Avaya Solution & Interoperability Test Lab

Application Notes for Configuring CenturyLink BroadWorks SIP Trunk service with Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1 and Avaya Session Border Controller for Enterprise Release 4.0.5Q02 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between CenturyLink BroadWorks SIP Trunk service and Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1, Avaya Session Border Controller for Enterprise Release 4.0.5Q02.

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 in both directions with various Avaya endpoints.

The CenturyLink BroadWorks SIP Trunk service provides PSTN access via a SIP trunk between the enterprise and the CenturyLink 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

This document provides the steps to configure Session Initiation Protocol (SIP) Trunking between Avaya Communication Server 1000 and the CenturyLink BroadWorks SIP Trunk service (hereafter referred to as CenturyLink or CenturyLink system). During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure the interoperability between the CenturyLink system and the Avaya CS1000.

In the sample configuration, the Avaya CS1000 solution consists of a CS1000 Rel. 7.5 (hereafter referred to as CS1000) , Avaya Aura® Session Manager Rel. 6.1 (hereafter referred to as Avaya Aura® Session Manager), Avaya Session Border Controller for Enterprise Rel. 4.0.5Q02 (hereafter referred to as Avaya SBCE) , and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya SBCE or Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The CS1000 system was connected to an Avaya SBCE via SIP trunks to the Avaya Aura® Session Manager. The Avaya SBCE was connected to the CenturyLink system via a SIP trunk. Various call types were made from the CS1000 to the CenturyLink system and vice versa to ensure interoperability between the CS1000 and the CenturyLink system.

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

2.1. Interoperability Compliance Testing

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

- Static IP.
- Incoming calls from the PSTN were routed to the DID numbers assigned by CenturyLink. Incoming PSTN calls were terminated to the following end points: Avaya 1100 Series 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 the CenturyLink BroadWorks network to the various PSTN destinations.
- 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 (w/voice mail off).
- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.

- Codec G.711u with VAD disabled. (CenturyLink only supports Codec G.711u).
- Voice mail and DTMF tone support in both directions (RFC2833) (Leaving voice mail, retrieving voice mail, etc.).
- CallPilot Voice Mail Server (Hosted in the CS1000).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- International calls.
- Calls to special numbers (411, 711, 911, Operator (0), 0+10 digits Operator Assisted calls, etc.).
- 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.
- G.711u fax pass-through support (inbound and outbound) (CenturyLink does not support T.38)
- Long duration calls (one hour).
- Early Media transmission

2.2. Test Results

Interoperability testing of CenturyLink BroadWorks SIP Trunk Service with the Avaya 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).
- **Calling Name Blocking:** In the CS1000, the "Calling Name" can be blocked/restricted from being displayed at the PSTN extension. With this setting enabled on the CS1000 extension, the CS1000 will send the "Calling Number" in the "From" header of the INVITE message and will set the Privacy to "user" (Privacy: user) in the same INVITE message. The expected result is the display of only the number and not the name. The actual result is the blocking of the number. Since the name was never delivered to the PSTN, as indicated above, neither the name nor the number are displayed at the PSTN extension with Calling Name restriction enabled on the CS1000 extension.
- **Blind Transfer of calls from the CS1000 to the PSTN:** Blind Transfers of calls from the CS1000 to the PSTN were failing with the BroadWorks switch sending a "500 Server Internal Error" in response to the UPDATE sent to the BroadWorks switch by the CS1000. The problem is that the CS1000 sends an UPDATE to the BroadWorks switch "before" the completion of the initial INVITE transaction, with this INVITE containing an offer. Per **RFC3311** an UPDATE cannot be sent with an offer unless the callee has generated an answer in a reliable provisional response. The INVITE needs to be answered by the CS1000 with a PRACK "before" sending the UPDATE. The solution to this problem is to apply patch **p30224_1.ntl** to the CS1000 Signaling Server (Linux) and

to upgrade the Signaling Server to the latest **VTRK** SU version. Version cs1000-vtrk-7.50.17.16-**34**.i386.000.ntl was used in the Avaya lab during testing. Also, testing was done with Plug-In **201 enabled** and Plug-In **501 disabled**. For the information on how to obtain and how to apply the patch please visit http://support.avaya.com

- **SIP Diversion Header for call re-direction:** CenturyLink does not support History-Info, instead requires SIP Diversion Header for calls that are re-directed at the CS1000. Session Manager was used to convert History-Info to SIP Diversion Header. This can be accomplished by using adaptation modules in Session Manager.
- **Caller-ID on re-directed calls to PSTN:** Caller ID works properly between the CS1000 and the CenturyLink 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., transfer) and not the Caller ID of the extension that originated the call. On the CenturyLink network, the PAI header is used to authenticate the call during call redirection scenarios. When a call is re-directed, the PAI header will be populated with the information of the extension that is doing the call redirection.
- **Routing Profiles:** When configuring Routing Profiles in the Avaya SBCE (**Section 7.3.2**), the selection of **Use Next Hop for In Dialog Messages** should **not** be checked. In the current software release of the Avaya SBCE (Release **4.0.5Q02**), when this field is not checked, messaging problems with the SIP **BYE** method where observed in between the Avaya SBCE and Avaya Aura® Session Manager. In order to correct this problem in the current software release of the Avaya SBCE (Release **4.0.5Q02**) patch **ipcs-bin-mvista_debug_20120413150346-2.i386.rpm** must be applied to the Avaya SBCE. The fix will be included in the next software release of the Avaya SBCE (Release **4.0.5Q09**). For the information on how to obtain and how to apply the patch please contact Avaya SBCE support at: **866-861-3113 toll free or +1 214-269-2424.**
- **SIP Header Optimization:** SIP header rules were implemented in the 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 and History-info if it is present in the INVITE. Also the multipart MIME SDP, which included 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.

2.3. Support

For technical support on CenturyLink system, please contact CenturyLink technical support at:
Toll Free: 1-877-290-5458

http://www.centurylink.com/Pages/Support/

3. Reference Configuration

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

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

- Avaya Communication Server 1000-E (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.
- Desk top with administration interfaces.

Located at the edge of the enterprise is the Avaya Session Border Controller for Enterprise (Avaya SBCE). It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and CenturyLink across the public IP network is SIP over UDP. The transport protocol between the Avaya SBCE and Avaya Aura® Session Manager across the enterprise IP network is SIP over TCP. The transport protocol between Avaya Aura® 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 Avaya Aura® 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 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 the Avaya Aura® Session Manager to carry the traffic to and from the service provider (two-way trunk group).

For inbound calls, the calls flowed from the CenturyLink network to the Avaya SBCE then to Avaya Aura® Session Manager. Avaya Aura® 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 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 Avaya Aura® Session Manager. The Avaya Aura® Session Manager once again used the configured dial patterns, adaptations, and routing policies to determine the route to the Avaya SBCE for egress to the CenturyLink network.

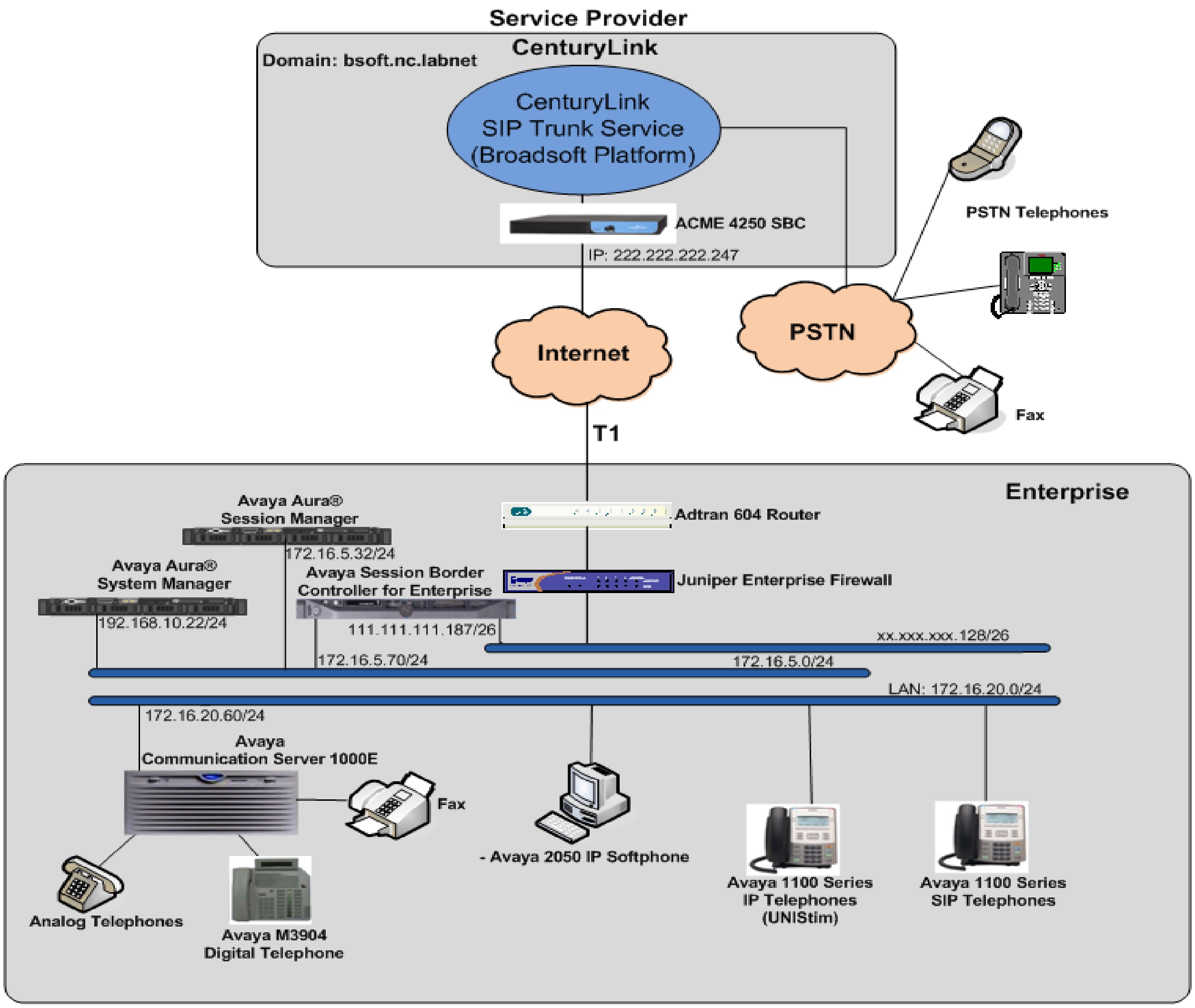


Figure 1: CenturyLink BroadWorks SIP Trunk service and Avaya CS1000E

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: 2012-01-10 16:47:54 (est)) Signaling Server: 7.50.17.00 **See Service Updates & Patches below**
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.1 service pack 5 (ASM 6.1.5.0.615006)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.1 Service Pack 5 Build No. 6.1.0.0.7345-6.1.5.502
Avaya Session Border Controller for Enterprise (Avaya SBCE)	4.0.5Q02
Avaya Phones	1110: 0623C8G (UniStim) 1120: 0624C8G (UniStim) 1165: 0626C8G (UniStim) 1120: 04.01.15.00 (SIP) M3904: --
Lucent Analog Phone	--
Fax Machines	--
CenturyLink:	
Equipment	**Release/Version**
BroadWorks Broadsoft	17 sp2
Sonus NBS	B07.02.07 F004
Sonus GSX	B07.02.07 F004
Acme Packet Net-Net 4250 Session Border Controller	SC6.1.0 MR-5 GA (Built 704)

Signaling Server Service Updates & Patches:
##
SUs:
cs1000-patchWeb-7.50.17.16-4.i386.000
cs1000-baseWeb-7.50.17.16-1.i386.001
ipsec-tools-0.6.5-14.el5.3_avaya_1.i386.000
cs1000-dbcom-7.50.17-02.i386.000
cs1000-shared-pbx-7.50.17.16-1.i386.000
cs1000-kcv-7.50.17.16-1.i386.000
cs1000-ipsec-7.50.17.16-1.i386.000
cs1000-linuxbase-7.50.17.16-6.i386.000

spiritAgent-6.1-1.0.0.108.208.i386.000
cs1000-EmCentralLogic-7.50.17.16-1.i386.000
cs1000-csmWeb-7.50.17.16-3.i386.000
cs1000-mscAnnc-7.50.17.16-1.i386.000
cs1000-mscTone-7.50.17.16-1.i386.000
cs1000-mscMusc-7.50.17.16-2.i386.000
cs1000-dmWeb-7.50.17.16-2.i386.000
tzdata-2011h-2.el5.i386.000
cs1000-Jboss-Quantum-7.50.17.16-10.i386.000
cs1000-sps-7.50.17.16-2.i386.000
cs1000-tps-7.50.17.16-11.i386.000
cs1000-ftrpkg-7.50.17.16-7.i386.000
cs1000-bcc-7.50.17.16-46.i386.000
cs1000-vtrk-7.50.17.16-34.i386.000
cs1000-emWeb_6-0-7.50.17.16-16.i386.000
####################
Patches:
p30224_1
####################

Note: The **VTRK** SU version should be "cs1000-vtrk-7.50.17.16-**15**.i386.000.ntl" or higher on all Signaling Servers to ensure proper operation of the blind transfer feature. Patch **p30224_1** is also required if problems with SIP **UPDATE** are observed during Call Redirection scenarios.

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

Enable Plug-In **201** and ensure Plug-In **501** is **disabled** as follows:
Log in 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**. Verify the status for **plug-in 501** shows **Disabled**.

5. Configure Avaya Communication Server 1000

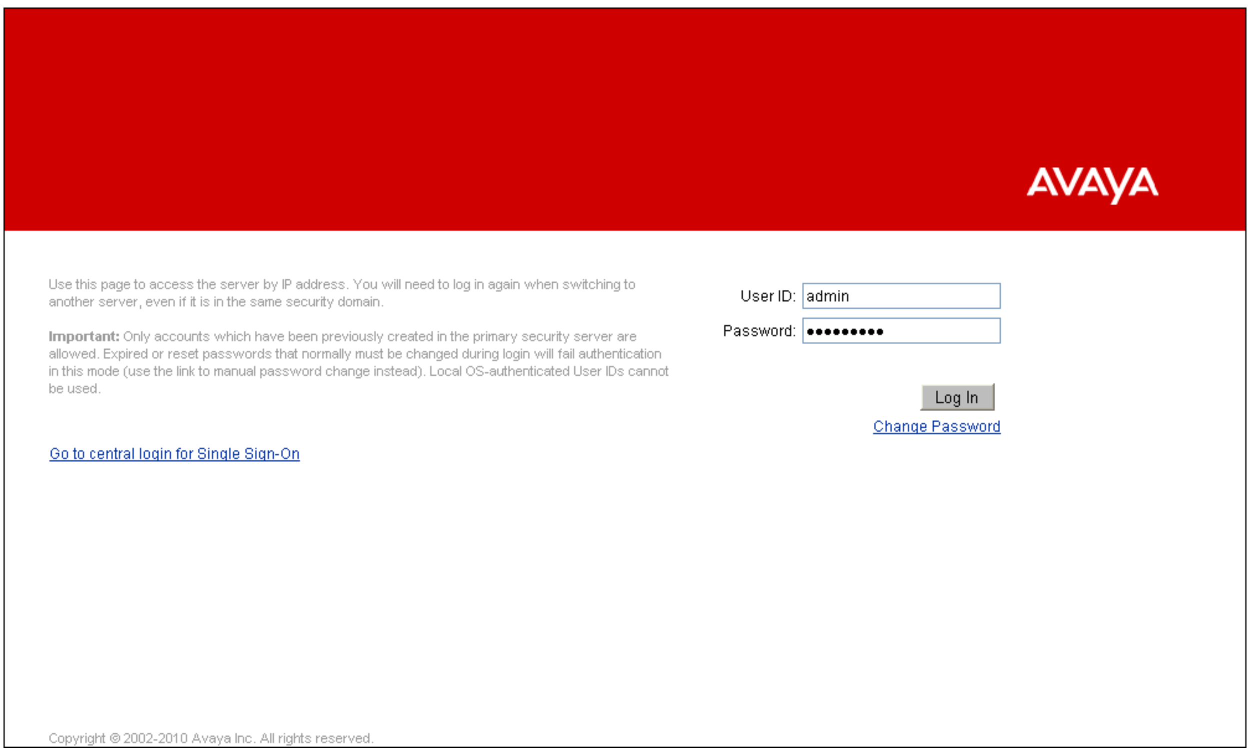
These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 11.**

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

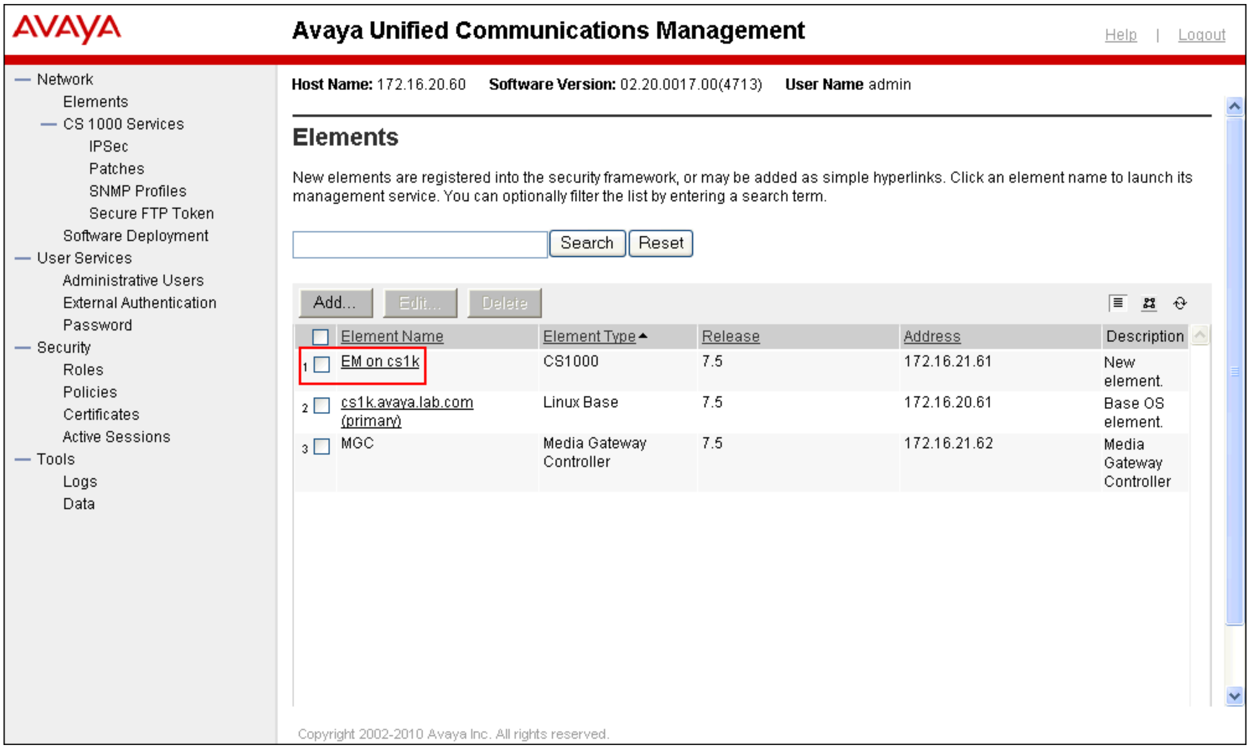
5.1. Log in to the CS1000 System

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

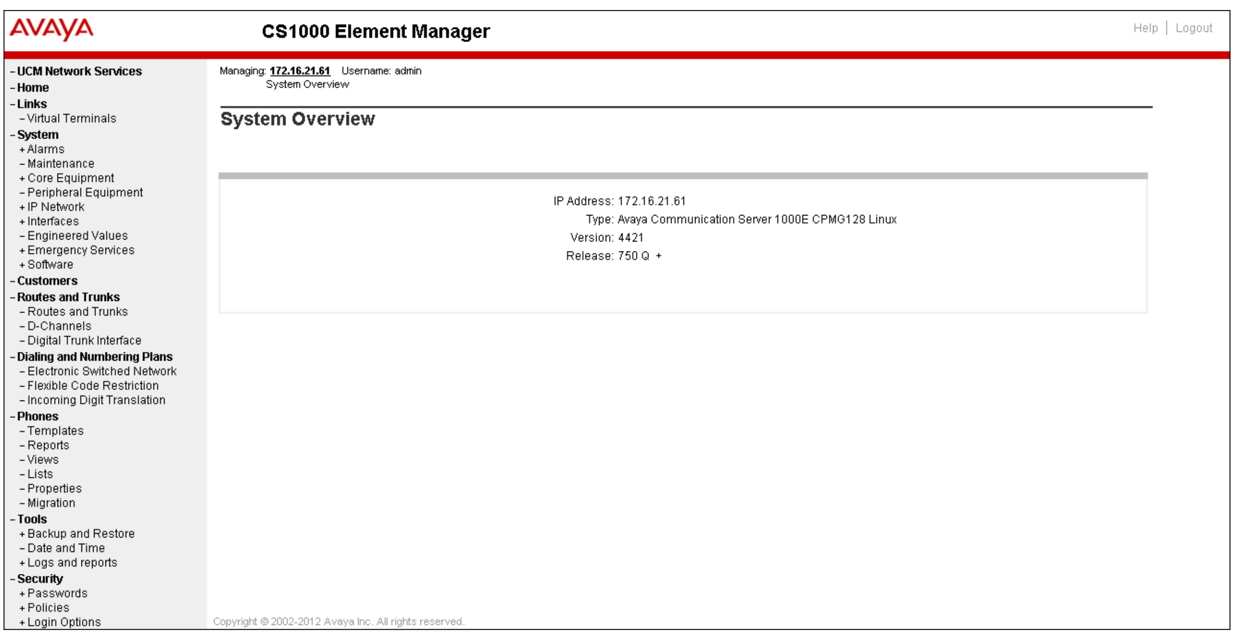
Open an instance of a web browser and connect to the UCM GUI at the following address: http://<UCM IP address> Log in using an appropriate Username and Password.



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. Log in to the Call Server Command Line Interface (CLI)

Using Putty, SSH to the IP address of 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
>
```

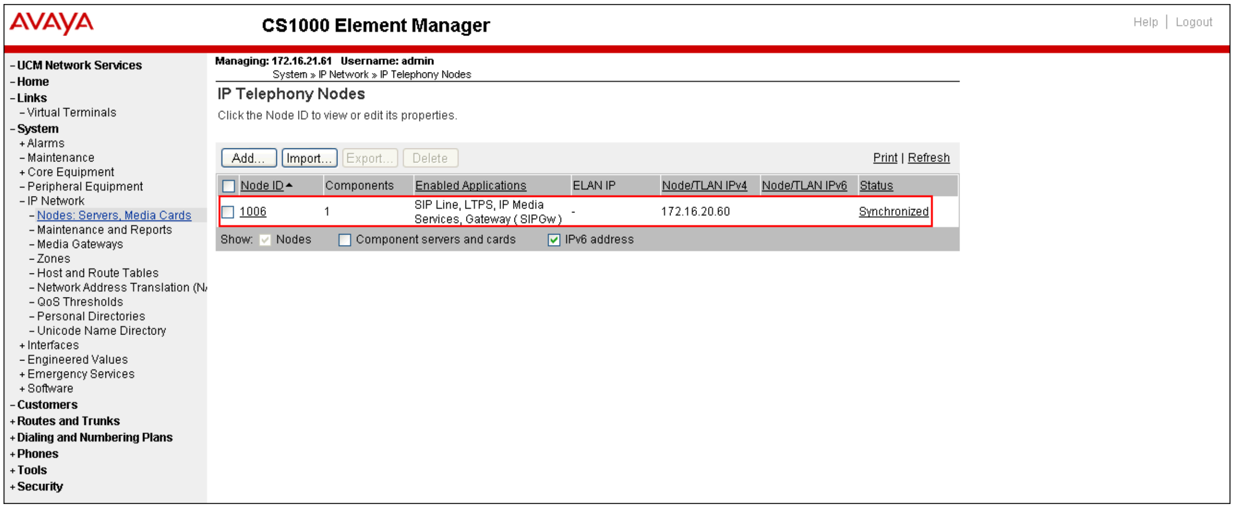
5.2. Administer a IP Telephony Node

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

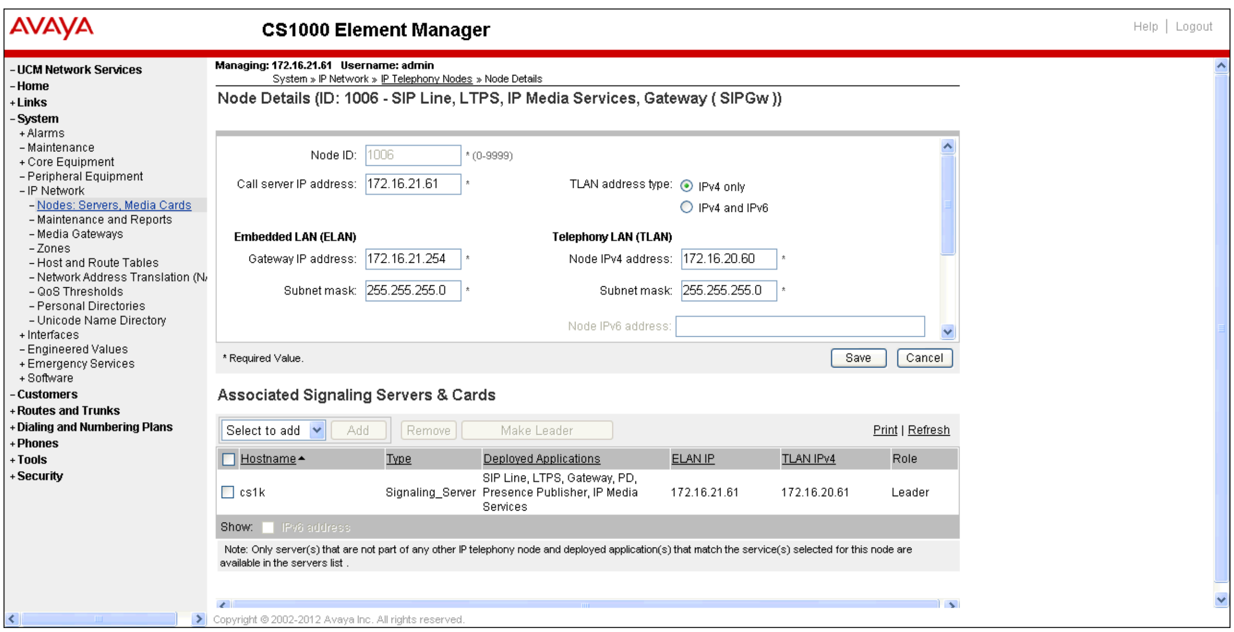
5.2.1. Obtain Node IP address

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

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

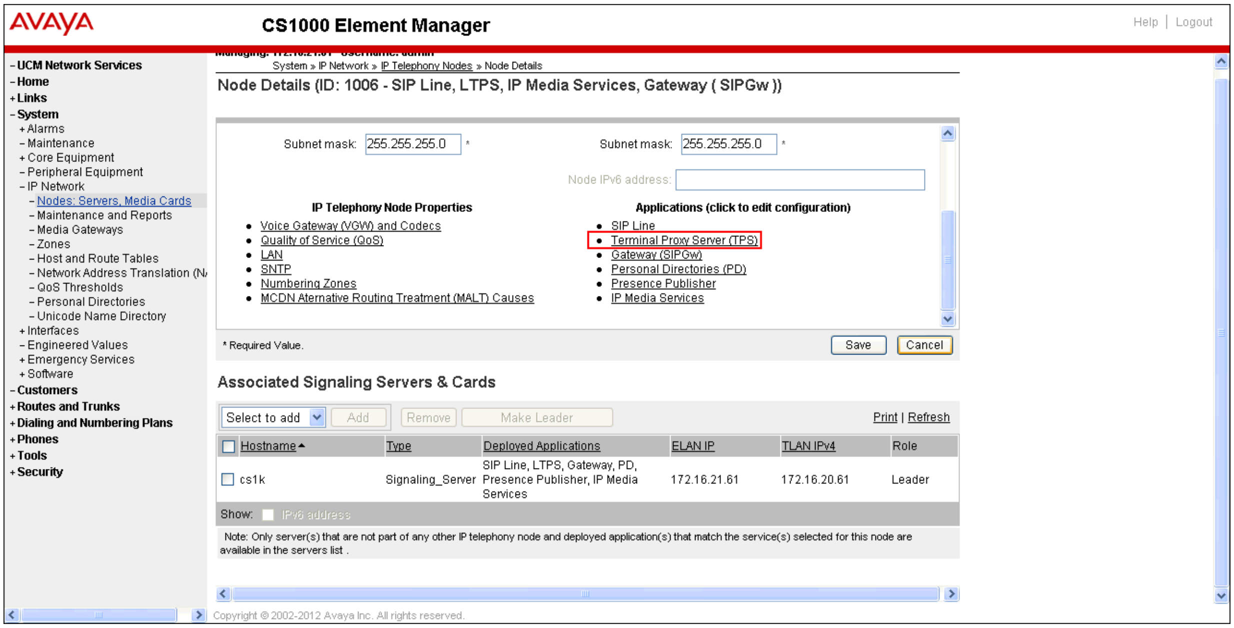


The **Node Details** screen is displayed as shown below with the IP address of the CS1000 node. The **Node IP Address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IP Address** to communicate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

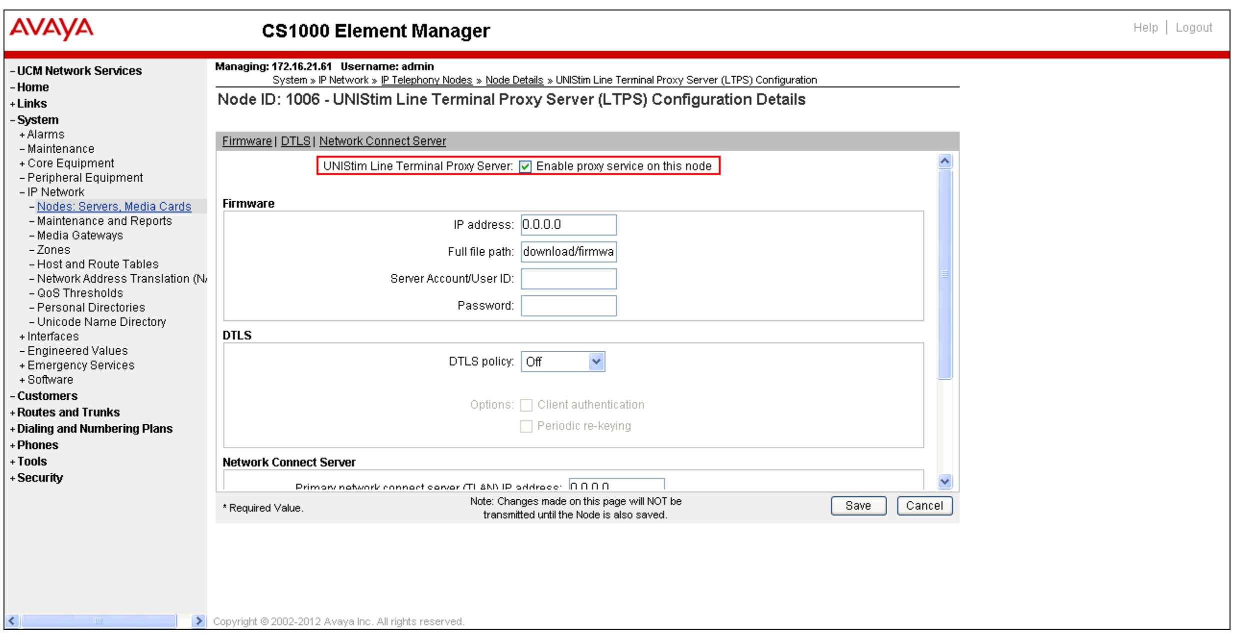


5.2.2. Administer TPS

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

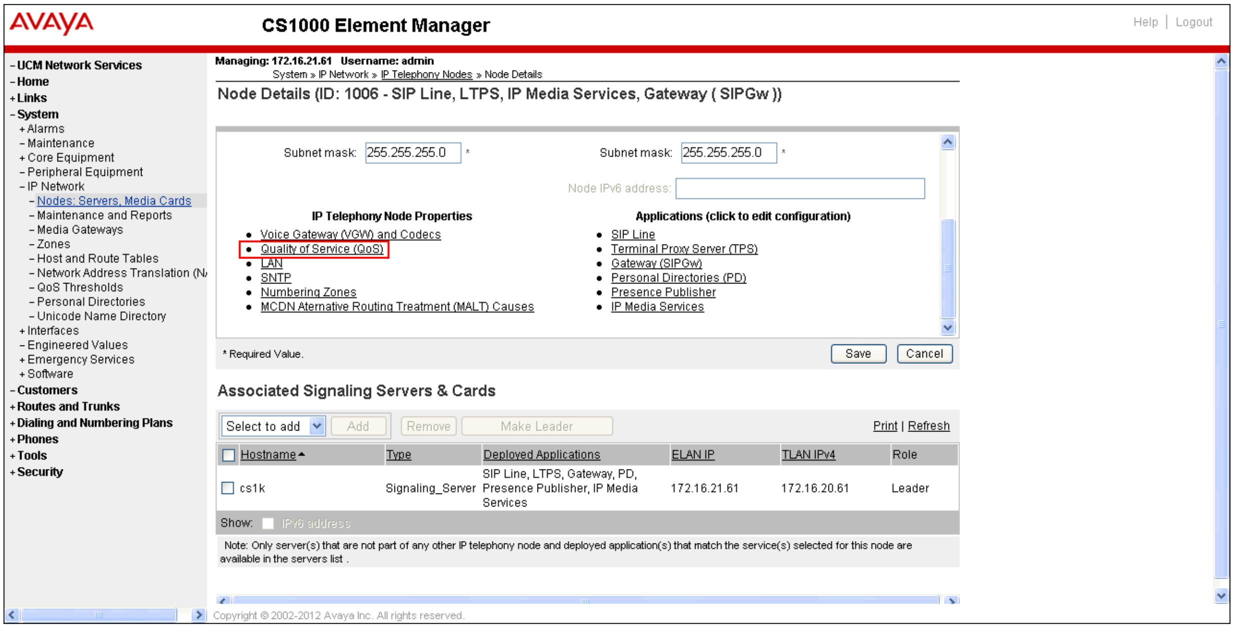


The **UNIStim Line Terminal Proxy Server (LTPS) Configuration Details** screen will be displayed as shown below. Check the **Enable proxy service on this node** check box and then click **Save**.

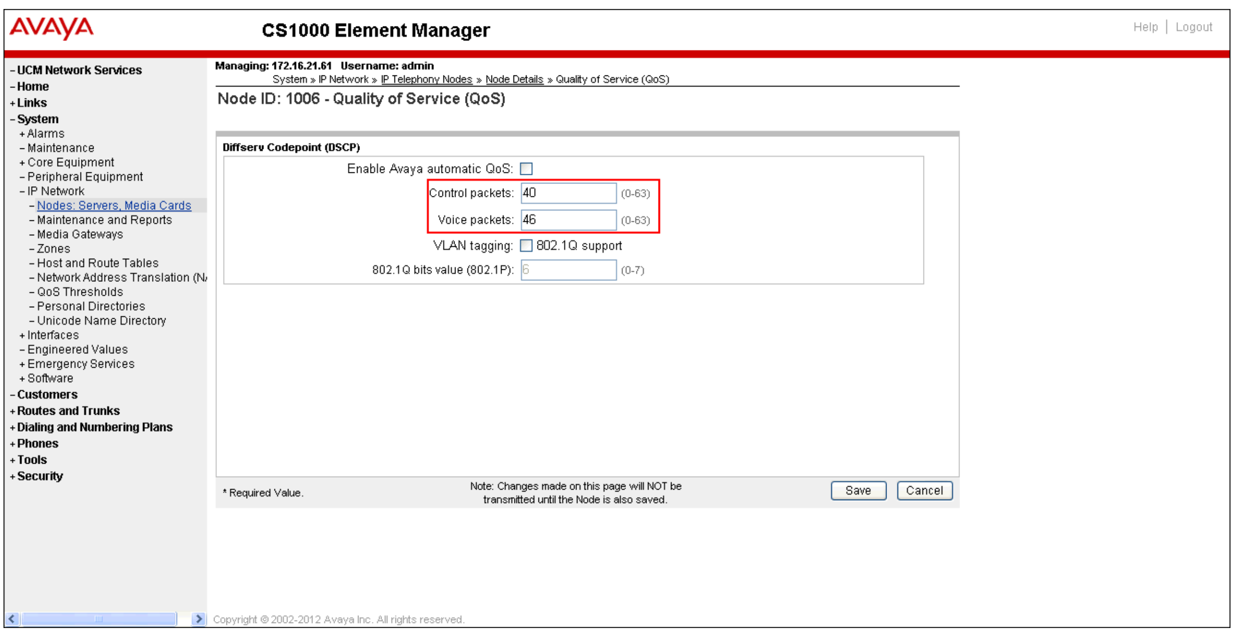


5.2.3. Administer Quality of Service (QoS)

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

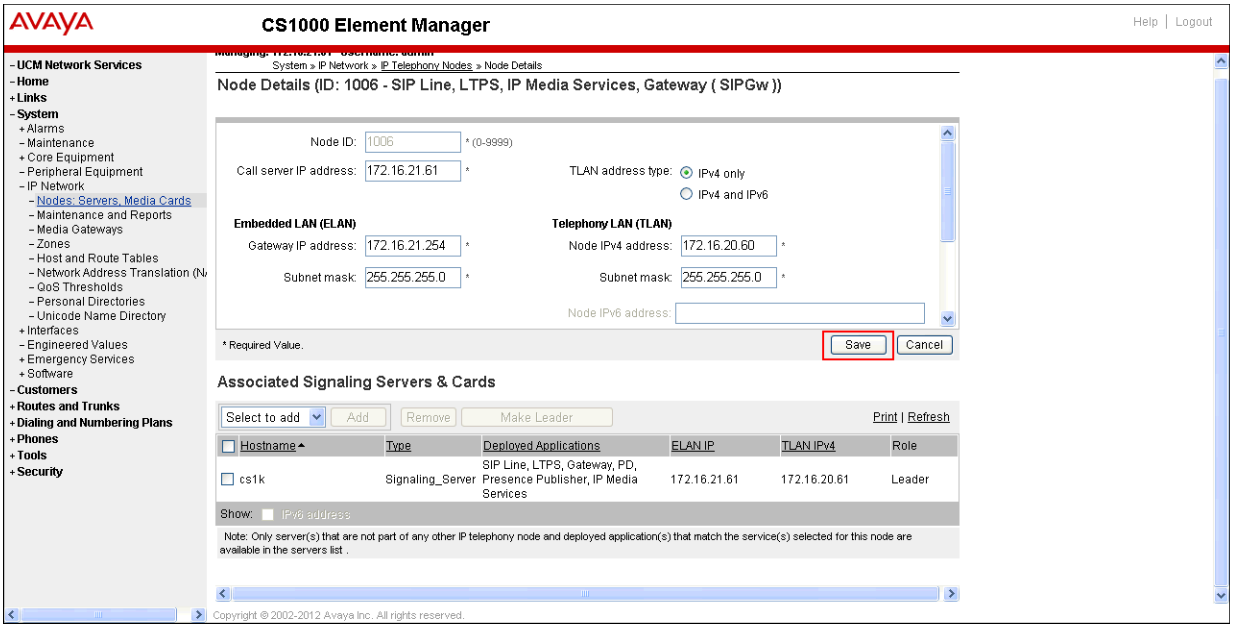


The **Quality of Service (QoS)** screen shown below will be displayed. Accept the default Diffserv values. Click the **Save** button.



5.2.4. Synchronize the New Configuration

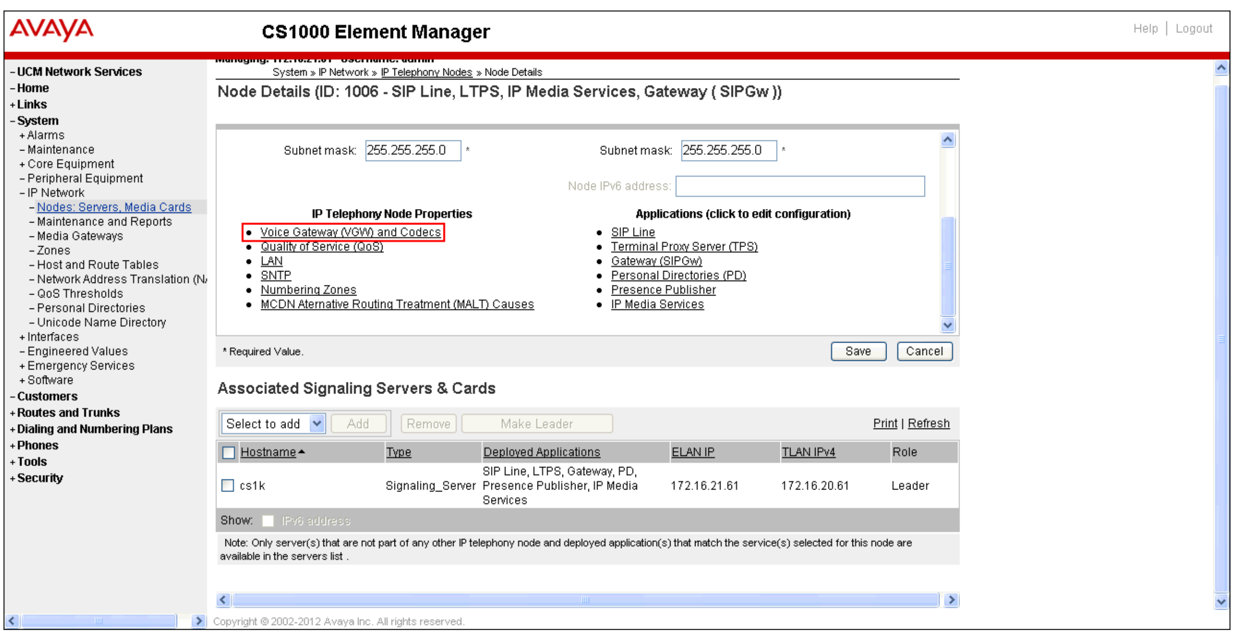
Continue from **Section 5.2.3**, return to the **Node Details** page shown below and click on the **Save** button. The **Node Saved** screen is displayed. Click on **Transfer Now** (not shown). The **Synchronize Configuration Files** screen is displayed (now shown). Check the Signaling Server check box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



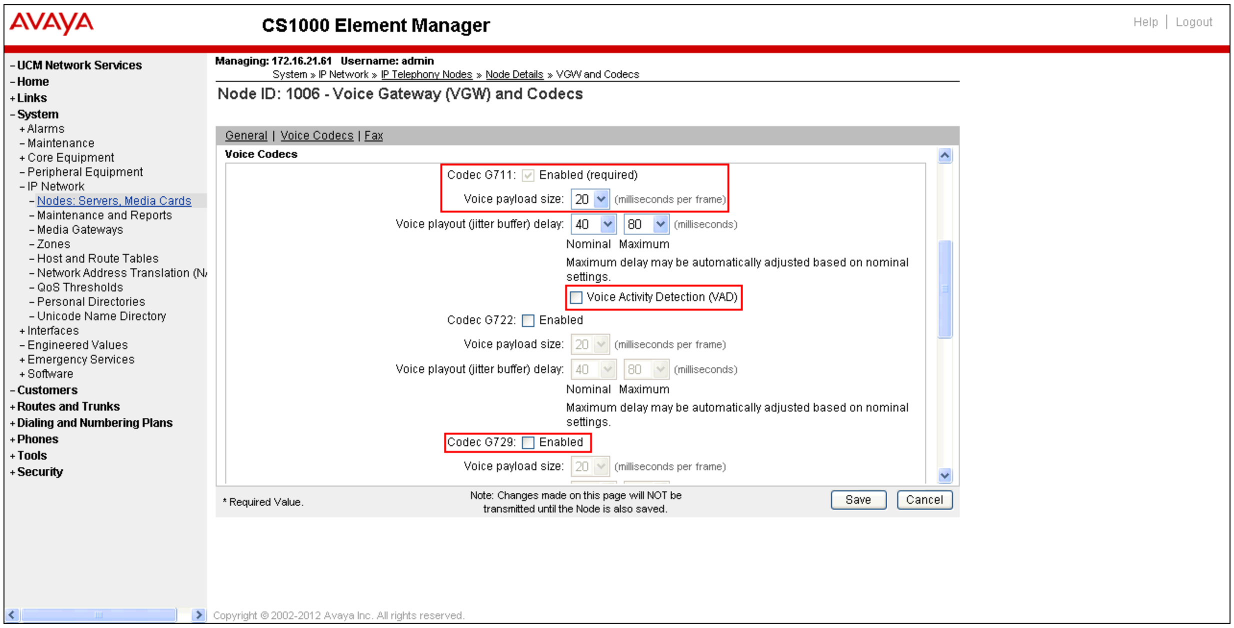
5.3. Administer Voice Codec

5.3.1. Enable Voice Codec, IP Telephony Node.

Select **IP Network → Nodes: Servers, Media Cards** Configuration from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed. On the **Node Details** page shown below, click on **Voice Gateway (VGW) and Codecs.**

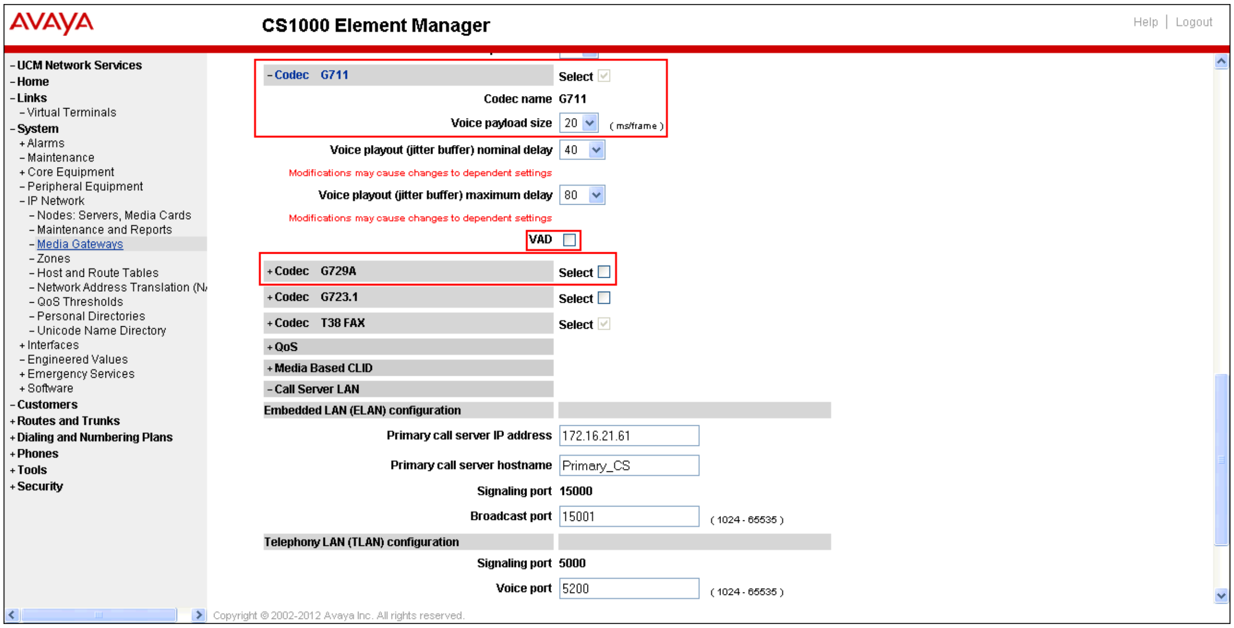


The **Voice Gateway (VGW) and Codecs** screen will be displayed as shown below. The CenturyLink system only supports **G711u** with **VAD** disabled. The CenturyLink system does not support **G729**. Ensure that for **G711** the **Voice Activity Detection (VAD)** is unchecked; uncheck Codec **G729** checkboxes as shown below. Click on **Save** and Synchronize as described in **Section 5.2.4**.

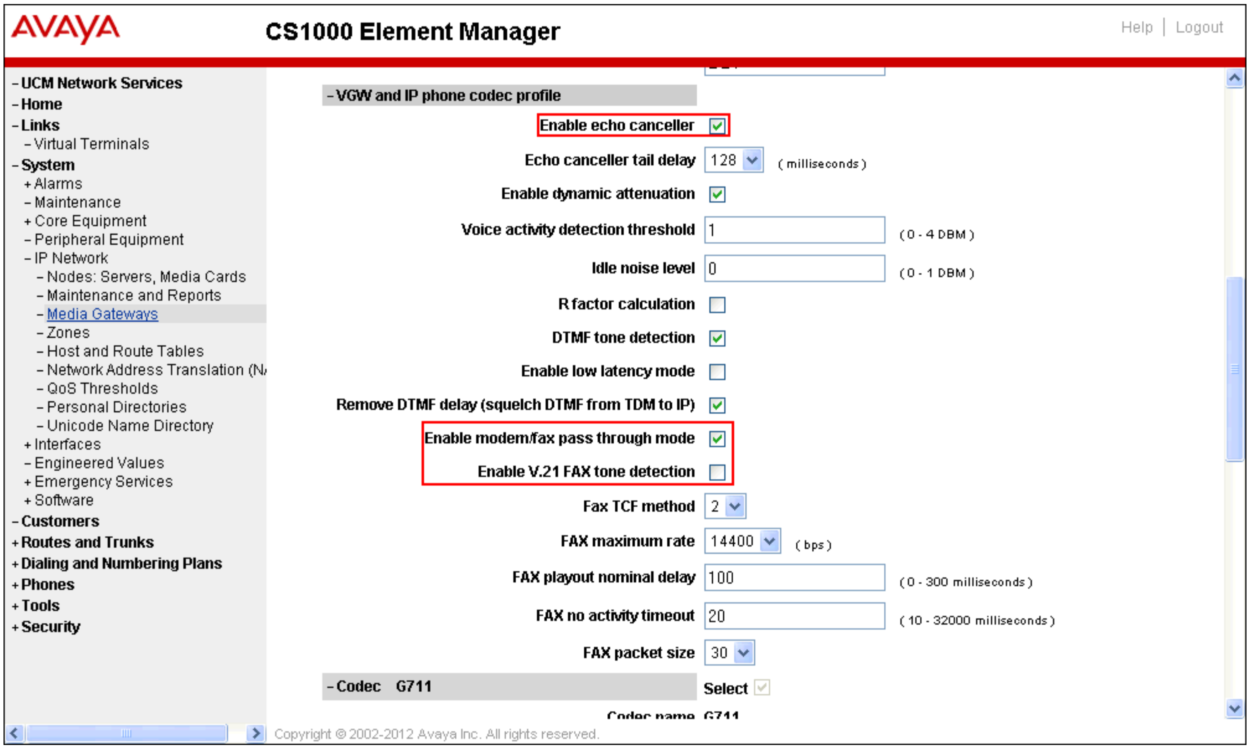


5.3.2. Enable Voice Codec on Media Gateways.

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



For Fax over IP, CenturyLink does not support **T.38**, only **G.711u pass-through**. G.711 was chosen as the default codec. Ensure that **Enable V.21 FAX tone detection** is unchecked, and that **Enable modem fax pass through mode** is checked. This configuration enables G.711 pass through codec for fax.

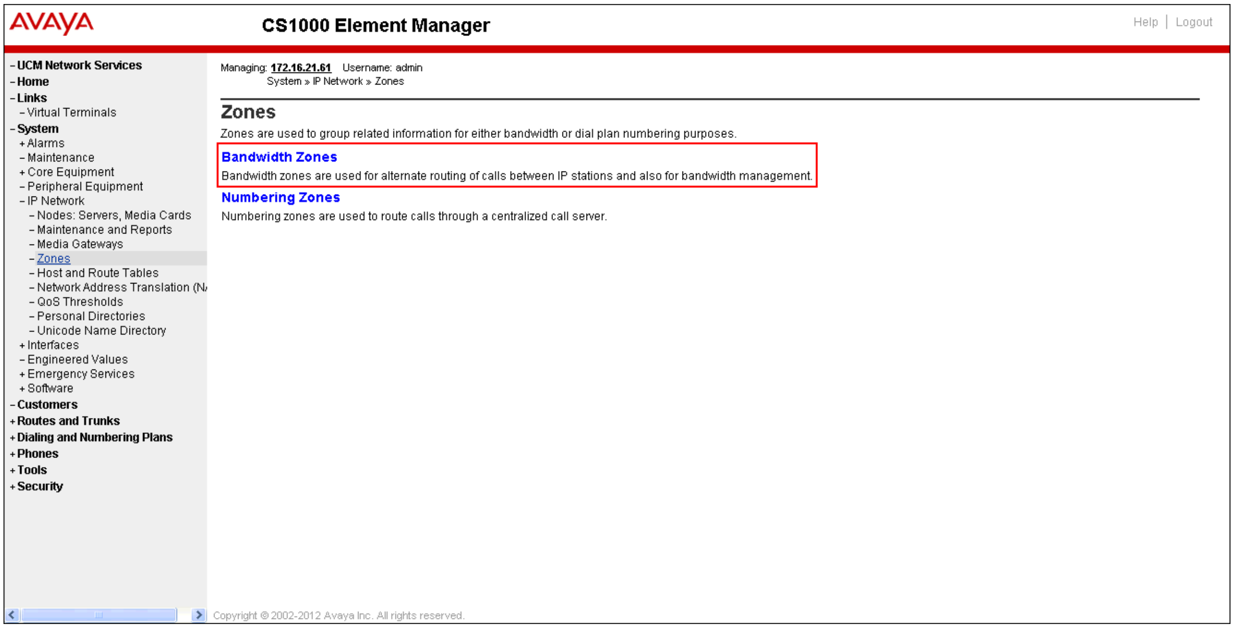


5.4. Administer Zones and Bandwidth

This section describes the steps to create 2 zones: **zone 5** for IP sets and **zone 4** for IP SIP Trunk.

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

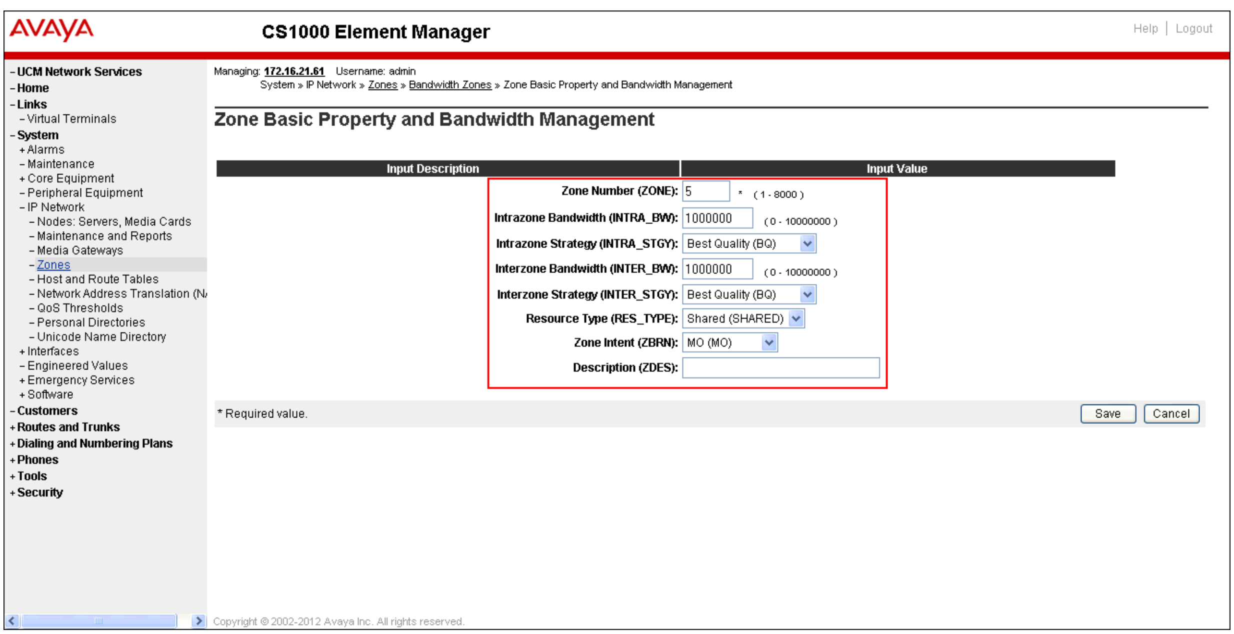
The following figures show how to configure a zone for IP sets for bandwidth management purposes. The bandwidth strategy can be adjusted to preference. Select **IP Network → Zones** configuration from the left pane, click on the **Bandwidth Zones** as shown below.



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

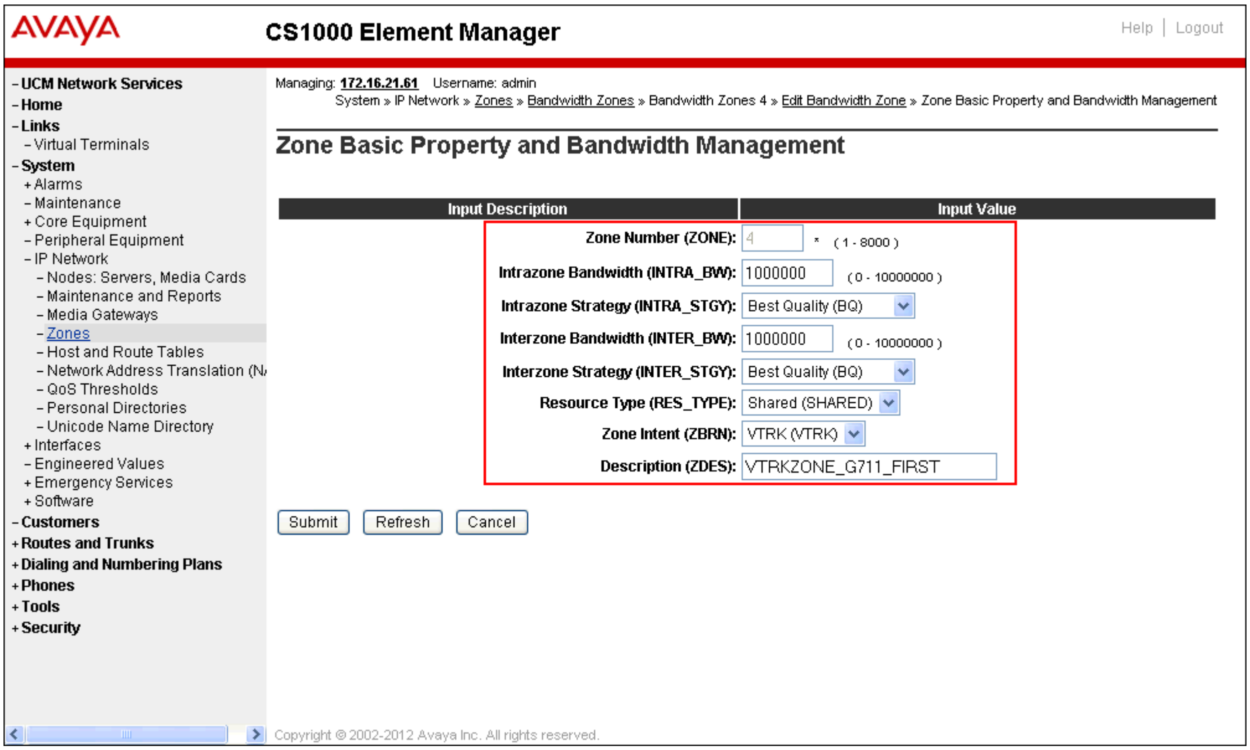
- **INTRA_STGY**: Bandwidth configuration for local calls, select **Best Quality (BQ).**
- **INTER_STGY**: Bandwidth configuration for the calls over trunk, select **Best Quality (BQ).**
- **ZBRN: Select MO** (**MO** is used for IP phones).

Note: BQ will use **G711** as first choice and **G729** as second choice. **BB** will use **G729** as first choice and G711 as second choice.



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

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

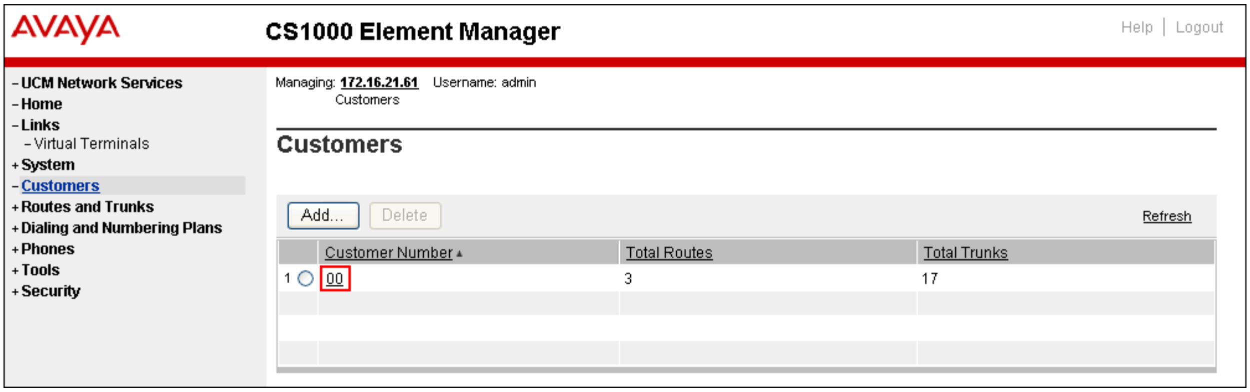


5.5. Administer SIP Trunk Gateway

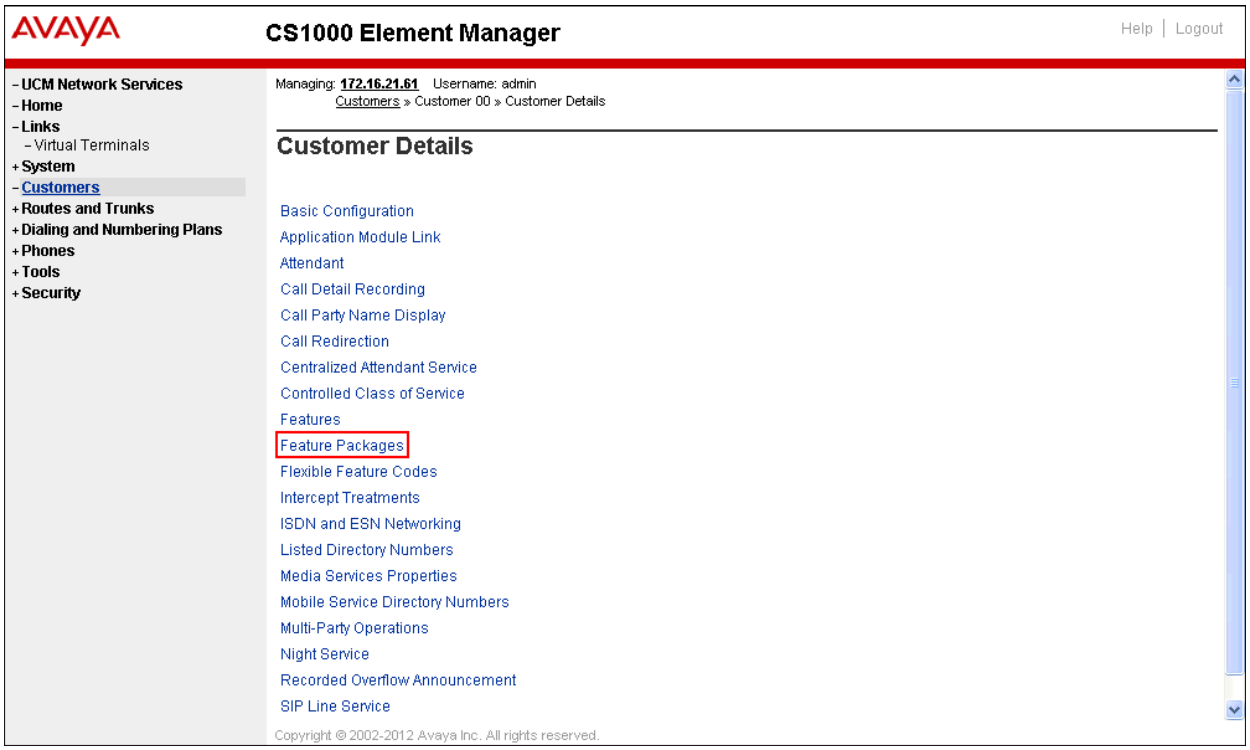
This section describes the steps for establishing a SIP IP connection between the SIP Signaling Gateway (SSG) and Session Manager (SM).

5.5.1. Integrated Services Digital Network (ISDN)

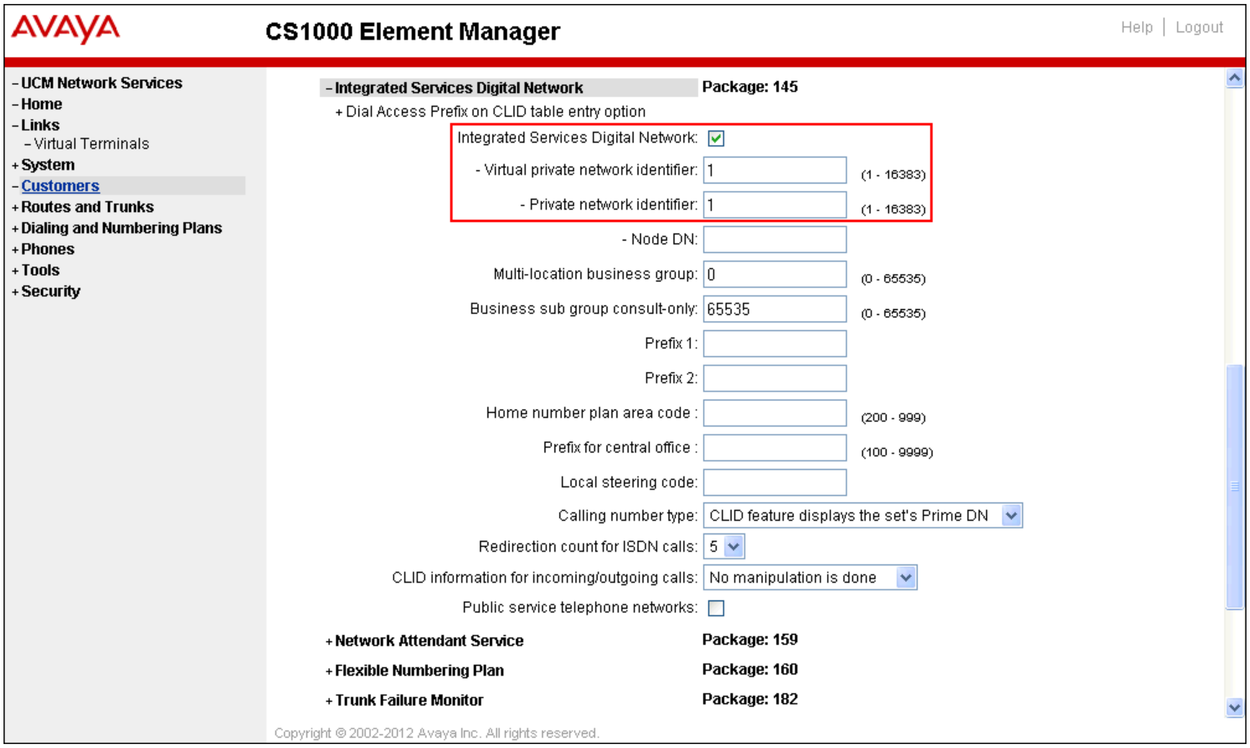
Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options.



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



The screen is updated with a list of **Feature Packages** populated on the CS1000. Select **Integrated Services Digital Network** to edit its parameters. The screen is updated with parameters populated below **Integrated Services Digital Network**. Check the **Integrated Services Digital Network** (ISDN) checkbox, and retain the default values for all remaining fields as shown below. Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page.



5.5.2. Administer the SIP Trunk Gateway to Session Manager

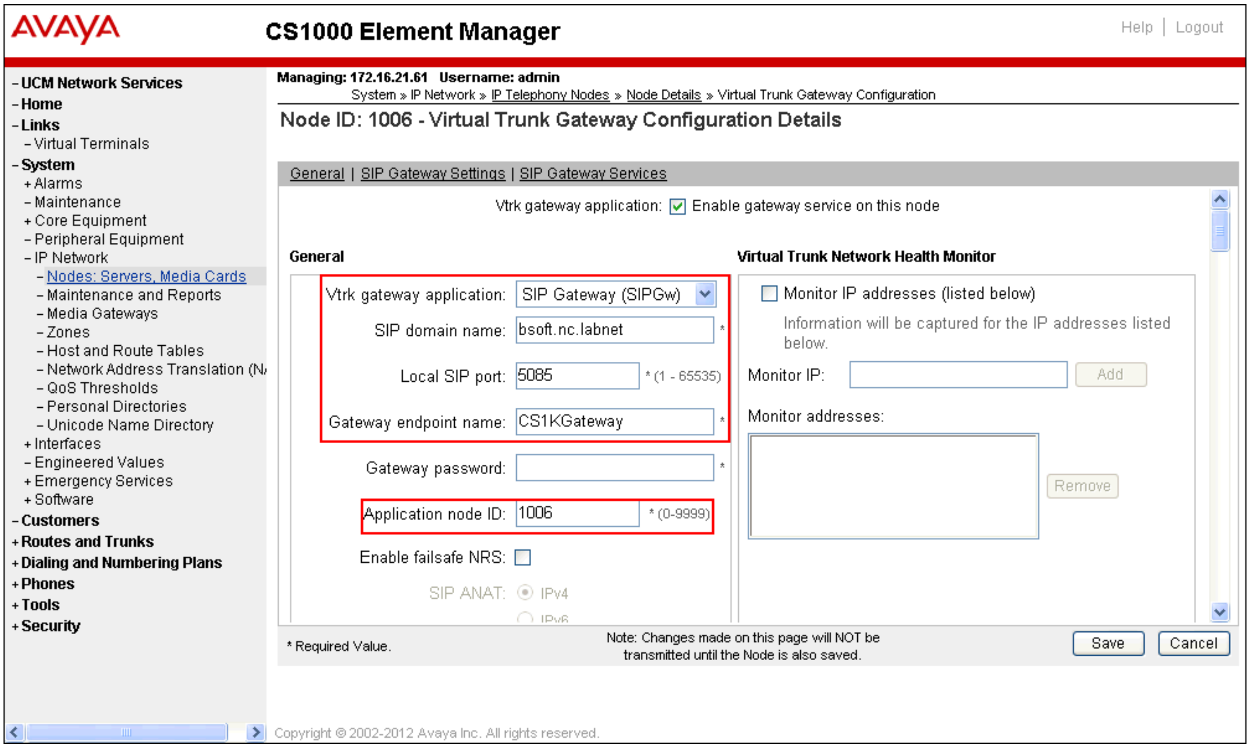
Select **IP Network → Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of this CS1000 system. The **Node Details** screen is displayed as shown in **Section 5.2.1**

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

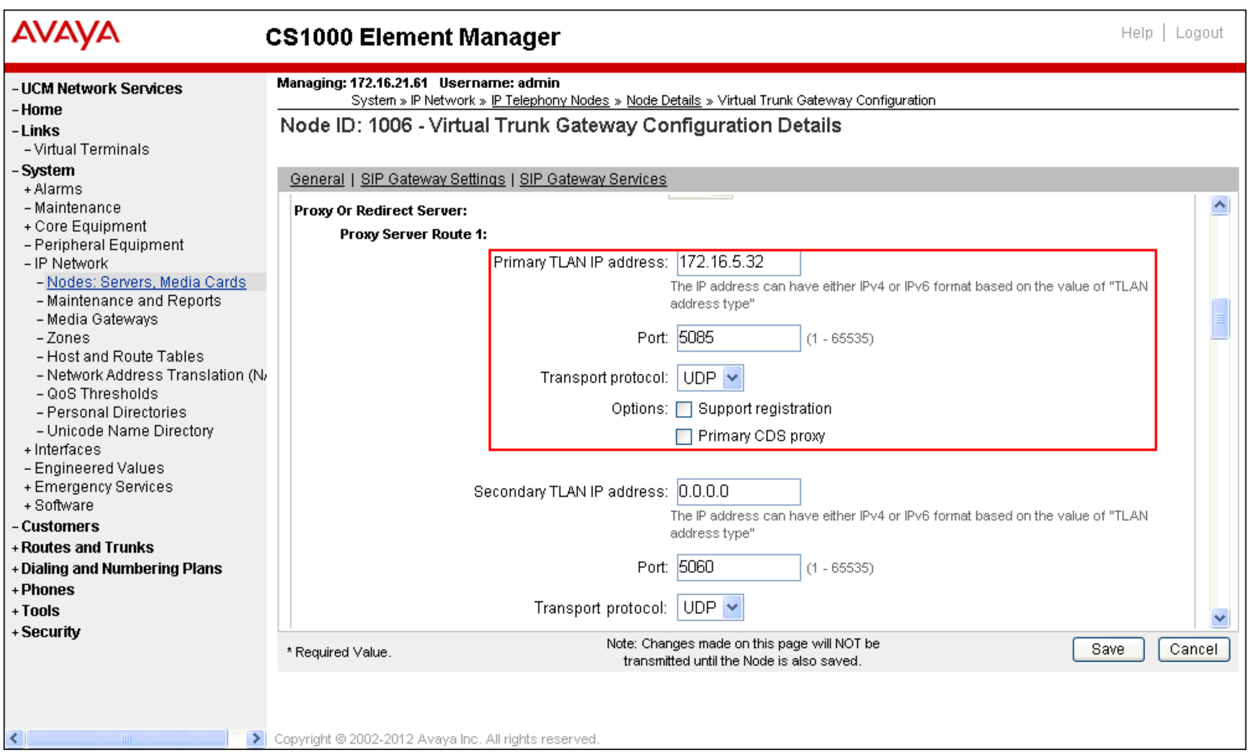
Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown below. The parameters (highlighted in red boxes) are filled in to match values entered under SIP Entity Link in the Avaya Aura® Session Manager (these are shown in **Section 6.6**).

- **Vtrk gateway application**: **SIP Gateway (SIPGw)**
- **SIP domain name**: bsoft.nc.labnet
- **Local SIP port**: 5085
- **Gateway endpoint name**: CS1KGateway
- **Application node ID**: 1006

The domain for CenturyLink (bsoft.nc.labnet) may change during installations.



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

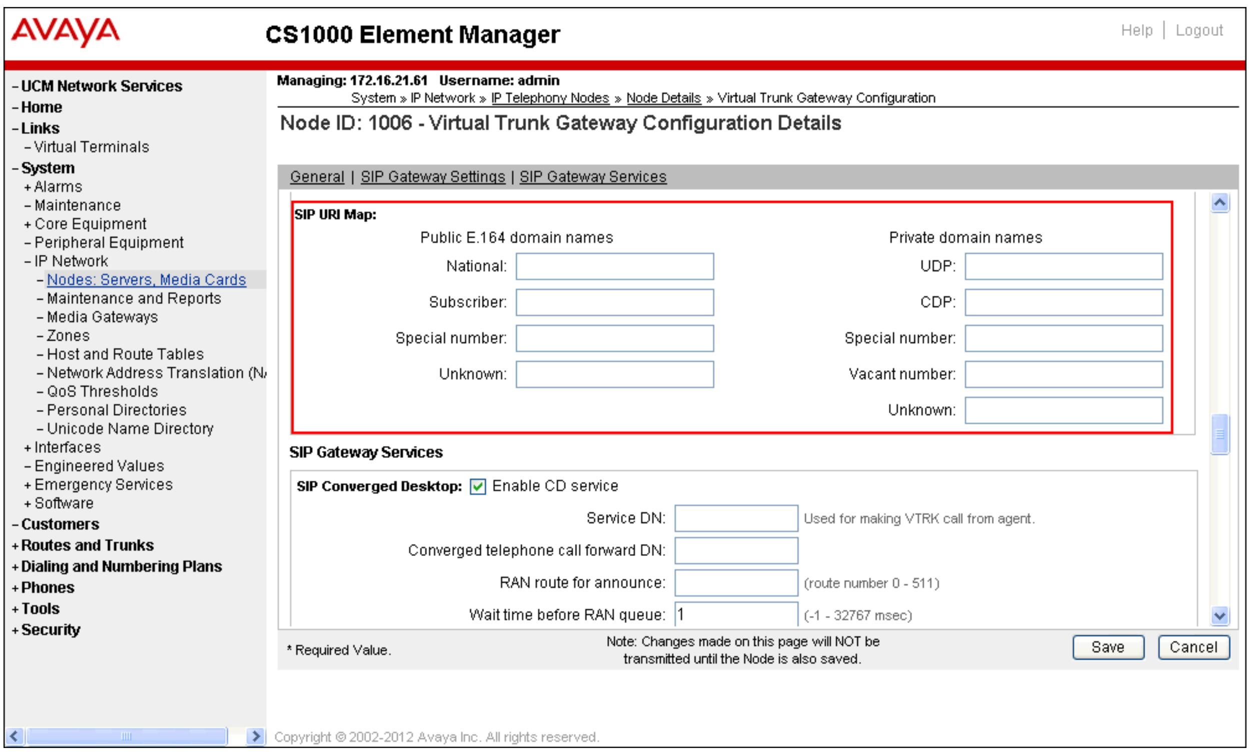


On the same page shown above, scroll down to the **SIP URI Map** section.
Under the **Public E.164 domain names**:
- **National**: leave this SIP URI field as blank
- **Subscriber**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

Under the **Private domain names**:
- **UDP**: leave this SIP URI field as blank
- **CDP**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Vacant number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

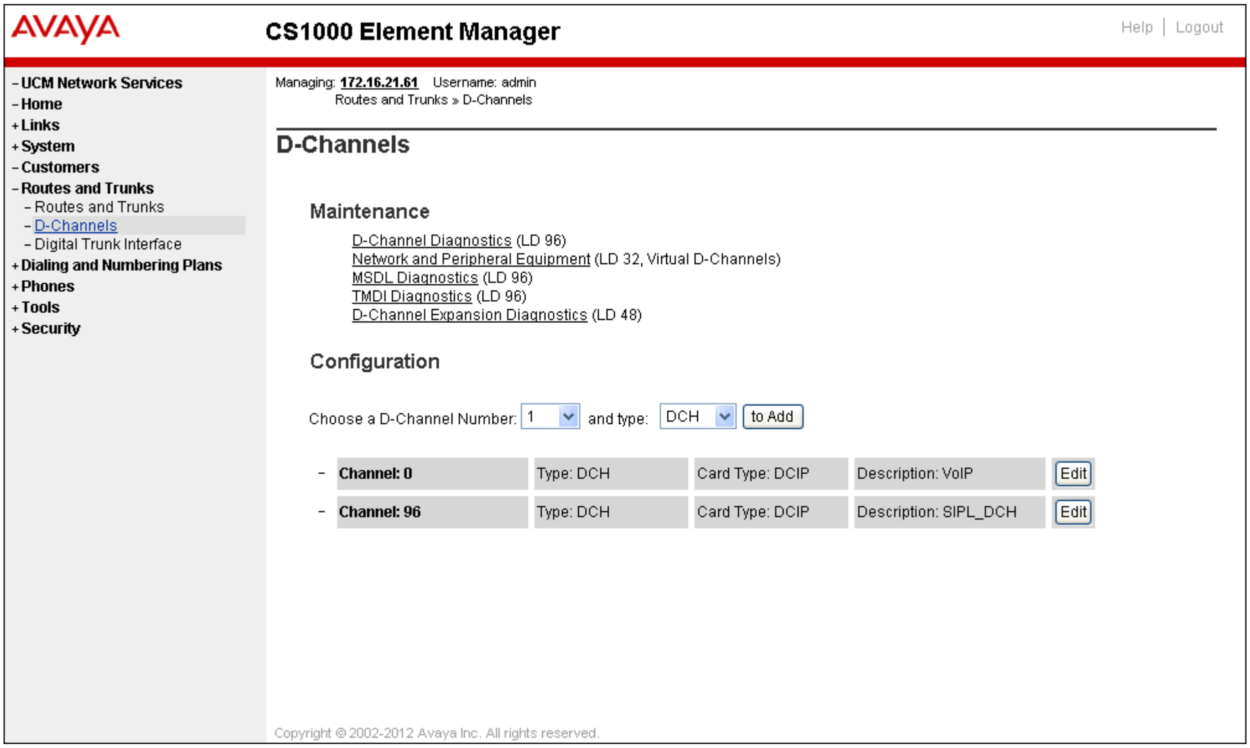
Note: These fields are shown with no entries (blank) for the Avaya DevConnect lab configuration. It is possible that customer installations will have domains names configured here.

Then click on the **Save** button.



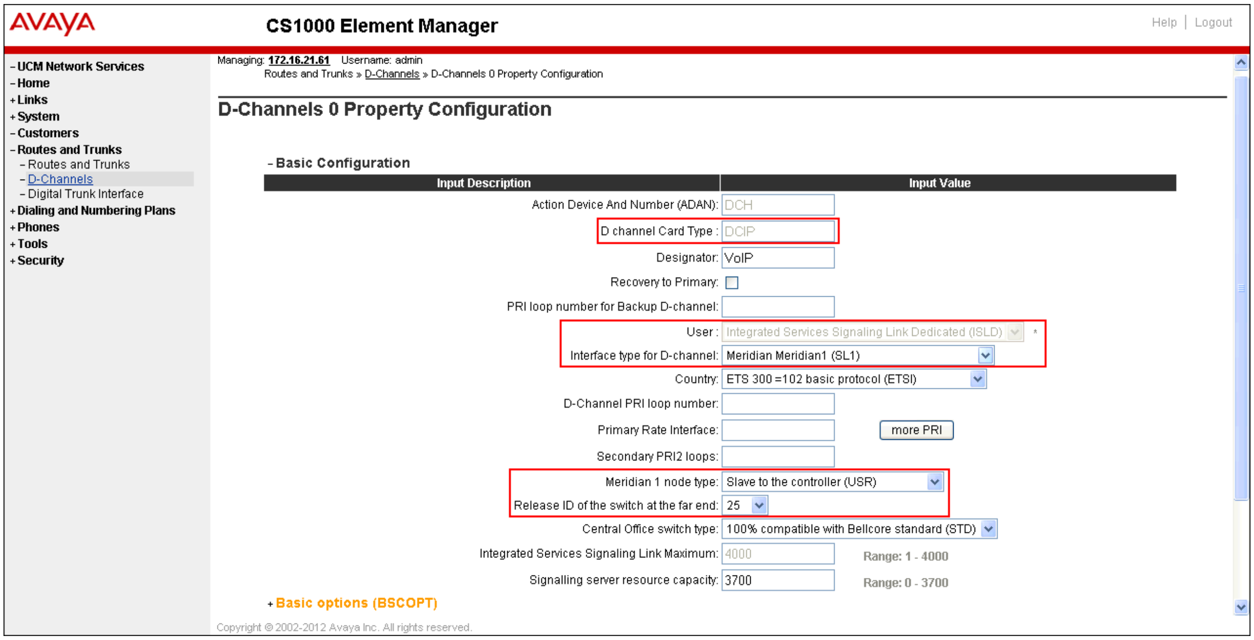
5.5.3. Administer Virtual D-Channel

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



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

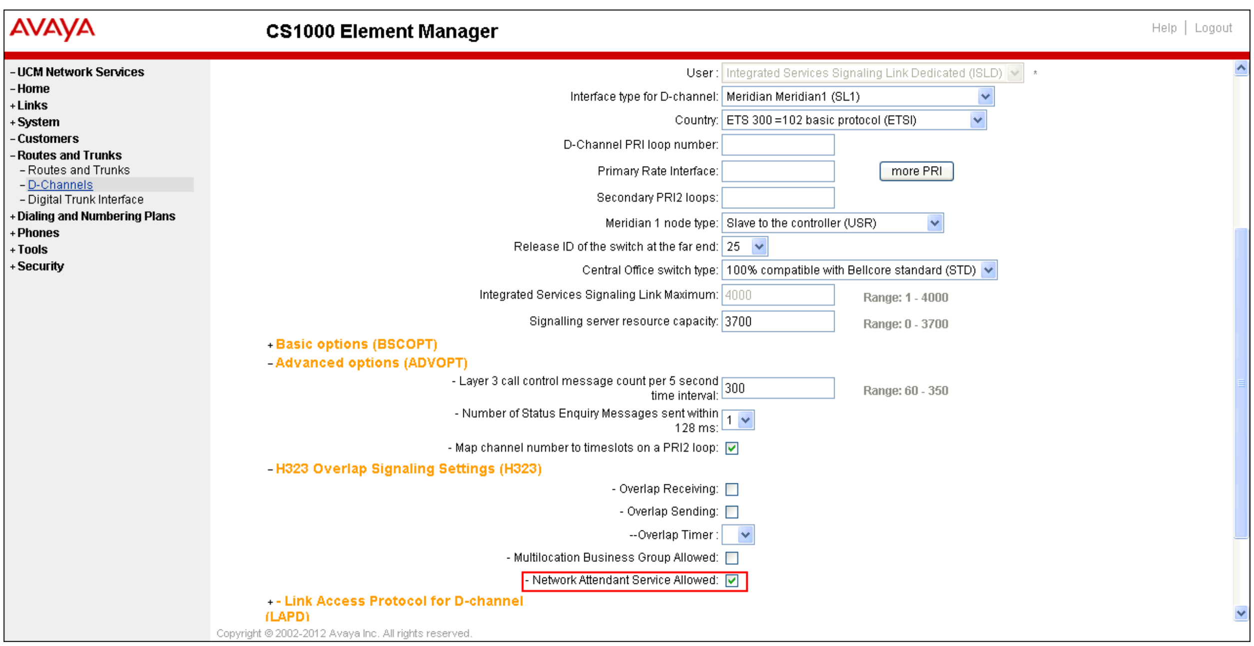
- **D channel Card Type (CTYP): D-Channel is over IP (DCIP)**
- **Designator (DES)**: A descriptive name
- **Interface type for D-channel (IFC): Meridian Meridian1 (SL1)**
- **Meridian 1 node type: Slave to the controller (USR)**
- **Release ID of the switch at the far end (RLS): 25**



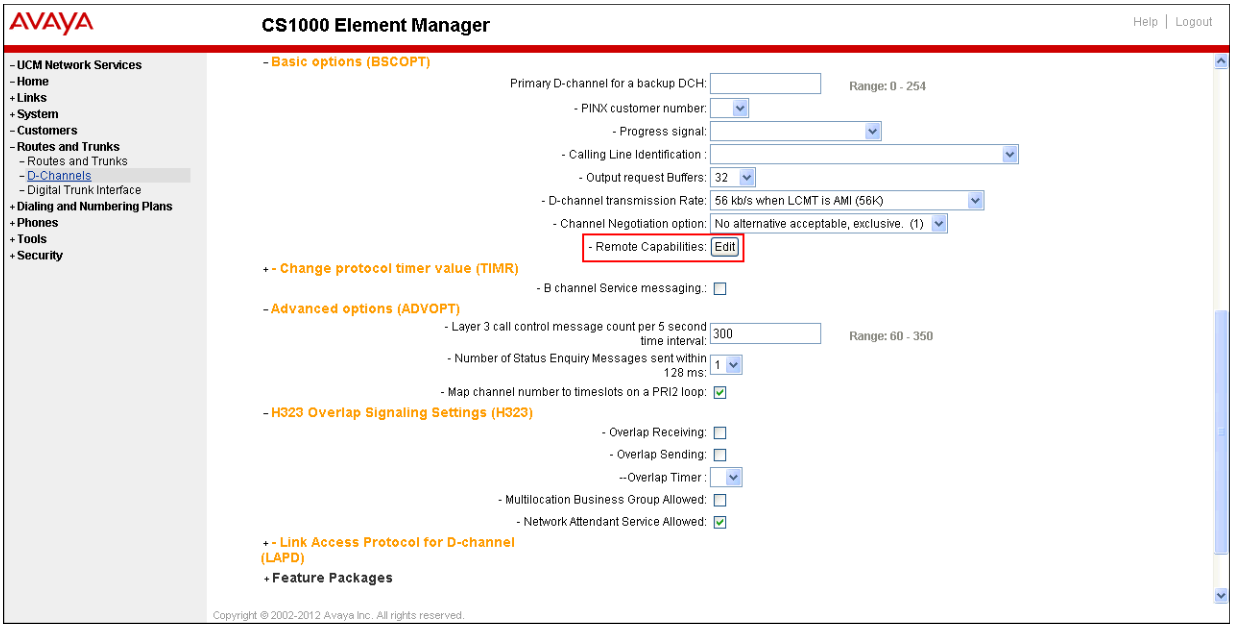
On the same page, scroll down and enter the following values for the specified fields:

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

Retain the default values for the remaining fields.

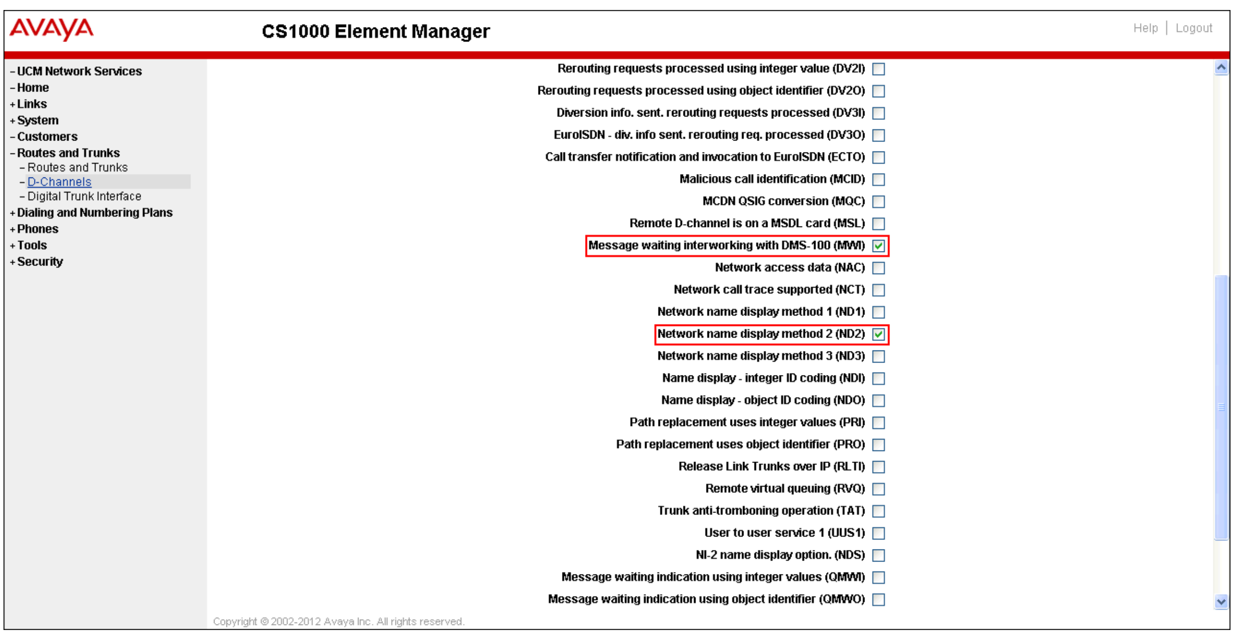


Click on the **Basic Options** and click on the **Edit** button at the **Remote Capabilities** (**RCAP**) attribute as shown below.



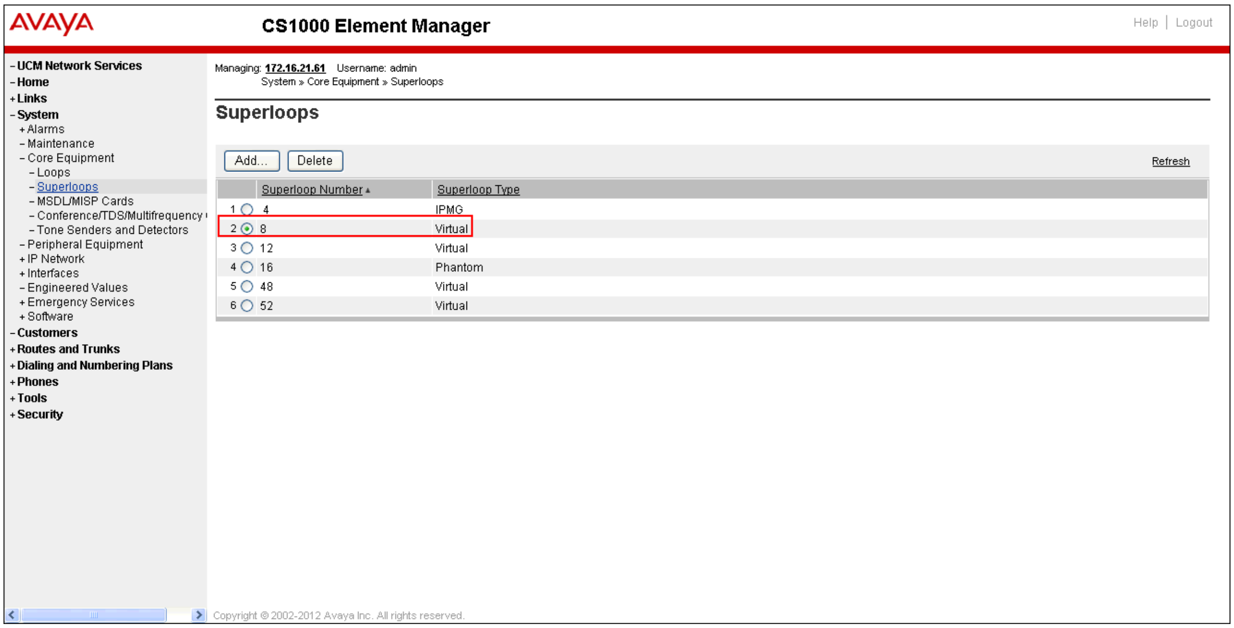
The **Remote Capabilities Configuration** page will appear. Check **ND2** and **MWI** (if PSTN mailboxes are present on the CS1K Call Pilot) checkboxes as shown below.

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



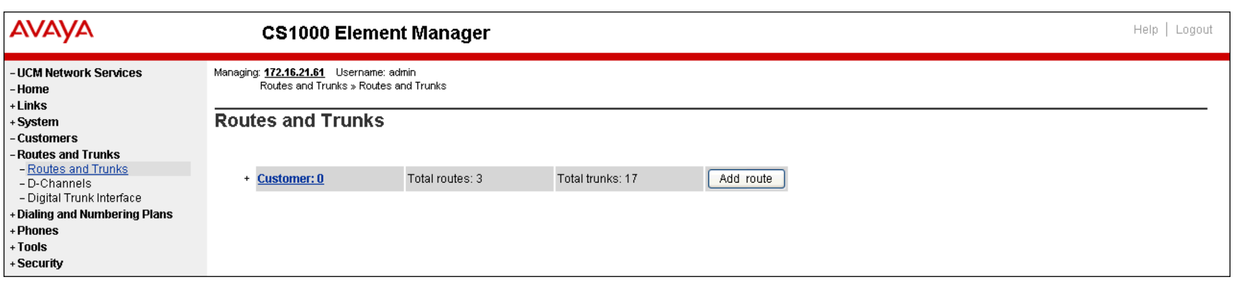
5.5.4. Administer Virtual Super-Loop

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



5.5.5. Administer Virtual SIP Routes

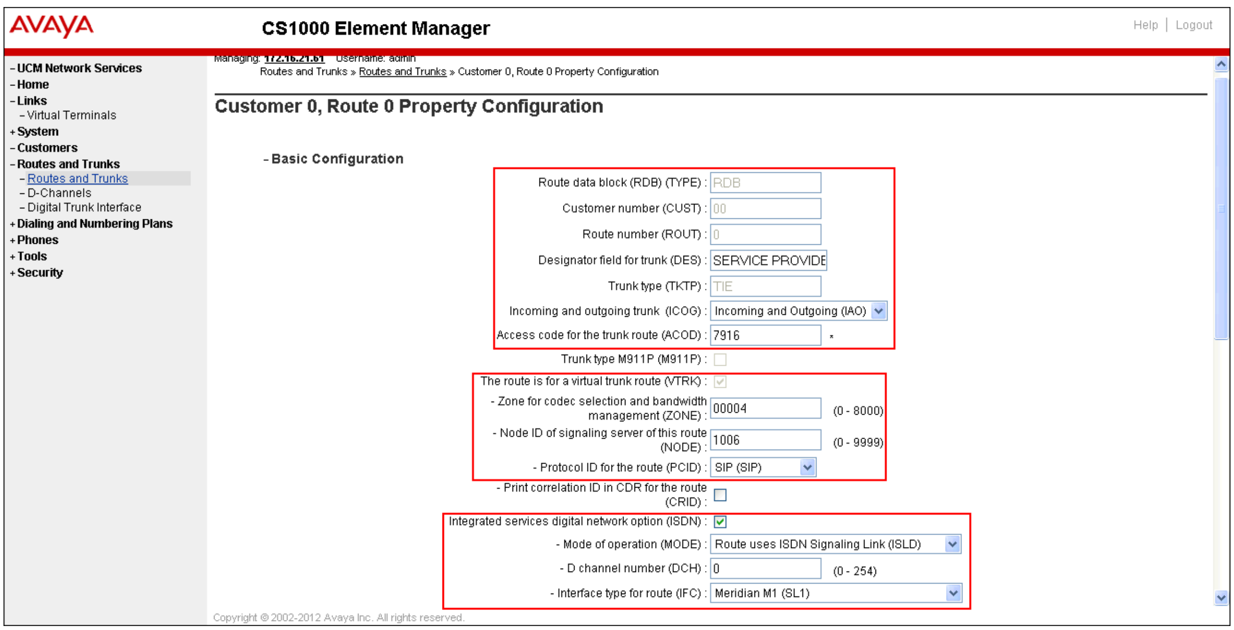
Select **Routes and Trunks → Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown below.



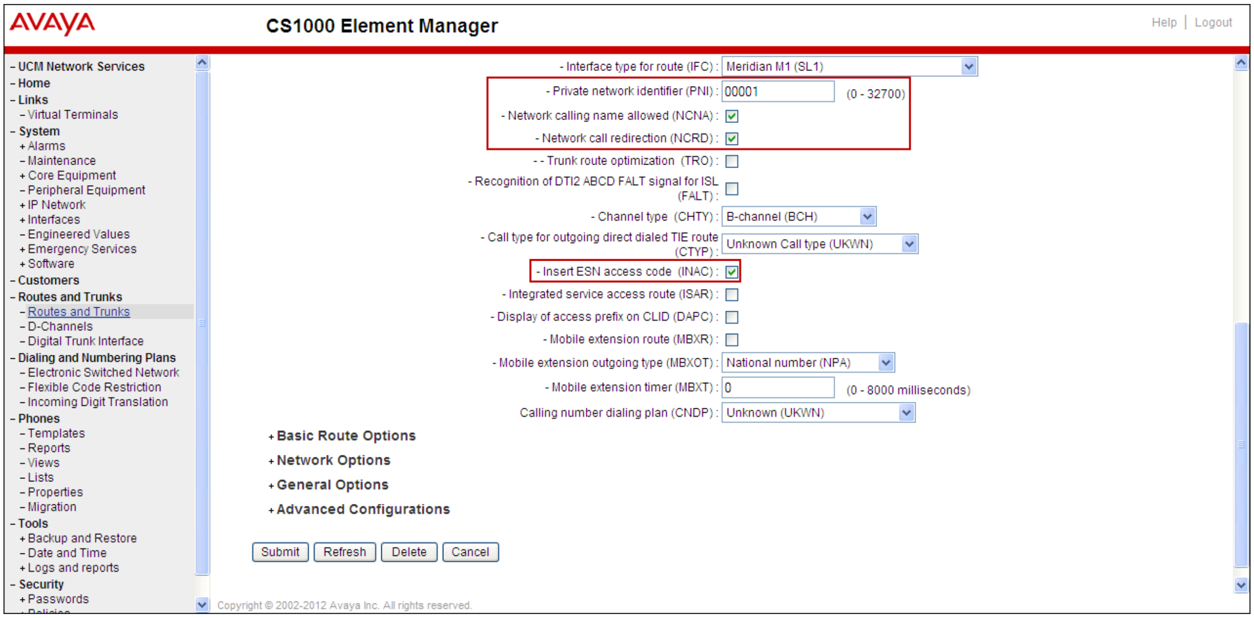
The **Customer 0**, New **Route Configuration** screen is displayed next. Scroll down until the **Basic Configuration** Section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown below.

- **Route Number (ROUT)**: Select an available route number.
- **Designator field for trunk (DES)**: A descriptive text.
- **Trunk Type (TKTP)**: **TIE trunk data block (TIE)**
- **Incoming and Outgoing trunk (ICOG)**: **Incoming and Outgoing (IAO)**
- **Access Code for the trunk route (ACOD)**: An available access code.

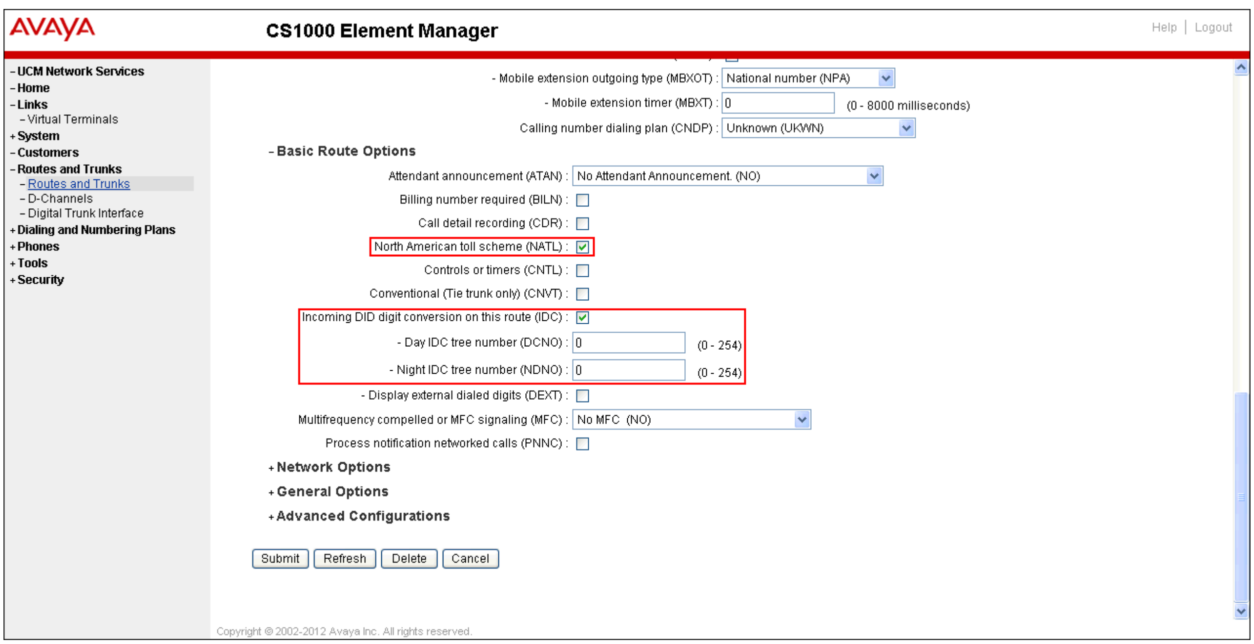
- Check the field **The route is for a virtual trunk route (VTRK)** to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter 4 (created in **Section 5.4.2**).
- For the **Node ID of signalling server of this route (NODE)** field, enter the node number 1006 (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated services digital network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen.
    - **Mode of operation (MODE)**: **Route uses ISDN Signalling Link (ISLD)**
    - **D channel number (DCH)**: D-Channel number 0 (created in **Section 5.5.3**)
    - **Interface type for route (IFC)**: Meridian M1 (SL1)



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

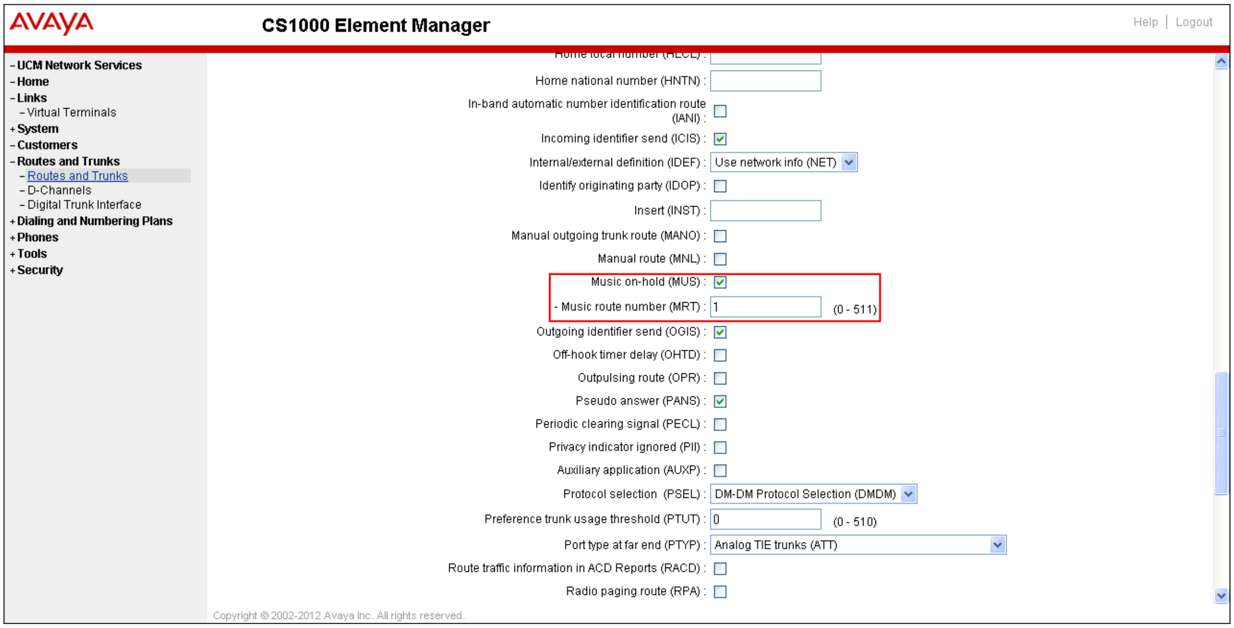


- Click on **Basic Route Options**, check the **North American toll scheme (NATL)** box and **Incoming DID digit conversion on this route (IDC)** box, input **DCNO 0** (created in **Section 5.6.5**) for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown below.



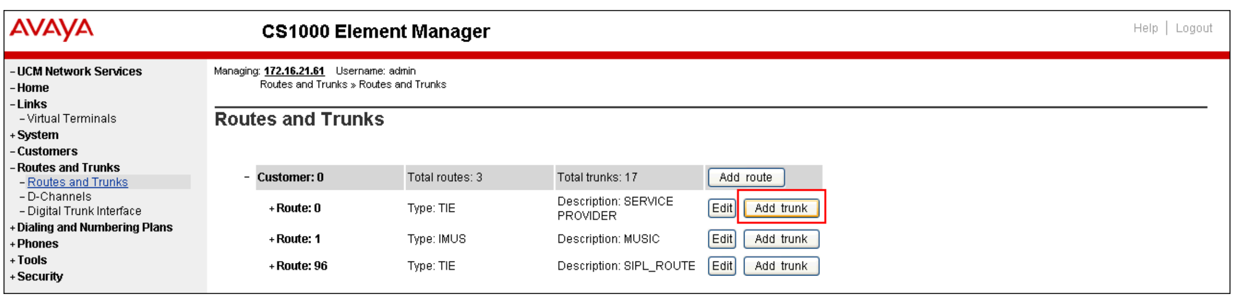
- Click on **Advance Configurations**; check **Music-on-hold** to enable music on hold on the route. Input music route 1 to the boxes as shown below. The CS1000 system has been pre-configured with route 1 as a music route.

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



5.5.6. Administer Virtual Trunks

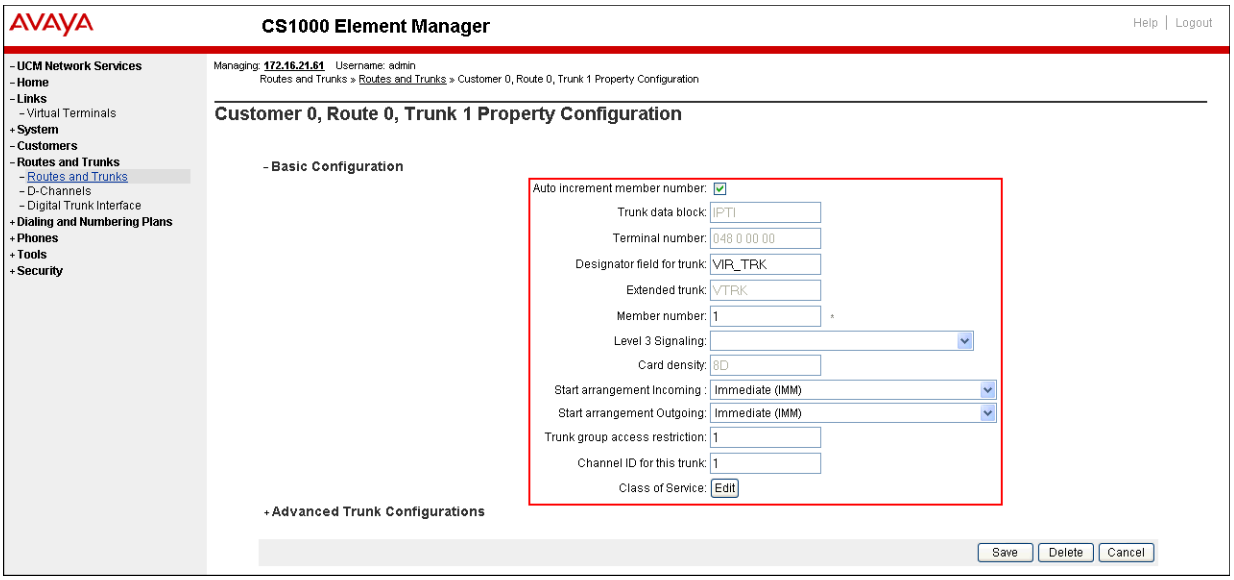
Continue on **Section 5.5.5** after click **Submit**, the **Routes and Trunks** screen is displayed and updated with the newly added route. In the example, Route 0 was being added. Click on the **Add trunk** button next to the newly added route 0 as shown below.



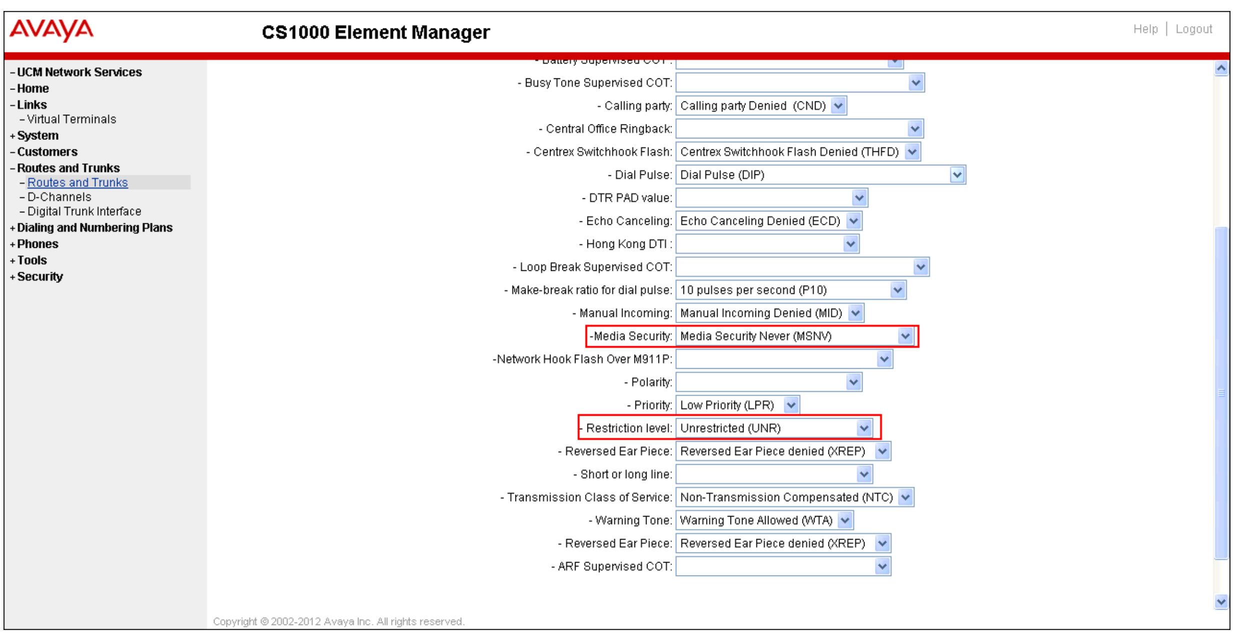
The **Customer 00, Route 0, Trunk 1 Property Configuration** screen is displayed as shown below**.** Enter the following values for the specified fields and retain the default values for the remaining fields. Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service** (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 5.5.4**)
- **Designator field for trunk** (**DES**): A descriptive text
- **Extended Trunk (XTRK): Virtual trunk (VTRK)**

- **Member number** (**RTMB**): Current route number and starting member
- **Start arrangement Incoming** (**STRI**): **Immediate (IMM)**
- **Start arrangement Outgoing** (**STRO**): **Immediate (IMM)**
- **Trunk Group Access Restriction (TGAR)**: Desired trunk group access restriction level
- **Channel ID for this trunk** (**CHID**): An available starting channel ID

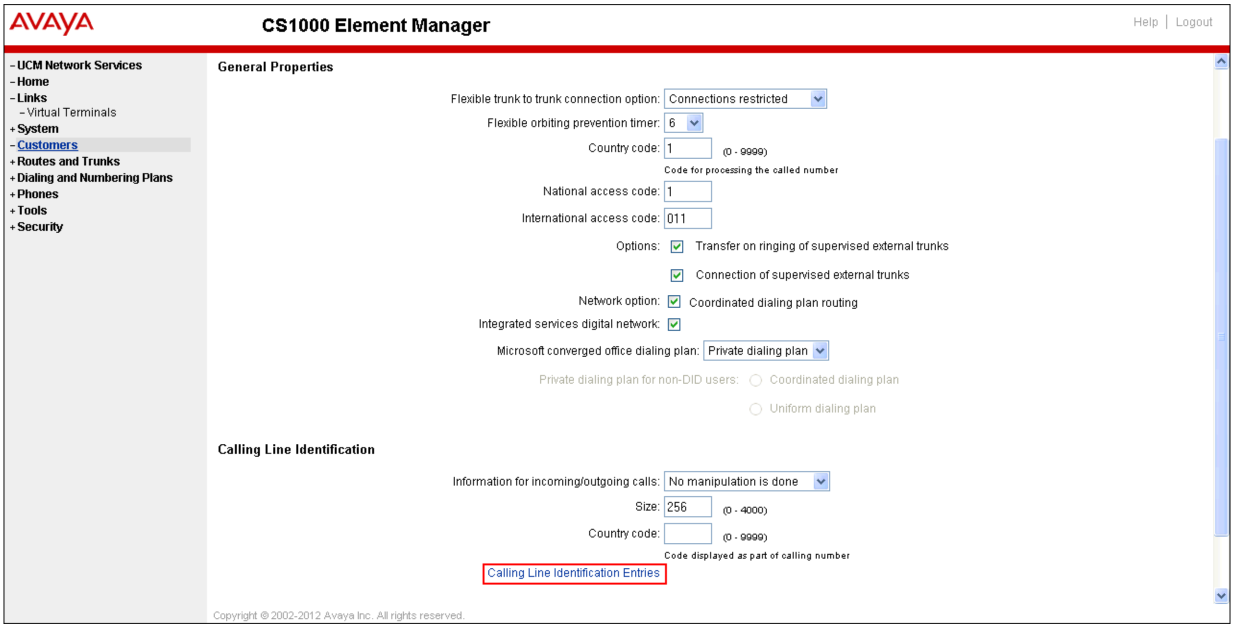


Click on **Edit** button next to **Class of Service**. For **Media Security**, select **Media Security Never** (**MSNV). For Restriction Level,** enter **Unrestricted (UNR)**. Use default for remaining values. Scroll down to the bottom of the screen and click **Return Class of Service** and then click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

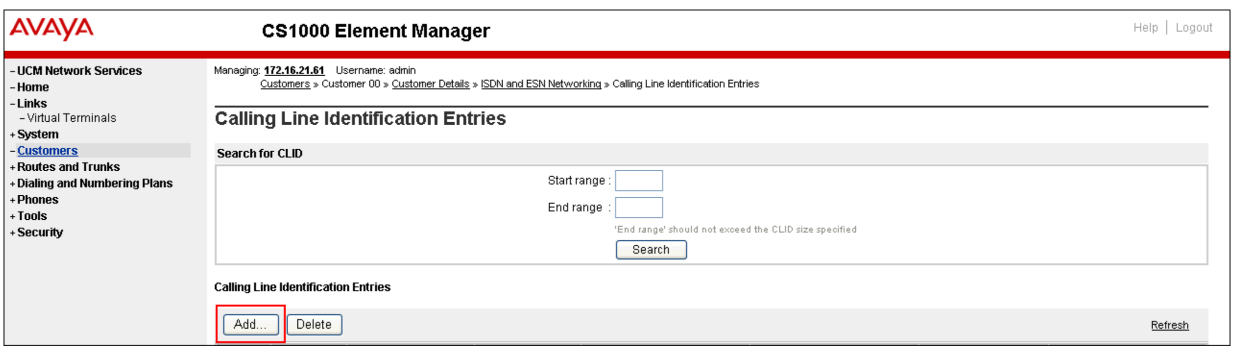


5.5.7. Administer Calling Line Identification Entries

Select **Customers → 00 → ISDN and ESN Networking**. Click on **Calling Line Identification Entries** as shown below.



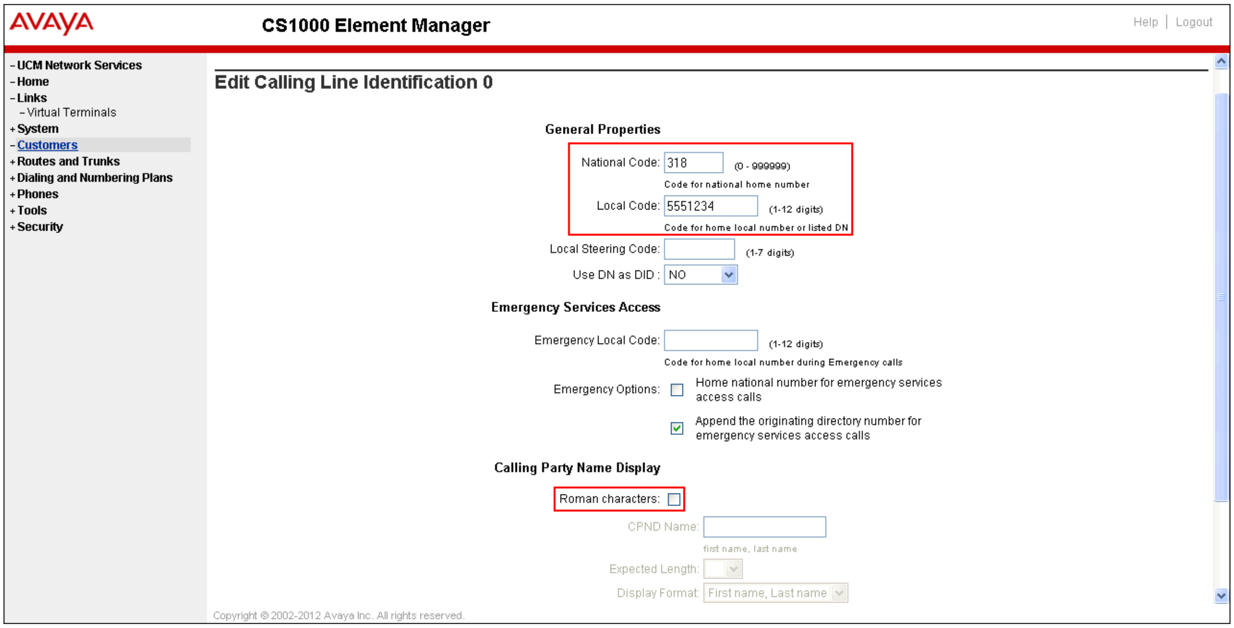
Click on **Add** as shown below.



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 318.
- **Local Code**: Input the seven digit number of the DID assigned by the service provider, in this case it is 5551234.
- **Calling Party Name Display**: Uncheck for **Roman characters**.

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



5.5.8. Enable External Trunk to Trunk Transferring

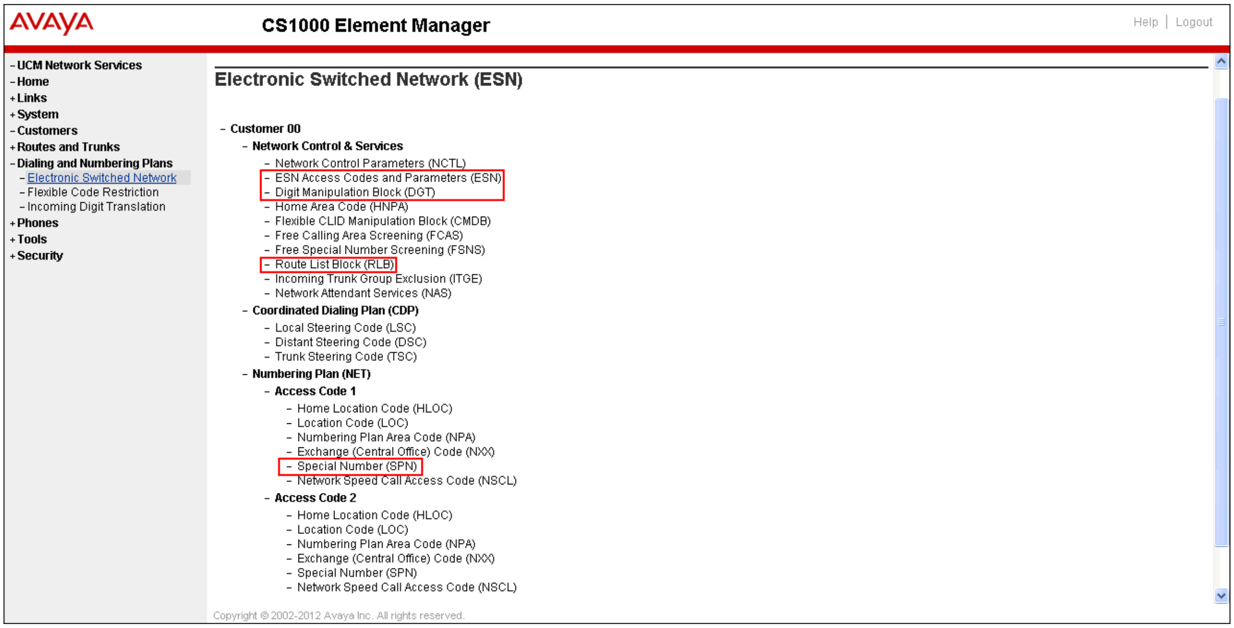
This section shows how to enable External Trunk to Trunk Transferring feature which is a mandatory configuration to make call transfer and conference work properly over a SIP trunk. Log in to the Call Server CLI (please refer to **Section 5.1.2** for more detail)
Allow External Trunk to Trunk Transferring 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
....
```

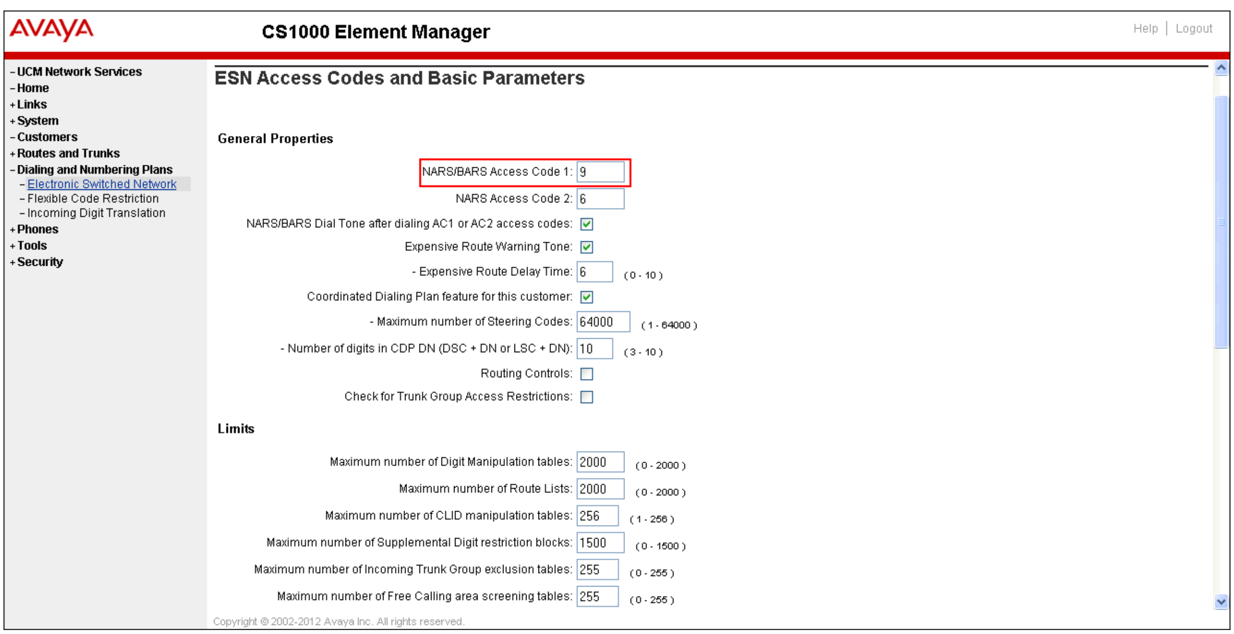
5.6. Administer Dialing Plans

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

Log in 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. 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
…
```

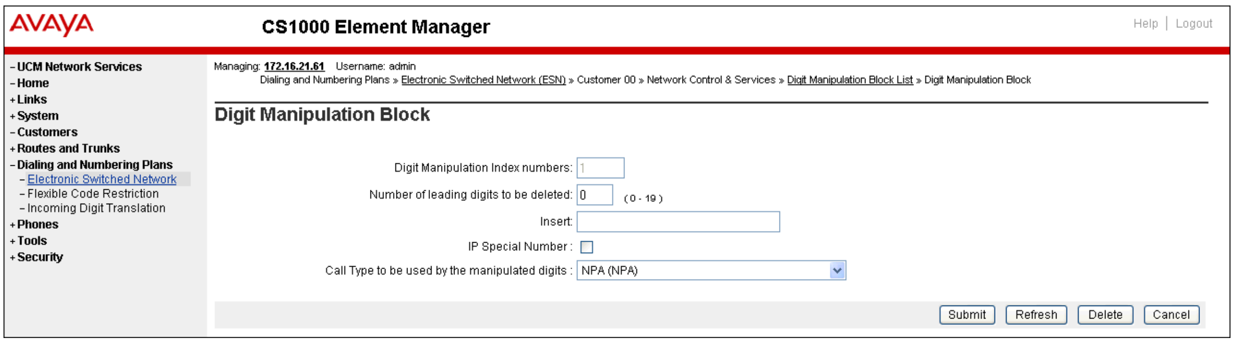
5.6.3. Digit Manipulation Block (DMI)

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

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

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

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

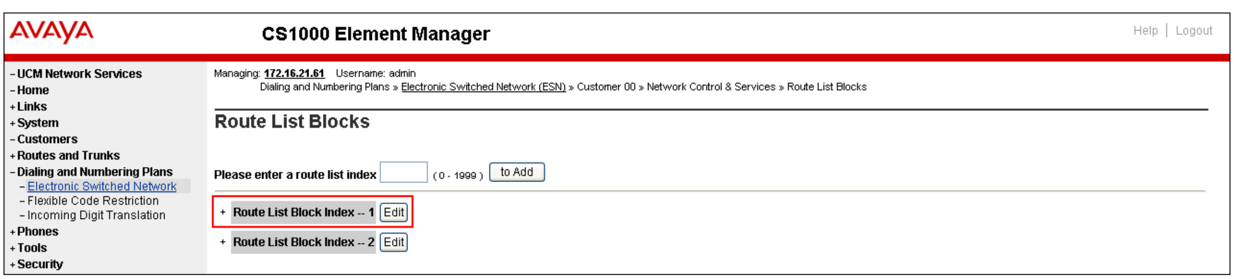


5.6.4. Route List Block (RLB)

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

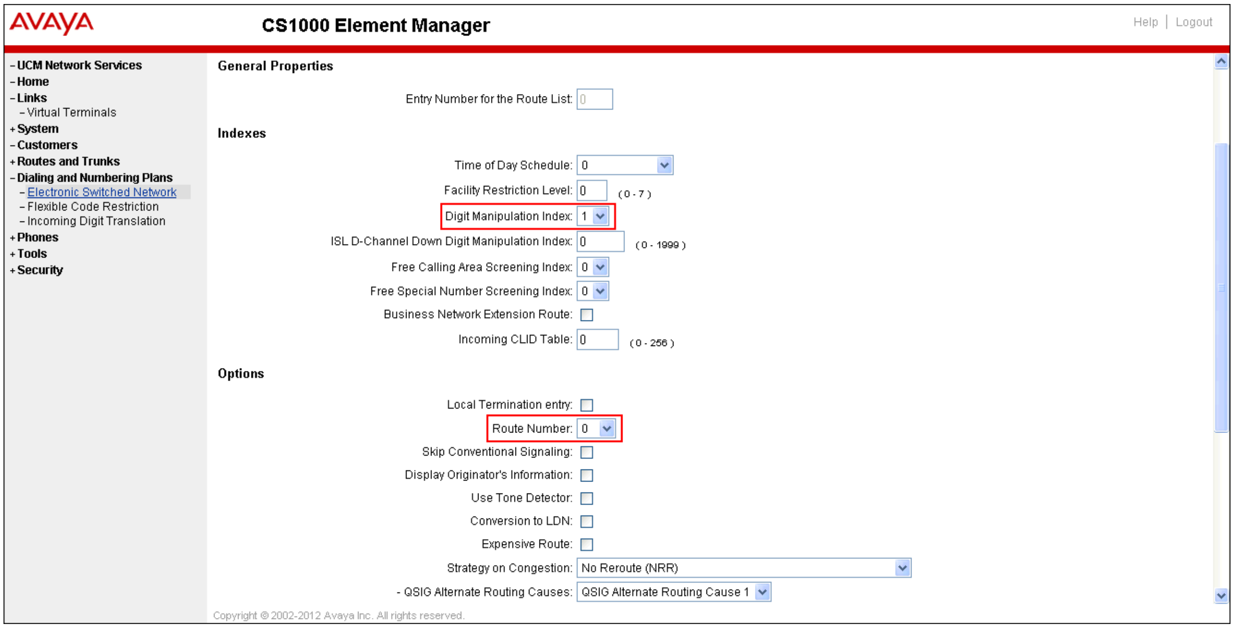
Enter an available index in the **Please enter a route list index** and click on the "**to Add"** button as shown below.

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



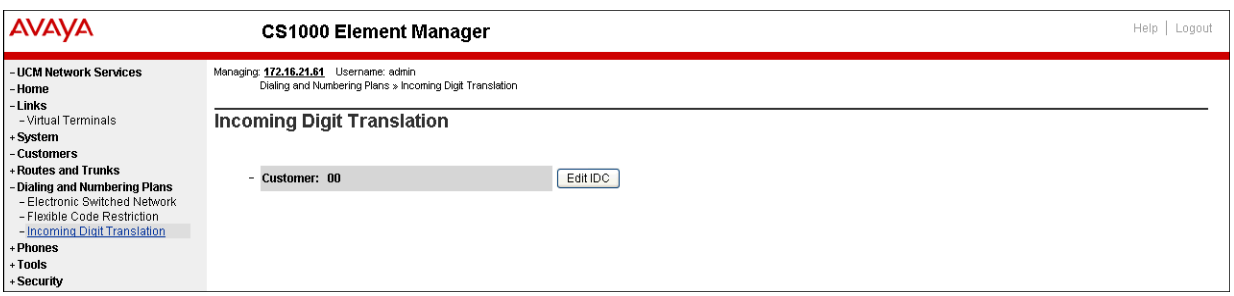
Enter the following values for the specified fields, and retain the default values for the remaining fields as shown below. Scroll down to the bottom of the screen, and click on the **Submit** button.

- **Route Number** (ROUT): 0 (created in **Section 5.5.5**)
- **Digit Manipulation Index** (DMI): 1 (created in **Section 5.6.3**)

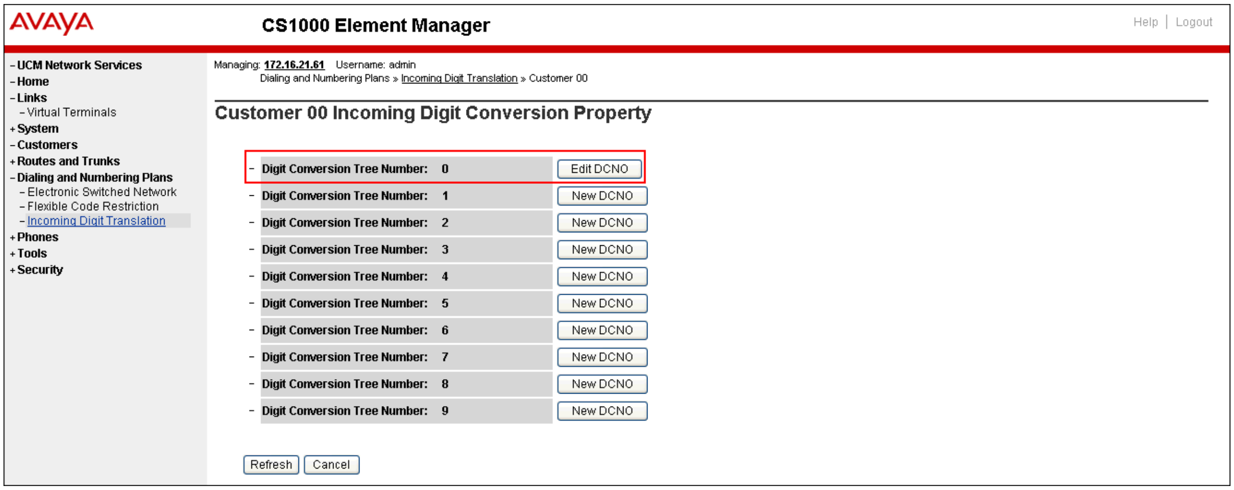


5.6.5. Inbound Call Digit Translation

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

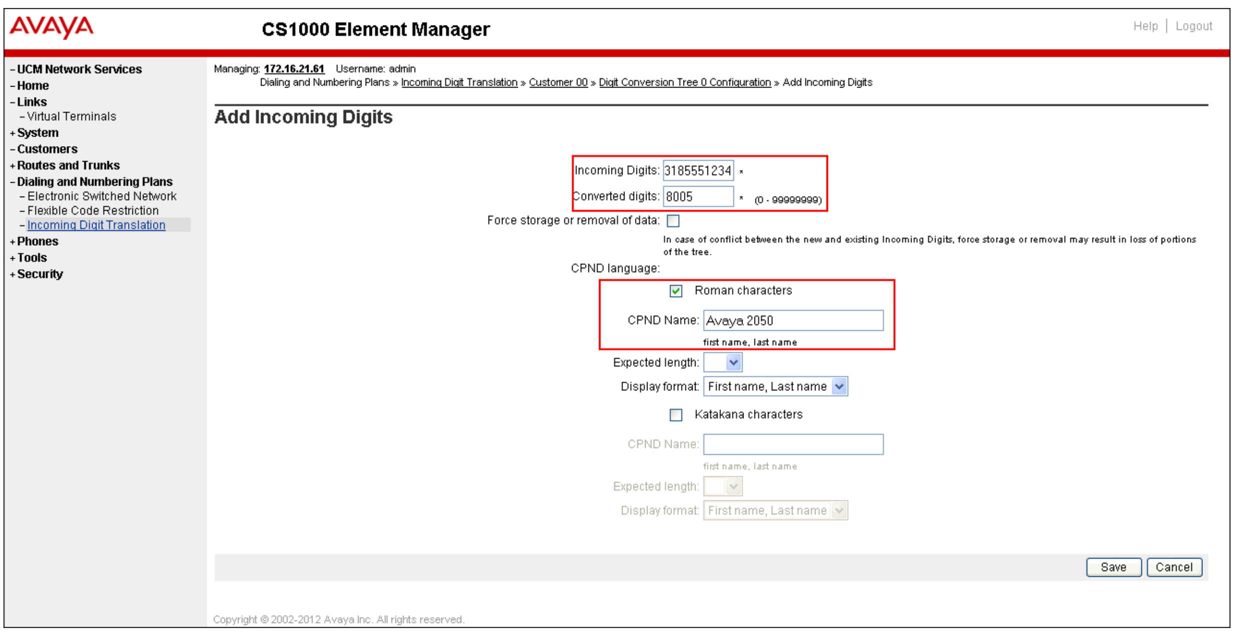


Click on the **New DCNO** button to create the digit translation mechanism. In this example, **Digit Conversion Tree Number (DCN0) 0** was created as shown below.



Detail configuration of the **DCNO** is shown below. The **Incoming Digits** can be mapped to the **Converted Digits** which would be the CS1000 system extension number. This **DCN0** has been assigned to route 0 as shown in **Section 5.5.5**.

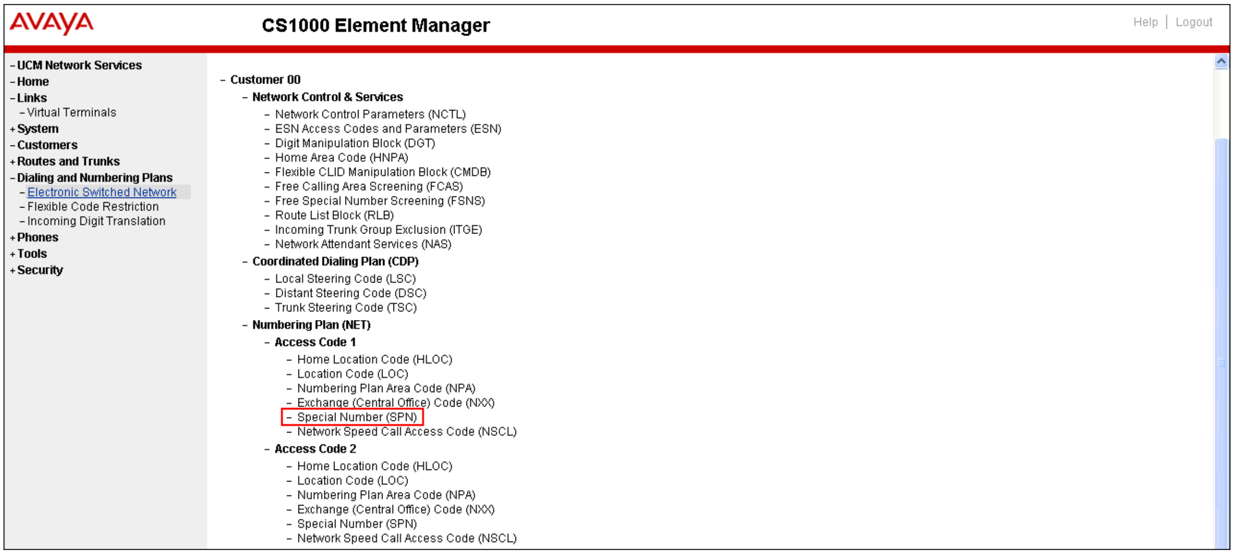
In the following configuration, the incoming call from PSTN with the prefix 3185551234 will be translated to the CS1000 extension number 8005.



5.6.6. Outbound Call - Special Number Configuration.

There are special numbers which have been configured to be used for this testing such as **0** to reach the Service Provider operator, **0+10** digits to reach Service Provider operator assistant, **011** prefix for international call, **1** for national long distance call, **411**, **911, 711** and so on.

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 numbers that were used for the testing are shown below.

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

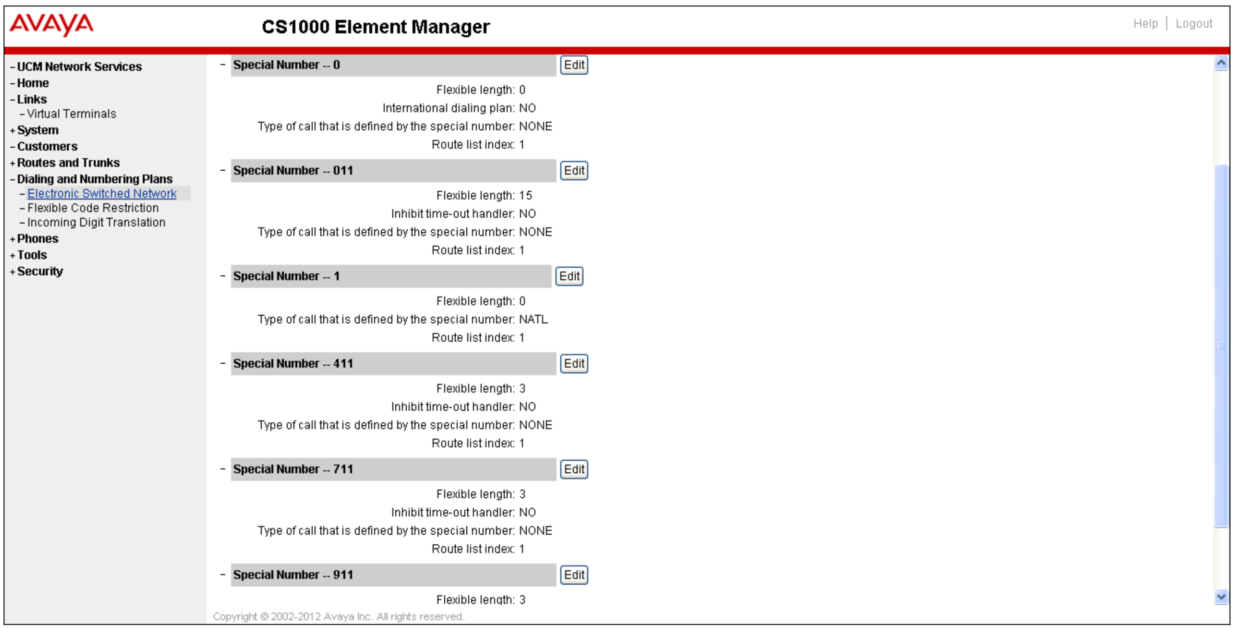
- **Flexible length**: 3
- **CallType**: None
- **Route list index**: 1, created in **Section 5.6.4**

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 under **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 extensions used during the testing.

5.7.1. Phone creation

Refer to **Section 5.5.4** 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.

Log in 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 DN03 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**. 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**. 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**. 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
```

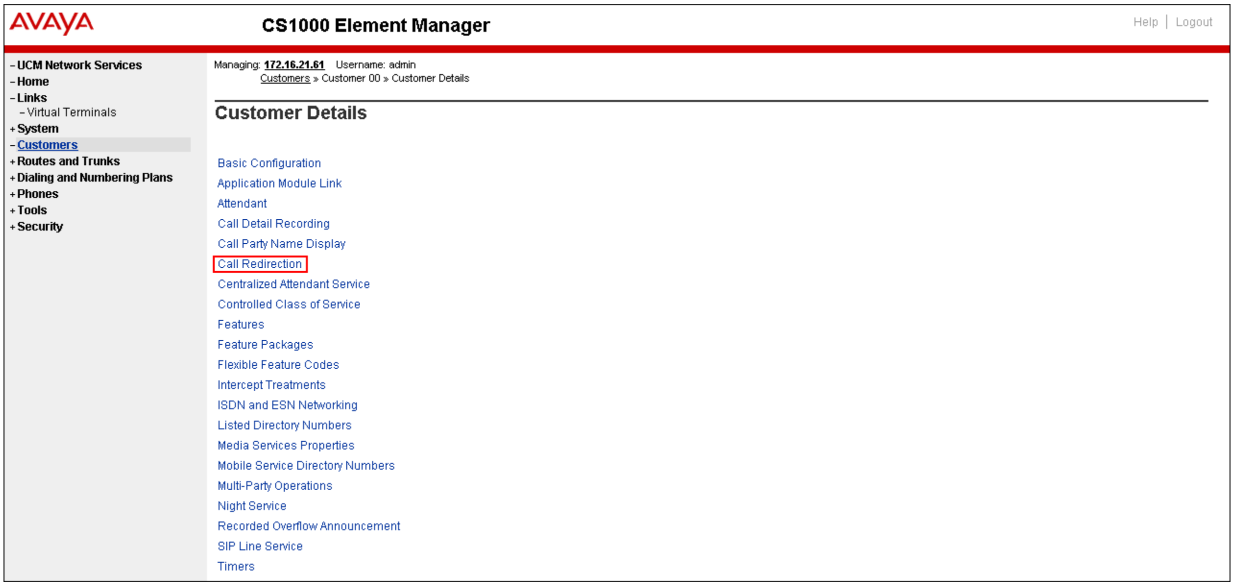
To allow display name and number, set CLS to **nama, ddga**. CS1000 will send header "Privacy:none" to Service Provider.

```
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.

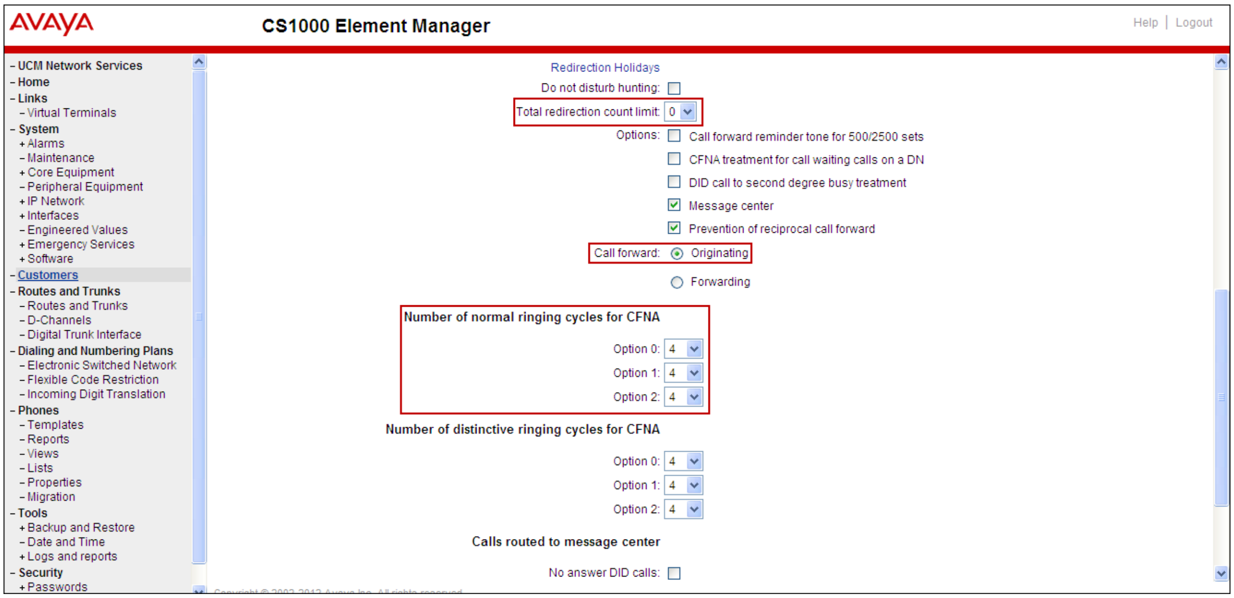
Select **Customer → 00 → Call Redirection**. The Call Redirection page is displayed as shown below.



Set the following fields:

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

Click on Save (not shown)



Enable **Call Forward All Call** (**CFAC**) for the phone over the SIP trunk by using **LD 11**, change its CLS to **CXFA,** then program the forward number on the phone set. Following is the configuration of a phone that has CFAC enabled, the phone is 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** then program the forward number as **HUNT**. Following is the configuration of a phone that has CFB enabled; the phone is CFB to the PSTN number **919195551212**.

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

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

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

5.7.4. Enable Call Waiting for the Phone

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

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 the Avaya Aura® Session Manager

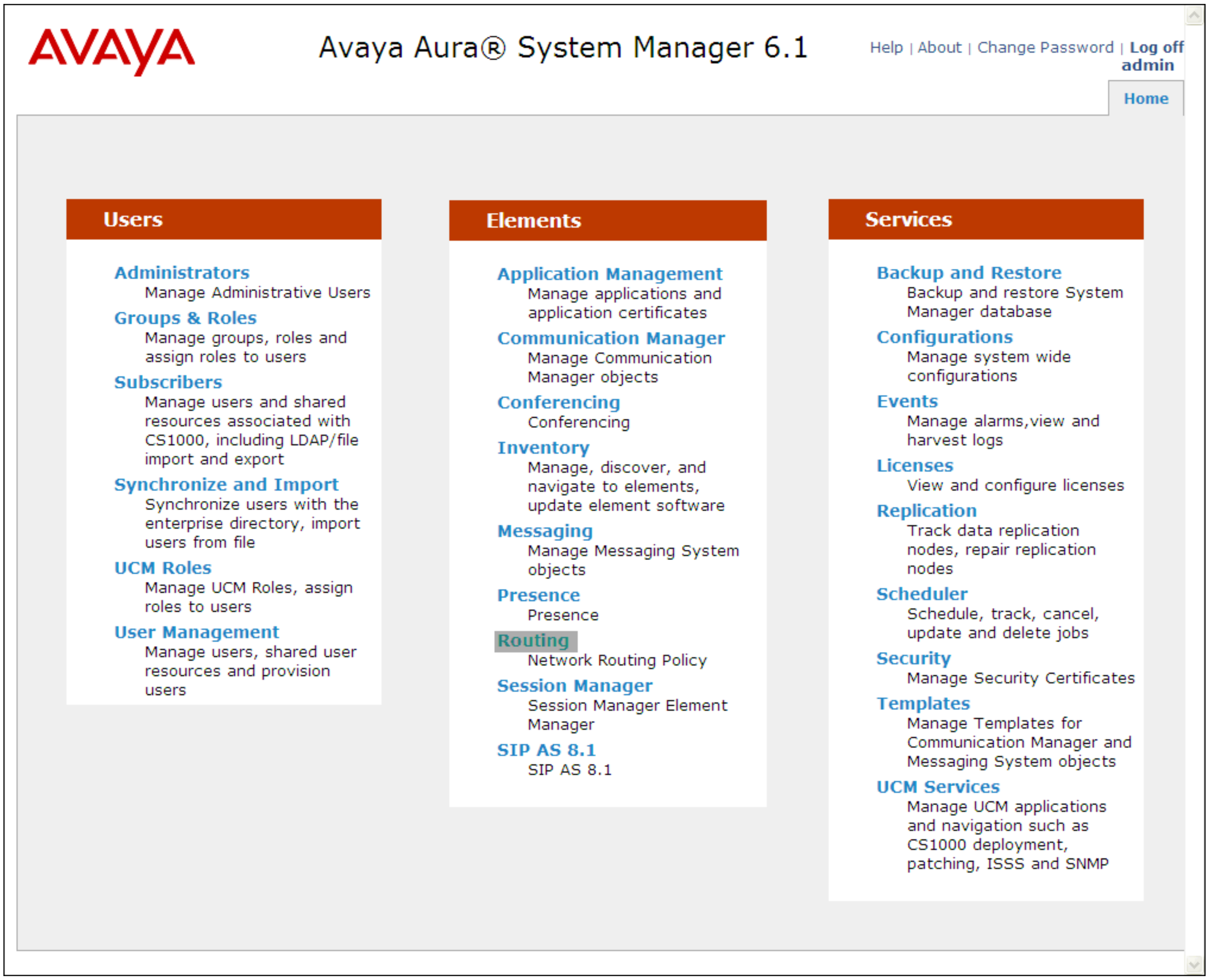
This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to the Avaya CS1000, the Avaya SBCE and Avaya Aura® Session Manager itself.
- Entity Links, which define the SIP trunk parameters used by Avaya Aura® 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
- Avaya Aura® Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager.

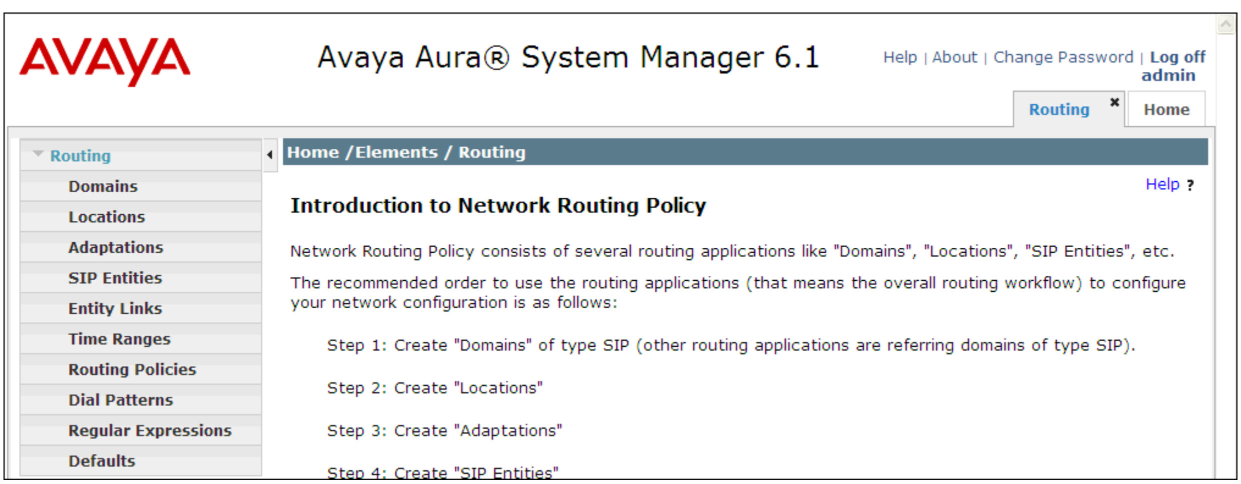
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Avaya Aura® Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities,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

6.1. System Manager Login and Navigation

Avaya Aura® 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

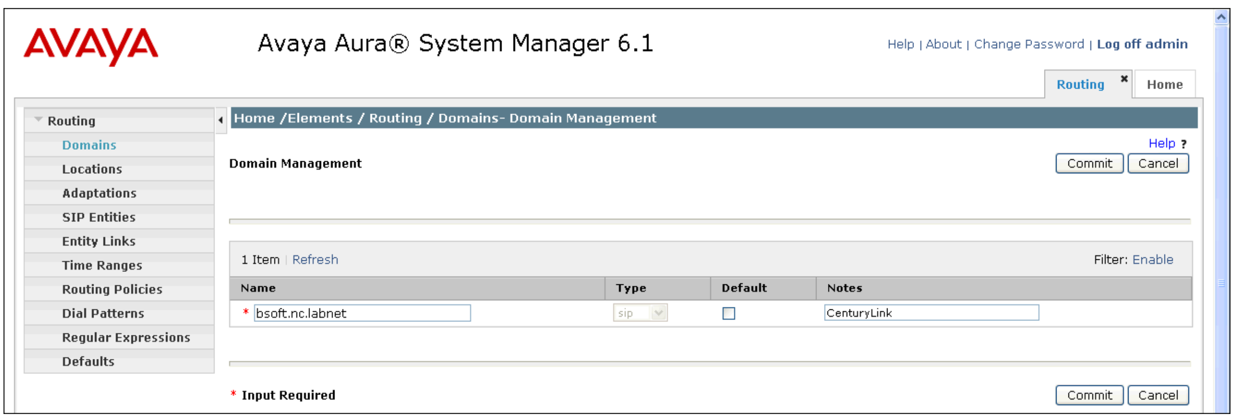
Create a SIP domain for each domain for which Avaya Aura® Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain: **avaya.lab.com** and the domain for CenturyLink: **bsoft.nc.labnet.**

The domain for CenturyLink (bsoft.nc.labnet) may change during installations.

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 CenturyLink 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).

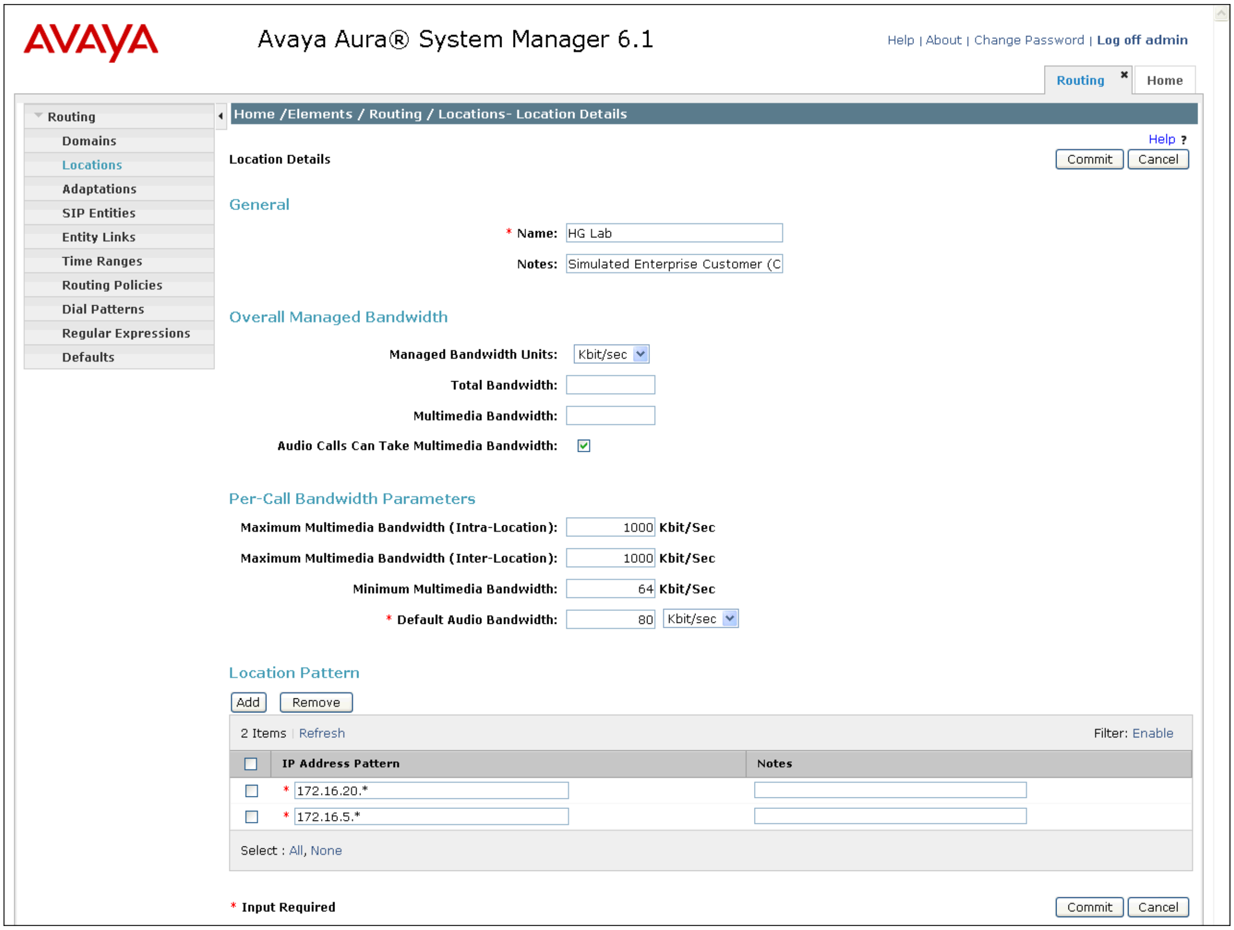
In the **General** section, enter the following values. Use default values for all remaining fields:

- **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 Avaya CS1000, Avaya SBCE and Avaya Aura® Session Manager itself. Click **Commit** to save.

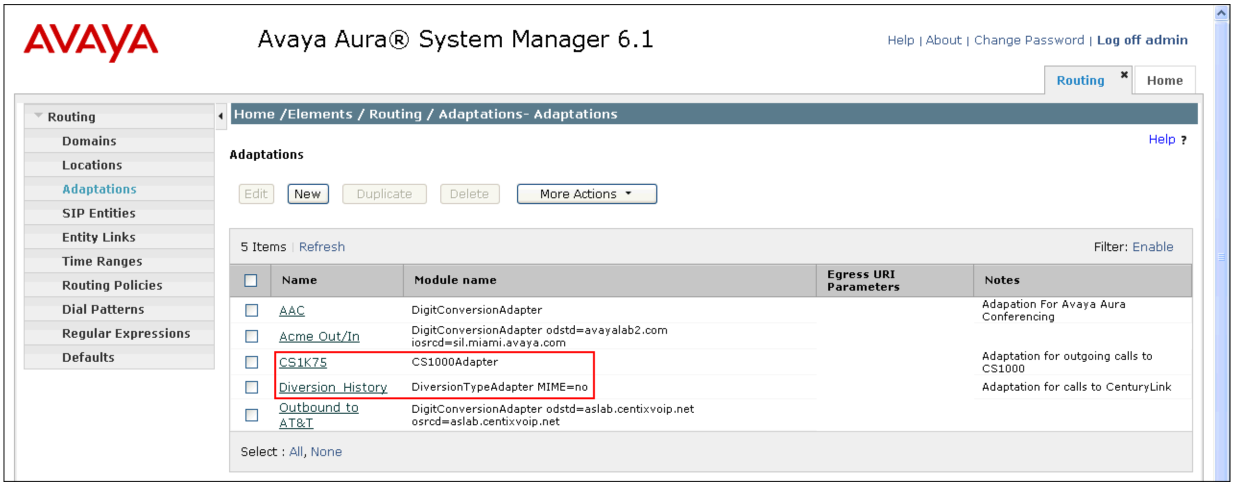


6.4. Add Adaptation Module

Avaya Aura® 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, 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 in the compliance test.



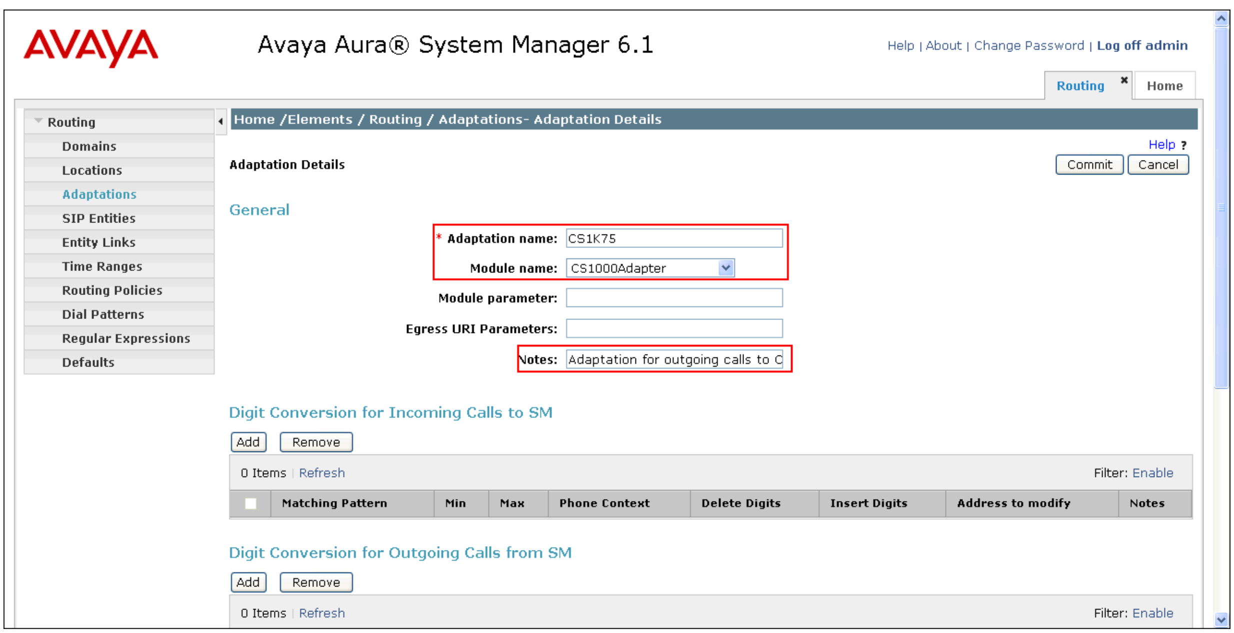
Settings for **CS1K75** Adaptation:

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:

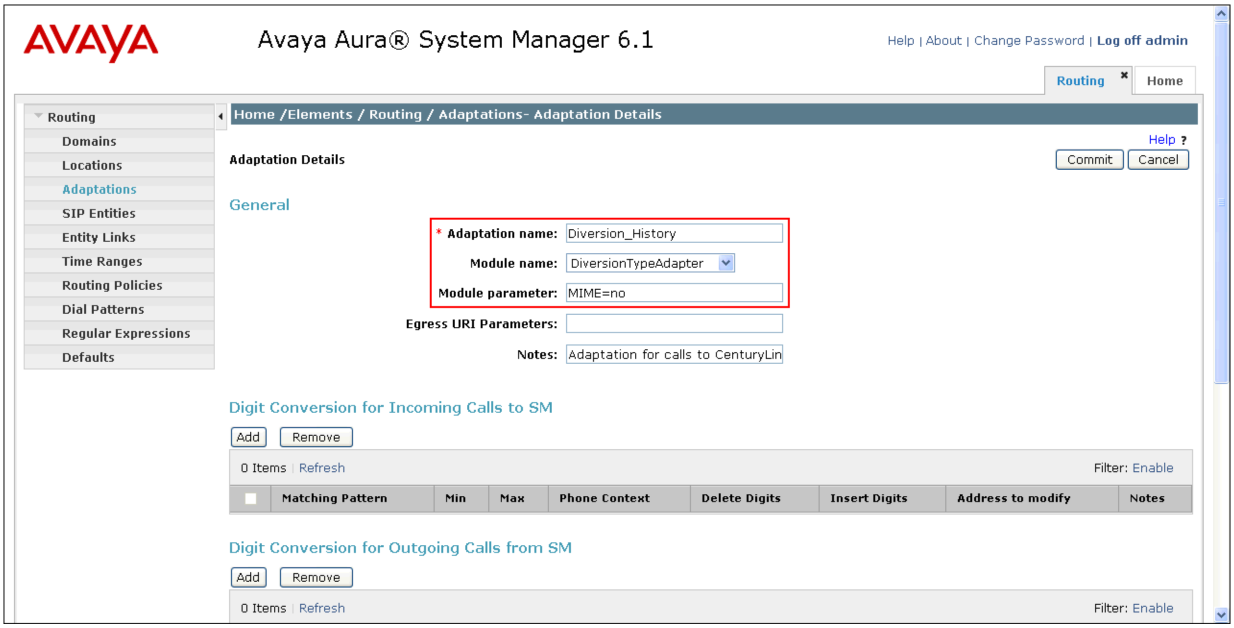
In the **General** section, enter the following values. Use default values for all remaining fields:

- **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 Avaya Aura® Session Manager and for each SIP telephony system connected to it which includes Avaya CS1000 and the 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 that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **Other** for Avaya CS1000 and the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** defined previously.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

To define the ports used by Avaya Aura® 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:

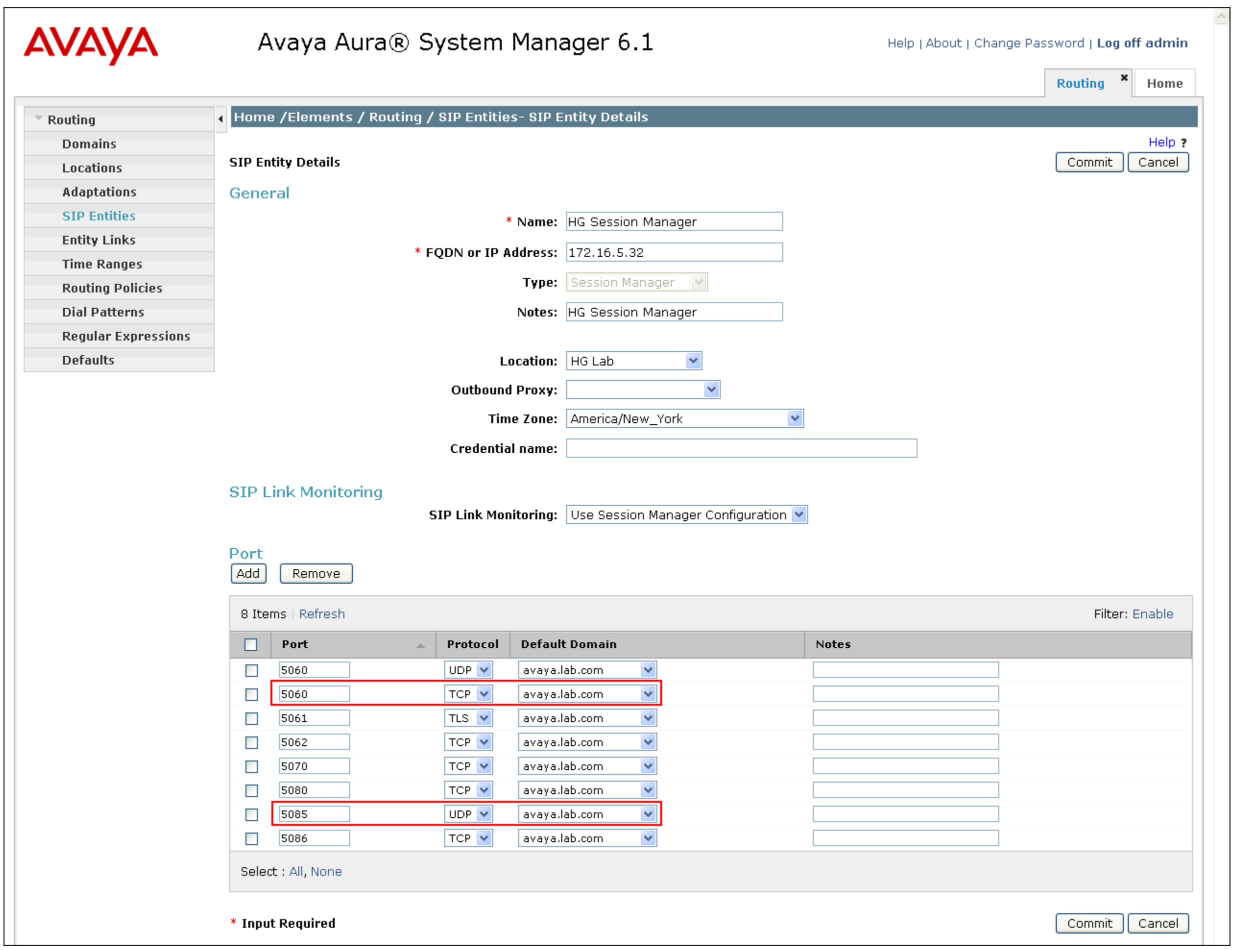
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

For the compliance test, only two Ports were used:

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

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.

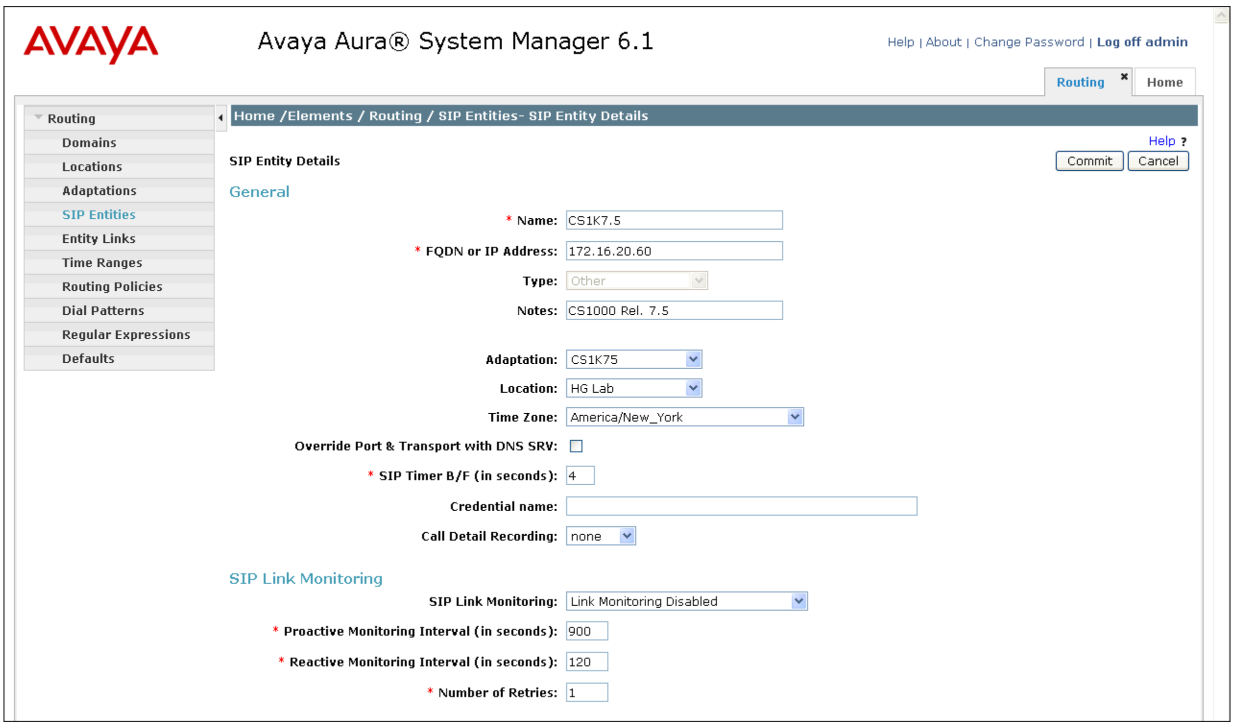


The following screen shows the addition of the Avaya CS1000 SIP entity.

A separate SIP entity for the Avaya CS1000, other than the one created for Avaya Aura® Session Manager during installation, is required in order to send SIP service provider traffic.

For the compliance test the following values were used:

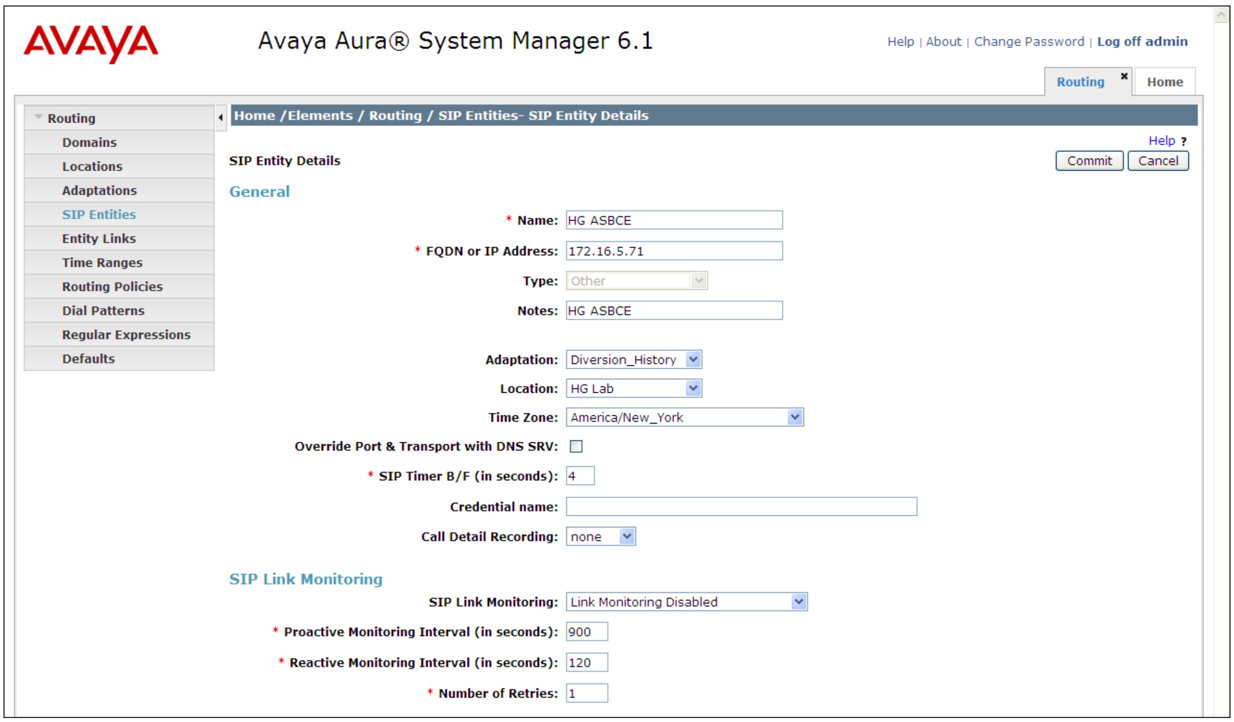
- **Name:** Enter a descriptive name.
- The **FQDN or IP Address** field is set to the TLAN IP address of the CS1000 Signaling Gateway (Node IP address).
- For Adaptation, select the **CS1K75** adaptation previously defined.
- For Location, select the **HG Lab** location previously defined.



The following screen shows the addition of the Avaya SBCE SIP entity.

For the compliance test the following values were used:

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



6.6. Add Entity Links

A SIP trunk between Avaya Aura® Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Avaya CS1000 and one to the 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:

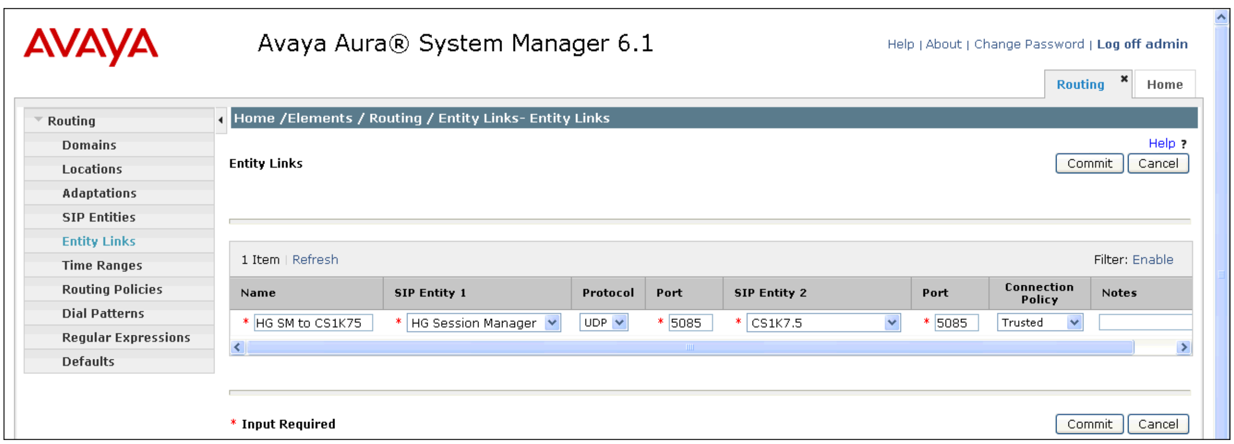
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Avaya Aura® Session Manager.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol defined under **SIP Entities** in **Section 6.5**
- **Port:** Port number on which Session Manager will receive SIP requests. This must match the port defined under **SIP Entities** in **Section 6.5**

- **SIP Entity 2:** Select the name of the other system. For the Avaya CS1000 and Avaya SBCE, select the CS1000 or the Avaya SBCE SIP entity defined in **Section 6.5**.
- **Port:** Port number on which the far-end is listening on. For the Avaya CS1000 this must match the port defined under **SIP Gateway Settings** tab, under **Proxy or Redirect Server** in **Section 5.5.2.** For the Avaya SBCE this must match the port defined under Server Configuration in **Section 7.3.3**
- **Connection Policy:** Select **Trusted** from the pull-down menu (not shown).

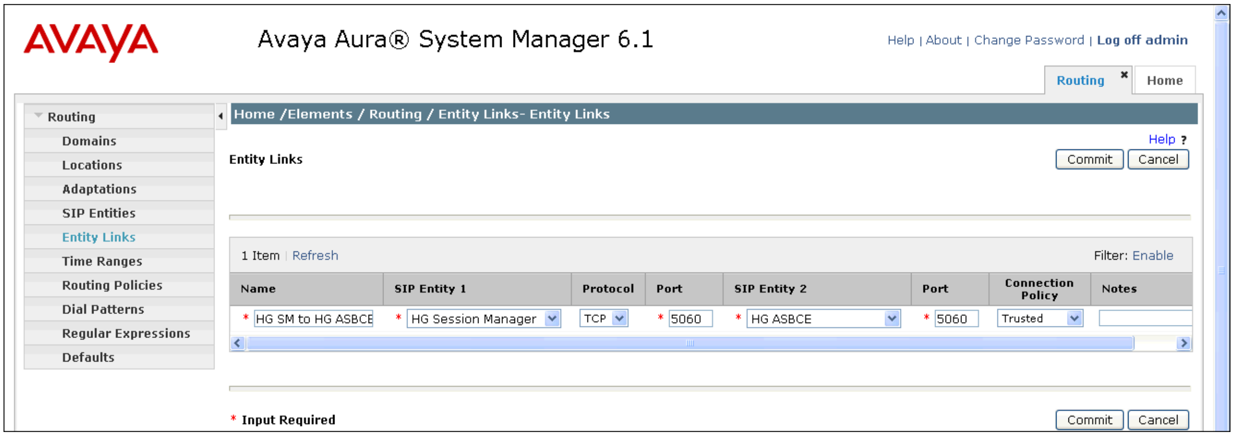
Click **Commit** to save.

It should be noted that in a customer environment the Entity Links to the Avaya CS1000 and to the Avaya SBCE may be configured with a protocol other than the ones shown on the sample configuration. For the compliance test, TCP was used to the Avaya SBCE and UDP was used to the CS1000 to aid in troubleshooting. The protocol and ports defined here must match the values used on the Avaya CS1000 and the Avaya SBCE.

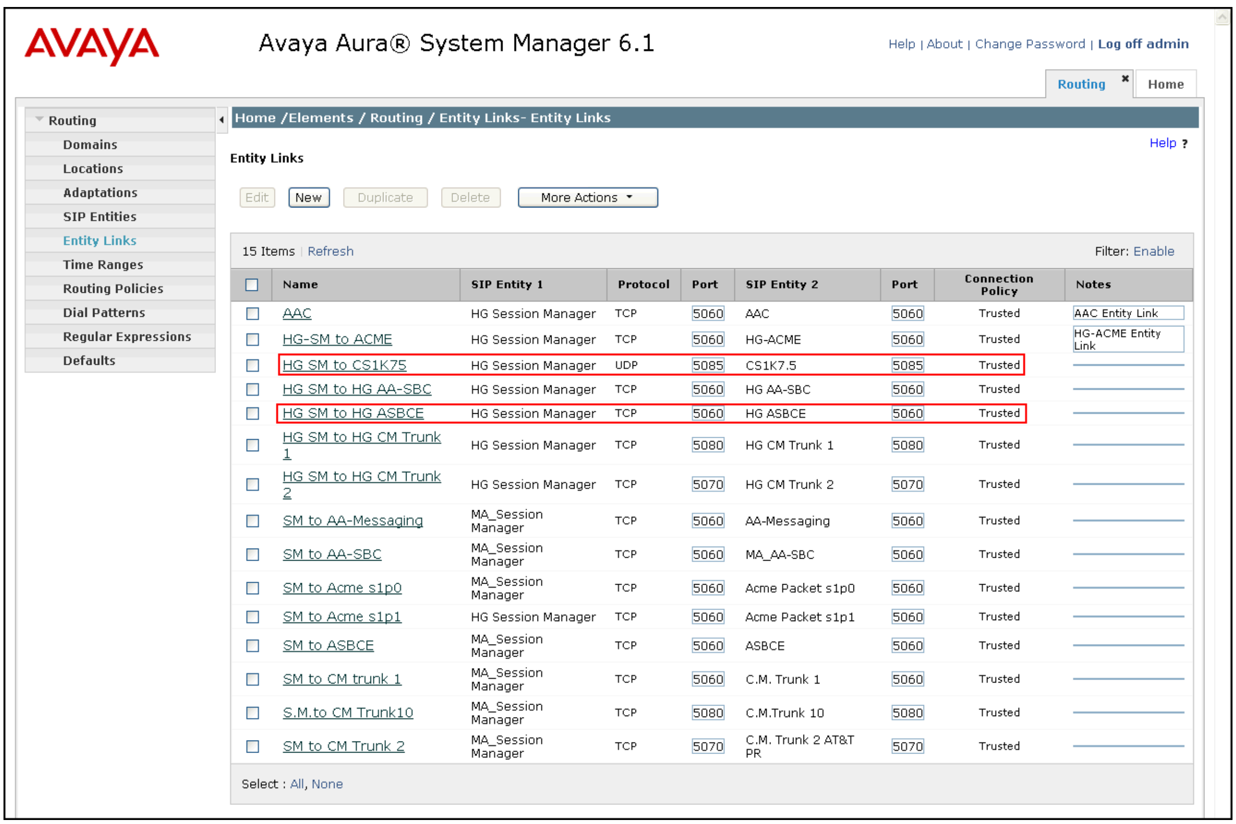
The following screens illustrate the Entity Link between Avaya Aura® Session Manager and the Avaya CS1000.



The following screens illustrate the Entity Link between Avaya Aura® Session Manager and 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 ones relevant to these Application Notes.



6.7. Add Routing Policies

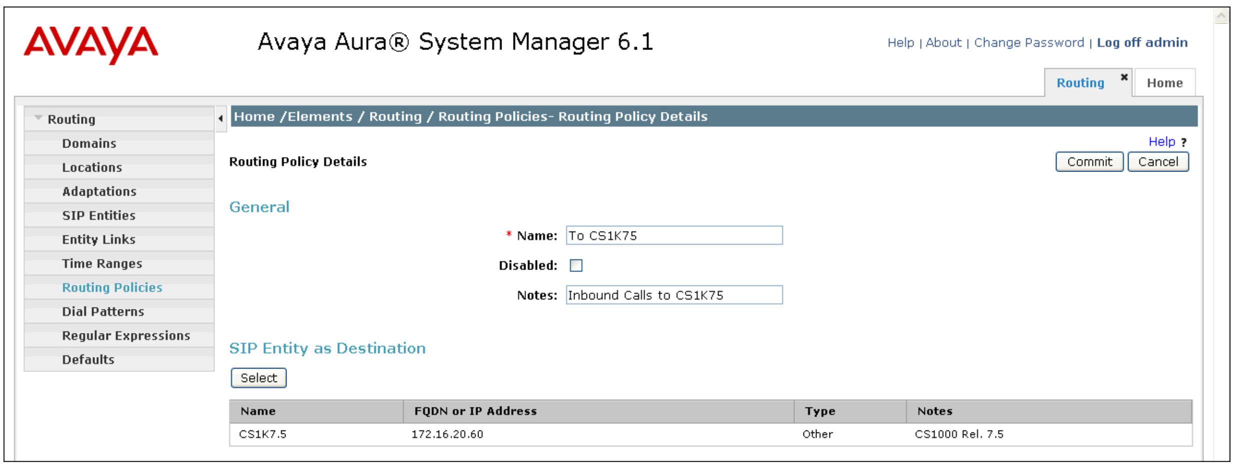
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for the Avaya CS1000 and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation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

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

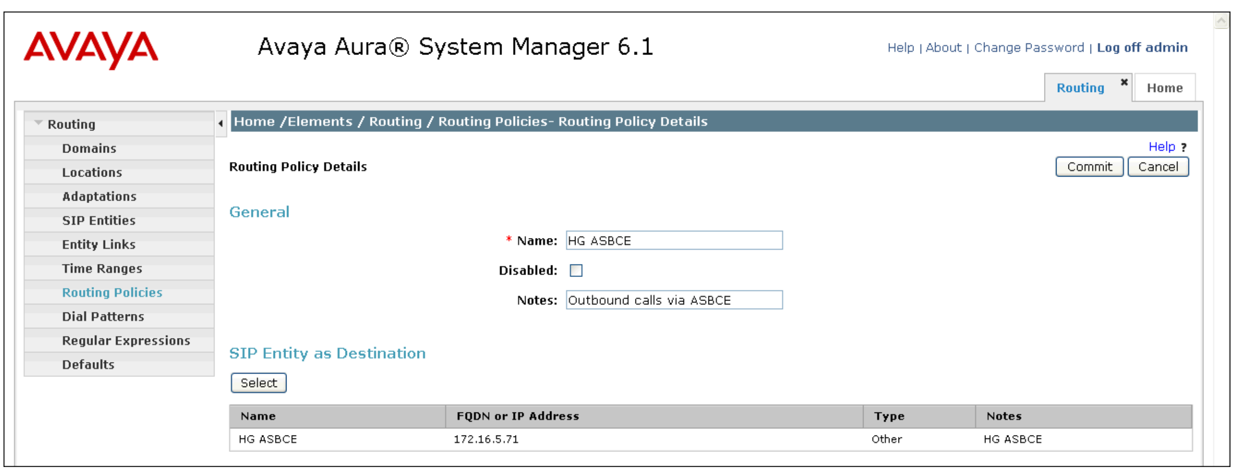
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

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 show the Routing Policy for the Avaya CS1000.



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



6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Avaya Aura® Session Manager. For the compliance test, dial patterns were needed to route calls from Avaya CS1000 to CenturyLink 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-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

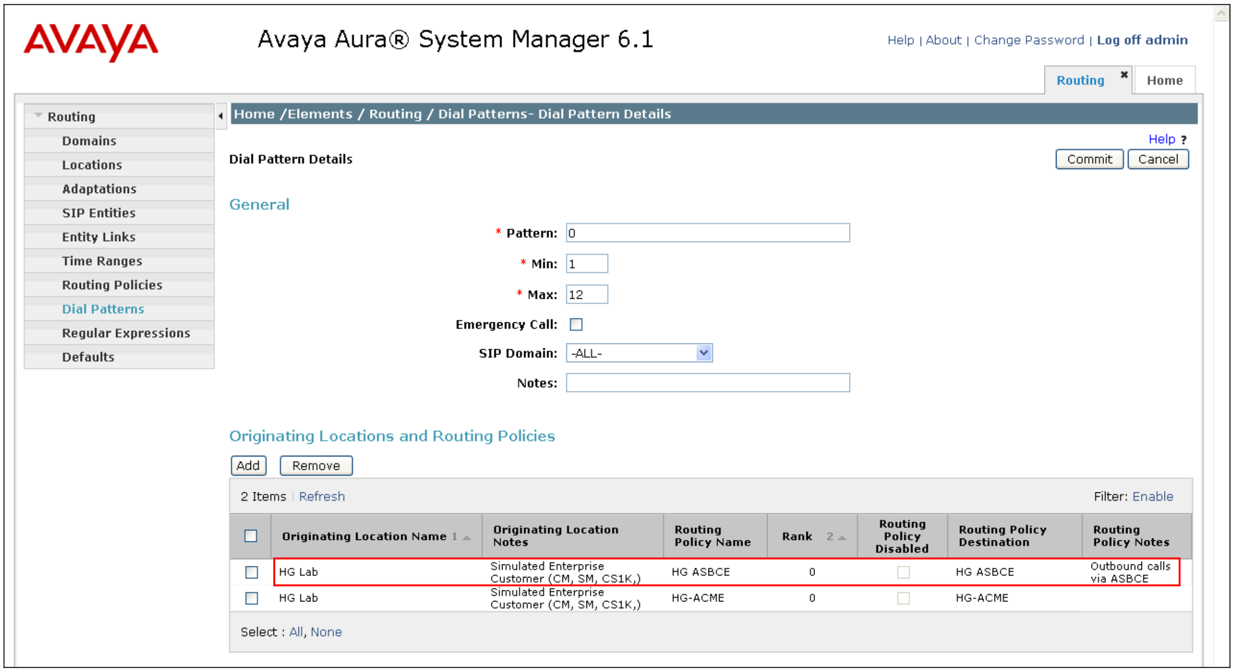
In the **General** section, enter the following values. Use default values for all remaining fields:

- **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 used in the match criteria.
- **Notes:** Add a brief description (optional).

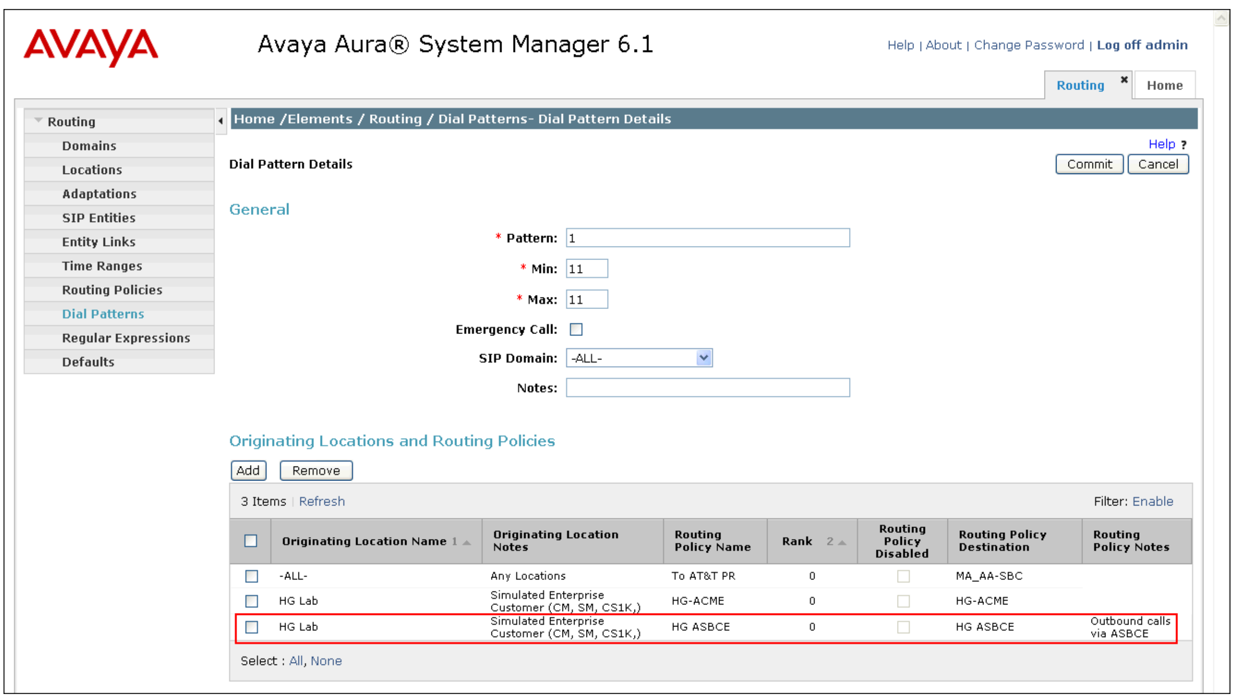
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

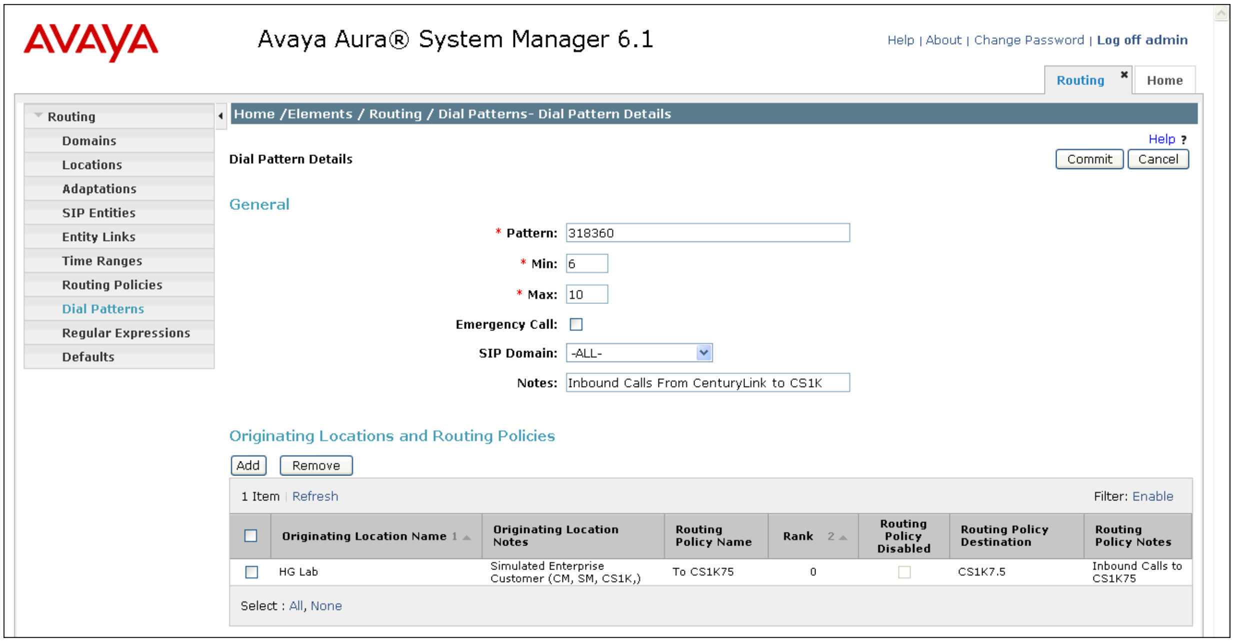
Examples of the dial patterns used for the compliance testing are shown below. The first example shows dial pattern "**0**" for calls to the Operator, have a destination domain of **ALL** (since it's shared among other test activities in the lab), **Originating Location Name** of **HG Lab,** uses **Routing Policy Name** of **HG ASBCE.**



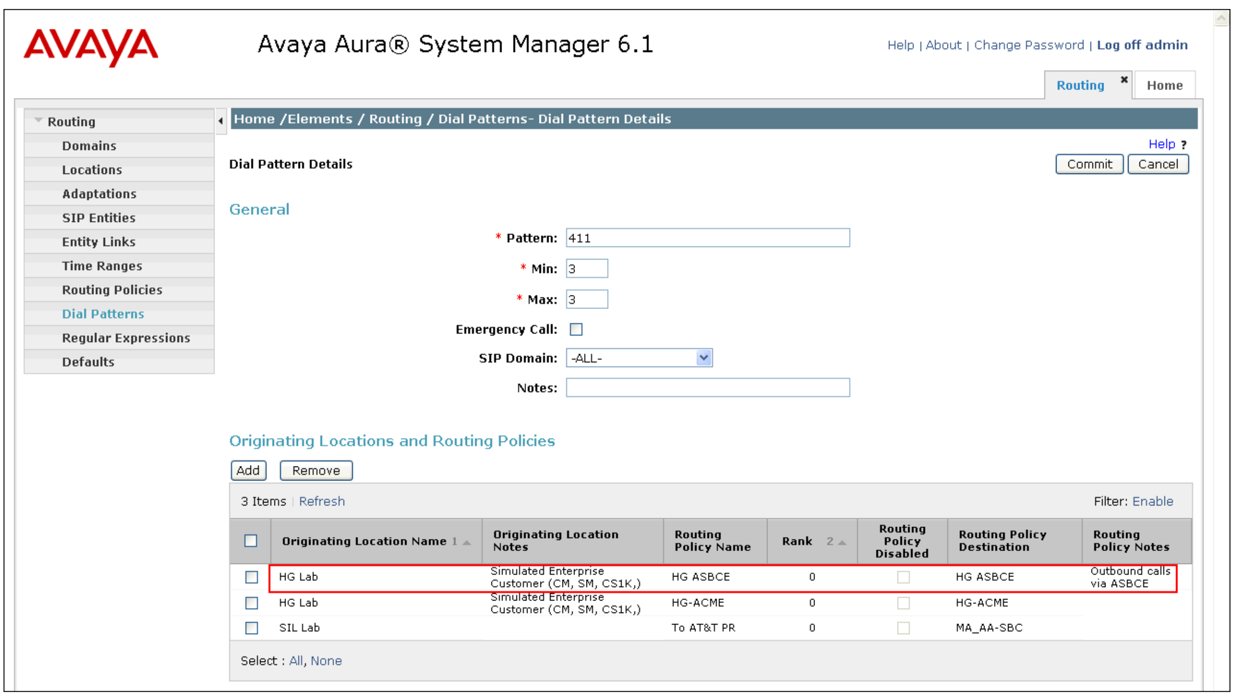
The next example shown below is for dial pattern "**1**" for the North American Numbering Plan area prefix, have a destination domain of **ALL** (since it's shared among other test activities in the lab), **Originating Location Name** of **HG Lab,** uses **Routing Policy Name** of **HG ASBCE.**



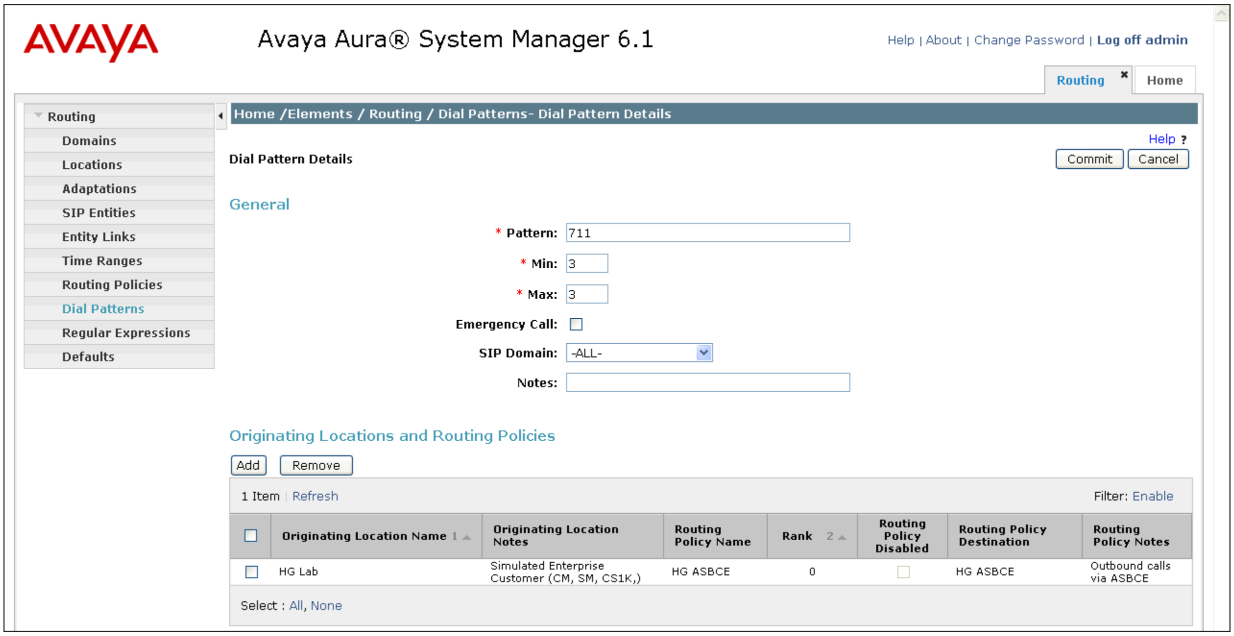
The next example shown below is for dial pattern "**318360**" to route inbound calls to DID numbers provided by CenturyLink (DID numbers assigned to extensions in the CS1000), have a destination domain of **ALL**, **Originating Location Name** of **HG Lab,** uses **Routing Policy Name** of **To CS1K75.**



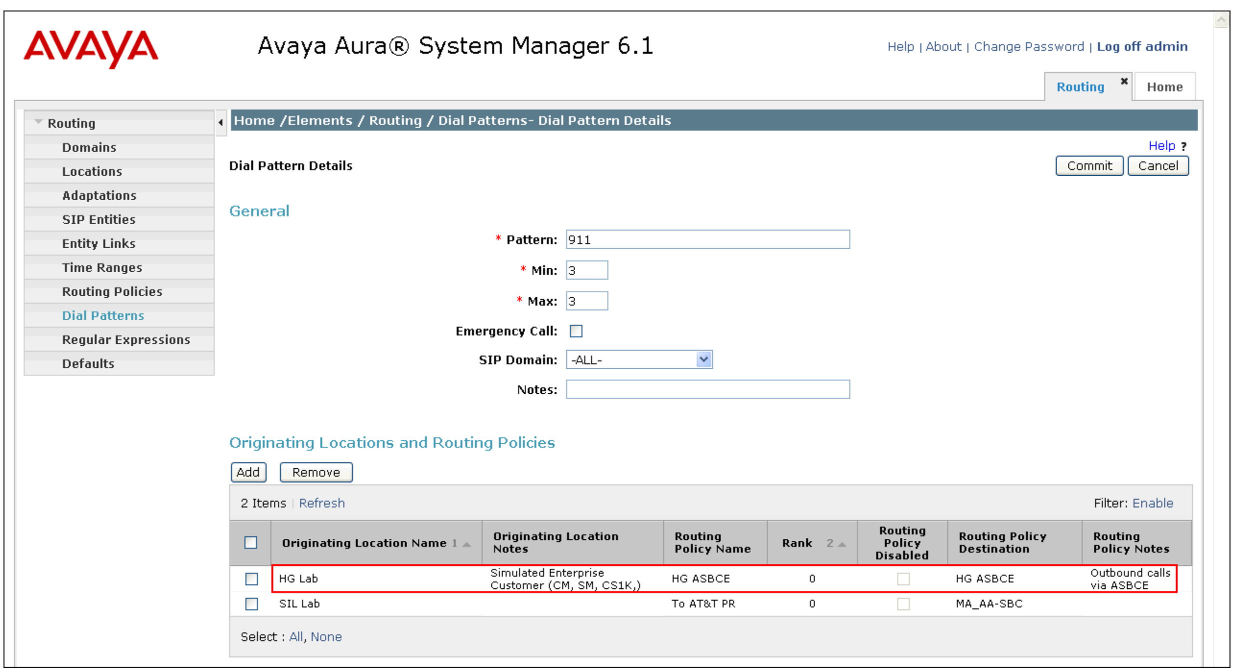
The next example shown below is for dial pattern "**411**" for calls to Directory Assistance, have a destination domain of **ALL** (since it's shared among other test activities in the lab), **Originating Location Name** of **HG Lab,** uses **Routing Policy Name** of **HG ASBCE.**



The next example shown below is for dial pattern “**711**” for calls for Telecommunications Relay Service, have a destination domain of **ALL** (since it’s shared among other test activities in the lab), **Originating Location Name** of **HG Lab,** uses **Routing Policy Name** of **HG ASBCE.**



The next example shown below is for dial pattern “**911**” for emergency calls, have a destination domain of **ALL** (since it’s shared among other test activities in the lab), **Originating Location Name** of **HG Lab,** uses **Routing Policy Name** of **HG ASBCE.**



6.9. Add/View Avaya Aura® Session Manager

The creation of an Avaya Aura® Session Manager element provides the linkage between Avaya Aura® System Manager and Avaya Aura® Session Manager. This was most likely done as part of the initial Avaya Aura® Session Manager installation. To add an Avaya Aura® 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 the Avaya Aura® 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 IP address of Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **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 this Avaya Aura® Session Manager. The screen below shows the Avaya Aura® Session Manager values used for the compliance test.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Home /Elements / Session Manager / Session Manager Administration- Session Manager Administration
Help ?
View Session Manager
Return
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All
General
SIP Entity Name HG Session Manager
Description Lab-HG SM
Management Access Point Host Name/IP 172.16.5.31
Direct Routing to Endpoints Enable
Security Module
SIP Entity IP Address 172.16.5.32
Network Mask 255.255.255.0
Default Gateway 172.16.5.254
Call Control PHB 46
QOS Priority 6
Speed & Duplex Auto
VLAN ID

7. Configure the Avaya Session Border Controller for Enterprise.

This section describes the required configuration of the Avaya SBCE to connect to CenturyLink BroadWorks SIP Trunk service. This configuration is done in two stages. The first part or initial configuration is done via the Provisioning Script, which requires a serial connection between a terminal device and the Console port of the Avaya SBCE.

Once the Avaya SBCE is provisioned and ready to be used on the IP network, the remainder of the configuration is accomplished using the Avaya SBCE web interface.

It is assumed in these Application Notes that the Avaya SBCE contains no previous configuration, and it is being provisioned for the first time.

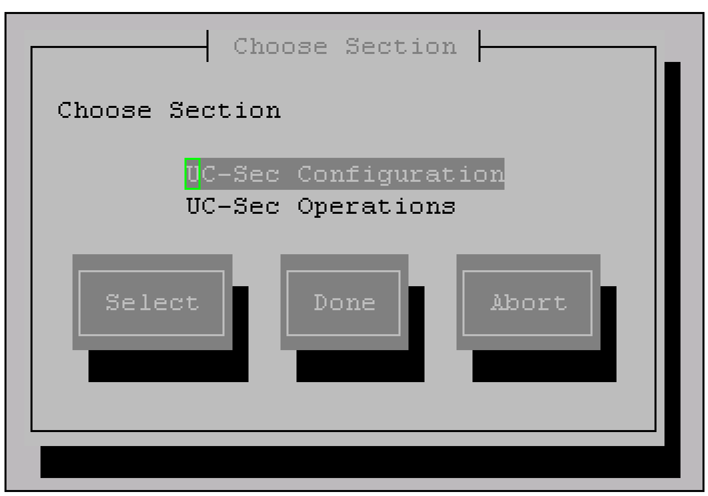
7.1. Provisioning Script

Use the following procedure to establish the initial serial connection to the Avaya SBCE:

- Connect a DB9 serial communications cable from a PC or terminal device to the Console port in the back of the Avaya SBCE.
- Configure the communications parameters of the terminal program in the PC, like HyperTerminal or Putty, to the following settings: **Baud rate: 19200, Data Bits: 8, Stop Bits: 1, Parity: None**
- Apply power to the chassis.

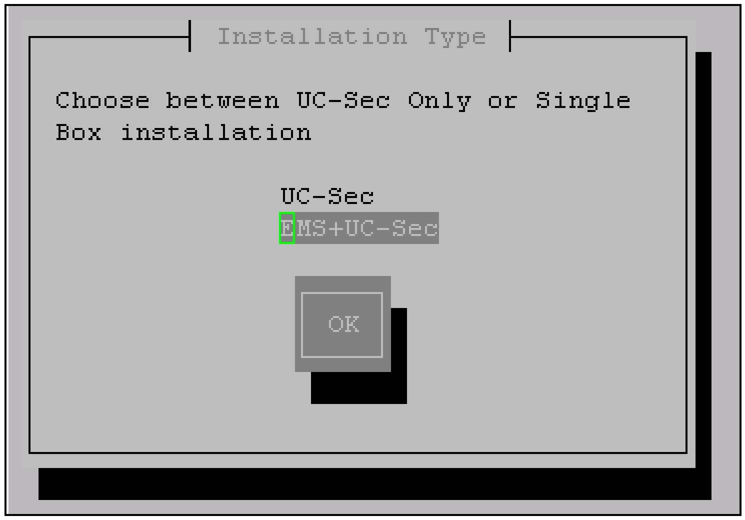
Once power has been applied to the Avaya SBCE, a series of scripts run automatically preparing the chassis to be configured. The provisioning process is ready to be completed when the prompt **Press ENTER to continue…** is displayed. Press the **ENTER** key.

The Top Level Provisioning Screen is displayed. Use the arrows to select **UC-Sec Configuration** and press **ENTER**.

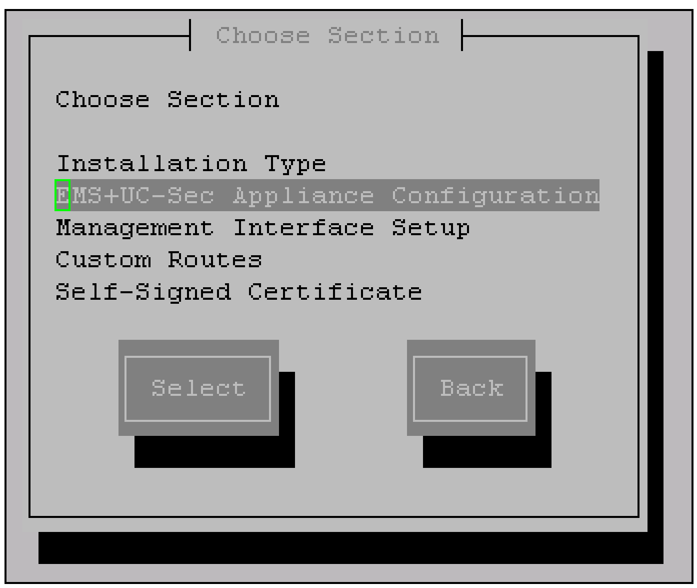


The Provisioning screen is displayed (not shown). **Select Installation Type**. Press **Select.**

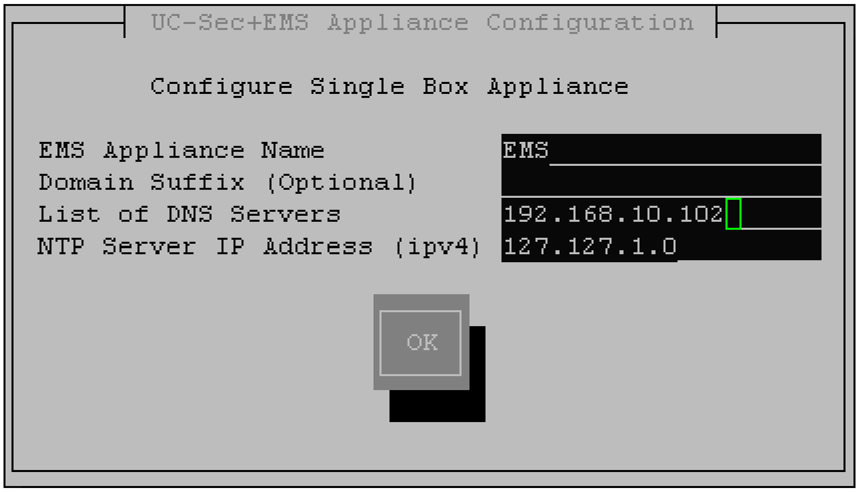
In our test scenario, both the SBC (UC-Sec) and the Element Management System (EMS) reside in the same server. Select **EMS+UC-Se**c for a single box installation. Click **OK**.



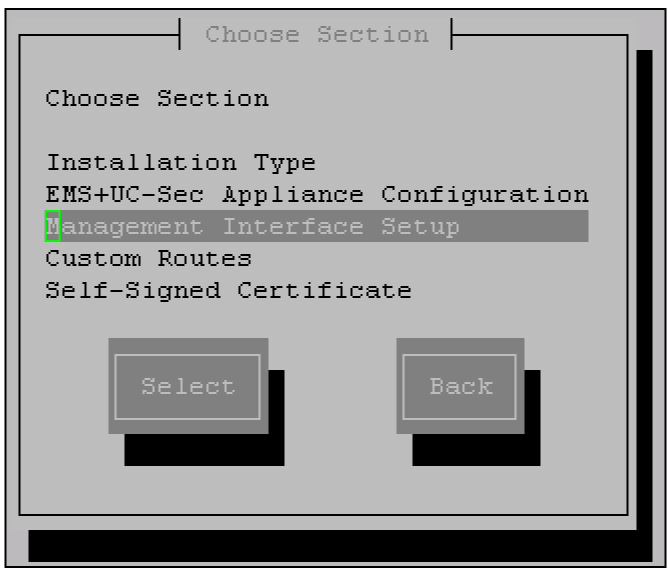
On the next screen, the EMS+UC-Sec Provisioning screen, select **EMS+UC- SEC Appliance Configuration.** Press **Select.**



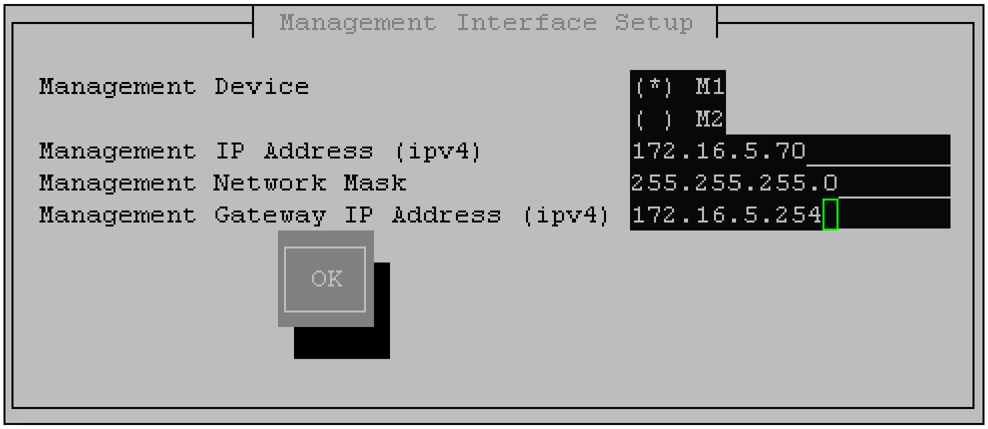
Enter the required information into the appropriate fields. Click **OK**.



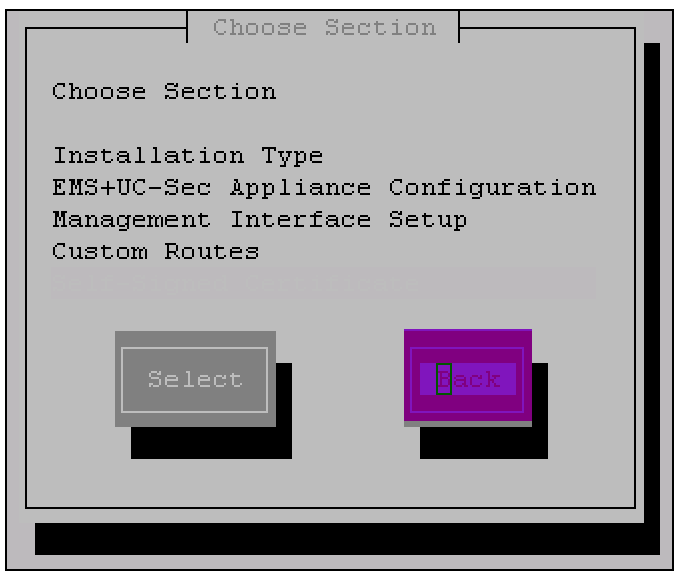
In the same EMS+UC-Sec Provisioning screen previously shown (shown below), select **Management Interface Setup** and press **Select**.



Select the **M1 Management Device**, and enter the IP address, Netmask and Gateway to be used to manage the Avaya SBCE on the network. Click **OK**.



Press **Back** at EMS+UC-Sec Provisioning screen. This will bring up the Top Level Provisioning screen. Select **Done**.

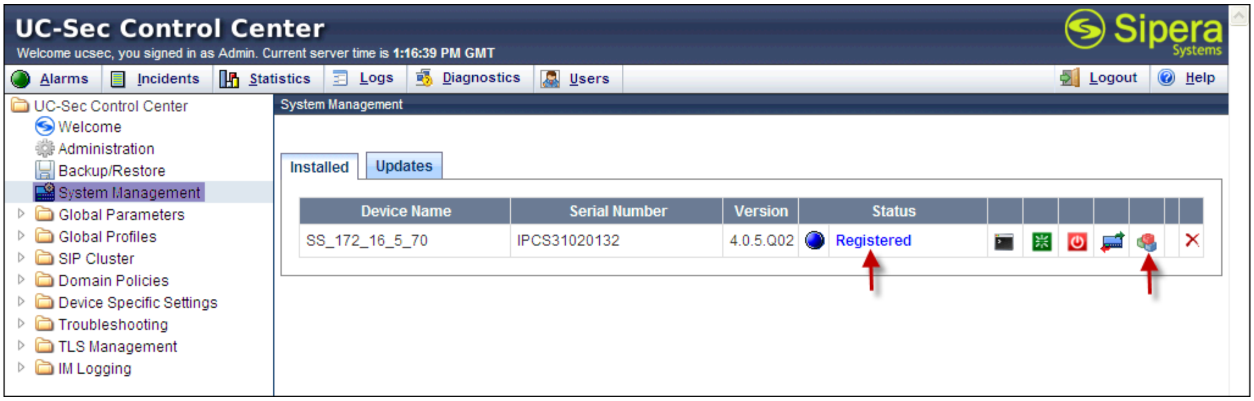


At this point the initial configuration is complete and the Avaya SBCE is ready to be administered via the browser through the Management Interface.

7.2. Install Device

Log on to the Avaya SBCE web interface by pointing a browser to the previously configured management interface address. For the Compliance Test, this was **https://172.16.5.70.** Click the **UC-Sec Control Center** box. Log in using the proper credentials (the GUI default password for the account "ucsec" is "ucsec"). Once in the UC-Sec Control Center home page, on the left hand side navigation panel select **System Management.** Select the **Installed** tab.

After the Avaya SBCE has been initially installed and connected to the network, it will show the status of **Registered**. In addition, the **Install Device** icon, (right arrow on the screen capture shown below), is displayed only for the devices which have not yet been configured.

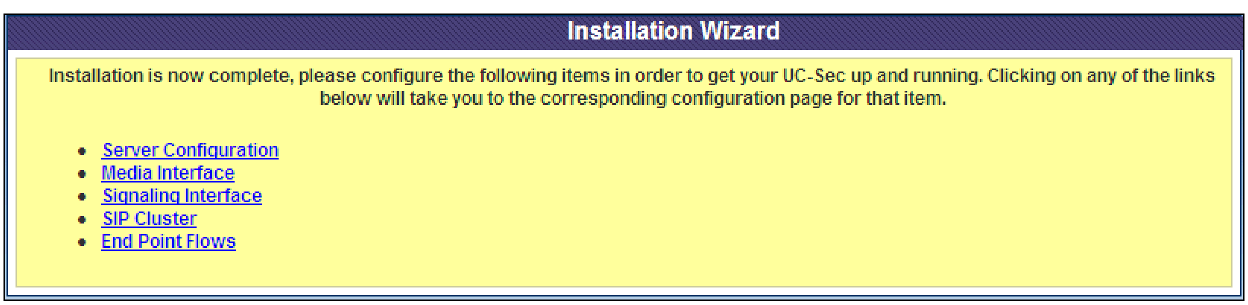


Click the **Install Device** icon (right arrow on the screen capture shown above).

On the Installation Wizard that follows, fill in the required information for the **Appliance Name**, DNS servers and the Private (A1) and Public (B1) interfaces of the Avaya SBCE as shown. Click **Finish** when done.

For the Public (B1) interface, enter the public IP address (outside address), **Netmask** and **Gateway**.

The last screen in the Wizard is a basic reminder of topics that need to be visited in order to complete the configuration. It can be closed at this point.



7.3. Global Profiles

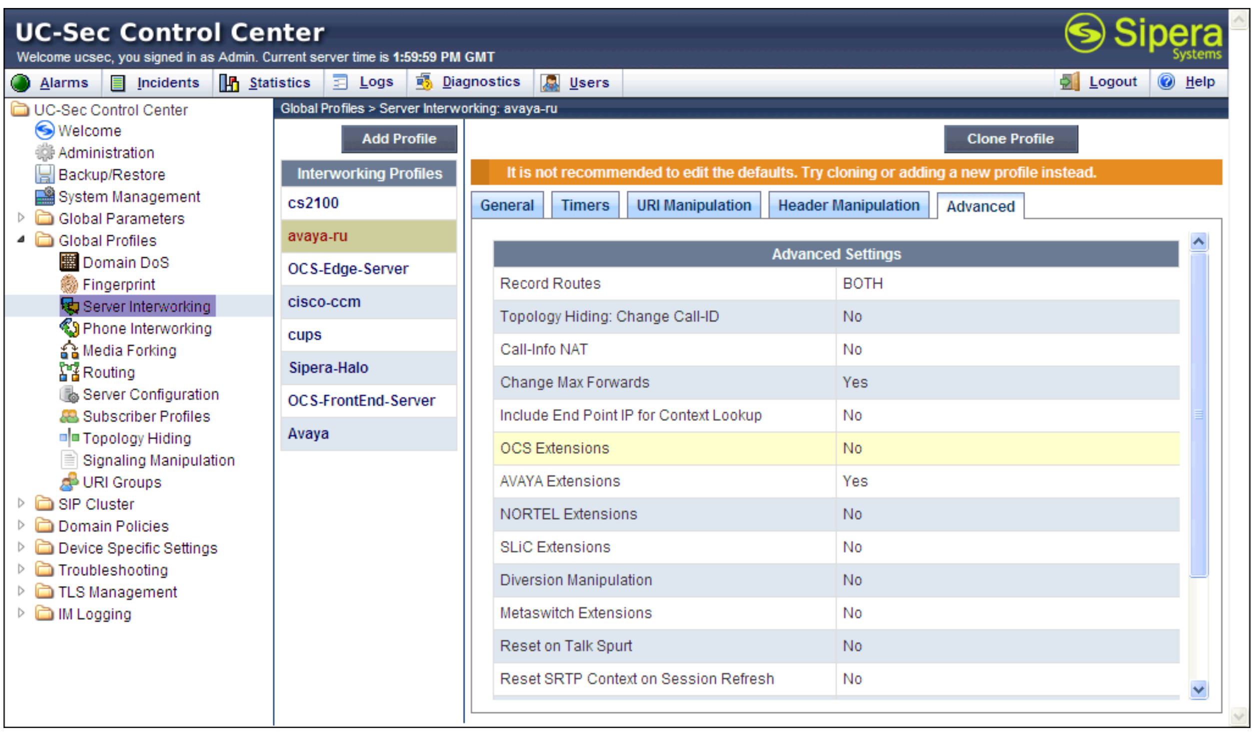
The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the EMS control.

7.3.1. Server Interworking

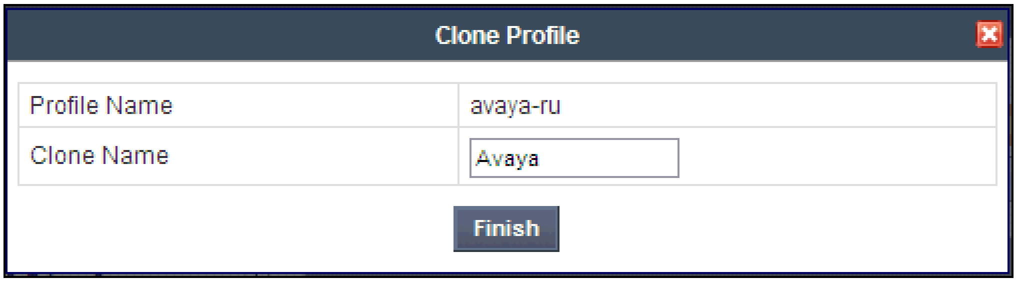
Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

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

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

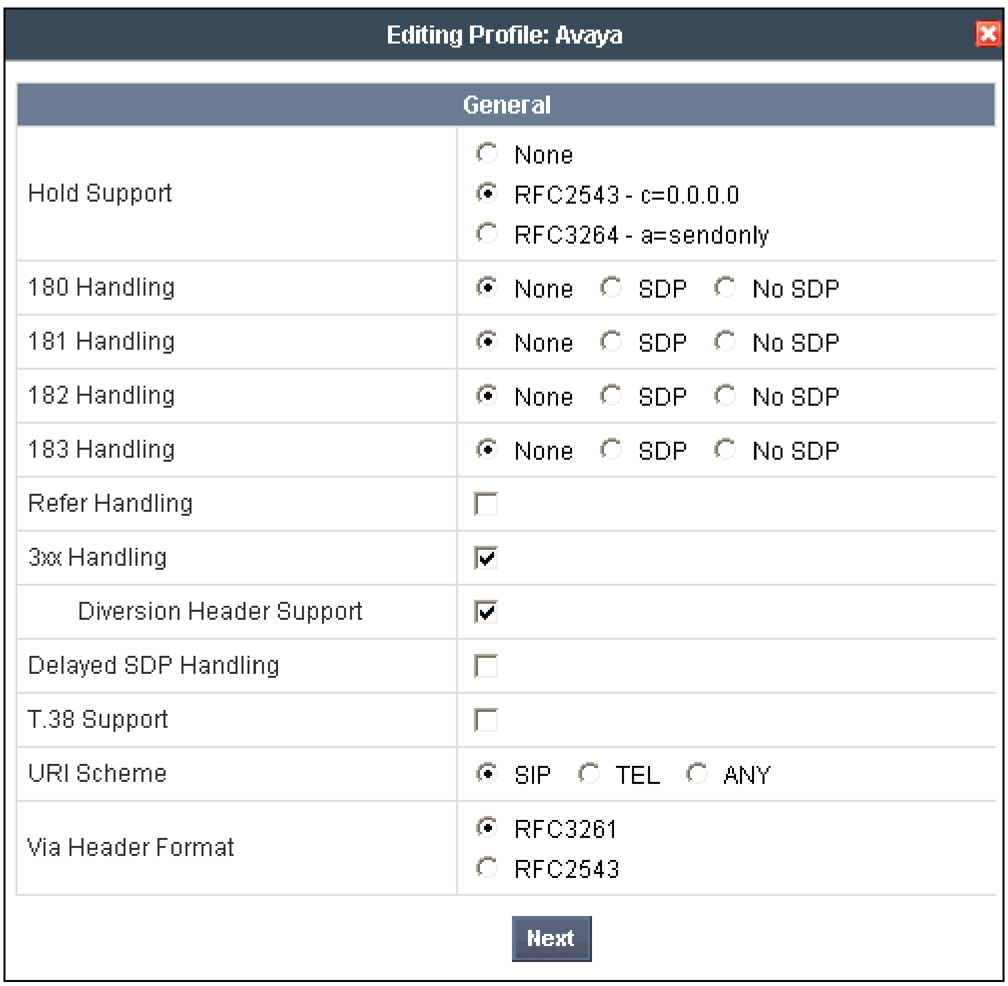


Enter the new profile name in the **Clone Name** field. Click **Finish**.

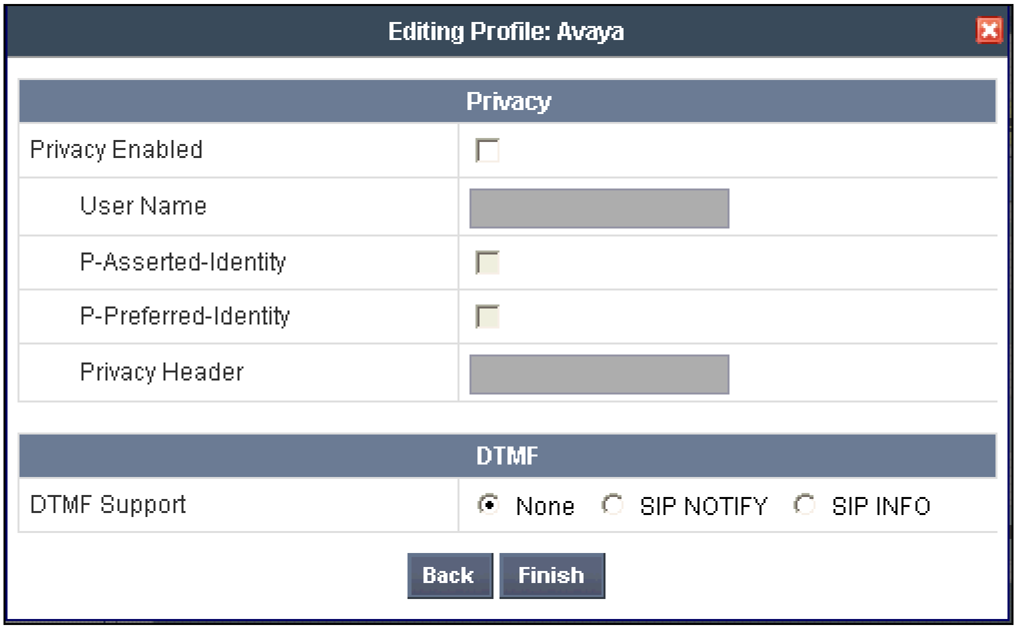


For the newly created Avaya profile, click **Edit** (not shown) at the bottom of the General tab

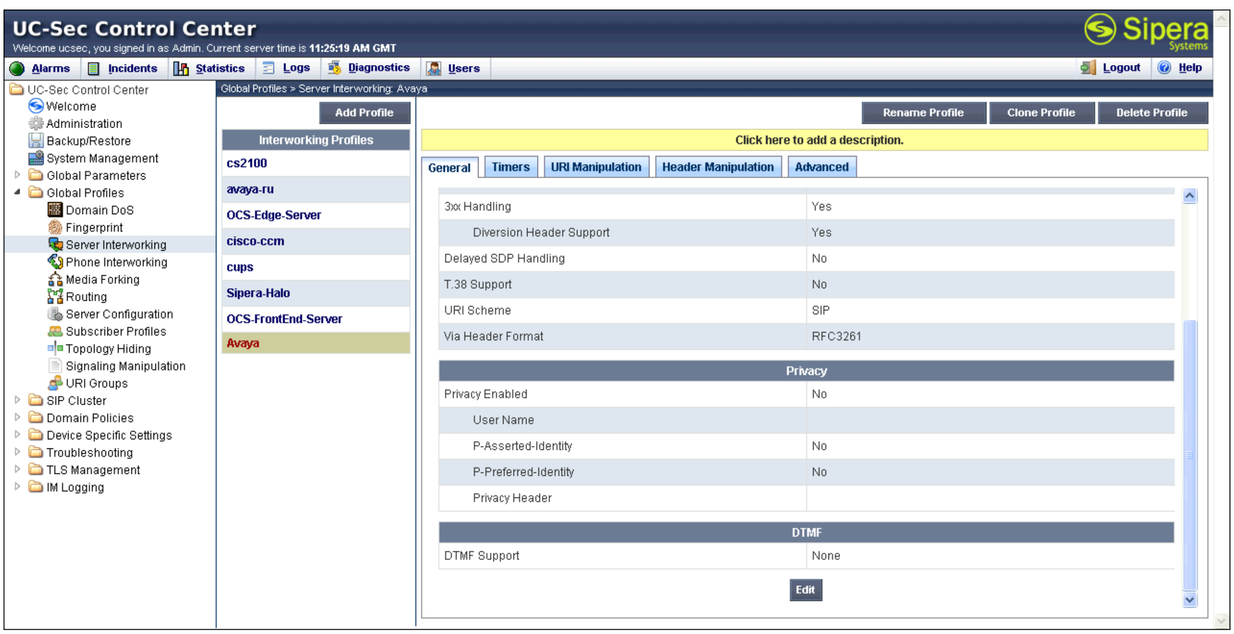
- Verify that for **Hold Support**, **RFC2543** is selected.
- Verify that **3xx Handling** and **Diversion Header Support** are selected.
- Leave other fields with their default values.
- Click **Next**.



Click **Finish** on the **Privacy and DTMF** tab.



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



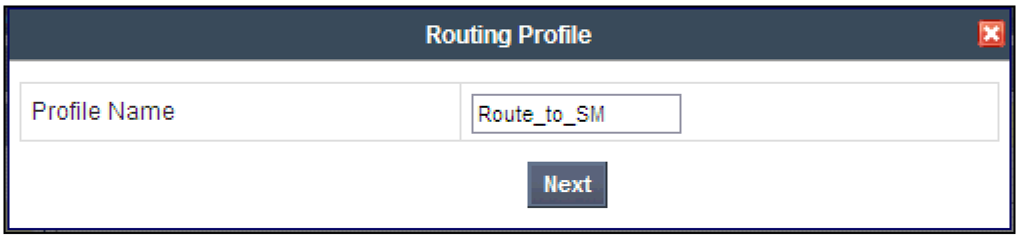
7.3.2. Routing Profiles

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:

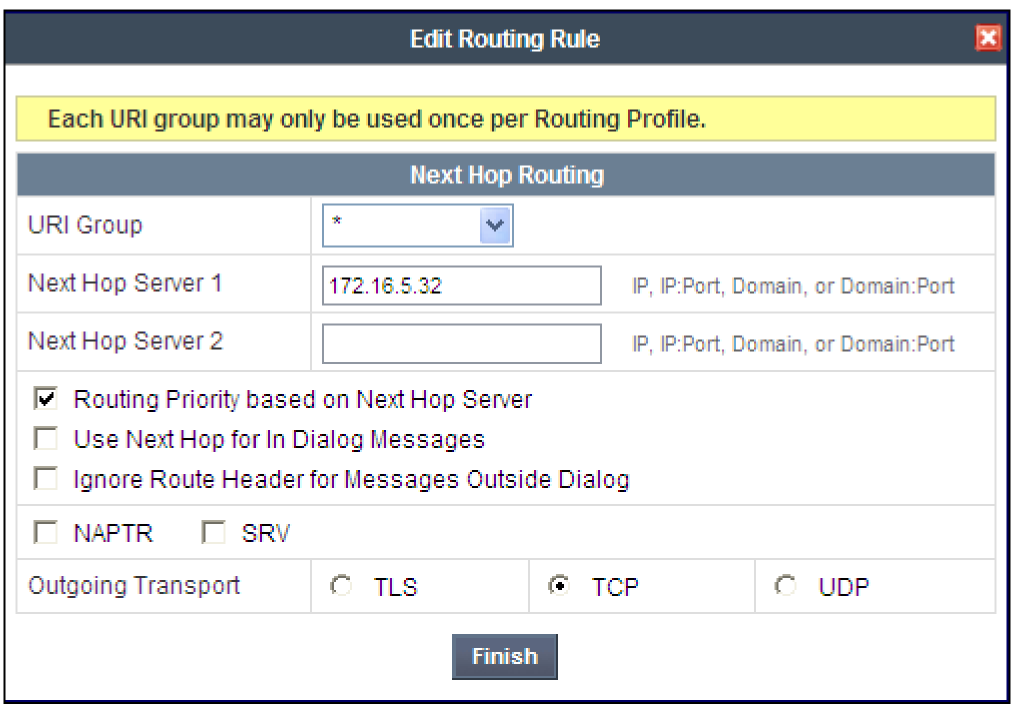
- Select **Routing**.
- Select **Add Profile.**
- Enter Profile Name: **Route_to_SM.**
- Click **Next.**



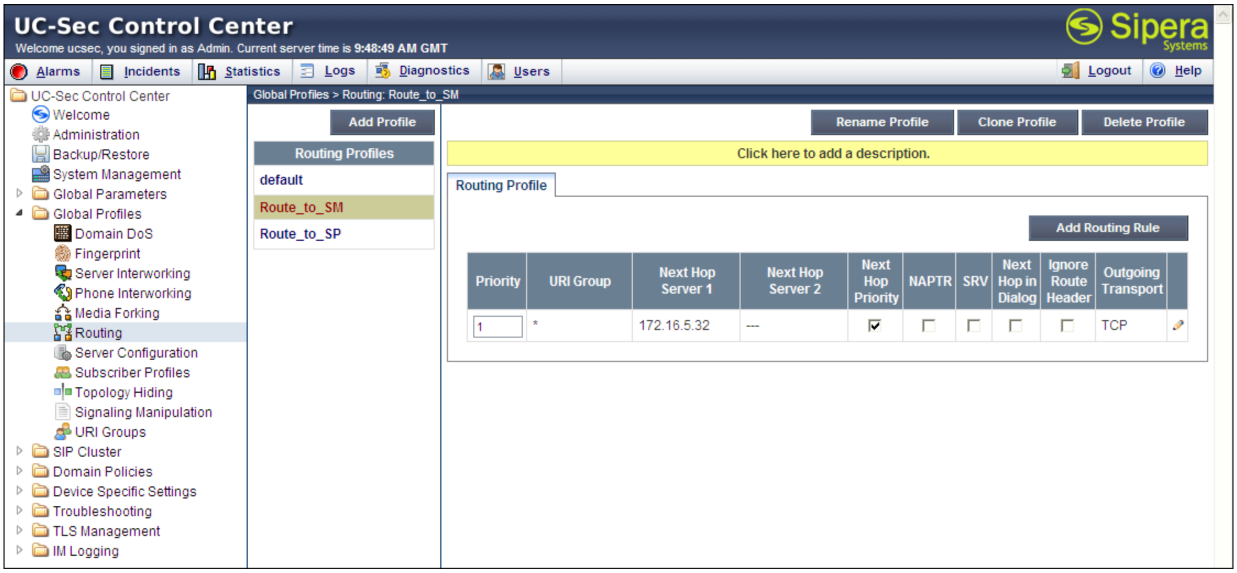
On the next screen, complete the following:

- **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.**

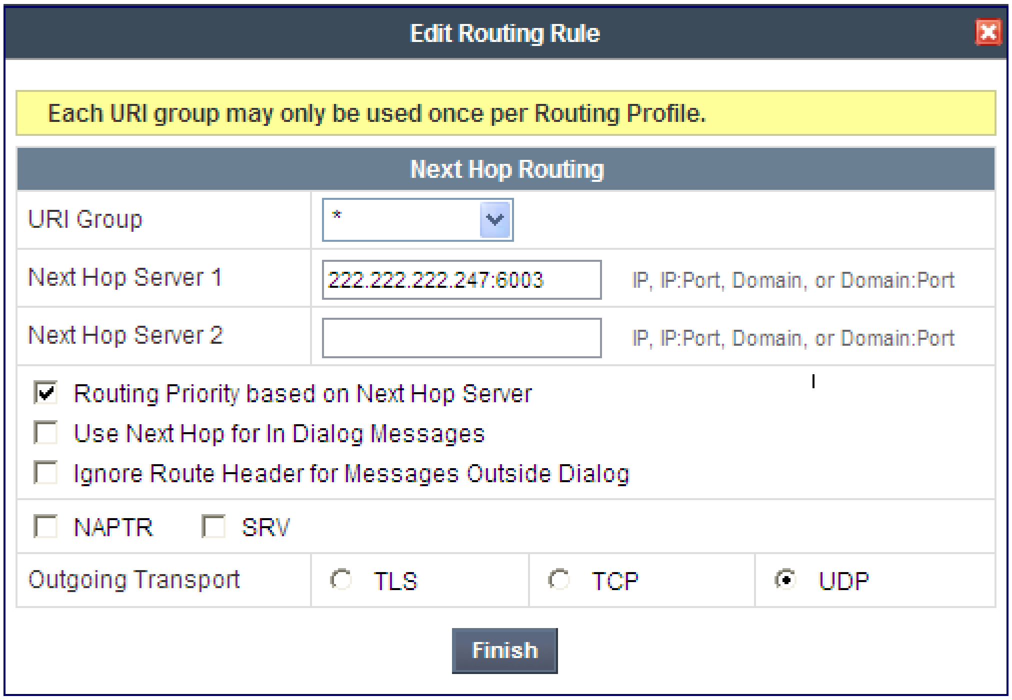


The following screen shows the newly added **Route_to_SM** Profile.

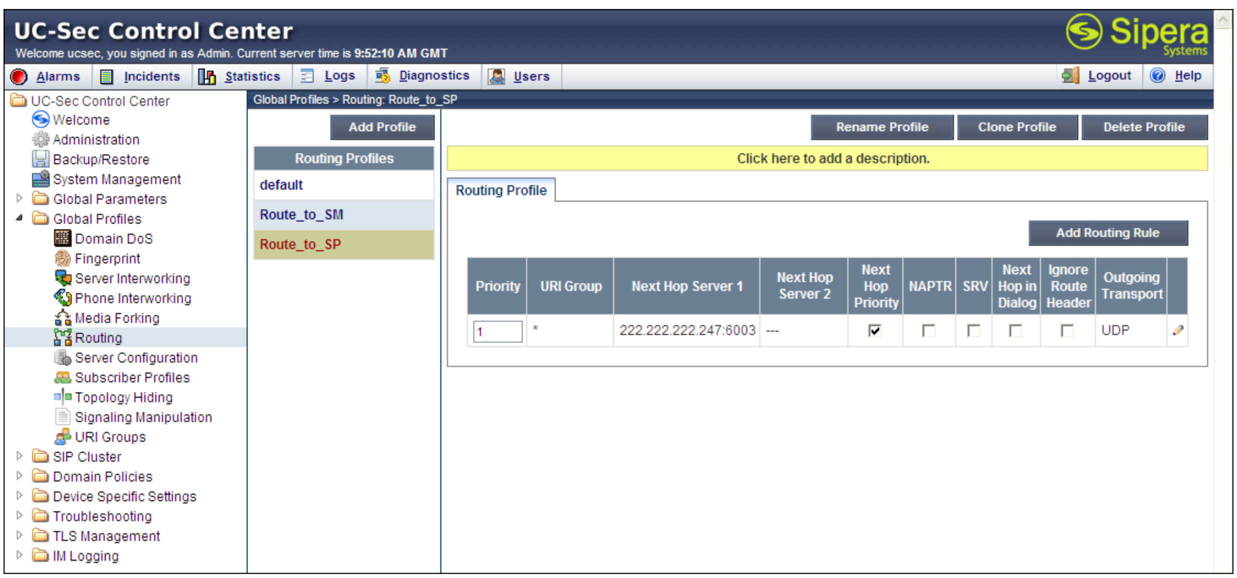


Similarly, for the outbound route:

- Select **Add Profile.**
- Enter Profile Name: **Route_to_SP**
- Click **Next.**
- **Next Hop Server 1: 222.222.222.247:6003** (service provider **SIP Proxy IP:Port).**
- 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.



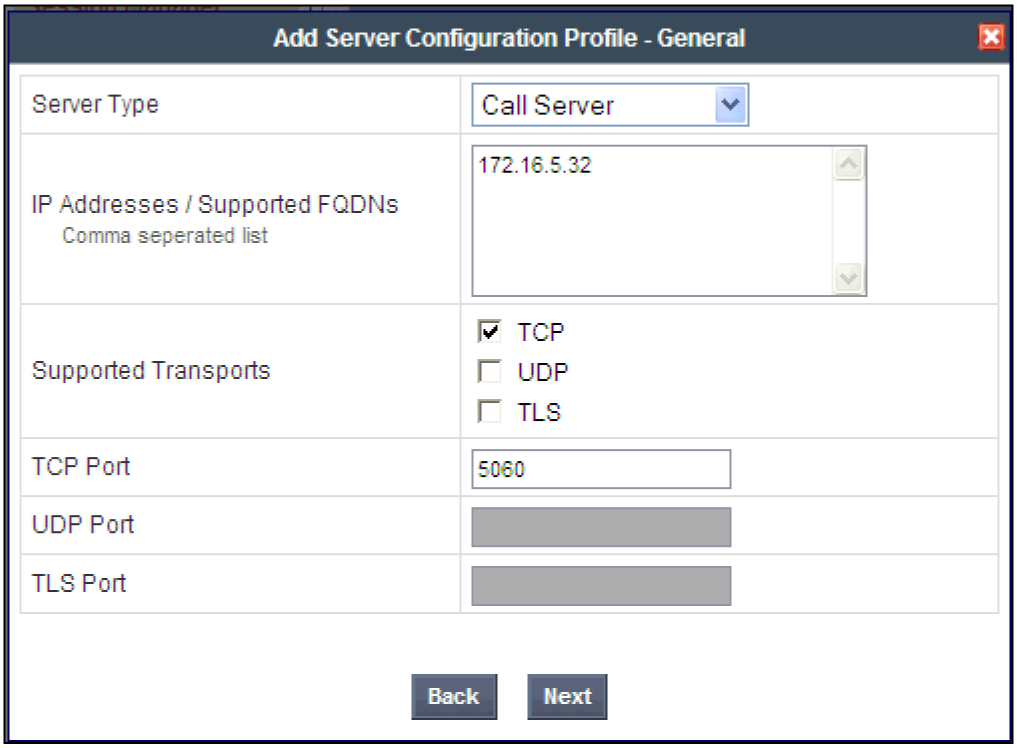
7.3.3. Server Configuration

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.

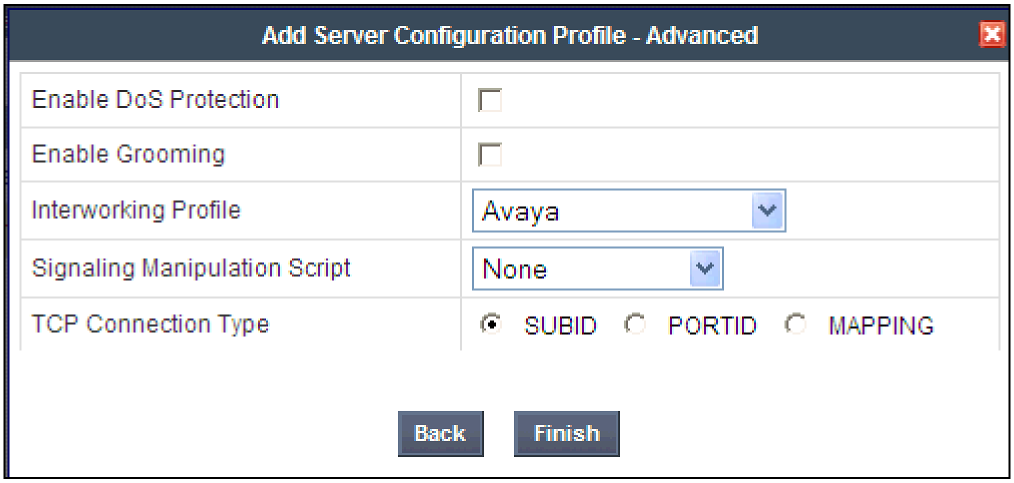
To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add Profile** and enter the profile name: **Session Manager**.

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

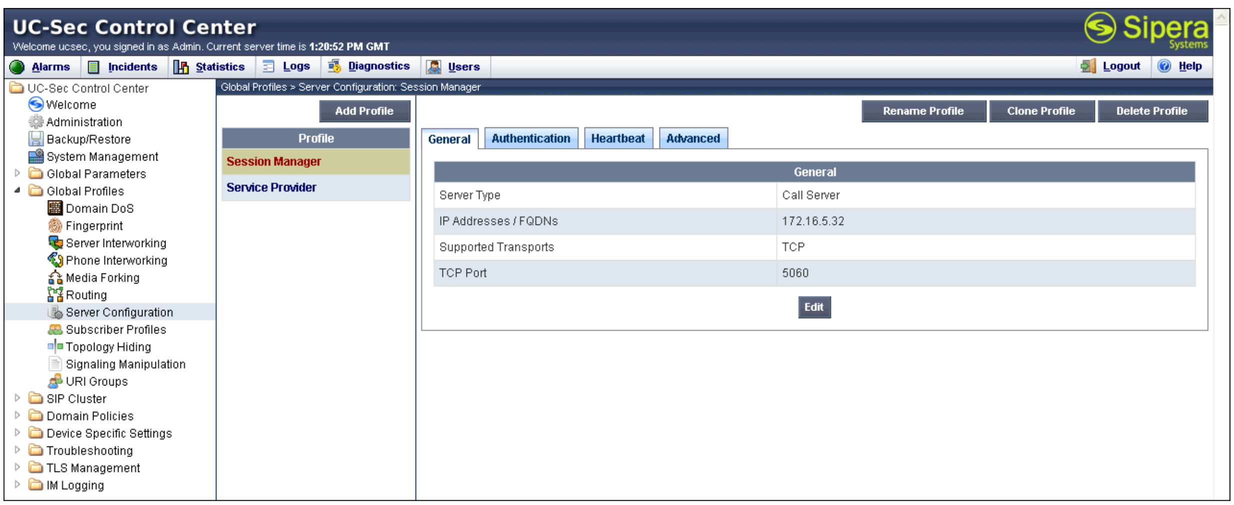
- Select **Server Type: Call Server**
- **IP Address: 172.16.5.32 (IP Address of Session Manager Security Module)**
- **Supported Transports**: Check **TCP**
- **TCP Port: 5060**
- Click **Next**



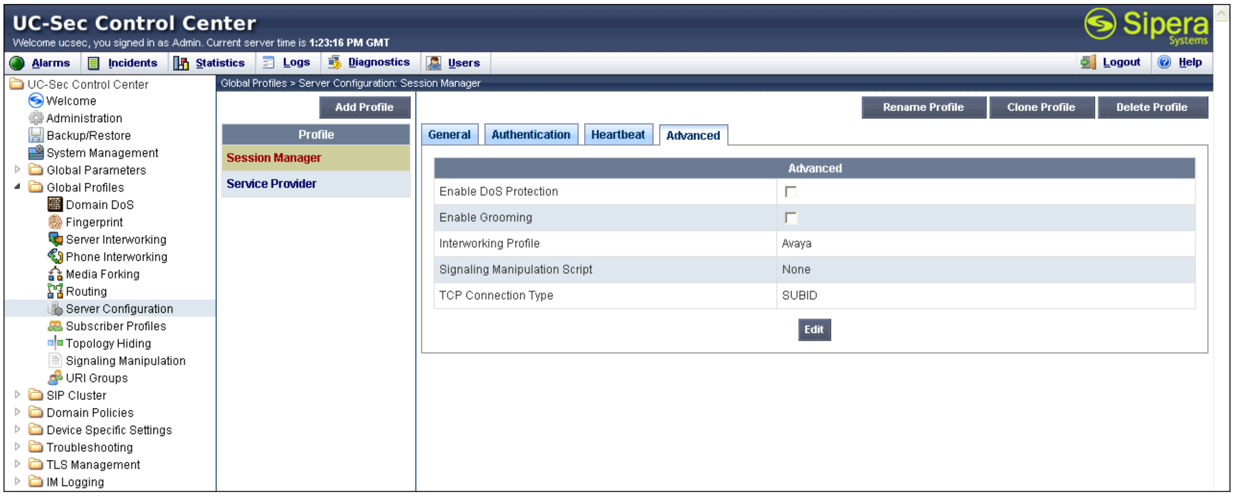
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish.**



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



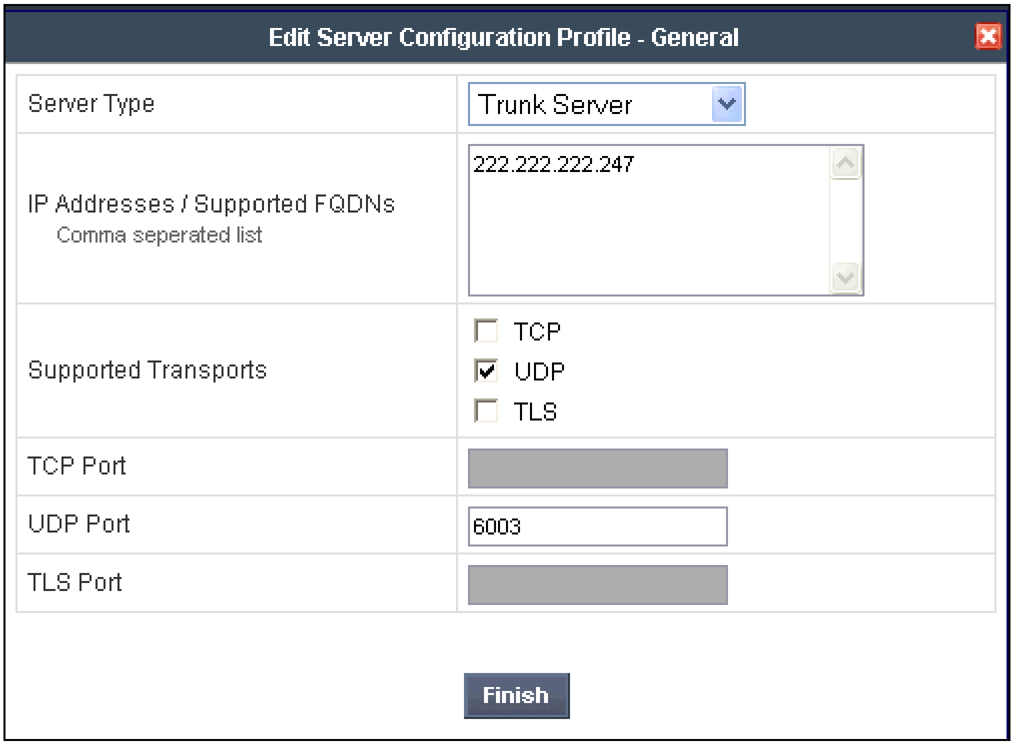
The following screen capture shows the **Advanced** tab of the added **Session Manager** Profile.



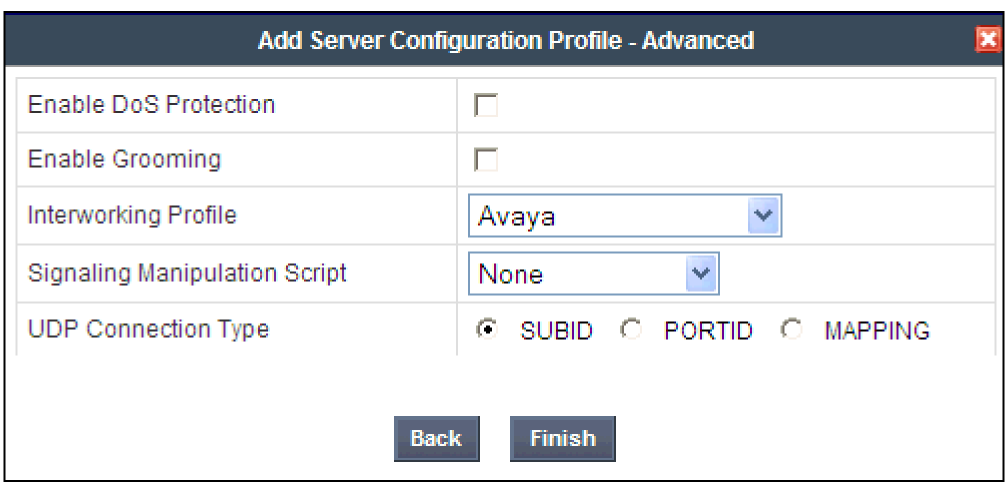
To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add Profile** and enter the profile name: **Service Provider.**

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

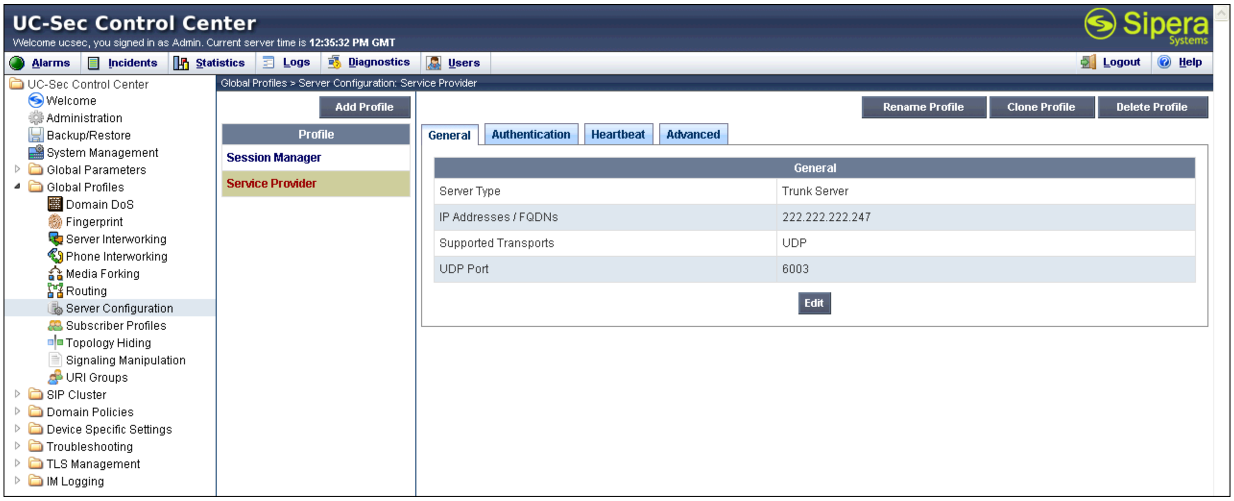
- Select **Server Type: Trunk Server**
- **IP Address: 222.222.222.247** (service provider's SIP Proxy IP address)
- **Supported Transports**: Check **UDP**.
- **UDP Port: 6003**
- Click **Next**



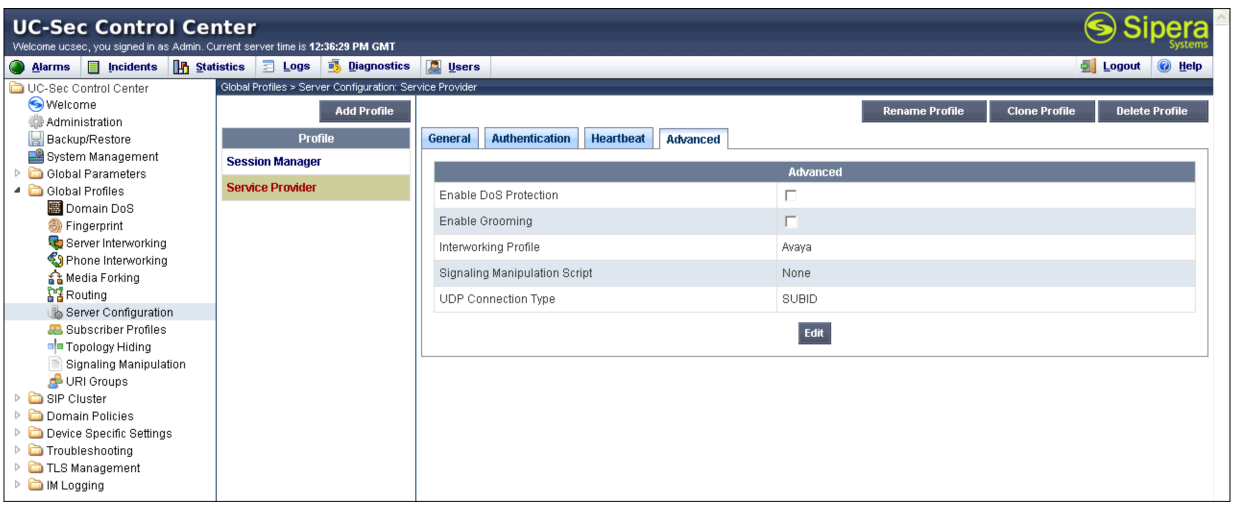
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave other fields with their default values for now, a **Signaling Manipulation** Script will be assigned later.
-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



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



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



7.3.4. 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.

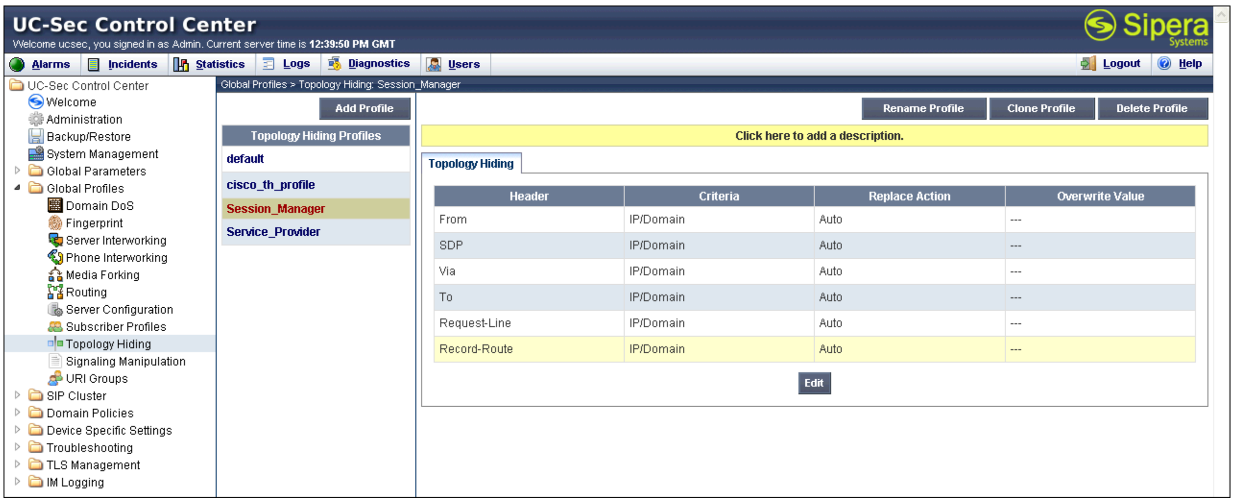
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

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:

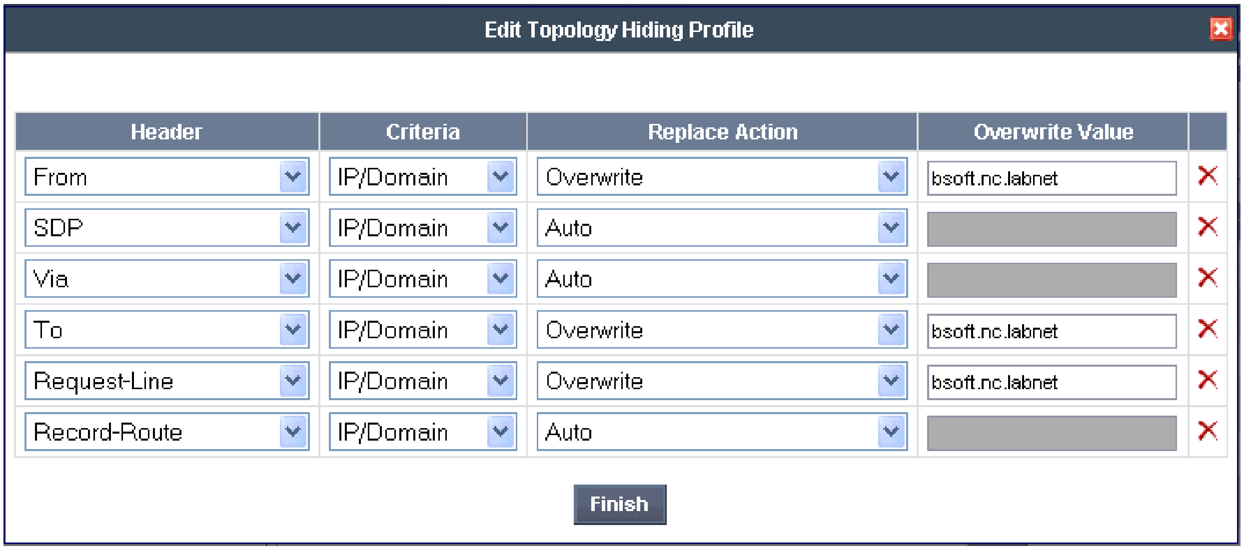
- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name**: **Session_Manager**.
- Leave all **Replace Action** as **Auto.**
- Click **Finish**.

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

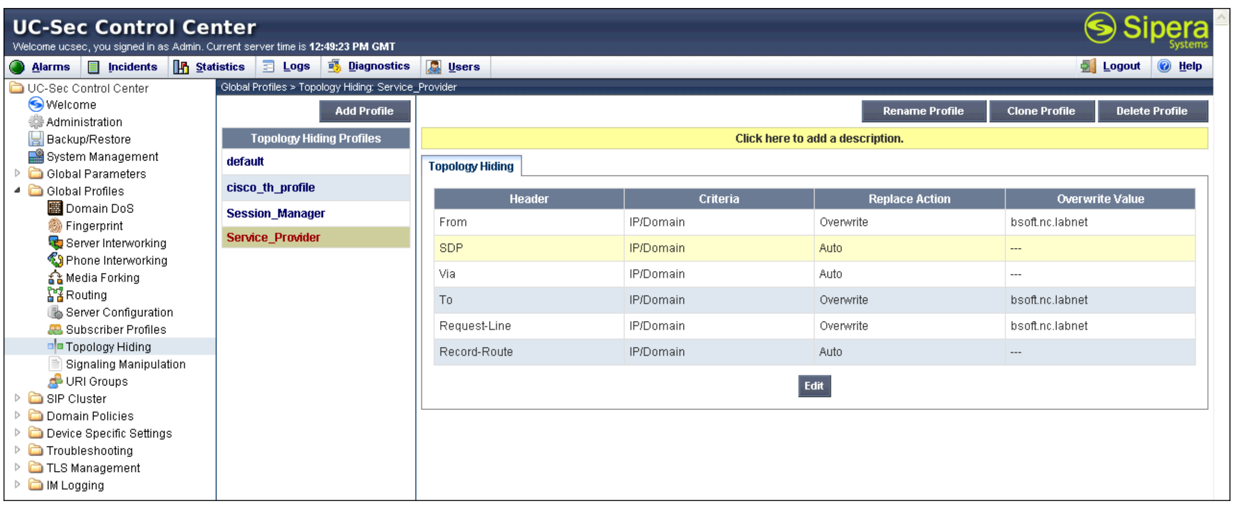


To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name**: **Service_Provider.**
- For the **From** header, chose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider under **Overwrite Value**.
- For the **To** header, chose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider under **Overwrite Value**.
- For the **Request-Line** header, chose **Overwrite** from the pull-down menu under **Replace Action,** enter the domain name for the Service Provider under **Overwrite Value**.
- Click **Finish**.



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



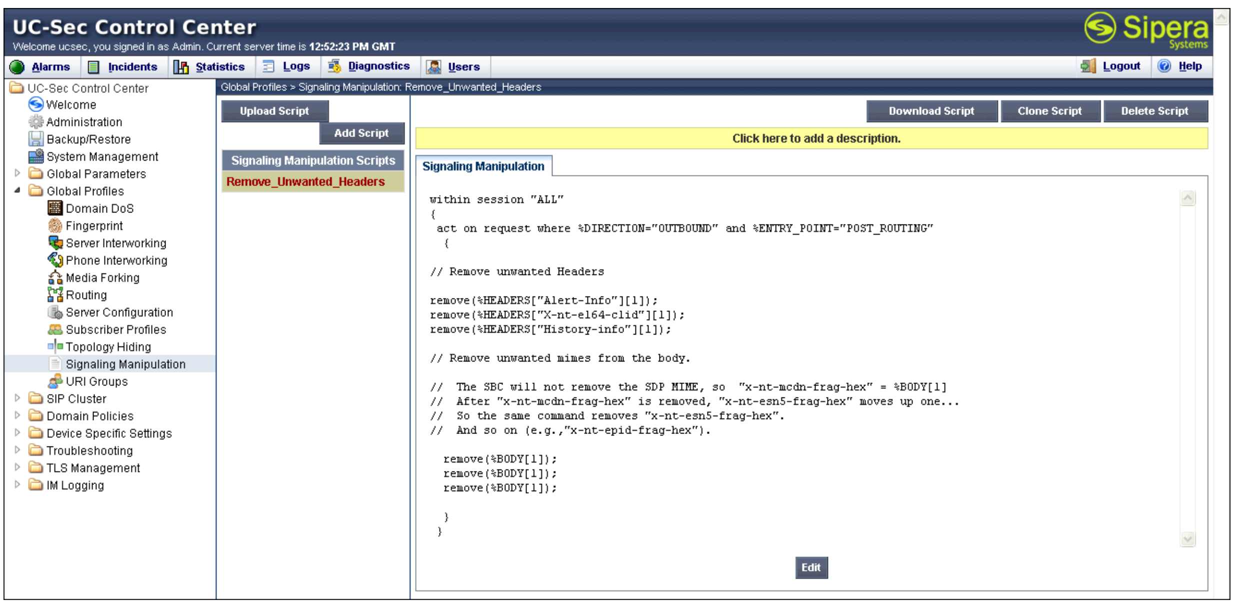
7.3.5. Signaling Manipulation

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 above.

For more information on the structure of the SigMa Scripting Language and details on its use, see **[13]**.

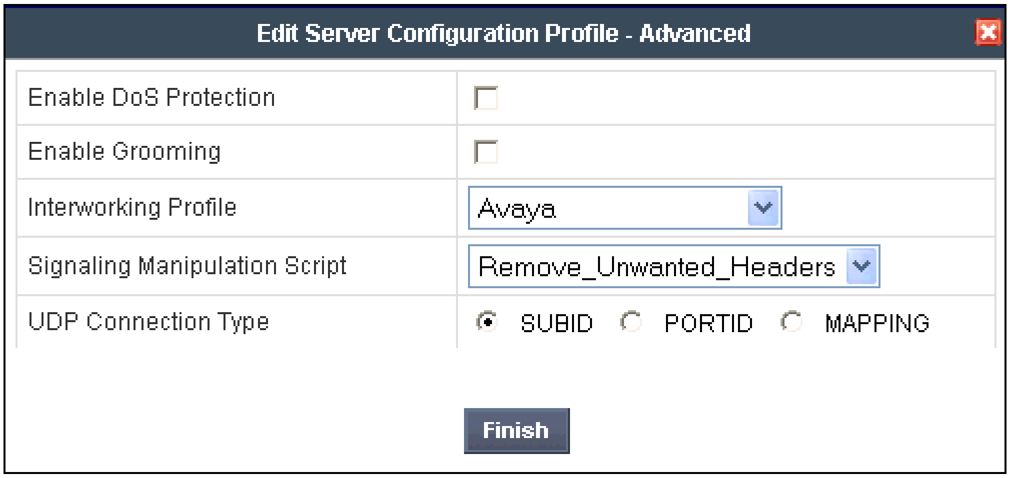
From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click on **Add Script** to open the SigMa Editor screen. On the **Title**, enter **Remove_Unwanted_Headers**. Enter the script as shown on the screen below:

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

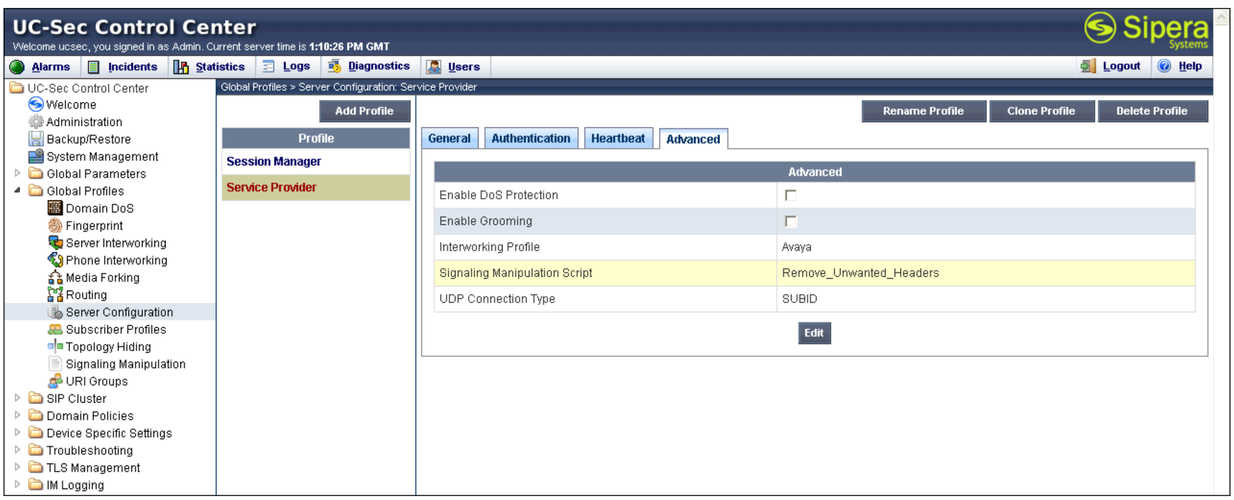


After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 7.3.3.**

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.

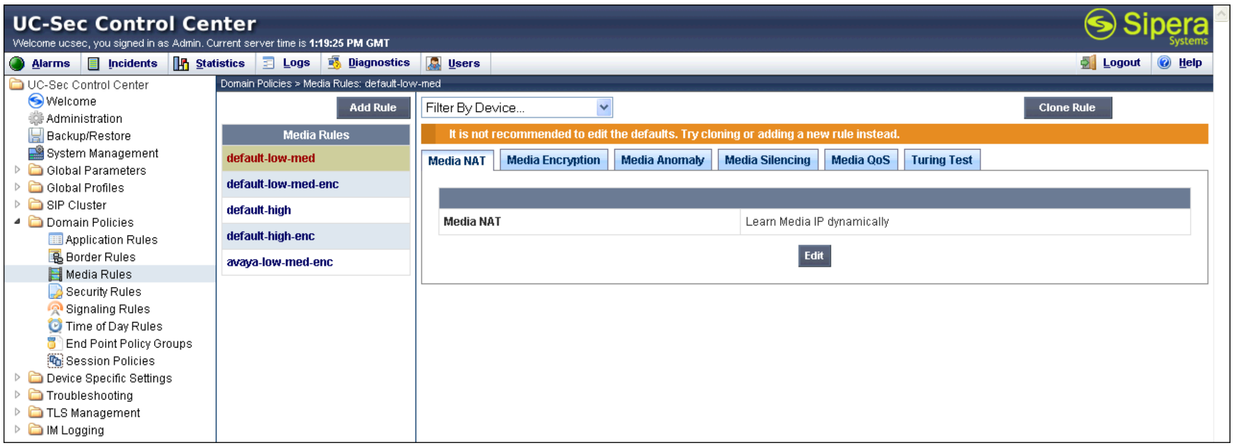


7.4. Domain Policies

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.

7.4.1. Media Rules

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



7.4.2. Signaling Rules

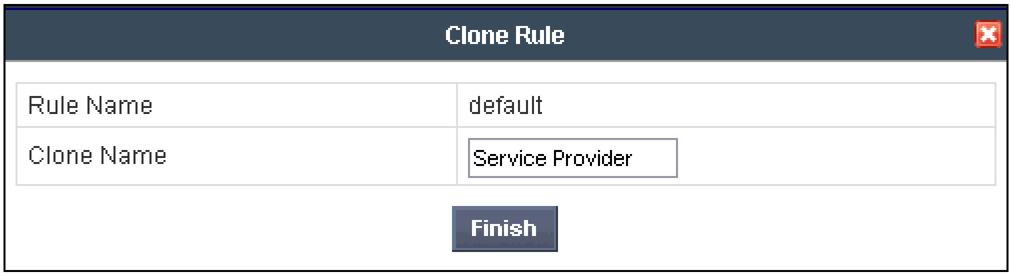
Signaling Rules define the actions to be taken (*Allow*, *Block*, *Block with Response*, etc.) for each type of SIP-specific signaling request and response message. They also allow the control of the Quality of Service of the signaling packets.

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

A Signaling Rule was created, to 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 from being propagated to the network, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on the **default** Signaling Rule.
- Click on **Clone Rule**.

Enter a name: **Service_Provider**. 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**

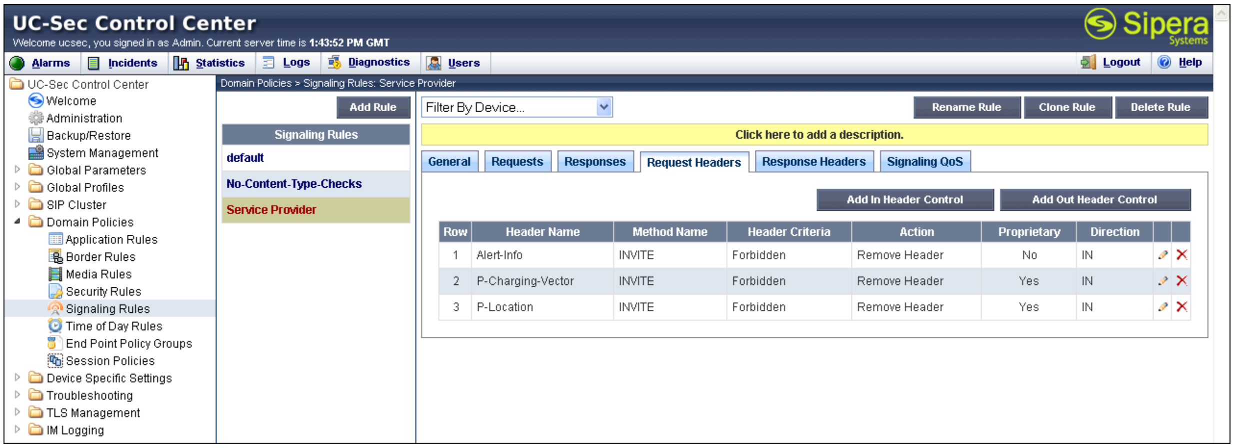
To add the P-Location header:

- 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 **Service Provider** 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:

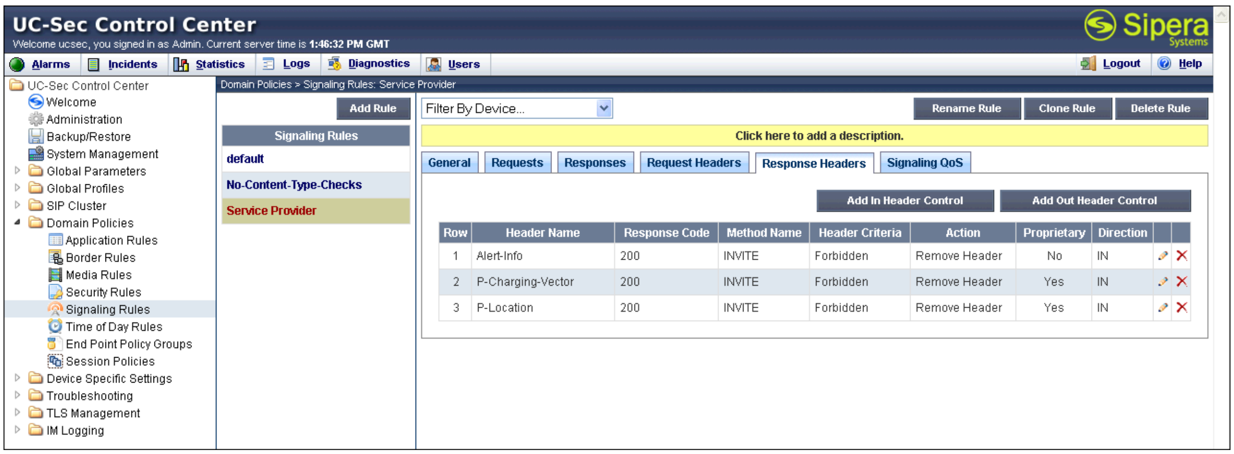
- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box
- **Header Name: P-Location**
- **Response Code: 200**
- **Method Name: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

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.

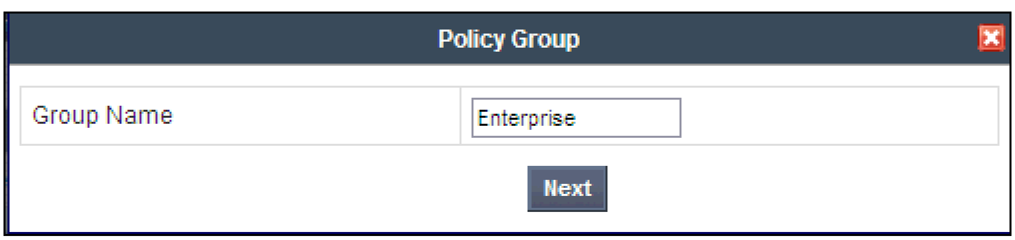


7.4.3. End Point Policy Groups

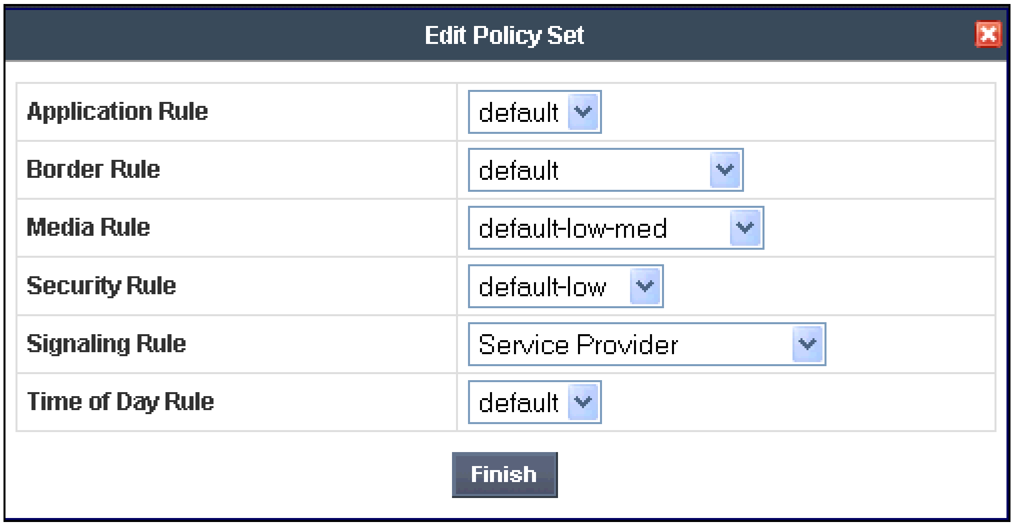
End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE.

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

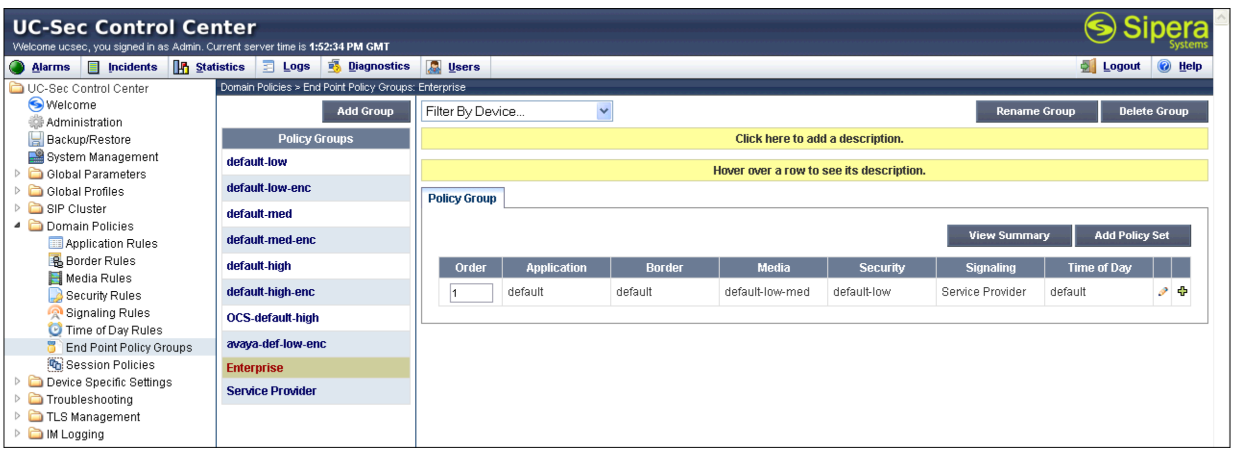
- **Group Name: Enterprise**.



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

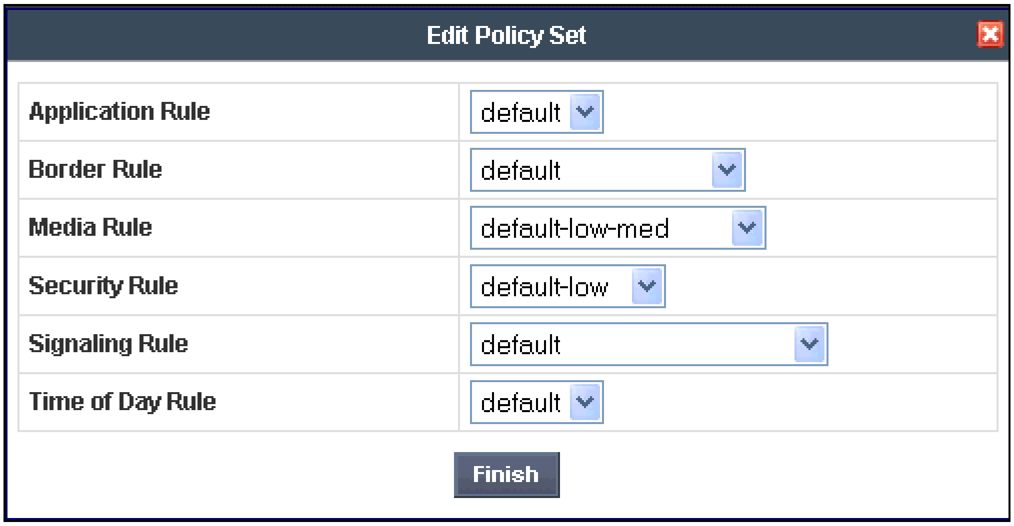


The following screen capture shows the newly added **Enterprise** End Point Policy Group.

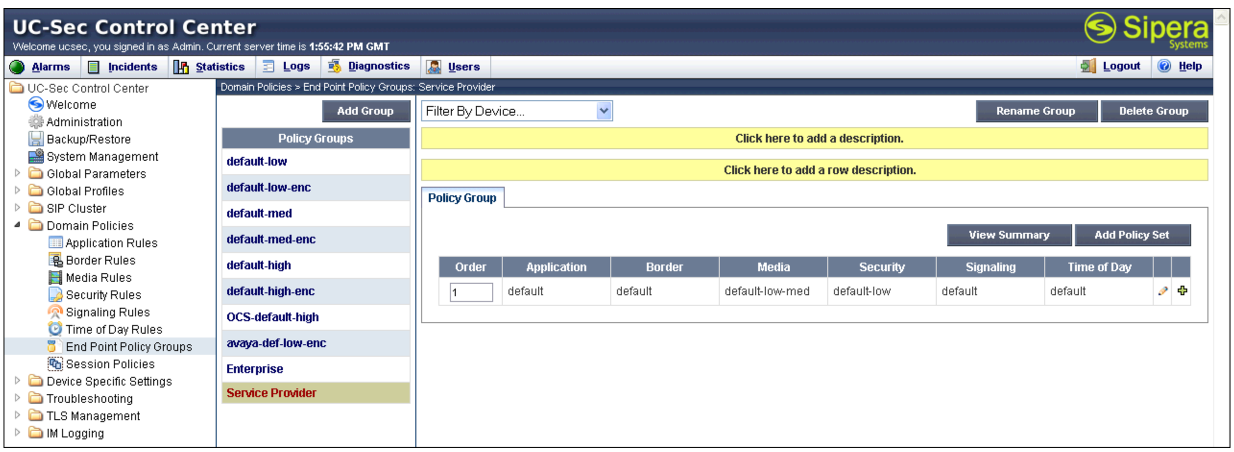


Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add Group**.

- **Group Name: Service Provider**.
- **Application Rule: default**
- **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.

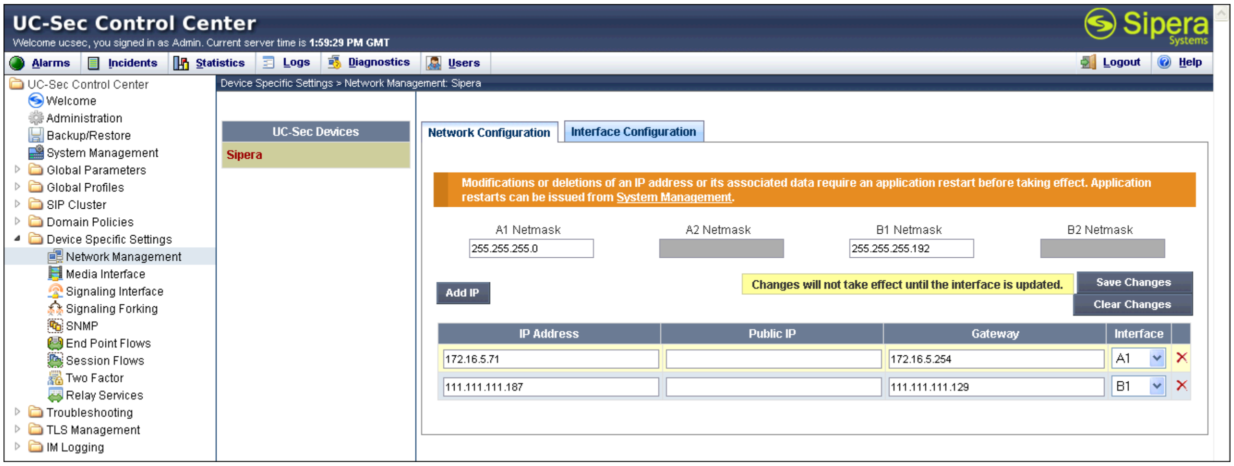


7.5. Device Specific Settings

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.

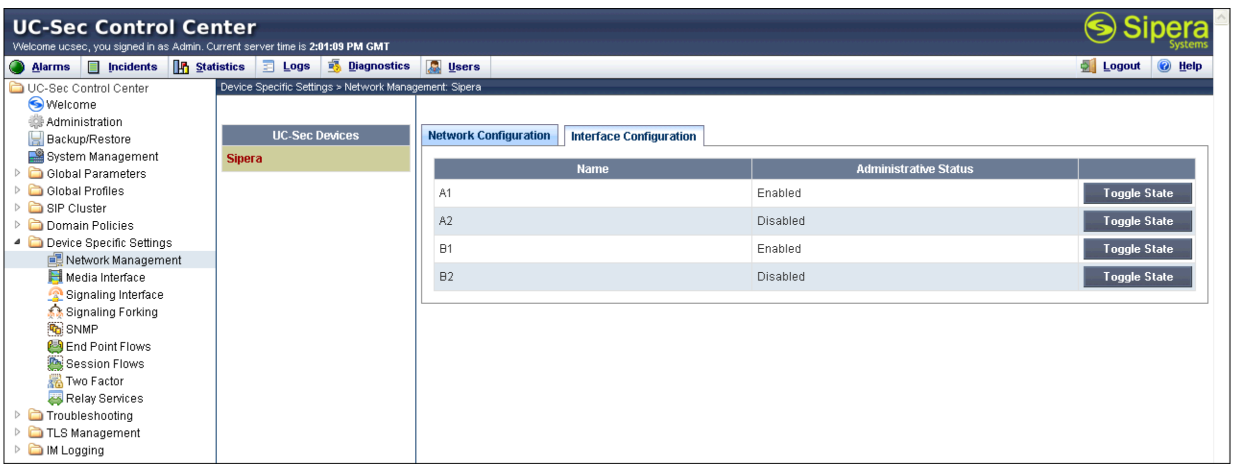
7.5.1. Network Management

The network information should have been previously completed in **Section 7.2**. To verify the network configuration, from the **Device Specific Menu** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.



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

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



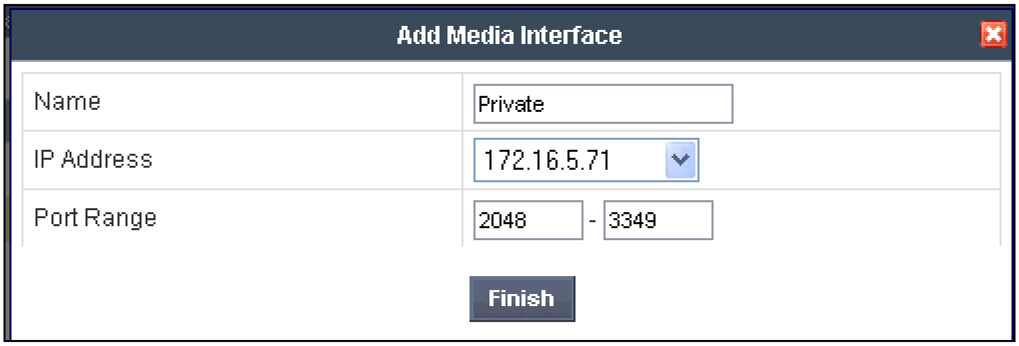
7.5.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private interface of the Avaya SBCE ports range 2048 to 3349 was used. On the Public interface port range 40150 to 40199 was used, matching the port range specified by the Service Provider.

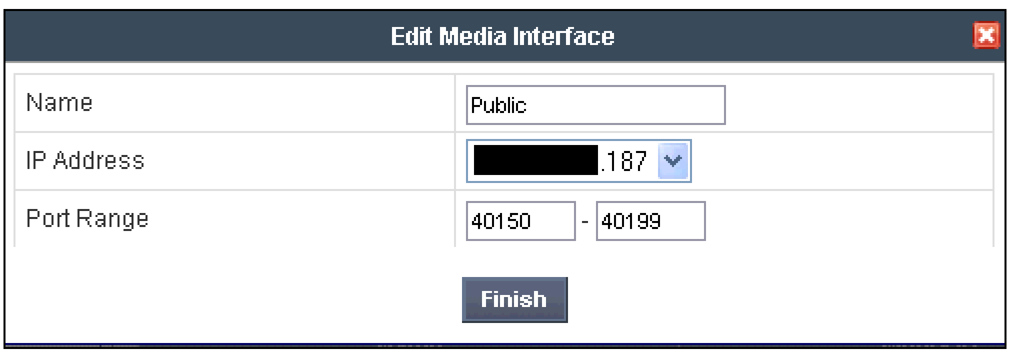
From the **Device Specific Settings** menu on the left-hand side, select **Media Interface.**

- Select **Add Media Interface**
- **Name: Private**

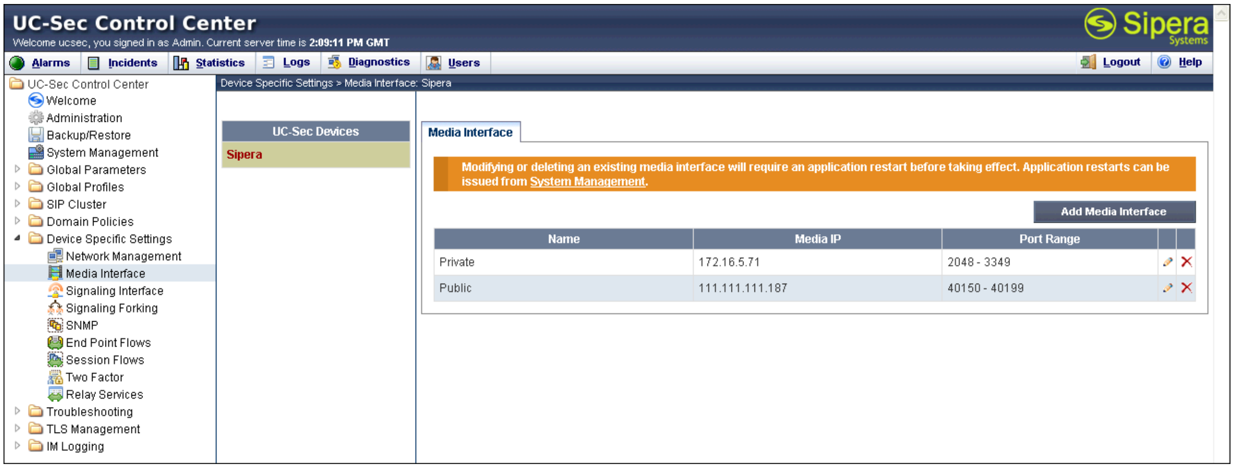
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager)
- **Port Range: 2048-3349**
- Click **Finish**



- Select **Add Media Interface**
- **Name: Public**
- Select **IP Address: 111.111.111.187** (Outside IP Address of the Avaya SBCE, toward Service Provider)
- **Port Range: 40150-40199**
- Click **Finish.**
-



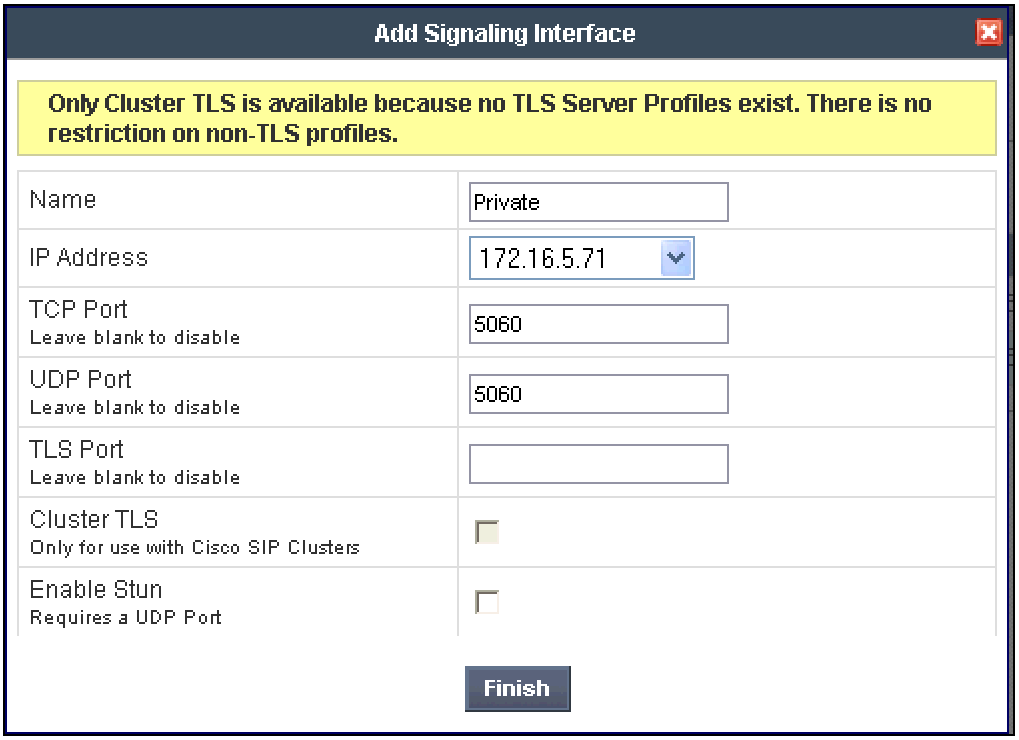
The following screen capture shows the added **Media Interfaces**.



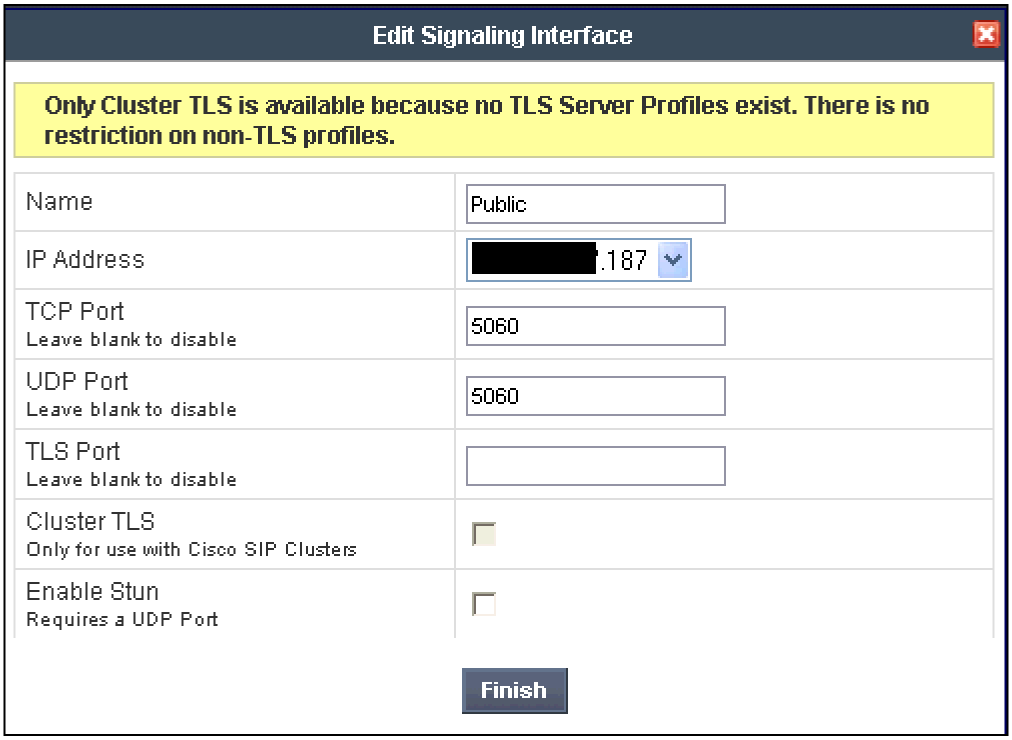
7.5.3. Signaling Interface

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

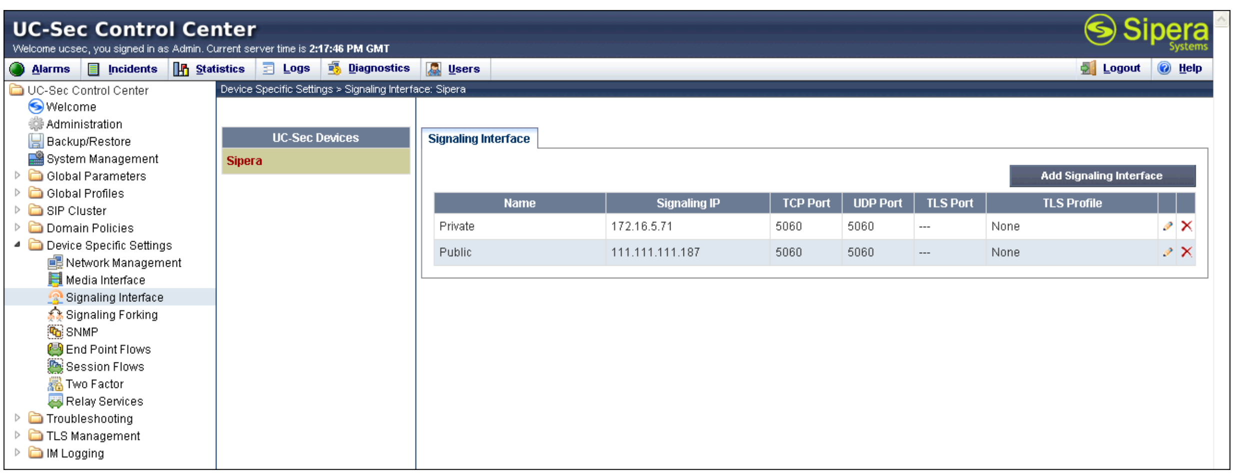
- Select **Add Signaling Interface**:
- **Name: Private**
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**



- Select **Add Signaling Interface**:
- **Name: Public**
- Select **IP Address: 111.111.111.187** (Outside IP Address of the Avaya SBCE, toward the Service Provider)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**



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



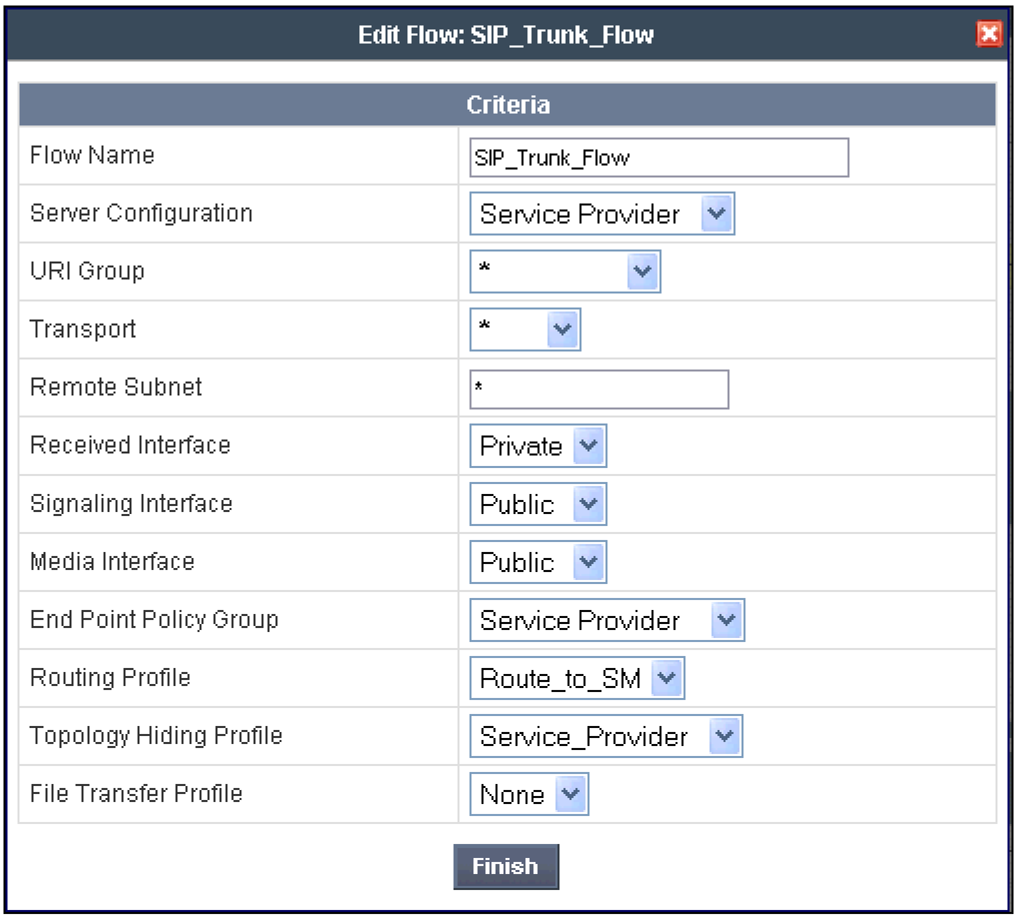
7.5.4. End Point Flows

The **End-Point Flows** allows you to 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**, tab **Server Flows**. Click **Add Flow**.

- **Name: SIP_Trunk_Flow**
- **Server Configuration**: **Service Provider**

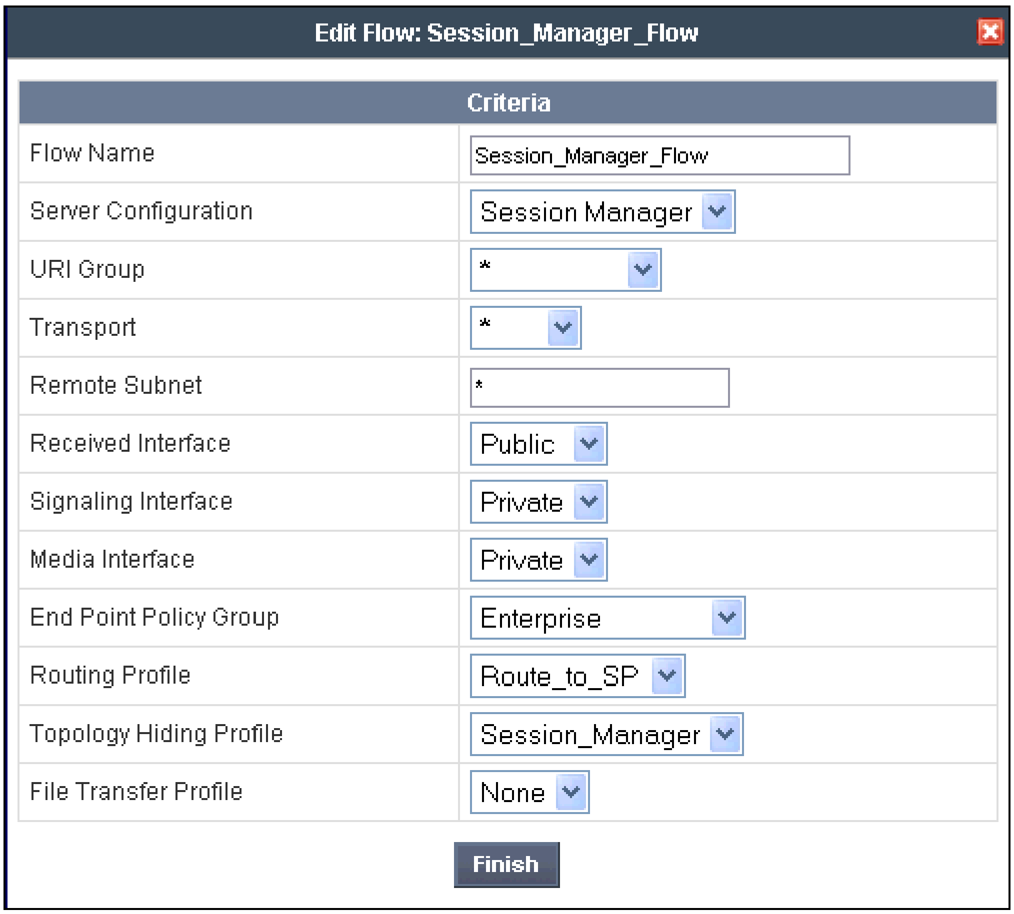
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private**
- **Signaling Interface: Public**
- **Media Interface**: **Public**
- **End Point Policy Group: Service Provider**
- **Routing Profile: Route_to_SM** (Note that this is the reverse route of the flow).
-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



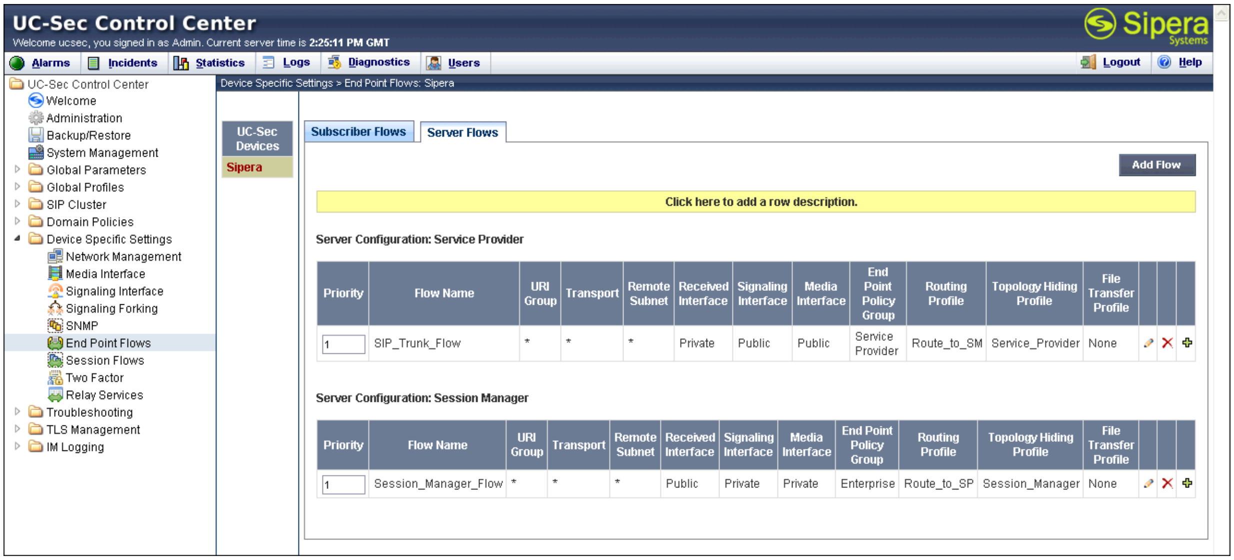
To create the call flow toward the Session Manager, click **Add Flow**.

- **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. CenturyLink BroadWorks SIP Trunk Service Configuration

To use CenturyLink BroadWorks SIP Trunk service, a customer must request the service from CenturyLink using their sales processes. The process can be started by contacting CenturyLink via the corporate web site at http://www.centurylink.com/Pages/Support/ and requesting information via the online sales links or telephone numbers.

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

The configuration between CenturyLink and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to CenturyLink's network.

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 name and number to ensure the correct info was sent/received. Perform hold/retrieve on calls. Verify the call remains stable for several minutes and disconnect properly.

9.2. Verify Call Establishment on the CS1000 Call Server

Active Call Trace (LD 80)

Following is an example of one of the commands available on the CS1000 to trace the DN when the call is in progress or idle. The call scenario involved the CS1000 extension 8005 calling PSTN phone number 7863311234.

- Log in to the Call Server CLI (please refer to **Section 5.1.2** for more detail).
- Log in to the Overlay command prompt, issue the command **LD 80** and then **trac 0 8005**.
- After the call is released, issue command **trac 0 8005** again to see if the DN is released back to idle state.

Below is the actual output of the Call Server Command Line mode when extension 8005 is in an active call:

```
>ld 80
TRA000
.trac 0 8005

ACTIVE  VTN 008 0 00 03

ORIG   VTN 008 0 00 03  KEY 0  SCR MARP  CUST 0  DN 8005  TYPE 2050PC
  SIGNALLING ENCRYPTION: INSEC
  FAR-END SIP SIGNALLING IP: 172.16.21.61
  FAR-END MEDIA ENDPOINT IP: 1.1.1.2  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: 2050
  FAR-END VendorID: AVAYA-SM-6.1.5.0.615006
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 91786331[redacted]
MAIN_PM  ESTD
TALKSLOT  ORIG  27   TERM  30    JUNCTOR  ORIG0   TERM0
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 190


----  ISDN ISL CALL (TERM) ----
CALL REF # =  395
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  318360[redacted]  NUM_PLAN:E164    TON:NATIONAL  ESN:NPA
CALLED NO  =  1786331[redacted]  NUM_PLAN:E164    TON:NATIONAL  ESN:NPA
```

Following is an example after the call on 8005 has been released.

```
trac 0 8005

IDLE VTN 008 0 00 03   MARP
```

Following is an example after the call has been released, which shows that there are no trunks busy.

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

9.3. Protocol Traces

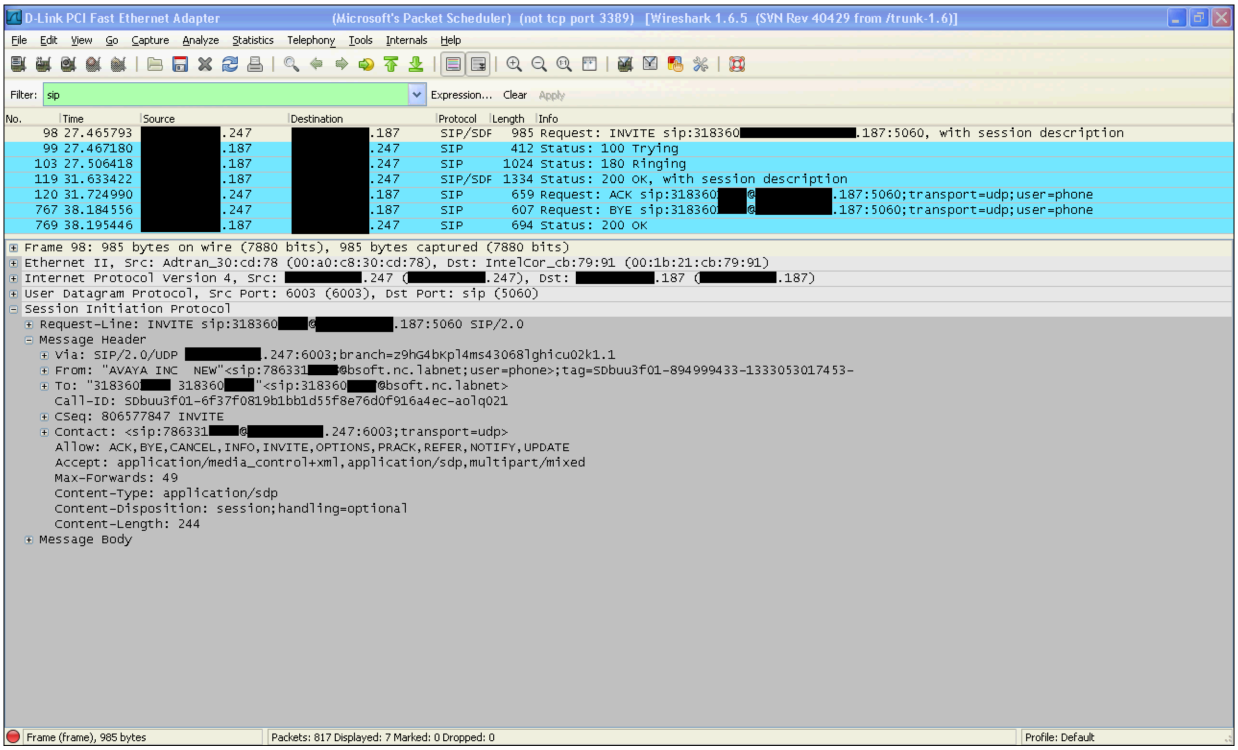
Wireshark was used to verify the following information for each call:

- 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 and number and reason code.
- P-Asserted-Identity: verify the display name and display number.
- Privacy: verify the "user, id" masking.

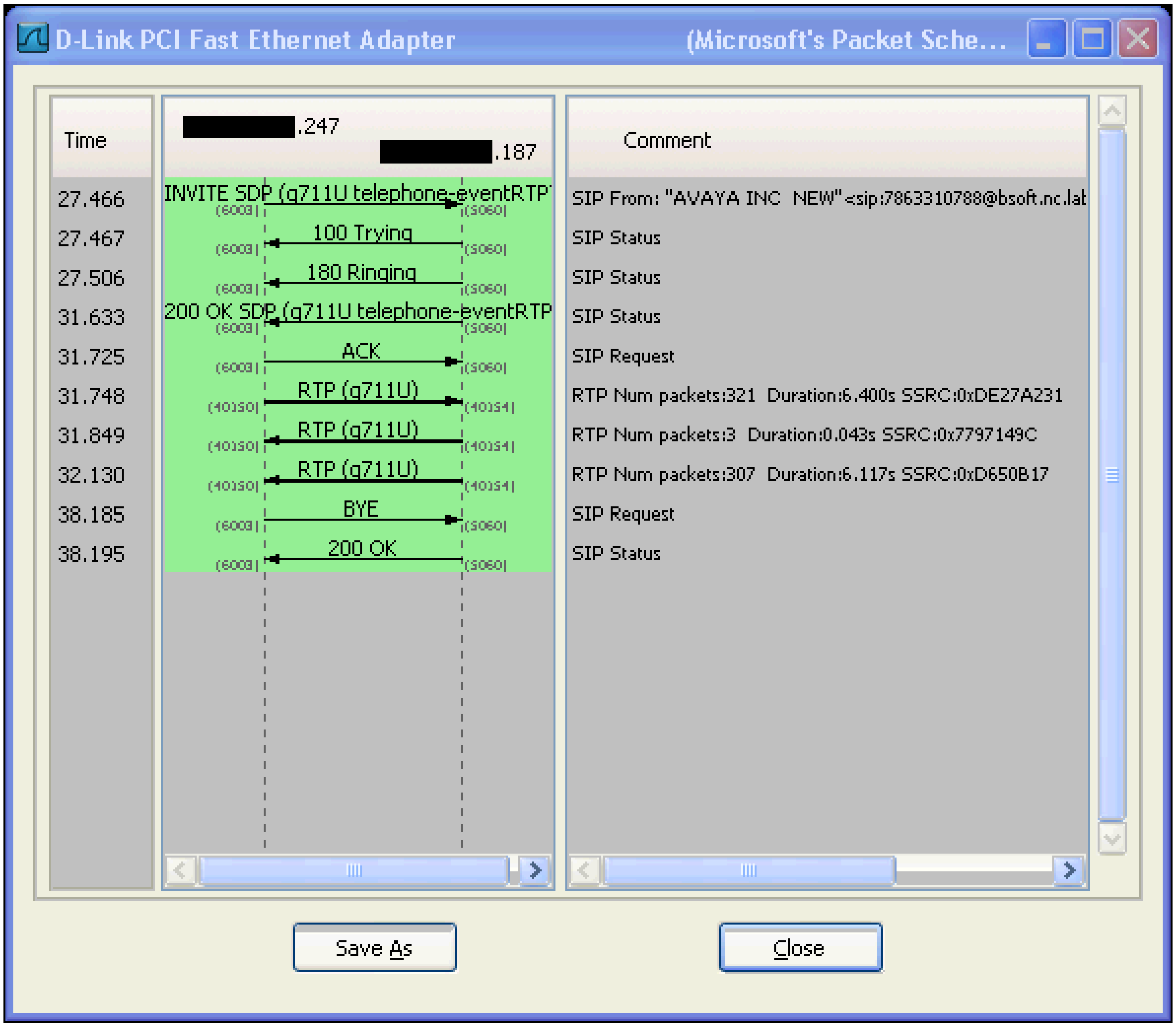
- Connection Information: verify IP addresses.
- Time Description: verify session timeout of far end endpoint
- Media Description: verify audio port, codec, and DTMF event description
- Media Attribute: verify specific audio port, codec, ptime, and send/receive ability
- DTMF event and fax attributes.

Following is an example of a typical capture for a call made from the PSTN (7863311234) to a CS1000 extension 8005 (DID 3183601234).

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



Following is the SIP messaging flow of the same call listed above seen from Telephony → VoIP Calls of Wireshark.



10. Conclusion

These Application Notes describe the procedures necessary to configure SIP Trunk connectivity between Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1, Avaya Session Border Controller for Enterprise Release 4.0.5Q02 and CenturyLink BroadWorks SIP Trunk service as shown in **Figure 1**.

CenturyLink BroadWorks SIP Trunk service passed compliance testing.

11. References

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

[1] Network Routing Service Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.
[2] IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010
[3] Communication Server 1000E Overview, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011
[4] Communication Server 1000 Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011
[5] Communication Server 1000 Dialing Plans Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010
[6] Product Compatibility Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011
[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 Manager, 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] Sipera Systems E-SBC Release Notes. Release 4.0.5.Q02. November 2011.
[15] RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/.
[16] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/

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.