Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E 7.5 and Avaya Session Border Controller for Enterprise 4.0.5 with CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6 – Issue 1.1

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6 and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E, Avaya Session Border Controller for Enterprise and various Avaya endpoints.

CenturyLink is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Solutions and Interoperability Test Lab, utilizing CenturyLink SIP Trunk services.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration of Avaya Communication Server 1000E release 7.5 and Avaya Session Border Controller for Enterprise release 4.0.5 integration with CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6. CenturyLink can offer SIP trunk service using several different platform technologies in the CenturyLink network. These Application Notes correspond to the SIP trunk service offered using a Sonus platform in the network.

In the sample configuration, the Avaya Session Border Controller for Enterprise (Avaya SBCE) is used as an edge device between Avaya Customer Premise Equipment (CPE) and CenturyLink SIP Trunk. The Avaya SBCE performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the CenturyLink SIP Trunk access method.

CenturyLink SIP Trunk is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

CenturyLink SIP Trunk will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE). CenturyLink SIP Trunk will also offer remote DID capability for a customer wishing to offer local numbers to their customers that can be aggregated in SIP format back to customer.

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. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya Communication Server 1000E (CS1000E) and Avaya SBCE to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to CenturyLink SIP Trunk service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included UNIStim, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included UNIStim, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client).
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, emergency calls (911) and local directory assistance (411).
- Inbound toll-free calls.
- Codecs G.729A, G.729B and G.711MU.
- DTMF transmission using RFC 2833.
- T.38 Fax.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and Mobile X (extension to cellular).

Items not supported or not tested included the following:

- SIP REFER method is not supported by Avaya CS1000E.
- Mid-Call features using Mobile X.

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunk was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/CenturyLink SIP Trunk solution. It is listed here simply as an observation.
- **History-Info and Diversion Headers**: CenturyLink SIP Trunk does not support SIP History-Info Headers. Instead, CenturyLink SIP Trunk requires that SIP Diversion Header be sent for redirected calls. The CS1000E includes History-Info header in messaging sent to Avaya SBCE. Avaya SBCE can add a Diversion Header required by CenturyLink. This is performed by creating a Sigma script in the Avaya SBCE configuration. See **Section 6.1.4** and **Appendix A**.

CenturyLink SIP Trunk (Legacy Qwest) passed compliance testing.

2.3. Support

2.3.1. Avaya

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

2.3.2. CenturyLink

For technical support on the CenturyLink SIP Trunk service, contact CenturyLink using the Customer Care links at www.centurylink.com

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to CenturyLink SIP Trunk. This is the configuration used for compliance testing.

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

- Communication Server 1000E on CP+DC server as co-resident configuration
- Communication Server 1000E Media Gateway
- Network Routing Server
- Call Pilot Voicemail
- Avaya Session Border Controller for Enterprise
- Avaya 1165E IP telephones (UNIStim)
- Avaya 1140E IP telephone (SIP)
- Avaya 2050 IP Softphone (UNIStim)
- Avaya one-X® Communicator (SIP)
- Avaya digital and analog telephones

The configuration is comprised of the Avaya CPE location connected via an Internet connection to the CenturyLink SIP Trunks East and West servers. The Avaya CPE location simulates a customer site.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external 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.

For security reasons, any actual public IP addresses used in the configuration have been either blocked out or replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

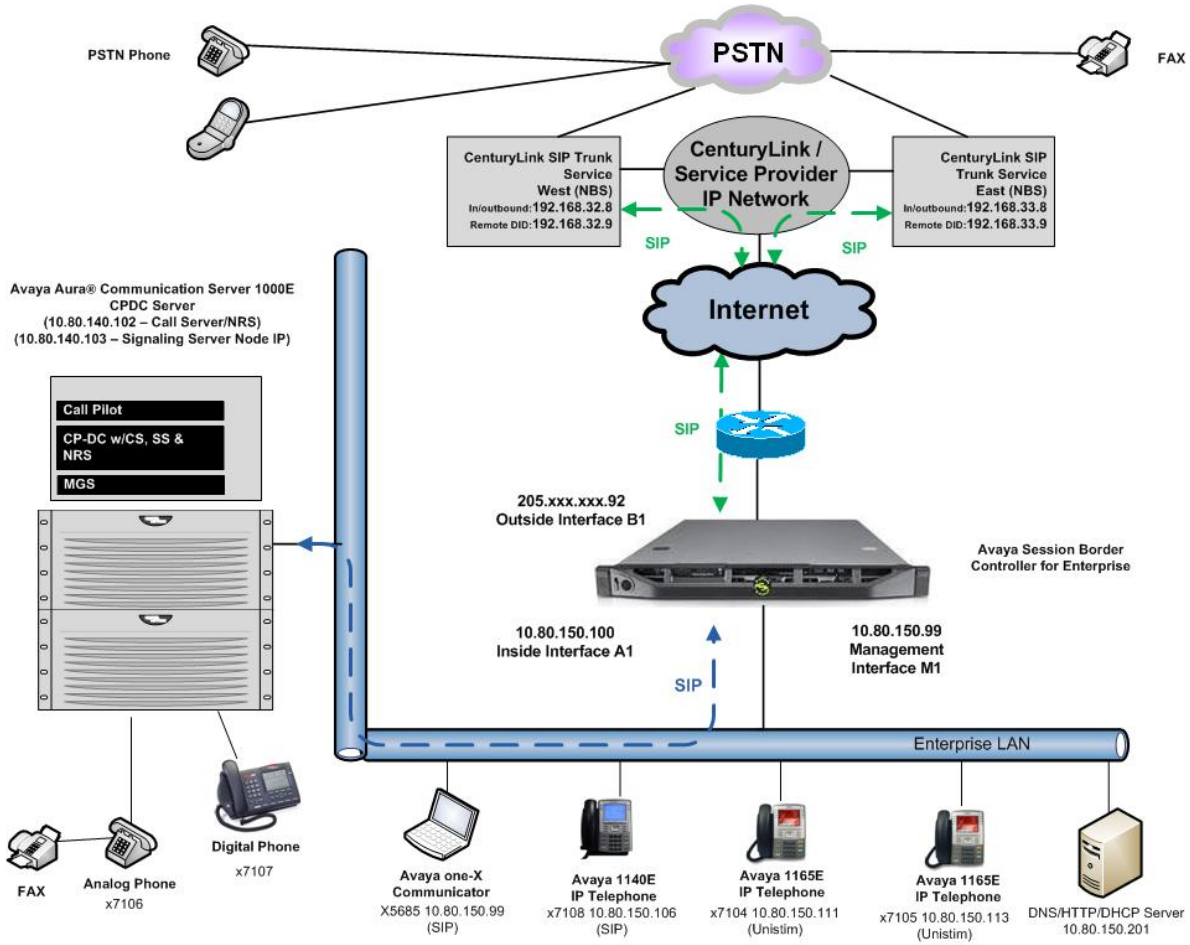


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Communication Server 1000E running on CP+DC server as co-resident configuration	• Call Server: 7.50 .17 GA (CoRes) Service Pack: 7.50.17_20120110 • SSG Server: 7.50.17 GA • SLG Server: 7.50.17 GA • NRS/SPS Server: 7.50.17 GA
Communication Server 1000E Media Gateway	CSP Version: MGCC CD02 MSP Version: MGCM AB01 APP Version: MGCA BA15 FPGA Version: MGCF AA19 BOOT Version: MGCB BA15 DSP1 Version: DSP4 AB01 BCSP Version: MGCC CD01
Avaya Session Border Controller for Enterprise	4.0.5Q9
Avaya 1165E (UNIStim)	0626C8A
Avaya 1140E (SIP)	04.03.09.00
Avaya 2050 IP Softphone (UNIStim)	4.2.0062
Avaya one-X Communicator (SIP)	CS6.1.0.25
Avaya M3904 (Digital)	n/a
Avaya 6210 Analog Telephone	n/a
CenturyLink (Legacy Qwest) SIP Trunking Solution Components	
Component	Release
Sonus Network Border Switch (NBS)	07.03.05 R006

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing.

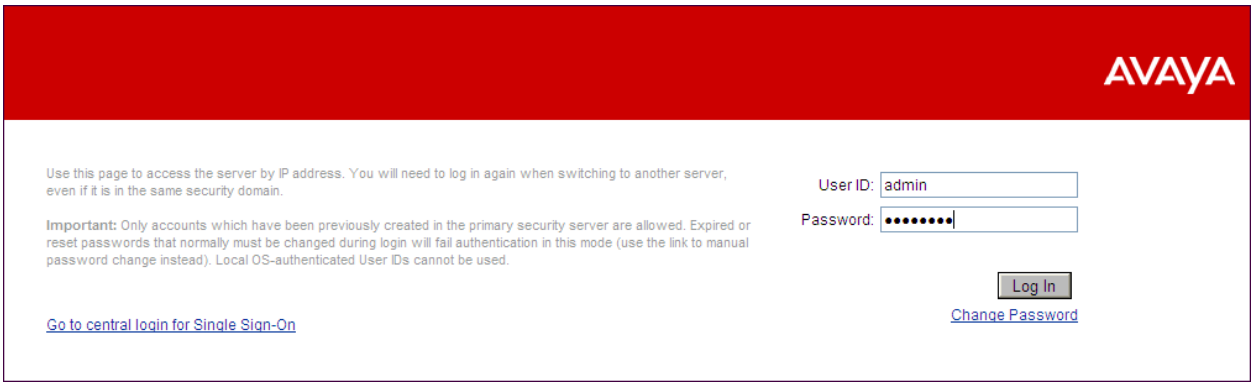
5. Configure Avaya Communication Server 1000E

This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to CenturyLink over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed as a co-resident system with the Network Routing Service (NRS), SIP Signaling Server, and Call Server applications all running on the same CP+DC server platform.

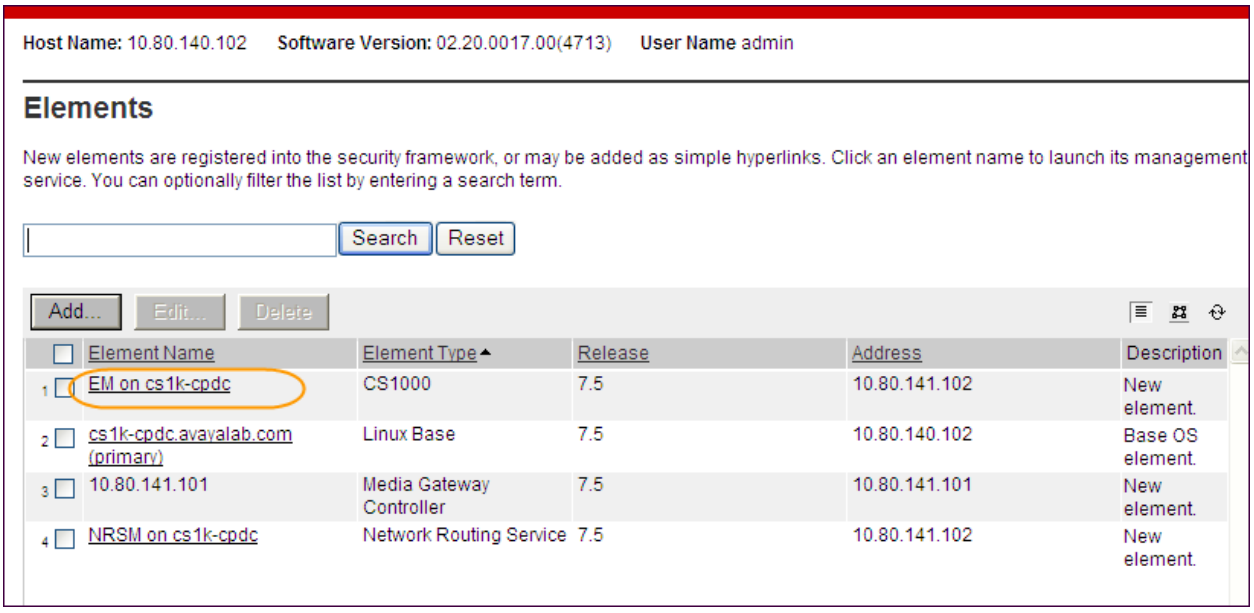
This section focuses on the SIP Trunking configuration. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the NRS, Call Server and SIP Signaling Server applications has been completed, and that the Avaya Communication Server 1000E is configured to support analog, digital, UNIStim, and SIP

telephones. For references on how to administer these functions of Avaya Communication Server 1000E, see **Section 10**.

Configuration will be shown using the web based Avaya Unified Communications Management GUI. The Avaya Unified Communications Management GUI may be launched directly via https://<ipaddress> where the relevant <ipaddress> in the sample configuration is 10.80.140.102. The following screen shows an abridged log in screen. Log in with appropriate credentials.



The Avaya Unified Communications Management Elements page will be used for configuration. Click on the Element Name corresponding to **CS1000** in the **Element Type** column. In the abridged screen below, the user would click on the Element Name **EM on cs1k-cpdc**.



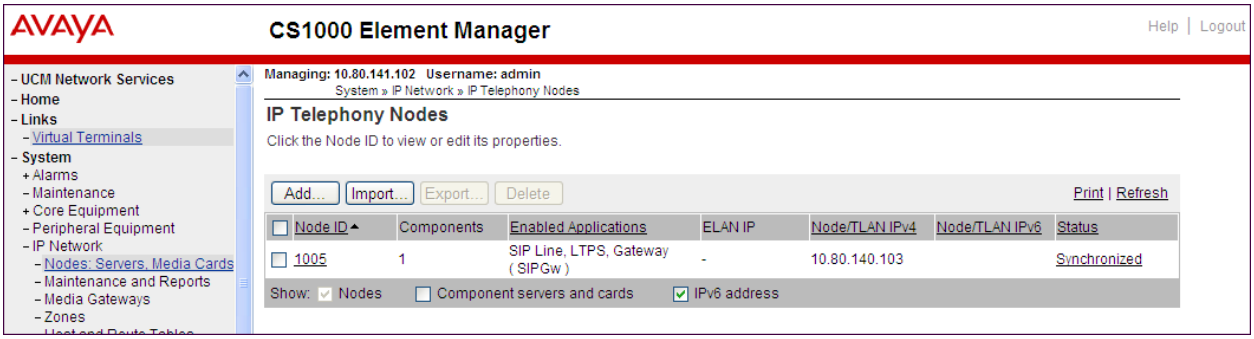
5.1. Administer an IP Telephony Node

This section describes how to configure an IP Telephony Node on the Communication Server 1000E.

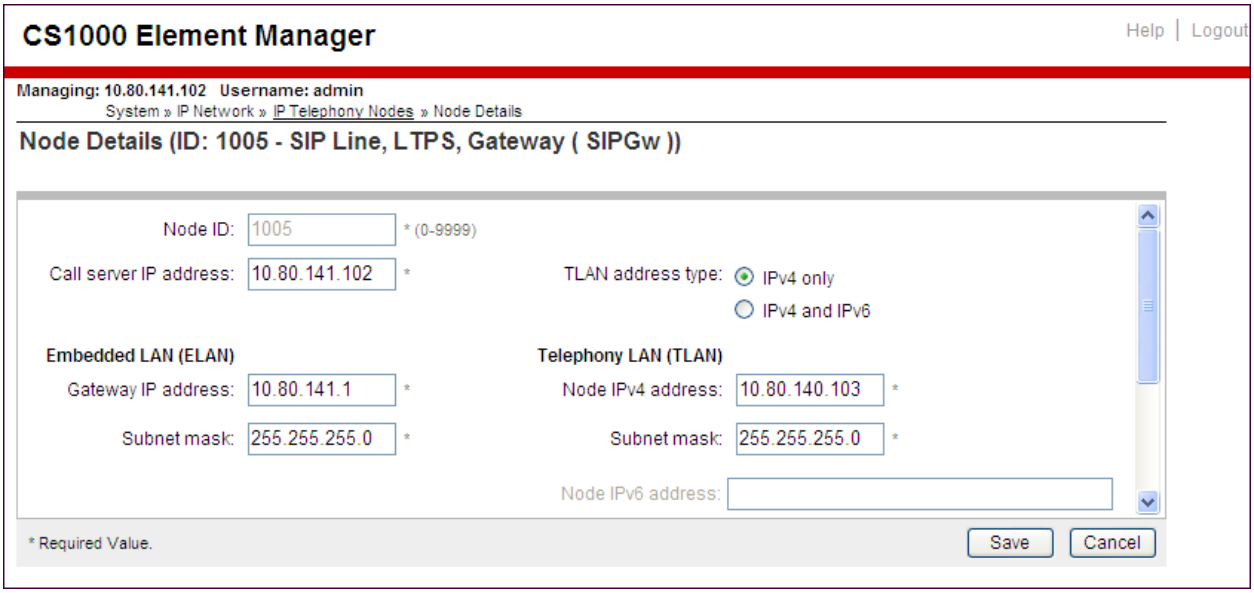
5.1.1. Obtain Node IP Address

Expand **System → IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

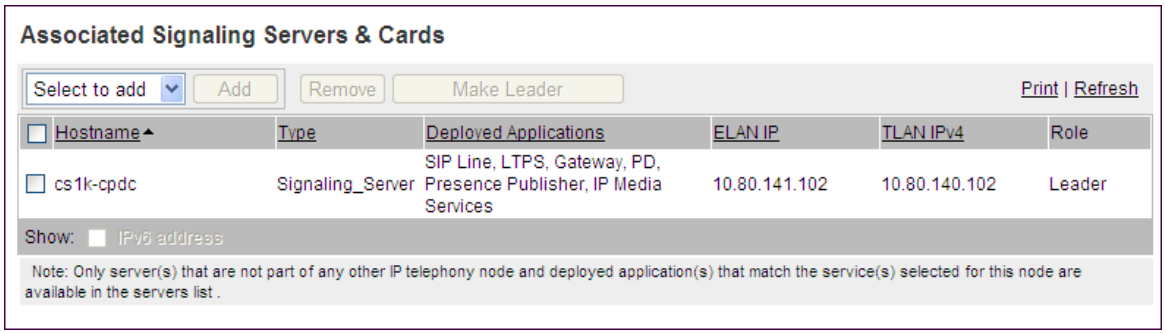
The **IP Telephony Nodes** page is displayed as shown below. Click **<Node id>** in the Node ID column to view details of the node. In the sample configuration, **Node ID 1005** was used.



The **Node Details** screen is displayed with additional details as shown below. Under the **Node Details** heading at the top of the screen, make a note of the **TLAN Node IPV4 address**. In the sample screen below, the **Node IPV4 address** is **10.80.140.103**. This IP address will register with the Network Routing Service to establish the SIP Gateway as described later in **Section 5.1.5**. This is also the IP address UNiStim phones and SIP phones will used to register to the CS1000E.

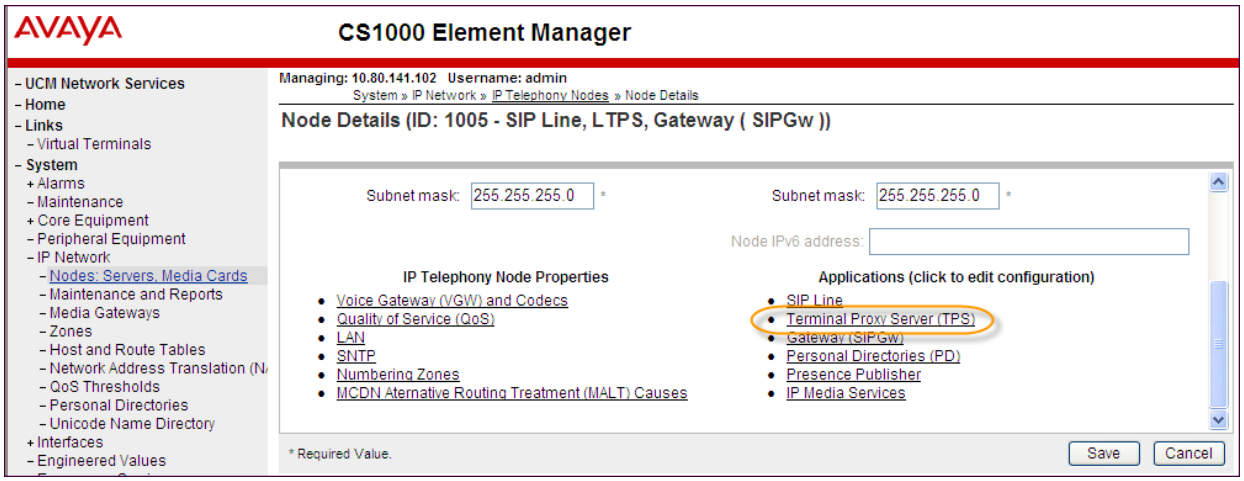


The following screen shows the **Associated Signaling Servers & Cards** heading at the bottom of the screen, simply to document the configuration.

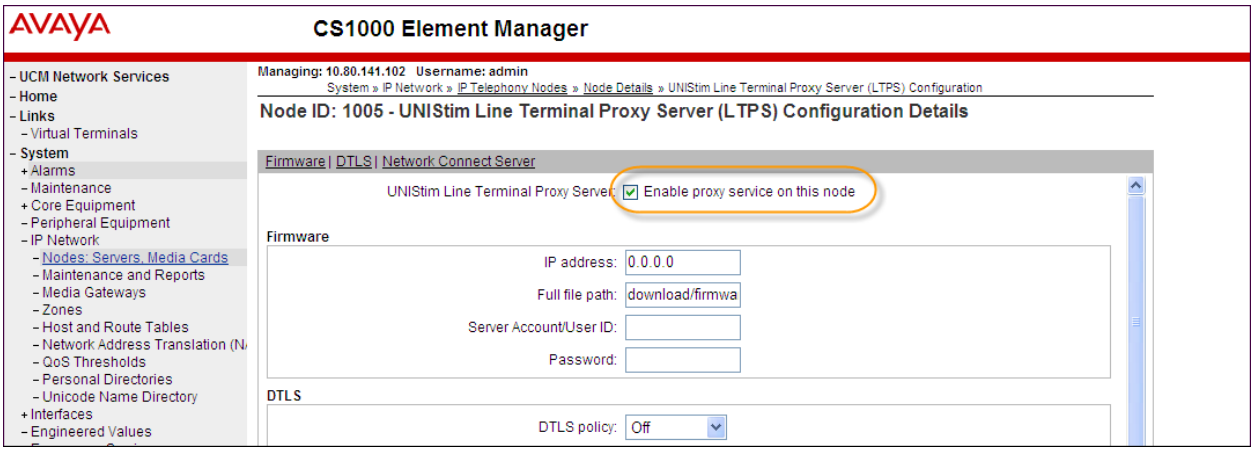


5.1.2. Terminal Proxy Server (TPS)

On the **Node Details** screen, scroll down in the top window and select the **Terminal Proxy Server (TPS)** link as show below.

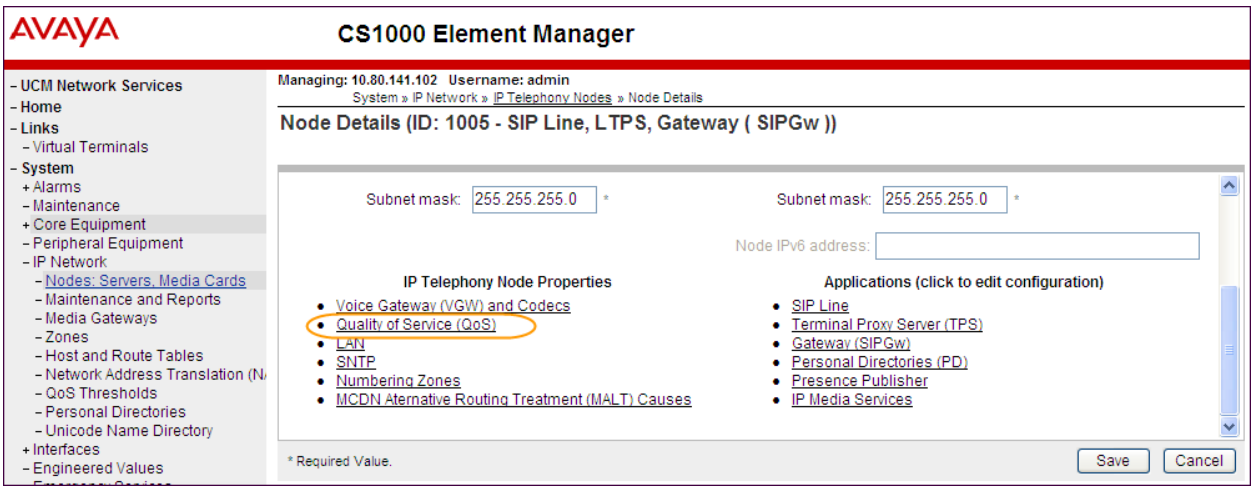


Check the **UNIStim Line Terminal Proxy Server** check box and then click the **Save** button (not shown).

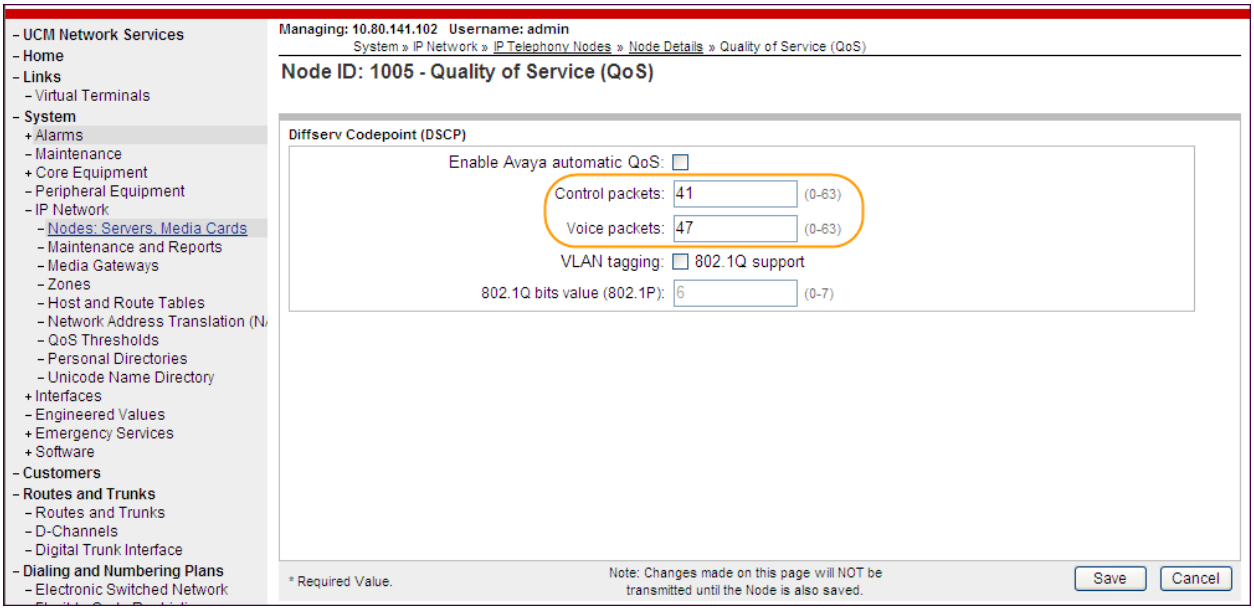


5.1.3. Quality of Service (QoS)

On the **Node Details** screen, scroll down in the top window and select the **Quality of Service (QoS)** link as shown below.

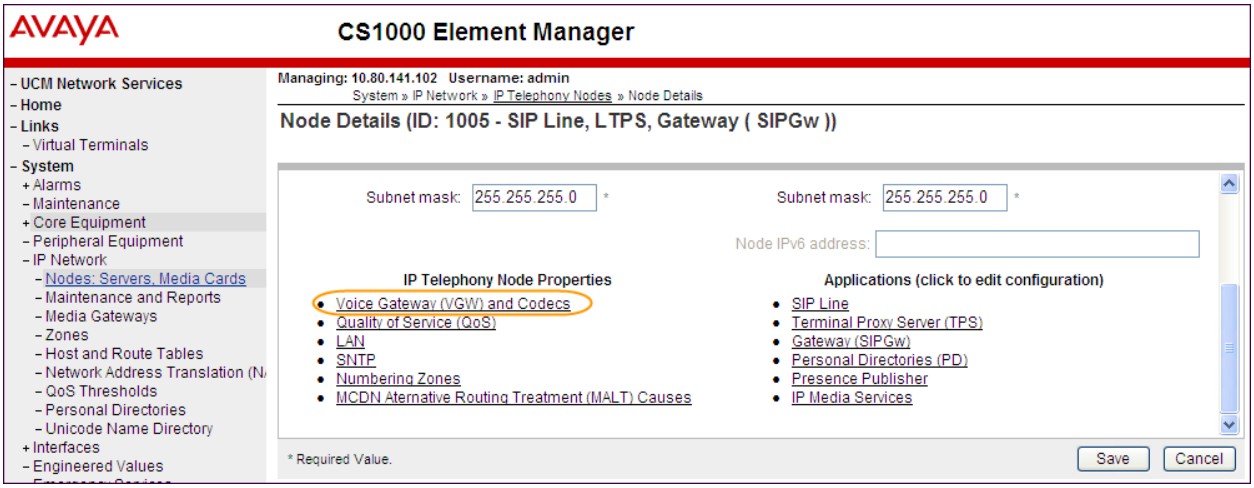


Set the **Control packets** and **Voice packets** values to the desired Diffserv settings required on the internal network. The default Diffserv values are shown below. Click on the **Save** button.

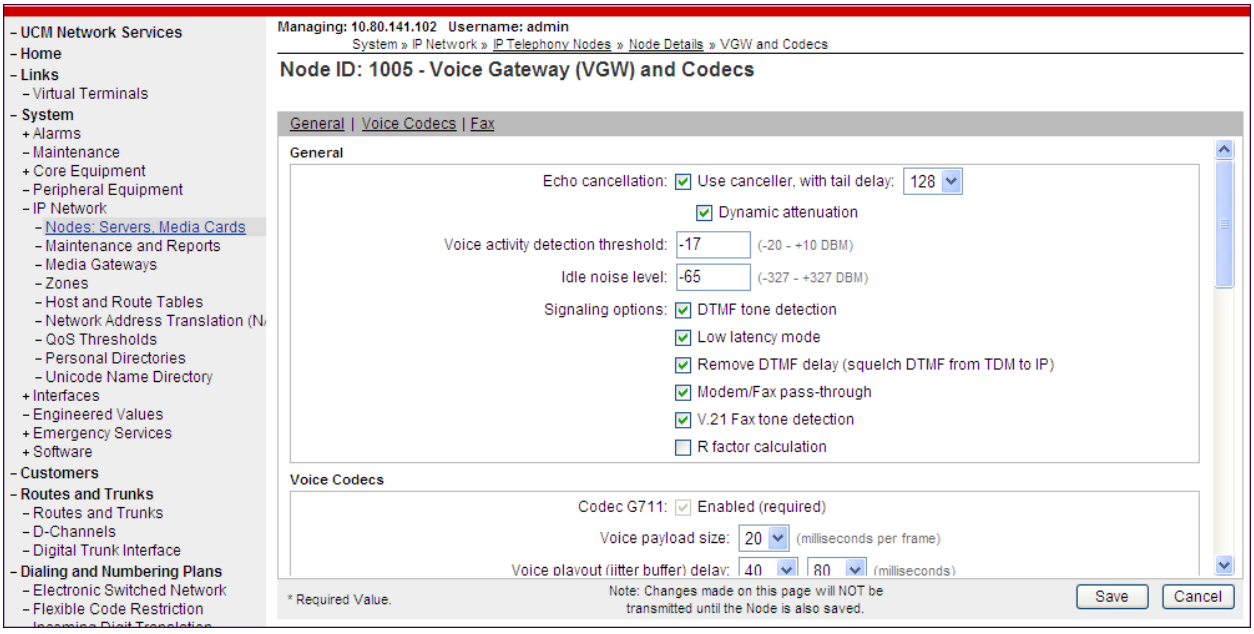


5.1.4. Voice Gateway and Codecs

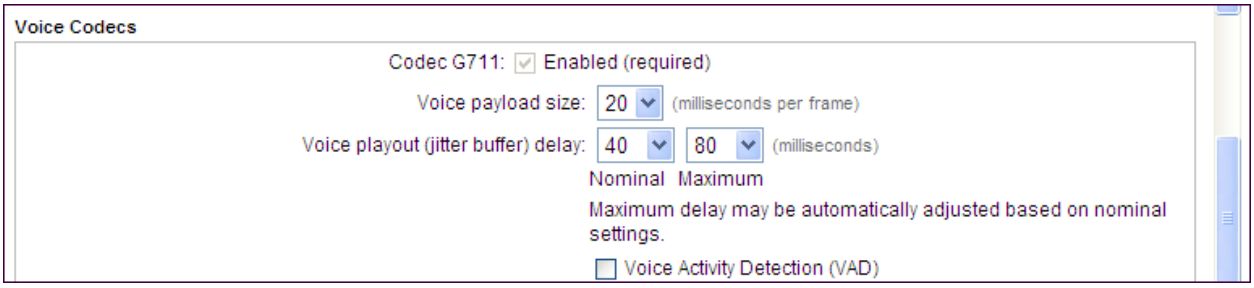
On the **Node Details** screen, scroll down in the top window and select the **Voice Gateway (VGW) and Codecs** link as shown below.



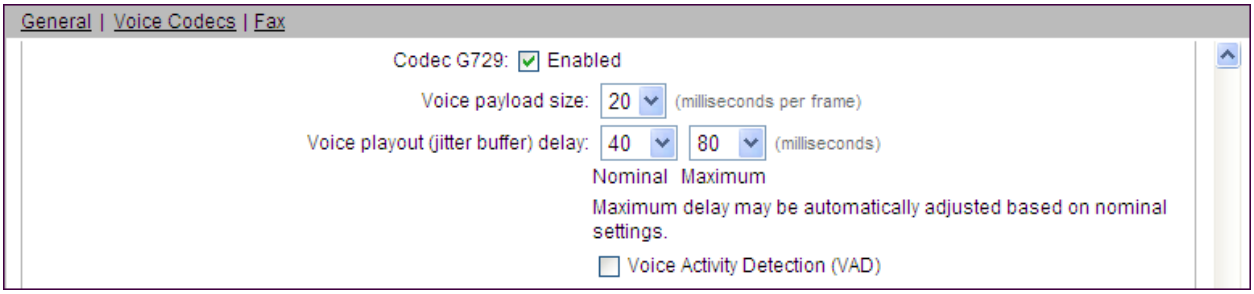
The following screen shows the General parameters used in the sample configuration.



Use the scroll bar on the right to find the area with heading **Voice Codecs**. Note that **Codec G.711** is enabled by default. The following screen shows the G.711 parameters used in the sample configuration.

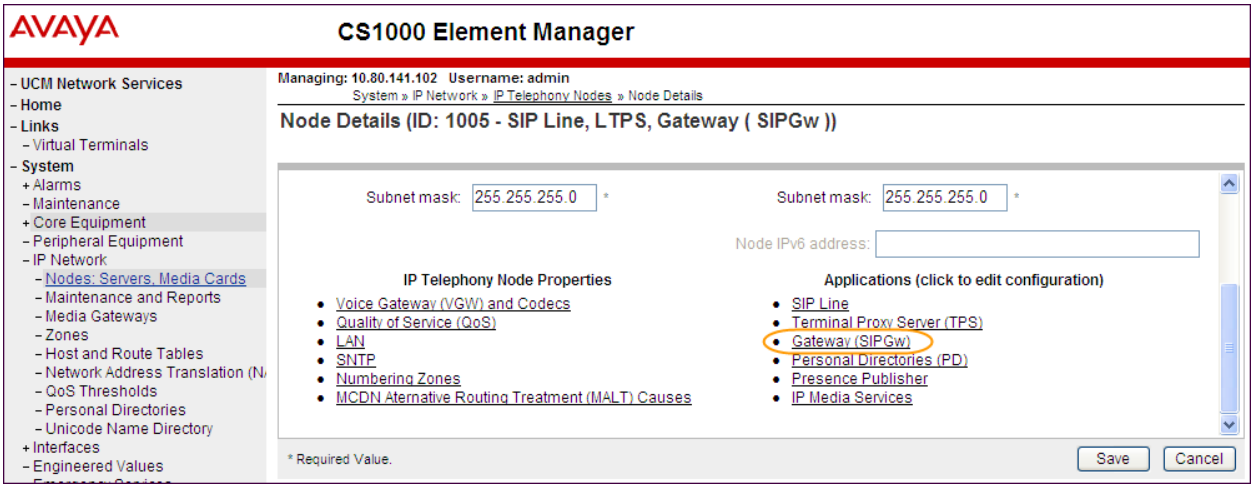


For the **Codec G.729**, ensure that the **Enabled** box is checked, and the **Voice Activity Detection (VAD)** box is un-checked, as shown below. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order. During compliance testing, the G.729B codec was also tested by checking the **Voice Activity Dectection (VAD)** box.



5.1.5. SIP Gateway

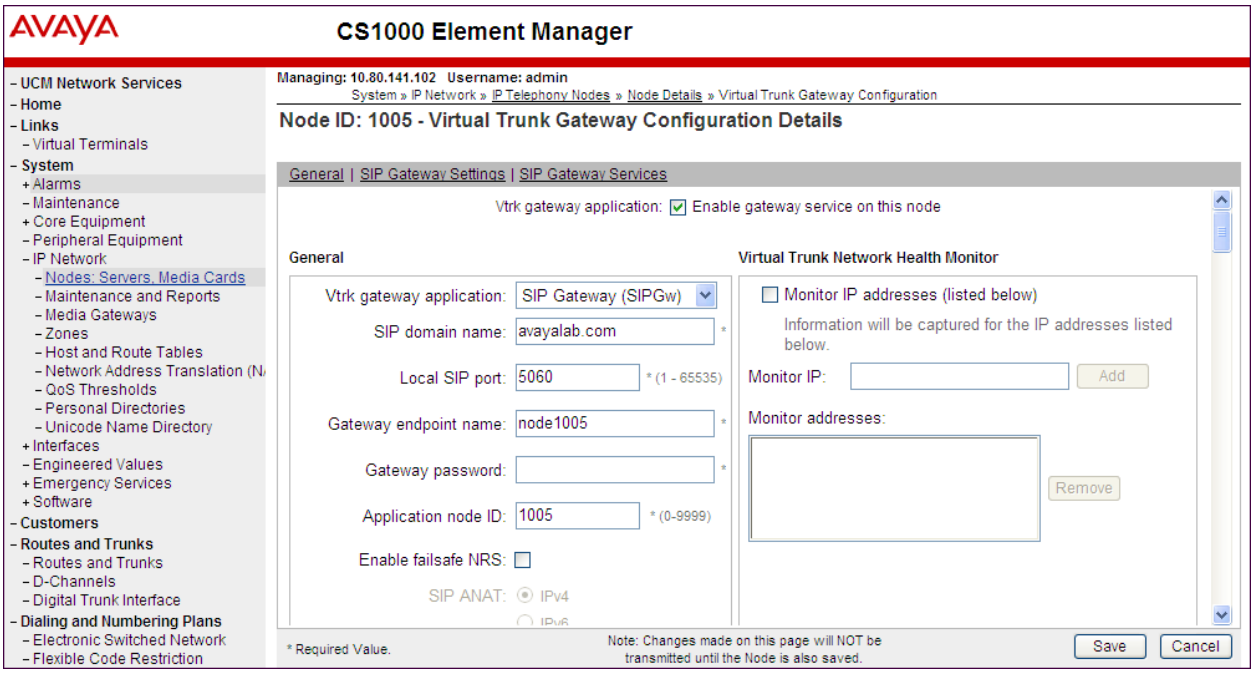
The SIP Gateway is the SIP trunk between the CS1000E Signaling Server and the Network Routing Server. On the **Node Details** screen, scroll down in the top window and select the **Gateway (SIPGw)** link as show below.



On the **Node ID: <id> – Virtual Trunk Gateway Configuration Details** page, enter the following values and use default values for remaining fields.

- **Sip domain name:** Enter the appropriate SIP domain for the customer network. In the sample configuration, **avayalab.com** was used in the Avaya Solutions and Interoperability Test lab environment.
- **Local SIP port:** Enter **5060**.
- **Gateway endpoint name:** Enter a descriptive name. This name will be used to register with the Network Routing Server (**Section 5.10.2**)
- **Application node ID:** Enter **<Node id>**. In the sample configuration, Node **1005** was used matching the node show in **Section 5.1**.

The values defined for the sample configuration are shown below.

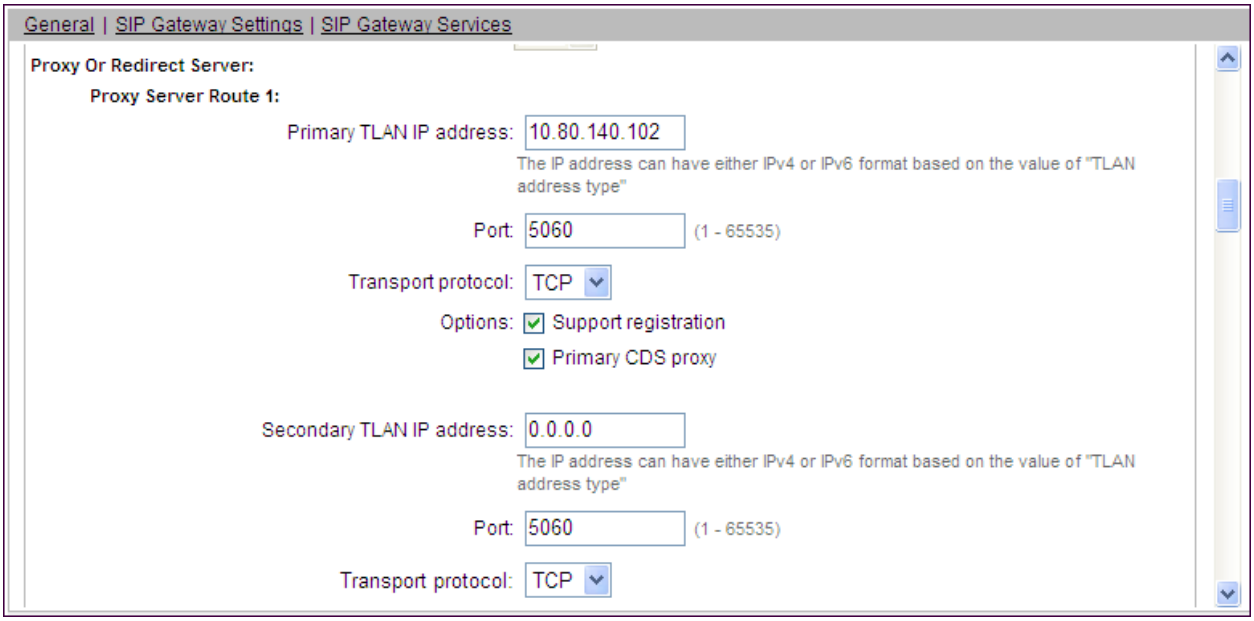


Scroll down to the **SIP Gateway Settings → Proxy or Redirect Server:** section.

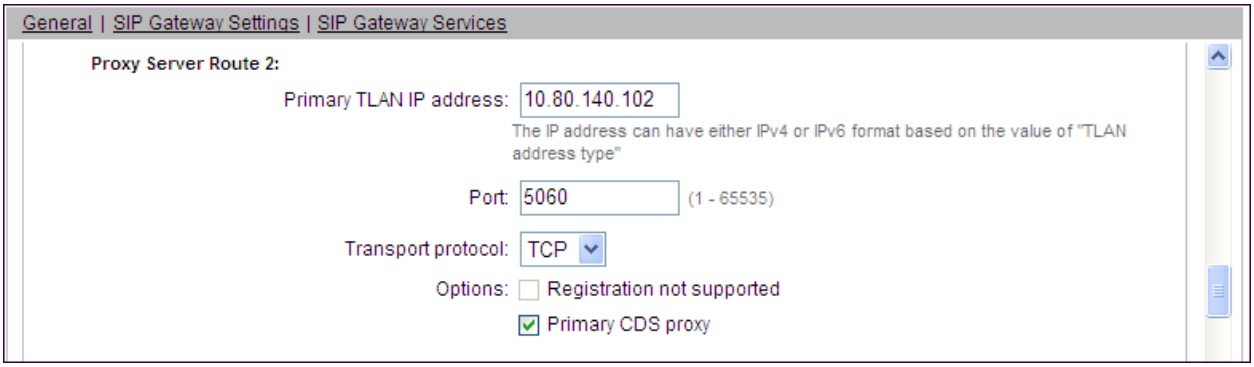
Under **Proxy Server Route 1**, enter the following and use default values for remaining fields.

- **Primary TLAN IP address**: Enter the IP address of the Network Routing Server (NRS). In the sample configuration, the NRS is co-resident with the Call Server so **10.80.104.102** was used.
- **Port**: Enter **5060**
- **Transport protocol**: Select **TCP**
- **Options:** Check both **Support registration** and **Primary CDS proxy.**

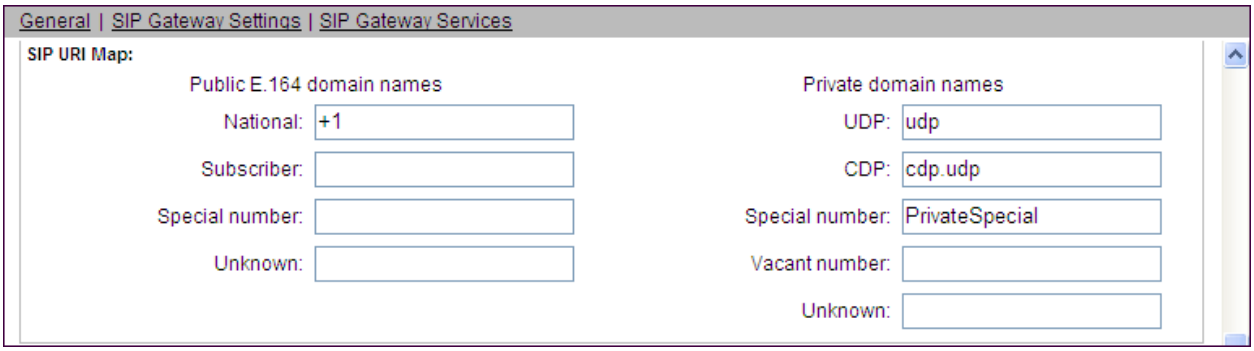
The values defined for the sample configuration are shown below.



Scroll down and repeat these steps for the **Proxy Server Route 2**.



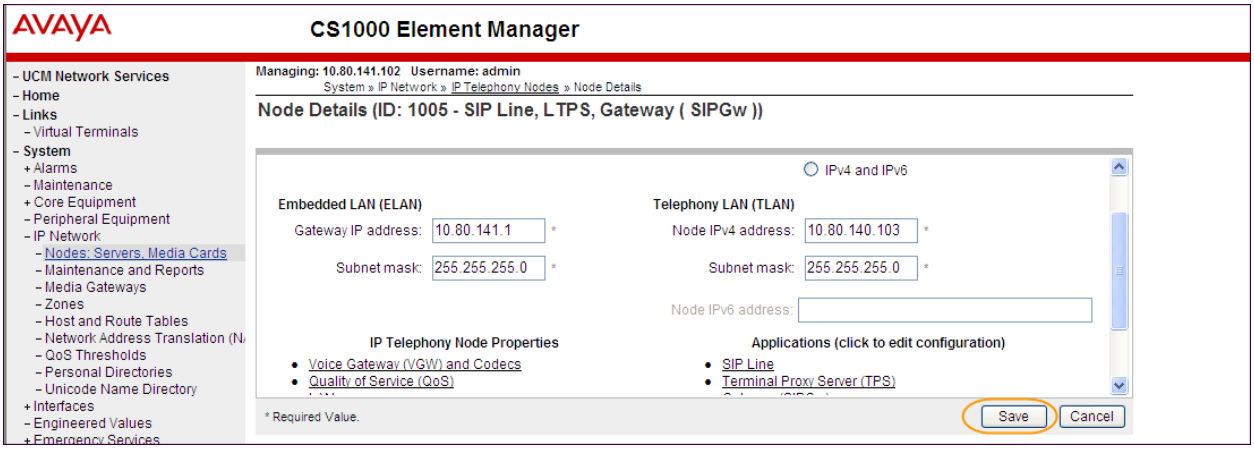
Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. The Avaya CS1000E will put the "string" entered in the **SIP URI Map** in the "phone-context=<string>" parameter in SIP headers such as the To and From headers. If the value is configured to blank, the CS1000E will omit the "phone-context=" in the SIP header altogether. For compliance testing, **+1** was added for **National** calling.



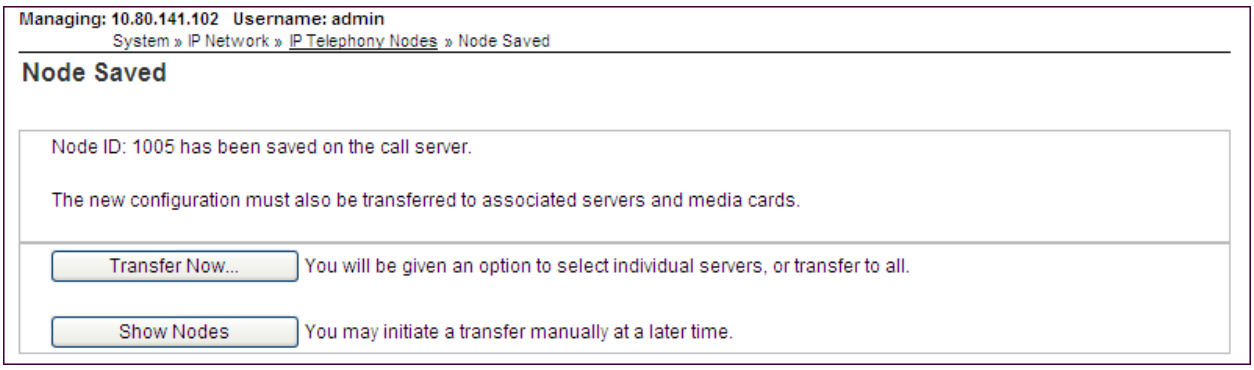
Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen.

5.1.6. Synchronize Node Configuration

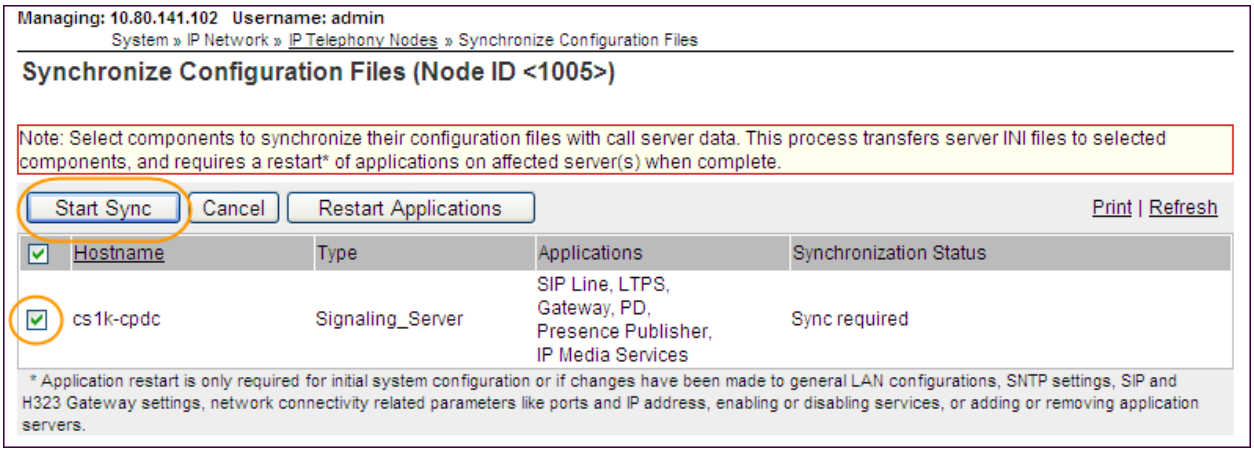
On the **Node Details** screen click **Save** as shown below.



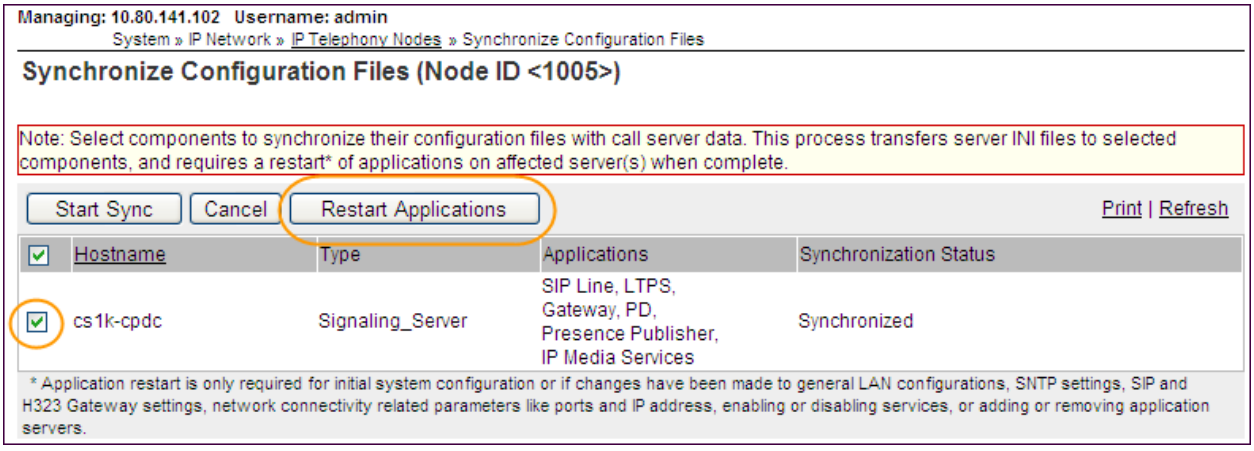
Select **Transfer Now** on the **Node Saved** page as show below.



Once the transfer is complete, the **Synchronize Configurations Files (NODE ID <id>)** page is displayed. Place a check mark next to the appropriate Hostname and click **Start Sync**. The screen will automatically refresh until the synchronization is finished.

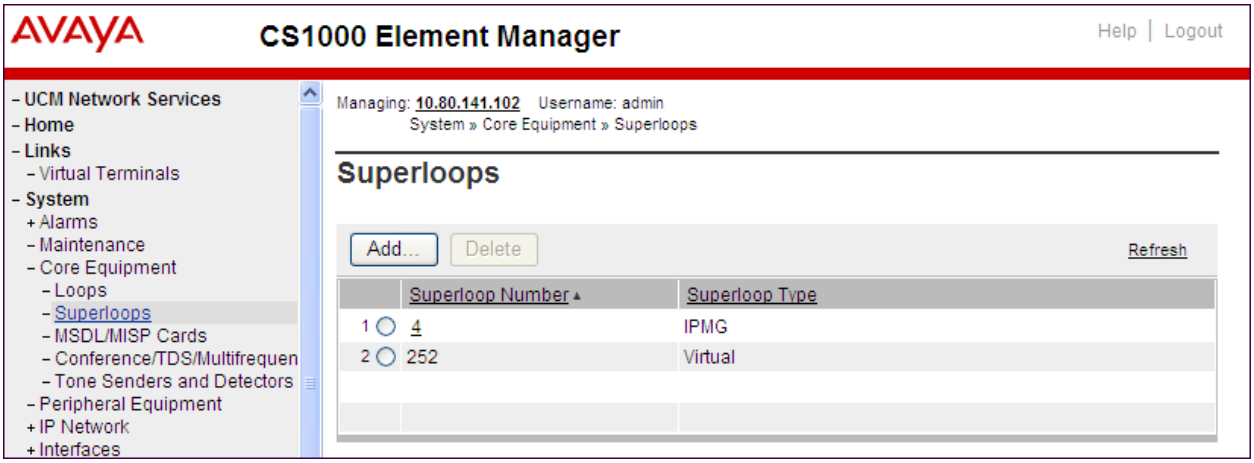


The **Synchronization Status** field will update from **Sync required** (as shown above) to **Synchronized** (as shown below). After synchronization completes, place a check mark next to the appropriate Hostname and click **Restart Applications**.



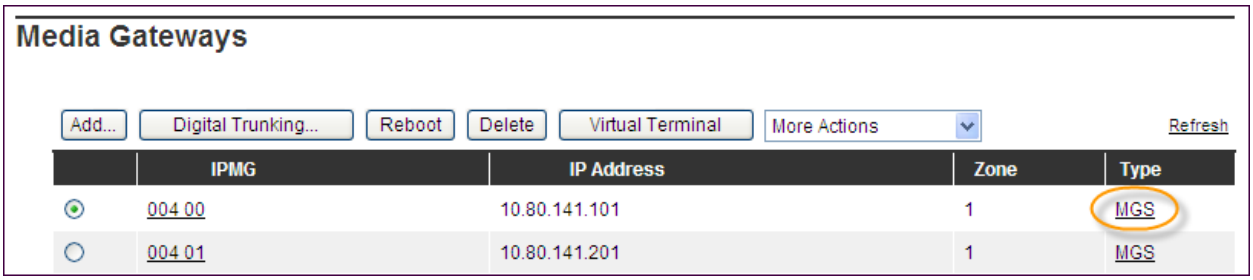
5.2. Virtual Superloops

Expand **System → Core Equipments** on the left panel and select **Superloops**. In the sample configuration, Superloop 4 is for the Media Gateway and Superloop 252 is the virtual Superloop used by the IP phones and SIP trunks.

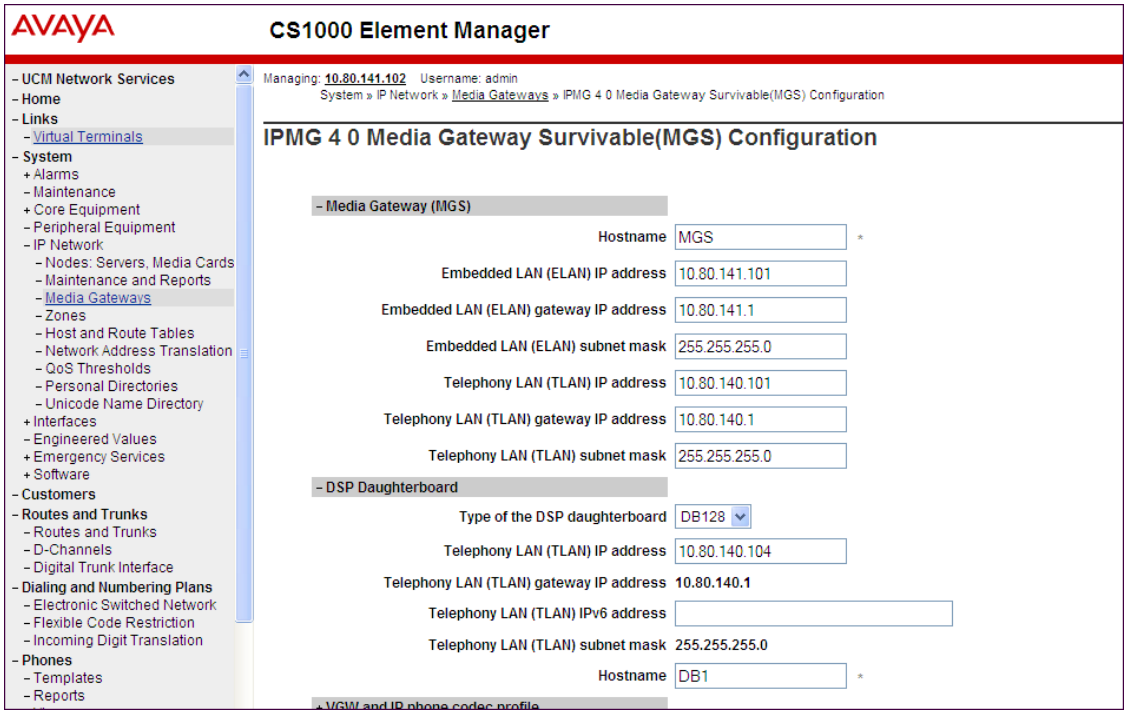


5.3. Media Gateway

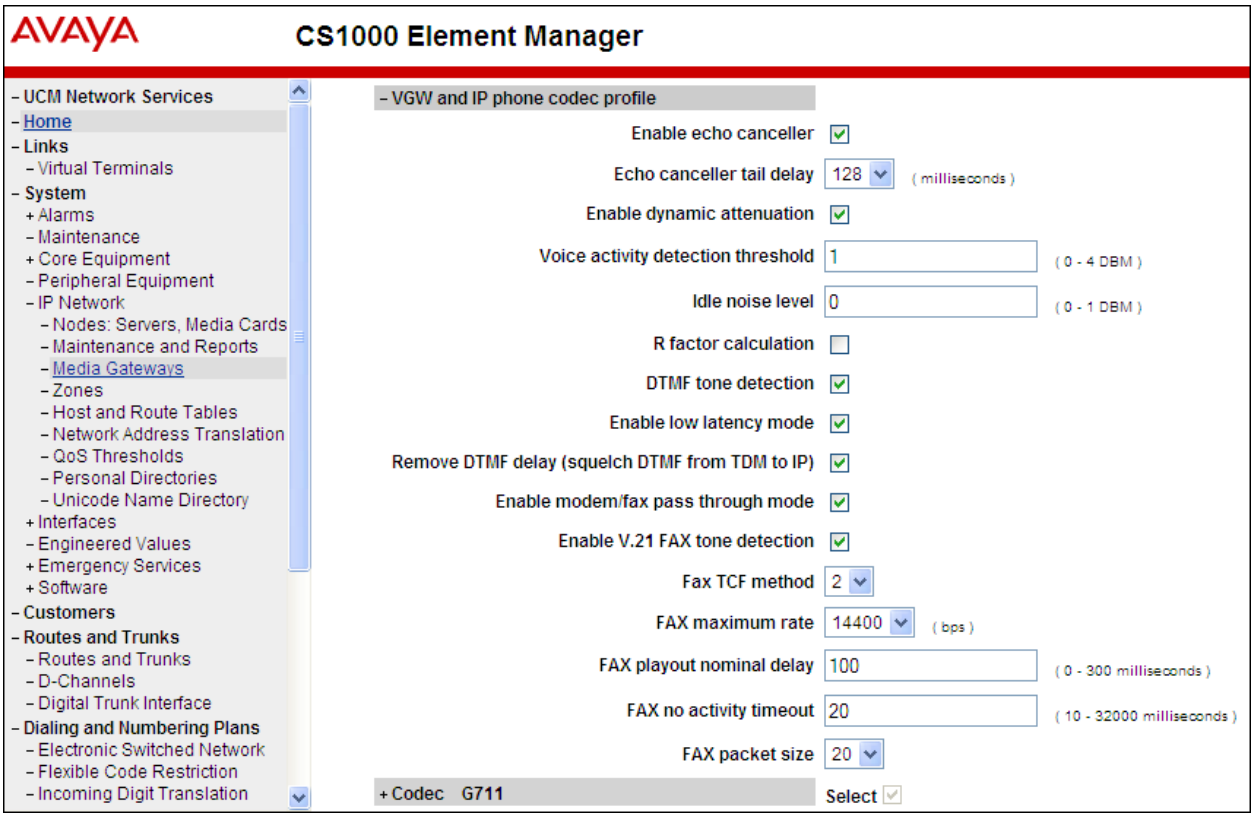
Expand **System → IP Network** on the left panel and select **Media Gateways**. Click the link in the **Type** column for the appropriate Media Gateway to be modified as shown below.



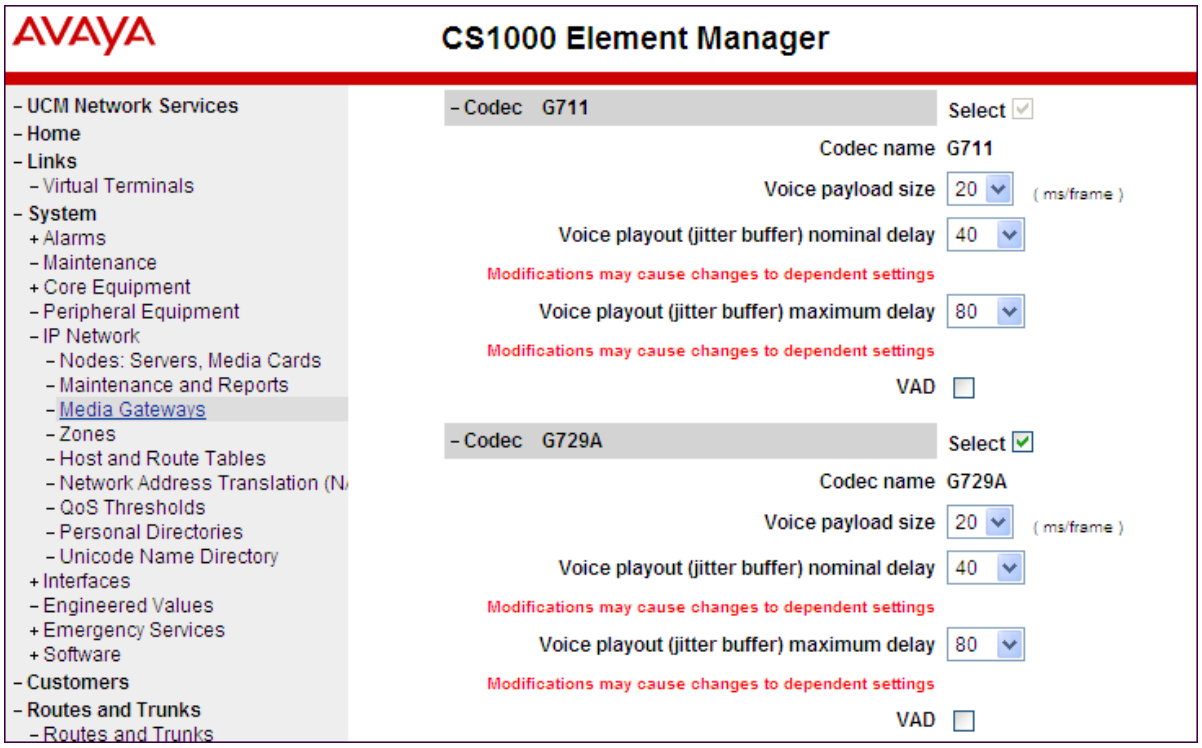
The **IPMG 4 0 Media Gateway Survivable(MGS) Configuration** window appears. The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard 1** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for a call from a digital telephone to the PSTN via CenturyLink SIP Trunk, the IP Address in the SDP in the INVITE message will be **10.80.140.104** in the sample configuration.



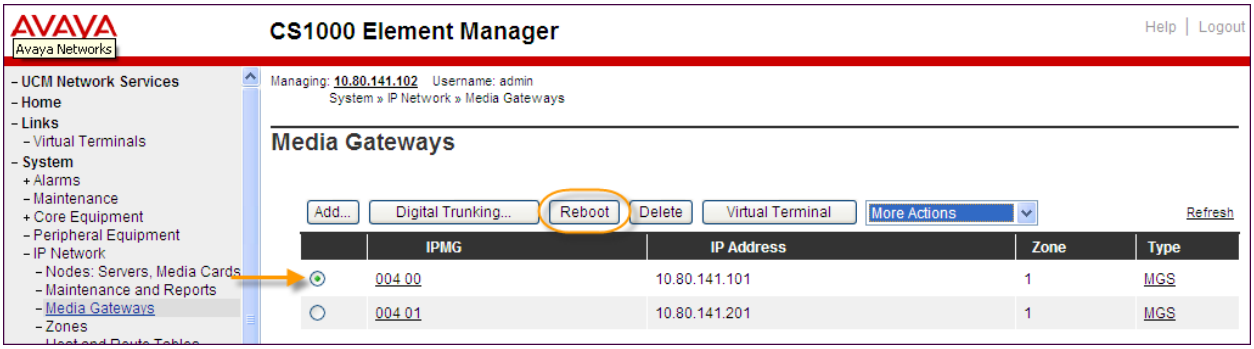
Scroll down to the area of the screen containing **VGW and IP phone codec profile** and expand it. The fax T.38 settings used for compliance testing is shown below.



The **Codec G.711** is enabled by default. Ensure that the **Select** box is checked for **Codec G729A** and the **VAD** (Voice Activity Detection) box is un-checked. The **Voice payload size** of **20** can be used with CenturyLink SIP Trunk for both G.729A and G.711. Click **Save** (not shown) at the bottom of the window. Then click **OK** in the dialog box (not shown) to save the IPMG configuration. During compliance testing, the G.729B codec was also tested by checking the **Voice Activity Dectection (VAD)** box. Scroll down and click **Save** and then click **OK** on the new dialog box that appears to save the configuration.



Once the configuration is saved, the **Media Gateways** page is displayed. Select the appropriate Media Gateway and click **Reboot** to load the new configuration.

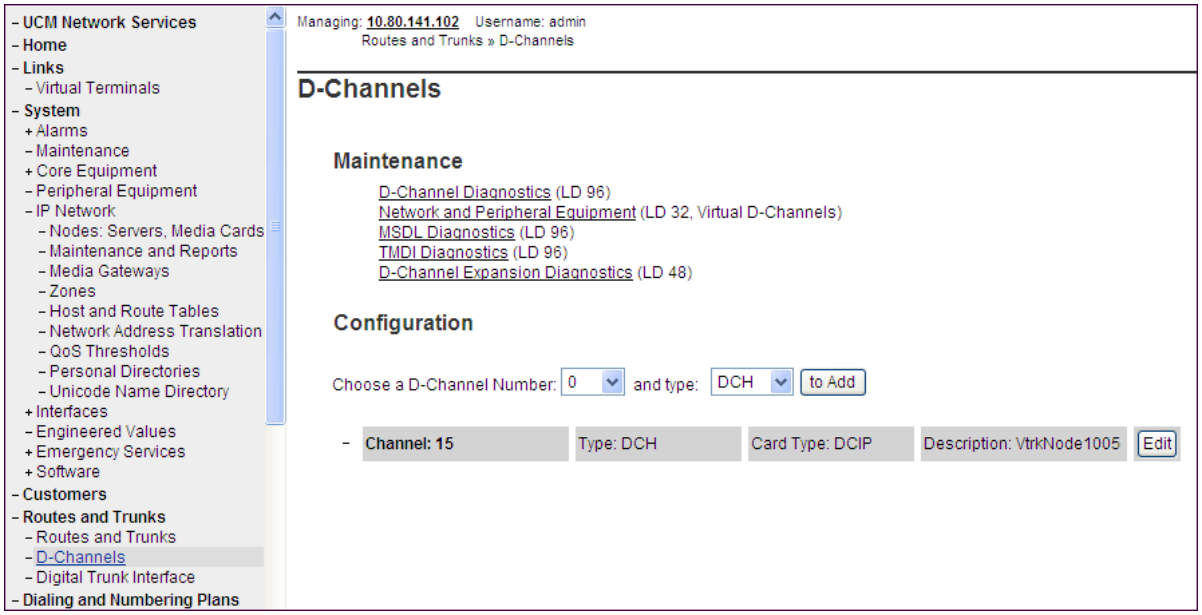


5.4. Virtual D-Channel, Routes and Trunks

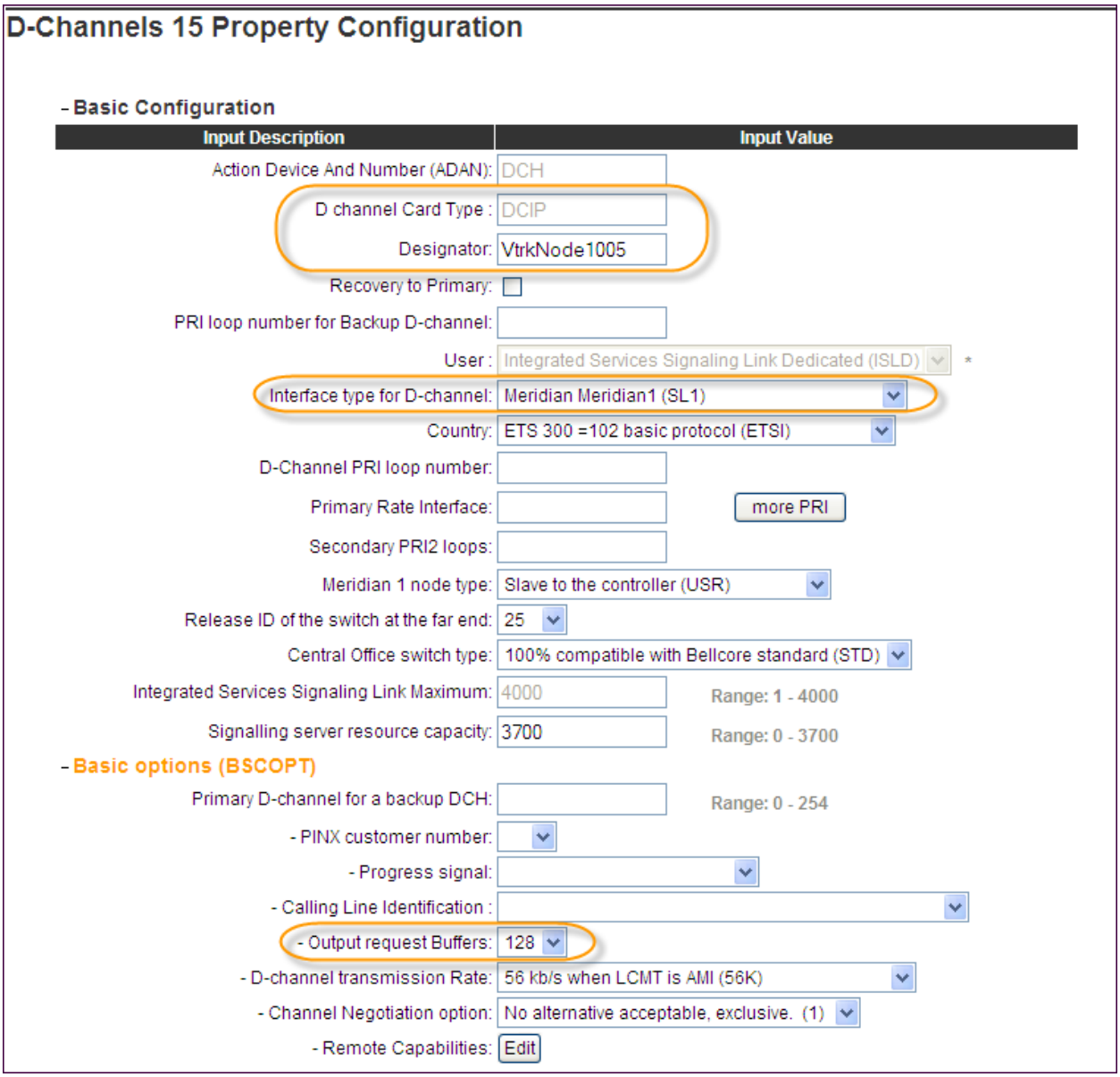
Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server.

5.4.1. Virtual D-Channel Configuration

Expand **Routes and Trunks** on the left panel and select **D-Channels**. In the sample configuration, there is a virtual D-Channel 15 associated with the Signaling Server.

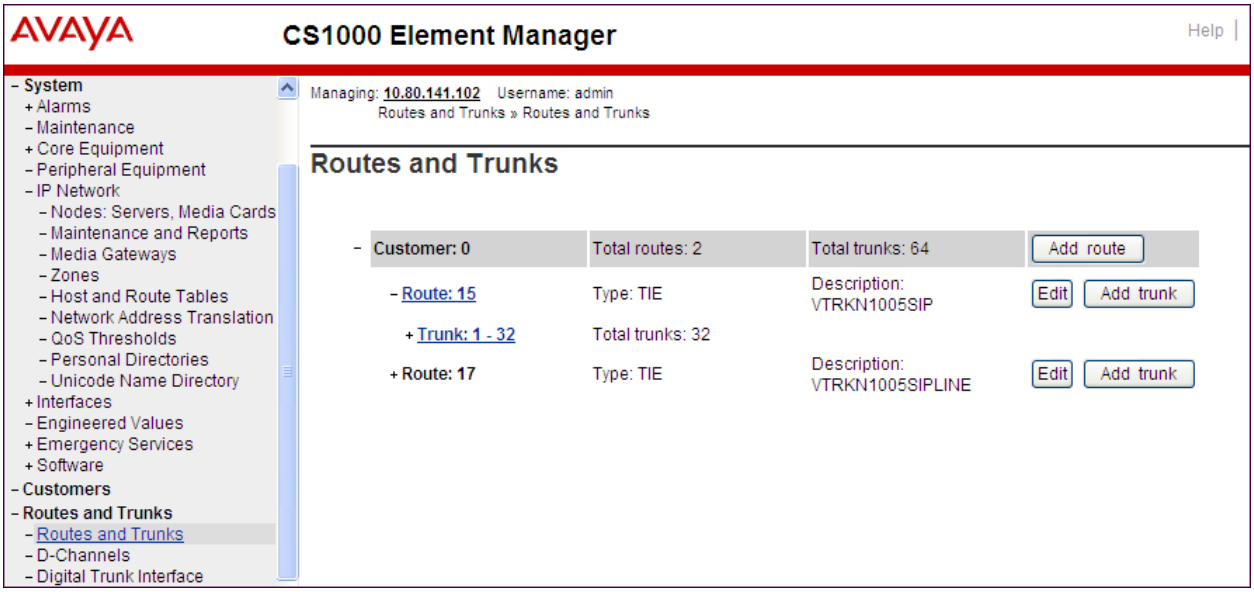


Select **Edit** to verify the configuration, as shown below. Verify **DCIP** has been selected for **D Channel Card Type** field and the **Interface type for D-Channel** is set to **Meridian Meridian 1(SL1)**. Under the Basic Options section, verify **128** is selected for the **Output request Buffers** value.

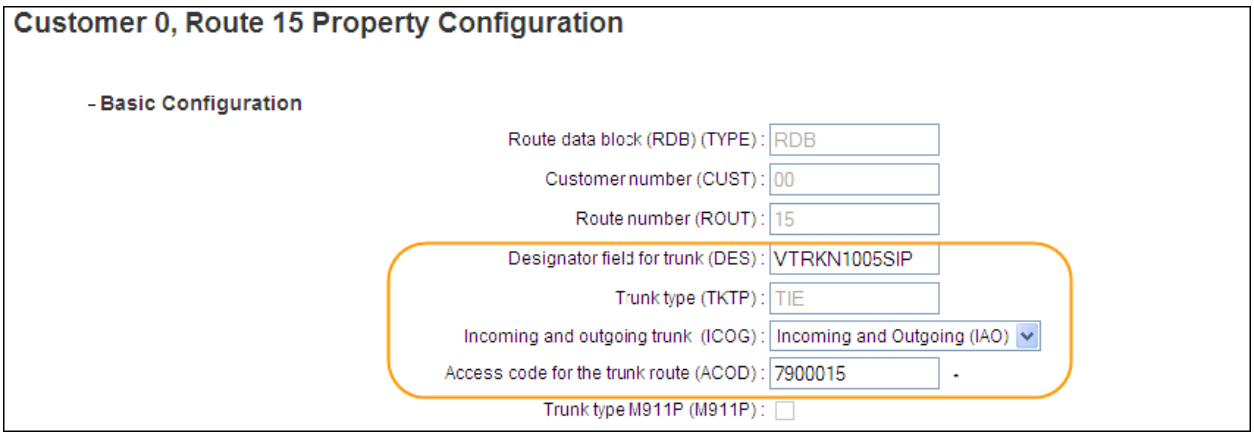


5.4.2. Routes and Trunks Configuration

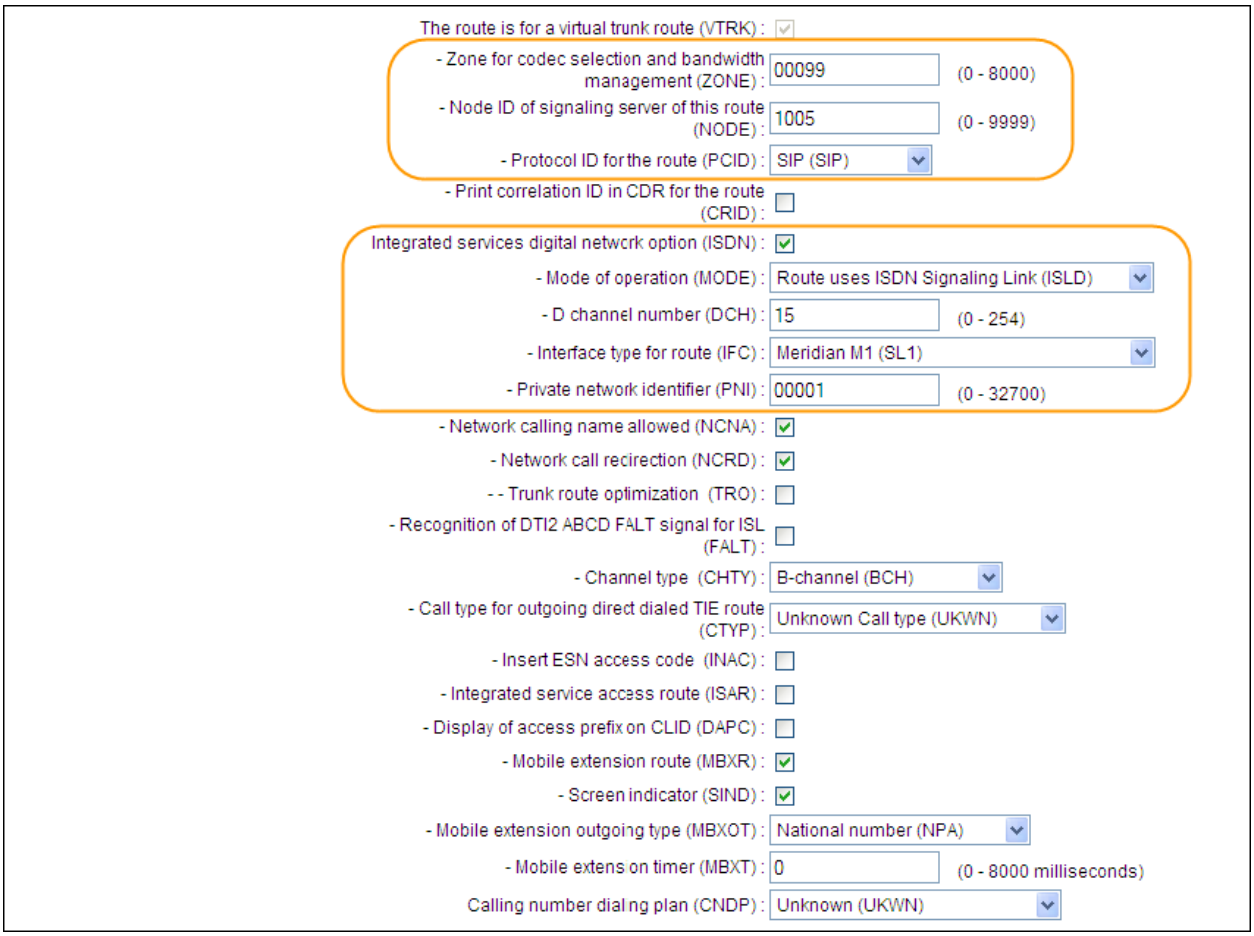
In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured. Expand **Routes and Trunks** on the left panel and expand the customer number. In the example screen that follows, it can be observed that Route 15 has 32 trunks in the sample configuration.



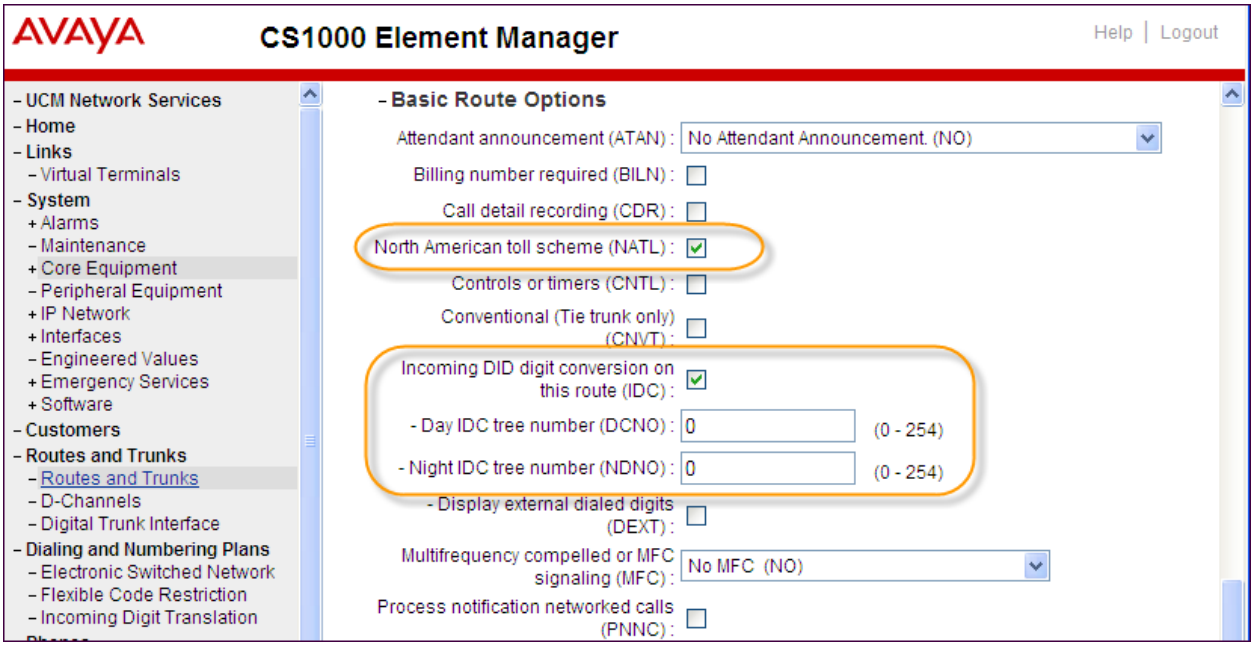
Select **Edit** to verify the configuration, as shown below. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may be observed on Avaya CS1000E display phones if an incoming call on the trunk is anonymous or marked for privacy.



Further down in the **Basic Configuration** section verify the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.1**. Also verify **SIP (SIP)** has been selected for **Protocol ID for the route (PCID)** field. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging. The **D channel number (DCH)** field must match the D-Channel number shown in **Section 5.4.1**.



Scroll down and expand the **Basic Route Options** section. Check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 0** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown below. The DCNO is created later on in **Section 5.5.6**.



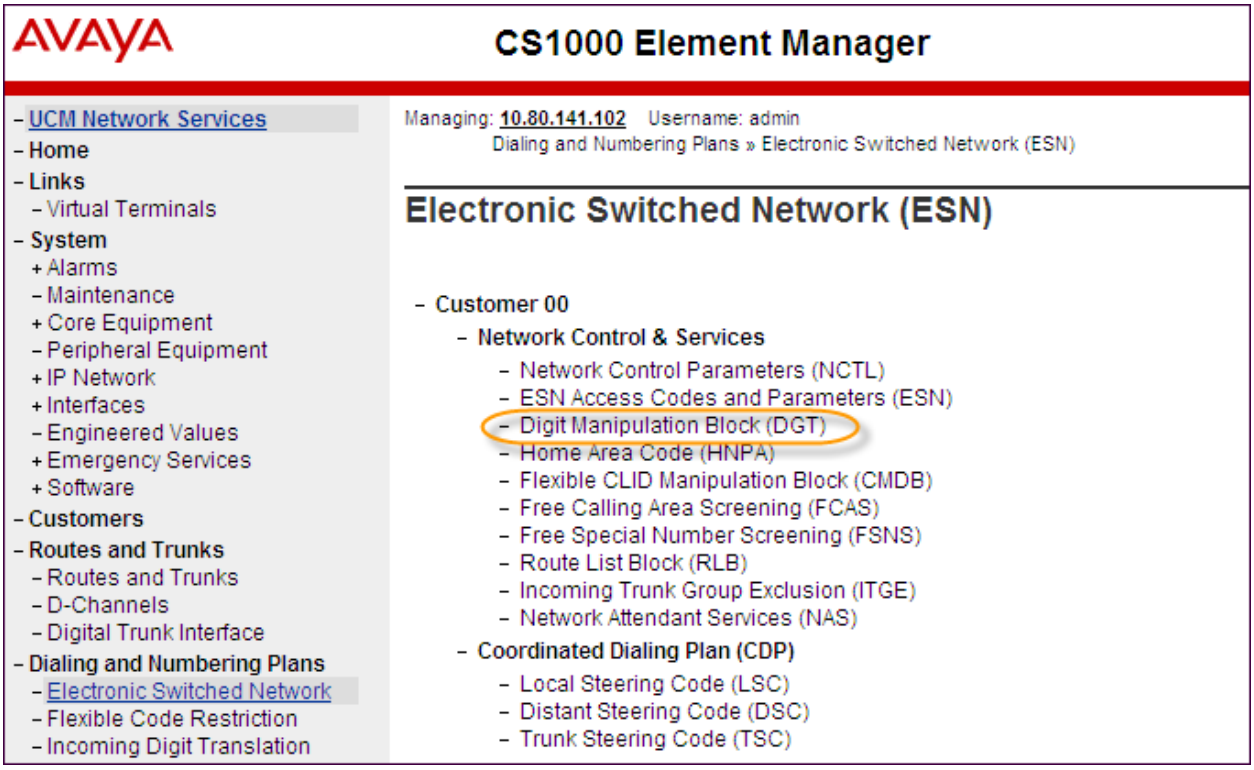
5.5. Dialing and Numbering Plans

This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Network Routing Server for calls destined for the CenturyLink SIP Trunk. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks.

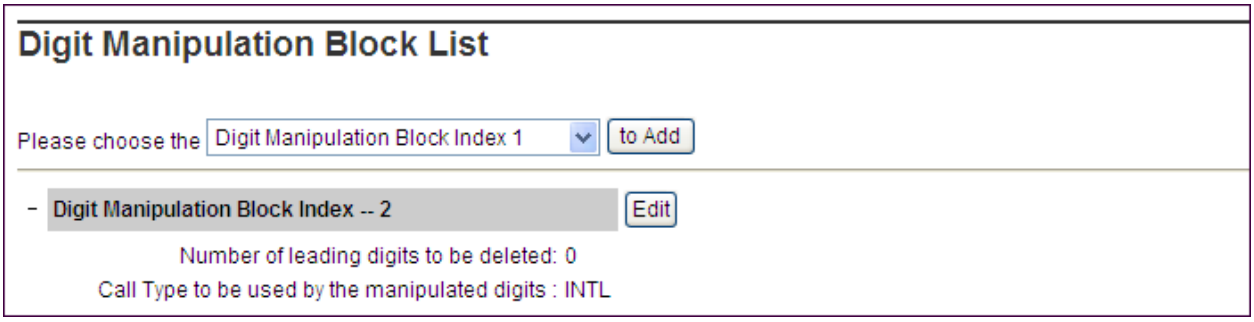
5.5.1. Digit Manipulation Block

A Digit Manipulation Block was created to properly identify International calls over the SIP Trunk between Avaya Communication Server 1000E and Network Routing Server.

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **Digit Manipulation Block (DGT)** on the **Electronic Switched Network (ESN)** page as shown below.

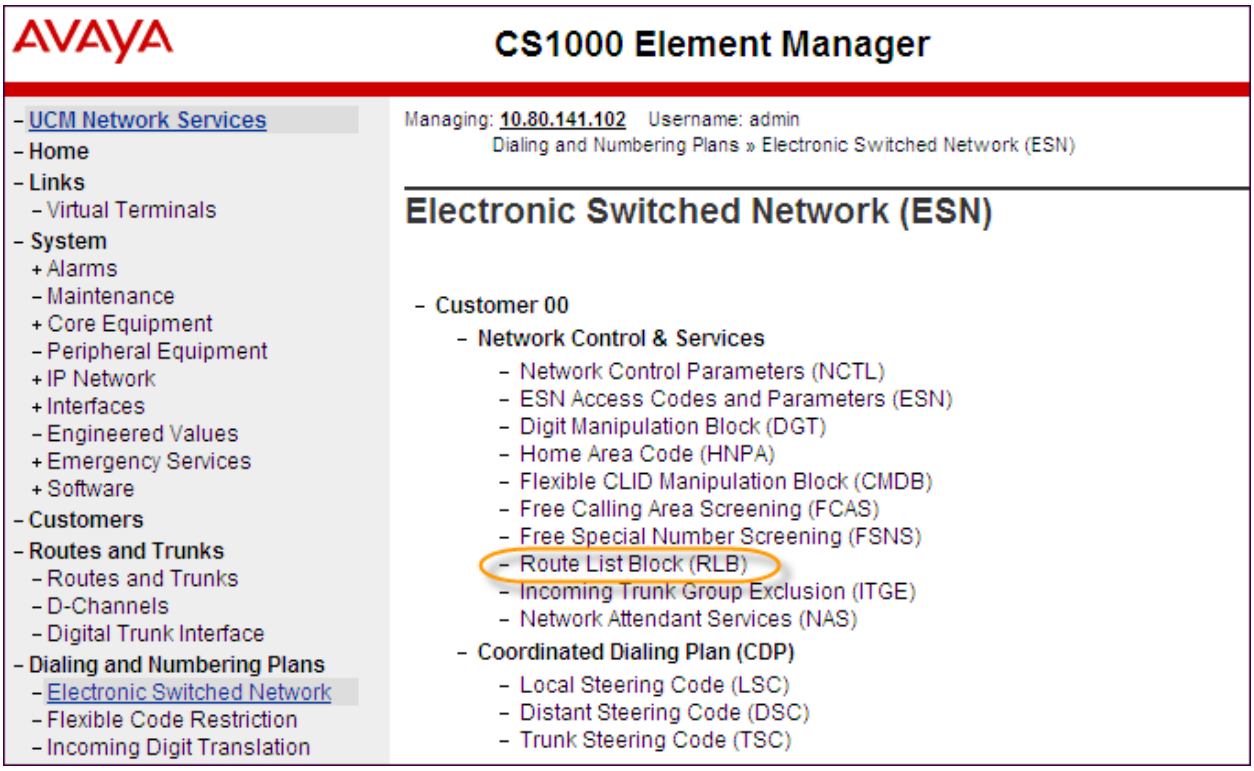


The **Digit Manipulation Block List** screen is displayed. In the sample configuration, a Digit Manipulation Block is needed to set the proper call type for International calls. Select an available Digit Manipulation Block Index number (other than 1) in the **Please Choose the** field and click **to Add**, or edit an existing entry by clicking the corresponding **Edit** button. In the sample configuration, **Digit Manipulation Block Index 2** is used. Select **INTL** for **Call Type to be used by the manipulated digits**.

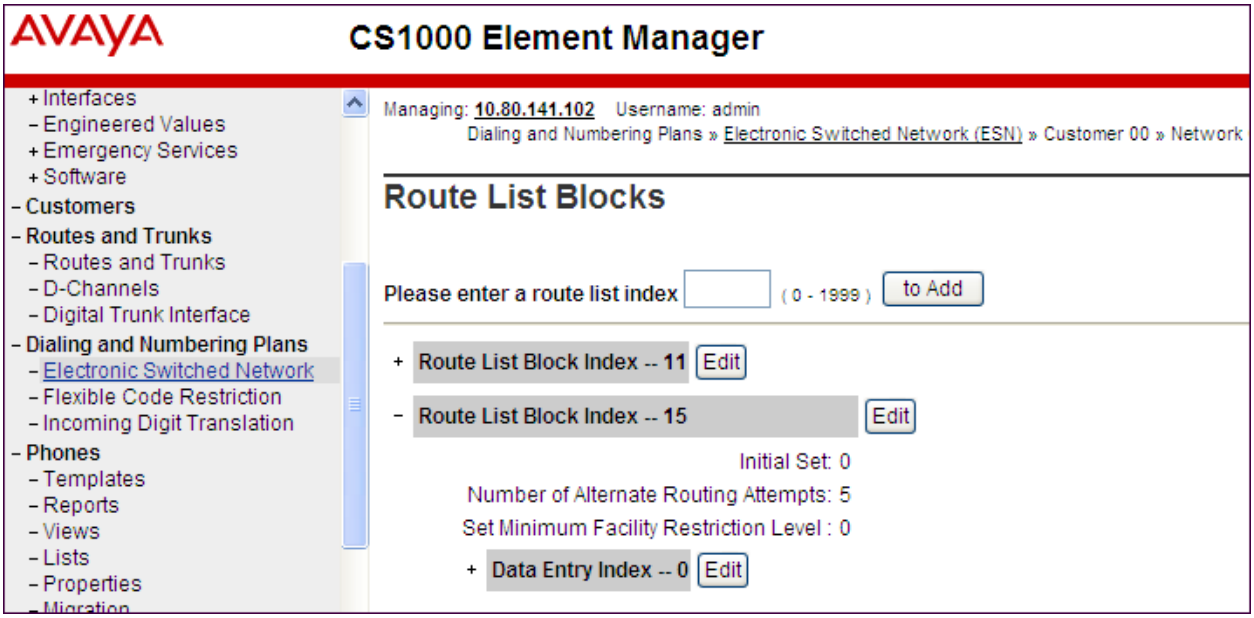


5.5.2. Route List Block

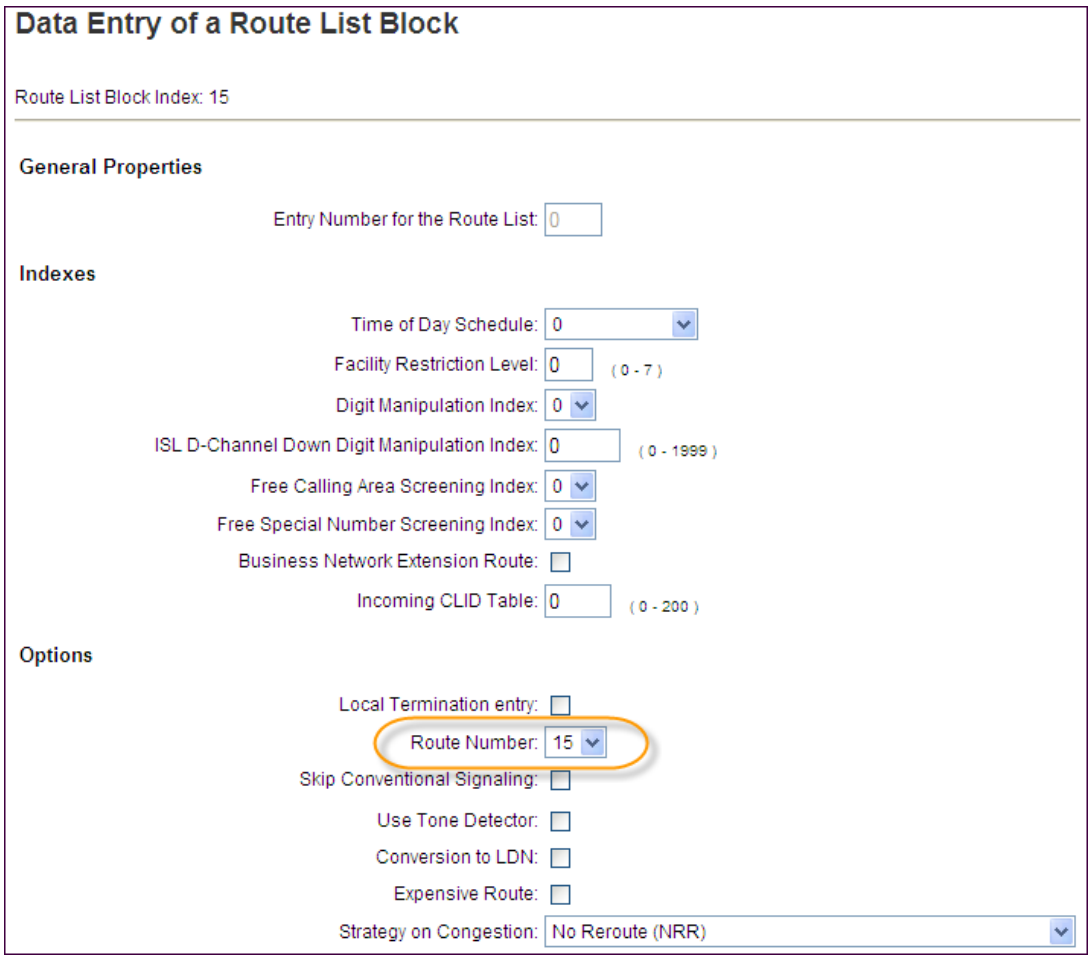
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown below.



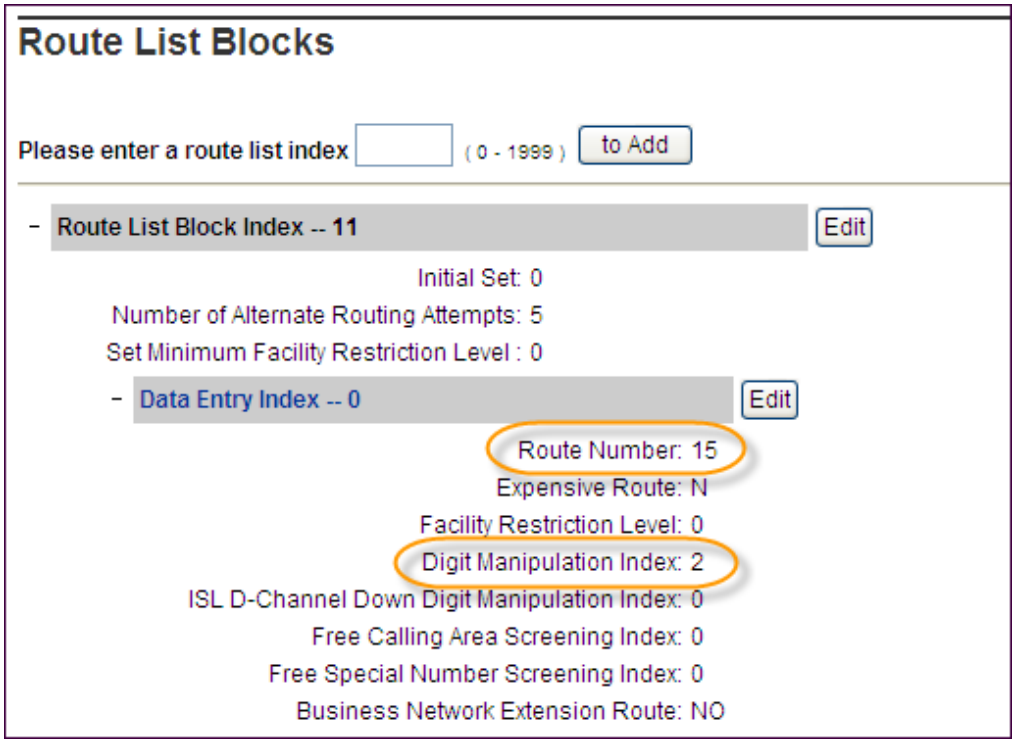
The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click **to Add**, or edit an existing entry by clicking the corresponding Edit button. In the sample configuration, route list block index **15** is used. If adding the route list index anew, scroll down to the **Options** area of the screen. If editing an existing route list block index, select the **Edit** button next to the appropriate Data Entry Index as shown below, and scroll down to the **Options** area of the screen.



Under the **Options** section, select **<Route id>** in the **Route Number** field. In the sample configuration route number **15** was used. Default values may be retained for remaining fields as shown below.

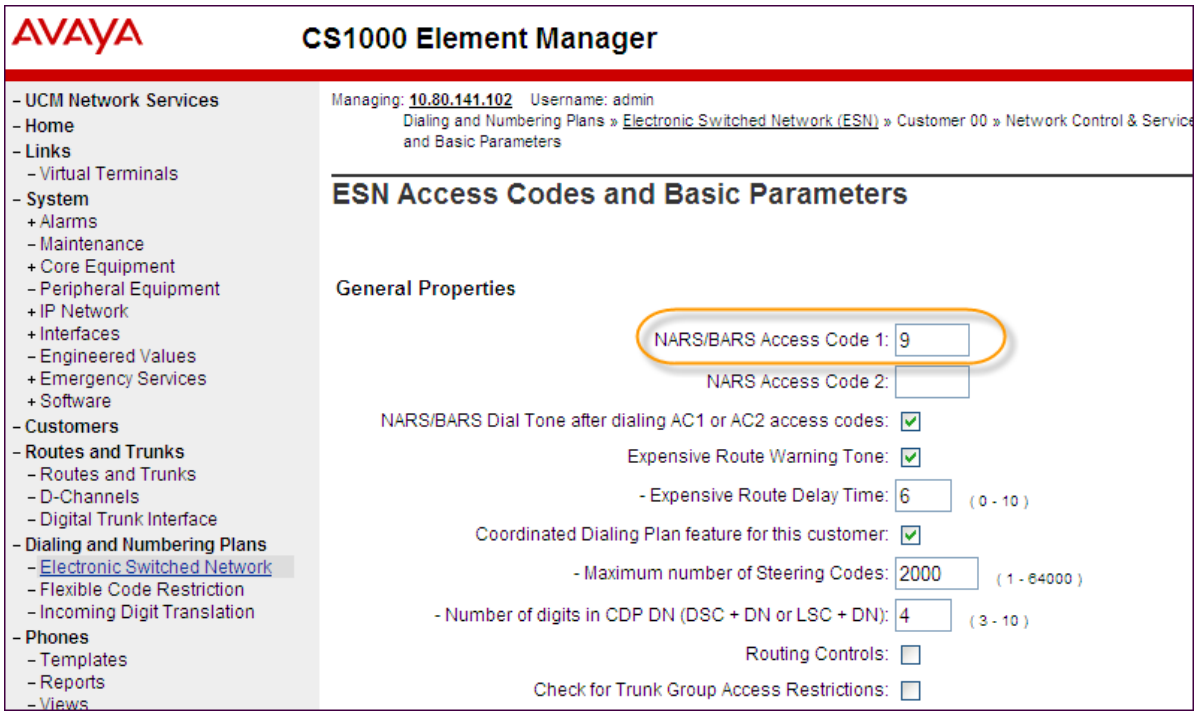


Repeat these steps to create a separate **Route List Block** used for International calls. In addition select the **Digit Manipulation Index** created in **Section 5.5.1**. In the sample configuration Route List Block 11 was created for International calls.



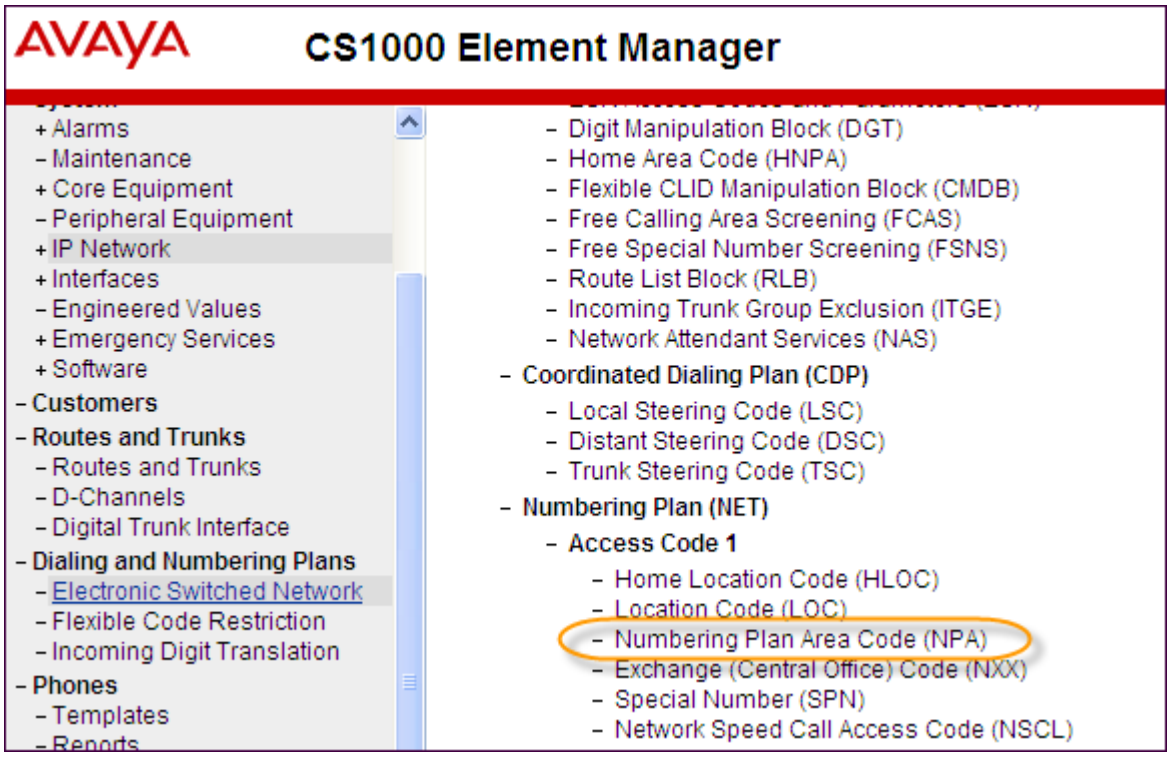
5.5.3. NARS Access Code

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **ESN Access Codes and Parameters (ESN)**. Although not repeated below, this link can be observed in the first screen in **Section 5.5.2**. In the **NARS/BARS Access Code 1** field, enter the number the user will dial before the target PSTN number. In the sample configuration, the single digit **9** was used.

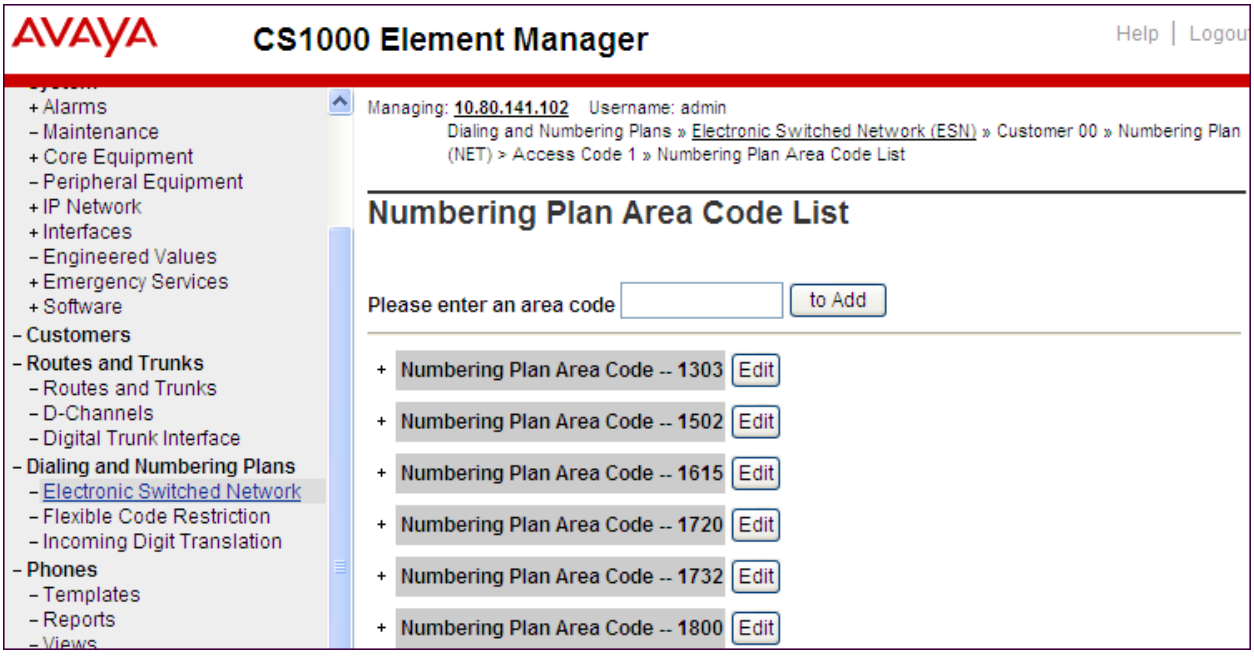


5.5.4. Numbering Plan Area Codes

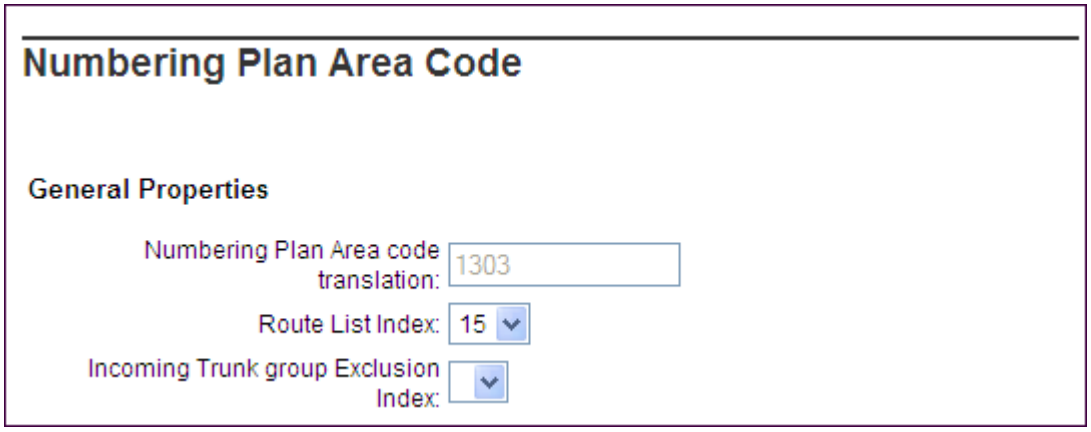
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Numbering Plan Area Code (NPA)** under the appropriate access code heading. In the sample configuration, this is **Access Code 1**, as shown below.



Add a new NPA by entering it in the **Please enter an area code** box and click **to Add** or click **Edit** to view or change an NPA that has been previously configured. In the screen below, it can be observed that various dial strings such as **1303** and **1800** are configured.



In the screen below, the entry for **1303** is displayed. In the Route List Index, **15** is selected to use the route list associated with the SIP Trunk to the NRS as shown in **Section 5.4.2**. Default parameters may be retained for other parameters. Repeat this procedure for the dial strings associated with other numbering plan area codes that should route to the SIP Trunk to the NRS.

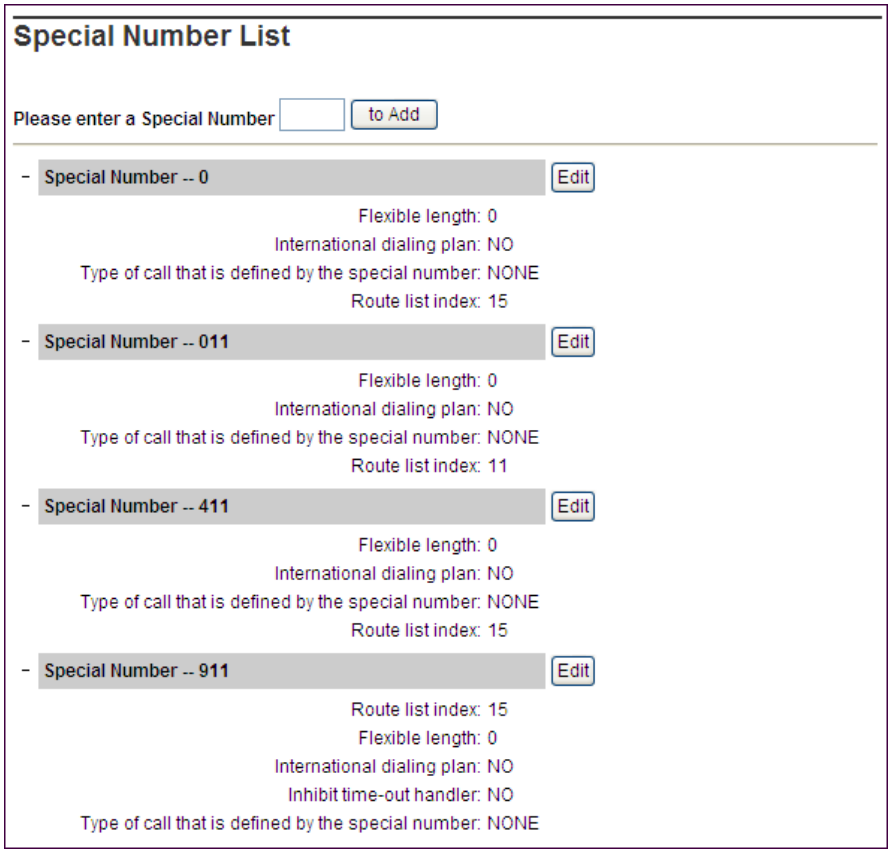


5.5.5. Special Number to Route to NRS

In the testing associated with these Application Notes, special service numbers such as x11, international calls, and operator assisted calls were also routed to the NRS and ultimately to the CenturyLink SIP Trunk. Although not intended to be prescriptive, one approach to such routing is summarized in this section.

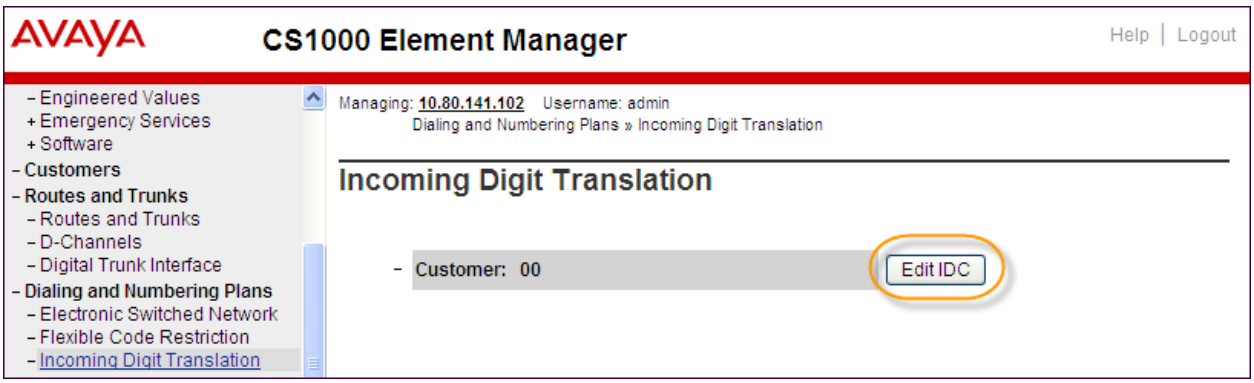
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Special Number (SPN)** under the appropriate access code heading (as can be observed in the first screen in **Section 5.5.4**).

Add a new number by entering it in the **Please enter a Special Number** box and click **to Add** or click **Edit** to view or change a special number that has been previously configured. In the screen below, it can be observed that various dial strings such as **0**, **011**, **411** and **911** calls are listed. With the exception of 011, Route list index **15** has been selected in the same manner as shown for the NPAs in the prior section. For International calls, Route list index **11** was selected.

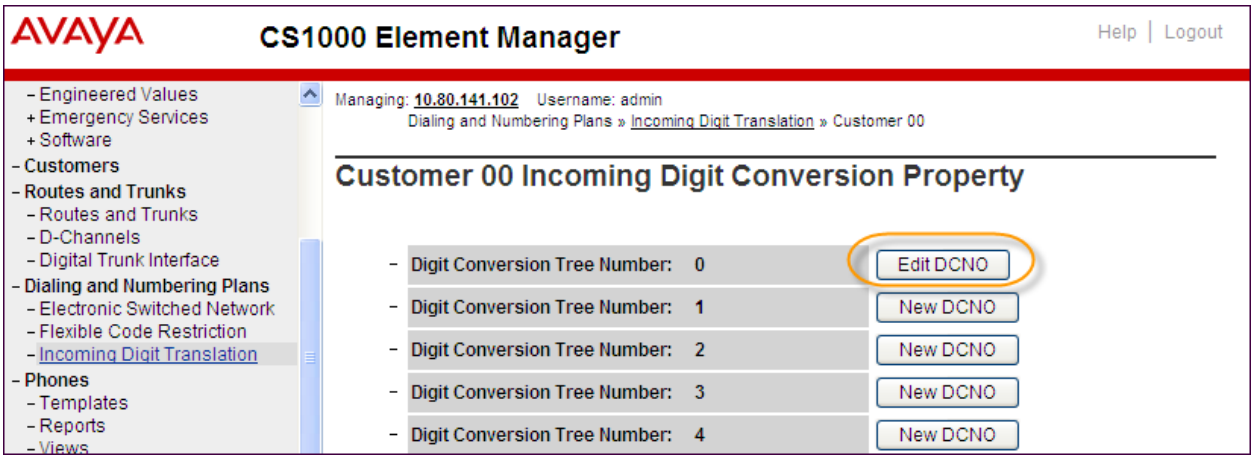


5.5.6. Incoming Digit Translation

In general, the incoming digit translation can be used to manipulate the digits received for an incoming call. Expand **Dialing and Numbering Plans** on the left panel and select **Incoming Digit Translation**. Click on the **Edit IDC** button as shown on the following screen.

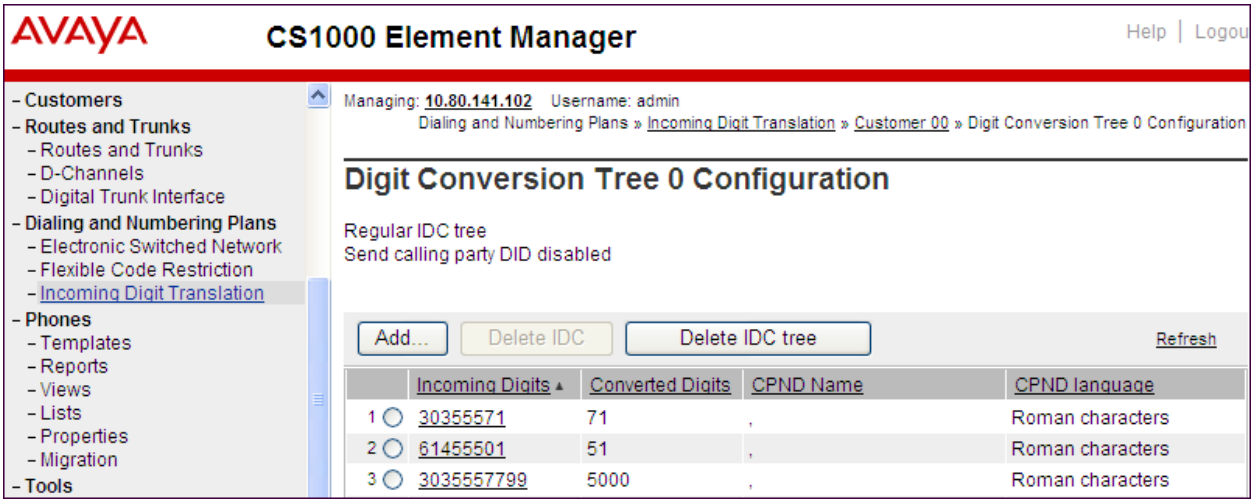


Click on the **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number (DCNO) 0** has been created as shown below.



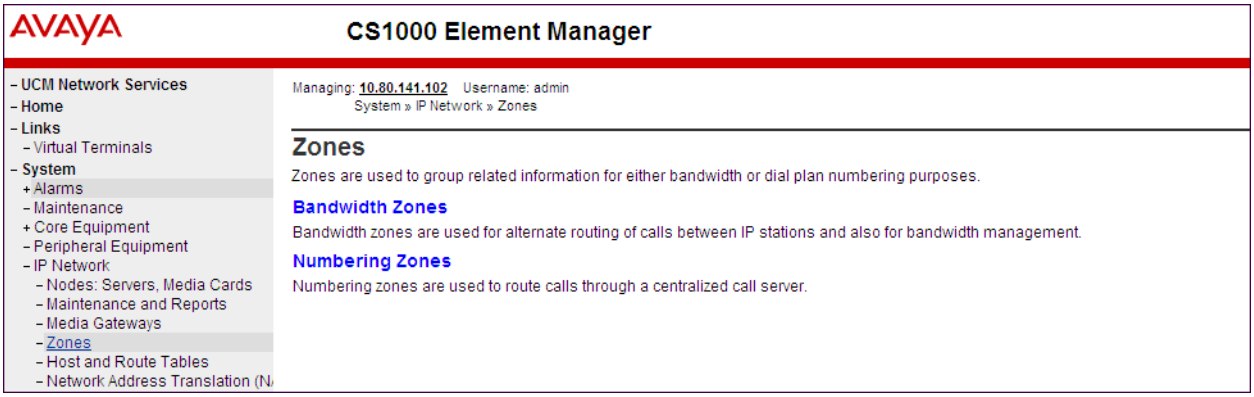
Detail configuration of the **DCNO** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000E system phones DN. This **DCNO** has been assigned to route 15 as shown in **Section 5.4.2**.

In the following configuration, the incoming call from PSTN with the prefix 303-555-71xx will be translated to CS1000E DN 71xx. The PSTN with the prefix 614-555-01xx will be translated to CS1000E DN 51xx. The DID 303-555-7799 is translated to 5000 for Voicemail accessing purpose.

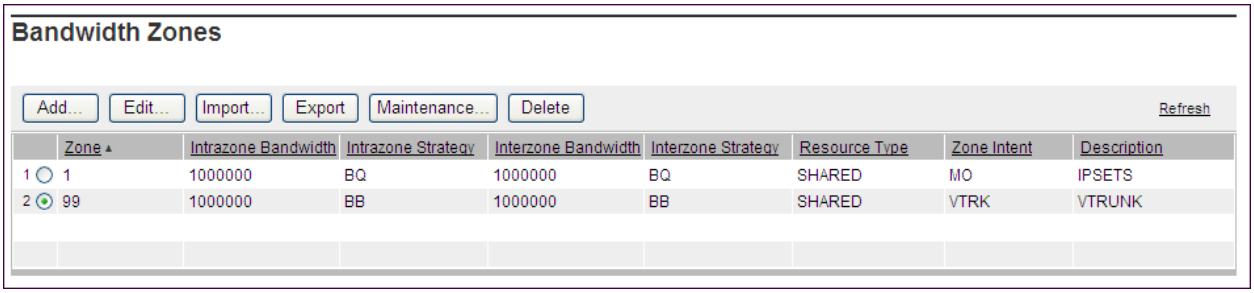


5.6. Zones and Bandwidth

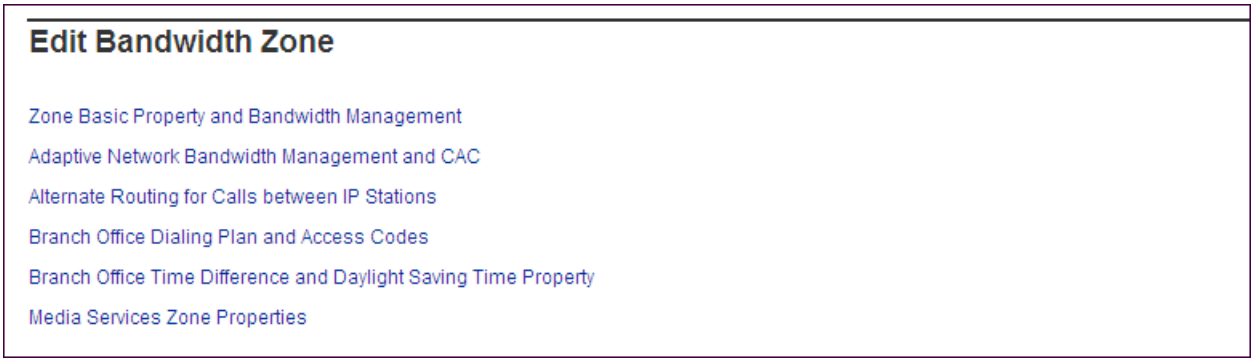
Zone configuration can be used to control codec selection and for bandwidth management. To configure, expand **System → IP Network** on the left panel and select **Zones** as shown below.



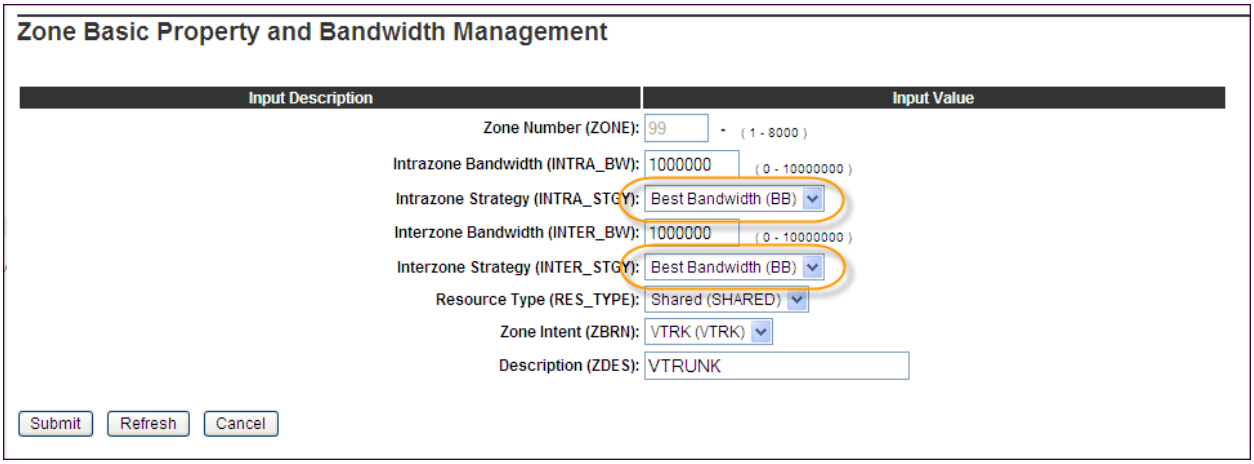
Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured as shown below. In production environments, it is likely that more zones will be required. Select the zone associated with the virtual trunk to the NRS and click **Edit** as shown below. In the sample configuration, this is Zone number **99**.



In the resultant screen shown below, select **Zone Basic Property and Bandwidth Management**.

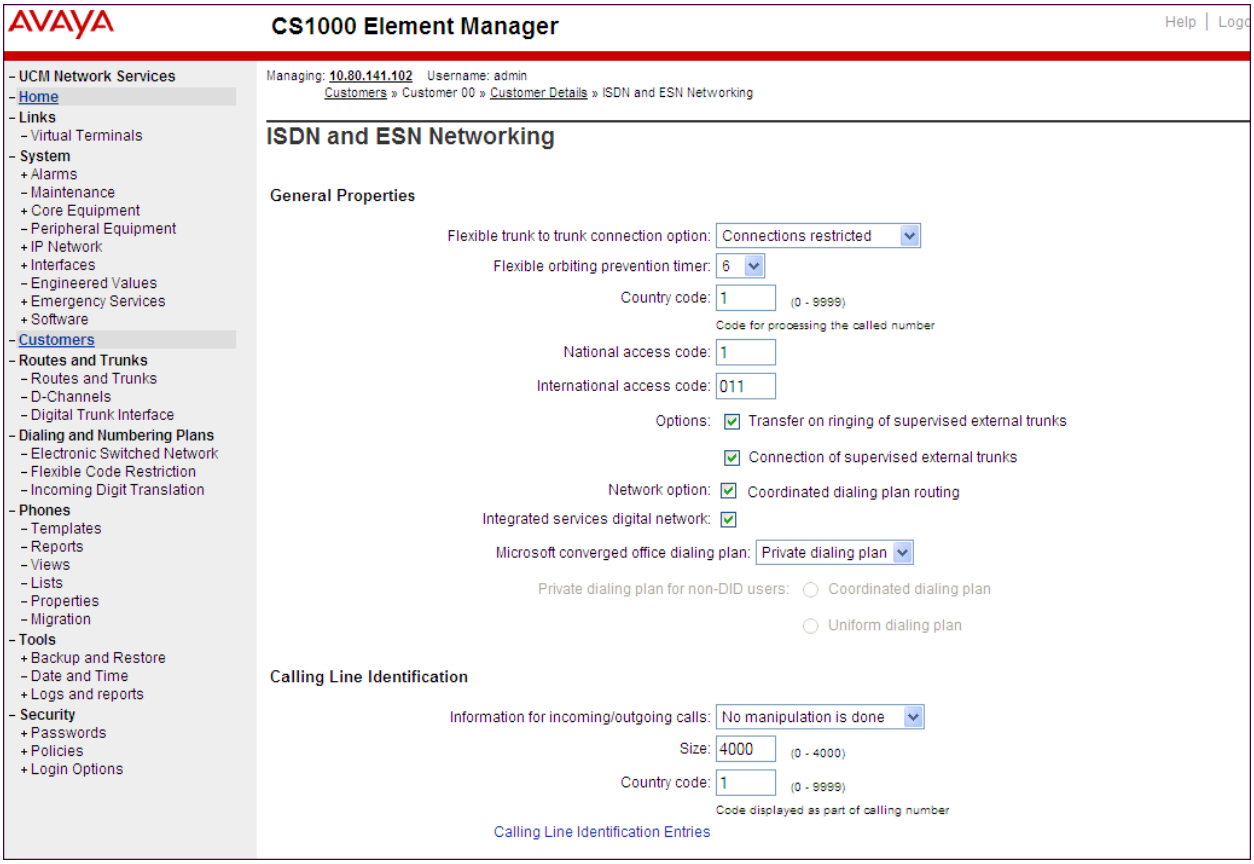


The following screen shows the Zone 99 configuration. Note that **Best Bandwidth (BB)** is selected for the zone strategy parameters so that codec G.729A is preferred over codec G.711MU for calls with CenturyLink SIP Trunk.

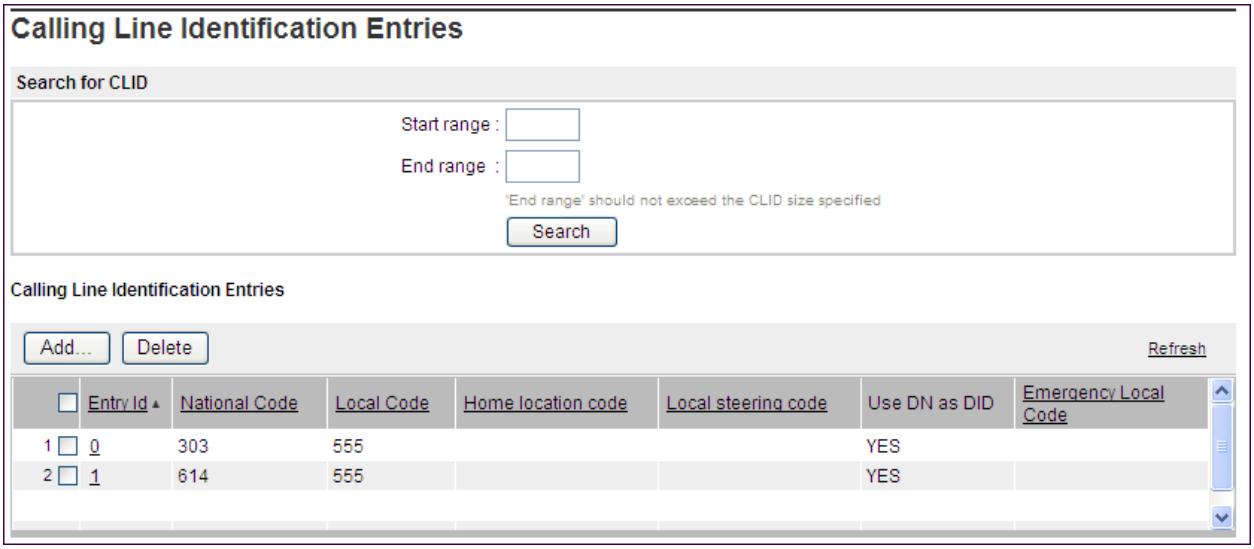


5.7. Customer Information and Calling Line Identification

This section documents basic configuration relevant to the sample configuration. Select **Customers** from the left panel menu, click on the appropriate **Customer Number** and select **ISDN and ESN Networking (not shown)**. The following screen shows the **General Properties** used in the sample configuration.



Click the **Calling Line Identification Entries** link as show above, and search for **the Calling Line Identification Entries** by **Entry ID**. As shown below, the **Use DN as DID** parameter was set to **YES** for the **Entry ID 0** and **1** used in the sample configuration.

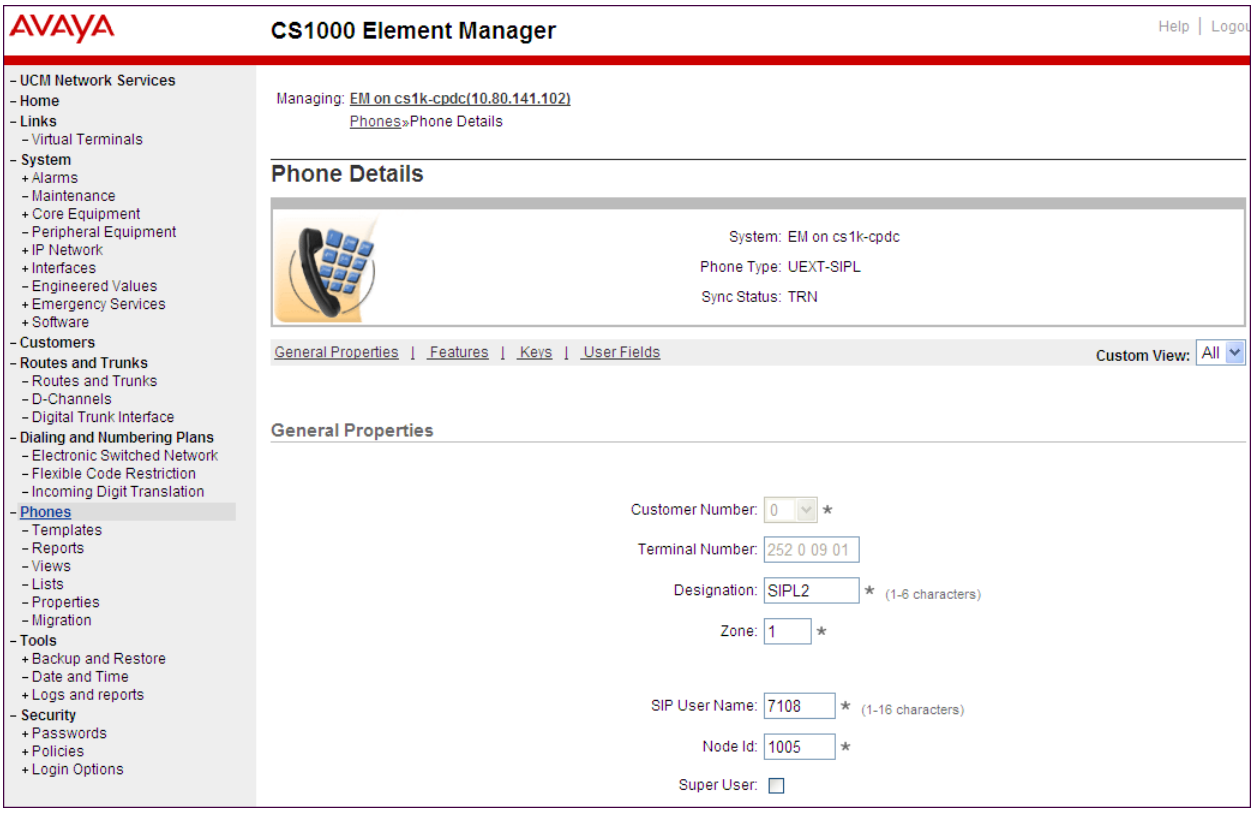


5.8. Example CS1000E Telephone Users

This section is not intended to be prescriptive, but simply illustrates a sampling of the telephone users in the sample configuration.

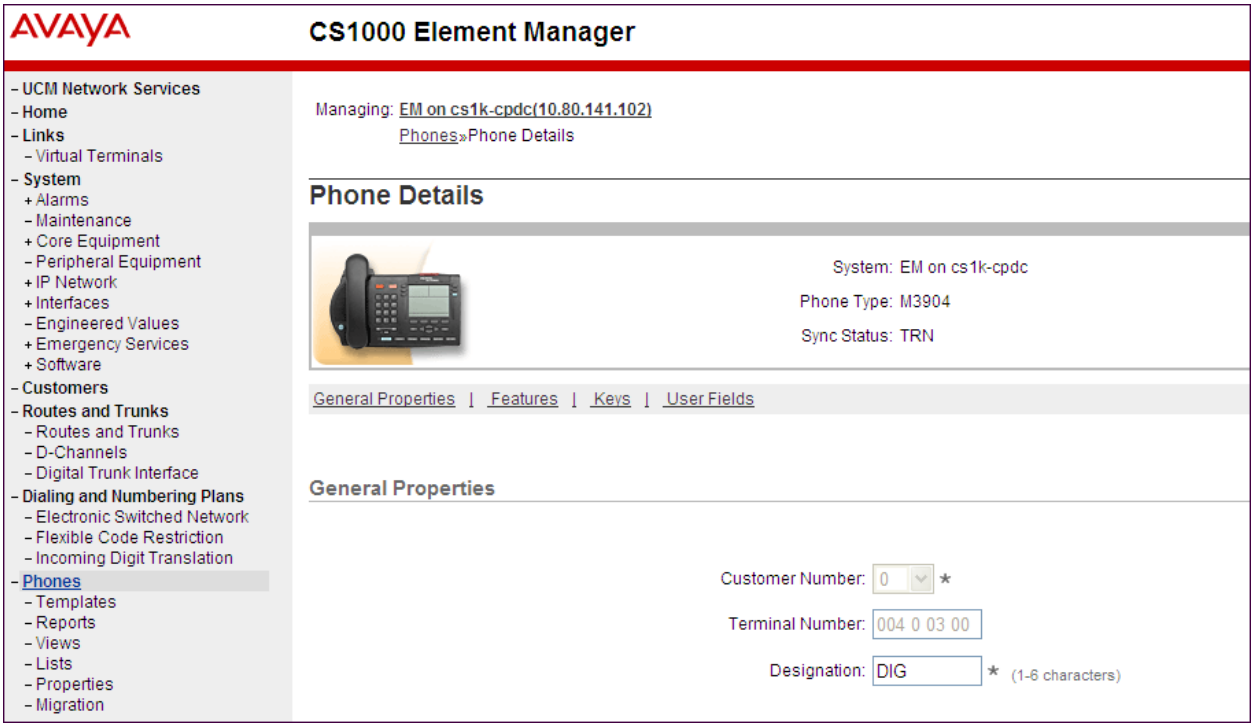
5.8.1. Example SIP Phone DN 7108, Codec Considerations

The following screen shows basic information for a SIP phone in the configuration. The telephone is configured as Directory Number 7108. Note that the telephone is in Zone 1 and is associated with Node 1005 (see **Section 5.1**). A call between this telephone and another telephone in Zone 1 will use a **best quality** strategy (see **Section 5.6**) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the CenturyLink SIP Trunk, the call would use a **best bandwidth** strategy, and the call would use G.729A.

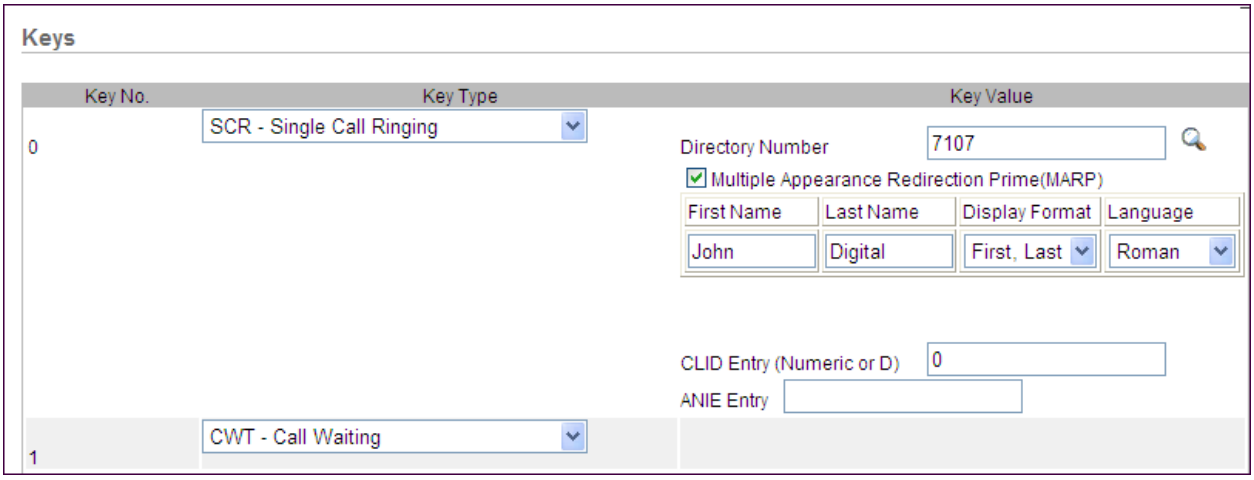


5.8.2. Example Digital Phone DN 7107 with Call Waiting

The following screen shows basic information for a digital phone in the configuration. The telephone is configured as Directory Number 7107.

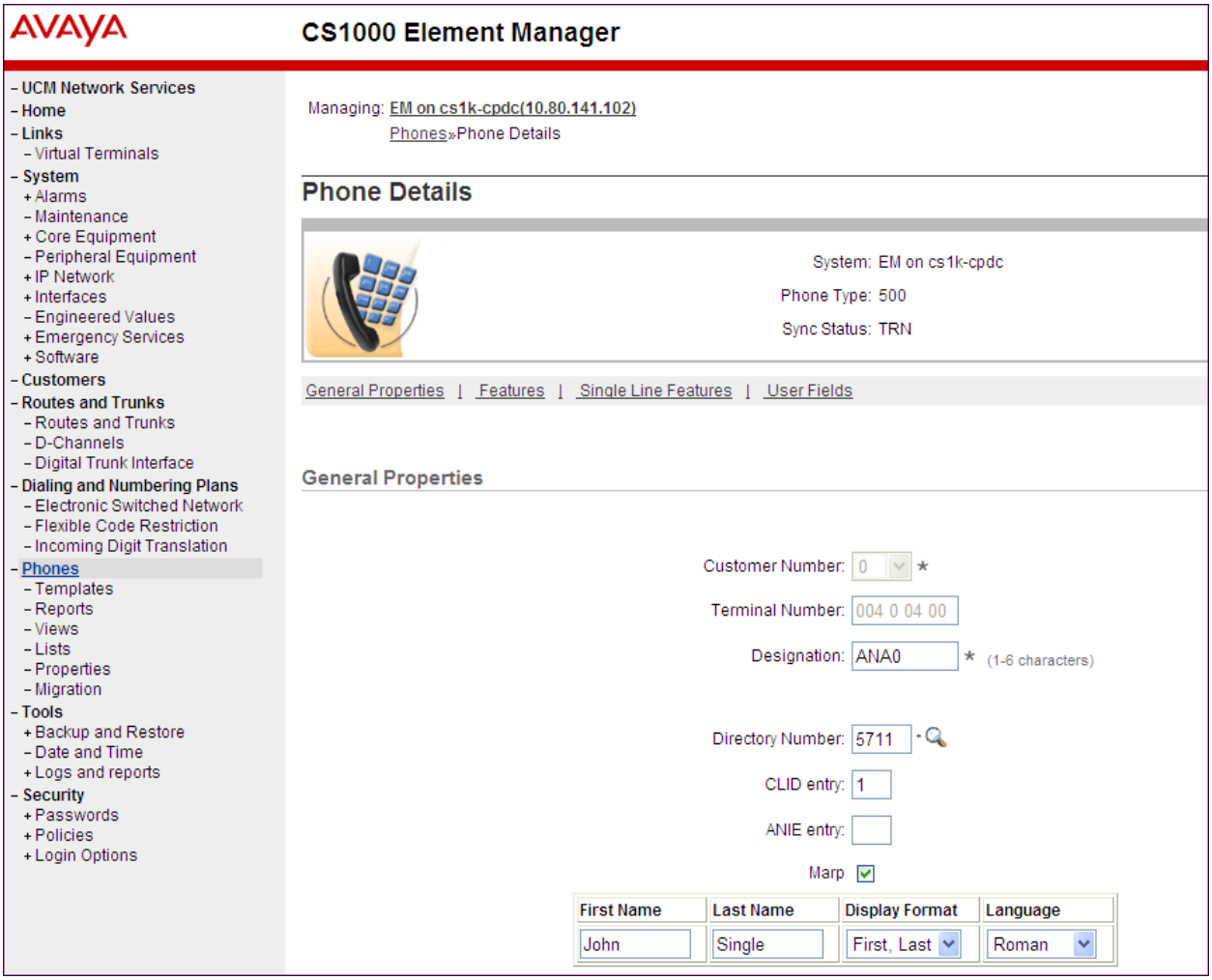


The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone, and uses **CLID Entry 0** (see **Section 5.7**). Although not shown in detail below, to use call waiting with tone, assign a key **CWT – Call Waiting**, set the feature **SWA – Call waiting from a Station** to **Allowed**, and set the feature **WTA – Warning Tone** to **Allowed**.



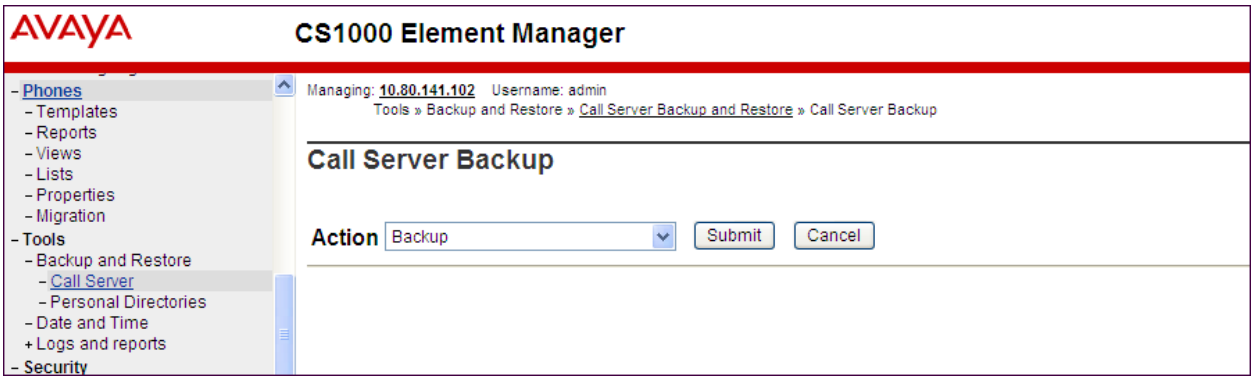
5.8.3. Example Analog Port with DN 5711, Fax

The following screen shows basic information for an analog port in the configuration that may be used with a telephone or fax machine and uses CLID Entry 1 (see **Section 5.7**). The port is configured as Directory Number 5711.



5.9. Save Configuration

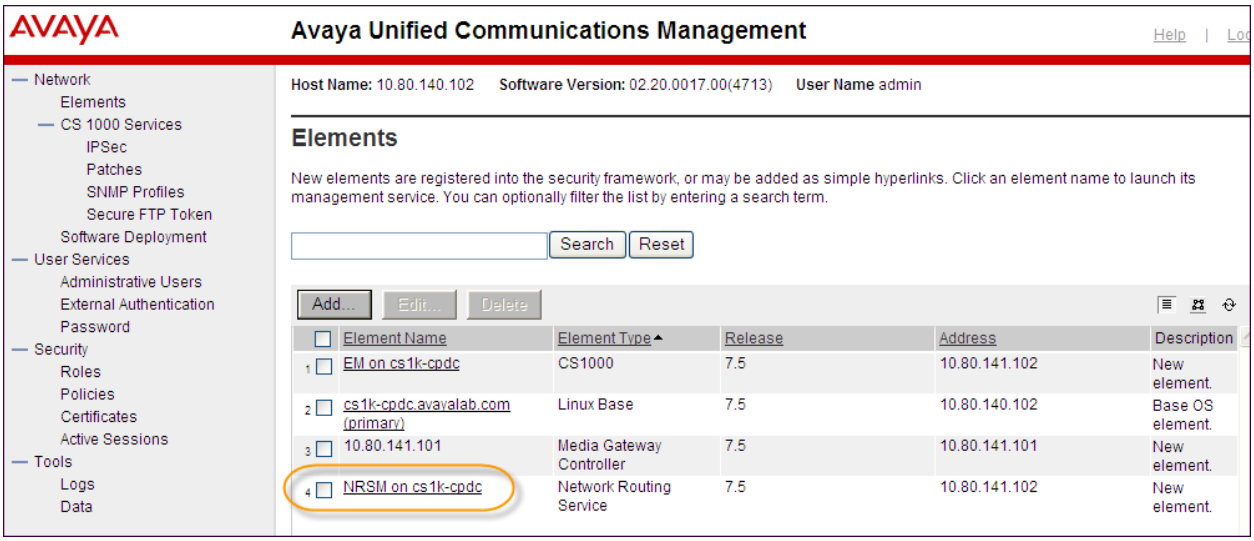
Expand **Tools → Backup and Restore** on the left panel and select **Call Server**. Select Backup (not shown) and click **Submit** to save configuration changes as shown below.



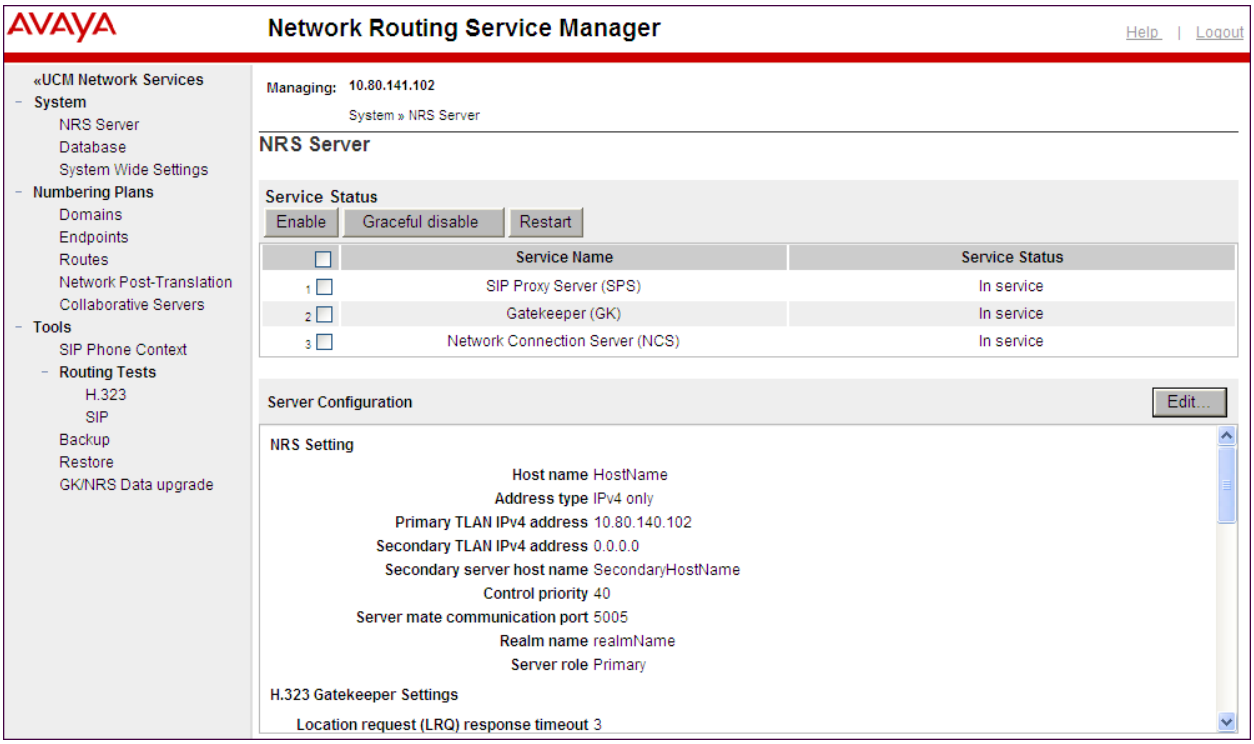
5.10. Network Routing Service Configuration

In this section, it shows how to configure a Network Routing Service (NRS) on Communication Server 1000E. Follow the steps below to setup the NRS server. It is assumed that the NRS has been deployed on the Communication Server 1000 Unified Communications Management (UCM) environment with all latest Service Pack applied.

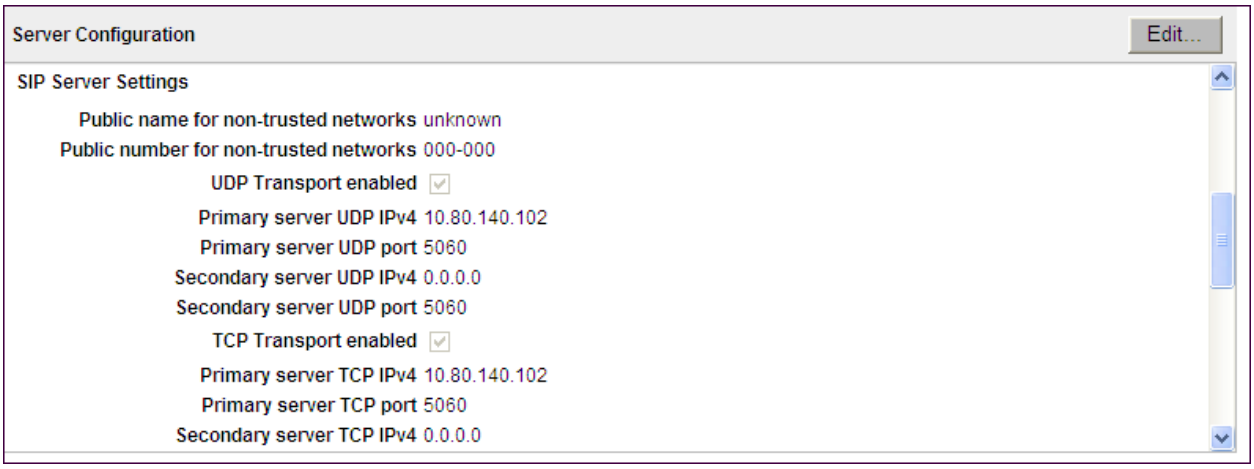
The Avaya Unified Communications Management Elements page will be used for configuration. Click on the Element Name corresponding to **Network Routing Service** in the Element Type column. In the abridged screen below, the user would click on the Element Name **NRSM on cs1k-cpdc**.



The **NRS Server** screen is displayed with additional details as shown below. Under the **Server Configuration** heading, make a note of the **Primary TLAN IPV4 address**. In the sample screen below, the **IPV4 address** is **10.80.140.102**. This IP address will be needed when configuring the Avaya SBCE with a Route Profile to the CS1000E NRS in **Section 6.1.1** and the Server Configuration for the CS1000E NRS in **Section 6.1.5.1**.

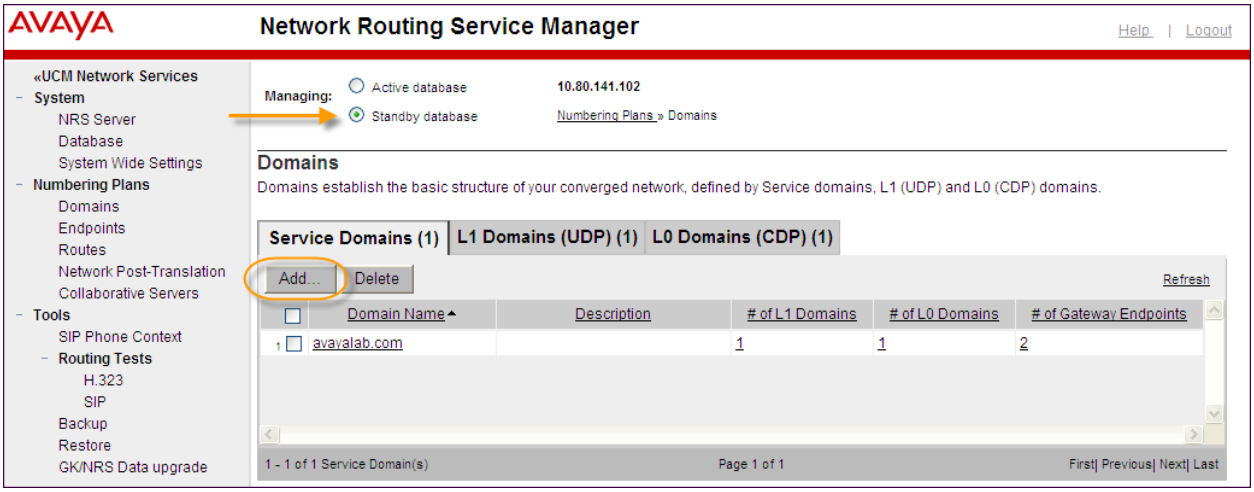


Scroll down and verify the **SIP Server Settings**. The **Primary server UDP port** and **Primary server TCP port** settings should match the ports entered in the SIP Gateway in **Section 5.1.5**.

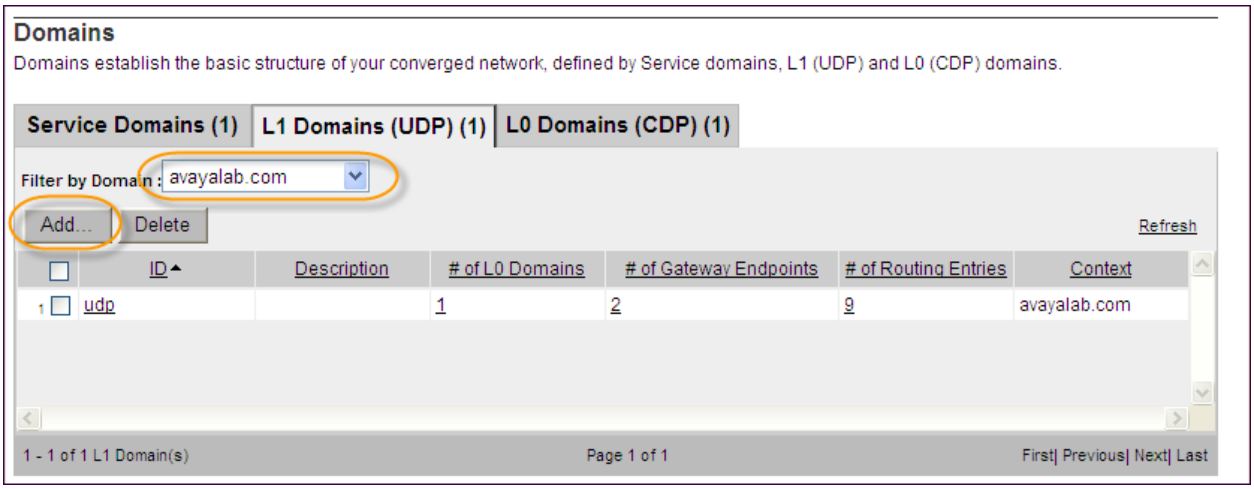


5.10.1. Domains

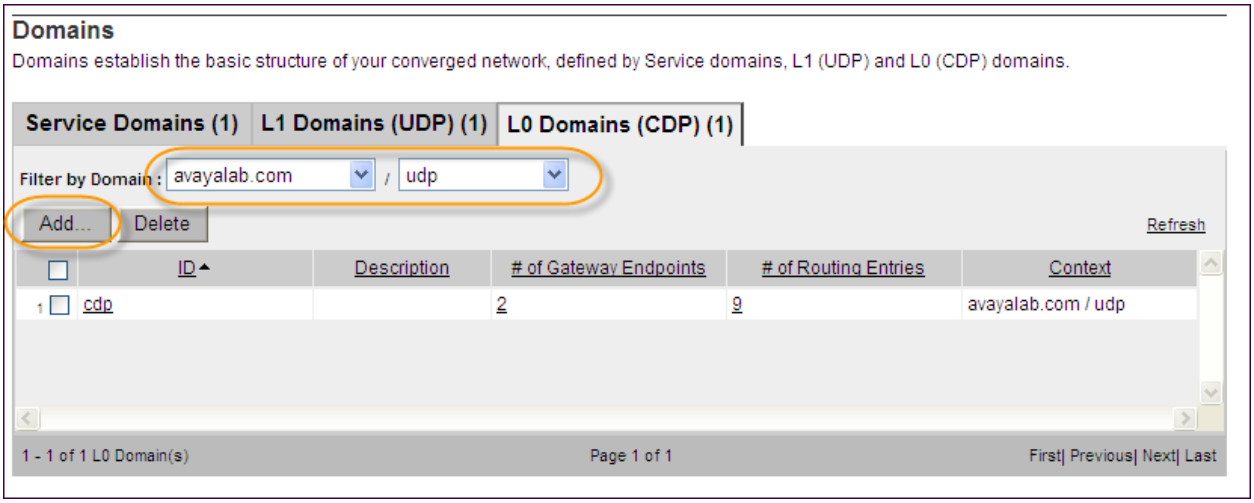
Create a SIP domain for each domain for which the NRS will need to be aware of in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**). Expand **Numbering Plans** on the left panel and select **Domains**. Click on the radio button of the **Standby database**. Then with the **Service Domains (1)** tab selected, click on the **Add** button. In the sample screen below, the domain name is **avayalab.com**.



Select the **L1 Domains (UDP) (1)** tab, and in the **Filter by Domain** select the newly created domain. Click on the **Add** button and enter **udp** as the L1 Domain name as shown below.

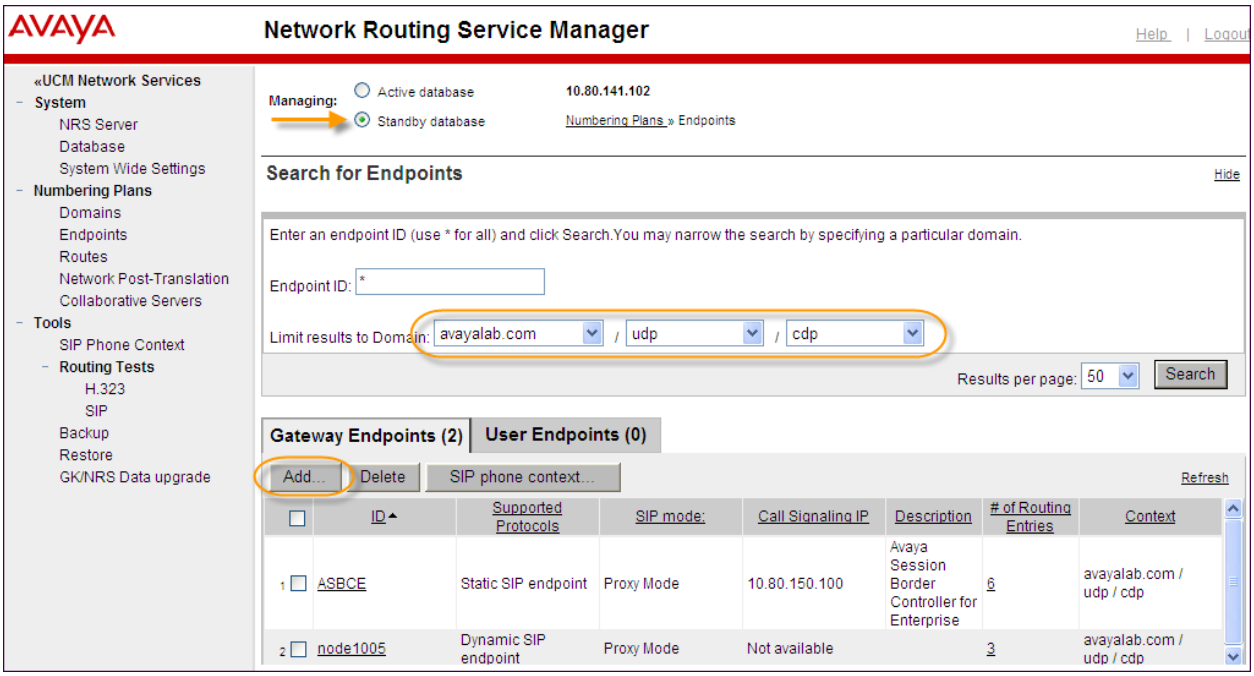


Select the **L0 Domains (CDP) (1)** tab and in the **Filter by Domain**, select the newly created domain and the newly created L1 domain. Click on the **Add** button and enter **cdp** as the L0 Domain name as shown below.



5.10.2. Endpoint for the SIP Signaling Gateway

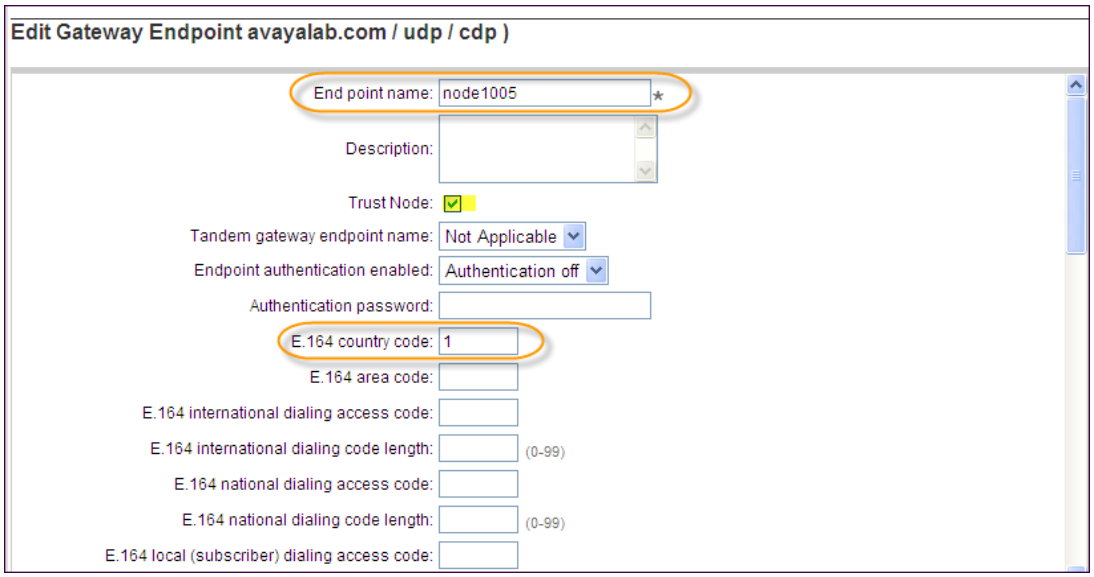
An Endpoint must be added for the CS1000E SIP Signaling Gateway and for the Avaya SBCE. Create a dynamic gateway endpoint for the CS1000E SIP Signaling Gateway. Expand **Numbering Plans** on the left panel and select **Endpoints**. Verify the **Standby database** radio button is still selected. Select the newly created domains in the **Limit results to Domain** section and click the **Add** button as shown below.

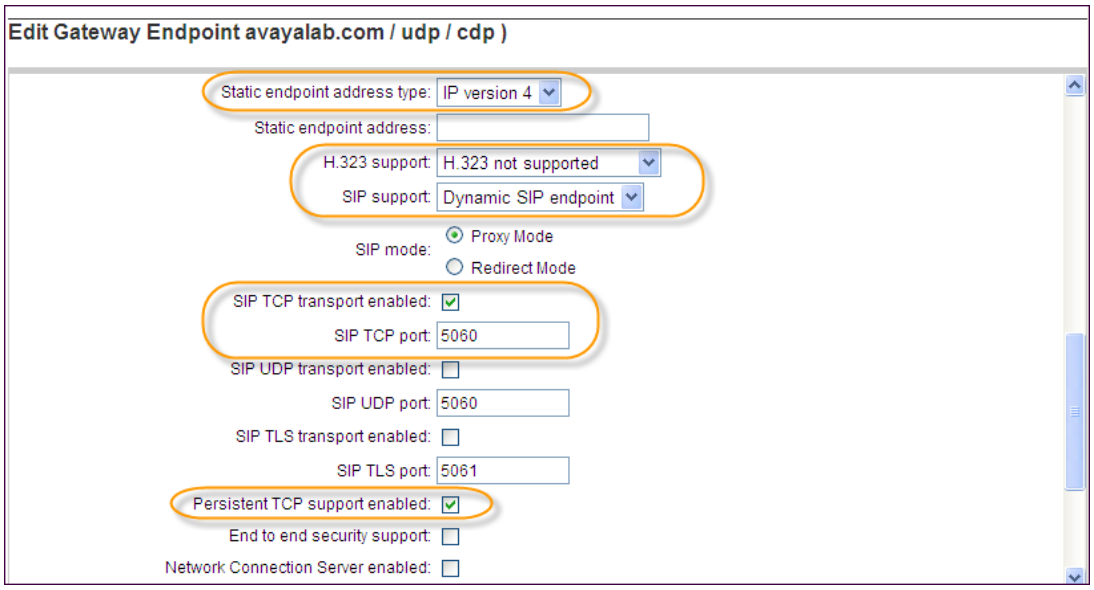


In the detail gateway endpoint configuration page that appears, enter the following values. Use default values for all remaining fields:

- **End point name:** Enter a descriptive name. This must match the name defined for the **Gateway endpoint name** in **Section 5.1.5**.
- **Trust Node:** Checked
- **E.164 country code**: Enter the proper country code.
- **Static endpoint address type**: Select **IP version 4**.
- **H.323 support**: Select **H.323 not supported**.
- **SIP Support**: Select **Dynamic SIP endpoint**.
- **SIP TCP transport enabled**: Checked.
- **SIP TCP port**: **5060**
- **Persistent TCP support enabled**: Checked.

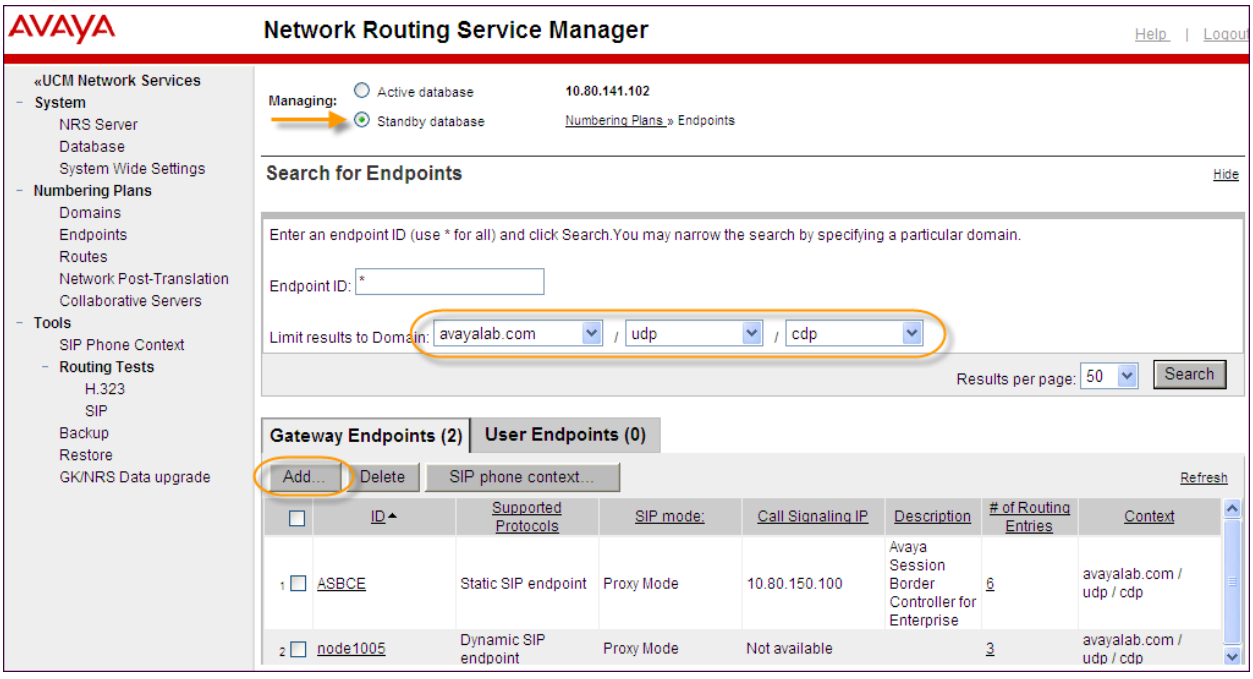
Click **Save** to continue (not shown).





5.10.3. Endpoint for Avaya Session Border Controller for Enterprise

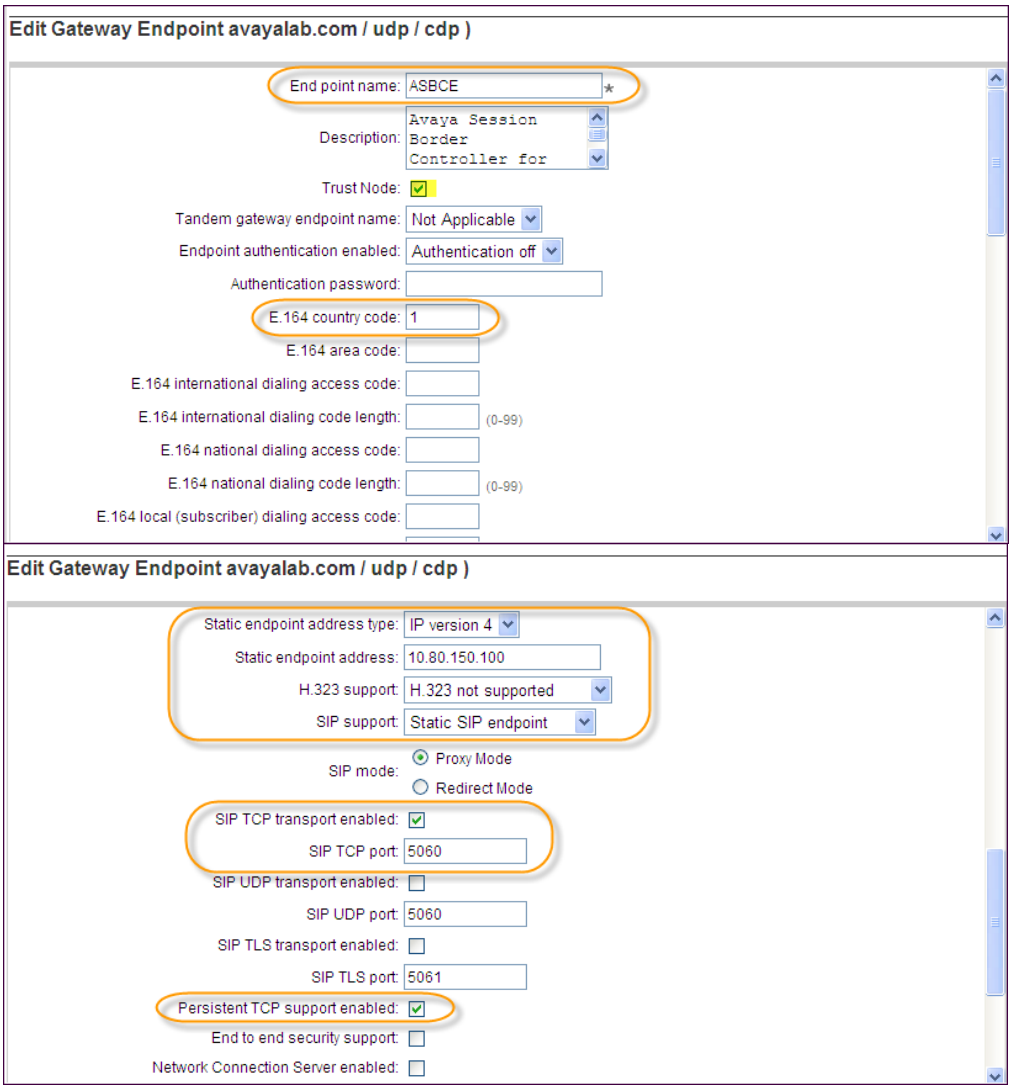
Create a static gateway endpoint for the Avaya Session Border Controller for Enterprise. Expand **Numbering Plan** on the left panel and select **Endpoints**. Verify the **Standby database** radio button is still selected. Select the newly created domains in the **Limit results to Domain** section and click the **Add** button as shown below.



In the detail gateway endpoint configuration page that appears, enter the following values. Use default values for all remaining fields:

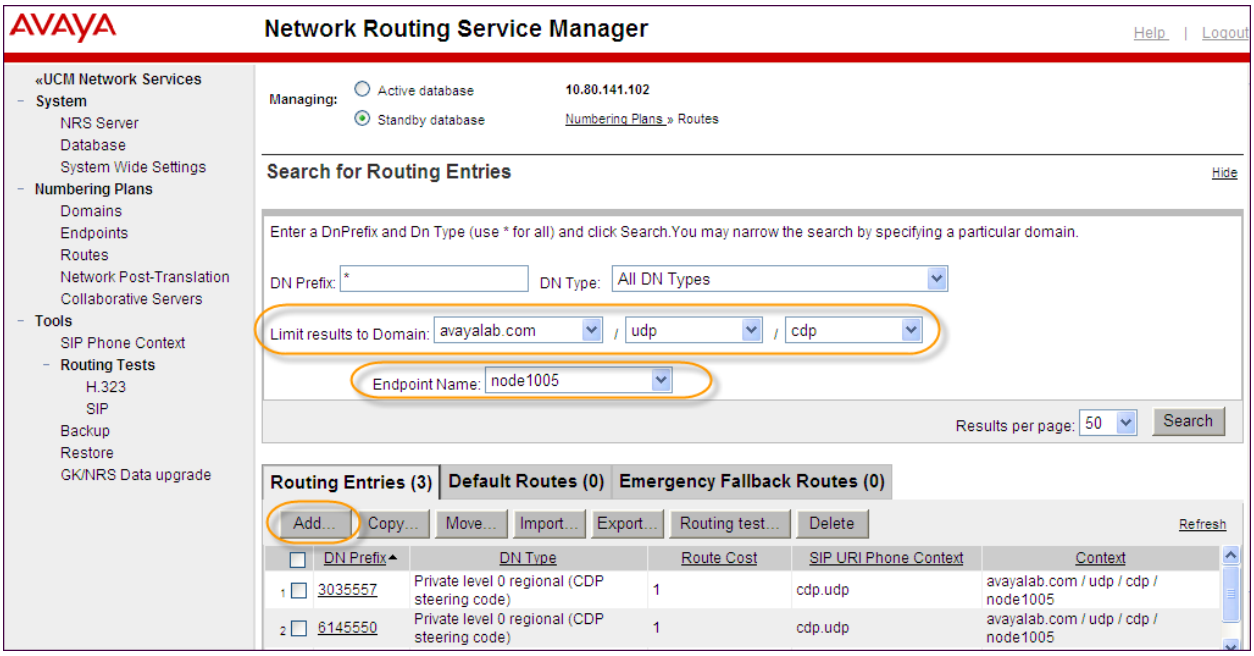
- **End point name:** Enter a descriptive name.
- **Trust Node:** Checked.
- **E.164 country code**: Enter the proper country code.
- **Static endpoint address type**: Select **IP version 4**.
- **Static endpoint address**: Enter the IP address of the Avaya SBCE inside interface (see **Section 6.3.1**).
- **H.323 support**: Select **H.323 not supported**.
- **SIP Support**: Select **Static SIP endpoint**.
- **SIP TCP transport enabled**: Checked.
- **SIP TCP port**: **5060**.
- **Persistent TCP support enabled**: Checked.

Click **Save** to continue (not shown).



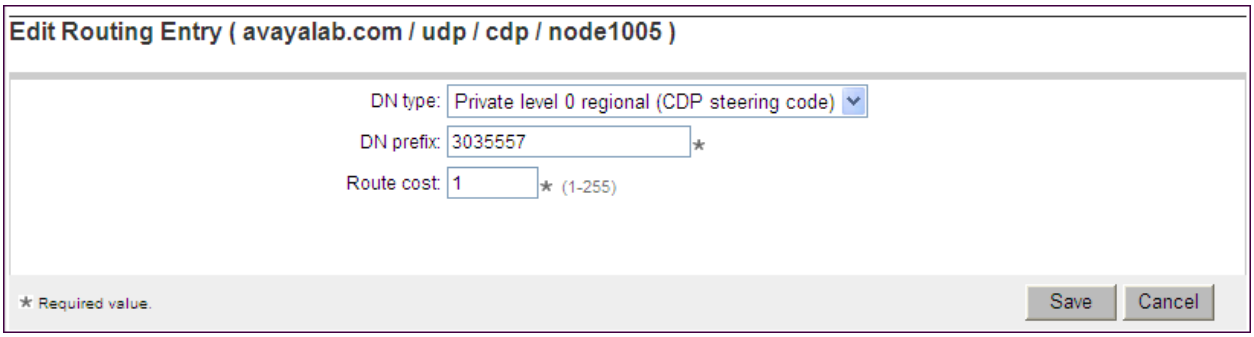
5.10.4. Routing Entry for CS1000E SIP Signaling Gateway

The NRS determines how to route SIP messages based on the information given in the Routing Entries. For compliance testing CenturyLink provided two sets of DID ranges, 303-555-7xxx and 614-555-0xxx. Route Entries **3035557** and **6145550** were created for the CS1000E SIP Signaling Gateway with the **Endpoint Name** of **node1005**. To add a Routing Entry, expand **Numbering Plans** on the left panel and select **Routes**. Select the domain names in the **Limit results to Domain** fields and select the **Endpoint Name** created for the CS100E SIP Signaling Gateway as shown below.



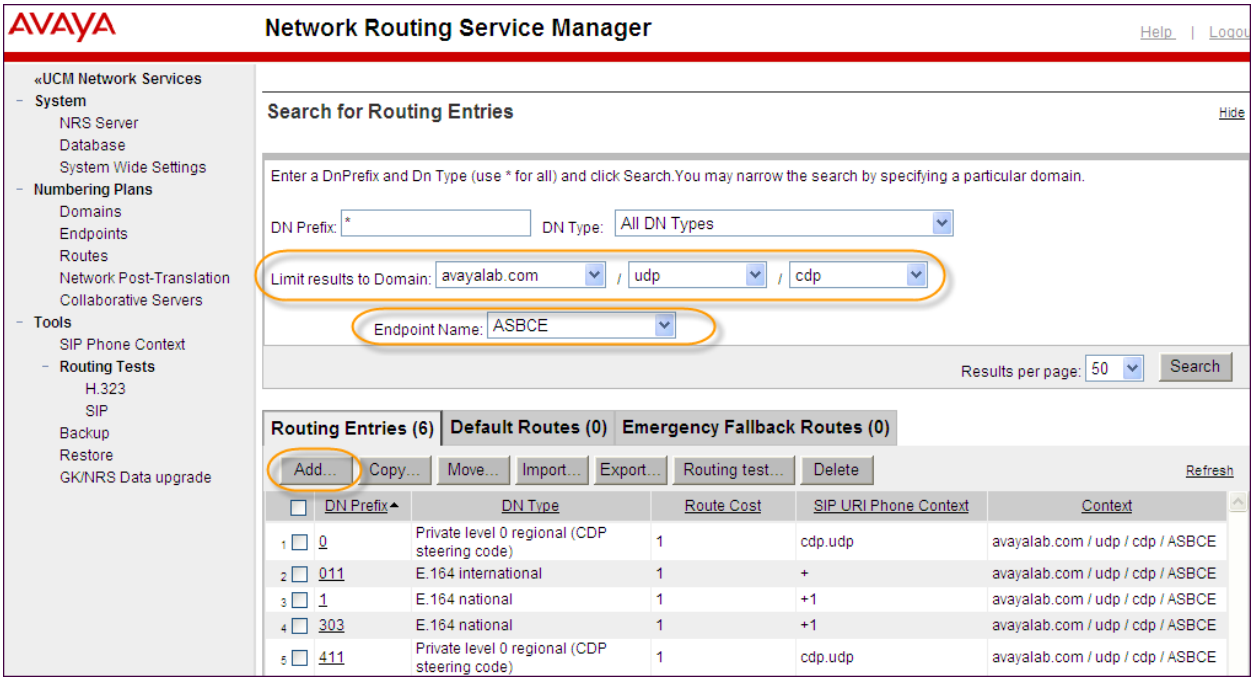
In the Routing Entry configuration page that appears, enter the following values:

- **DN type:** **Private level 0 regional (CDP steering code)**.
- **DN prefix:** Enter a prefix to match (e.g., **3035557**).
- **Route cost**: **1**



5.10.5. Routing Entry for Avaya Session Border Controller for Enterprise

The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks. To add a Routing Entry for Avaya SBCE, expand **Numbering Plans** on the left panel and select **Routes**. Select the domain names in the **Limit results to Domain** fields and select the **Endpoint Name** created for the Avaya SBCE as shown below.

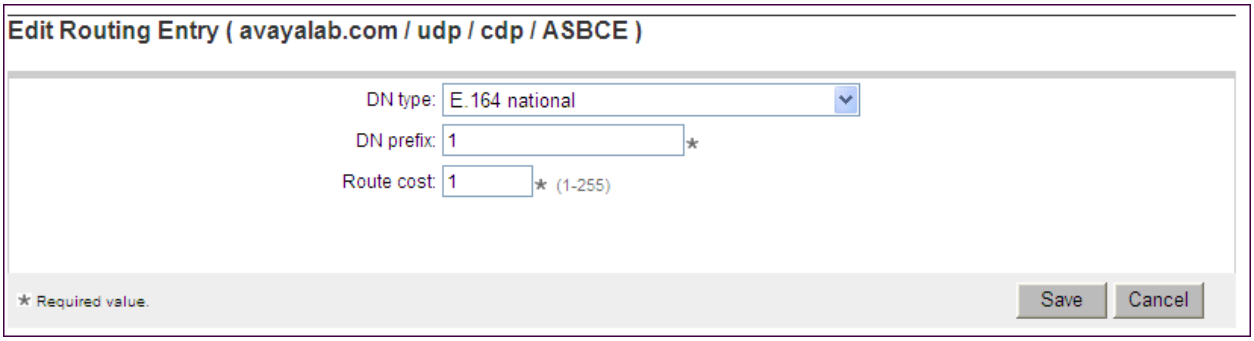


In the Routing Entry configuration page that appears (not shown), enter the following values:

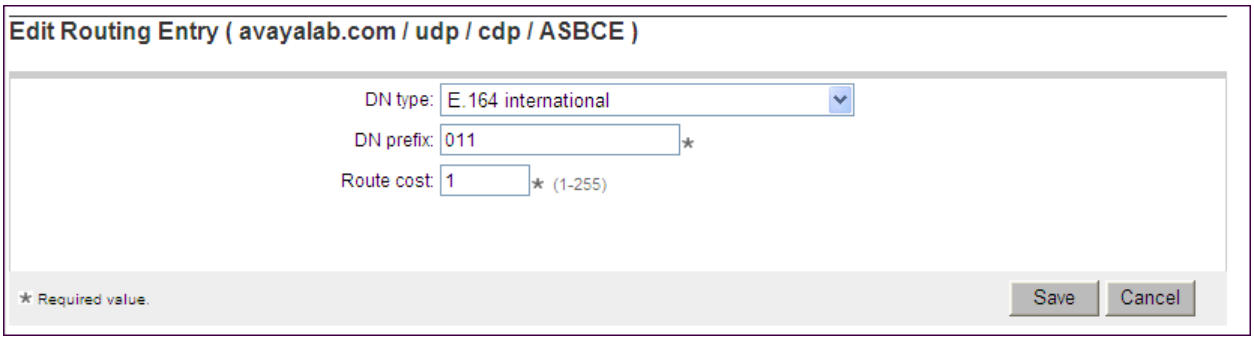
- **DN type:** Select the appropriate entry based on the type of call (see examples below).
- **DN prefix:** Enter a prefix to match (see examples below). The full list of DN prefixes used during the compliance testing is shown in the previous screen.
- **Route cost**: **1**

Click **Save** to continue.

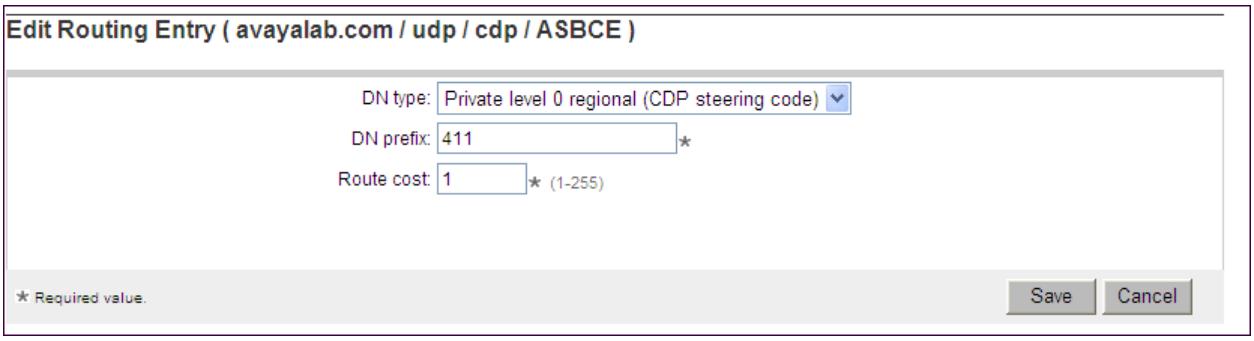
The screen below shows the route entry added for any number that begins with a 1. This represents long distance calls based on the North American Numbering Plan. The **DN type** is set to **E.164 national**.



The screen below shows the route entry added for any number that begins with a 011. This represents international calls based on the North American Numbering Plan. The **DN type** is set to **E.164 international**.

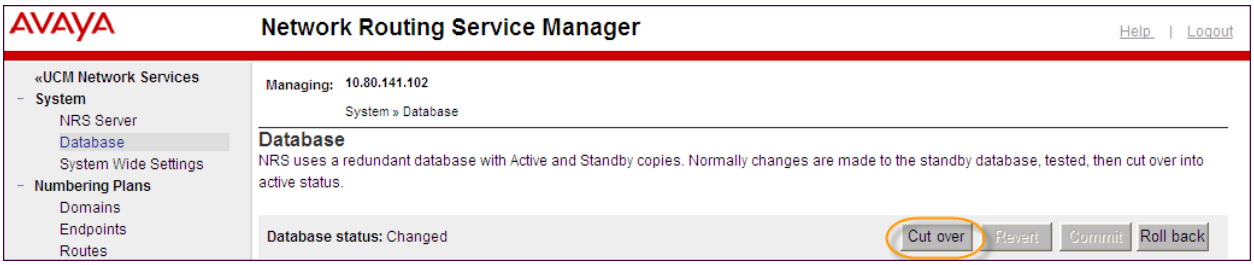


The screen below shows the route entry added for directory assistance. The **DN type** is set to **Private level 0 regional (CDP steering code)**.

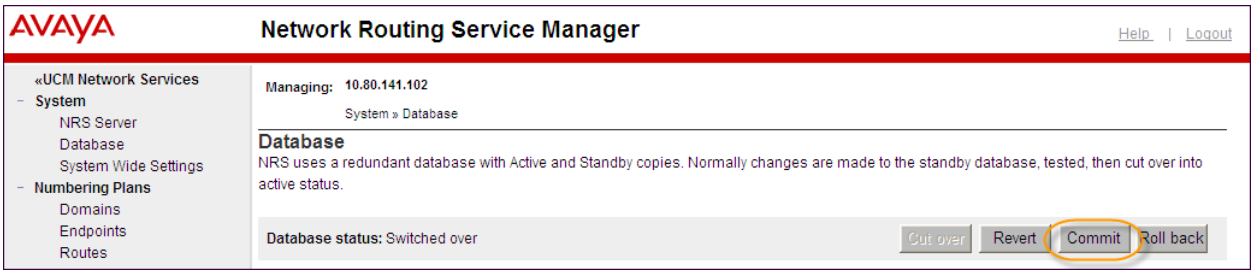


5.10.6. Activate Configuration

All configuration changes thus far have been done on the Standby database. Before the changes will take affect the standby database must be cut over and committed to the active database. Expand **System** on the left panel and select **Database**. Select the **Cut over** button as shown below.



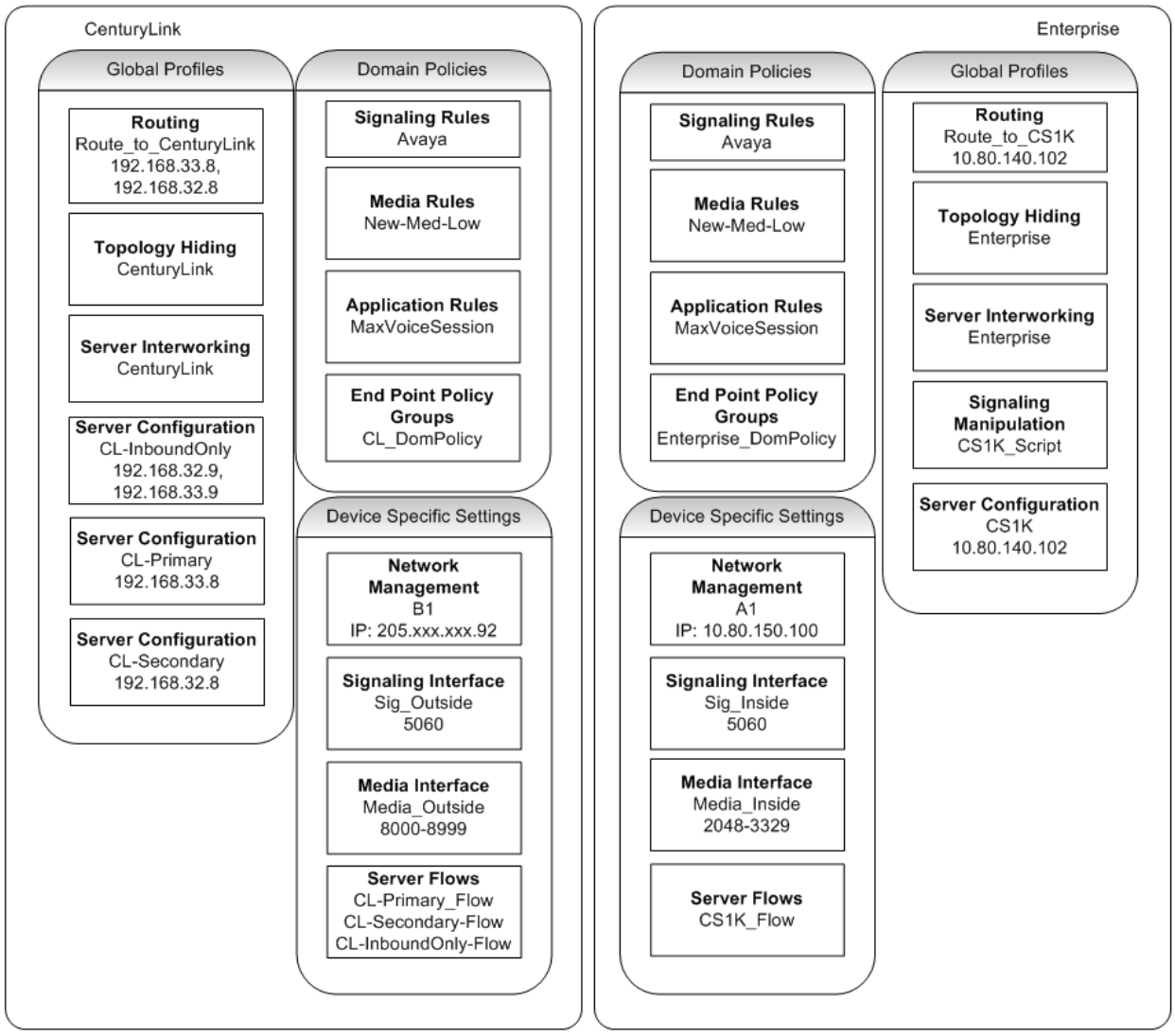
The **Database status** field will update from **Changed** (as shown above) to **Switched over** (as shown below). Click on the **Commit** button to activate the database.



6. Configure Avaya Session Border Controller for Enterprise

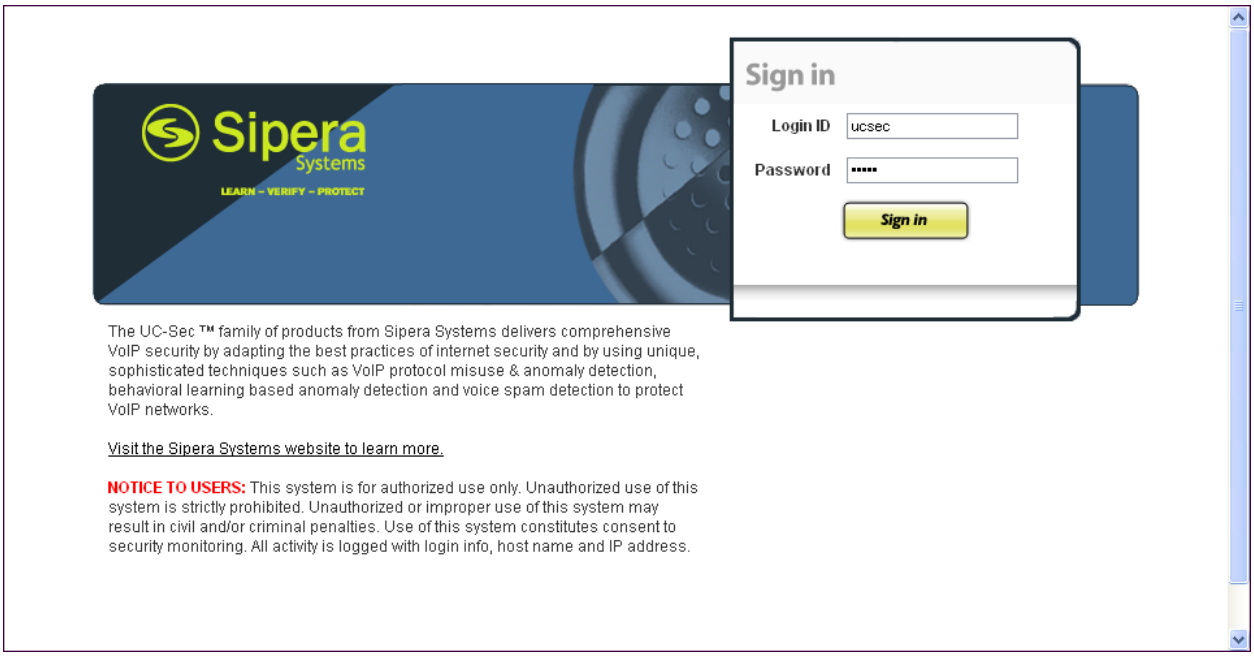
This section covers the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed. For additional information on these configuration tasks, see **Reference** [**8**] and [**9**].

A pictorial view of this configuration is shown below. It shows the components needed for the compliance test. Each of these components is defined in the Avaya SBCE web configuration as described in the following sections.

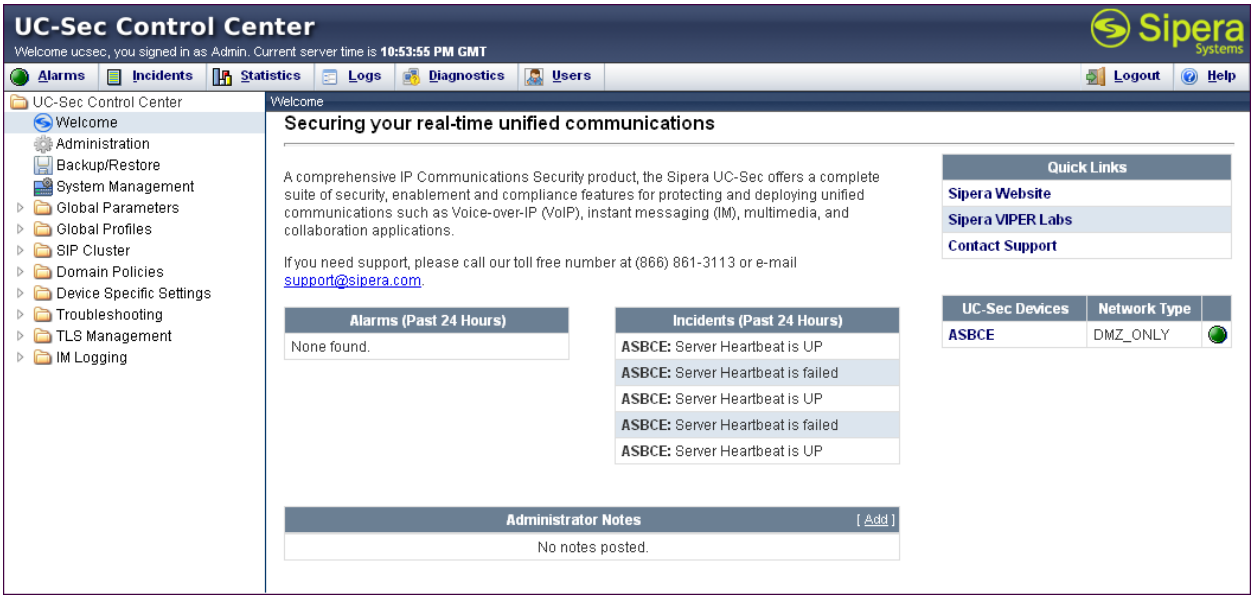


Use a WEB browser to access the Element Management Server (EMS) web interface, and enter https://<ip-addr>/ucsec in the address field of the web browser, where <ip-addr> is the management LAN IP address of the Avaya SBCE.

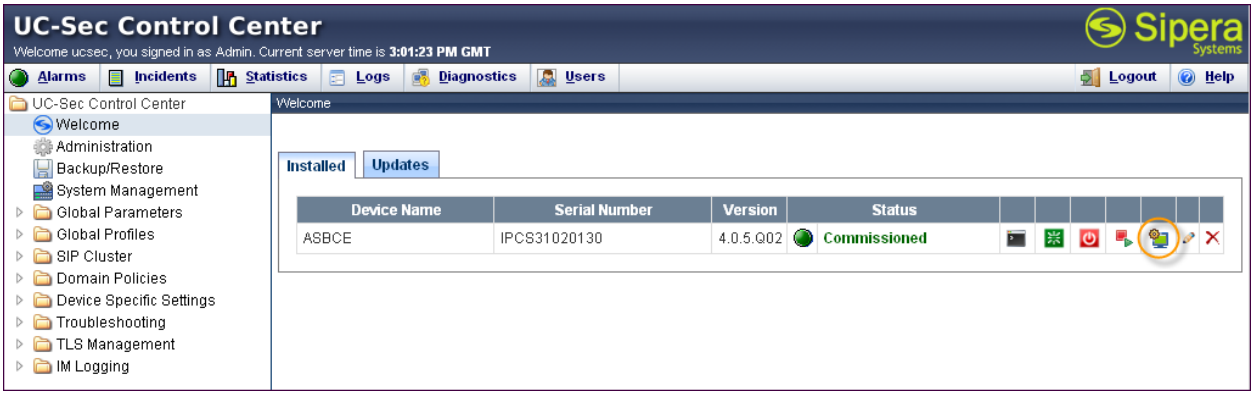
Log in with the appropriate credentials. Click **Sign In**.



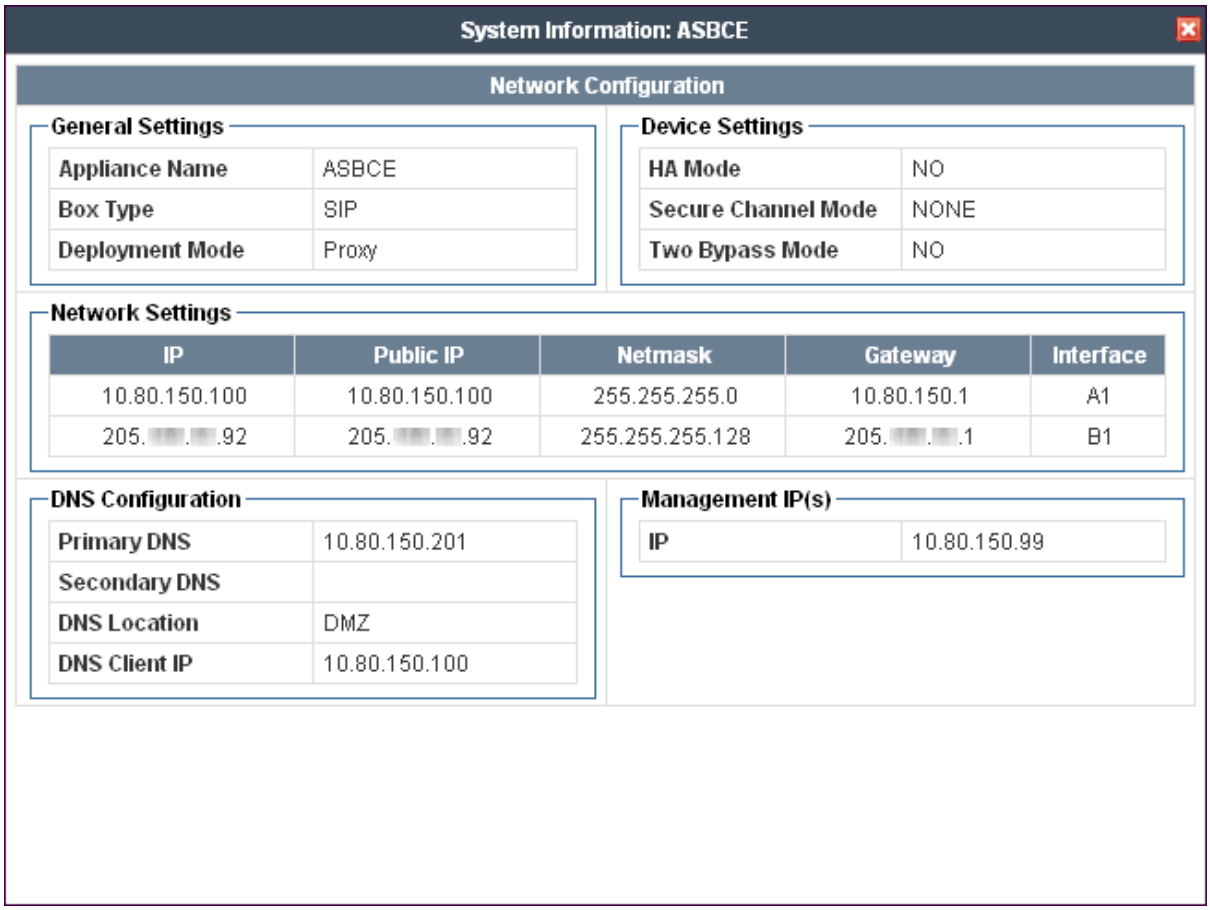
The main page of the UC-Sec Control Center will appear.



To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **ASBCE** is shown. To view the configuration of this device, click the monitor icon as shown below.



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



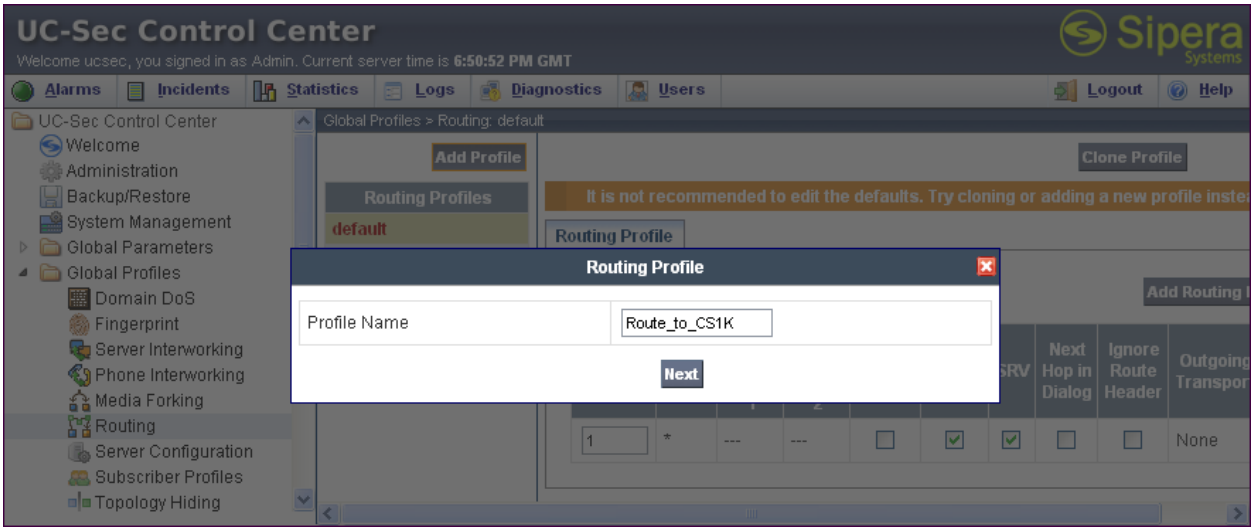
6.1. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.1.1. Routing Profile

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

Create a Routing Profile for the CS1000E and CenturyLink SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.

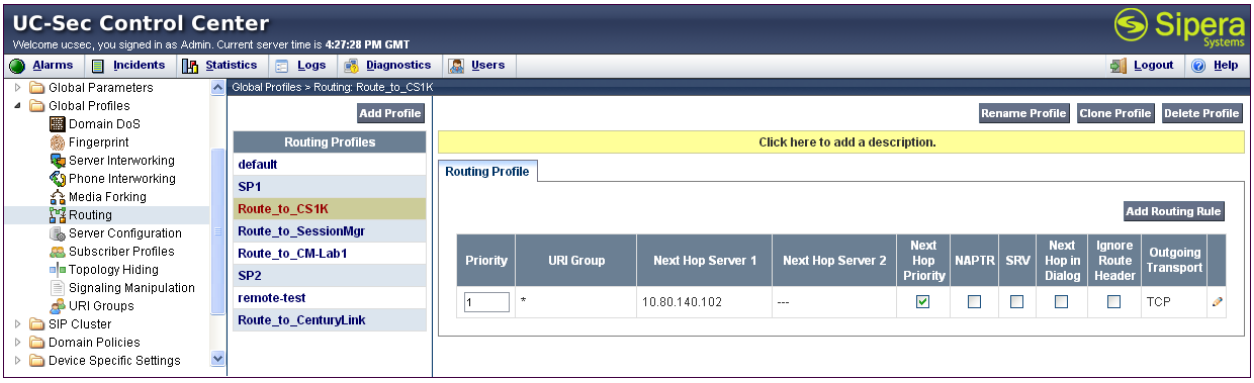


In the new window that appears, enter the following values (not shown). Use default values for all remaining fields:

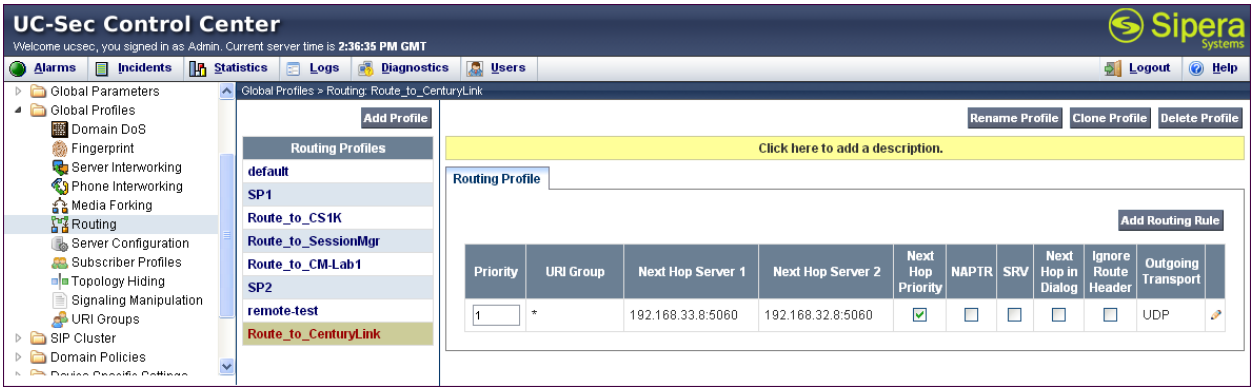
- **URI Group:** Select "*****" from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server**: Checked.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish**.

In the shared test environment the following screen shows the Routing Profile to CS1000E. The **Next Hop Server 1** IP address must match the IP address of the NRS in **Section 5.10**. The Outgoing Transport must match the Avaya SBCE Endpoint created on the NRS in **Section 5.10.3**.



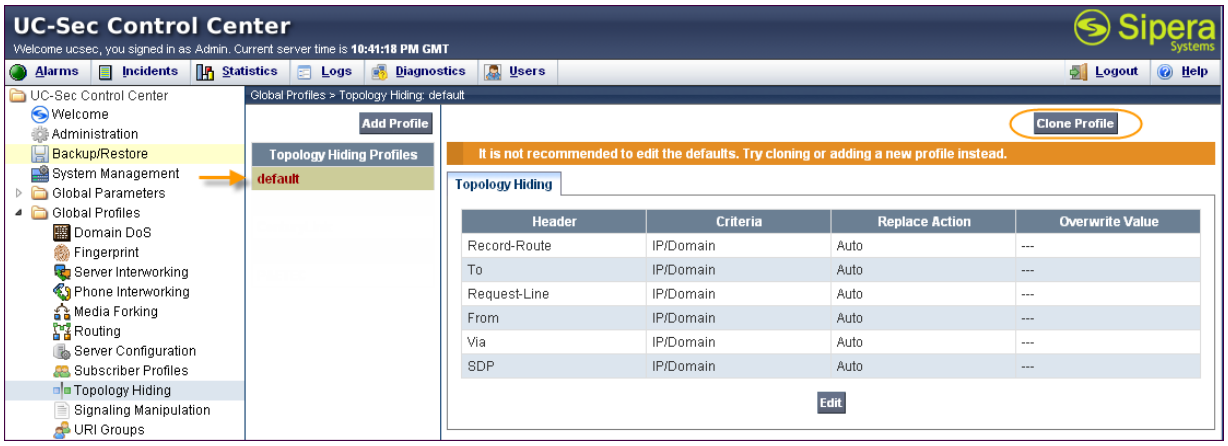
The following screen shows the Routing Profile to CenturyLink. For compliance testing CenturyLink had four SIP servers assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound traffic. Only the two SIP servers allocated for outbound traffic were added to the Routing Profile.



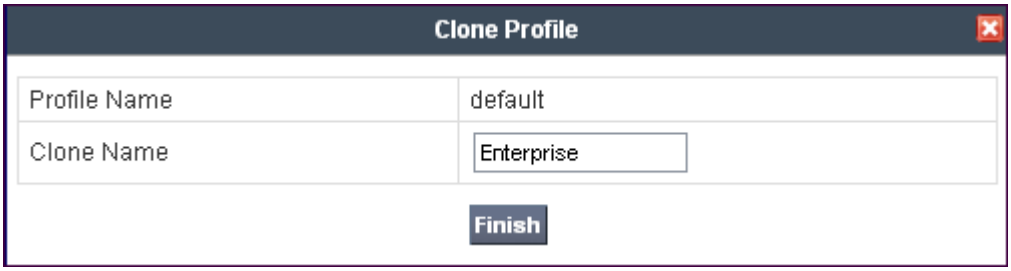
6.1.2. Topology Hiding Profile

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

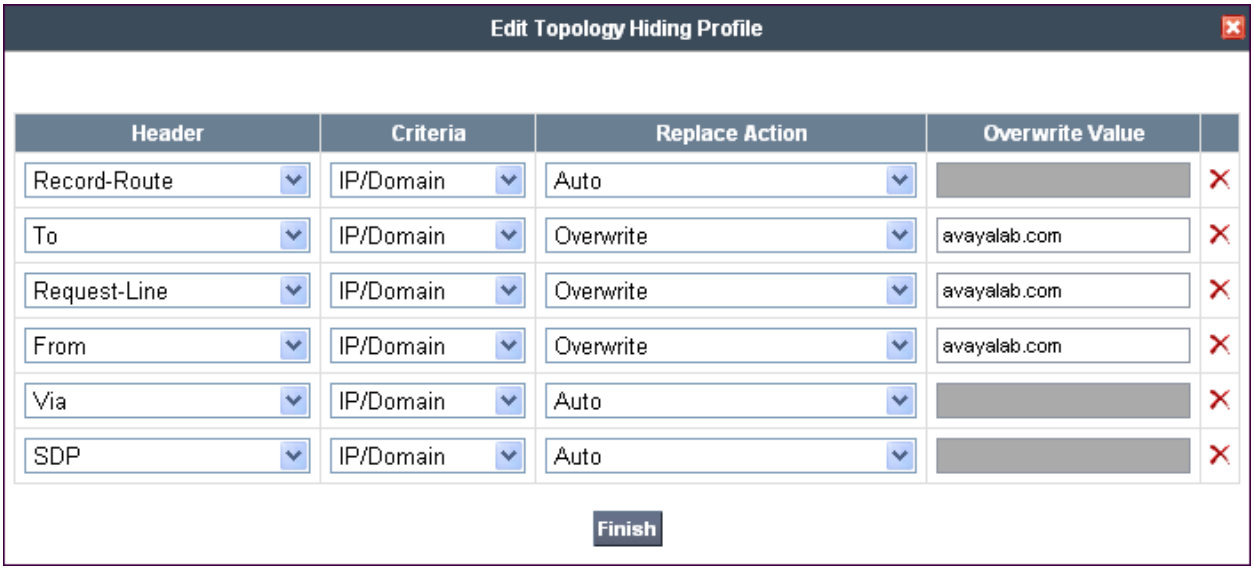
Create a Topology Hiding Profile for the enterprise and CenturyLink SIP Trunk. In the sample configuration, the **Enterprise** and **CenturyLink** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center → Global Profiles → Topology Hiding**. Select the **default** profile and click on **Clone Profile** as shown below.



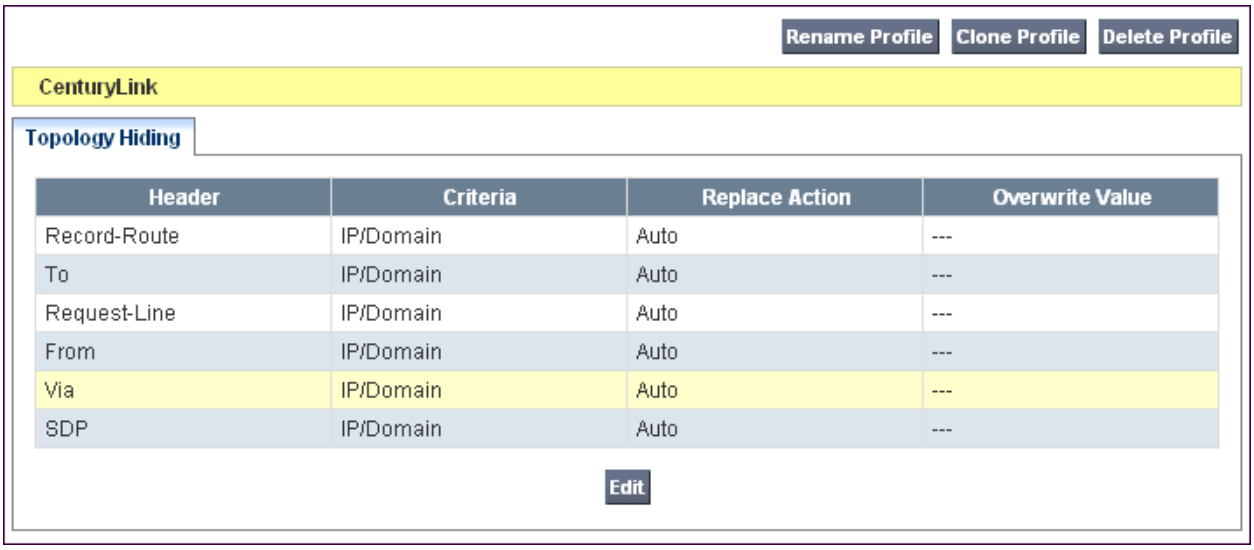
Enter a descriptive name for the new profile and click **Finish**.



Edit the **Enterprise** profile to overwrite the headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in the NRS (**Section 5.10.1**). Click **Finish** to save the changes.



It is not necessary to modify the **CenturyLink** profile from the default values. The following screen shows the Topology Hiding Policy created for CenturyLink.



When creating or editing Topology Hiding Profiles, there are six types of headers available for selection in the Header drop-down list to choose from. In addition to the six headers, there are additional headers not listed that are affected when either of two types of listed headers (e.g., **To Header** and **From Header**) are selected in the **Header** drop-down list. **Table 2** lists the six headers along with all of the other affected headers in three header categories (e.g., **Source Headers**, **Destination Headers**, and **SDP Headers**).

Topology Hiding Headers	
Main Header Names	**Header(s) Affected by Main Header**
Source Headers	
Record-Route	
From	(1) Referred-By (2) P-Asserted Identity
Via	
Destination Headers	
To	(1) ReferTo
Request-Line	
SDP Headers	
Origin Header	

Table 2: Topology Hiding Headers

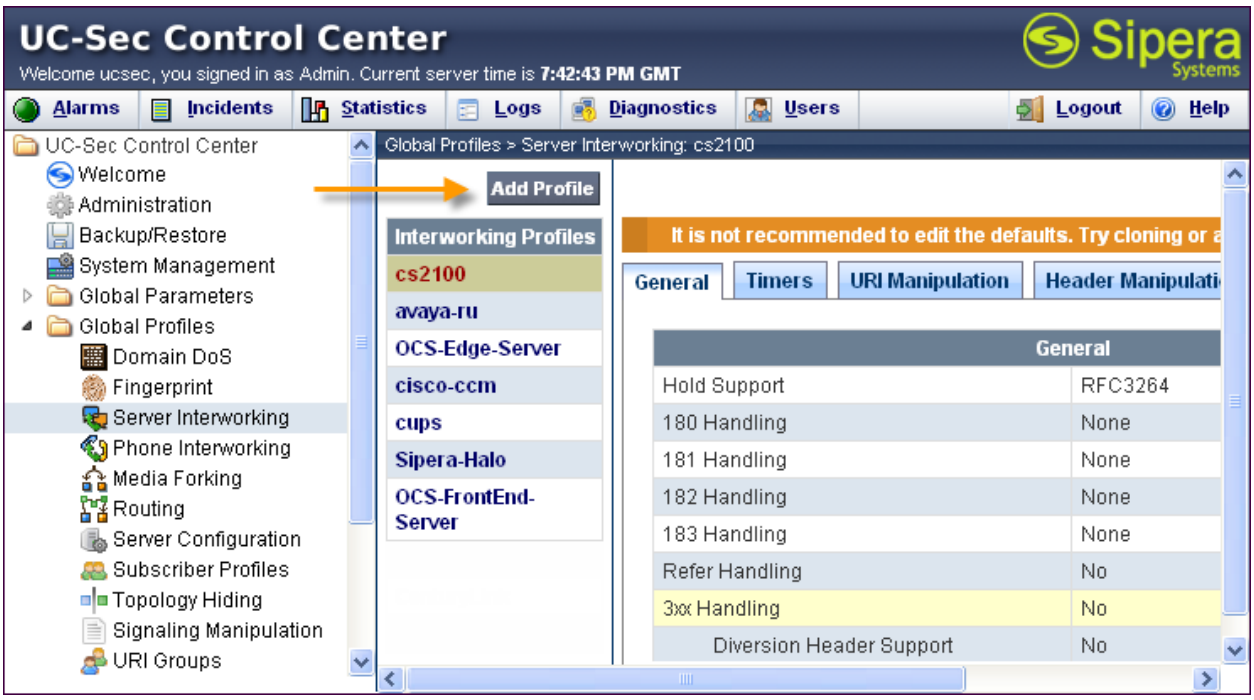
6.1.3. Server Interworking Profile

The Server Internetworking profile configures and manages various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. Interworking Profile features are configured based on different Trunk Servers. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

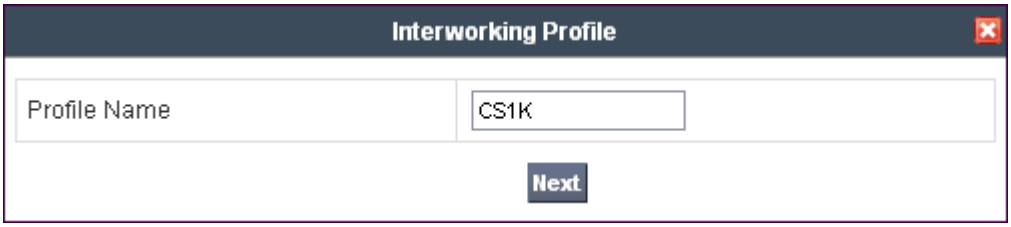
In the sample configuration, separate Server Interworking Profiles were created for **Enterprise** and **CenturyLink**.

6.1.3.1 Server Interworking Profile – Enterprise

To create a new Server Interworking Profile for the enterprise, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on **Add Profile** as shown below.



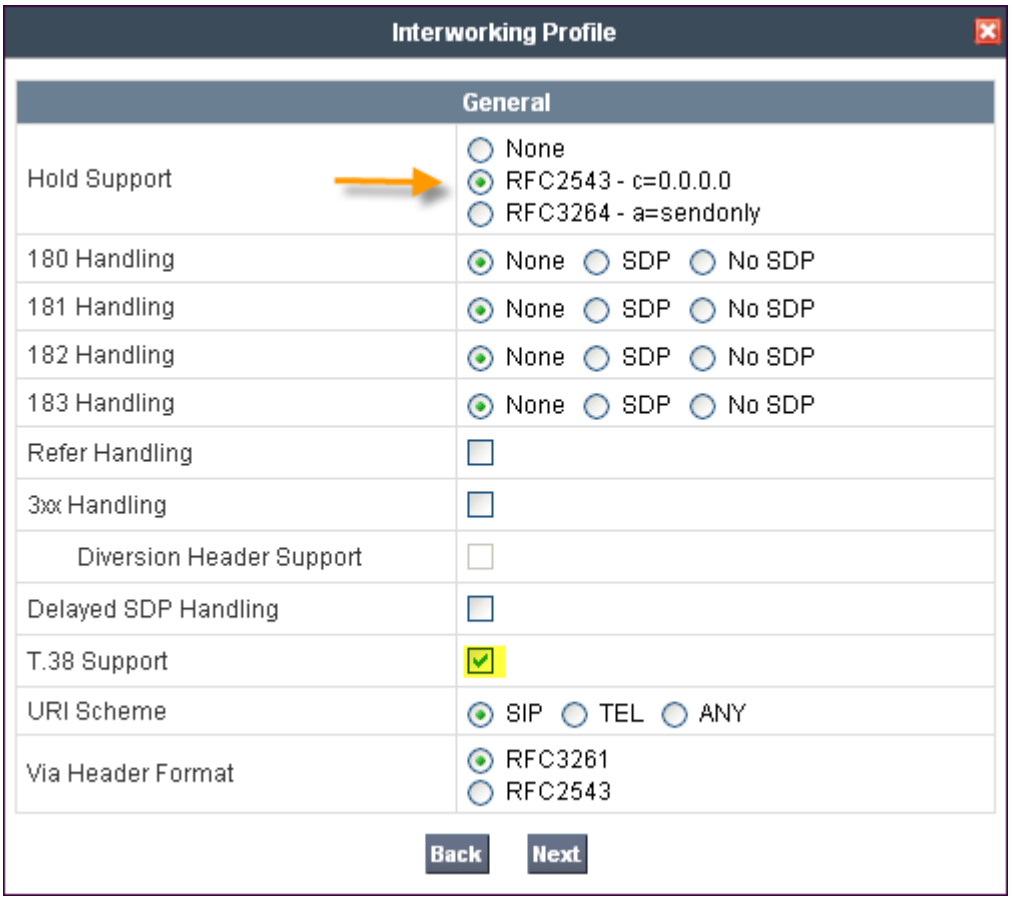
Enter a descriptive name for the new profile and click **Next** to continue.



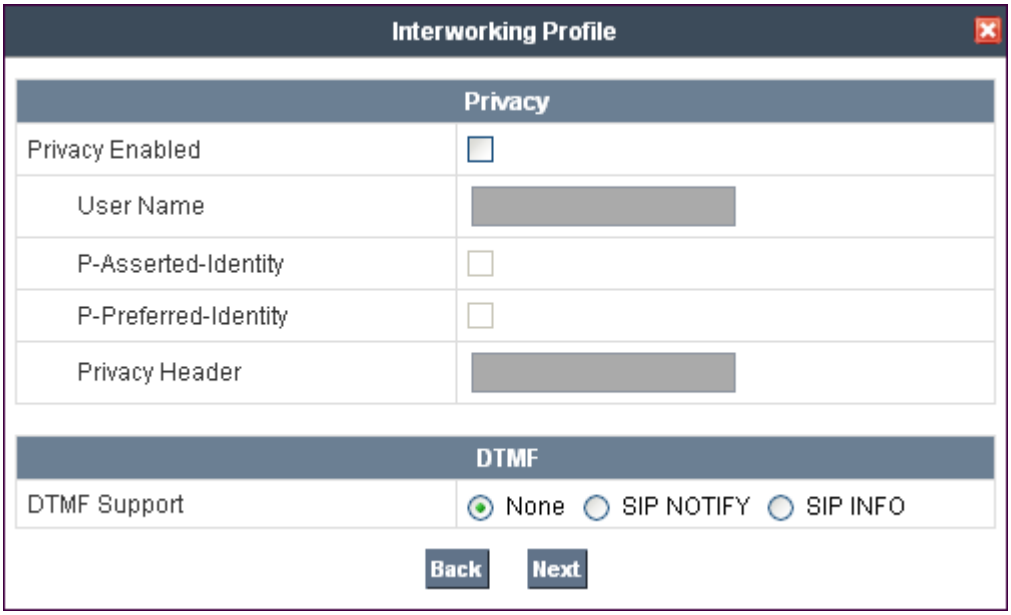
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Hold Support:** Select **RFC2543 - c=0.0.0.0**.
- **T.38 Support:** Checked.

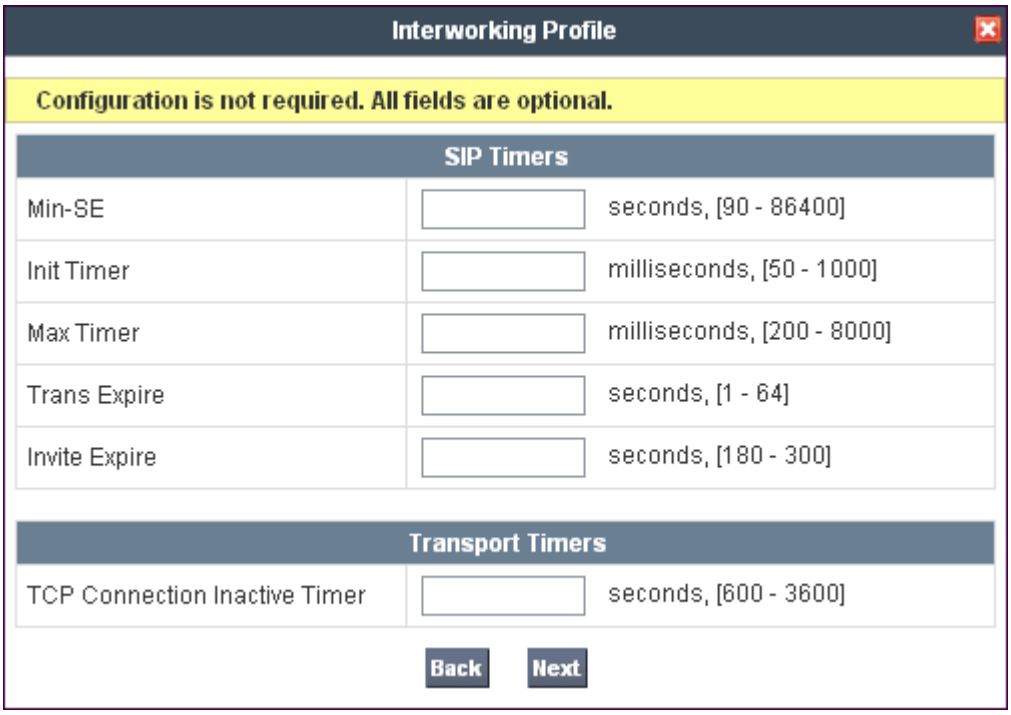
Click **Next** to continue**.**



Default values can be used for the next window that appears. Click **Next** to continue.



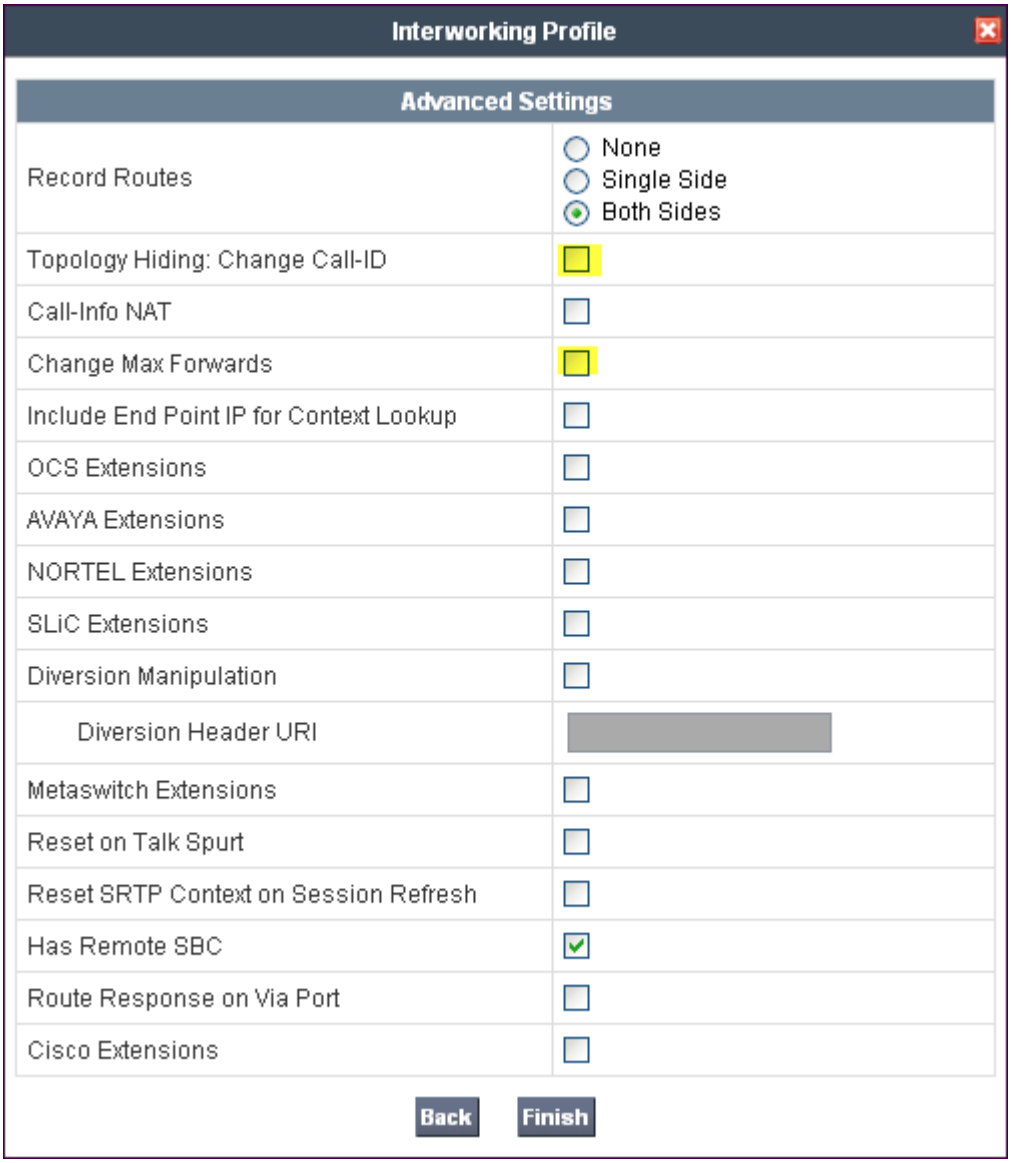
Default values can be used for the next window that appears. Click **Next** to continue.



On the **Advanced Settings** window uncheck the following default settings:

- **Topology Hiding: Change Call-ID**
- **Change Max Forwards**

Click **Finish** to save changes.



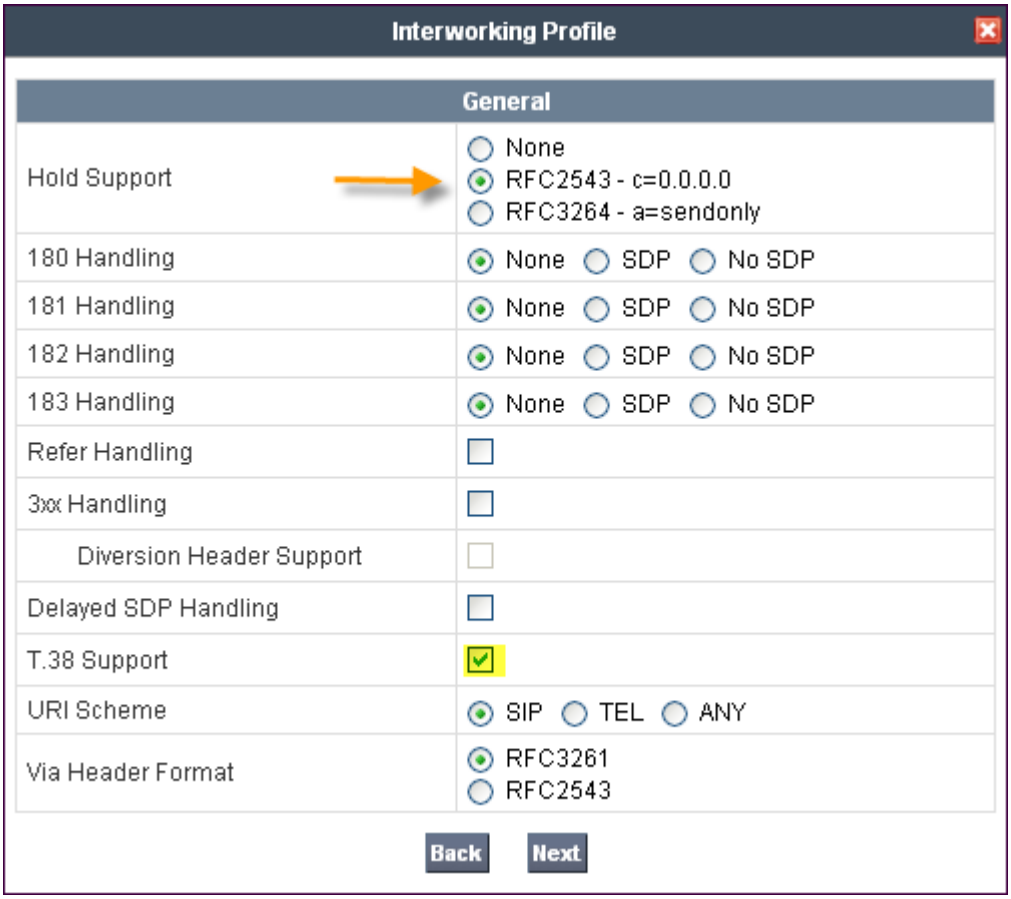
6.1.3.2 Server Interworking Profile – CenturyLink

To create a new Server Interworking Profile for CenturyLink, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on **Add Profile** as shown in the previous section. Enter a descriptive name for the new profile and click **Next** to continue.

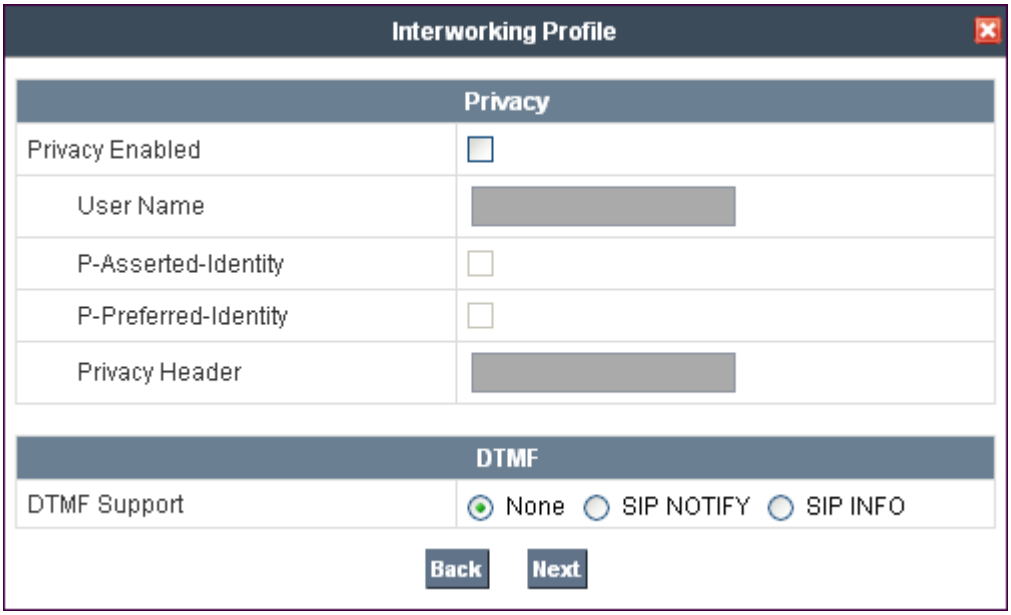
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Hold Support:** Select **RFC2543 - c=0.0.0.0**.
- **T.38 Support:** Checked.

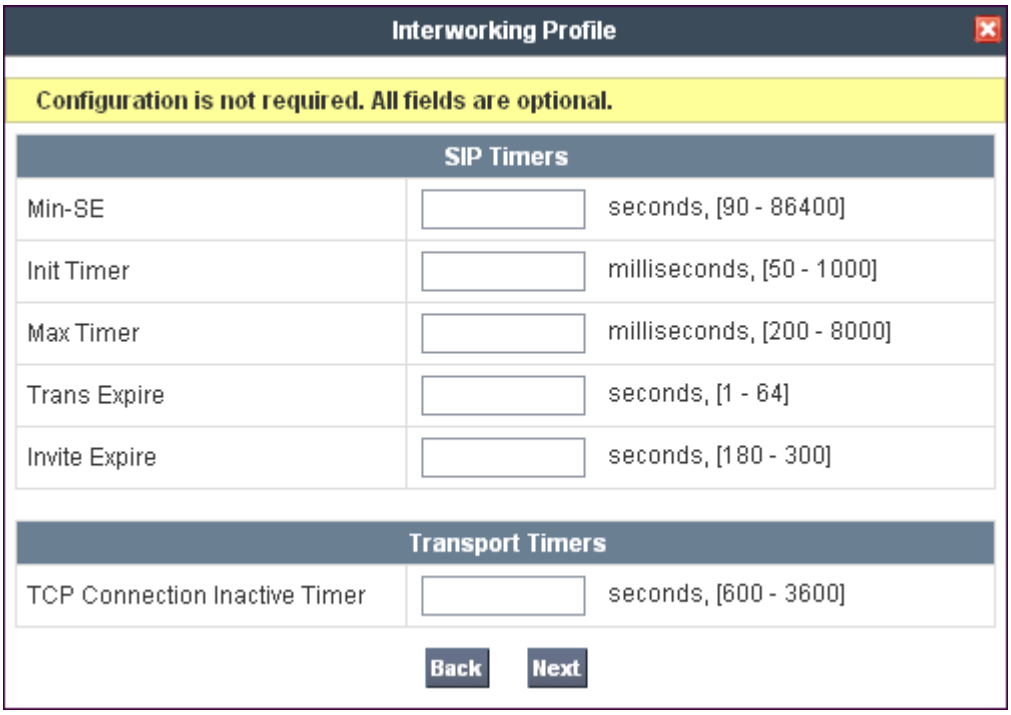
Click **Next** to continue**.**



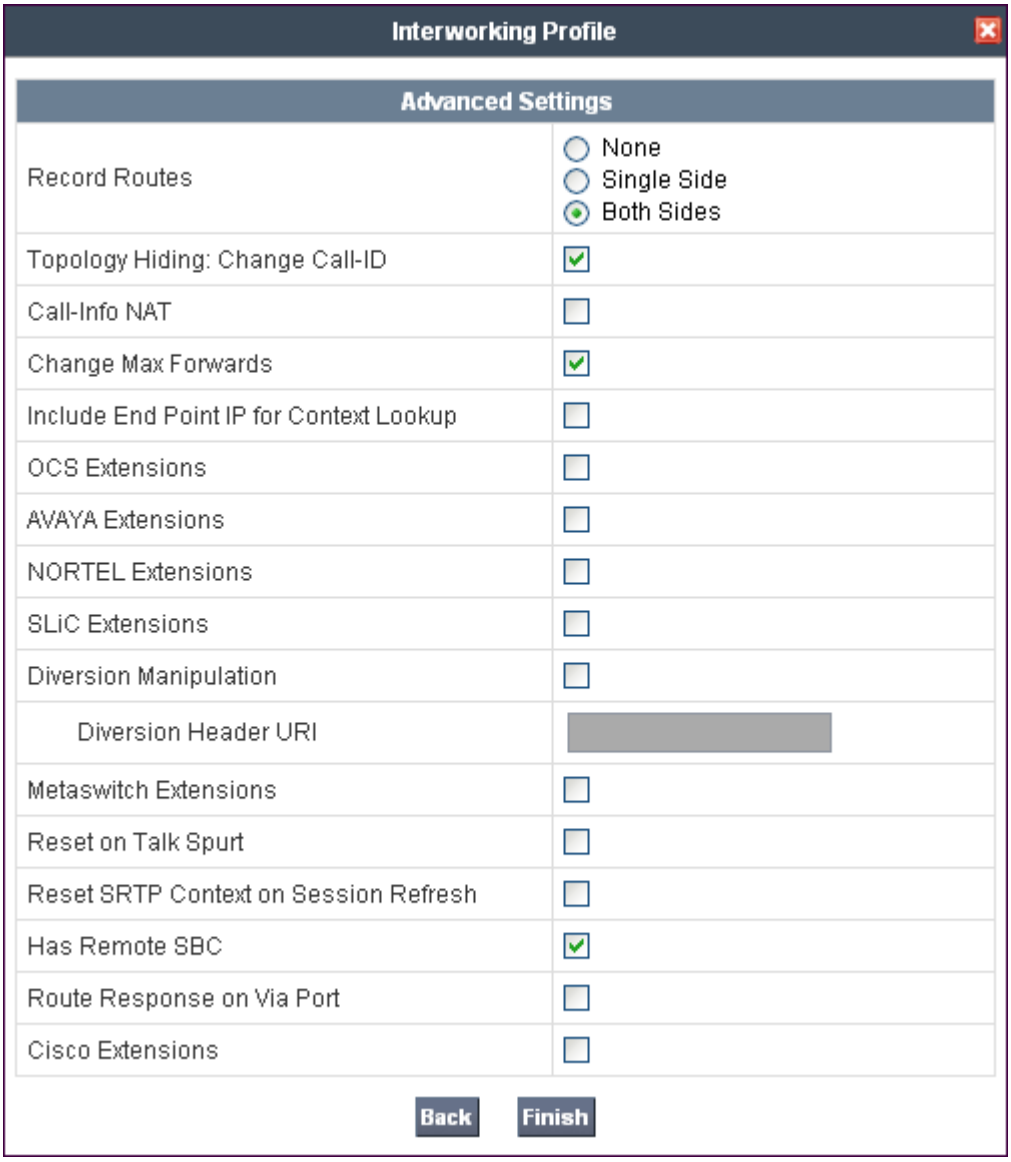
Default values can be used for the next window that appears. Click **Next** to continue.



Default values can be used for the next window that appears. Click **Next** to continue.



On the **Advanced Settings** the default values can be used. Click **Finish** to save changes.



6.1.4. Signaling Manipulation

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

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the E-SBC. Using this language, a script can be written and tied to a given flow through the EMS GUI. The E-SBC appliance then interprets this script at the given entry point or "hook point".

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding, add a Diversion header, remove unwanted headers and convert the multipart Content-Type to a standard Session Description Protocol (SDP) in the message body.

To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script**. A new blank SigMa Editor window will open.

The following sample script is written in two sections. The first section will act on the response of an inbound call from CenturyLink (e.g., 180 Ringing and 200 OK) while the second acts on the request of an outbound call to CenturyLink. The script is further broken down as follows:

- **within session "ALL"** Transformations applied to all SIP sessions.
- **act on response** Actions to be taken to the response of an INVITE (e.g., 180 Ringing and 200 OK).
- **%DIRECTION="INBOUND"** Applied to a messages arriving to Avaya SBCE.
- **%ENTRY_POINT="PRE_ROUTING"** The "hook point" to apply the script before the SIP message has routed through Avaya SBCE.
- **%HEADERS["p-asserted-identity"][1]** Used to retrieve an entire header. The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message**.**
- **.regex_replace ("avayalab\.com","255.xxx.xxx.92:5060")** An action to replace a given match with the provide string (e.g., find "avayalab.com" and replace it with the external interface).

The P-Asserted-Identity header will be modified by replacing the domain "avayalab.com" with the external IP address of Avaya SBCE and the SIP port of 5060 in both the response and request sessions. The request sessions are also modified by removing unwanted headers, unwanted

MIMEs in the body of the message and adding a Diversion header. During a call forward off-net over a SIP trunk, CS1000E sends the original calling party number in the FROM header and the called party number in the History-Info header. If the number in the FROM header is not one that is assigned to the SIP trunk, they require a Diversion header to have a number that is assigned and ignores the History-Info header.

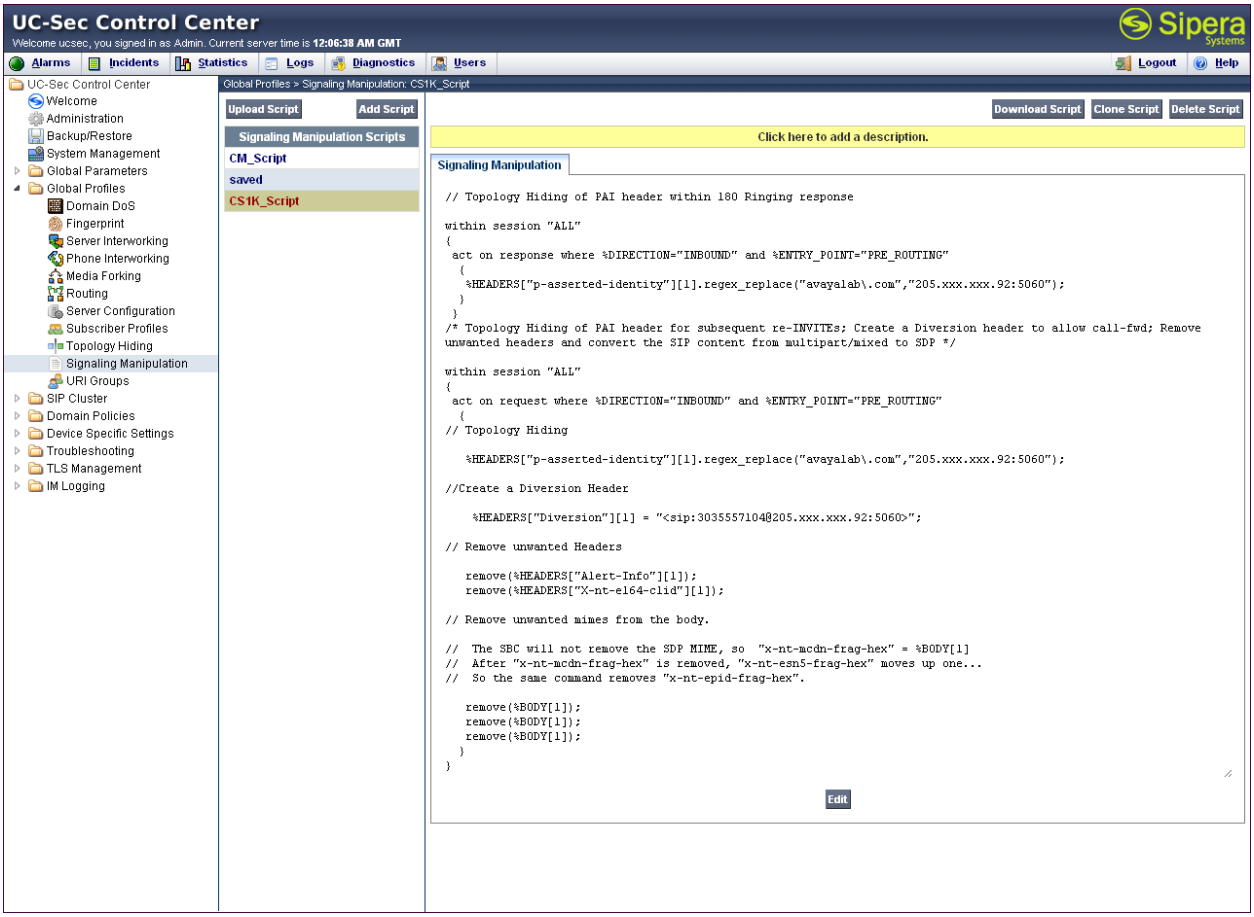
SigMa Editor

Options

Title CS1K_Script Save

```
// Topology Hiding of PAI header within 180 Ringing response

within session "ALL"
{
 act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
   %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com","205.168.62.92:5060");
  }
 }
/* Topology Hiding of PAI header for subsequent re-INVITEs; Create a Diversion header to allow call-fwd; Remove unwanted
headers and convert the SIP content from multipart/mixed to SDP */

within session "ALL"
{
 act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
// Topology Hiding

   %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com","205.168.62.92:5060");

//Create a Diversion Header

    %HEADERS["Diversion"][1] = "<sip:3036157104@205.168.62.92:5060>";

// Remove unwanted Headers

   remove(%HEADERS["Alert-Info"][1]);
   remove(%HEADERS["X-nt-e164-clid"][1]);

// Remove unwanted mimes from the body.
```

The following screen shows the finished Signaling Manipulation Script **CS1K_Script**. The script will later be added to the Server Configuration for the CS1000E in **Section 6.1.5.1**. The details of these script elements can be found in **Appendix A**.



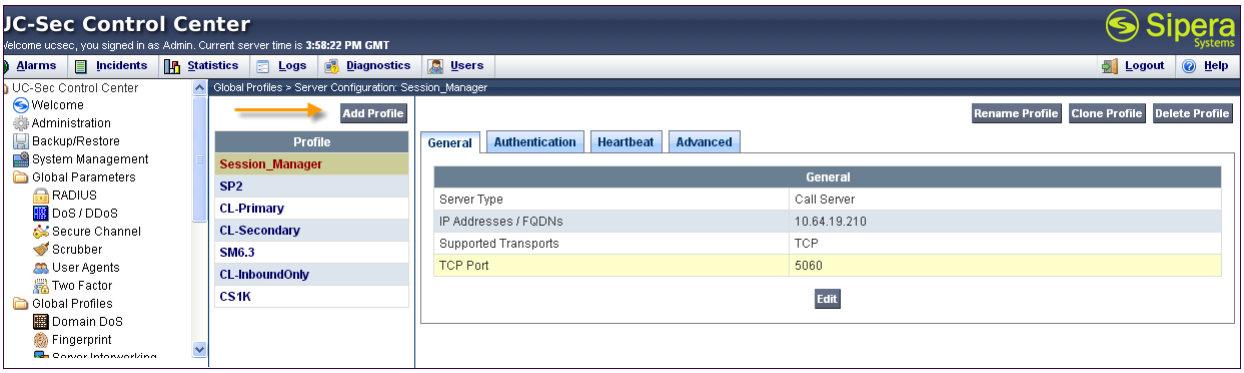
6.1.5. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

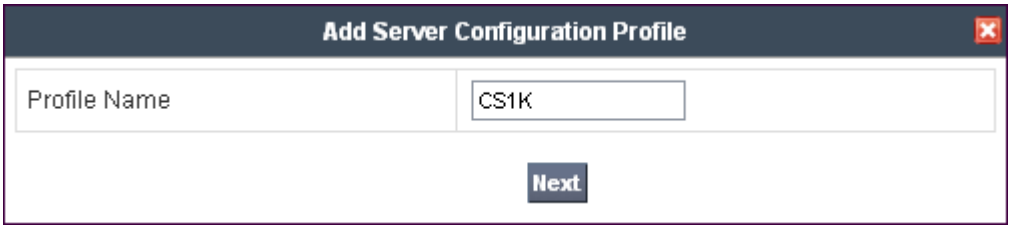
In the sample configuration, separate Server Configurations were created for CS1000E and CenturyLink.

6.1.5.1 Server Configuration – CS1000E

To add a Server Configuration Profile for CS1000E, navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** as shown below**.**



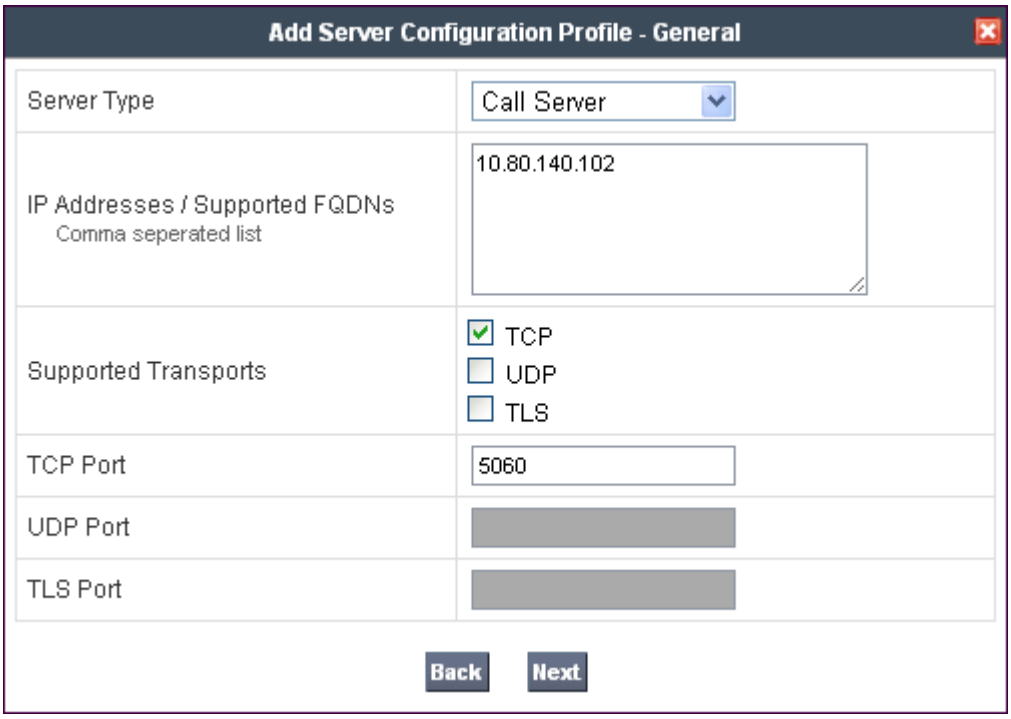
Enter a descriptive name for the new profile and click **Next**.



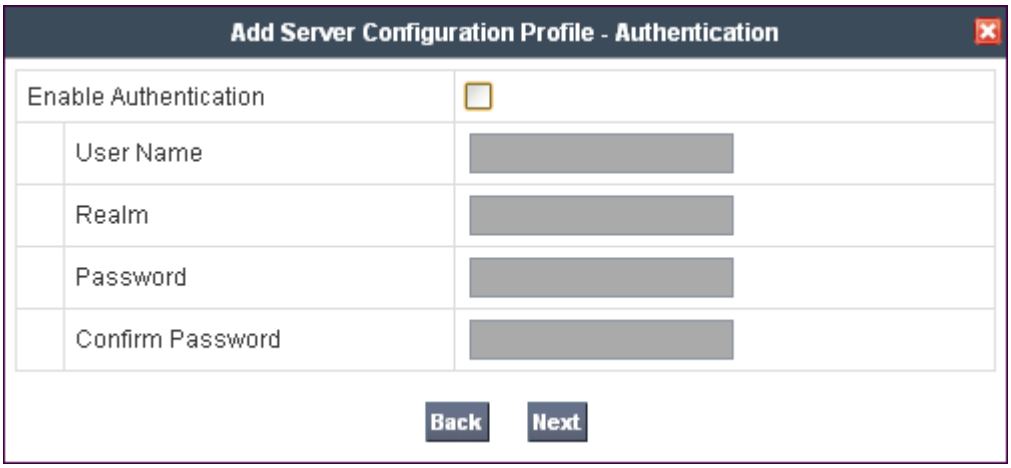
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Call Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the NRS (see **Section 5.10**).
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Endpoint on the NRS in **Section 5.10.3**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Endpoint on the NRS in **Section 5.10.3**.

Click **Next** to continue.



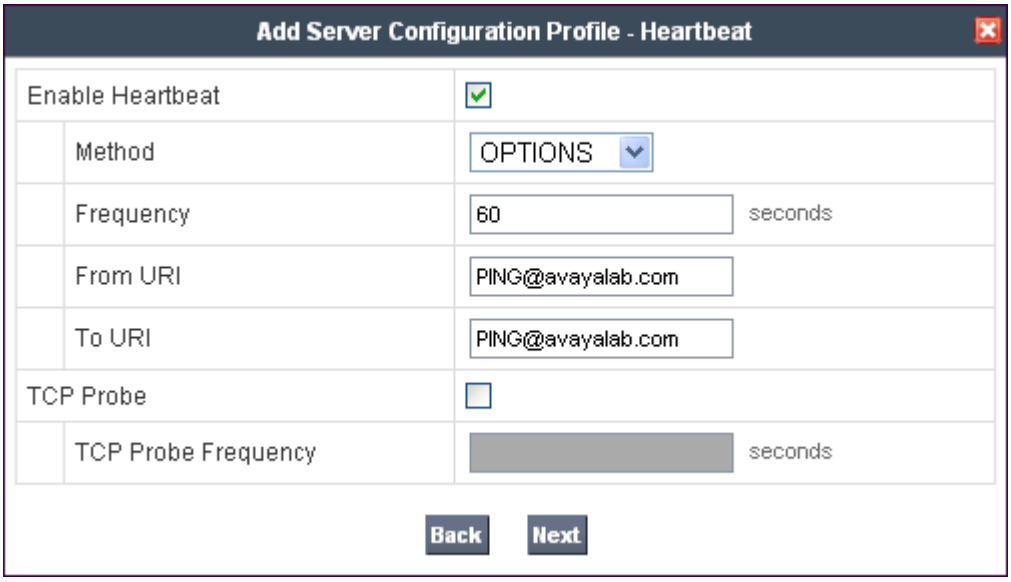
Verify **Enable Authentication** is unchecked as the CS1000E does not require authentication. Click **Next** to continue.



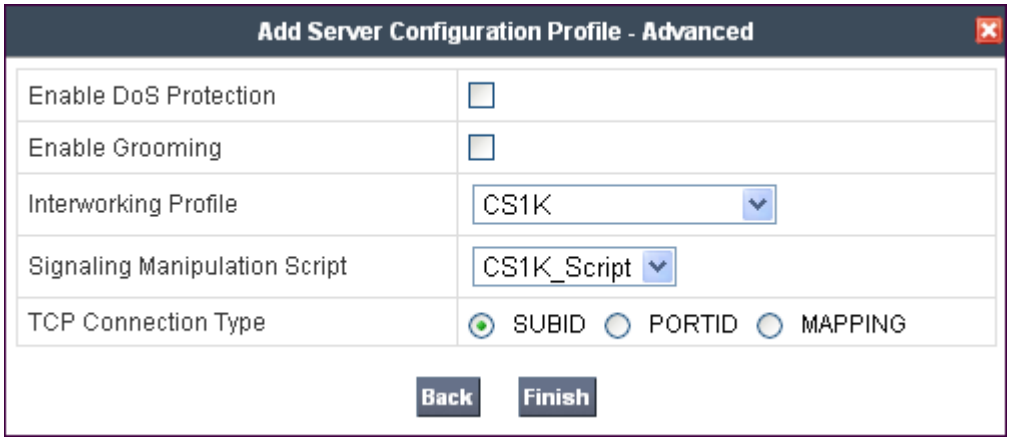
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS to the CS1000E. For compliance testing **60** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

Click **Next** to continue.



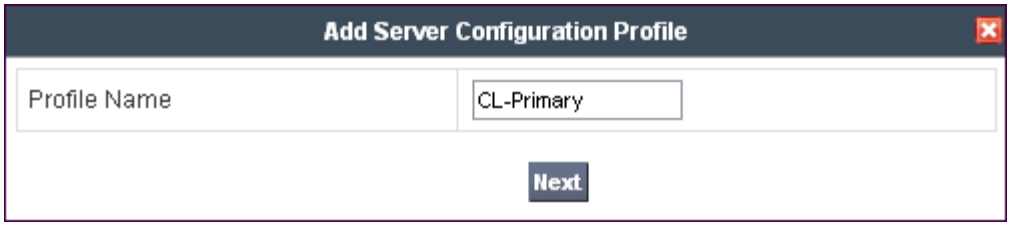
In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 6.1.3.1**. Select the **Signaling Manipulation Script** created in **Section 6.1.4**. Use default values for all remaining fields. Click **Finish** to save the configuration.



6.1.5.2 Server Configuration - CenturyLink

For compliance testing CenturyLink had four SIP servers assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound. Separate Server Configuration Profiles were created for the Primary and Secondary inbound and outbound IP addresses. A third Server Configuration Profile was created for the inbound only IP addresses.

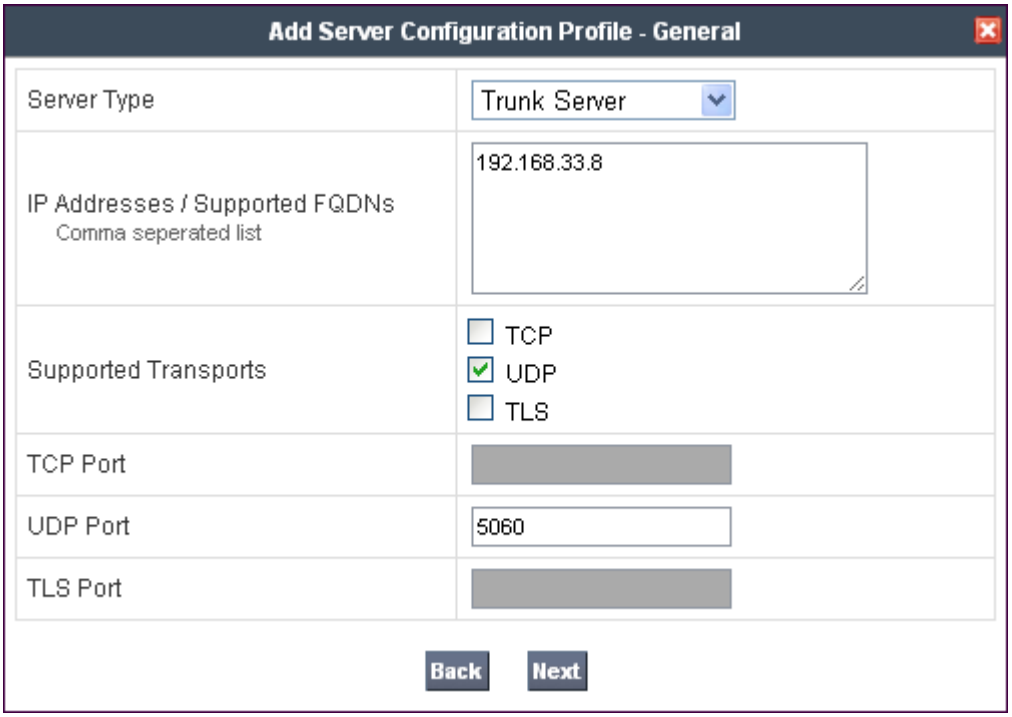
To add Server Configuration Profiles for CenturyLink, navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** (not shown). Enter a descriptive name for the new profile and click **Next**.



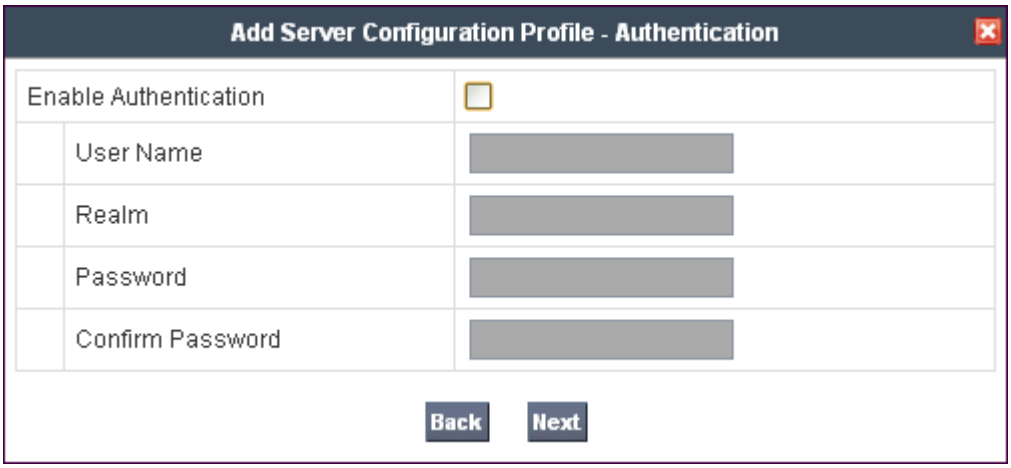
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Trunk Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the SIP proxy of the service provider. In the sample configuration, this is 192.168.33.8 for the Primary server and 192.168.32.8 for the Secondary server. This will associate the inbound SIP messages from CenturyLink's SIP server to this Sever Configuration.
- **Supported Transports:** Select the transport protocol to be used for SIP traffic between Avaya SBCE and CenturyLink. For compliance testing **UDP** was used.
- **UDP Port:** Enter the port number that CenturyLink uses to send SIP traffic. For compliance testing **5060** was used.

Click **Next** to continue.



Verify **Enable Authentication** is unchecked as CenturyLink does not require authentication. Click **Next** to continue.

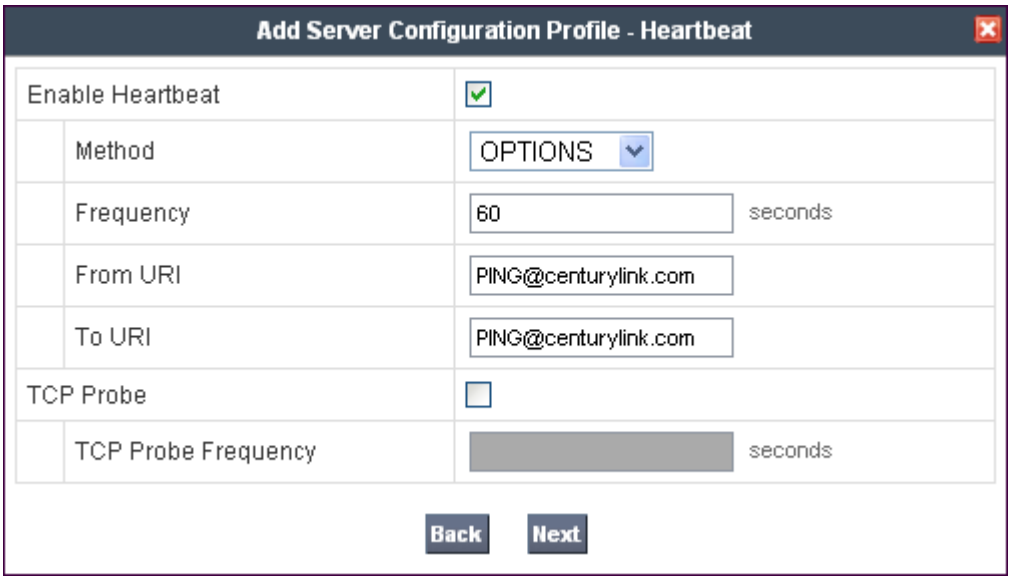


In the new window that appears, enter the following values. Use default values for all remaining fields:

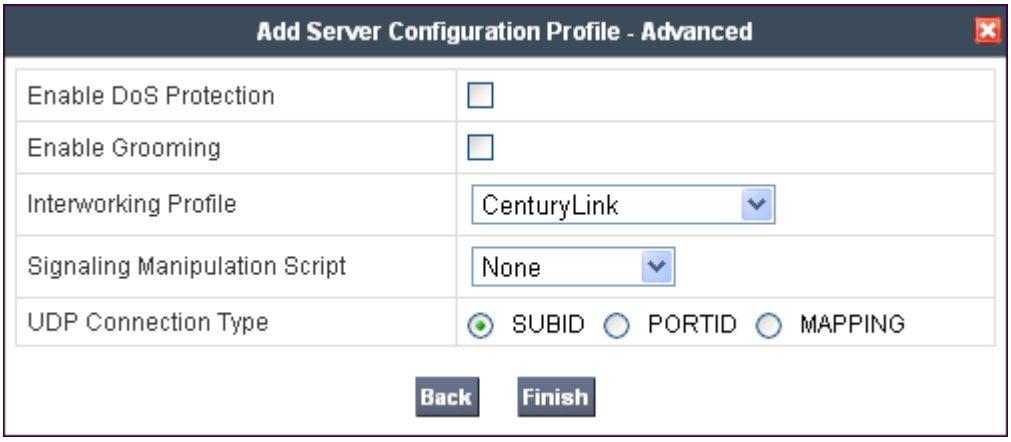
- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Sipera E-SBC will send SIP OPTIONS to each CenturyLink server. For compliance testing **60** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

Click **Next** to continue.

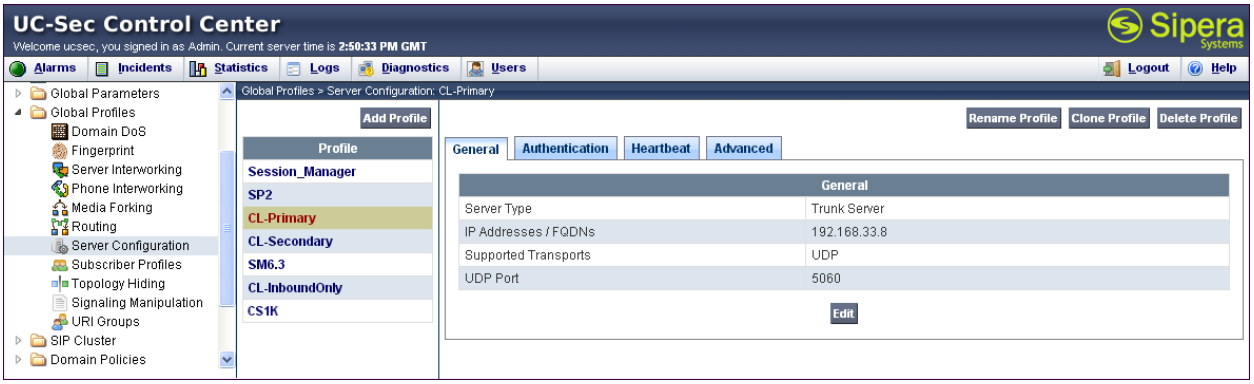
The SIP OPTIONS are sent to the SIP servers entered in the **IP Addresses /Supported FQDNs** in the **Server Configuration Profile** as show previously**.** The URI of PING@centurylink.com was used in the sample configuration to better identify the SIP OPTIONS in the call traces. CenturyLink does not look at the From and To headers when replying to SIP OPTIONS so any URI can be used as long as it is in the proper format (USER@DOMAIN).



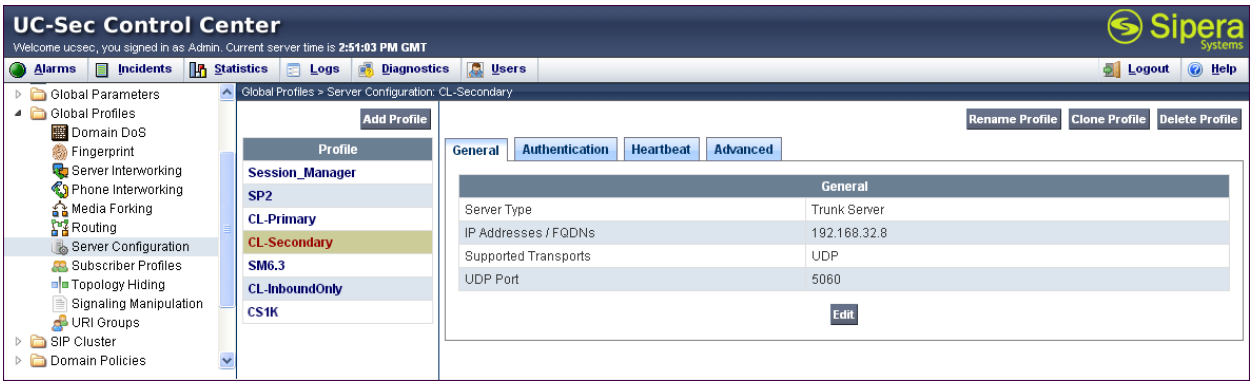
In the new window that appears, select the **Interworking Profile** created for CenturyLink in **Section 6.1.3.2**. Use default values for all remaining fields. Click **Finish** to save the configuration.



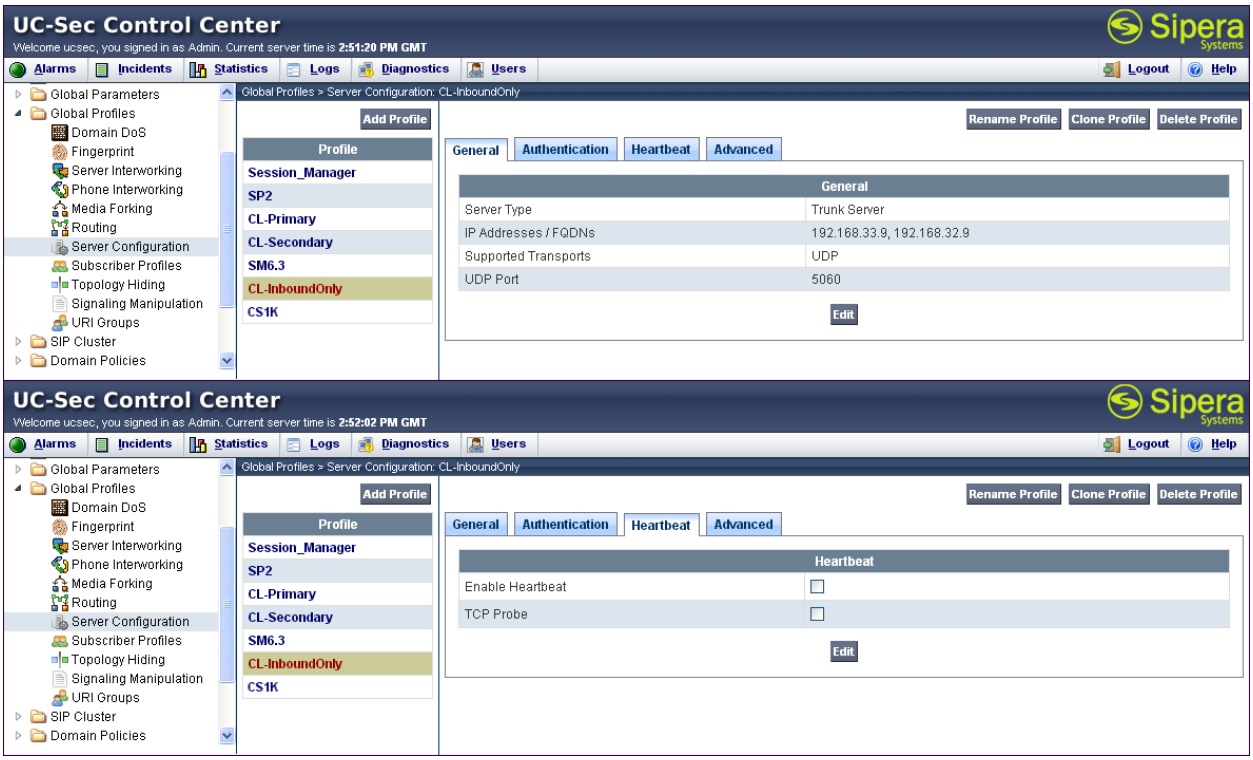
Once configuration is completed, the **CL-Primary** server configuration profile will appear as follows.



Repeat these procedures to create a separate server configuration for the secondary IP address for CenturyLink. Once configuration is completed, the **CL-Secondary** server configuration profile will appear as follows.



The inbound only IP addresses can be placed into one server configuration profile with the Heartbeat disabled as shown below.



6.2. Doman Policies

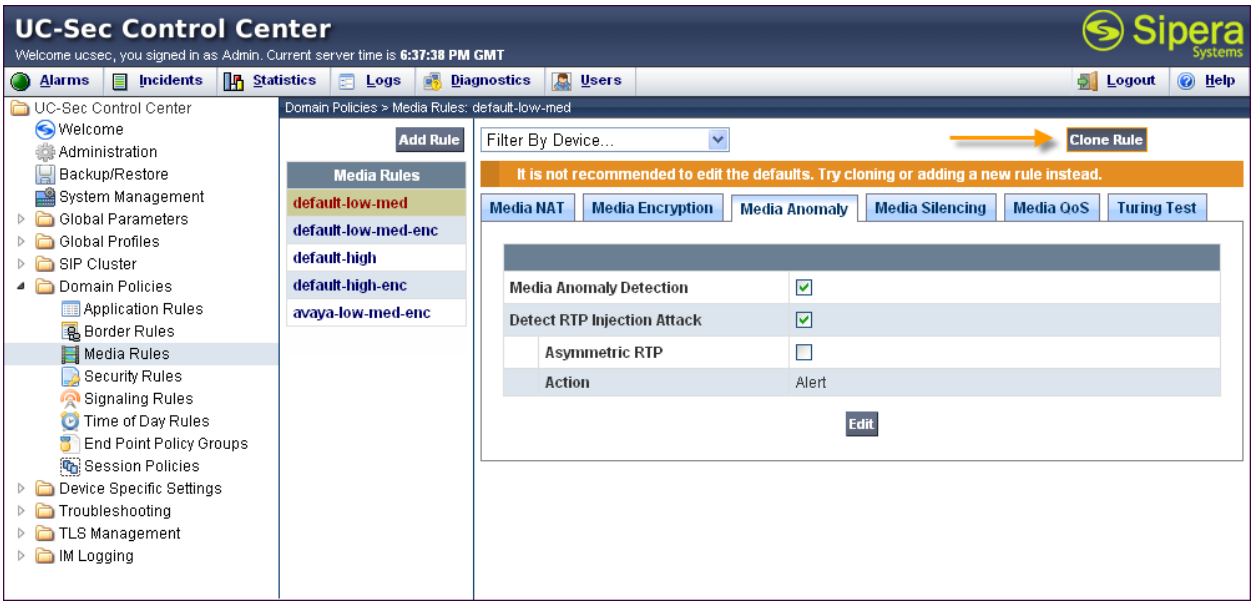
The Domain Policies feature configures, applies, and manages various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies which, in turn, activate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

6.2.1. Media Rule

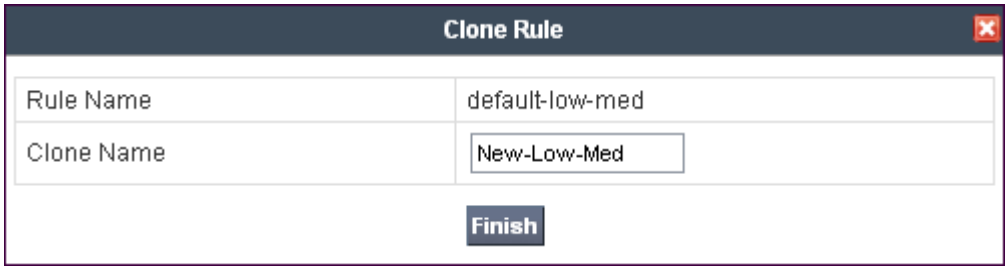
Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be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

Create a custom Media Rule to set the Quality of Service and Media Anomaly Detection. The sample configuration shows a custom Media Rule **New-Low-Med** was created for CenturyLink and the enterprise.

To create a custom Media Rule, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**. With **default-low-med** selected, click **Clone Rule** as shown below.

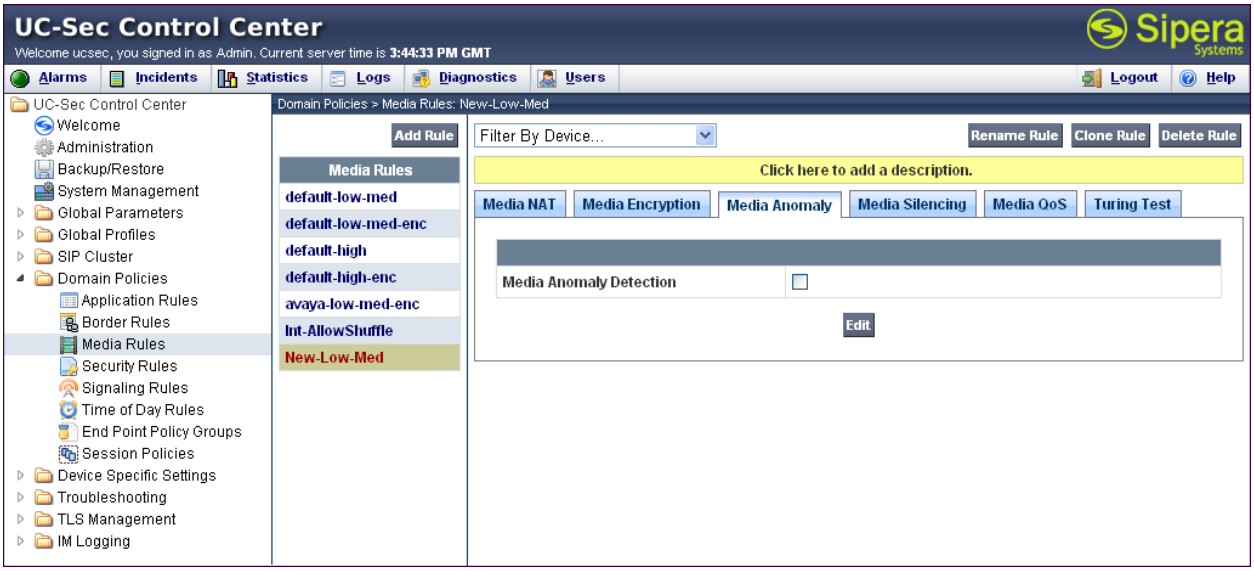


Enter a descriptive name for the new rule and click **Finish**.

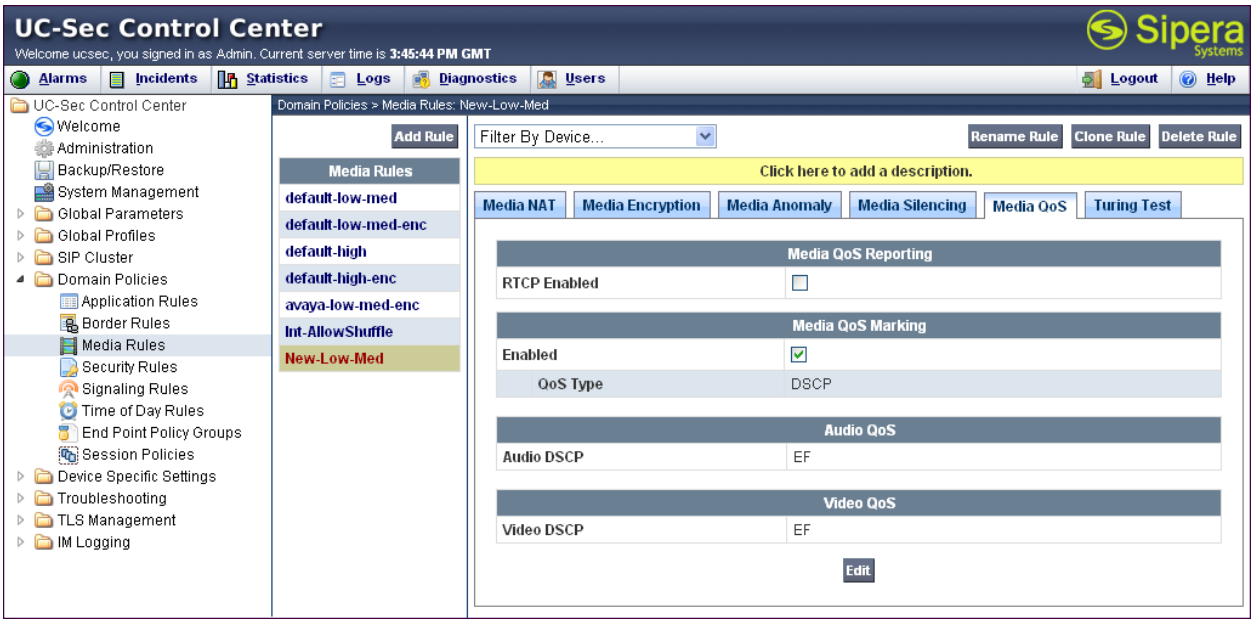


When the RTP packets of a call are shuffled from one IP endpoint to another within the CS1000E, Avaya SBCE will interpret this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created during an audio shuffle. To modify the rule, select the **Media Anomaly** tab and click **Edit**. Uncheck **Media Anomaly Detection** and click **Finish** (not shown)**.**

The following screen shows the **New-Low-Med** rule with **Media Anomaly Detection** disabled.



On the **Media QoS** tab select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies for the media. The following screen shows the QoS values used for compliance testing.

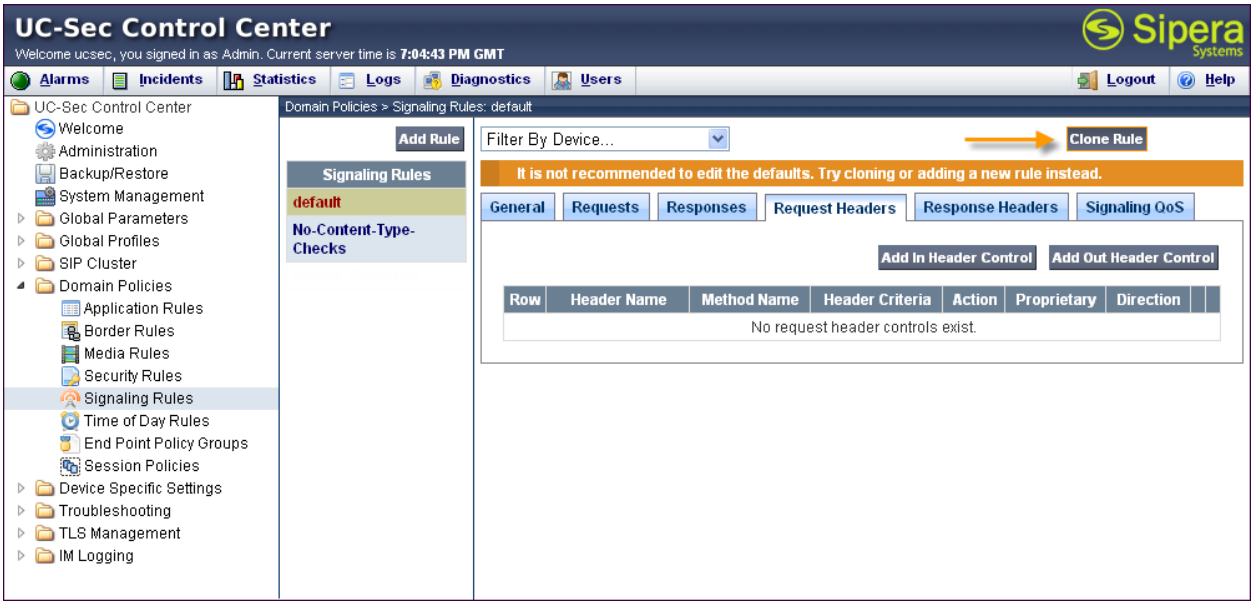


6.2.2. Signaling Rule

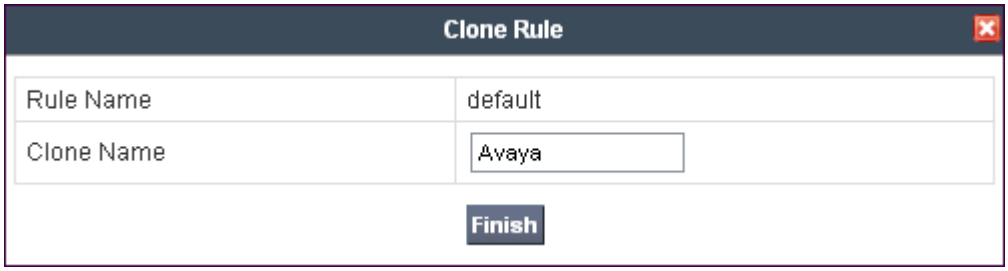
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling

criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

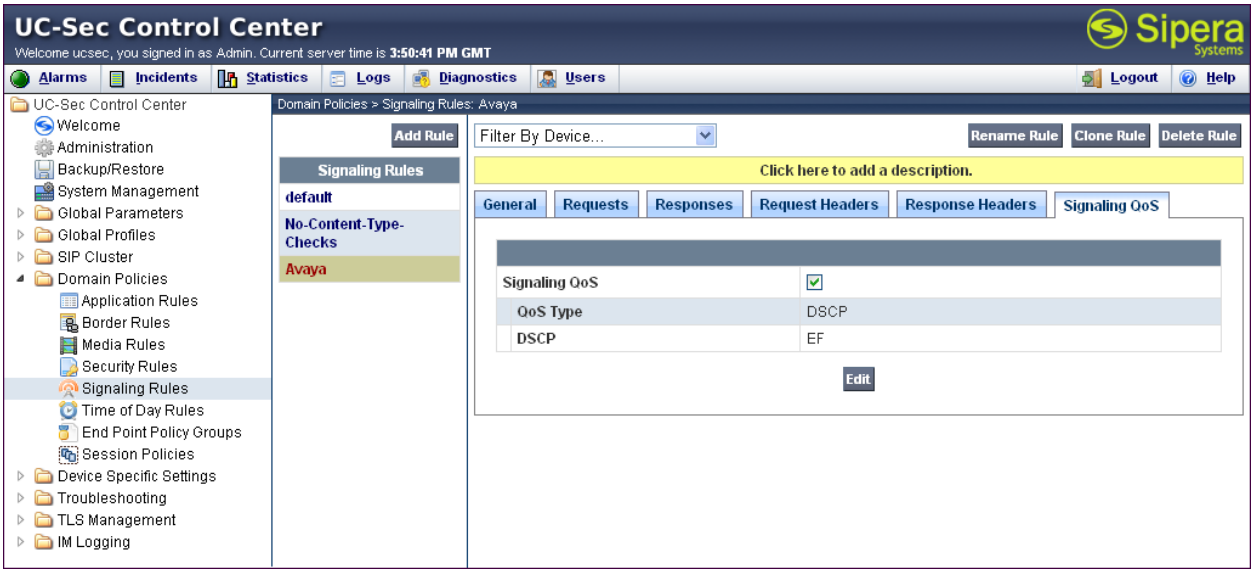
Clone and modify the default signaling rule to add the proper quality of service to the SIP message. To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.



Enter a descriptive name for the new rule and click **Finish**.



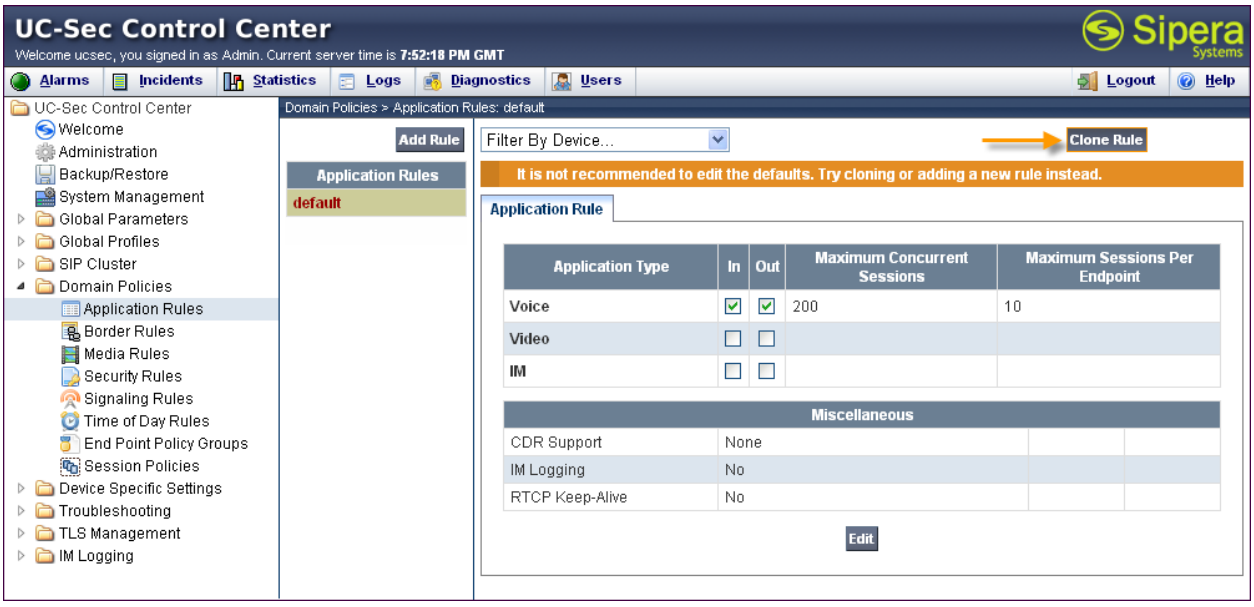
On the **Signaling QoS** tab select the proper Quality of Service (QoS). The Sipera E-SBC can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies for signaling. The following screen shows the QoS values used for compliance testing.



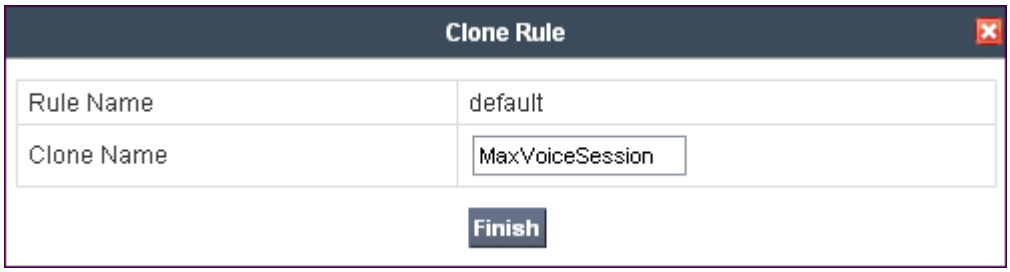
6.2.3. Application Rule

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

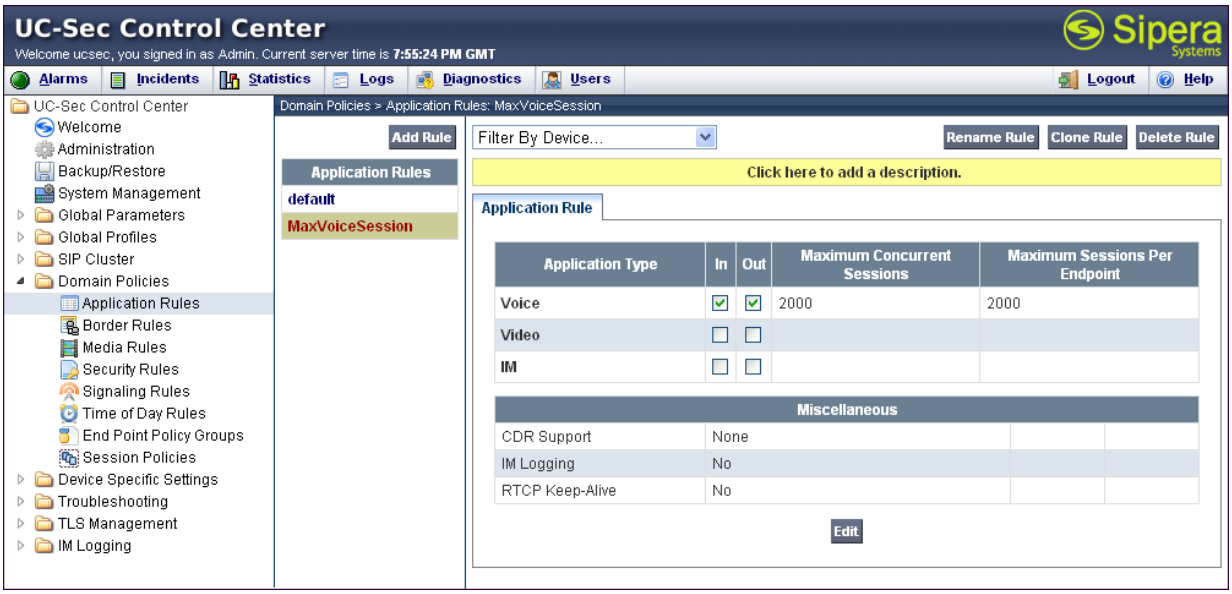
Create an Application Rule to increase the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**. To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.



Enter a descriptive name for the new rule and click **Finish**.



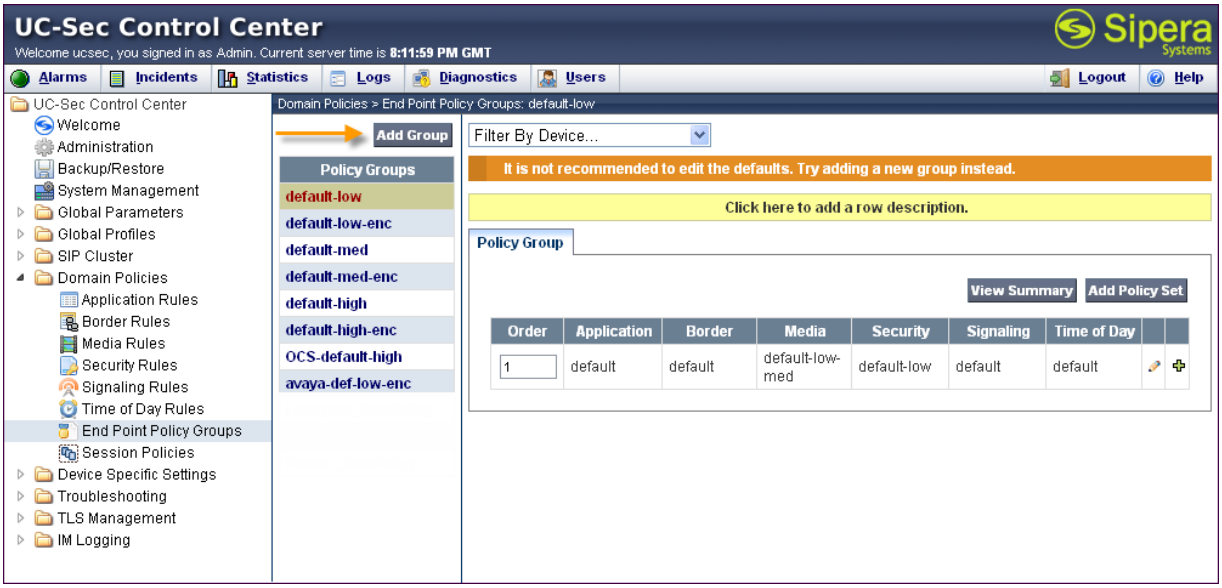
Edit the rule by clicking the **Edit** button as shown above. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. Set the values high enough for the amount of traffic the network is able process. Keep in mind Avaya SBCE takes 30 seconds for sessions to be cleared after disconnect.



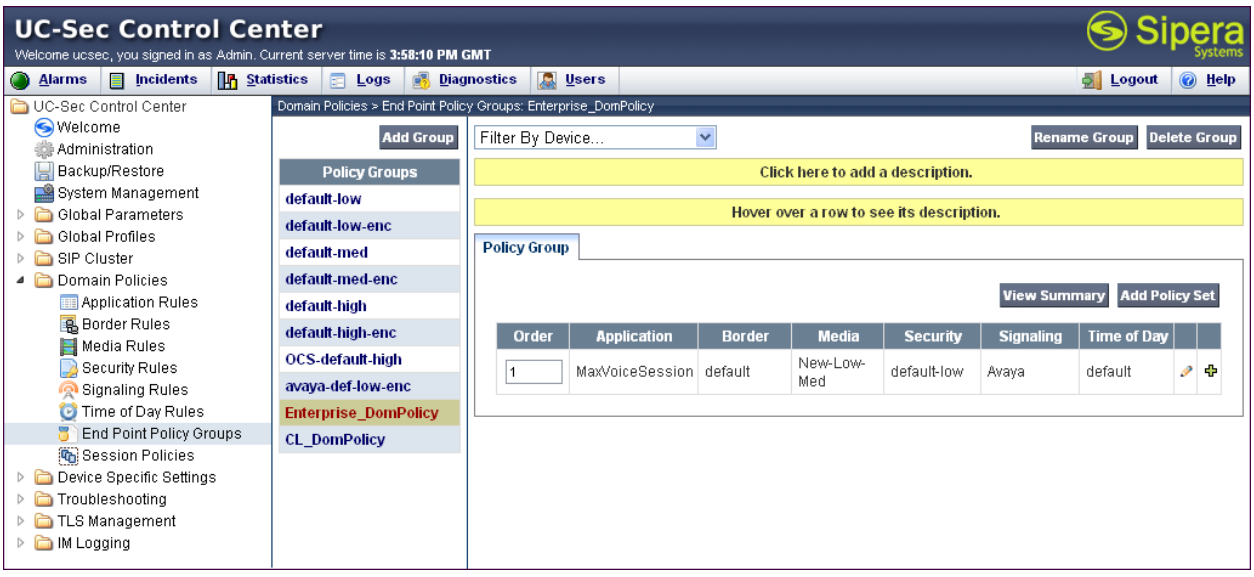
6.2.4. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 6.3.4**. Create a separate Endpoint Policy Group for the enterprise and the CenturyLink SIP Trunk.

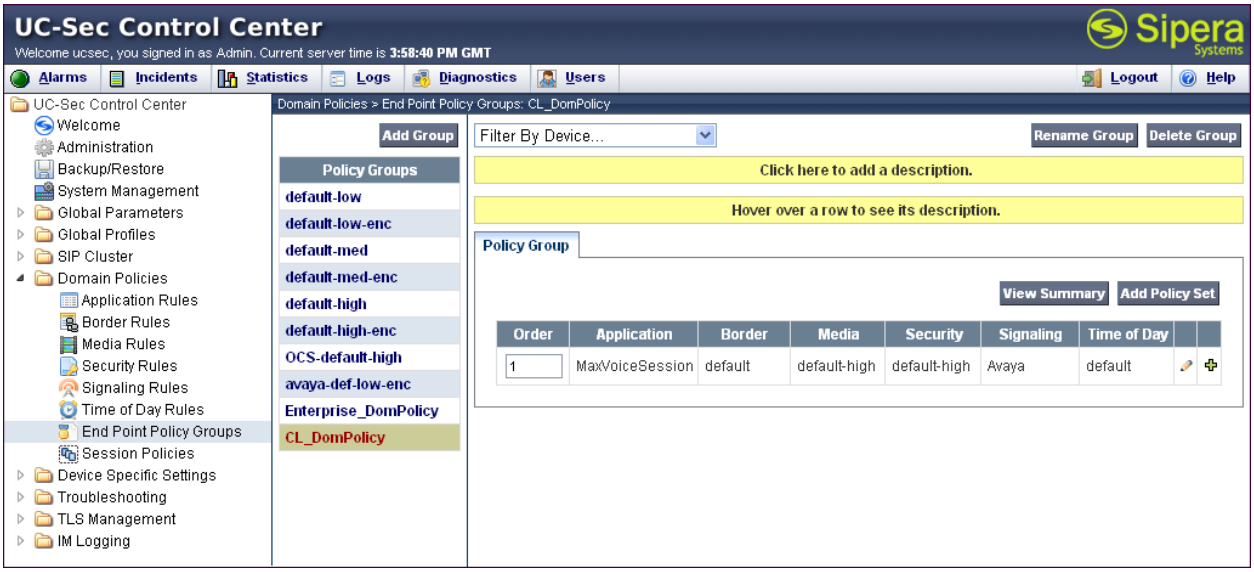
To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** as shown below.



The following screen shows **Enterprise_DomPolicy** created for the enterprise. Set the **Application**, **Media**, and **Signaling** rules to the ones previously created. Set the **Border**, **Security** and **Time of Day** rules to **default** or **default-low**.



The following screen shows **CL_DomPolicy** created for CenturyLink SIP Trunk. Set the **Application**, **Media**, and **Signaling** rules to the one previously created. Set the **Border**, **Security**, and **Time of Day** rules to **default** or **default-high**.



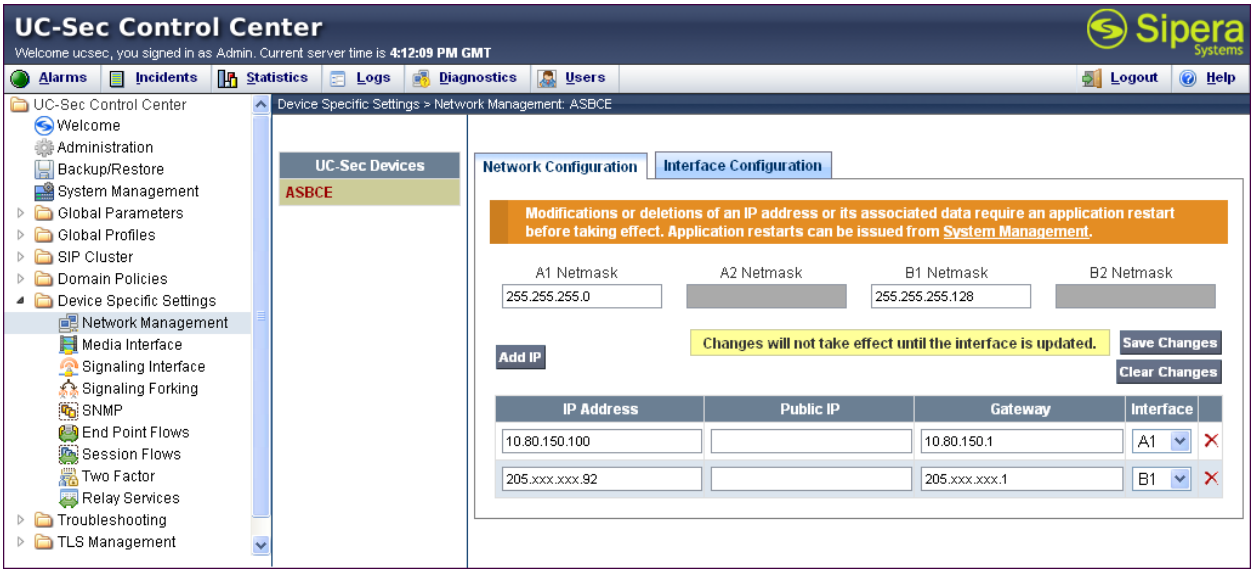
6.3. Device Specific Settings

The Device Specific Settings feature allows aggregate system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

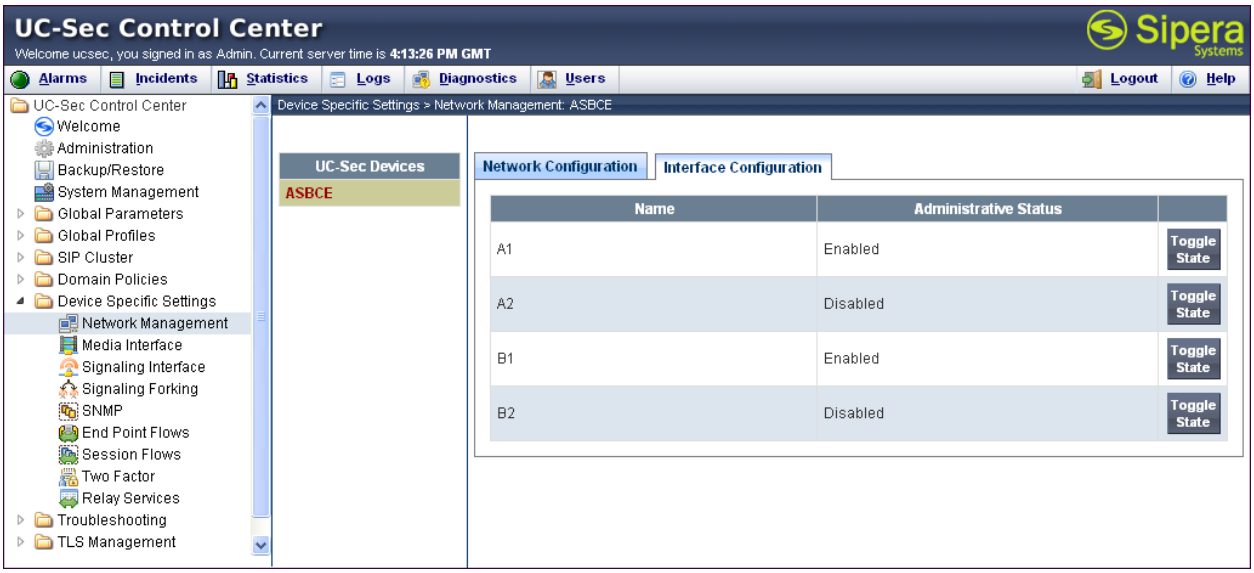
6.3.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

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



The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click its **Toggle State** button.

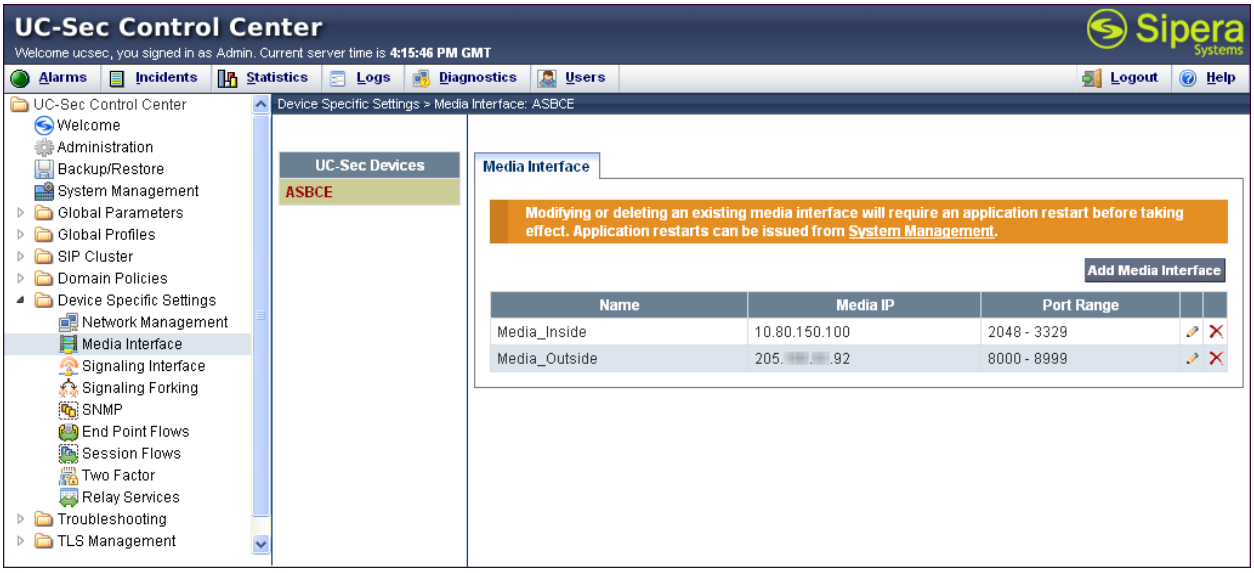


6.3.2. Media Interface

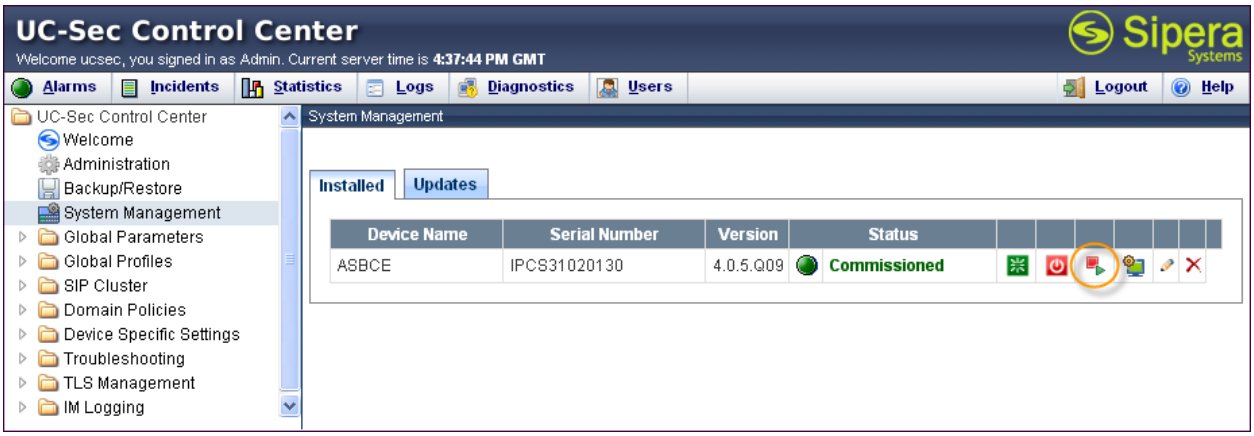
The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will listen for SIP media on the defined ports. Create a SIP Media Interface for both the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface.**

The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces..



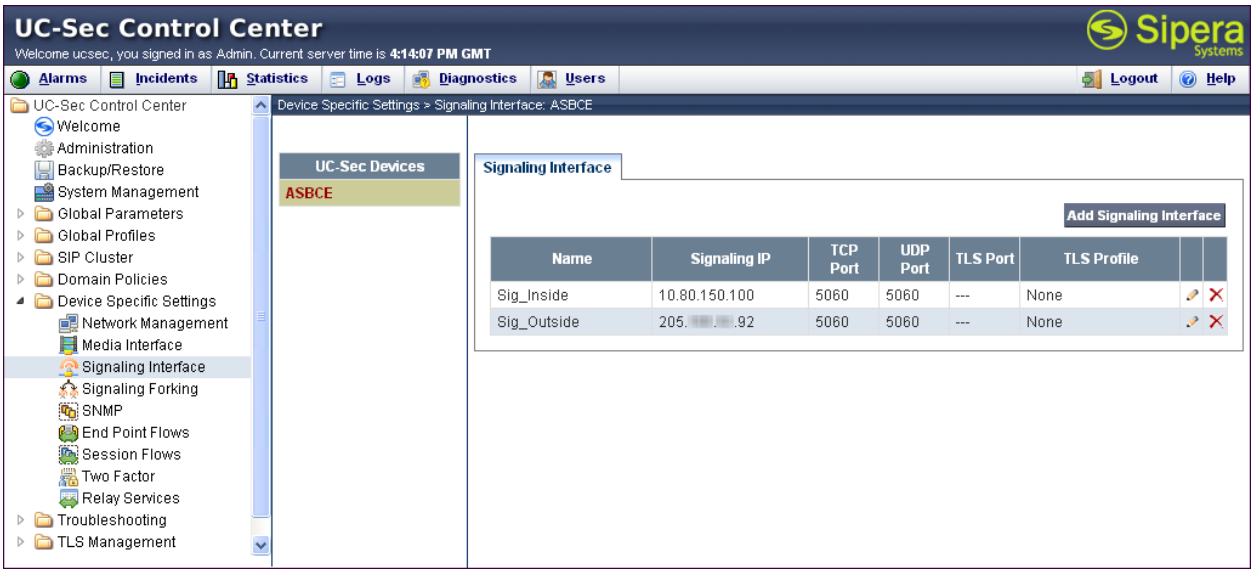
After the media interfaces are created, an application restart is necessary before the changes will take effect. Navigate to **UC-Sec Control Center → System Management** and click the forth icon from the right to restart the applications as highlighted below.



6.3.3. Signaling Interface

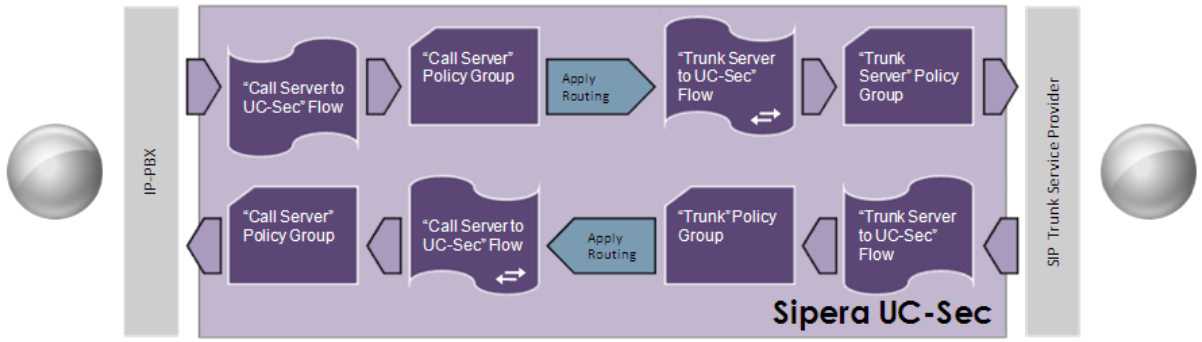
The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Signaling Interface** and click **Add Signaling Interface.**

The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

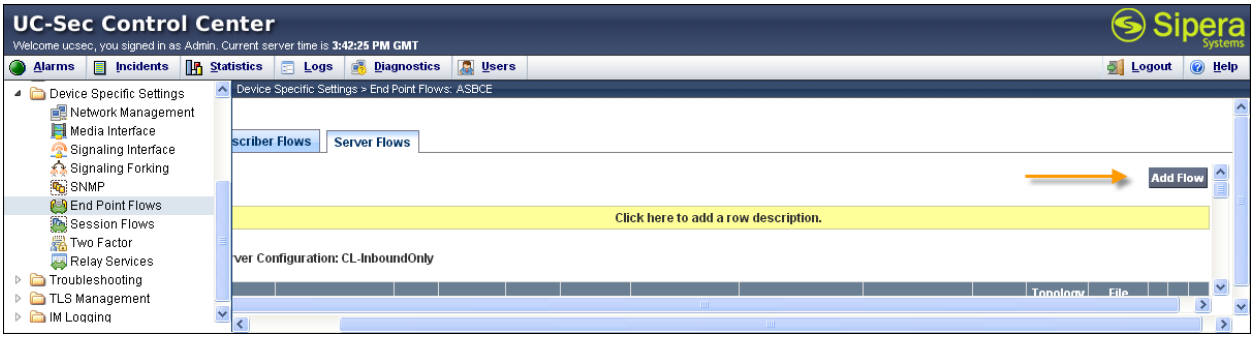


6.3.4. End Point Flows - Server Flow

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



Create a Server Flow for CS1000E and the CenturyLink SIP Trunk. To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** as shown in below.

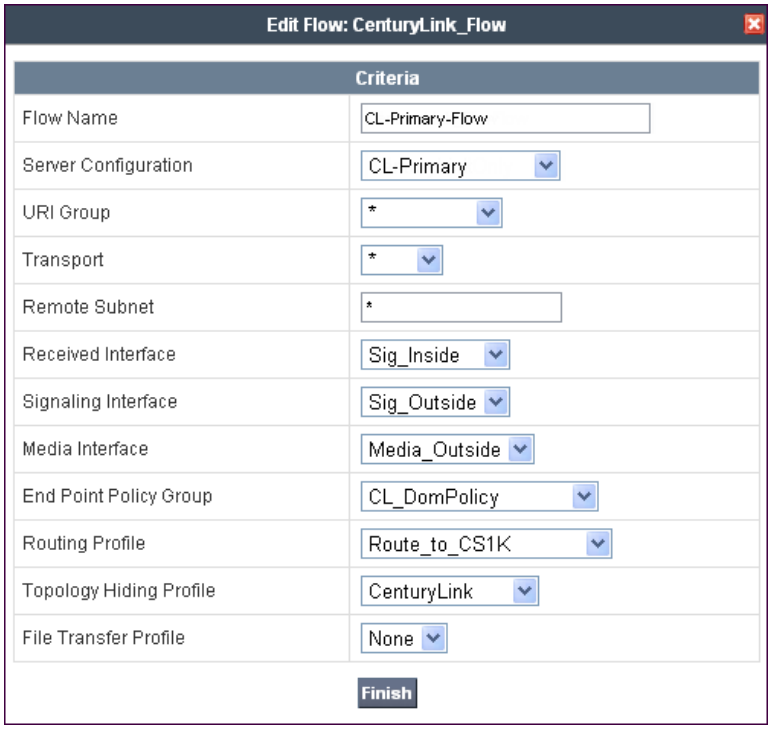


In the new window that appears, enter the following values. Use default values for all remaining fields:

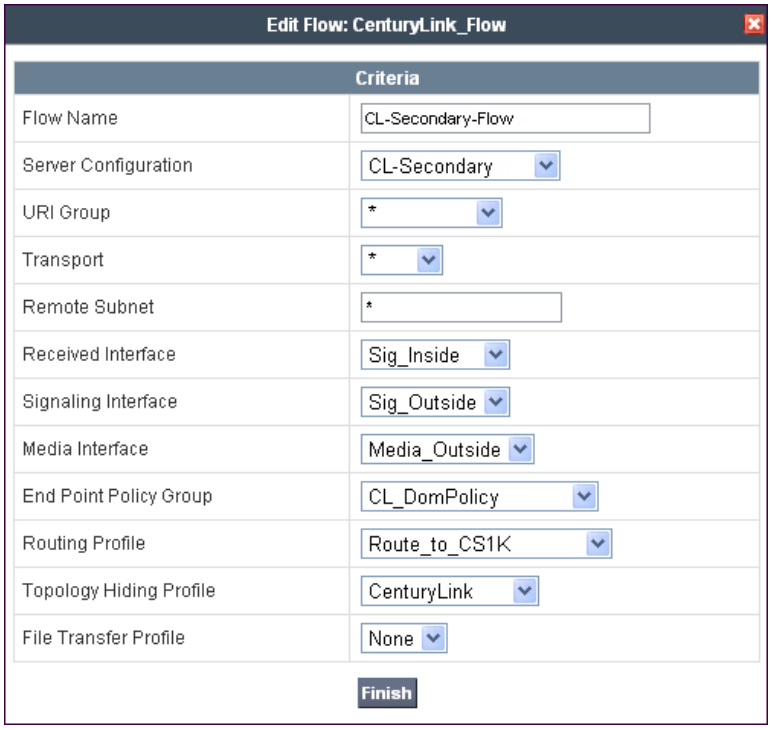
- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 6.1.5** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration.
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration.

Click **Finish** to save and exit.

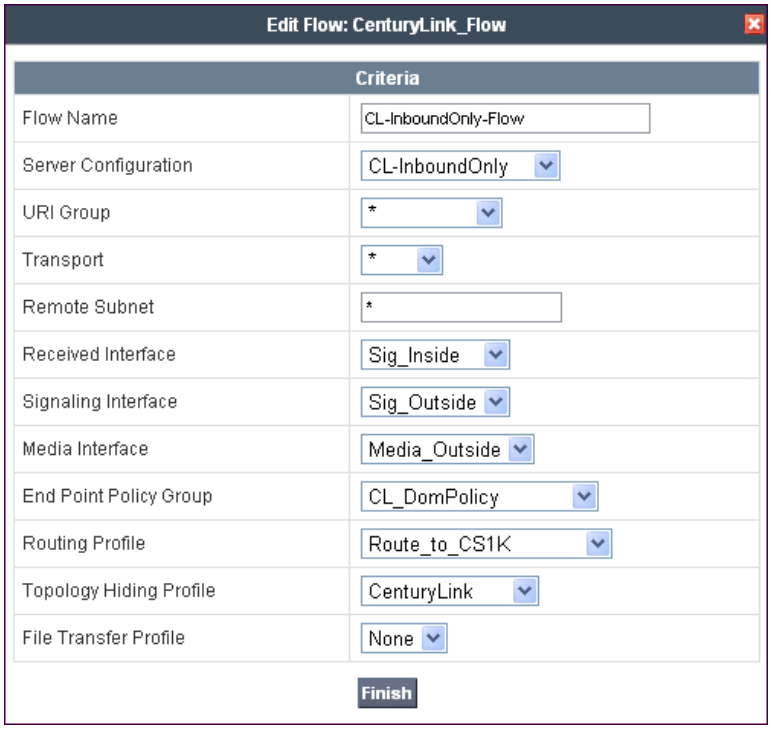
The following screen shows the Server Flow for CL-Primary:



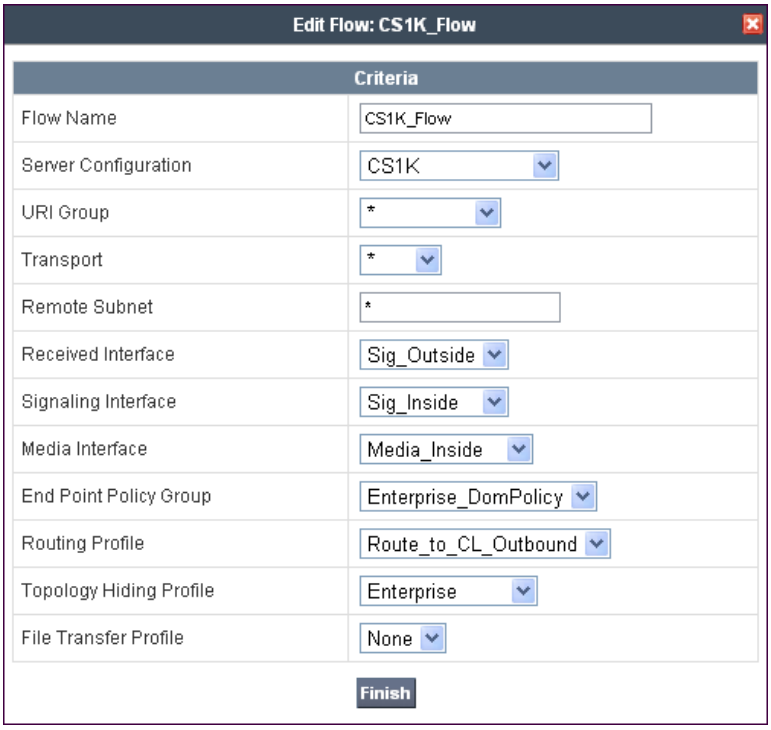
The following screen shows the Server Flow for CL-Secondary:



The following screen shows the Server Flow for CL-InboundOnly-Flow:



The following screen shows the Sever Flow for CS1000E:



7. CenturyLink SIP Trunk Configuration

To use CenturyLink SIP Trunk, a customer must request the service from CenturyLink using their sales processes. This process can be initiated by contacting CenturyLink via the corporate web site at www.centurylink.com and requesting information via the online sales links or telephone numbers.

8. Verification Steps

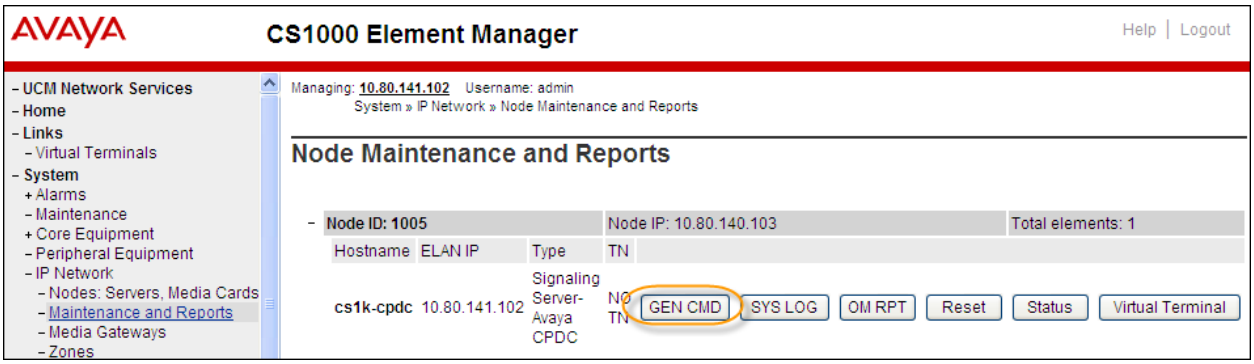
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

8.1. Avaya Communication Server 1000E Verifications

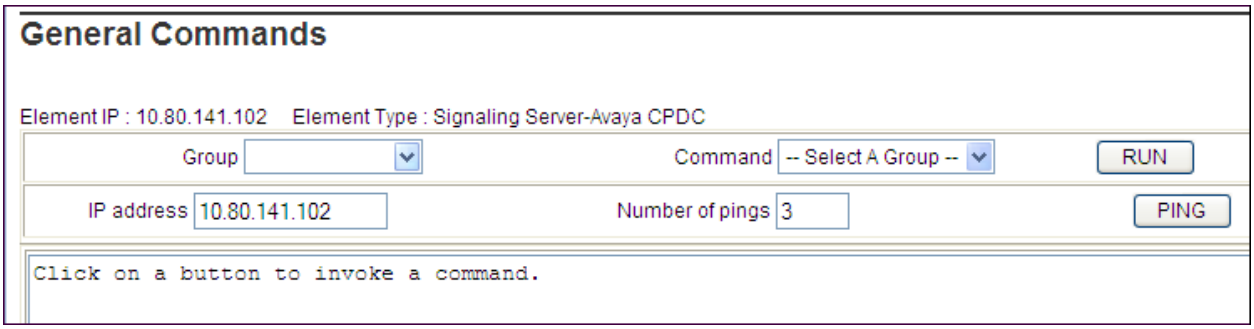
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

8.1.1. IP Network Maintenance and Reports Commands

From Element Manager, navigate to **System → IP Network → Maintenance and Reports** as shown below. In the resultant screen on the right, click the Gen CMD button.

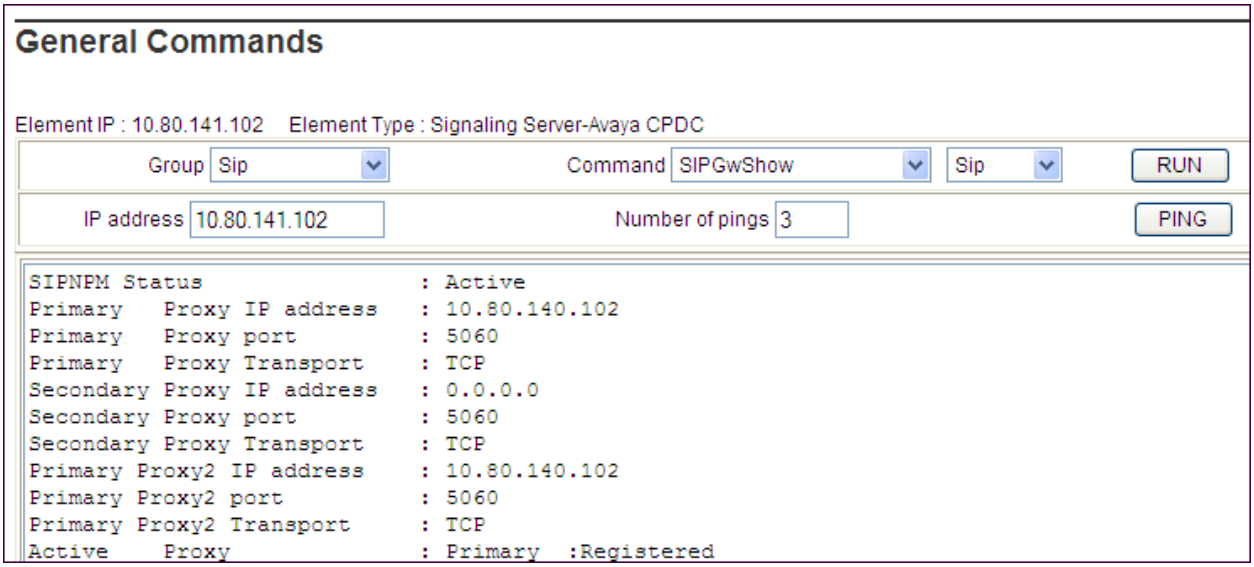


The **General Commands** page is displayed as shown below.

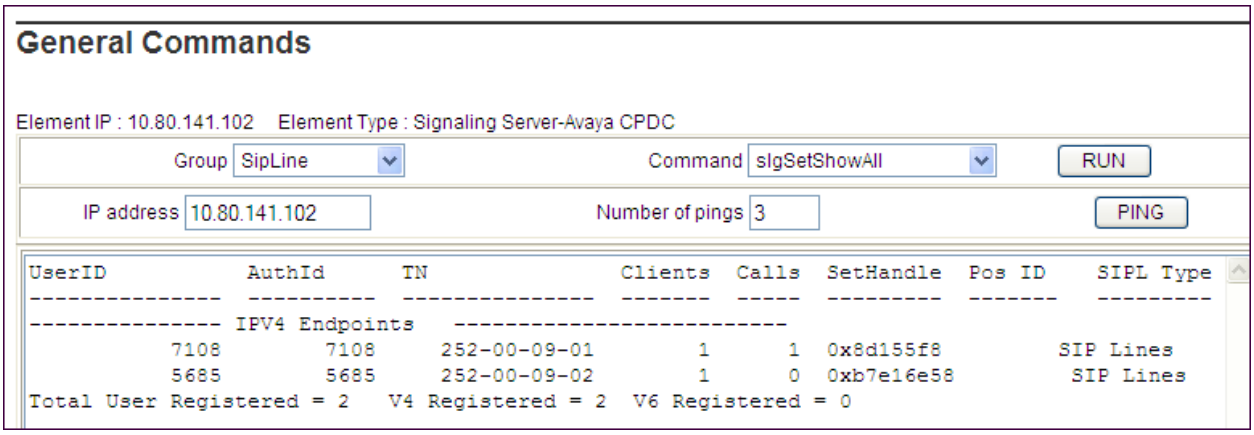


A variety of commands are available by selecting an appropriate Group and Command from the drop-down menus, and selecting Run.

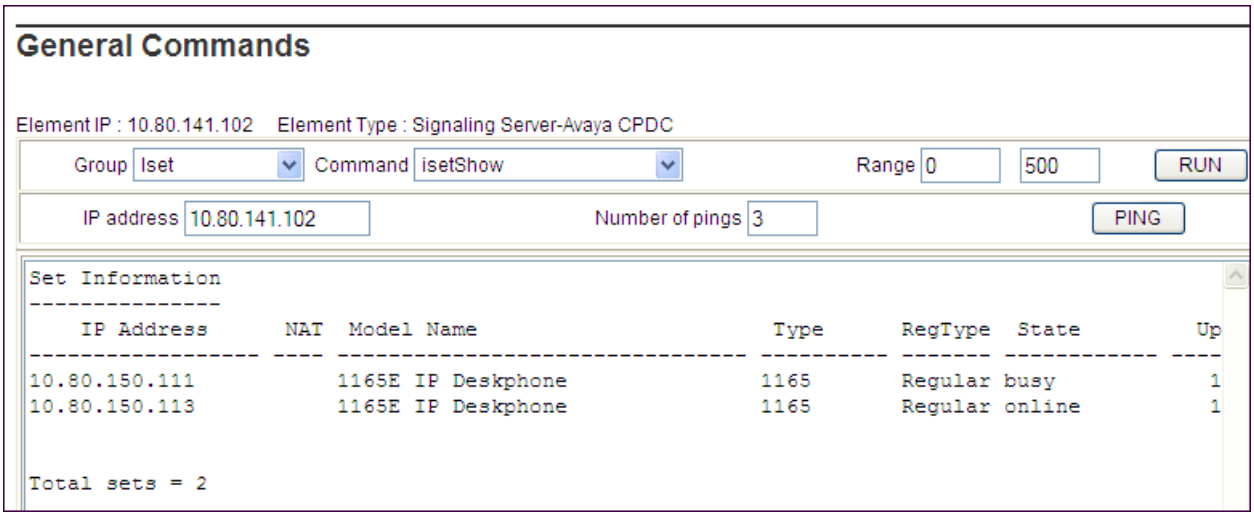
To check the status of the SIP Gateway to the NRS in the sample configuration, select **Sip** from the Group menu and **SIPGwShow** from the **Command** menu. Click Run. The example output below shows that the NRS (10.80.140.102, port 5060, TCP) has **SIPNPM Status** Active.



The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command sigSetShowAll** in **Group SipLine**. At the time this screen was captured, the SIP telephone with DN 7108 was involved in an active call with the CenturyLink SIP Trunk service.



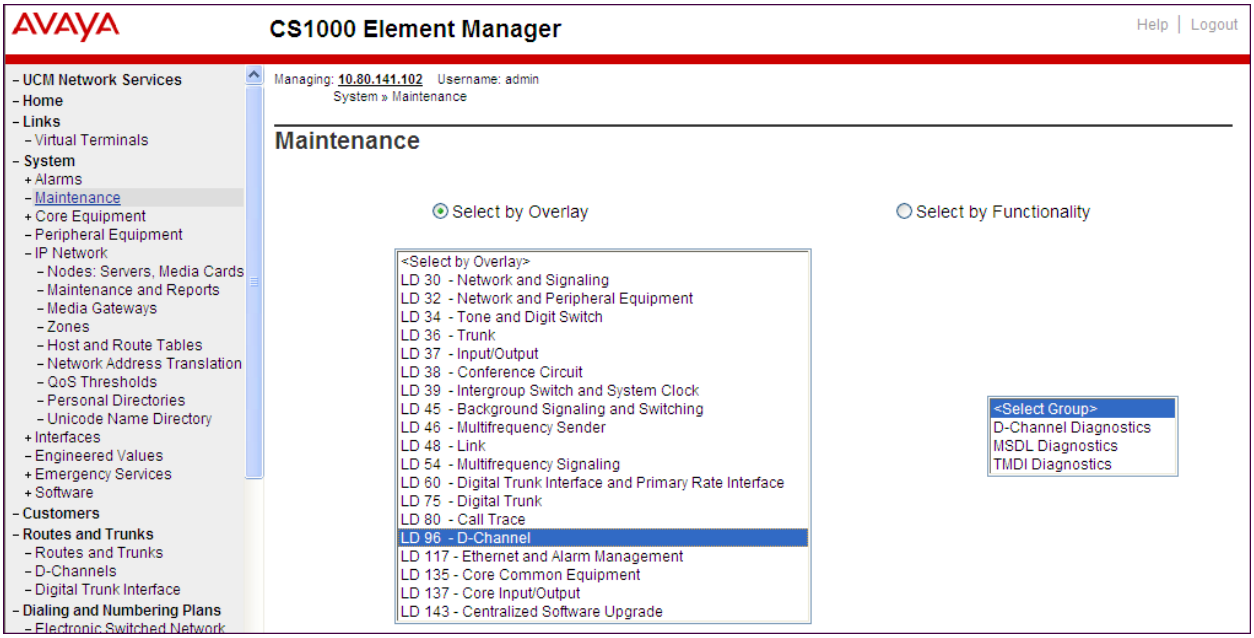
The following screen shows a means to view IP UNIStim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**. At the time this screen was captured, the UNIStim telephone with IP address **10.80.150.111** was involved in an active call with the CenturyLink SIP Trunk service.



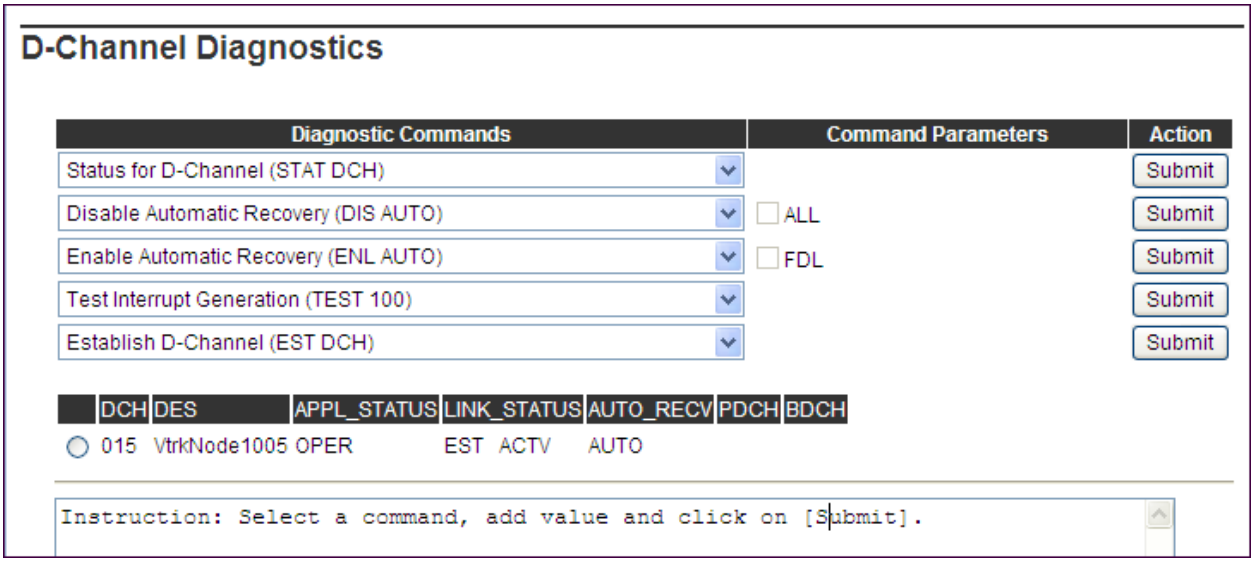
8.1.2. System Maintenance Commands

A variety of system maintenance commands are available by navigating to **System → Maintenance** using Element Manager. The user can navigate the maintenance commands using either the **Select by Overlay** approach or the **Select by Functionality** approach.

The following screen shows an example where **Select by Overlay** has been chosen. The various overlays are listed, and the **LD 96 – D-Channel** is selected.

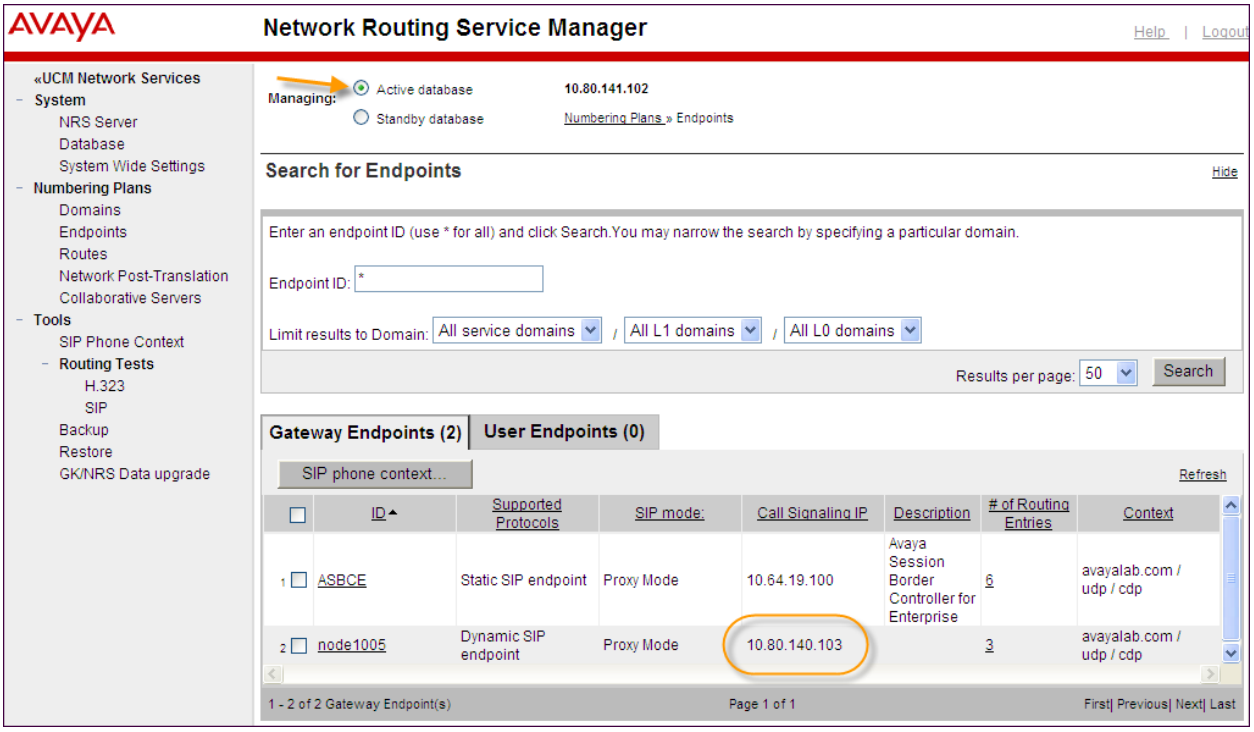


On the preceding screen, **if D-Channel Diagnostics** is selected on the right, a screen such as the following is displayed. D-Channel number 15, which is used in the sample configuration, is established **EST** and active **ACTV**.

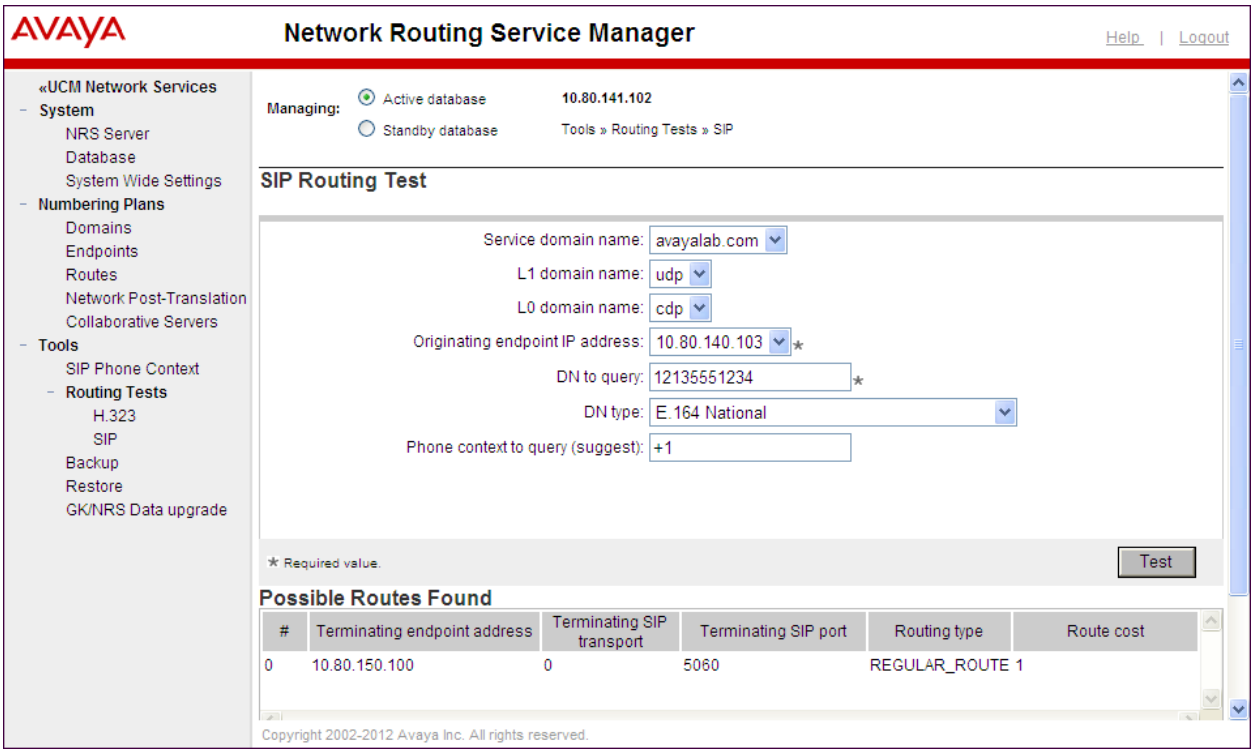


8.1.3. Network Routing Service Routing Verification

Verify the Signaling Server has successfully registered with the Network Routing Server. From the **Network Routing Server Manager**, navigate to **Numbering Plans → Endpoints**. Click on the radio button of the **Active** database. On the **Gateway Endpoints** tab, verify the IP address of the Signaling Server node is in the **Call Signaling IP** column as shown below.



Verify the call routing administration on the NRS by executing the Routing Tests. From the Network Routing Service Manager, navigate to **Tools → Routing Tests → SIP**. Populate the field for the call parameters of interest. For example, the following screen shows a call routing test for an outbound call to PSTN via CenturyLink. Under **Possible Routes Found**, observe the call will route via Avaya SBCE to CenturyLink.



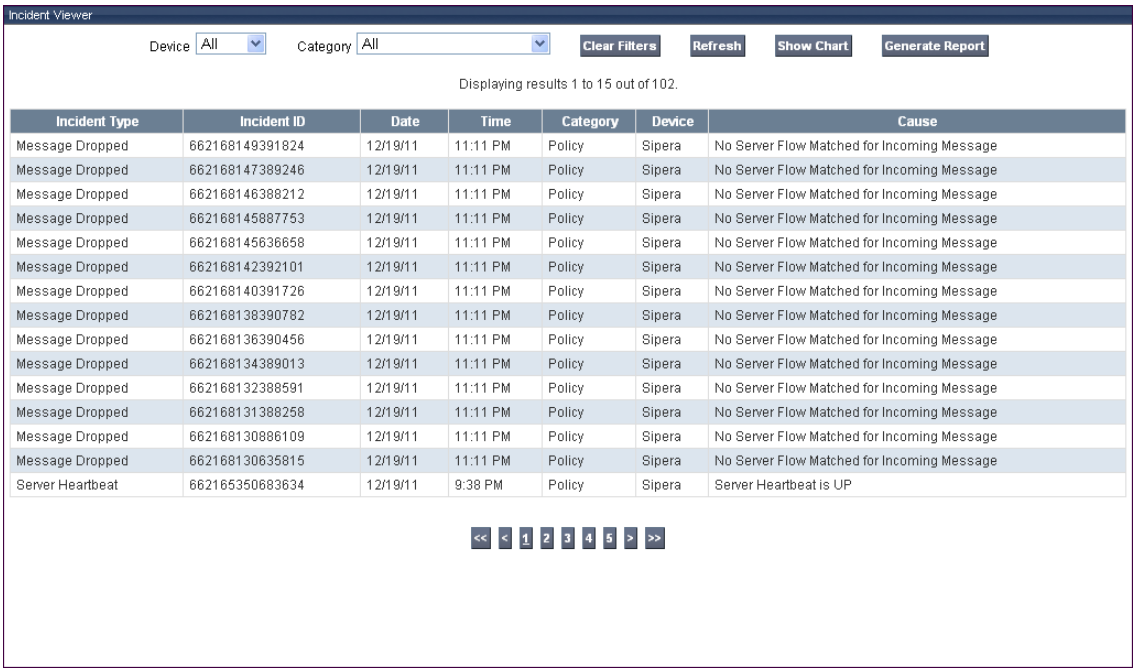
8.2. Avaya Session Boarder Controller for Enterprise Verification

This section contains verification steps that may be performed using the Avaya Session Border Controller for Enterprise.

8.2.1. Incidents

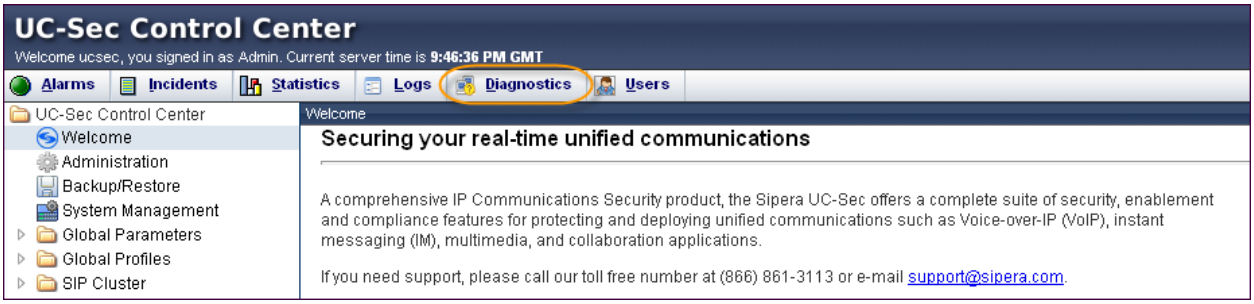
The Incidents Log Viewer display alerts captured by the Avaya SBCE appliance. Select the **Incidents** link along the top of the screen.

The following screen shows an example SIP messages that do not match a Server Flow for an incoming message.

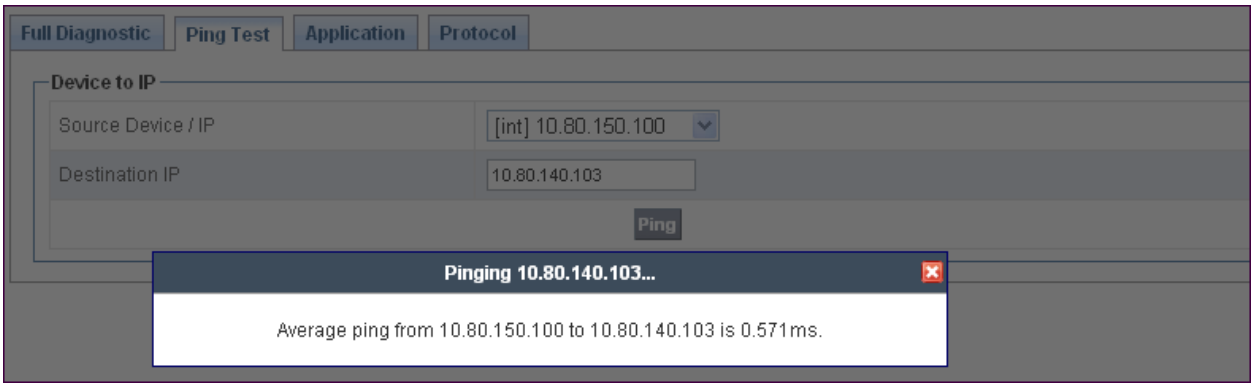


8.2.2. Diagnostics

The Diagnostics tool allows for PING tests and displays application and protocol use. Select the **Diagnostics** link along the top of the screen.

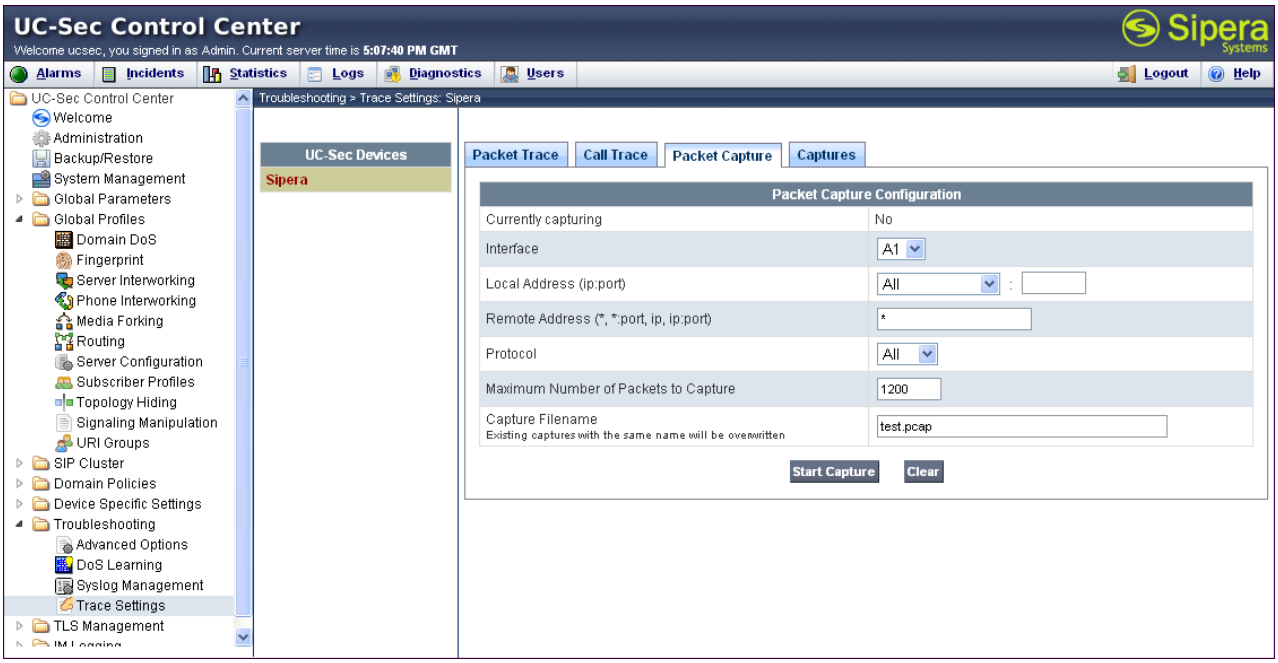


The following screen shows an example PING to the NRS server from the internal signaling interface of the Avaya SBCE.

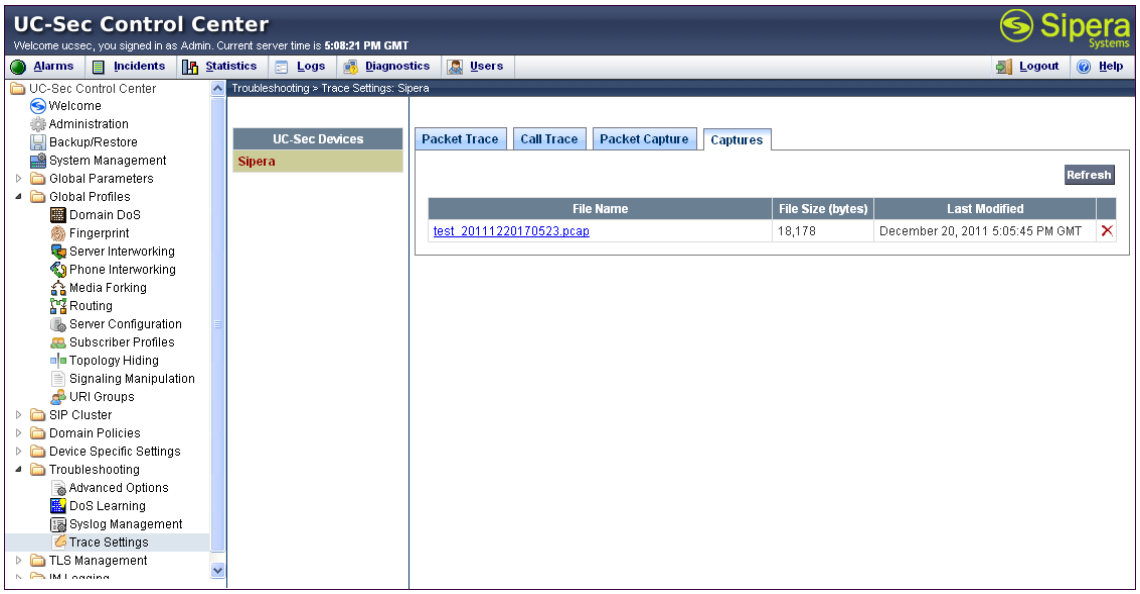


8.2.3. Trace Settings

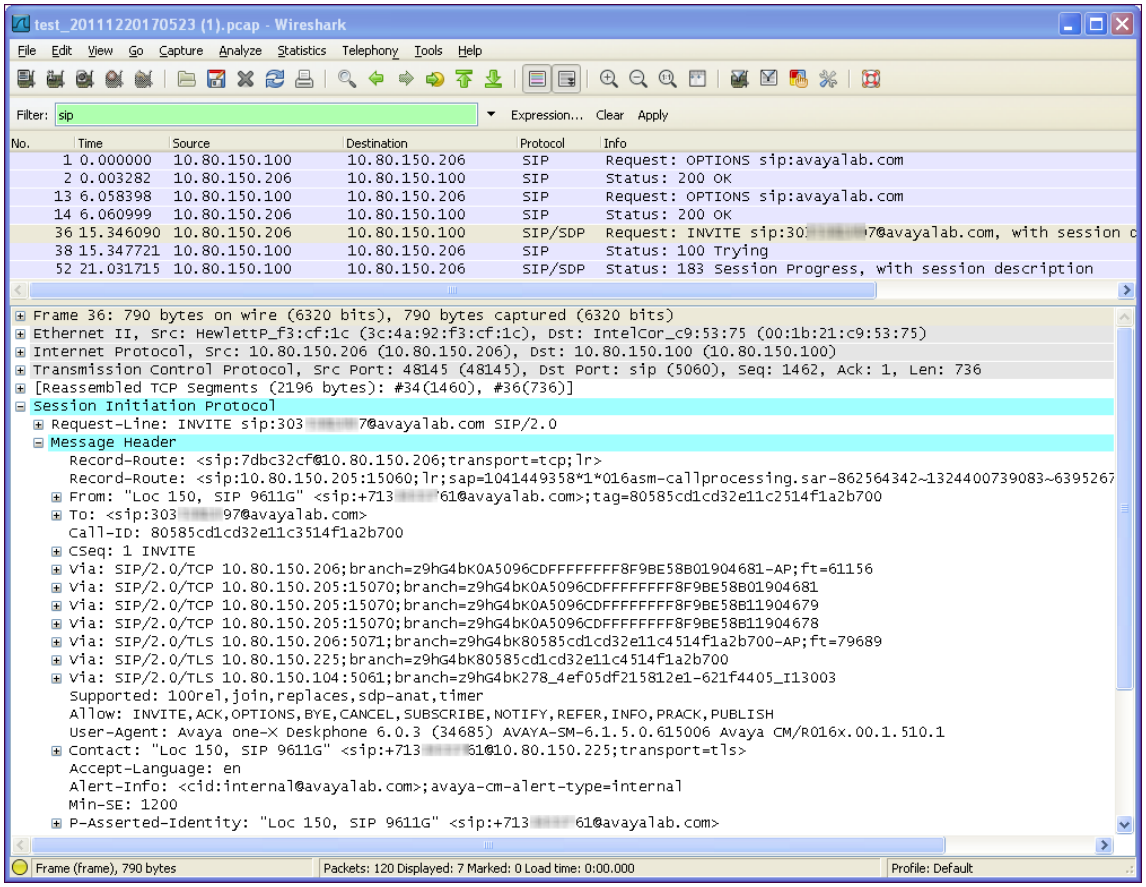
The Trace Settings tool is for configuring and displaying call traces and packet captures for the Avaya SBCE. Navigate to **Troubleshooting → Trace Settings** as shown below. The following screen shows an example packet capture on interface **A1** with a **Maximum Number of Packets to Capture** set to **1200**. The **Capture Filename test.pcap** will be created once the **Start Capture** button is pressed.



The following screen shows a completed packet capture.



The packet capture file can be downloaded and viewed using a Network Protocol Analyzer like Wireshark:



9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya SBCE and Avaya Communication Server 1000E to the CenturyLink SIP Trunk (Legacy Qwest) Service. The CenturyLink SIP Trunk is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The CenturyLink SIP Trunk provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

10. Additional References

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

[1] *Avaya Communication Server 1000E Installation and Commissioning,* November 2010, Document Number NN43041-310.
[2] *Feature Listing Reference Avaya Communication Server 1000,* November 2010, Document Number NN43001-111, 05.01.
[3] *RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/*
[4] *Signaling Server IP Line Applications Fundamentals Avaya Communication Server 1000,* Document Number NN43001-125, 03.09 October 2011
[5] *Network Routing Service Fundamentals Avaya Communication Server 1000,* Document Number NN43001-130, 03.10 September 2011
[6] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000,* Document Number NN43001-315, 05.18 January 2012
[7] *SIP Software for Avaya 1100 Series IP Deskphones-Administration* , Document Number NN43170-600, Standard 04.02 December 2011
[8] *UC-Sec Install Guide* (102-5224-400v1.01)
[9] *UC-Sec Administration Guide* (010-5423-400v106)

Appendix A

Included below is the Sigma Script used during the compliance testing. The contents have been modified to mask the external IP address and the routable phone number of the Diversion header.

```
// Topology Hiding of PAI header within 180 Ringing response

within session "ALL"
{
 act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
   %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com","205.xxx.xxx.92:5060");
  }
 }

/* Topology Hiding of PAI header for subsequent re-INVITEs; Create a Diversion header to allow
call-fwd; Remove unwanted headers and convert the SIP content from multipart/mixed to SDP */

within session "ALL"
{
 act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
// Topology Hiding

   %HEADERS["p-asserted identity"][1].regex_replace("avayalab\.com","205.xxx.xxx.92:5060");

//Create a Diversion Header

    %HEADERS["Diversion"][1] = "<sip:3035557104@205.xxx.xxx.92:5060>";

// Remove unwanted Headers

   remove(%HEADERS["Alert-Info"][1]);
   remove(%HEADERS["X-nt-e164-clid"][1]);

// Remove unwanted mimes from the body.

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

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

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