for trunk (DES)**: A descriptive text.
- **Trunk Type (TKTP)**: **TIE trunk data block (TIE).**
- **Incoming and Outgoing trunk** (**ICOG**): **Incoming and Outgoing (IAO).**
- **Access Code for the trunk route (ACOD)**: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



- **Network calling name allowed (NCNA)**: Check box.
- **Network call redirection (NCRD)**: Check box.
- **Insert ESN access code (INAC):** Check box.

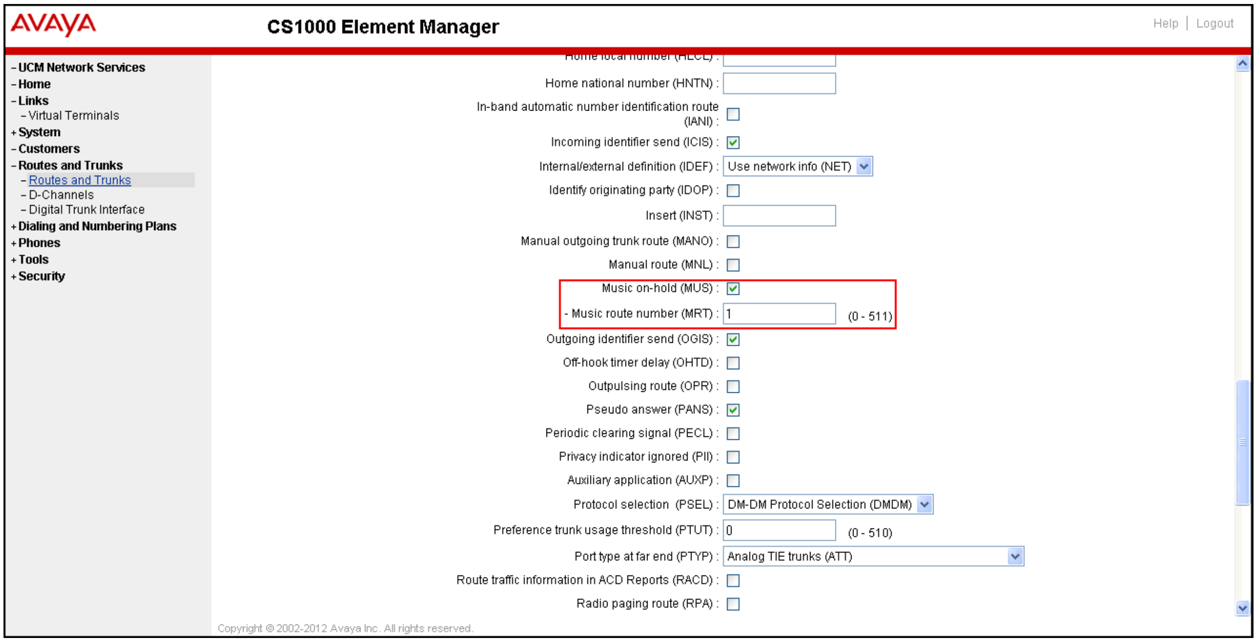


- In **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **0** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown below. The IDC is discussed in **Section** Error! Reference source not found..



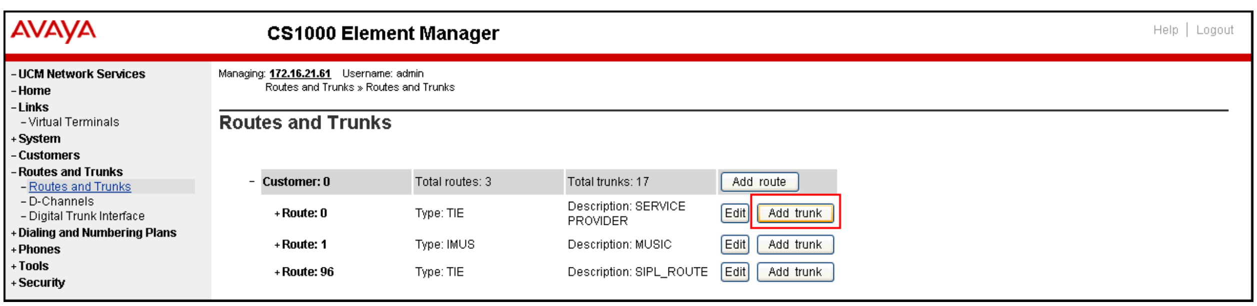
- In **Advance Configurations** (not shown); check **Music-on-hold** to enable music on hold on the route. Input **Music route number 1** in the box as shown below. The CS1000 system is pre-configured with route 1 as a music route.

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



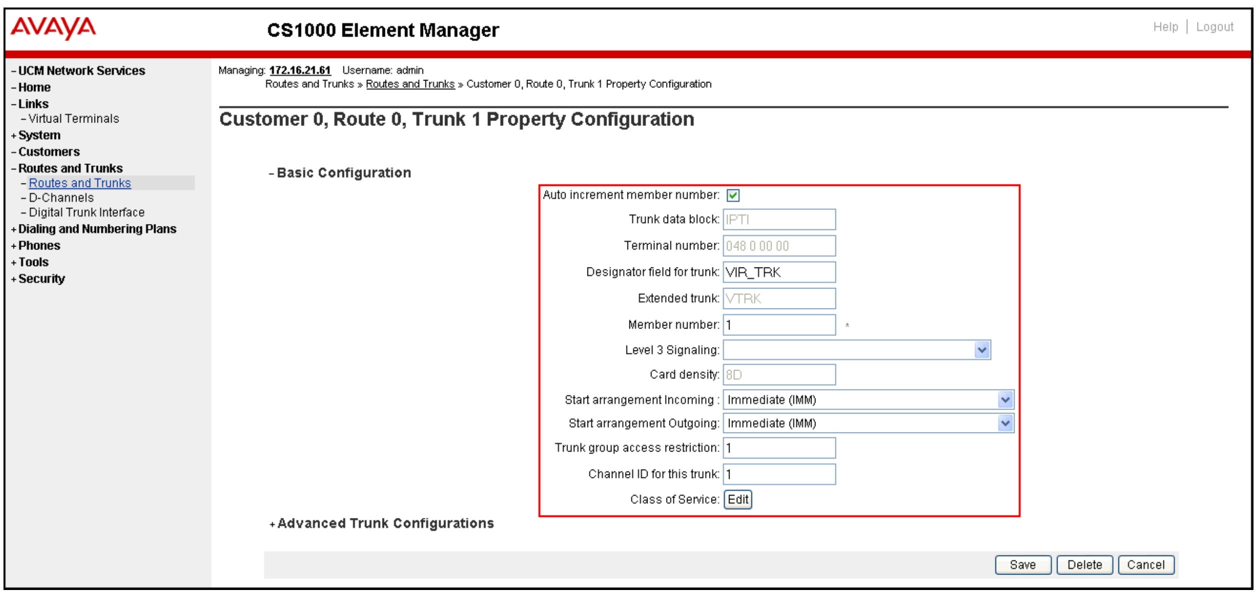
5.5.5. Administer Virtual Trunks

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

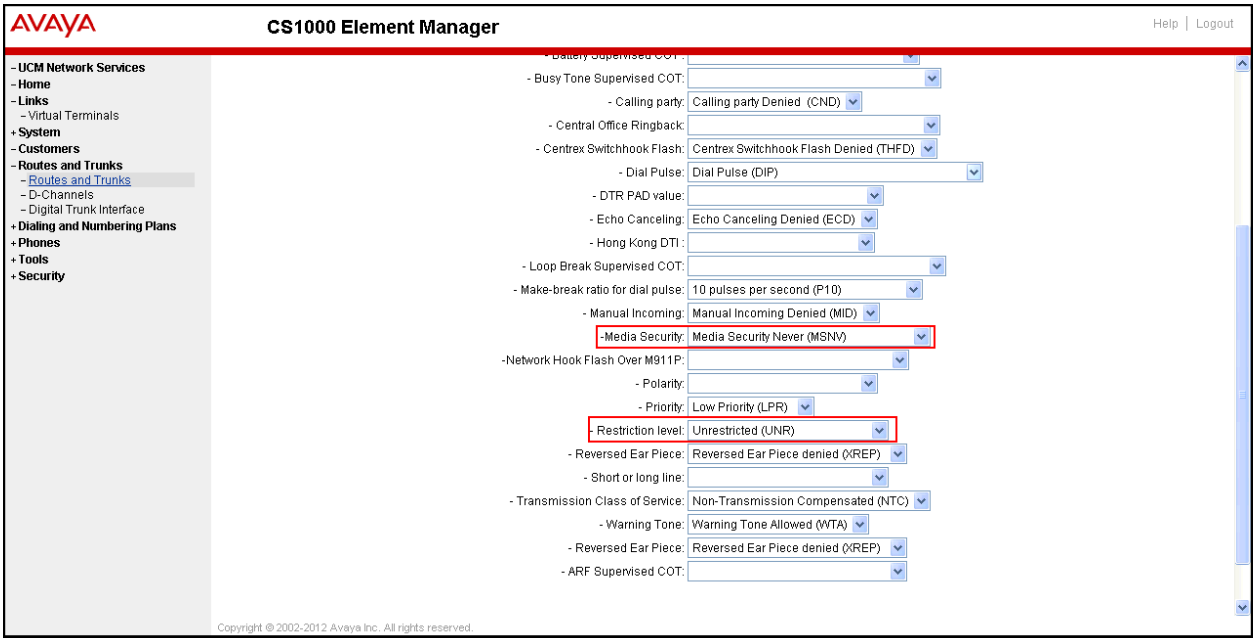


The **Customer 0, Route 0, Trunk 1 Property Configuration** screen is displayed as shown below. Enter the following values for the specified fields and retain default values for the remaining fields. The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service (CLS)**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

- 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 (created in **Section 5.5.3**).
- **Designator field for trunk** (**DES**): A descriptive text.
- **Extended Trunk (XTRK): Virtual trunk (VTRK).**
- **Member number** (**RTMB**): Current route number and starting member.
- **Start arrangement Incoming** (**STRI**): **Immediate (IMM).**
- **Start arrangement Outgoing (STRO)**: **Immediate (IMM).**
- **Trunk Group Access Restriction (TGAR)**: Desired trunk group access restriction level.
- **Channel ID for this trunk** (**CHID**): An available starting channel ID.

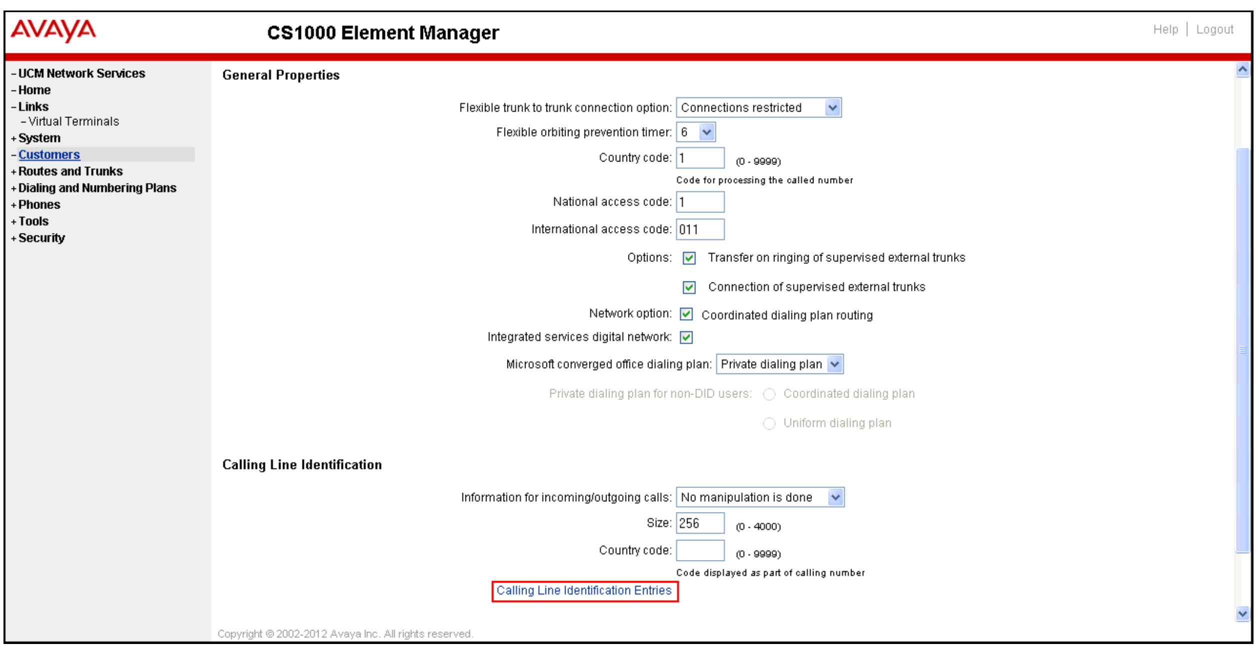


Click on **Edit Class of Service** (shown on previous screen), For **Media Security** select **Media Security Never** (**MSNV**)**,** for **Restriction Level** select **Unrestricted (UNR)**. Use default for remaining values. Scroll down to the bottom of the screen and click **Return Class of Service**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

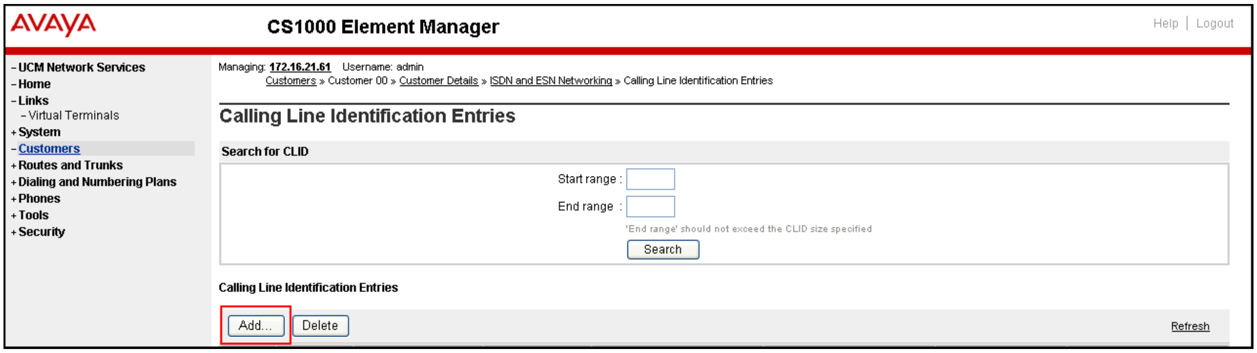


5.5.6. Administer Calling Line Identification Entries

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



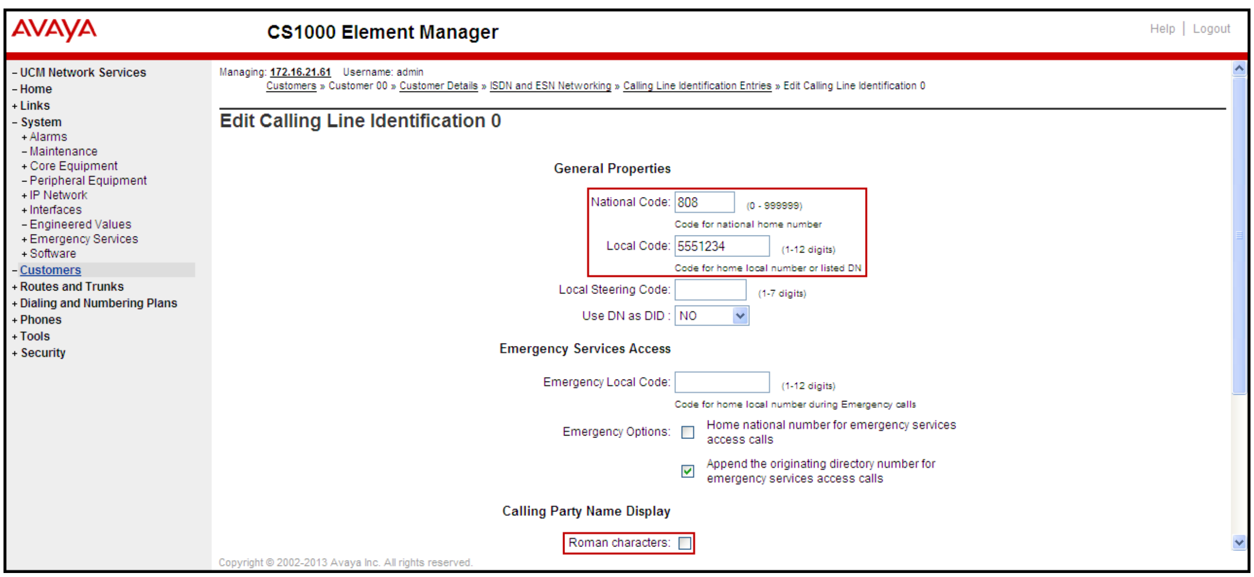
Click on **Add** as shown below.



Add entry **0** as shown below.

- **National Code**: Input the three digit area code prefix of the DID number assigned by the service provider, in this case **808**.
- **Local Code**: input the seven digit number of the DID assigned by Service Provider, in this case it is **5551234**.
- **Calling Party Name Display**: Uncheck the **Roman characters** box.

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



5.5.7. Enable External Trunk to Trunk Transferring

This section shows how to enable the External Trunk to Trunk Transferring feature which is a mandatory configuration to make call transfers and conferences 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**.

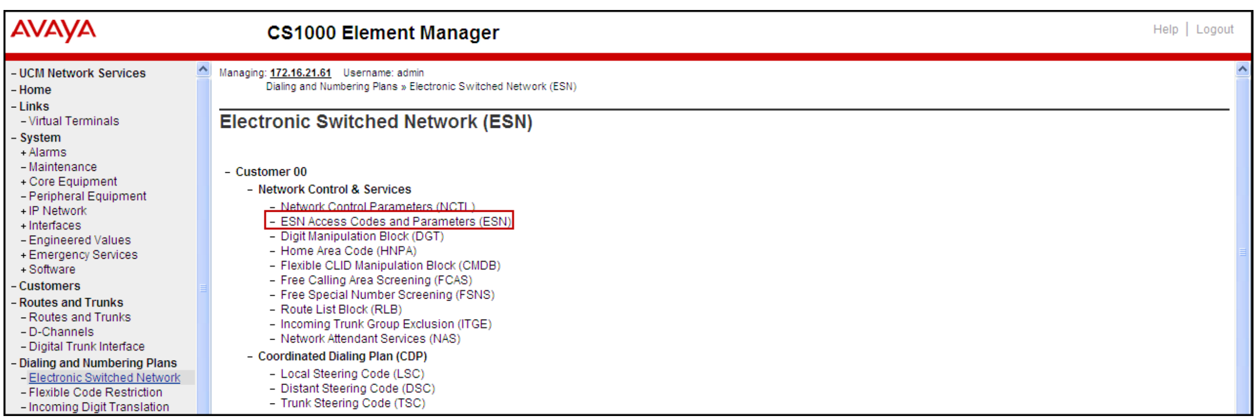
```
>ld 15 CDB000
MEM AVAIL: (U/P): 43552101    USED U P: 371282 939078    TOT: 44862461
DISK SPACE NEEDED: 1713 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
....
TRNX yes
EXTT yes
....
```

5.6. Administer Dialing Plans

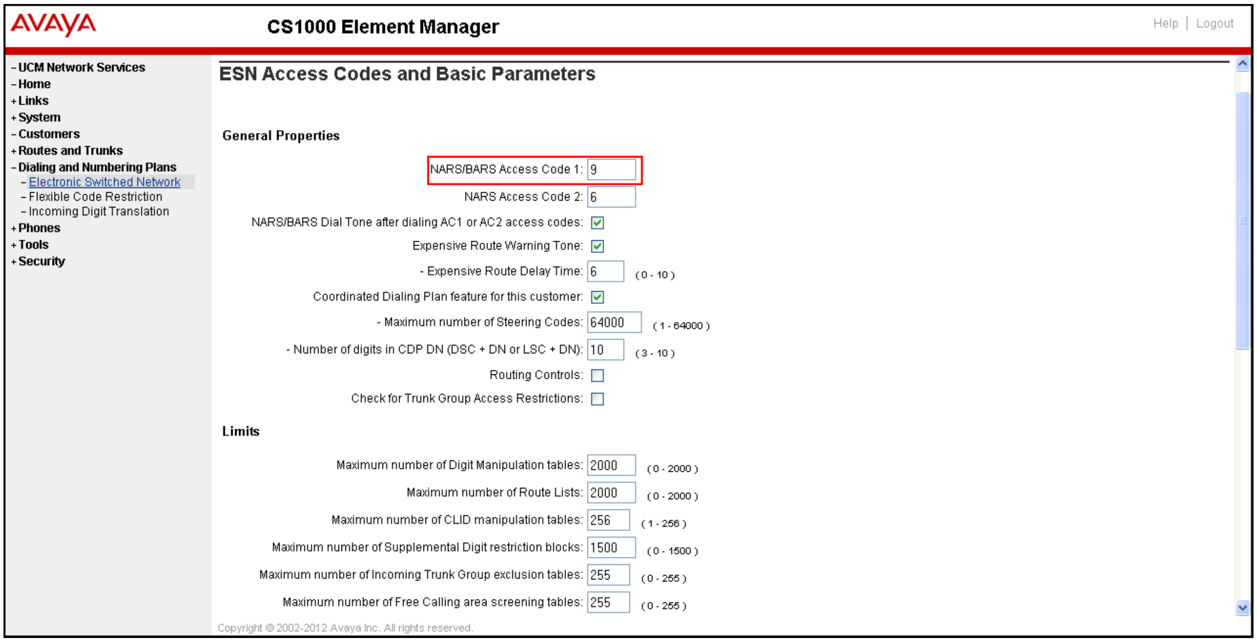
This section describes how to administer dialing plans on the CS1000.

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).



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

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

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

Verify Customer Net_Data Block by using **LD 21**

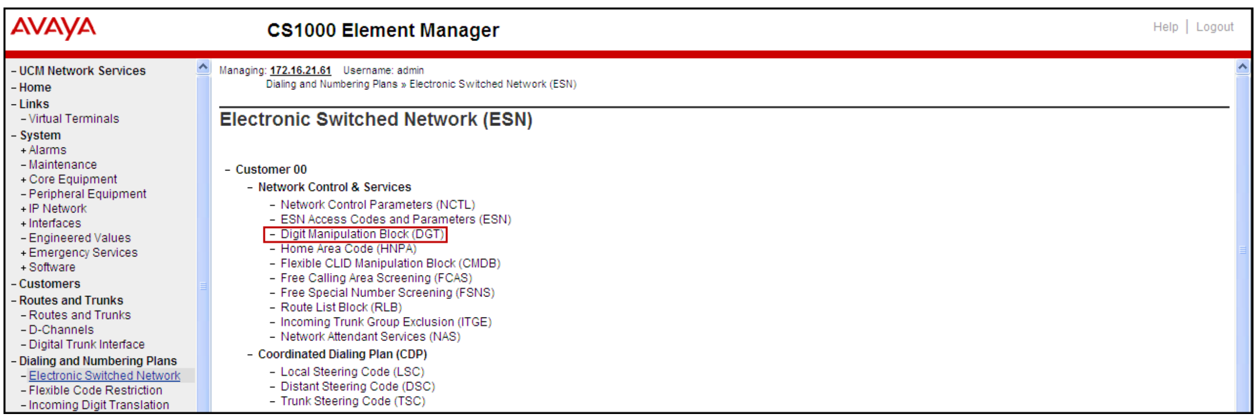
```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

5.6.3. Digit Manipulation Block Index (DMI)

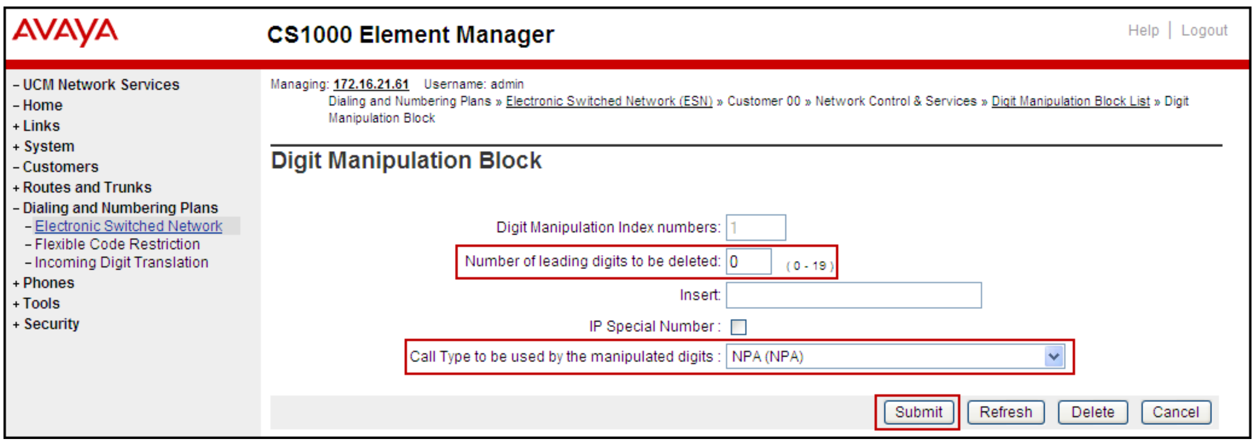
Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Digit Manipulation Block (DGT)** as shown below.



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

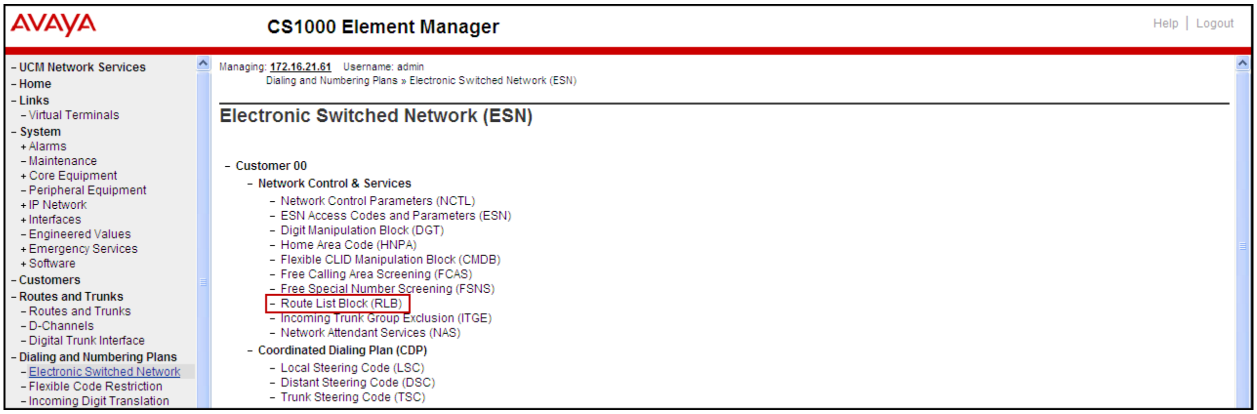
In the example shown below **Digit Manipulation Block Index 1** was previously added.

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



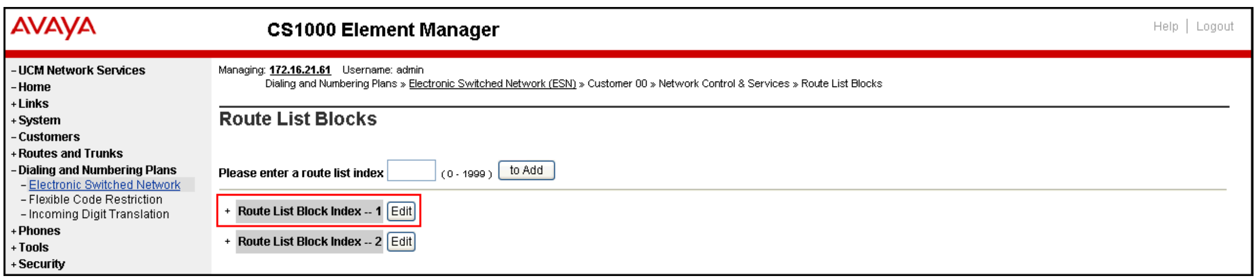
5.6.4. Route List Block (RLB)

This section shows how to add a RLB associated with the DMI created in **Section 5.6.3.** Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)** as shown below.



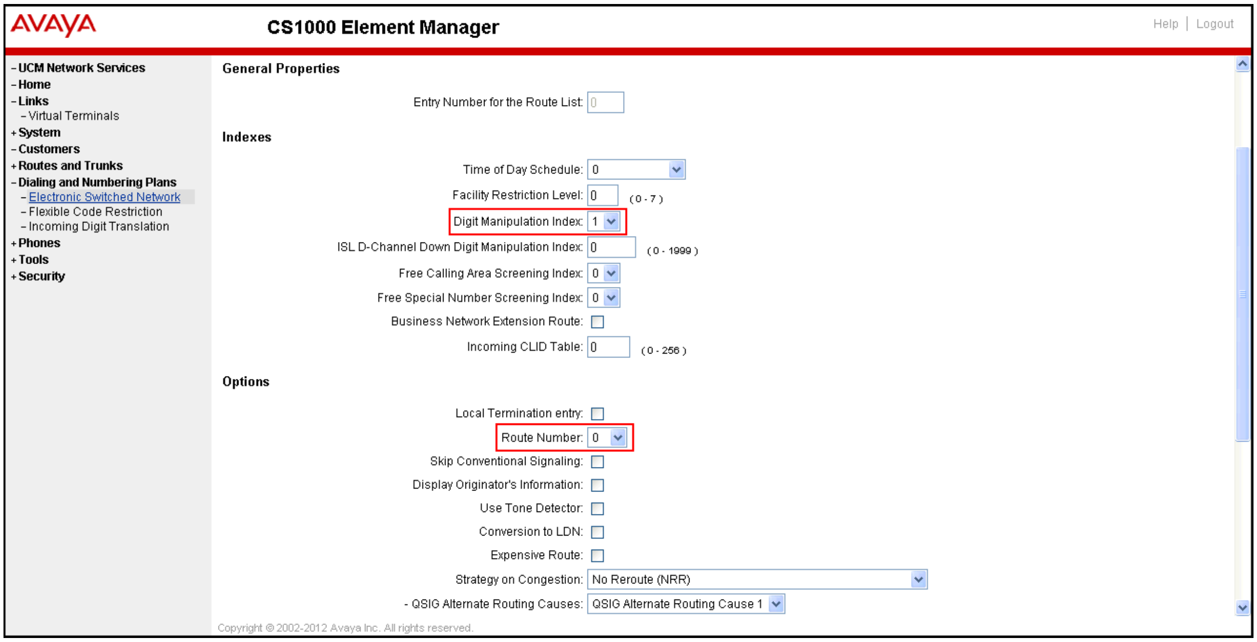
Select an available value in the **Please enter a route list index** field and click on the "**to Add"** button as shown below.

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



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

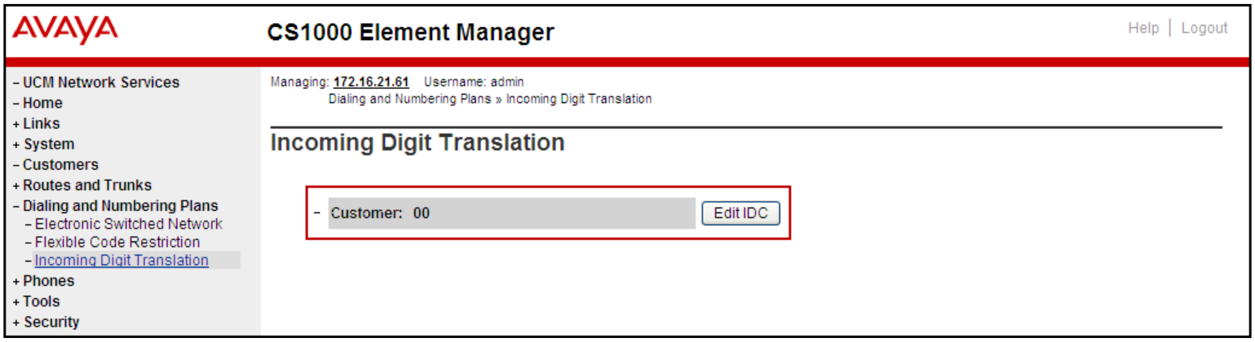
- **Digit Manipulation Index** (DMI): **1** (created in **Section 5.6.3**).
- **Route number** (ROUT): **0** (created in **Section 5.5.4**).



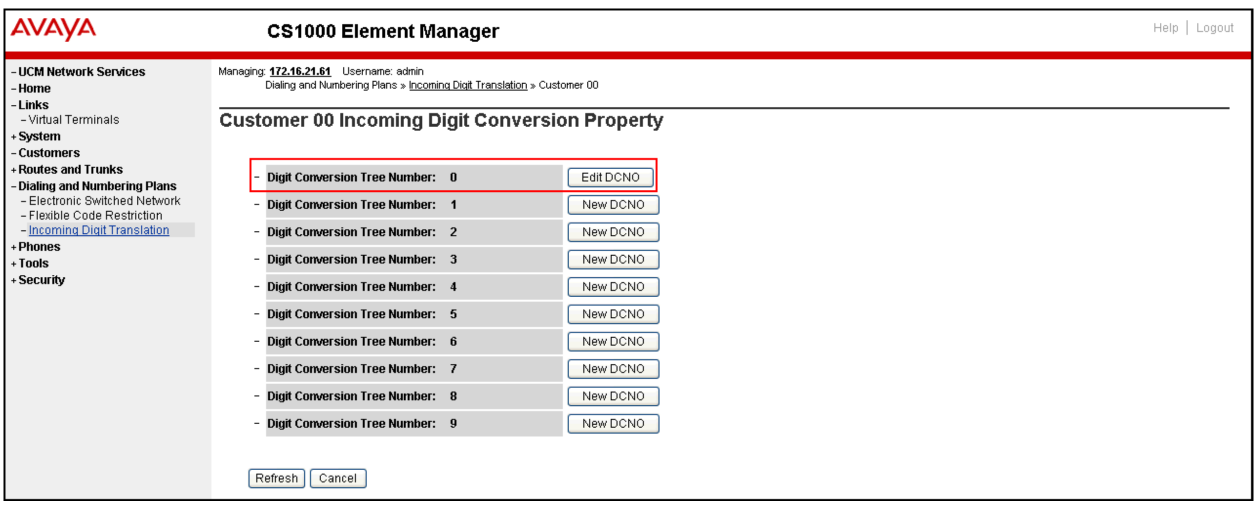
5.6.5. Inbound Call Digit Translation

This section describes the steps for receiving calls from the PSTN via Hawaiian Telecom's network.

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.

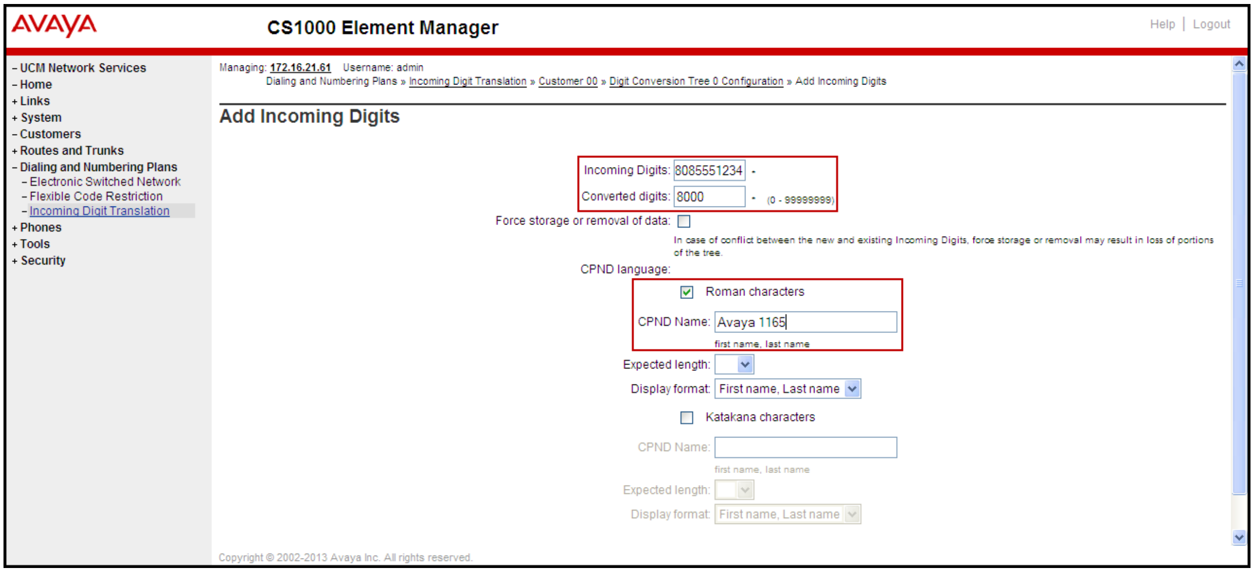


Click on **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number (DCN0) 0** was created as shown below.



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

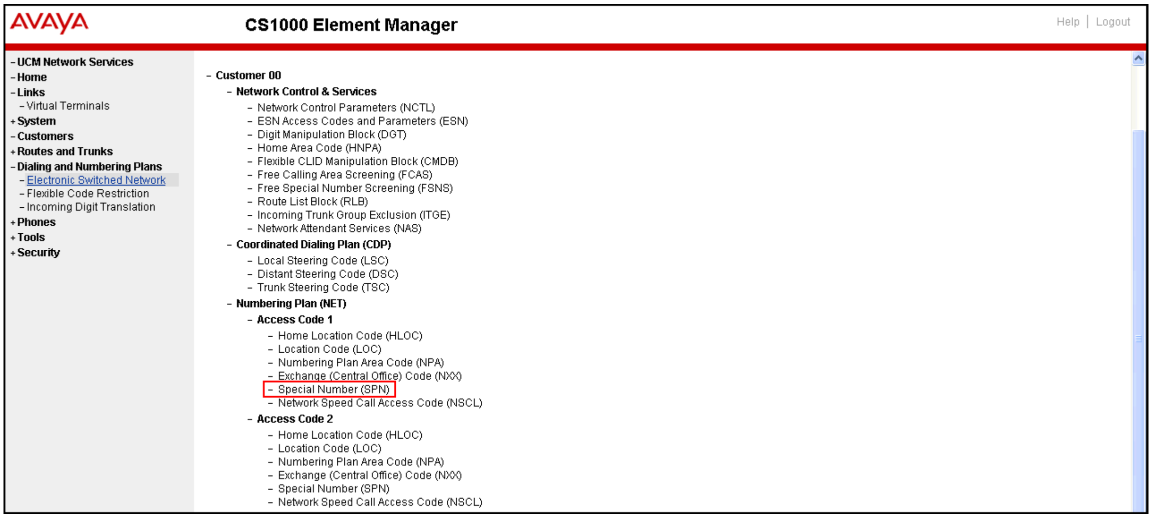
In the following configuration, the incoming call from PSTN with the prefix **8085551234** will be translated to the CS1000 extension number **8000**.



5.6.6. Outbound Call - Special Number Configuration.

There are special numbers which are configured to be used for this testing such as **0** to reach 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**, **911, 711** and so on. Calls to special numbers shown here are for reference only and may not have been tested for various reasons. Refer to **Items not supported or not tested** in **Section 2.2.**

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen. Select **Special Number (SPN)** as shown 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: 0** (flexible, unlimited and accept the character # to ending dial number).
- **CallType**: **NATL**.
- **Route list index**: **1**, created in **Section 5.6.4.**

Special Number: 411

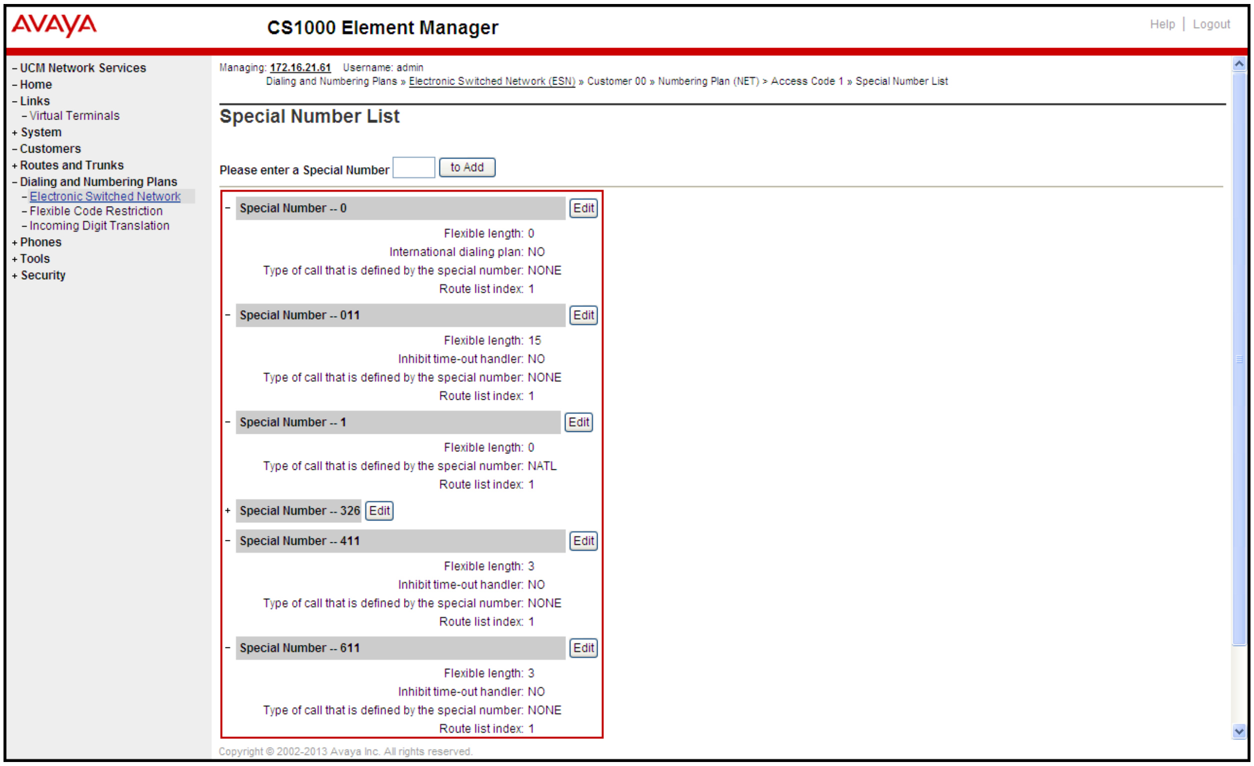
- **Flexible length**: **3**.
- **CallType**: None.
- **Route list index**: **1**, created in **Section 5.6.4.**

Special Number: 711

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

Special Number: 911

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



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

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

5.7. Administer Phone

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

5.7.1. Phone creation

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

For CS1000 FAX over IP Support recommendation refer to the Avaya Product Support Notice (PSN) referred to in **Section 11** [16], including the **Analog Station provisioning for T.38** section and **Minimum Vintage Loadware Recommendation** for MGC.

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

```
REQ: prt
TYPE: 1110
TN
CUST
TEN
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES  8001
TN   008 0 00 01  VIRTUAL
TYPE 1110
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00005
CUR_ZONE 00005
MRT
ERL  0
ECL  0
FDN
TGAR 0
LDN  NO
NCOS 5
SGRP 0
RNPG 0
SCI  0
SSU
XLST
SCPW
SFLT NO
CAC_CIS 0
CAC_MFC 0
CLS  UNR FBA WTA LPR MTD FNA HTA TDD CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBD
     ICDA CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA 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
     MSNV FRA  PKCH MWTD DVLD CROD ELCD
CPND_LANG ENG
RCO  0
EFD
HUNT
EHT
LHK  0
PLEV 02
PUID
UPWD
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 SCR 8001 1     MARP
        CPND
          CPND_LANG ROMAN
            NAME Avaya, 1110_Uni
            XPLN 14
            DISPLAY_FMT FIRST,LAST
        ANIE 0
     01
     02
     03
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16 MWK 8056
     17 TRN
     18 AO6
     19 CFW 12
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
     27
```

5.7.2. Enable Privacy for Phone

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

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

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

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

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

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

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

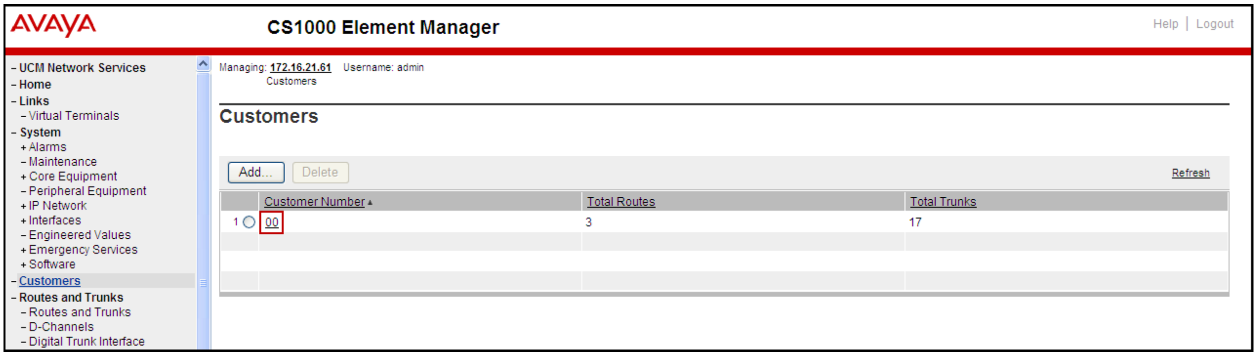
To allow display name and number, set CLS to **nama, ddga**. The CS1000 will send header "Privacy:none" to Service Provider.

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

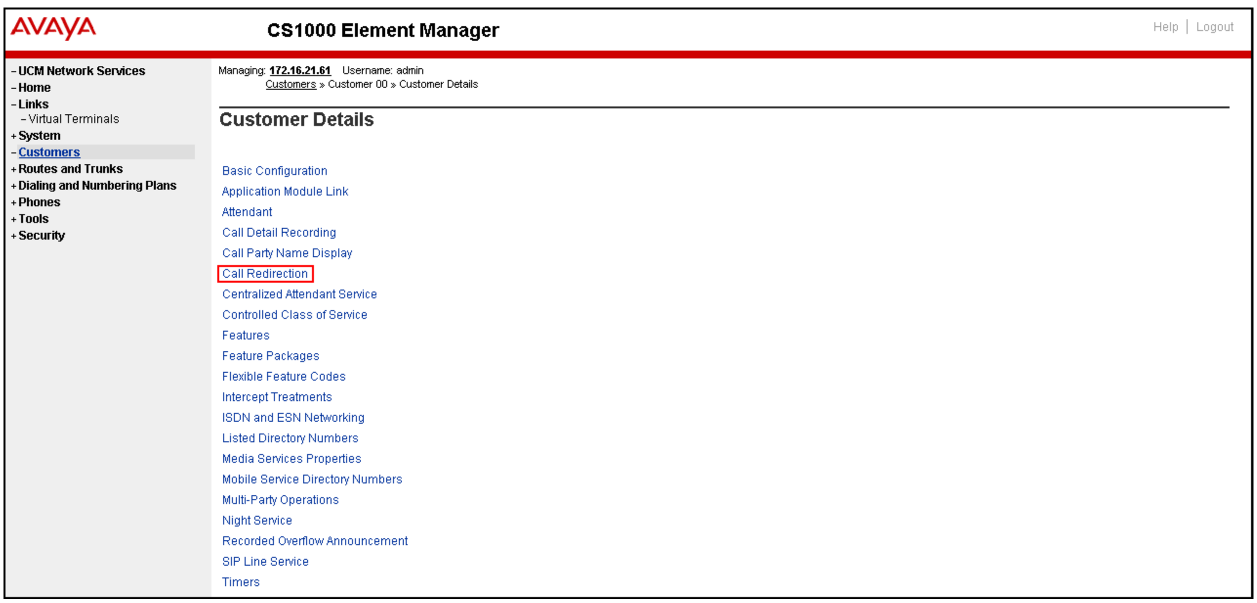
5.7.3. Enable Call Forward for the Phone

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

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



Select **Call Redirection** as shown below.

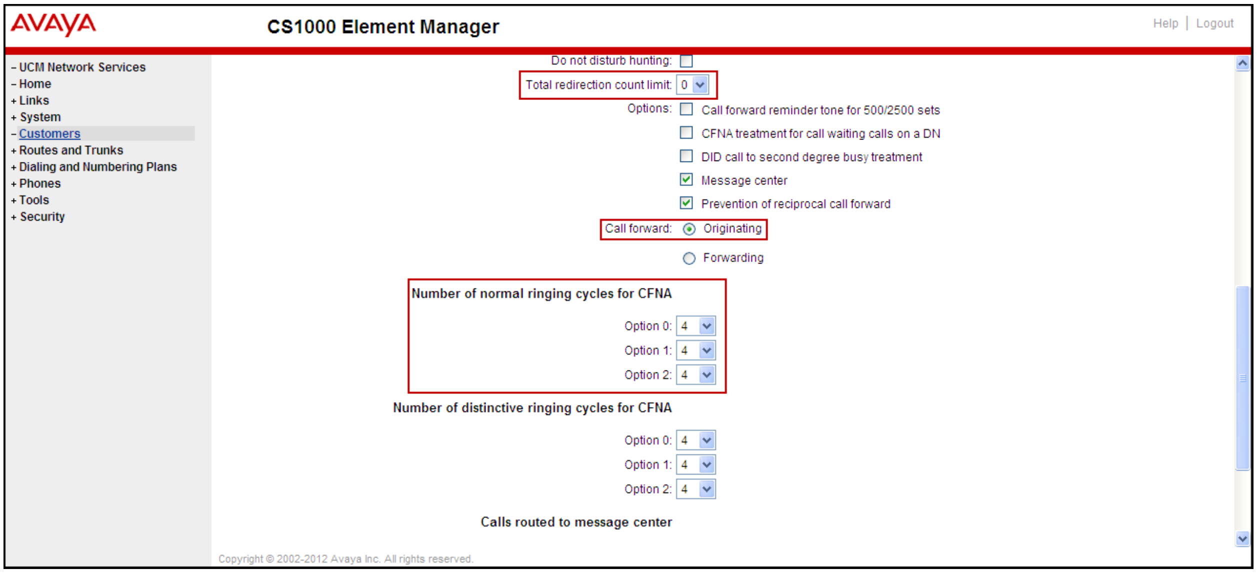


The **Call Redirection** page is displayed as shown below.

Set the following fields:

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

Click on **Save** (not shown)



Enable **Call Forward All Calls** (**CFAC**) for the phone over the SIP trunk by using **LD 11**. Change its CLS to **CXFA** and 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
```

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
....
```

Enable **Call Forward No Answer (CFNA)** for the phone over the SIP trunk by using **LD 11**. Change its CLS to **FNA, SFA** and 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 Session Manager

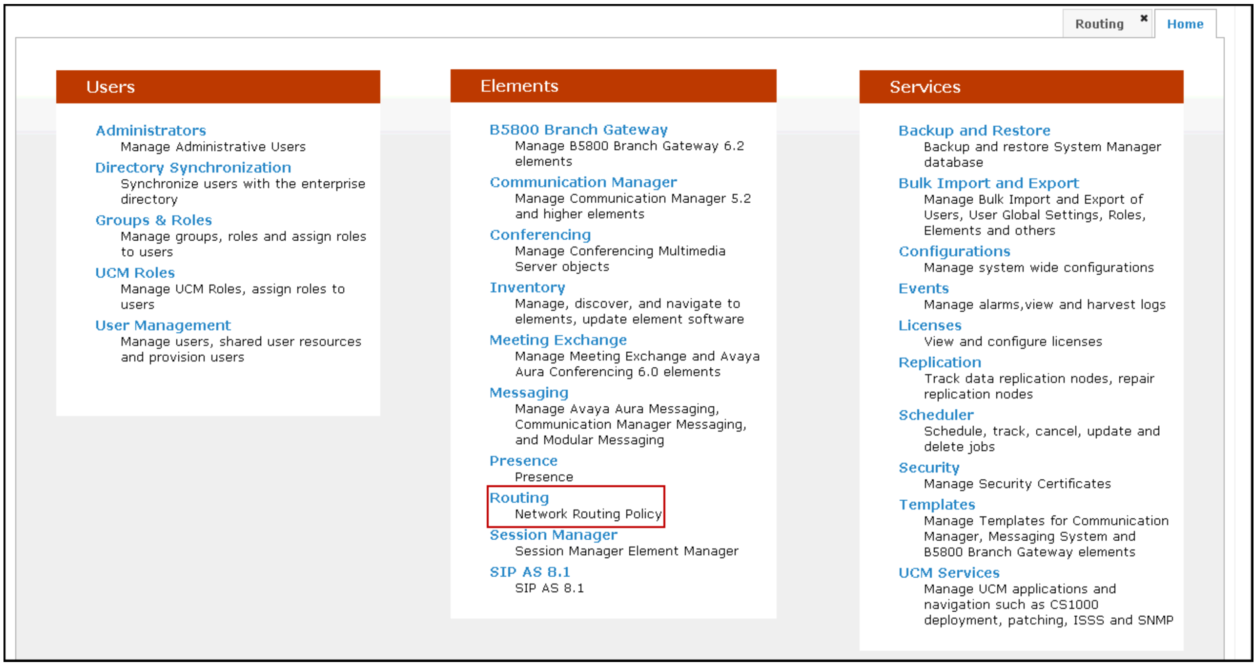
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Location(s) that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to the CS1000, Avaya SBCE and Session Manager itself.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- Regular Expressions, which also can be used to route calls.
- Session Manager, corresponding to the Session Manager Server to be managed by Avaya Aura® System Manager.

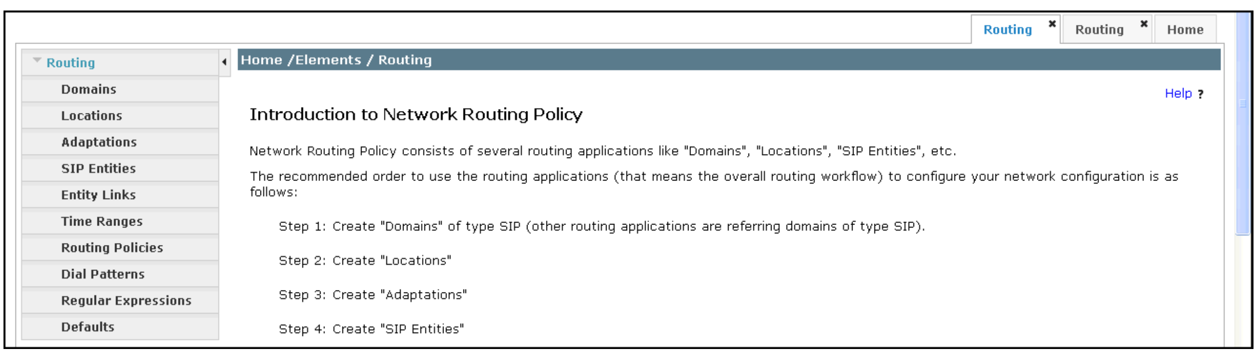
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. System Manager Login and Navigation

Session Manager Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials and click on **Login** (not shown). The screen shown below is then displayed; click on **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.



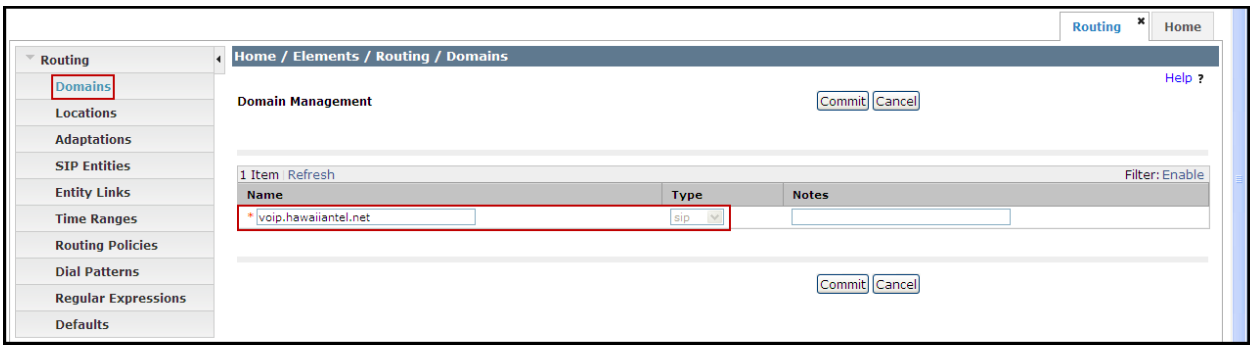
6.2. Specify SIP Domains

Create a SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, the domain **voip.hawaiiantel.net** was added.

To add a domain Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the Hawaiian Telecom domain.



6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

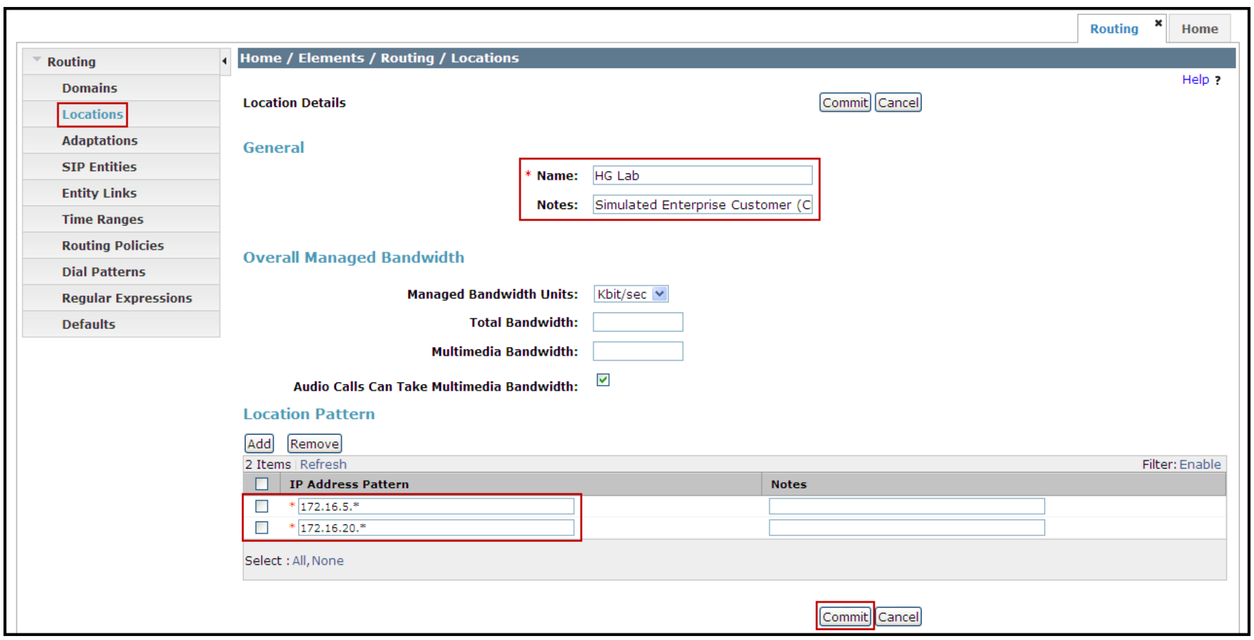
In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

In the **Location Pattern**, click **Add** and enter the following values. Use default values for all remaining fields:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

The screen below shows the addition of the **HG Lab** location, which includes all equipment on the **172.16.5.x** and **172.16.20.x** subnets including the CS1000, Avaya SBCE and Session Manager. Click **Commit** to save.

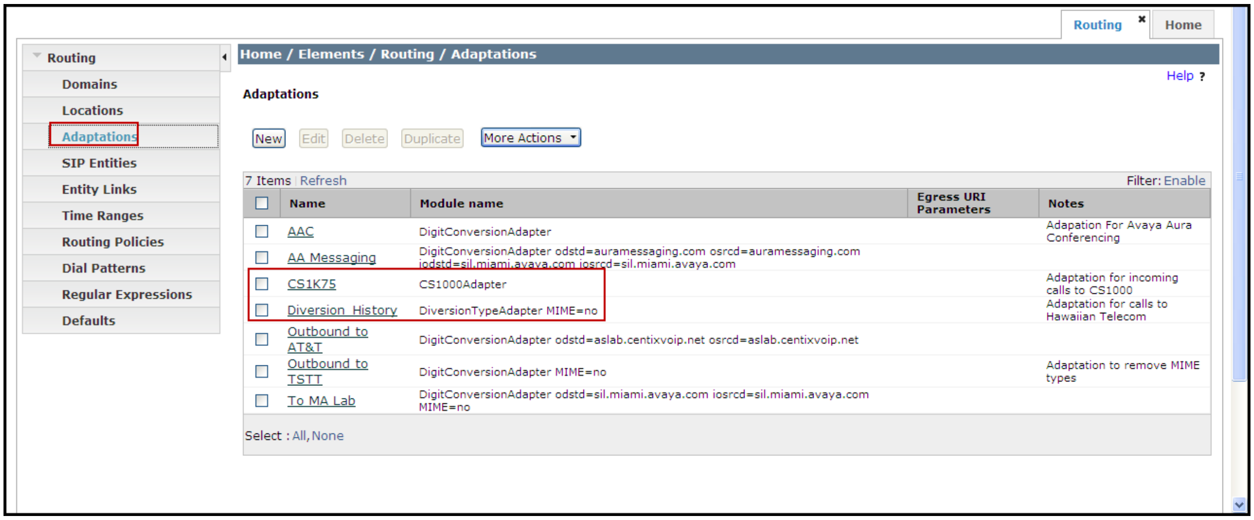


6.4. Add Adaptation Module

Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic module and can modify other headers to permit interoperability with third party SIP products.

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed. The following screen shows a portion of the list of adaptations in the sample configuration.

The adaptations named **CS1K75** and **Diversion_History** were created and used during the compliance test.



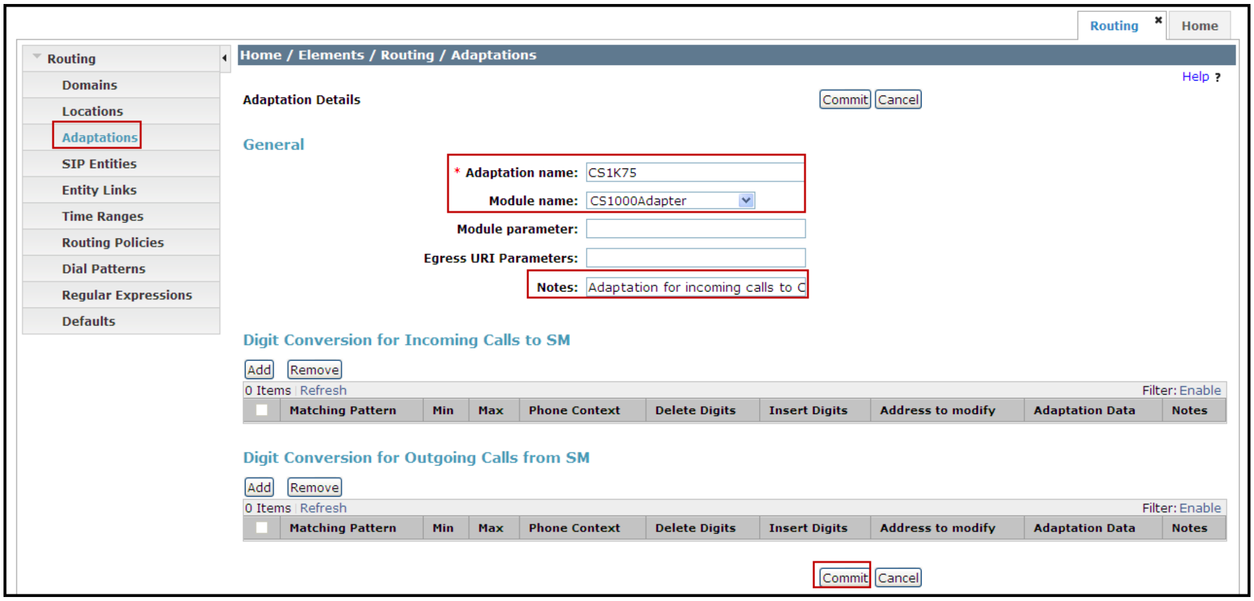
Settings for **CS1K75** Adaptation:

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **CS1000Adapter**.

Click **Commit** to save.

The **CS1K75** adaptation shown below will later be assigned to the **CS1K7.5** SIP entity.



Settings for **Diversion_History** Adaptation:

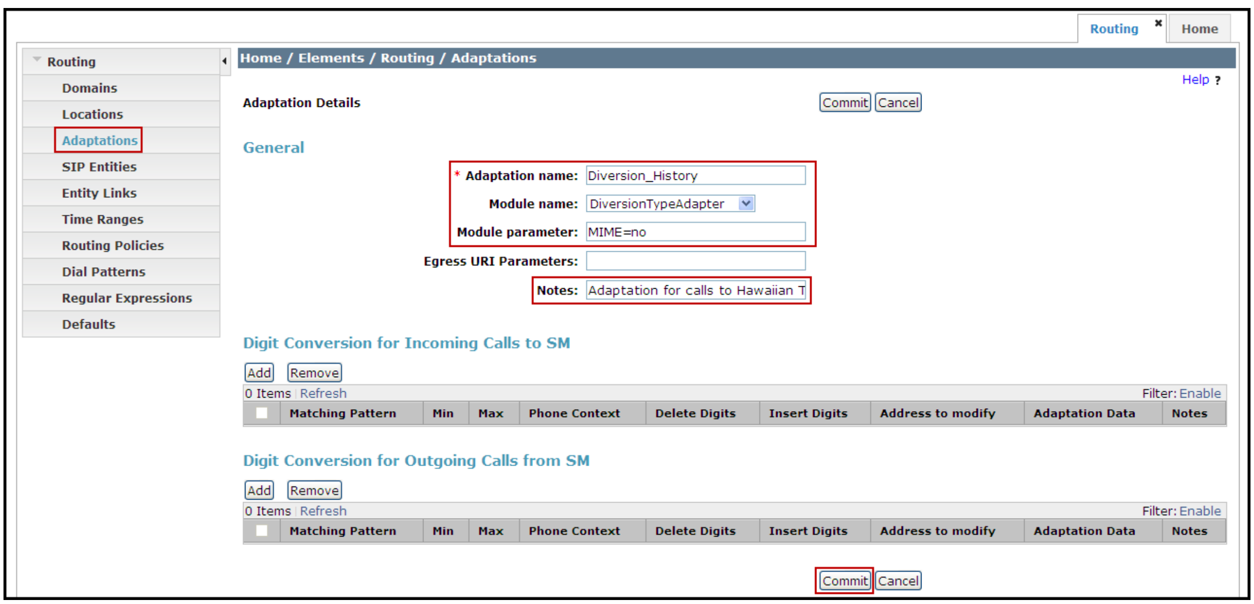
The adapter named **Diversion_History** will later be assigned to the Avaya SBCE SIP entity for calls to Hawaiian Telecom. This adaptation uses the **DiversionTypeAdapter** to convert the History-Info header to a Diversion header. The Module parameter **MIME=no** will remove MIME types inserted by the CS1000 which are not used for call processing and should not be sent to Hawaiian Telecom.

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **DiversionTypeAdapter.**
- **Module parameter:** Enter **MIME=no**

Click **Commit** to save.

The **Diversion_History** adaptation shown below will later be assigned to the **HG ASBCE** SIP entity.



6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes the CS1000 and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity interface that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **Other** for the CS1000 and Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** defined in **Section 6.4**.
- **Location:** Select one of the locations defined in **Section 6.3**.
- **Time Zone:** Select the time zone to which the entity belongs.

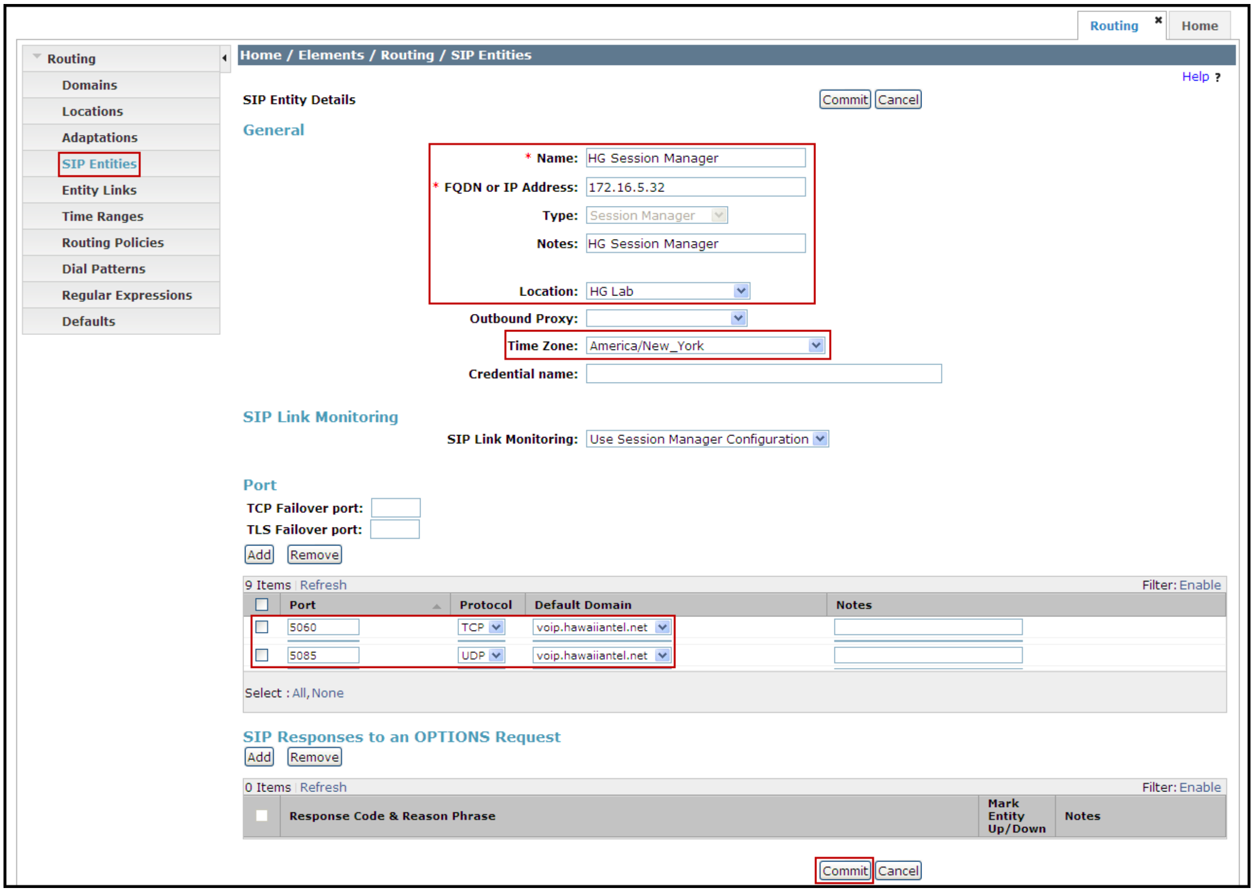
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.
In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

Click **Commit** to save.

For the compliance test, only two Ports were used:

- **5060** with **TCP** for connecting to Avaya SBCE.
- **5085** with **UDP** for connecting to the CS1000.

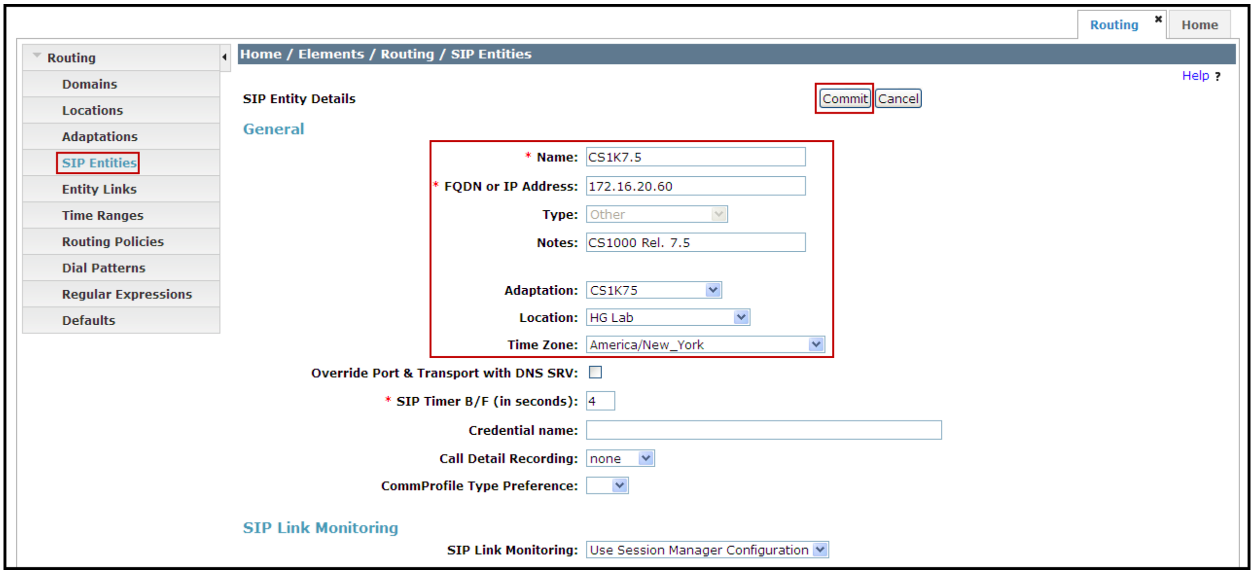
The following screen shows the addition of Session Manager. The IP address of the Session Manager Security Module Interface is entered for **FQDN or IP Address**.



A separate SIP entity for the CS1000 is required in order to send SIP service provider traffic. The following screen shows the addition of the CS1000 SIP entity.

For the compliance testing, the following values were used:

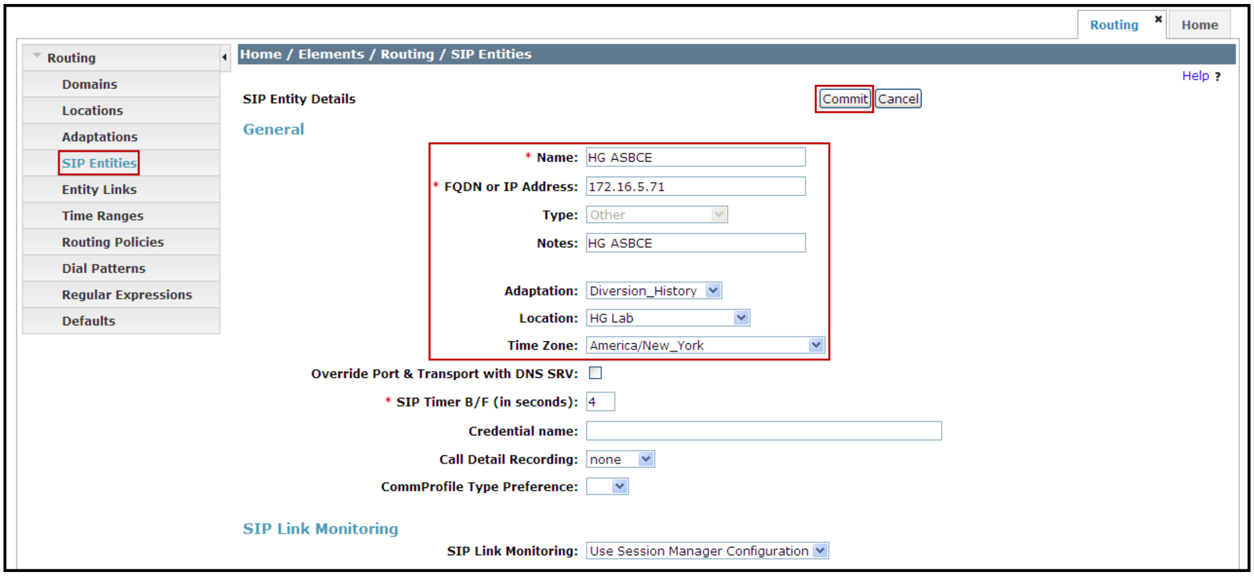
- **Name:** Enter a descriptive name.
- The **FQDN or IP Address** field is set to the TLAN IP address of the CS1000 Signaling Gateway (Node IP address), refer to **Section 5.2.1**.
- For Adaptation select the **CS1K75** adaptation defined in **Section 6.4**.
- For Location select the **HG Lab** location defined in **Section 6.3**.



A separate SIP entity for the Avaya SBCE is required in order to route calls to the service provider. The following screen shows the addition of Avaya SBCE SIP entity.

For the compliance test the fallowing values were used:

- **Name**: Enter a descriptive name.
- The **FQDN or IP Address** field is set to the IP address of the private network interface of the Avaya SBCE (see **Figure 1**).
- For Adaptation select the **Diversion_History** adaptation defined in **Section 6.4**.
- For Location select the **HG Lab** location defined **Section 6.3**.



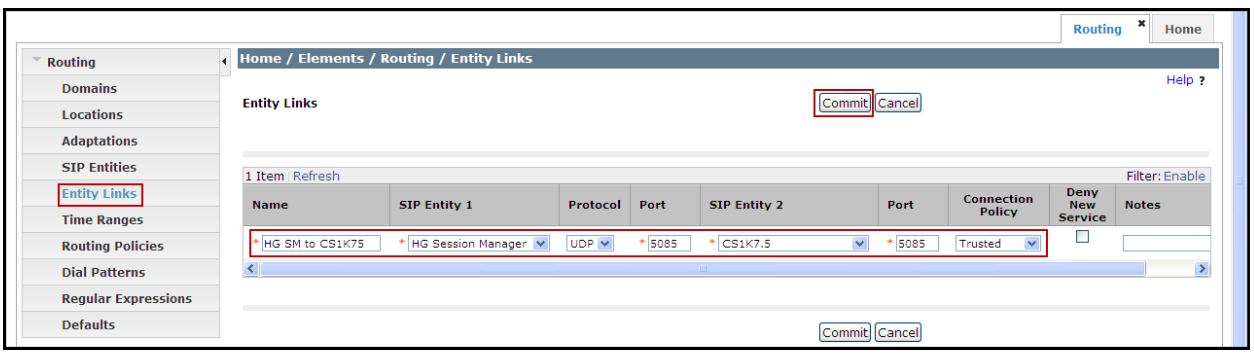
6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the CS1000 and the other to Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

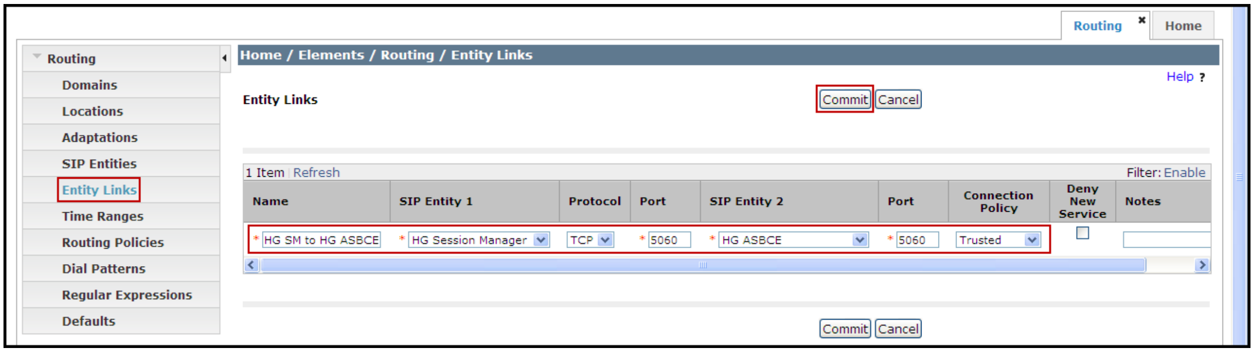
- **Name**: Enter a descriptive name.
- **SIP Entity 1**: Select the Session Manager entity configured in **Section 6.5**.
- **Protocol**: Select the transport protocol used for this link. This must match the protocol defined in **Section 6.5.**
- **Port**: Port number on which Session Manager will receive SIP requests. This must match the port defined in **Section 6.5.**
- **SIP Entity 2**: Select the name of the other system. For the CS1000 and Avaya SBCE, select the CS1000 or Avaya SBCE SIP entity defined in **Section 6.5**.
- **Port**: Port number on which the CS1000 will receive SIP requests. For the CS1000 this must match the port defined under **SIP Gateway Settings** tab, under **Proxy or Redirect Server** in **Section 5.5.1**. For the Avaya SBCE this must match the port defined under **Server Configuration** in **Section 7.2.4.**
- **Connection Policy**: Select **Trusted** from the pull-down menu.

Click **Commit** to save.

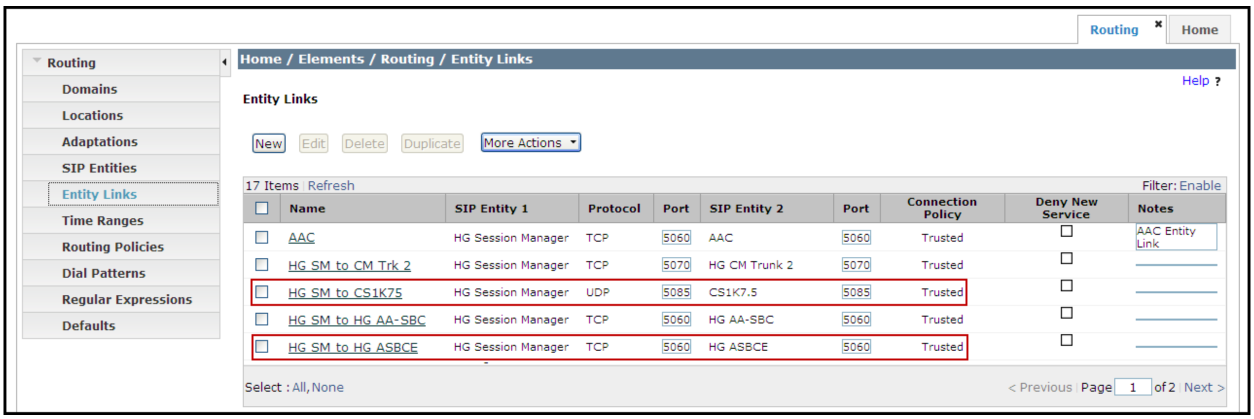
The following screen illustrates the Entity Link to the CS1000.



The following screen illustrates the Entity Link to the Avaya SBCE.



The following screen shows the list of Entity Links. Note that only the highlighted links were created for the compliance test, and are the relevant links for these Application Notes.



6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added for this compliance test: One for the CS1000 and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed.

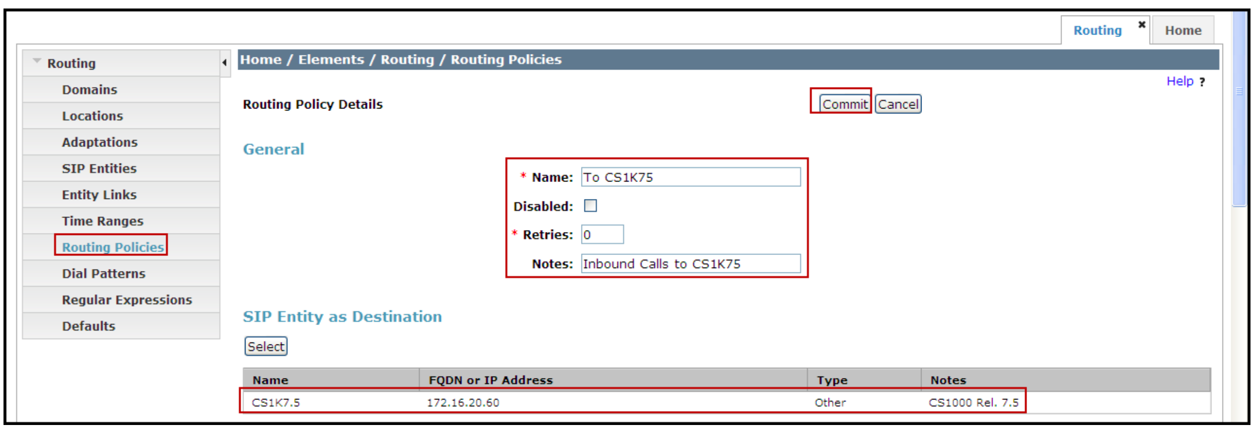
In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

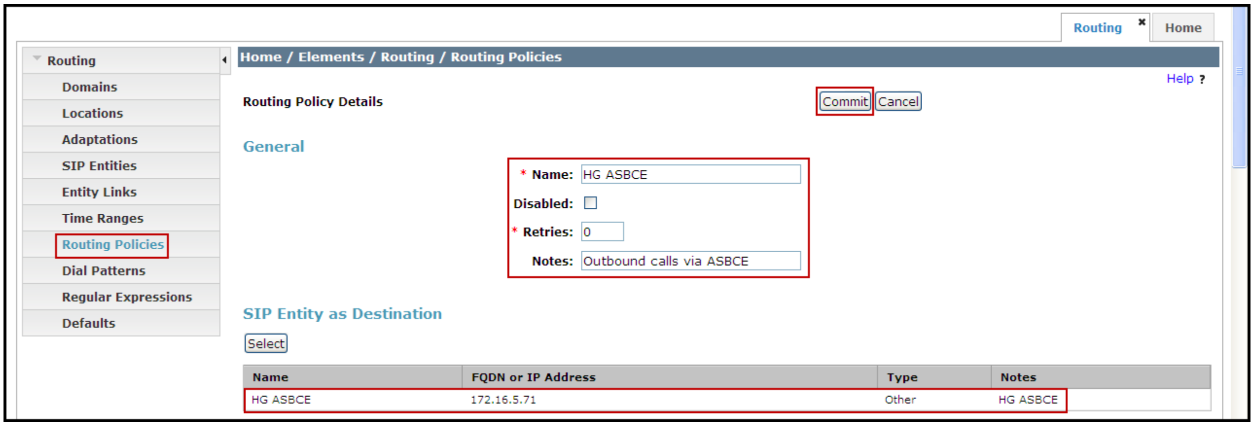
In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields.

Click **Commit** to save.

The following screen shows the Routing Policy for the CS1000.



The following screen shows the Routing Policy for the Avaya SBCE.



6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were configured to route calls from the CS1000 to Hawaiian Telecom and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

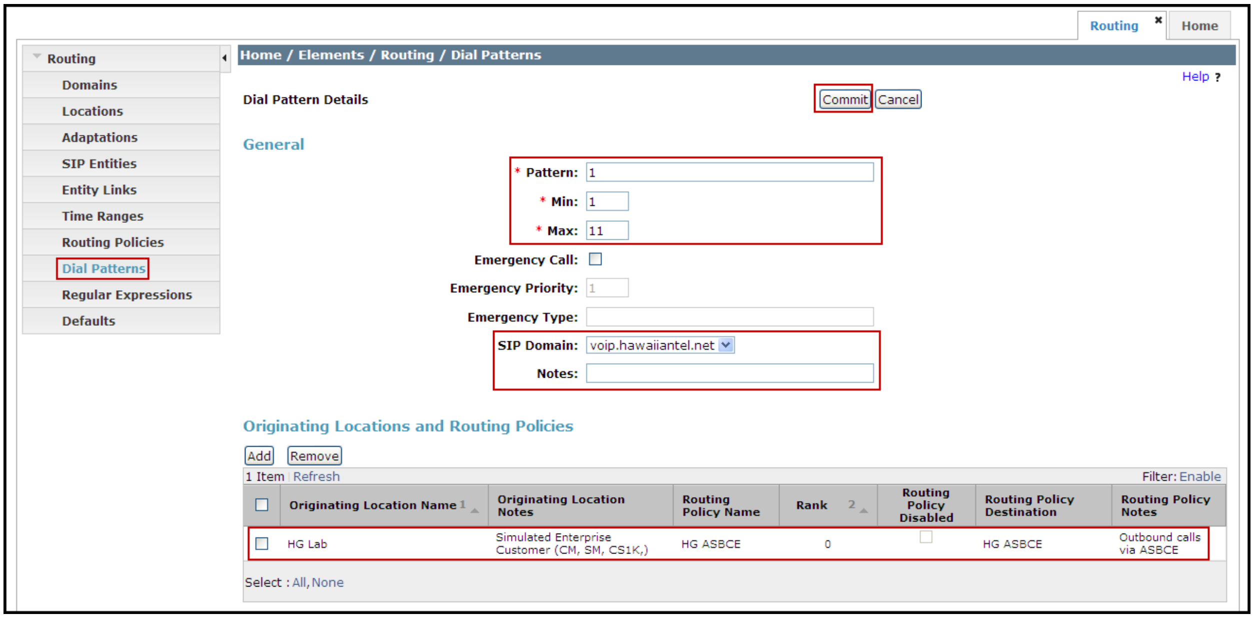
In the **General** section, enter the following values. Use default values for all remaining fields:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain configured in **Section 6.2** used in the matching criteria.
- **Notes:** Add a brief description (optional).

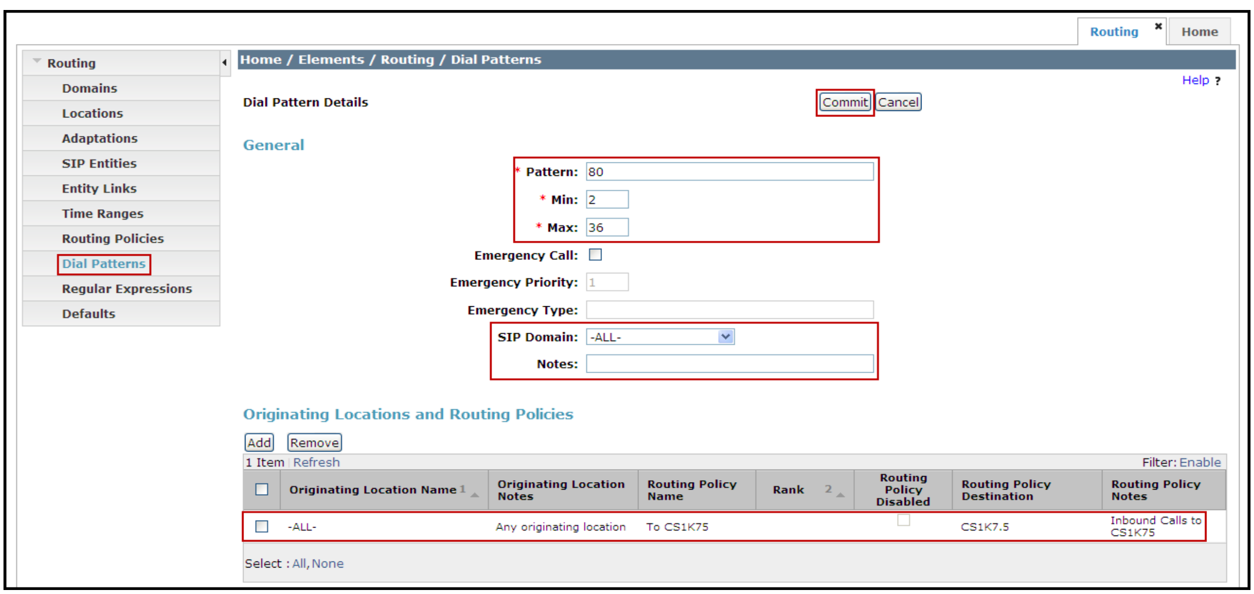
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

The example shown below is for dial pattern **1** for the North American Numbering Plan area prefix, which have a destination domain of **voip.hawaiiantel.net**, Originating Location Name of **HG Lab,** and uses Routing Policy **HG ASBCE.**



The next example shown below is for dial pattern **80** to route inbound calls to DID numbers provided by Hawaiian Telecom (DID numbers assigned to extensions in the CS1000), which have a destination domain of **–ALL-**, Originating Location Name of **–ALL-**, and uses Routing Policy **To CS1K75.** Note that **–ALL-** is being used for the SIP Domain and the Originating Location Name since pattern **80** is being shared with other domain and originating locations being used by other test activities in the lab.



The same procedure should be followed to add other required dial patterns.

6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was done as part of the initial Session Manager installation. To add Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

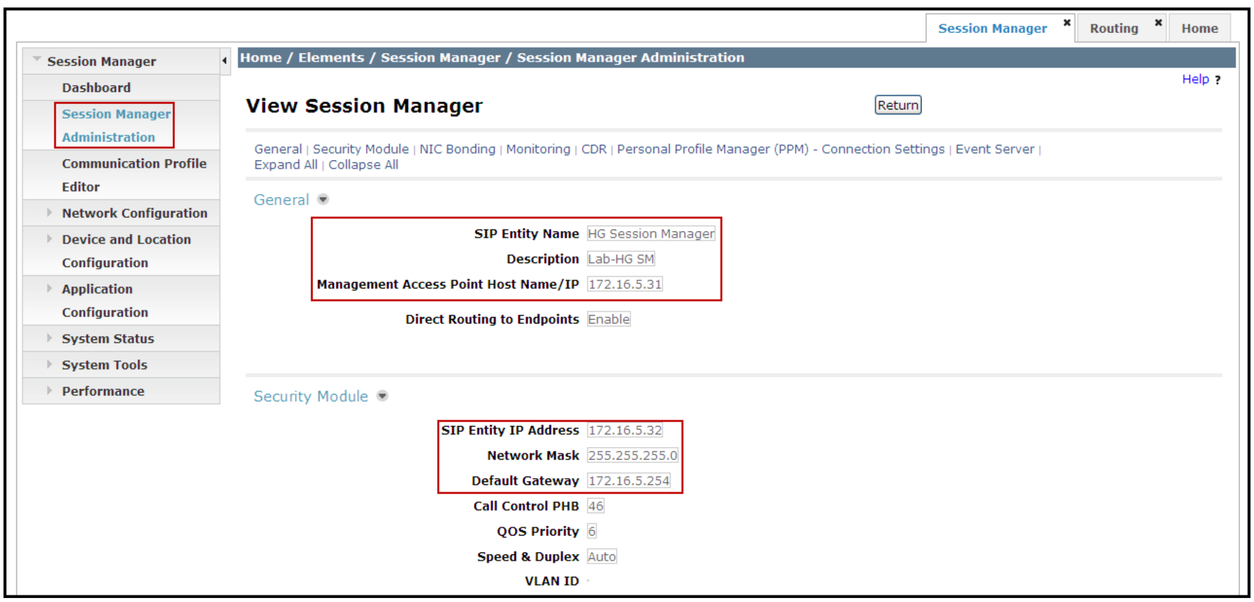
In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name, otherwise, enter the IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager above.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add Session Manager. The screen below shows the Session Manager values used for the compliance test.



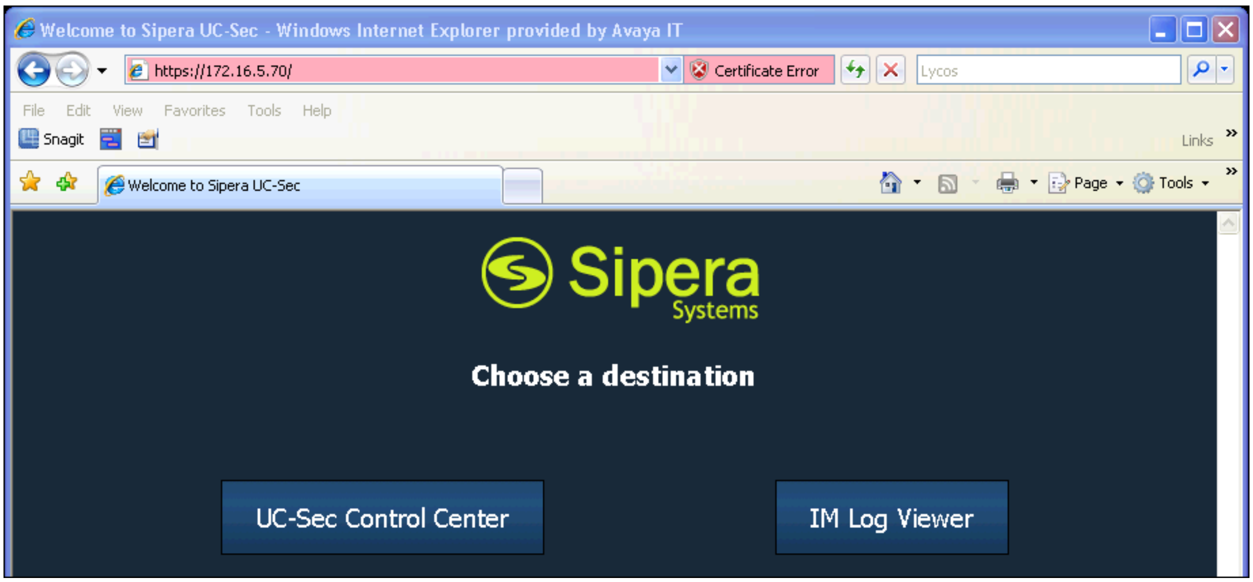
7. Configure the Avaya Session Border Controller for Enterprise (Avaya SBCE).

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

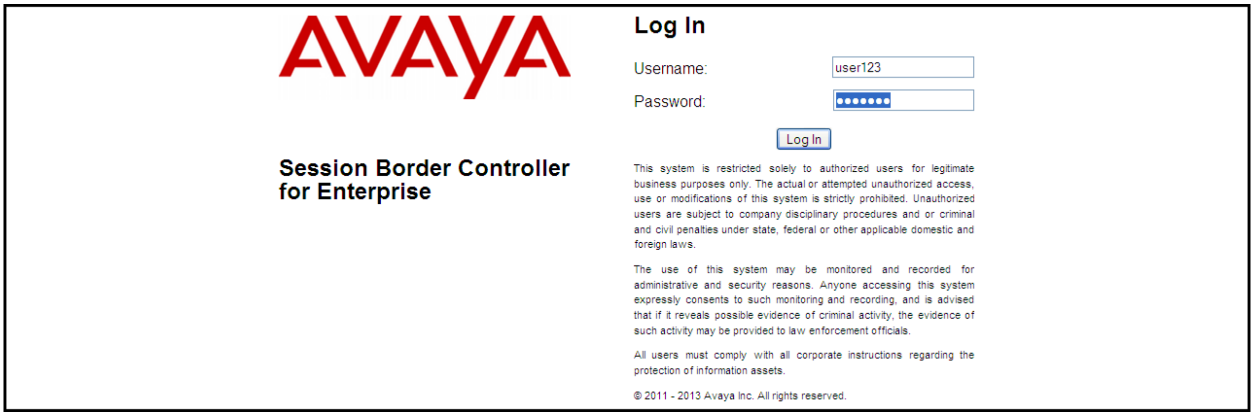
It is assumed that the Avaya SBCE is provisioned and ready to be used on the IP network. The configuration shown here is accomplished using the Avaya SBCE web interface.

7.1. Log in Avaya SBCE

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



Select **UC-Sec Control Center** and enter the **Username** and **password.**



7.2. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the UC-Sec control Center.

7.2.1. Server Interworking Avaya-SM

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

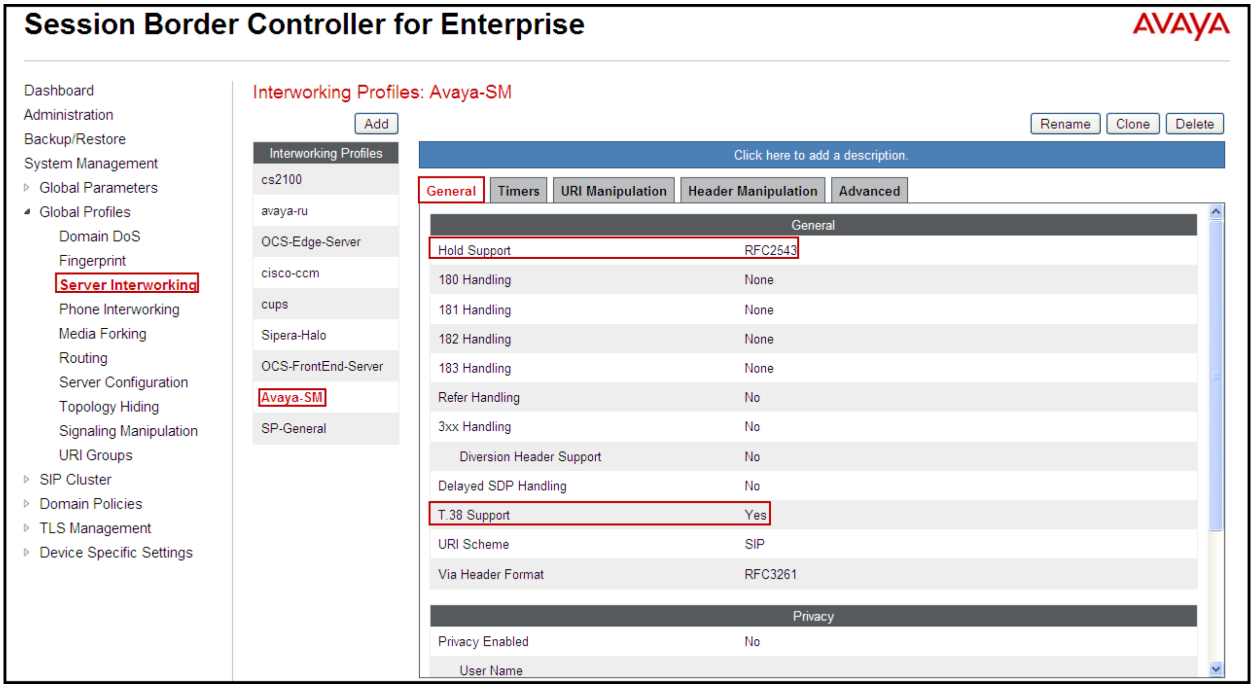
Several profiles have already been pre-defined and are populated in the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or “cloned”. Since modifying a default profile 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** (not shown)**.**

Enter the new profile name in the **Clone Name** field, the name of **Avaya-SM** was chosen in this example. Click **Finish.**
For the newly created **Avaya-SM** profile, click **Edit** (not shown) at the bottom of the General tab

- Verify that for **Hold Support**, **RFC2543** is selected.
- Verify that **T.38 Support** is selected.
- Click **Next**.
- Leave other fields with their default values.
- Click **Finish** on the **Privacy and DTMF** tab (not shown).

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



7.2.2. Server Interworking SP-General

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

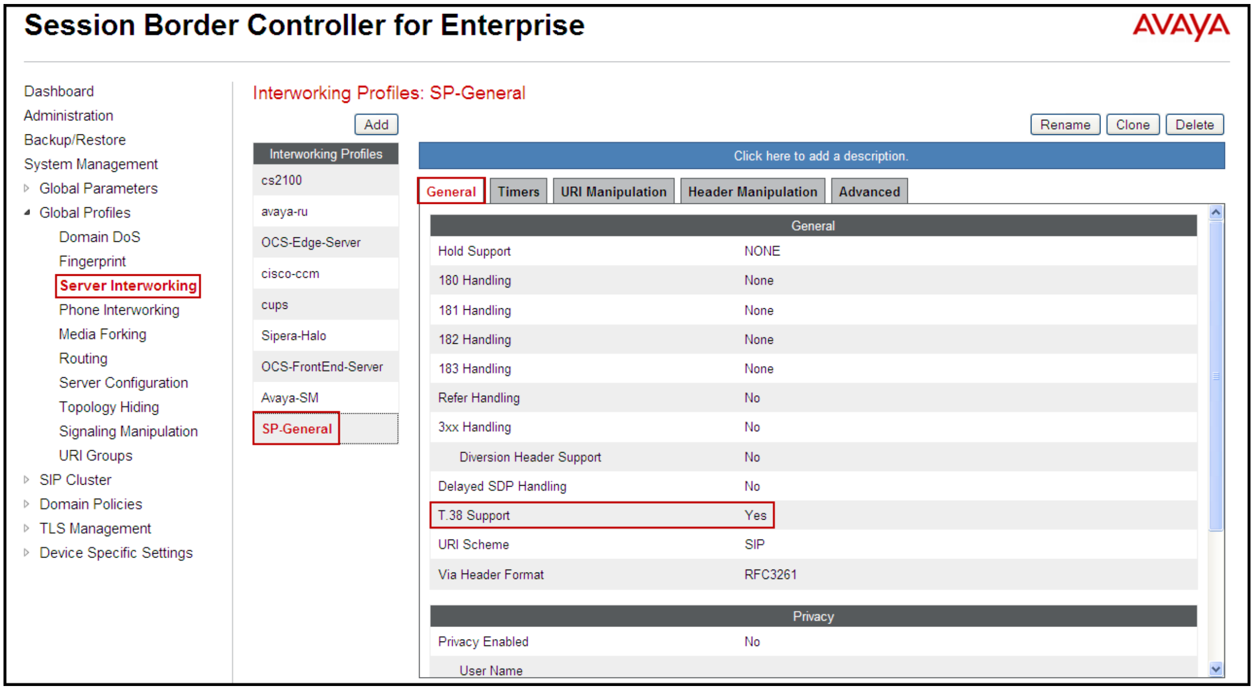
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add.**

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

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

- Select **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 newly added **SP-General** Profile.



7.2.3. Routing Profiles

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

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

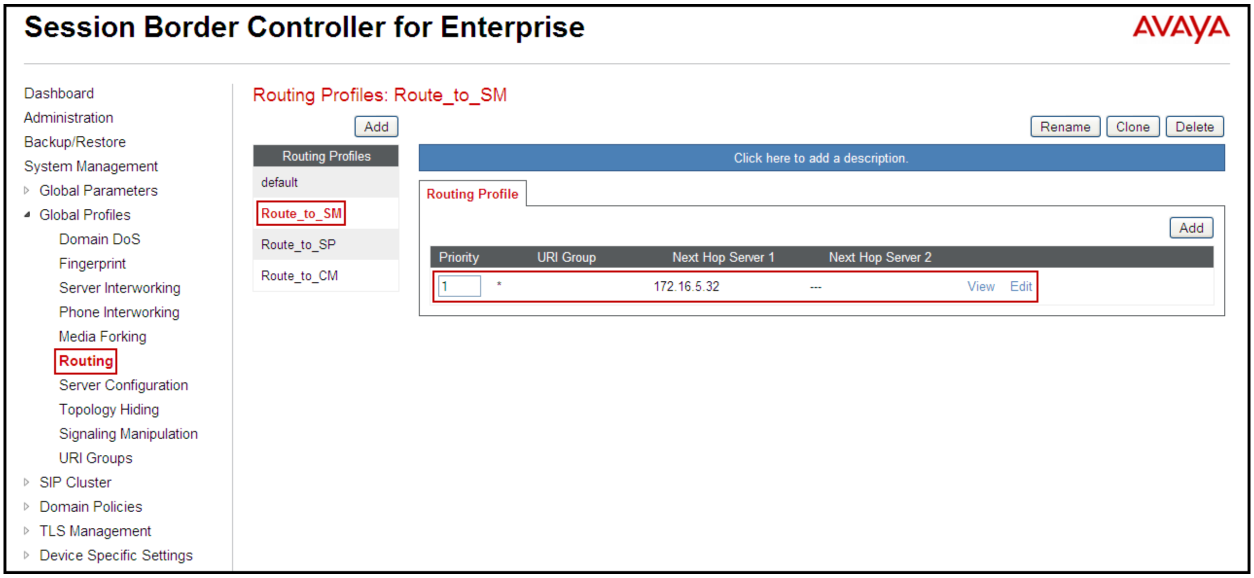
To create the inbound route, from the **Global Profiles** menu on the left-hand side:

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

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.32** (Session Manager IP address).
- Check **Routing Priority Based on Next Hop Server.**
- **Outgoing Transport: TCP.**
- Click **Finish.**

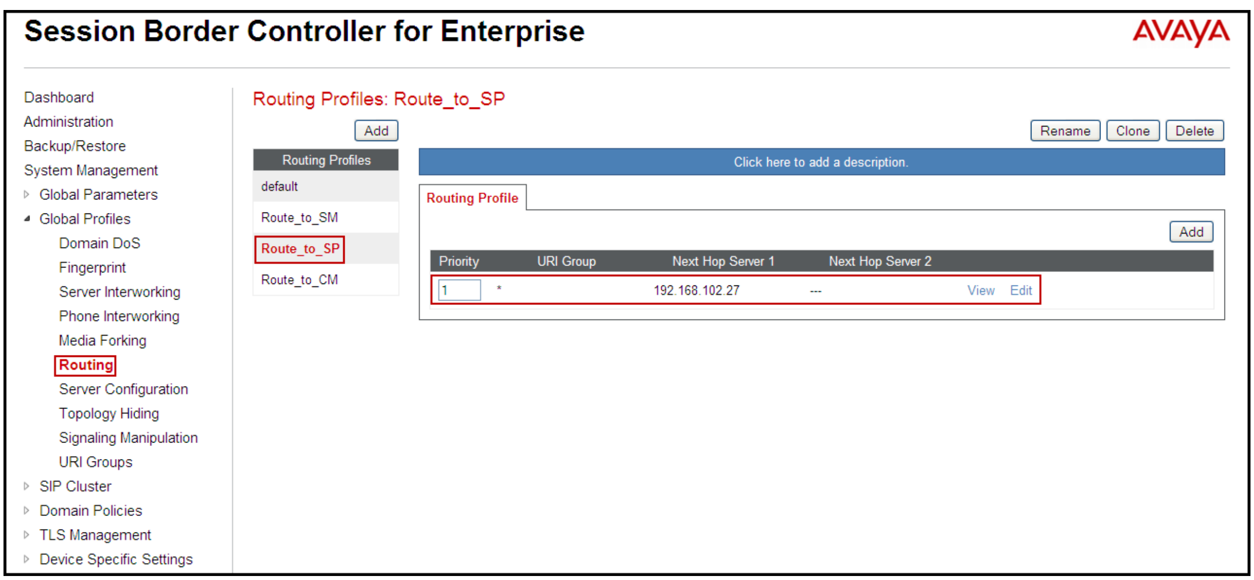
The following screen shows the newly added **Route_to_SM** Profile.



Similarly, for the outbound route:

- Select **Add Profile.**
- Enter Profile Name: **Route_to_SP**
- Click **Next.**
- **Next Hop Server 1: 192.168.102.27** (Service Provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server.**
- **Outgoing Transport: UDP.**
- Click **Finish.**

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



7.2.4. Server Configuration

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

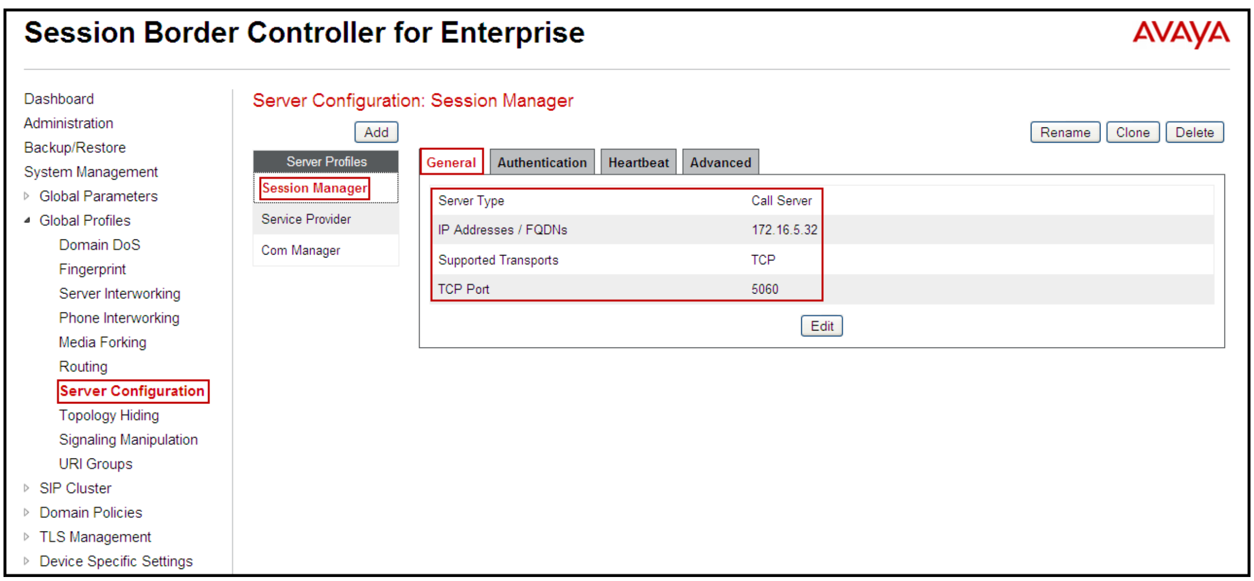
To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add Profile** and enter the profile name: **Session Manager**.

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

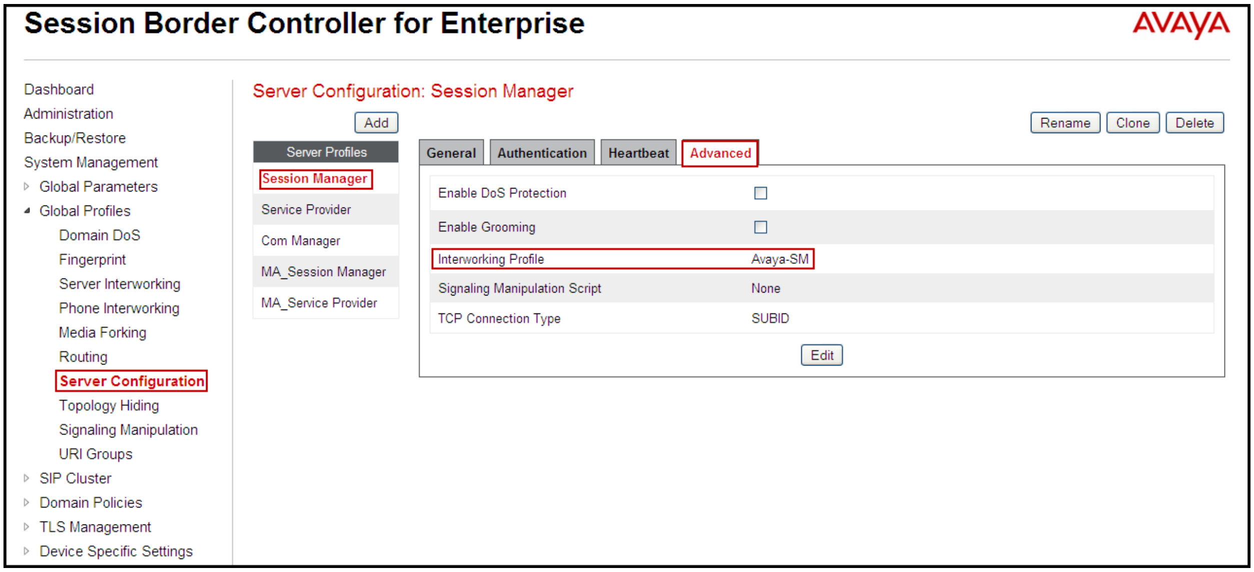
- Select **Call Server** for **Server Type**.
- **IP Address: 172.16.5.32 (**IP Address of Session Manager Security Module**).**
- **Supported Transports**: Check **TCP.**
- **TCP Port: 5060.**
- Click **Next.**
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Avaya-SM** from the **Interworking Profile** drop down menu.

  Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish.**

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



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



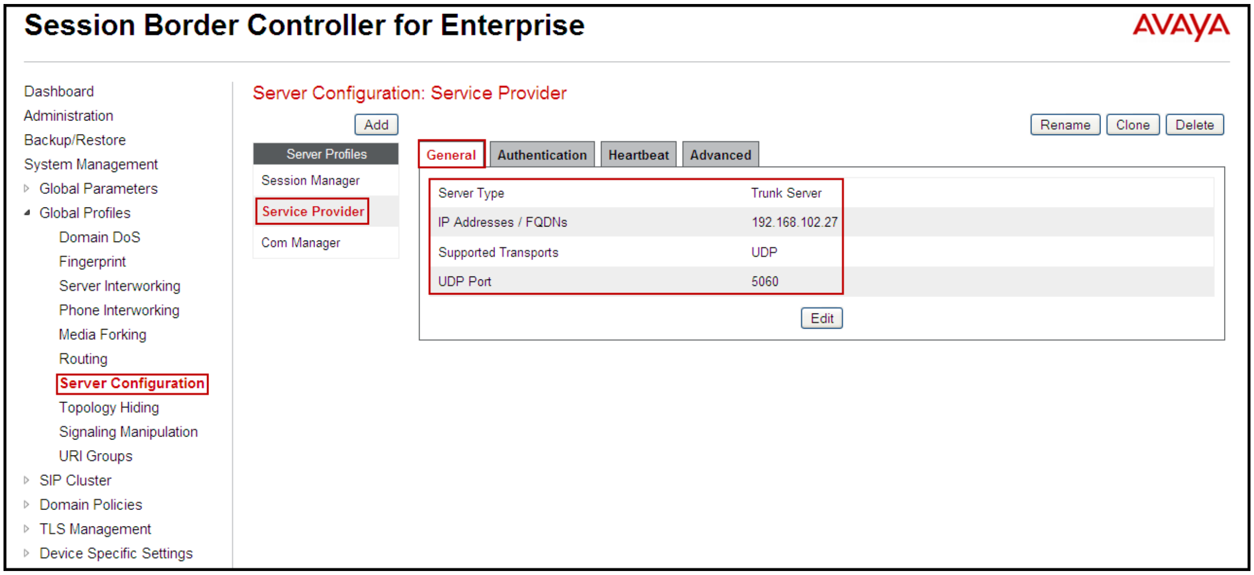
To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add Profile** and enter the profile name: **Service Provider.**

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

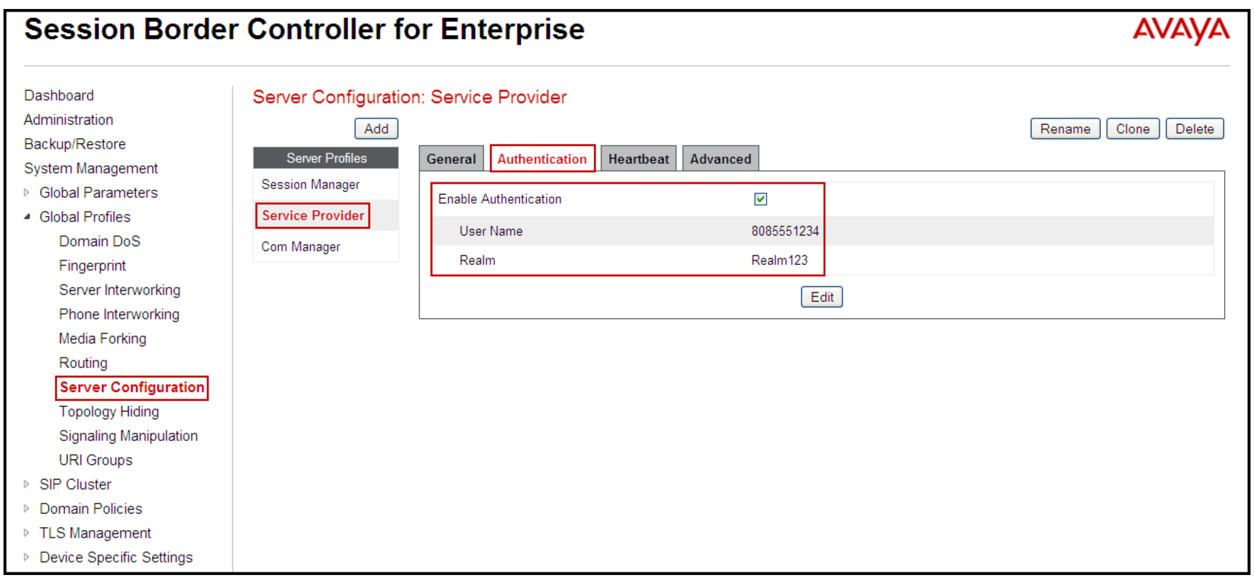
- Select **Trunk Server** for **Server Type**.
- **IP Address: 192.168.102.27** (service provider's SIP Proxy IP address).
- **Supported Transports**: Check **UDP**.
- **UDP Port: 5060.**
- Click **Next.**
- Select **Enable Authentication**.
- Enter the **user name** provided by Hawaiian Telecom in the **User Name** field.
- Enter the **realm** provided by Hawaiian Telecom in the **Realm** field.
- Enter the **password** provided by Hawaiian Telecom in the **Password** field.
- Re-enter the password provided by Hawaiian Telecom in the **Confirm Password** field
- Click **Next** to continue.
- Select **Enable Heartbeat**.
- Select **Register** under **Method.**
- Enter **frequency** for registration challenges (Value of **60** seconds was used in the compliance testing).
- Enter the **From URI** information (i.e., **8085551234@192.168.157.187**)
  Explanation of values used in the compliance testing:
  - **8085551234** is the pilot user provided by Hawaiian Telecom for registration purpose.
  - **192.168.157.187** is the outside IP address assigned to the Avaya SBCE.
- Enter the **To URI** information (i.e., **8085551234@hawaiiantel.net**).
  - **8085551234** is the pilot user provided by Hawaiian Telecom for registration purpose.
  - **Hawaiiantel.net** is the domain name provided by Hawaiian Telecom.

- Click **Next** to continue.
- On the **Advanced** tab, select **SP General** from the **Interworking Profile** drop down menu.
  Leave other fields with their default values for now, a **Signaling Manipulation** Script will be assigned later.
- Click **Finish.**

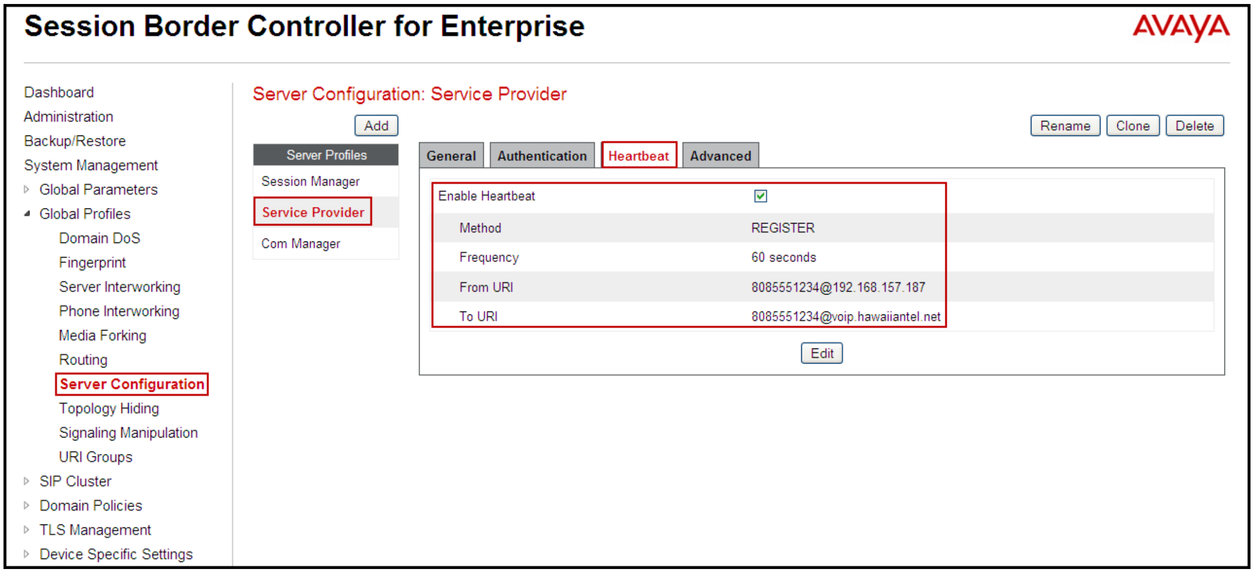
The following screen capture shows the **General** tab of the **Service Provider** Profile.



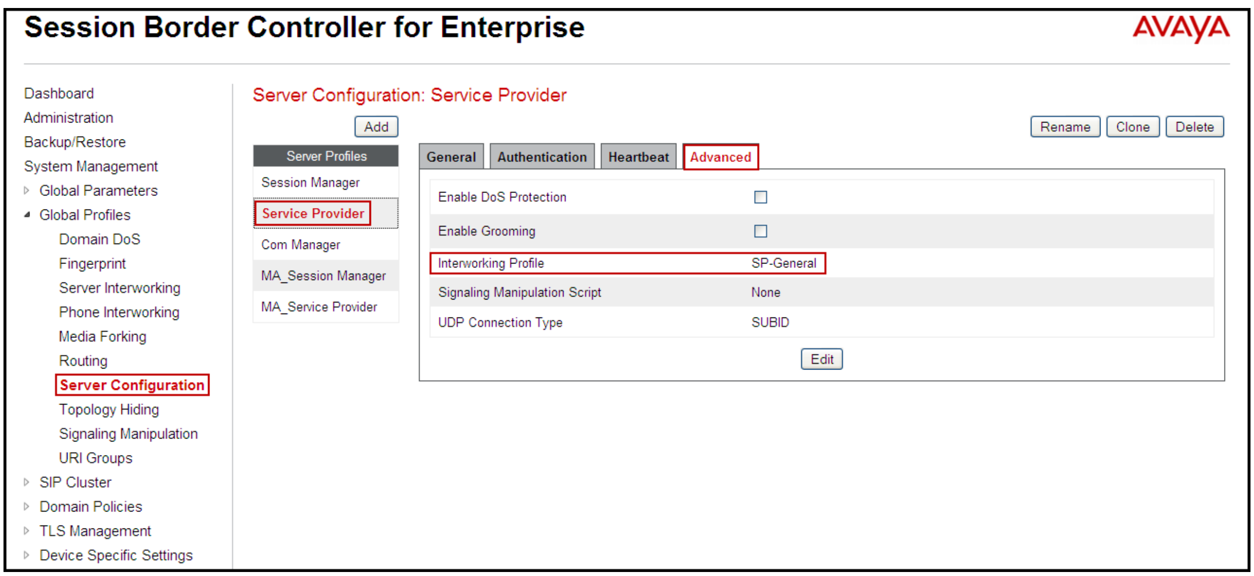
The following screen capture shows the **Authentication** tab of the **Service Provider** Profile.



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



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



7.2.5. 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.

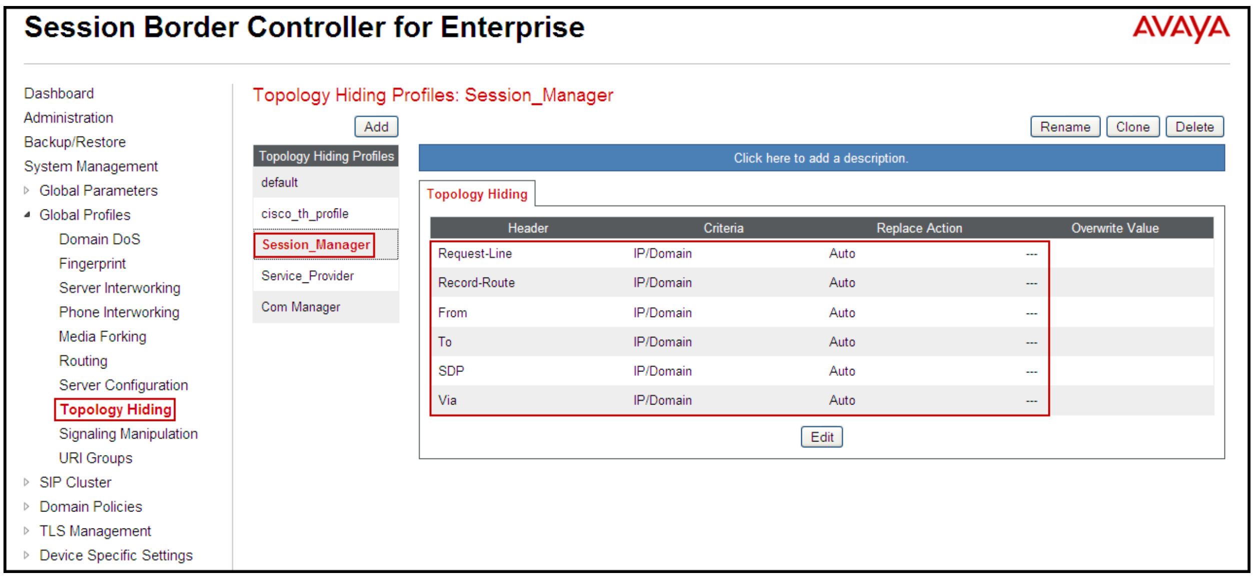
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

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

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

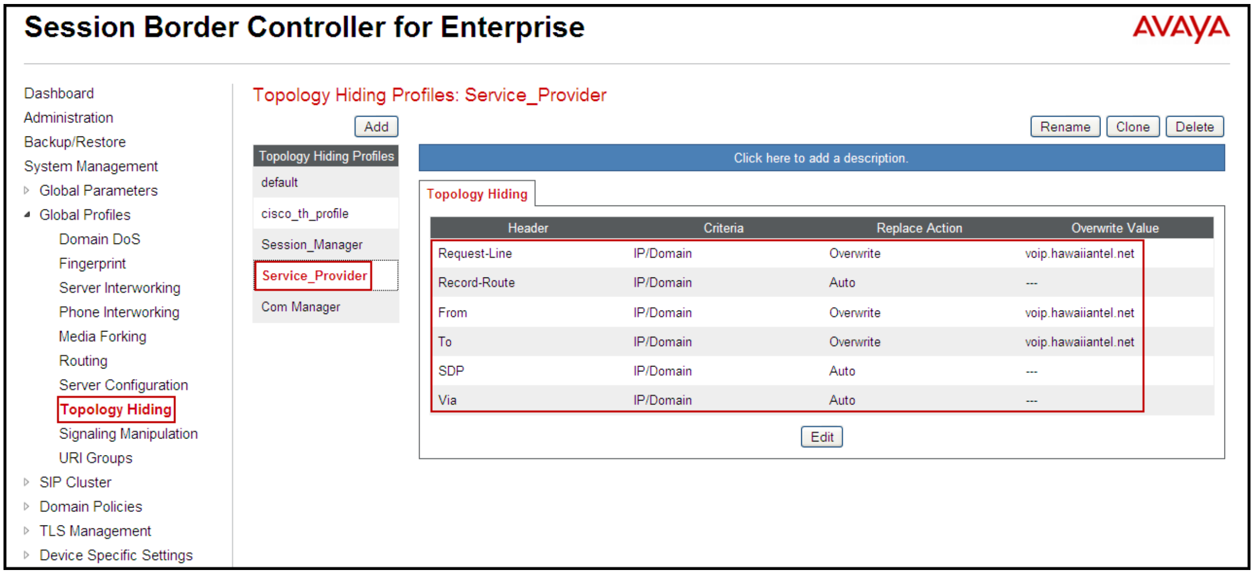


To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on the **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 the **From** header, choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider **(voip.hawaiiantel.net)** under **Overwrite Value**.
- For the **To** header, choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider **(voip.hawaiiantel.net)** under **Overwrite Value**.

- For the **Request-Line**, choose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider **(voip.hawaiiantel.net)** under **Overwrite Value**.
- Click **Finish**.

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



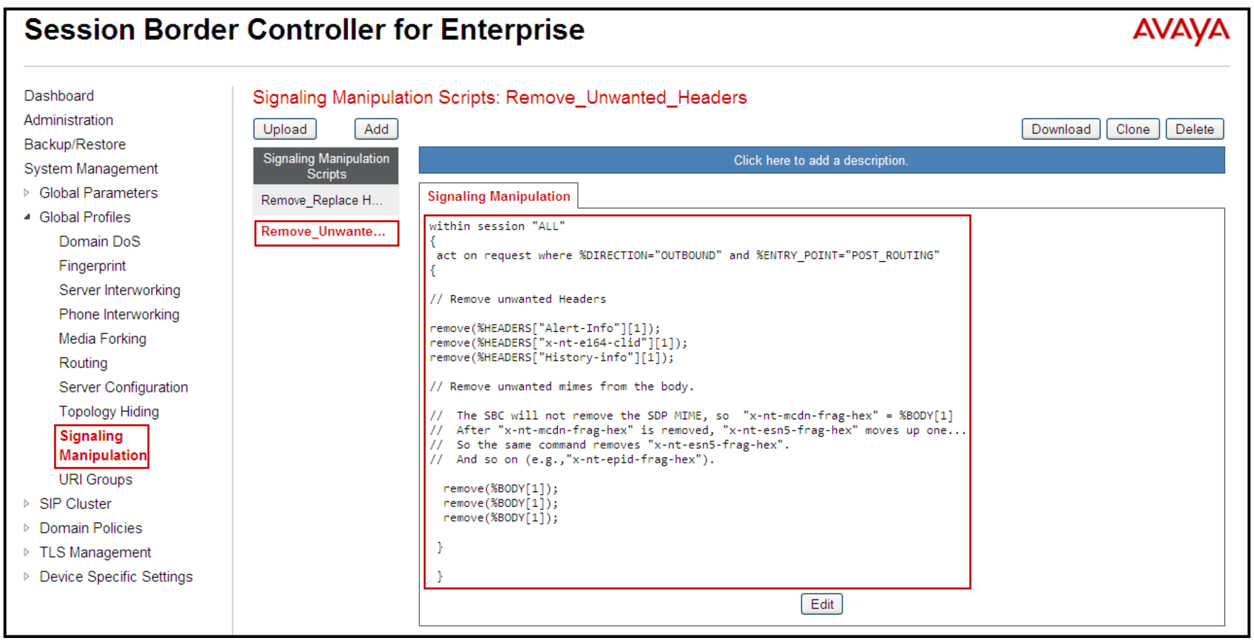
7.2.6. Signaling Manipulation

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.

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

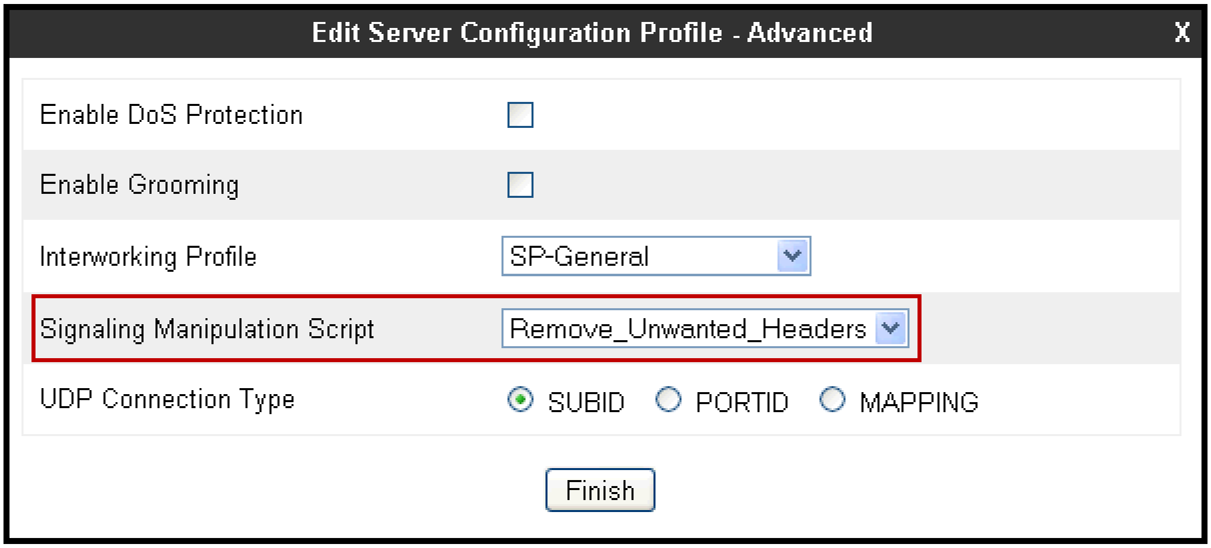
- For the **Title**, enter **Remove_Unwanted_Headers**.
- Enter the script as shown on the screen below.
- click **Save**

The following screen capture shows the added **Remove_Unwanted_Headers** Script.

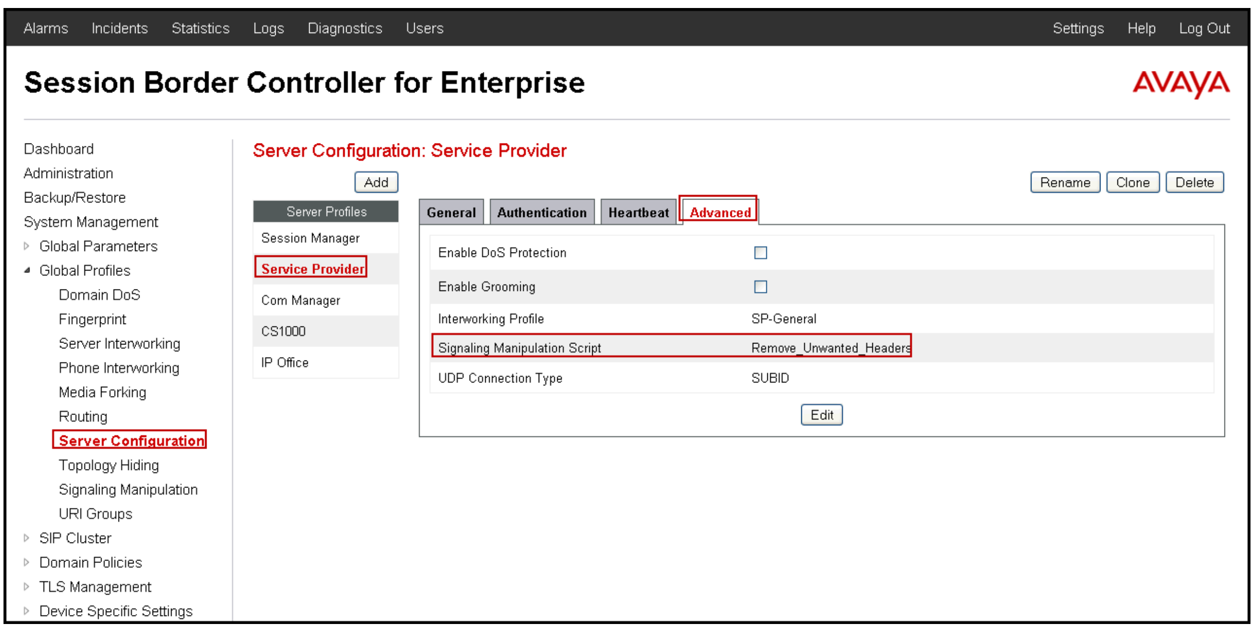


After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 7.2.4.**

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



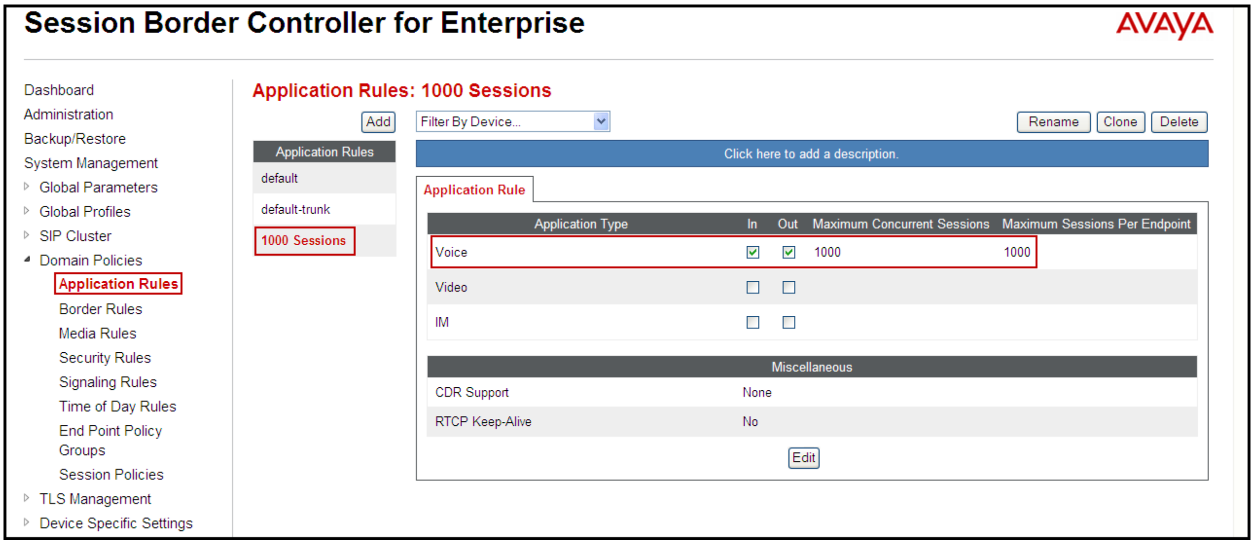
7.3. Domain Policies

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.

7.3.1. Create Application Rules

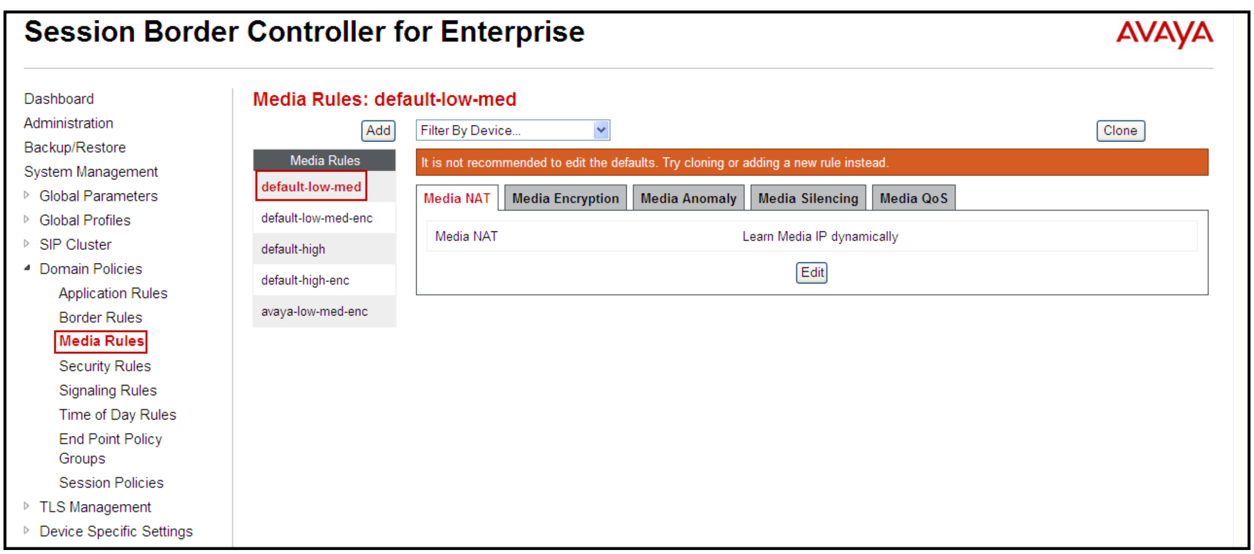
Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: Voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in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

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



7.3.2. Media Rules

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



7.3.3. 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 control of the Quality of Service of the signaling packets.

The Alert-Info, P-Location and P-Charging-Vector headers are sent in SIP messages from Session Manager to the Avaya SBCE, and then to the Service Provider's network. These headers should not be exposed outside of the enterprise. For simplicity, these headers were removed (blocked) from both requests and responses for both inbound and outbound calls.

A Signaling Rule was created, to be later applied in the direction of the Enterprise or the Service Provider. To create a rule to block the Alert-Info, P-Location and P-Charging-Vector headers coming from Session Manager, and from being propagated to the network, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on **default** Signaling Rules.
- Click on **Clone Rule**.
- Enter a name: **Remove Headers**.
- Click **Finish**.

Select the **Request Headers** tab of the newly created Signaling Rule.

To add the Alert-Info header:

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

To add the P-Location header:

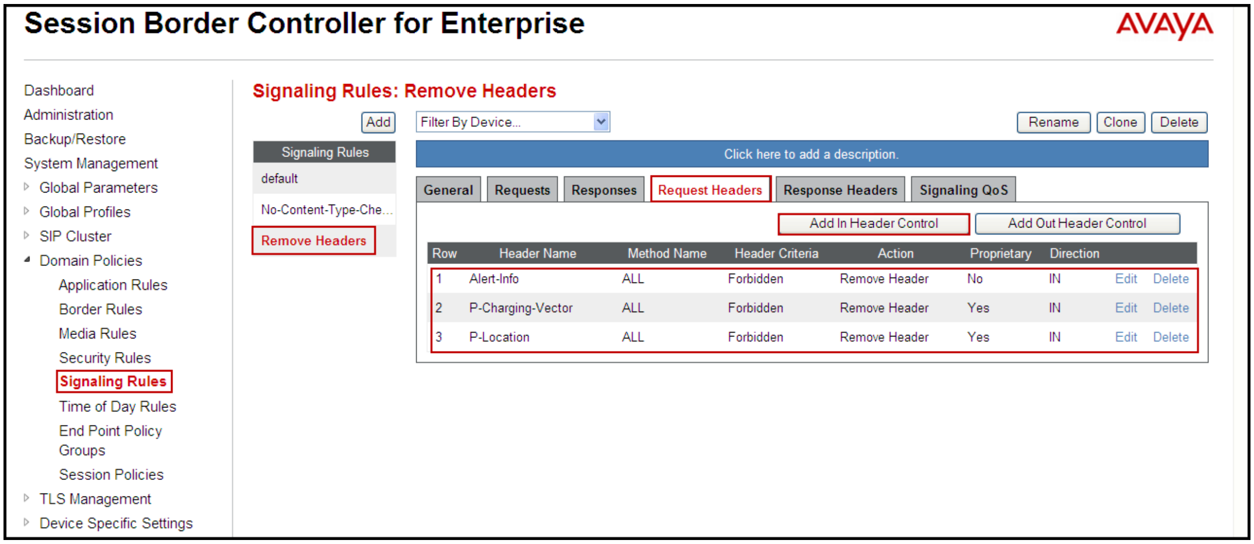
- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: P-Location.**
- **Method Name: INVITE.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

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: INVITE.**

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

The following screen capture shows the **Request Headers** tab of the **Remove Headers** Signaling Rule.



Select the **Response Headers** tab.

To add the Alert-Info header:

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

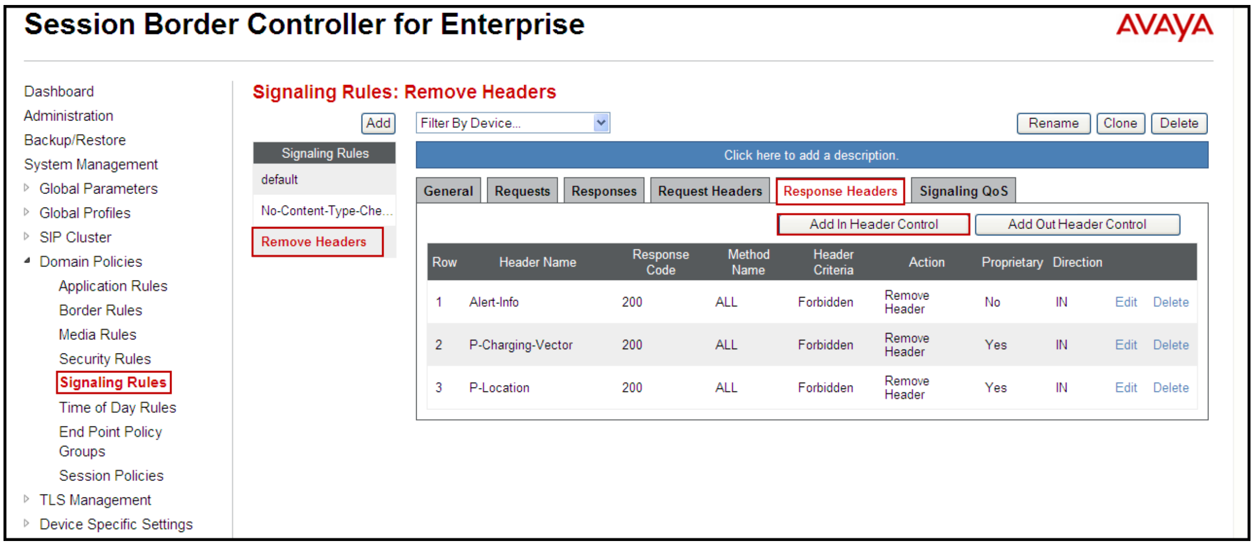
To add the P-Location header:

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

The following screen capture shows the **Response Headers** tab of the **Service Provider** Signaling Rule.



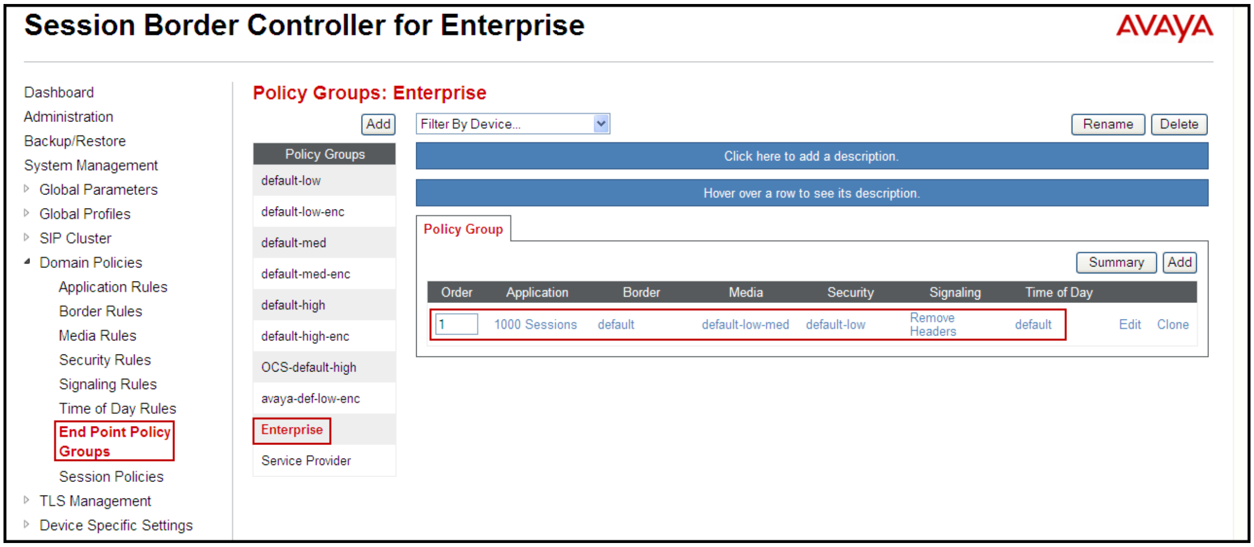
7.3.4. End Point Policy Groups

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

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

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

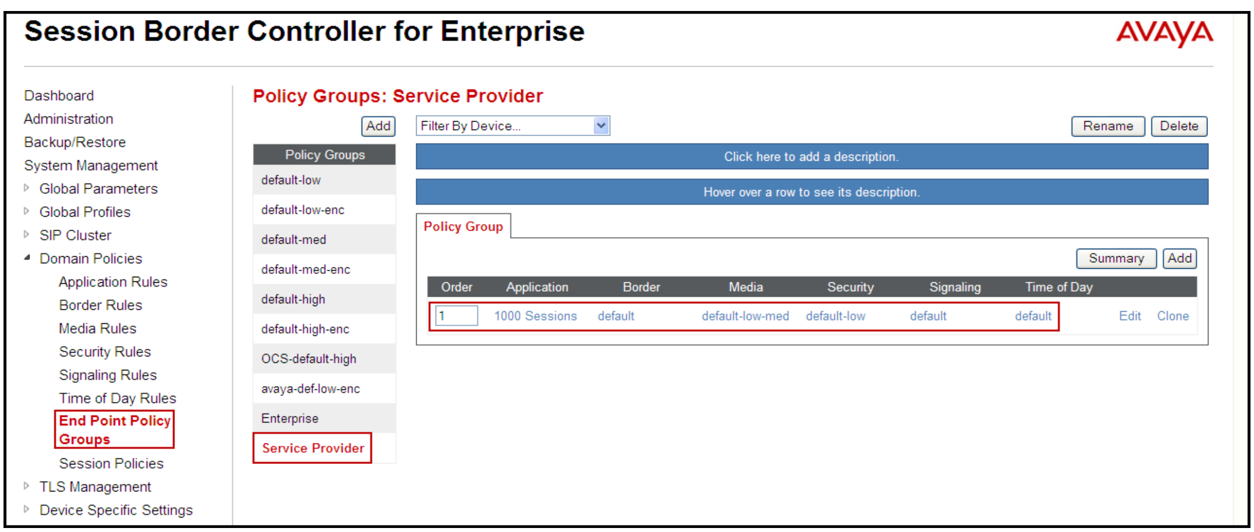
The following screen capture shows the newly added **Enterprise** End Point Policy Group.



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

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

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

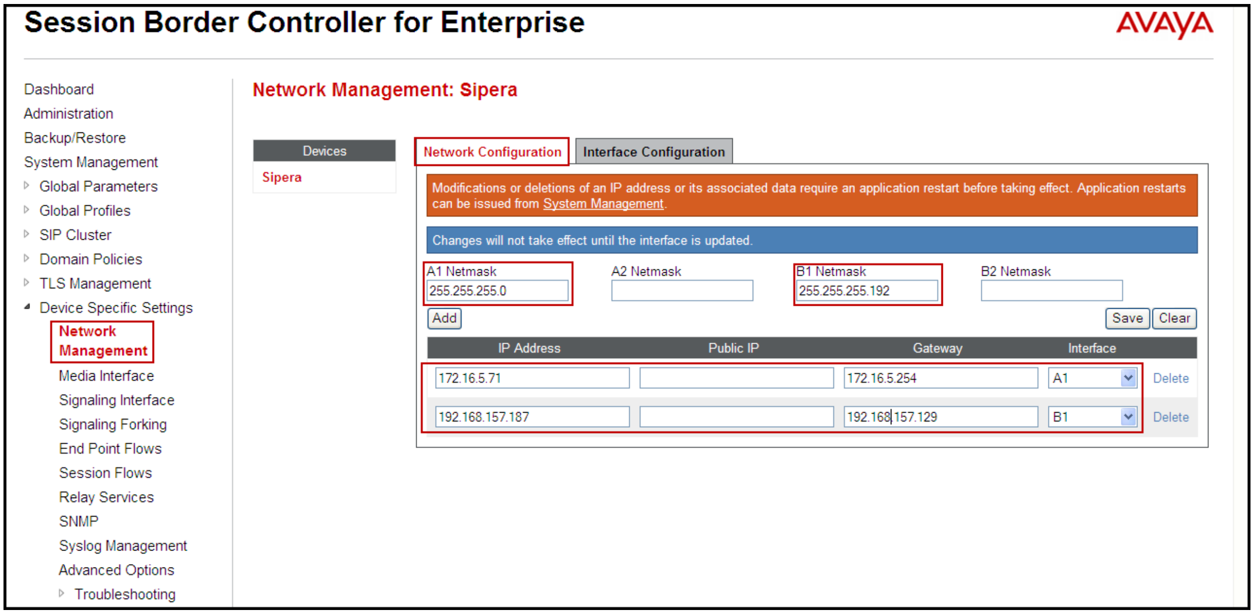


7.4. Device Specific Settings

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.

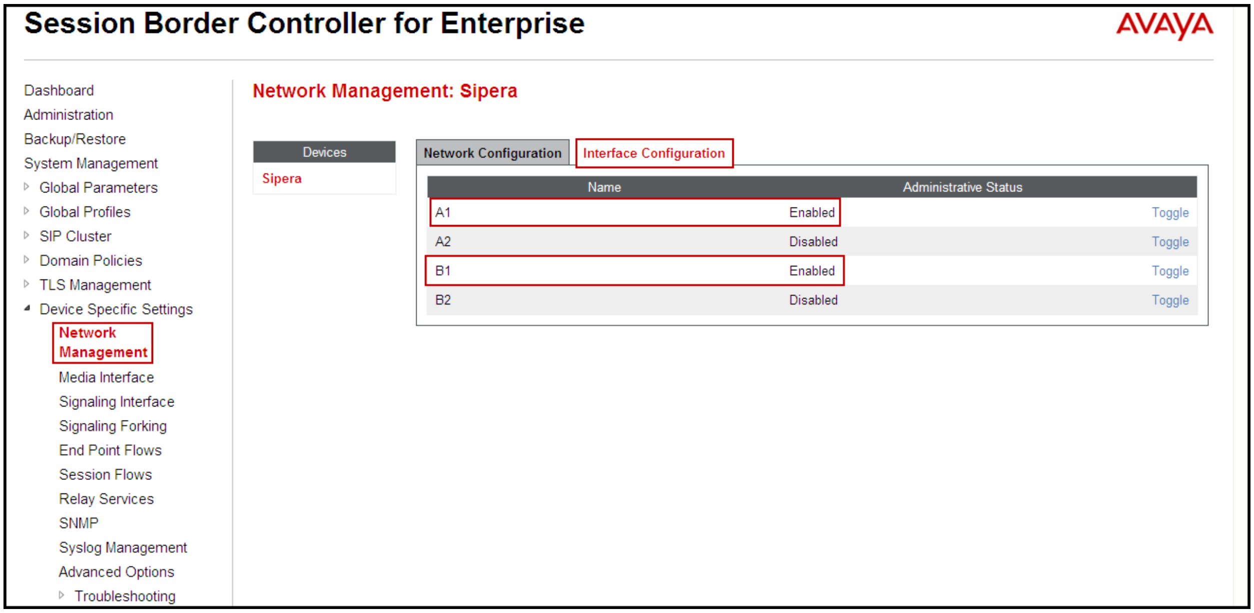
7.4.1. Network Management

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 **Network Configuration** tab.



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

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



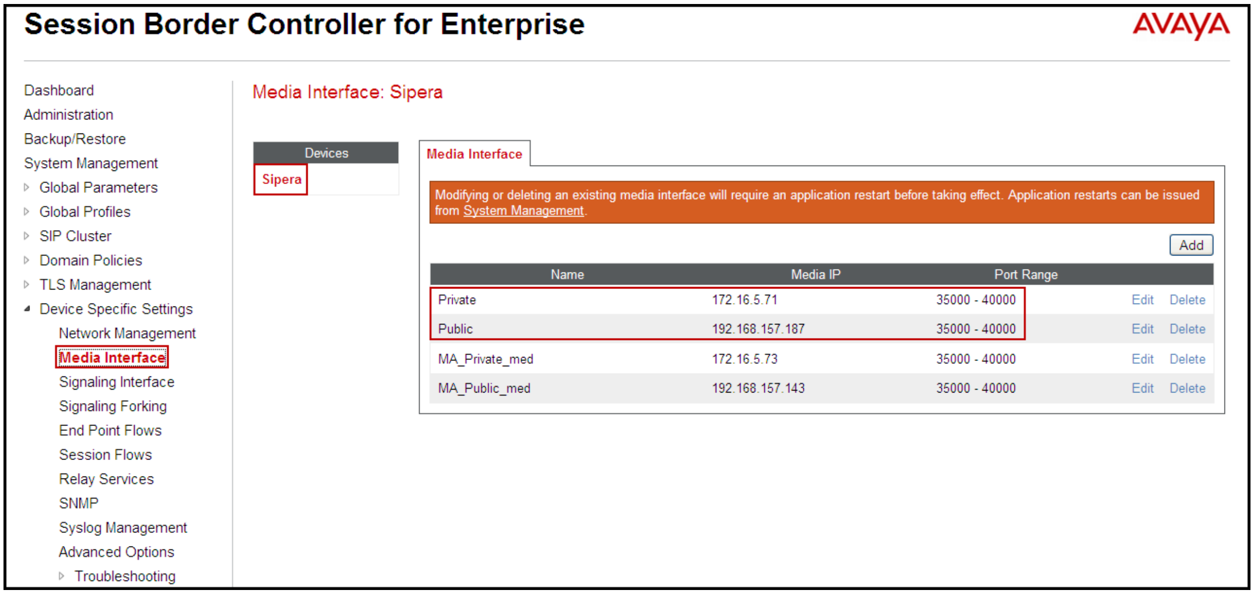
7.4.2. Media Interface

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, the port range of 35000 to 40000 was used.

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

- Select **Add Media Interface.**
- **Name: Private.**
- **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range: 35000-40000.**
- Click **Finish.**
- Select **Add Media Interface.**
- **Name: Public.**
- **IP Address: 192.168.157.187** (Outside IP Address of the Avaya SBCE, toward Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish.**

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

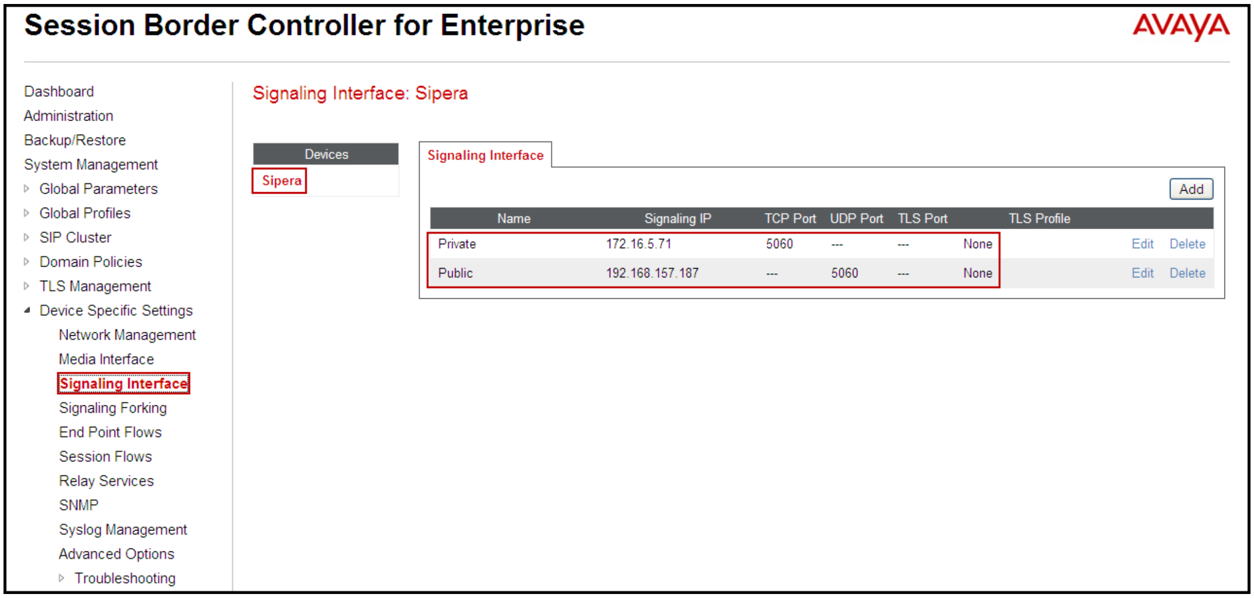


7.4.3. Signaling Interface

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

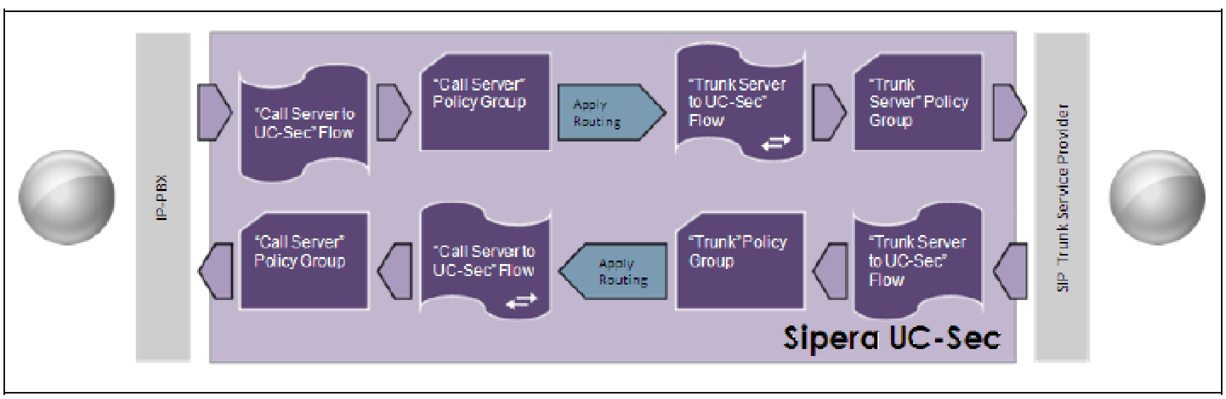
- Select **Add Signaling Interface**:
- **Name: Private.**
- **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **TCP Port: 5060.**
- Click **Finish.**
- Select **Add Signaling Interface**:
- **Name: Public**
- **IP Address: 192.168.157.187** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish.**

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



7.4.4. End Point Flows

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

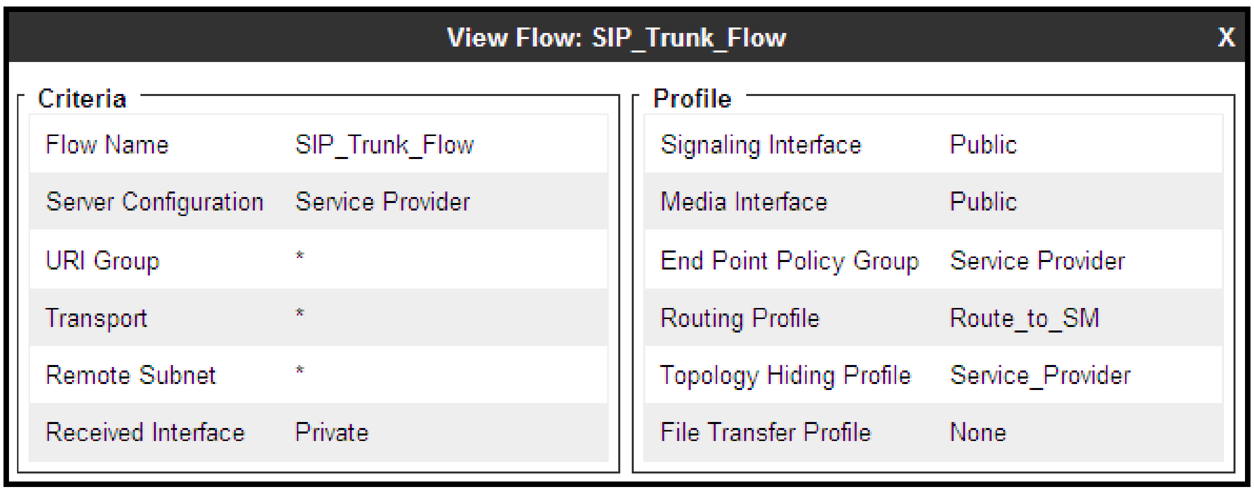


The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

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

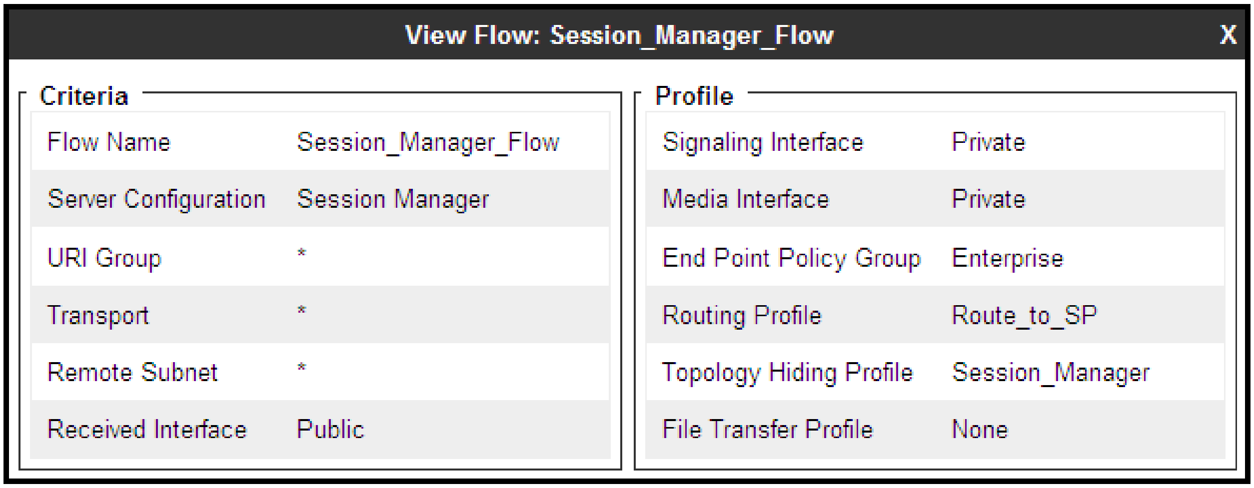
- **Name: SIP_Trunk_Flow.**

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

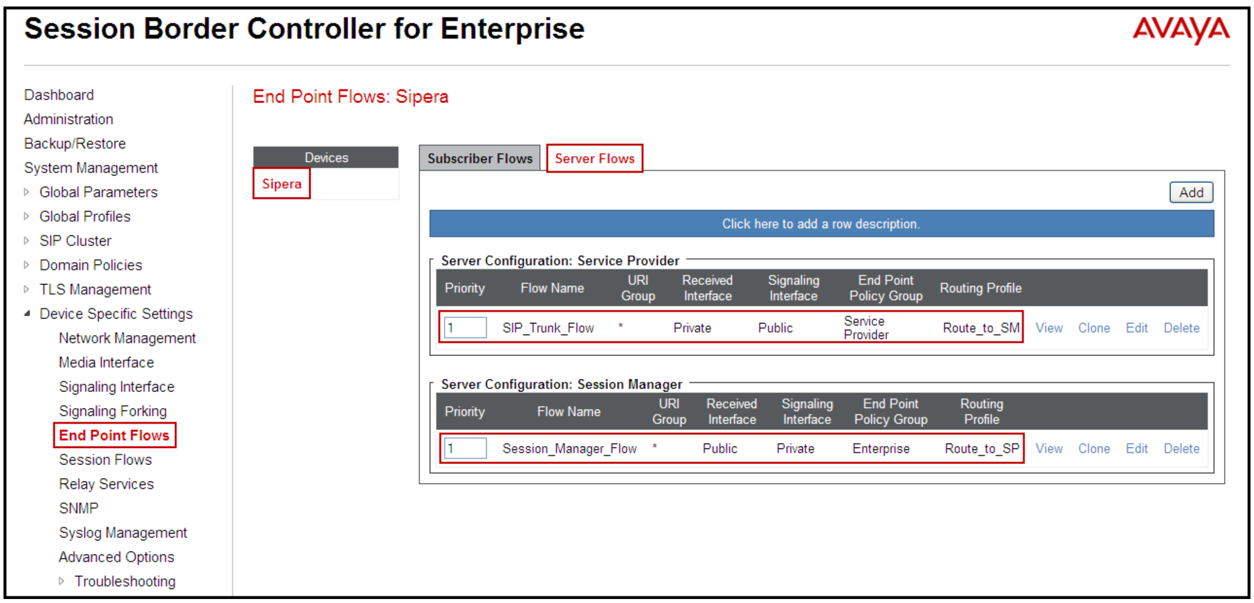


To create the call flow toward Session Manager, click **Add Flow**.

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



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



8. Hawaiian Telecom SIP Trunk Service Configuration

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

https://www.hawaiiantel.com/business/Business.aspx or by calling: 1-808-643-0944 and requesting information.

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

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

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

9.2. 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 in progress and/or idle. The call scenario involved the CS1000 extension 8000 calling a PSTN phone number (7861234567).

- 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**.
- After the call is released, issue the command **trac 0 8000** again to see if the DN is released back to an 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.

```
>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: 172.16.20.32  PORT: 5200
  FAR-END VendorID: Not available
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: 35032
  FAR-END VendorID: AVAYA-SM-6.3.1.0.631004
MEDIA PROFILE: CODEC G.729A NO-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 91786[illegible]
MAIN_PM  ESTD
TALKSLOT  ORIG  12   TERM  17    JUNCTOR  ORIG0   TERM0
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 309


----  ISDN ISL CALL (TERM) ----
CALL REF # =  395
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  808[illegible]  NUM_PLAN:E164    TON:NATIONAL  ESN:NPA
CALLED NO  =  1786[illegible]  NUM_PLAN:E164    TON:NATIONAL  ESN:NPA
```

The following screen shows an example after the call on 8000 has been released.

```
.trac 0 8000

IDLE VTN 008 0 00 00    MARP
```

The following screen shows an example after the call has been released, It shows that there are no trunks busy.

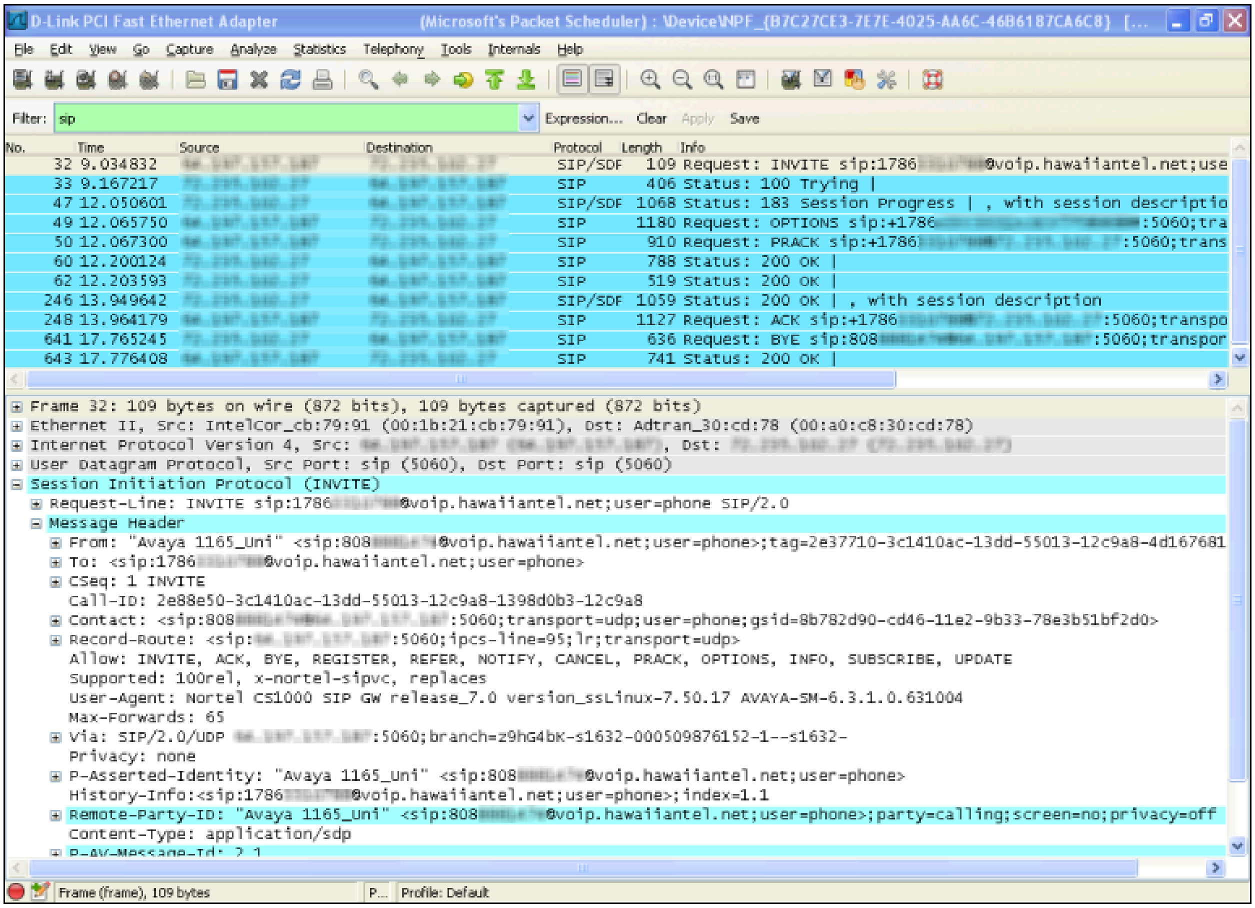
```
>ld 32
NPR000
.stat 48 0
012 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

9.3. Protocol Traces

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

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

The following screen shows an example of a typical capture for a call made from an 1165 Deskphone (DID: 8085551234) on the CS1000 to a PSTN number (7865551234).



10. Conclusion

These Application Notes describe the procedures necessary to Configure Hawaiian Telecom SIP Trunk service with Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 as shown in **Figure 1**.

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

11. References

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

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

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

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

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

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

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

[7] *Installing and Configuring Avaya Aura® System Platform*, Release 6.0.3, February 2011.

[8] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.

[9] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.

[10] *Installing and Configuring Avaya Aura® Session Manager*, April 2011, Document Number 03-603473.

[11] *Administering Avaya Aura® Session Manage*r, November 2010, Document Number 03-603324.

[12] *Sipera Systems E-SBC 1U Installation Guide*. Release 4.0.5.November 2011.

[13] *Sipera Systems E-SBC Administration Guide*. Release 4.0.5. November 2011.

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

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

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

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.