Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Cincinnati Bell eVantage IP Service with Avaya Communication Server 1000E 7.5, Avaya Aura® Session Manager 6.2, Avaya Session Border Controller for Enterprise 4.0.5 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Cincinnati Bell eVantage IP Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E, Avaya Aura® Session Manager, Avaya Session Border Controller for Enterprise and various Avaya endpoints.

Cincinnati Bell 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 via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration of Avaya Communication Server 1000E release 7.5 Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5 (Avaya SBCE) integration with Cincinnati Bell eVantage IP Service.

In the sample configuration, the Avaya Session Border Controller for Enterprise is used as an edge device between Avaya Customer Premise Equipment (CPE) and Cincinnati Bell eVantage IP Service. 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 Cincinnati Bell eVantage IP Service access method.

The Cincinnati Bell eVantage IP Service solution is a turn-key business trunking solution for customers. Cincinnati Bell eVantage IP Service provides customers with a single IP connection that converges voice and data services to drive optimization, reduce costs, and offer enhanced features not typically available in the traditional PSTN network. Voice services, such as local, long distance and toll free calling, as well a high speed data and Internet services, are the primary applications of the Cincinnati Bell eVantage solution.

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), Session Manager, and Avaya SBCE to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to Cincinnati Bell eVantage IP 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, and outbound toll-free
- Codecs G.729A, G.729B and G.711MU
- DTMF transmission using RFC 2833
- G711 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

Items not supported or not tested included the following:

- Inbound toll-free, operator, operator services (0 + 10 digits) and emergency calls (911) are supported but were not tested as part of the compliance test
- Calls forwarded off-net were not supported on the test circuit used for the compliance test, but Cincinnati Bell eVantage IP Service production environment does support these types of calls.
- SIP REFER method is not supported by Avaya CS1000E
- CS1000E Mobile-X features were not tested

2.2. Test Results

Interoperability testing of Cincinnati Bell eVantage IP Service 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/Cincinnati Bell eVantage IP Service solution. It is listed here simply as an observation.
- **T.38 Fax**: At the time of original publication of these Application Notes, Cincinnati Bell eVantage IP Service supported fax over T.38 within their local calling area only. Any fax calls placed outside of the Cincinnati Bell local calling area will be transferred using G.711 codec. The recommended workaround is to configure the CS1000E fax endpoints to use the G.711codec for outbound calling. See **Section 5.7.3**

Cincinnati Bell eVantage IP Service passed compliance testing.

2.3. Support

For technical support on the Cincinnati Bell eVantage IP Service, contact Cincinnati Bell using the Customer Care links at www.Cincinnati Bell.com.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via an Internet connection to the Cincinnati Bell eVantage IP Services. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an Avaya SBCE provides NAT functionality and SIP header manipulation. The Avaya SBCE receives traffic from Cincinnati Bell eVantage IP Service on port 5060 and sends traffic to the Cincinnati Bell eVantage IP Service using destination port 5060, using the UDP protocol. For security reasons, any actual public IP addresses used in the configuration have been 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.

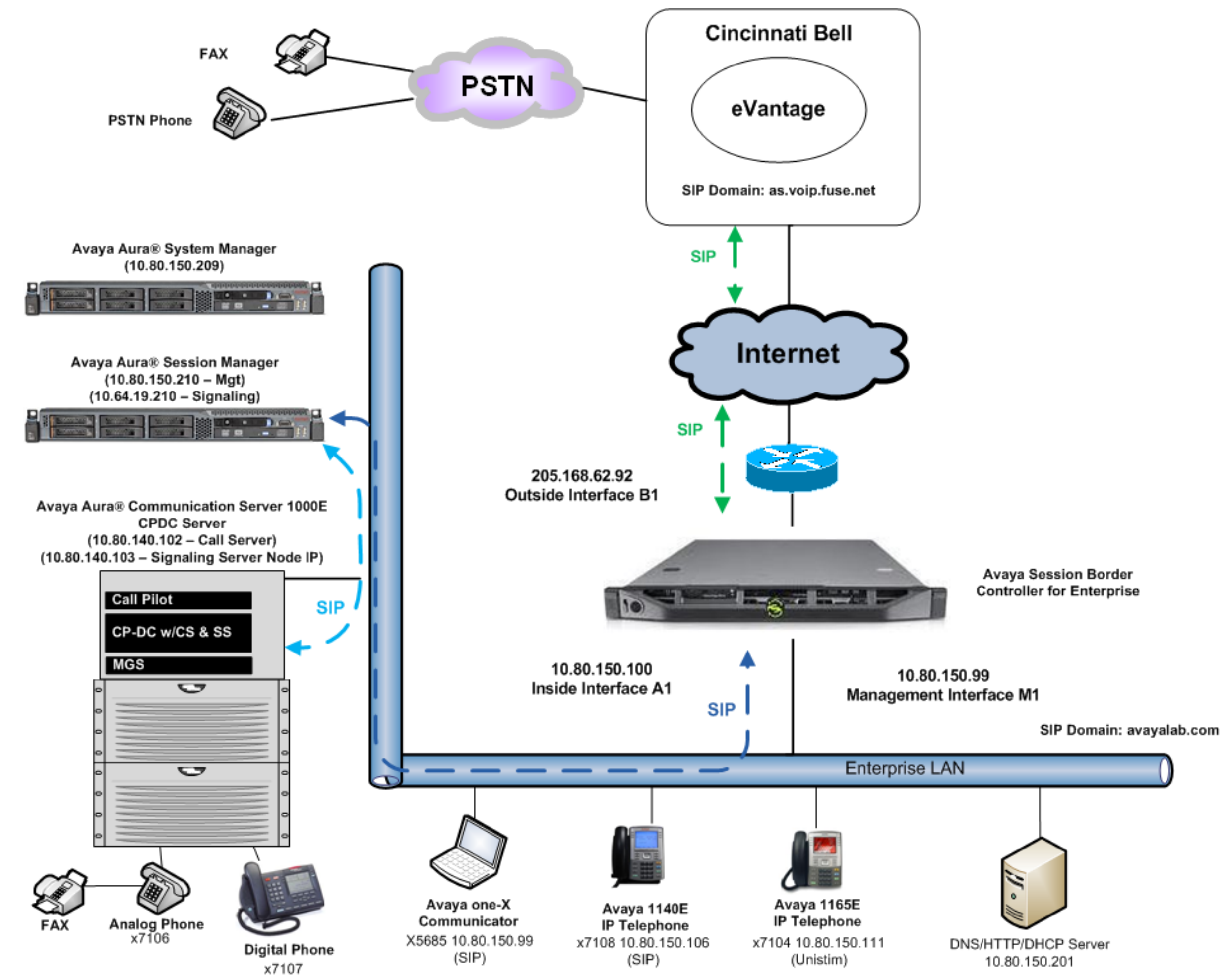


Figure 1: Avaya Interoperability Test Lab Configuration

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_20120919 • SSG Server: 7.50.17 GA • SLG Server: 7.50.17 GA
Communication Server 1000E Media Gateway	CSP Version: MGCC CD03 MSP Version: MGCM AB02 APP Version: MGCA BA15 FPGA Version: MGCF AA19 BOOT Version: MGCB BA15 DSP1 Version: DSP4 AB06 BCSP Version: MGCC CD01
Avaya Session Border Controller for Enterprise	4.0.5Q18
Avaya 1165E (UNIStim)	0626C8A
Avaya 1140E (SIP)	04.03.12.00
Avaya one-X Communicator (SIP)	CS6.1.1.02 SP1 36207
Avaya M3904 (Digital)	n/a
Avaya 6210 Analog Telephone	n/a
Cincinnati Bell eVantage IP Service Components	
Component	Release
BroadSoft	Version 17

Table 1: Equipment and Software Tested

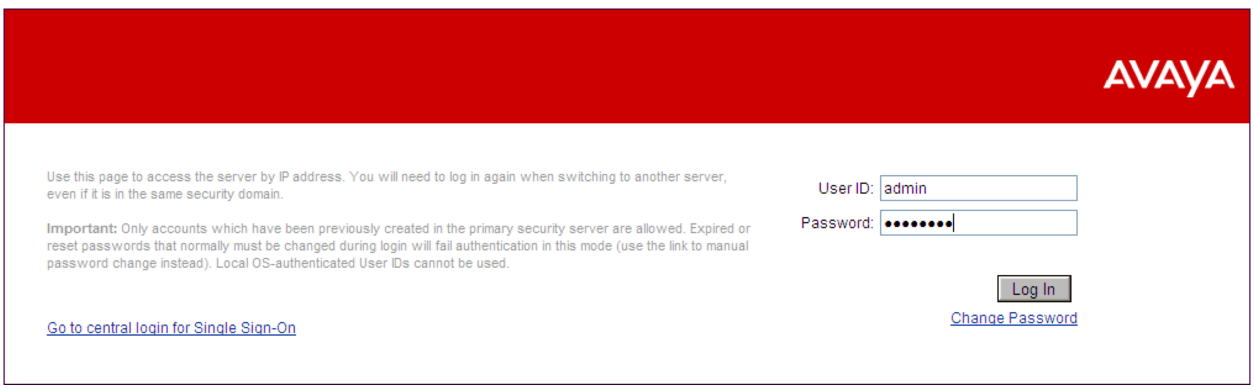
The specific configuration above was used for the compatibility testing.

5. Configure Avaya Communication Server 1000E

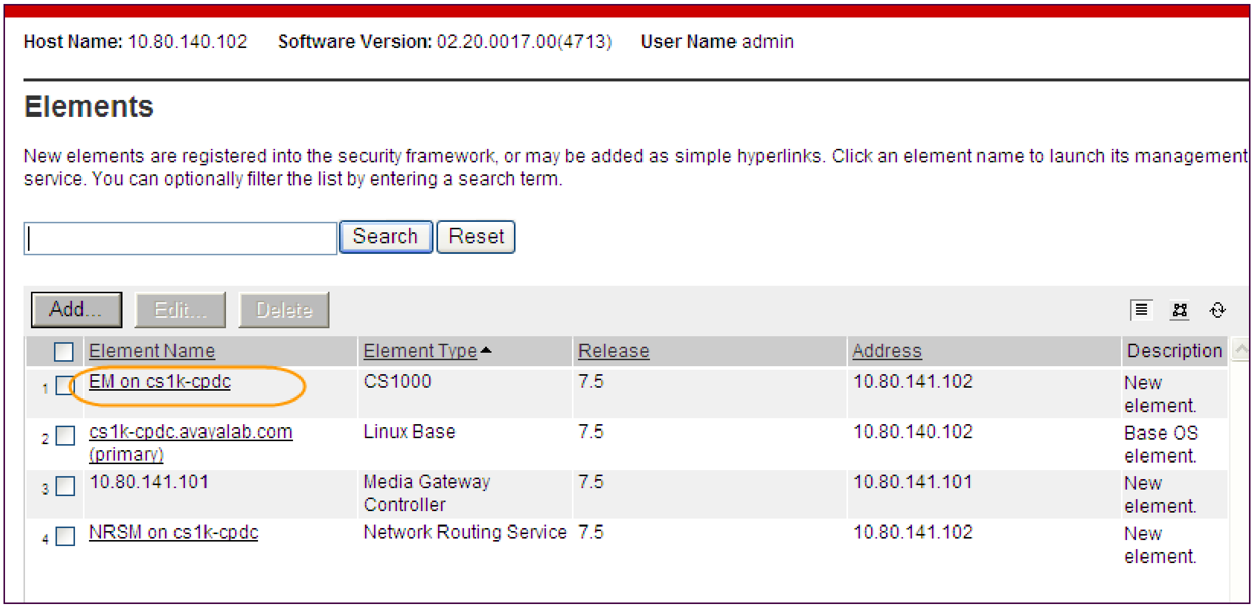
This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to Cincinnati Bell over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed as a co-resident system with the SIP Signaling Server, and Call Server 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 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 11**.

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**.



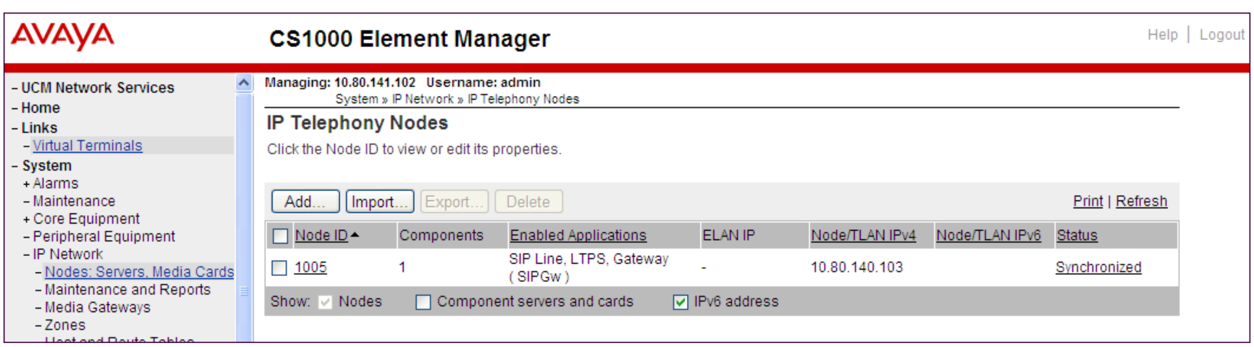
5.1. Administer an IP Telephony Node

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

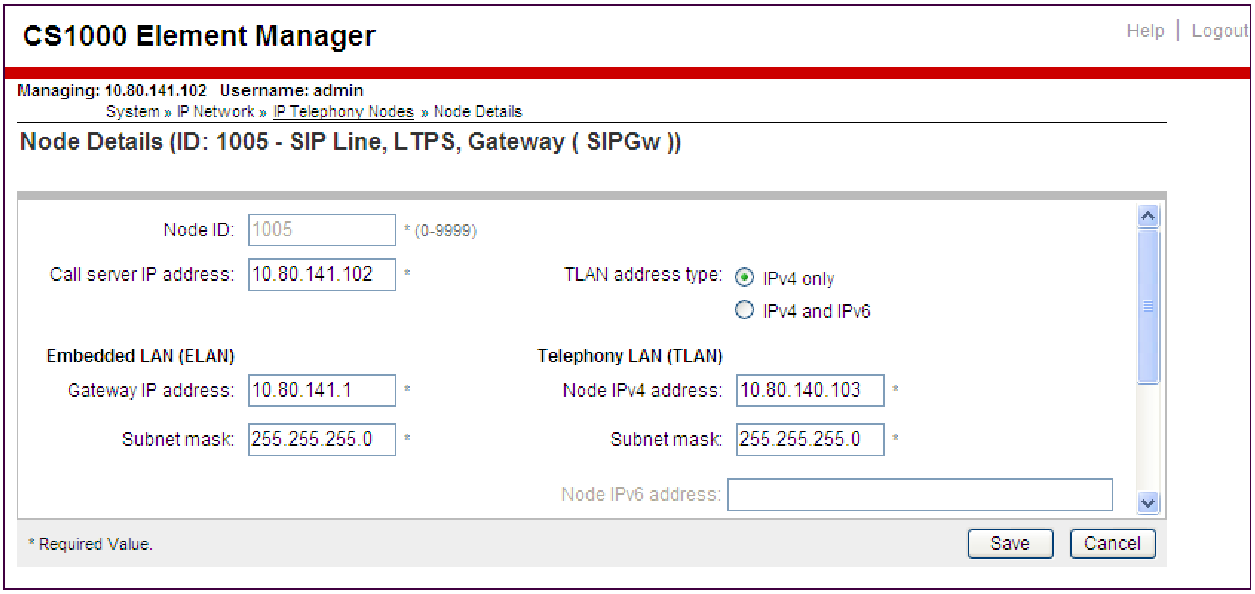
5.1.1. Obtain Node IP Address

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

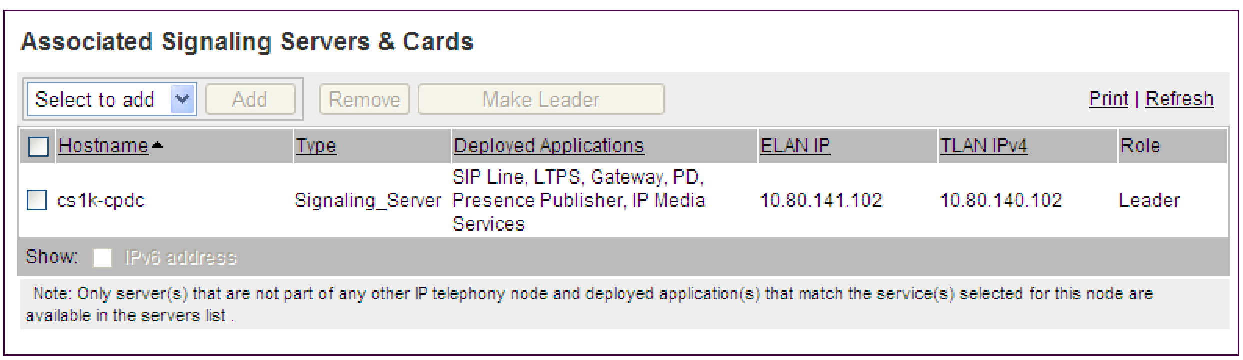
The **IP Telephony Nodes** page is displayed as shown below. Click **<Node id>** in the Node ID column to view details of the node. In the sample configuration, **Node ID 1005** was used.



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 be needed when configuring Session Manager with a SIP Entity for the CS1000E in **Section 6.5**.

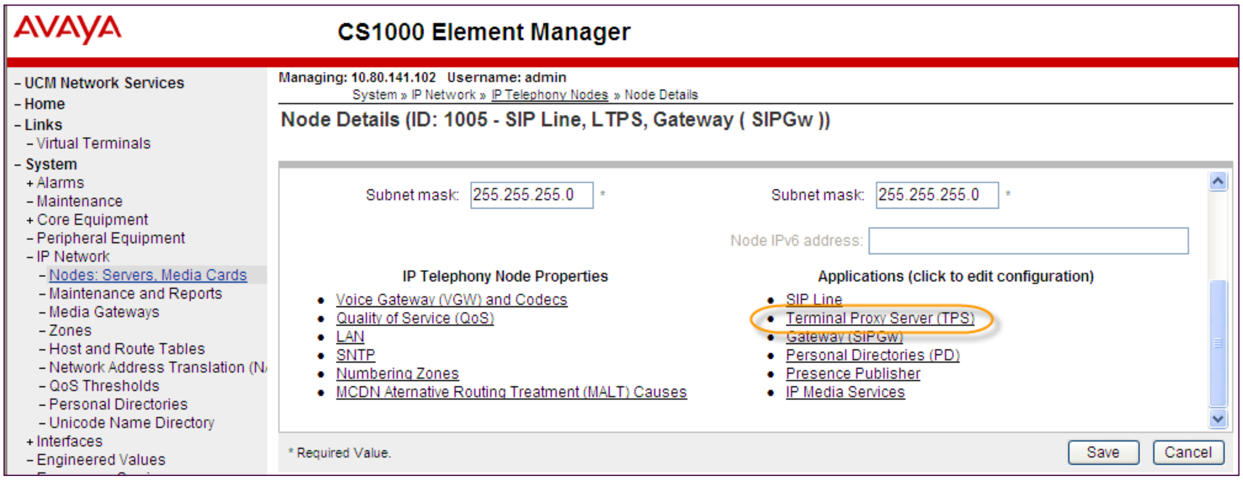


The following screen shows the **Associated Signaling Servers & Cards** heading at the bottom of the screen, simply to document the configuration.

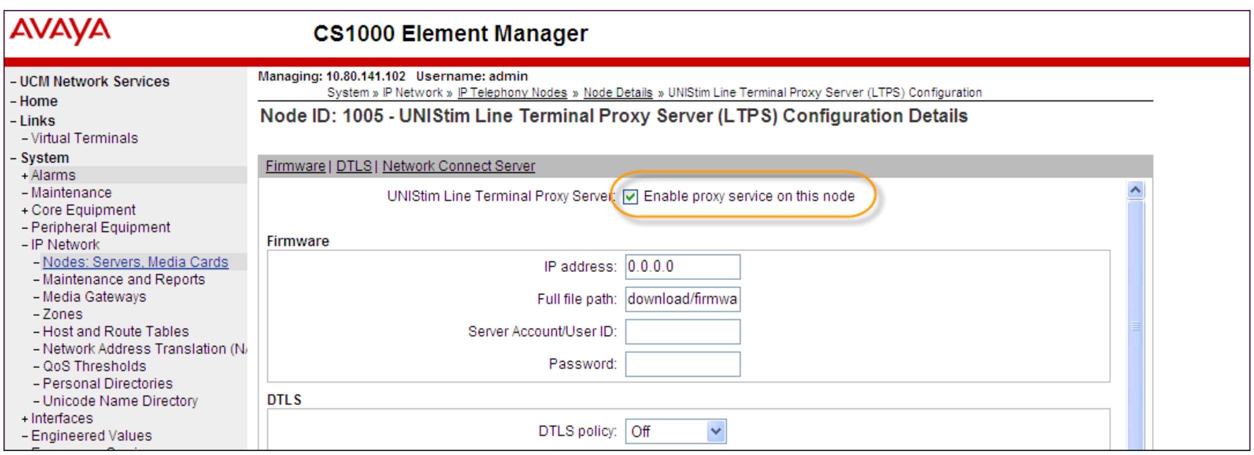


5.1.2. Terminal Proxy Server (TPS)

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

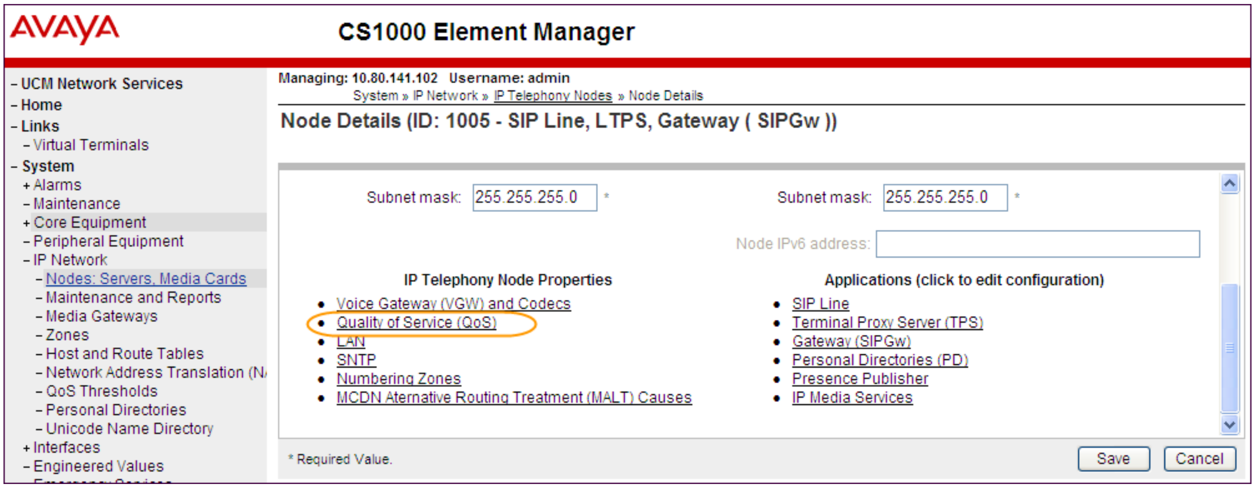


Check the **UNIStim Line Terminal Proxy Server** check box and then click the **Save** button (not shown).

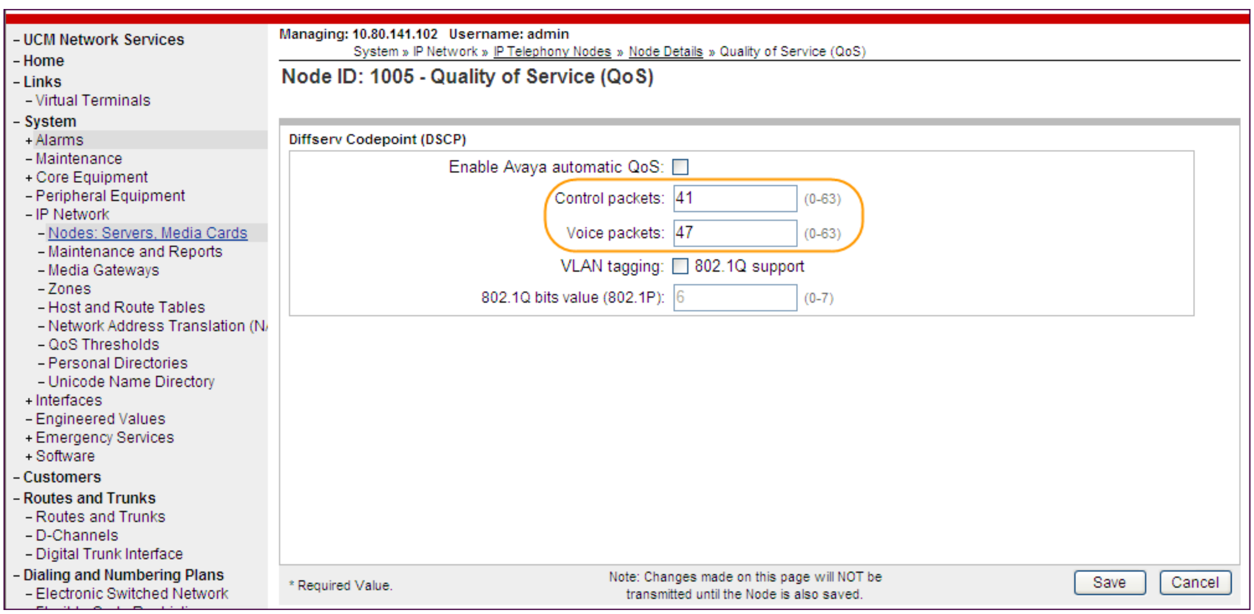


5.1.3. Quality of Service (QoS)

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

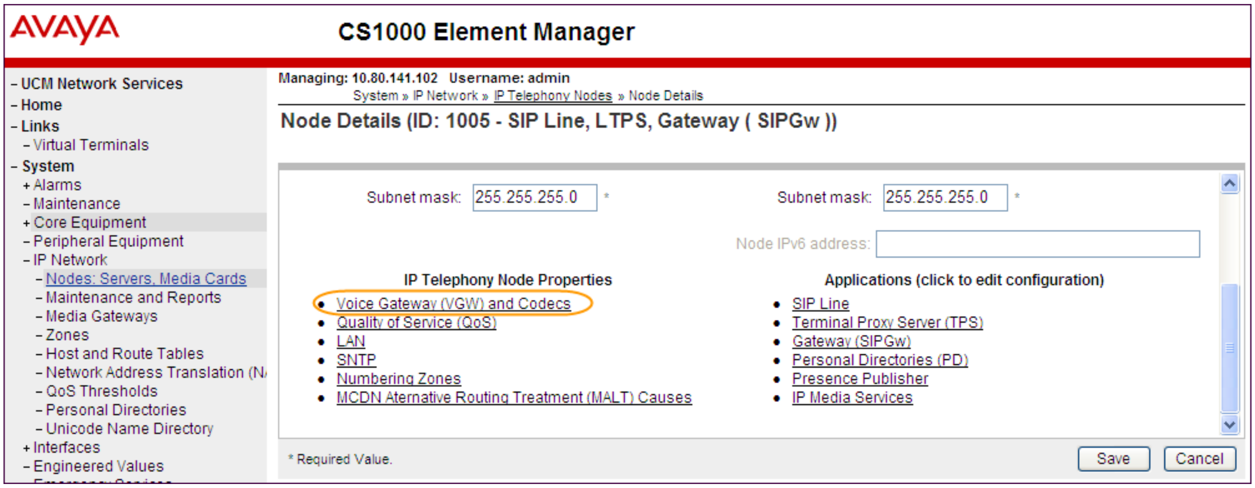


Set the **Control packets** and **Voice packets** values to the desired Diffserv settings required on the internal network. The default Diffserv values are shown below. Click on the **Save** button.

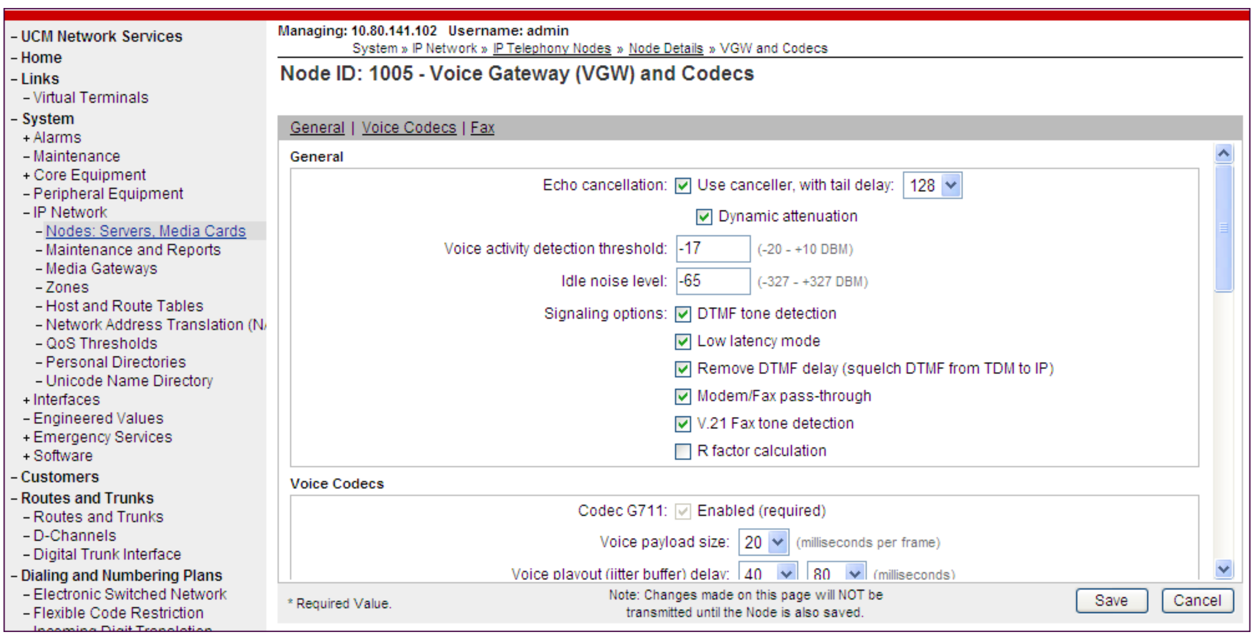


5.1.4. Voice Gateway and Codecs

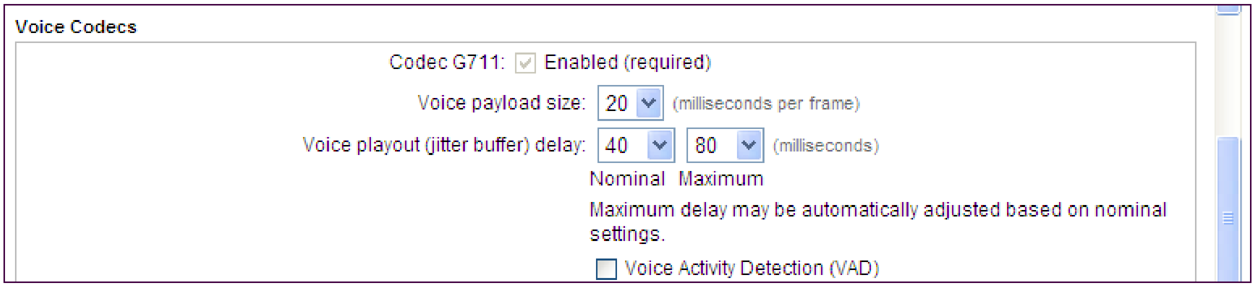
On the **Node Details** screen, scroll down in the top window and select the **Voice Gateway (VGW) and Codecs** link as shown below.



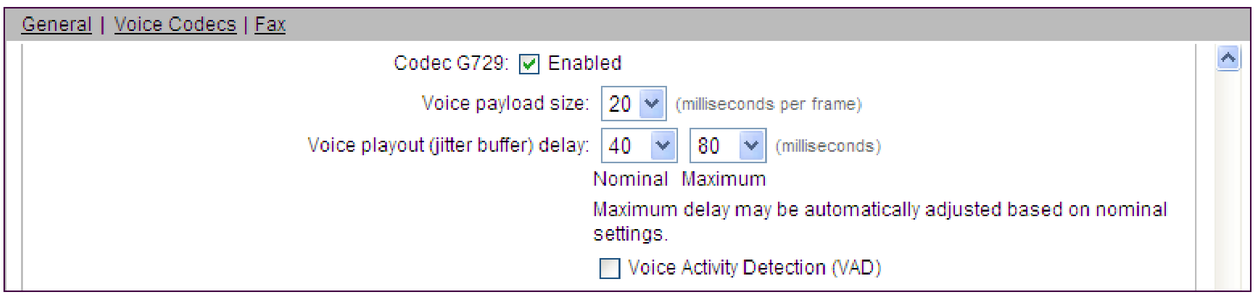
The following screen shows the General parameters used in the sample configuration.



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.

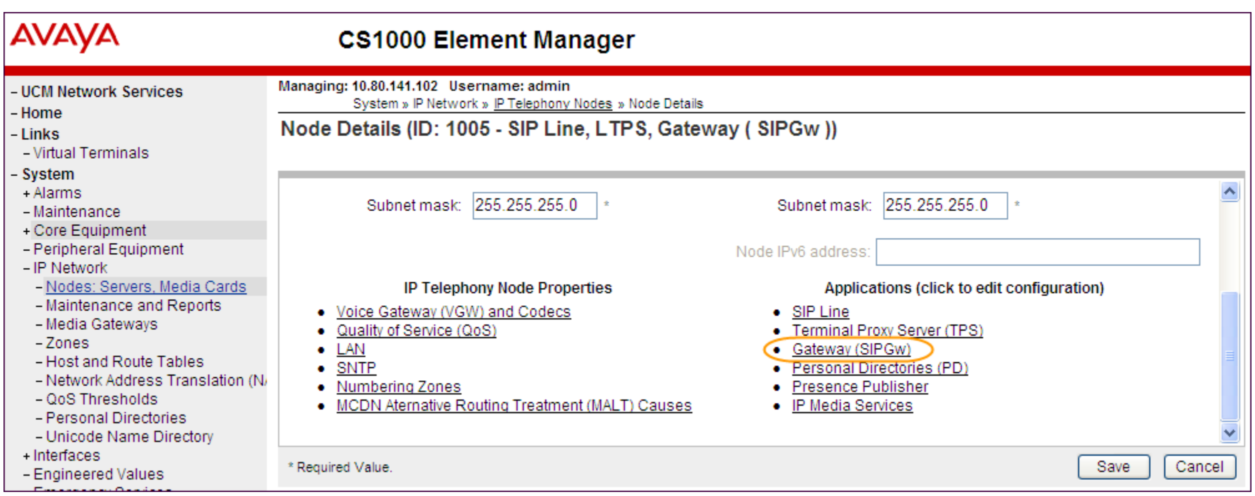


For the **Codec G.729**, ensure that the **Enabled** box is checked, and the **Voice Activity Detection (VAD)** box is un-checked. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order. During compliance testing, the G.729B codec was also tested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



5.1.5. SIP Gateway

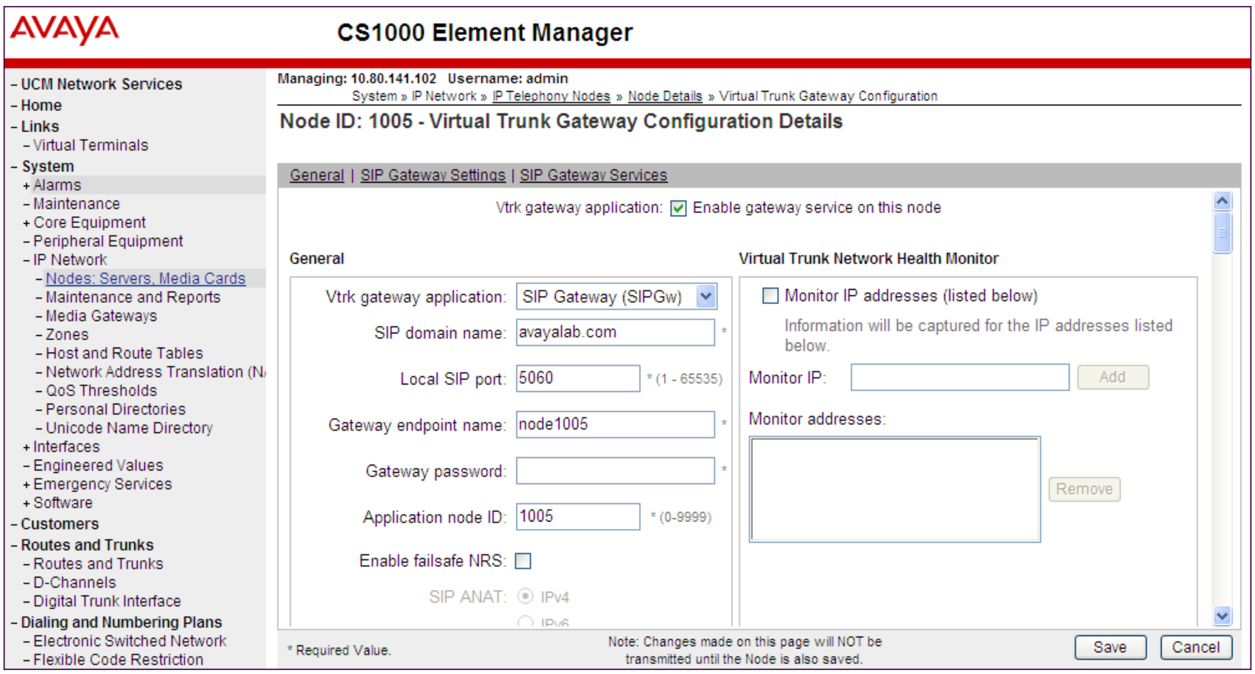
The SIP Gateway is the SIP trunk between the CS1000E and Session Manager. On the **Node Details** screen, scroll down in the top window and select the **Gateway (SIPGw)** link as show below.



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.
- **Application node ID:** Enter **<Node id>**. In the sample configuration, Node **1005** was used matching the node show in **Section 5.1.1**.

The values defined for the sample configuration are shown below.

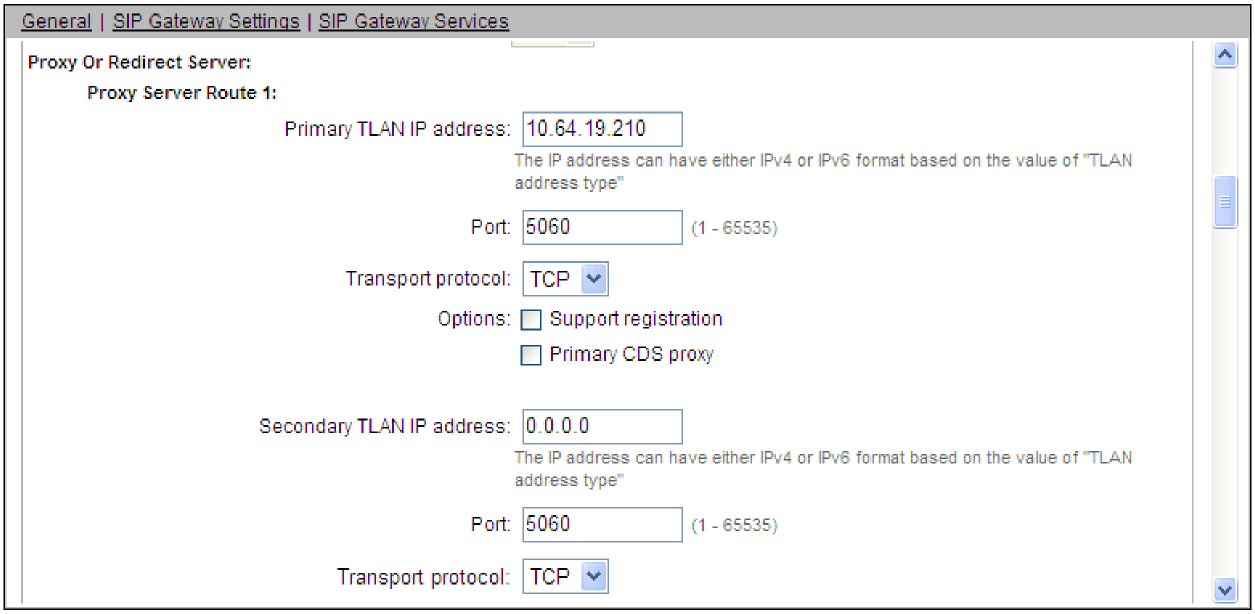


Scroll down to the **SIP Gateway Settings → Proxy or Redirect Server:** section.

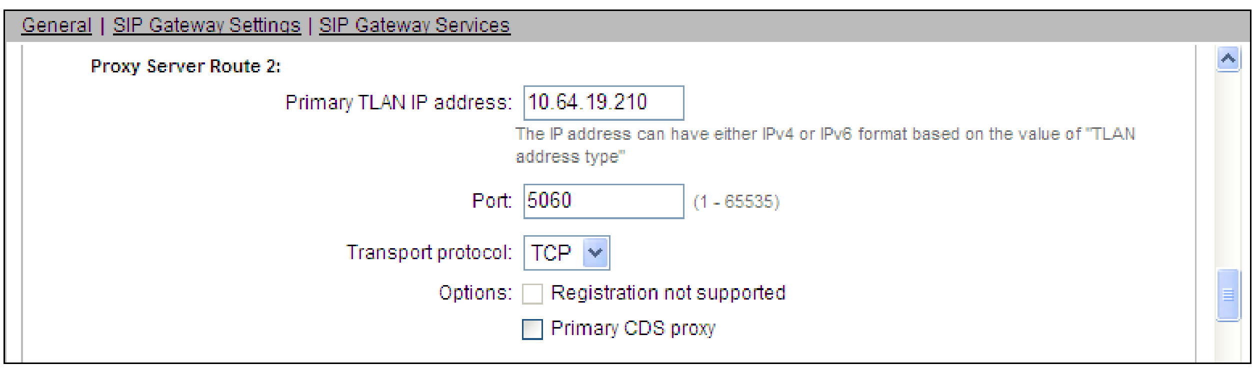
Under **Proxy Server Route 1**, enter the following and use default values for remaining fields.

- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface. In the sample configuration **10.64.19.210** was used.
- **Port:** Enter **5060**
- **Transport protocol:** Select **TCP**

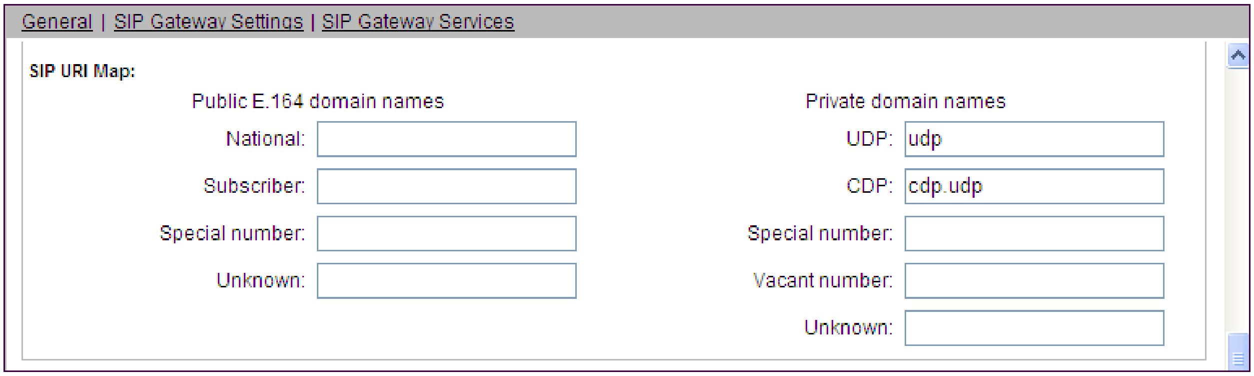
The values defined for the sample configuration are shown below.



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



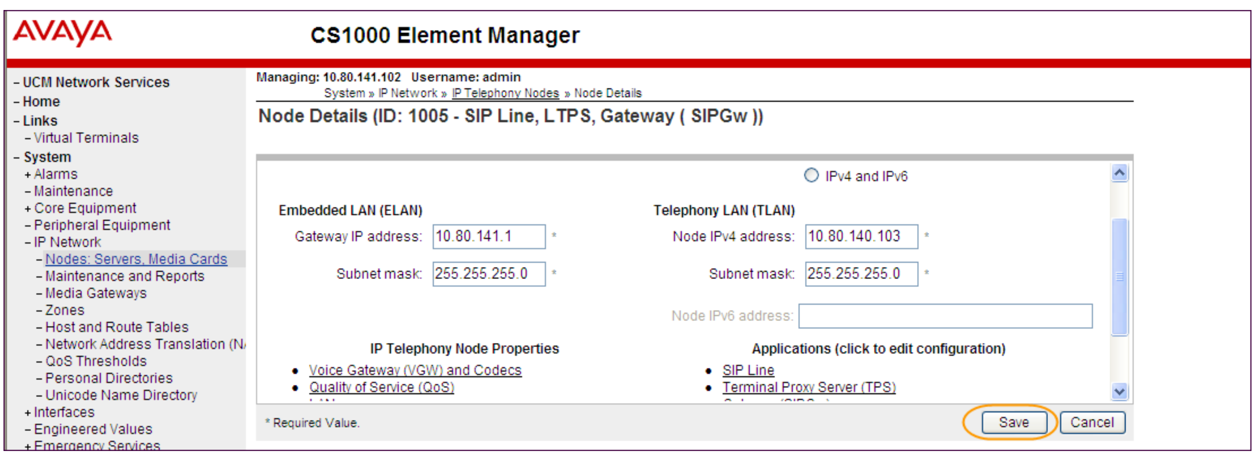
Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. The Avaya CS1000E will put the "string" entered in the **SIP URI Map** in the "phone-context=<string>" parameter in SIP headers such as the To and From headers. If the value is configured to blank,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



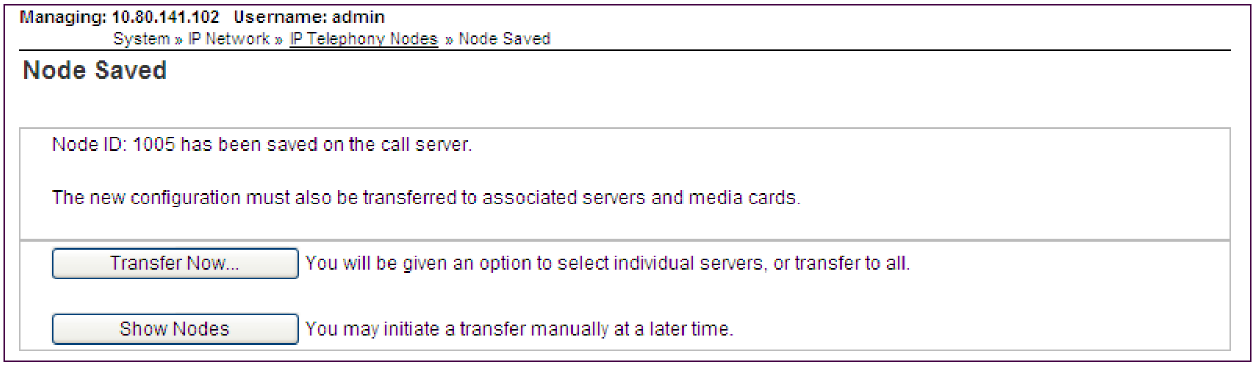
Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen.

5.1.6. Synchronize Node Configuration

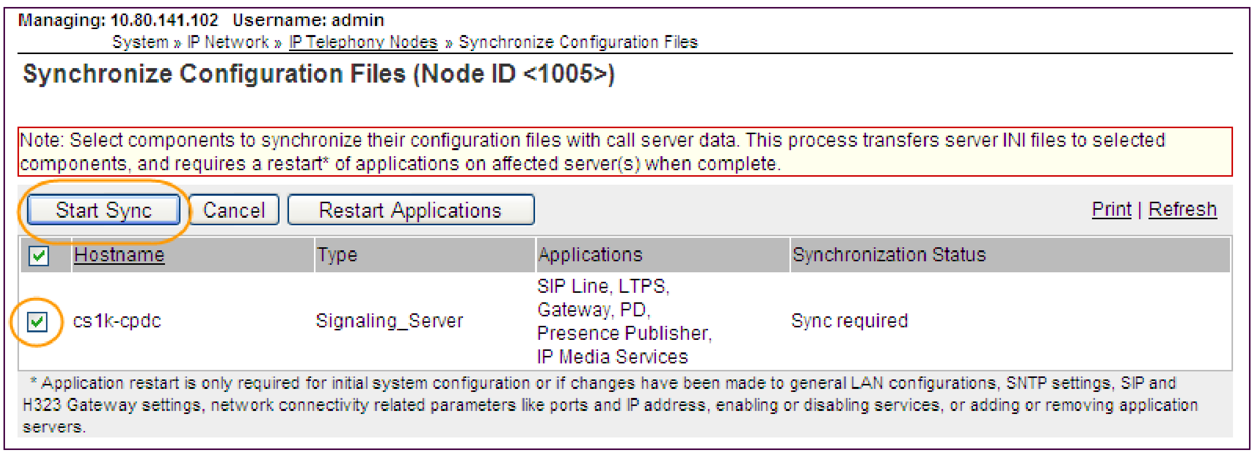
On the **Node Details** screen click **Save** as shown below.



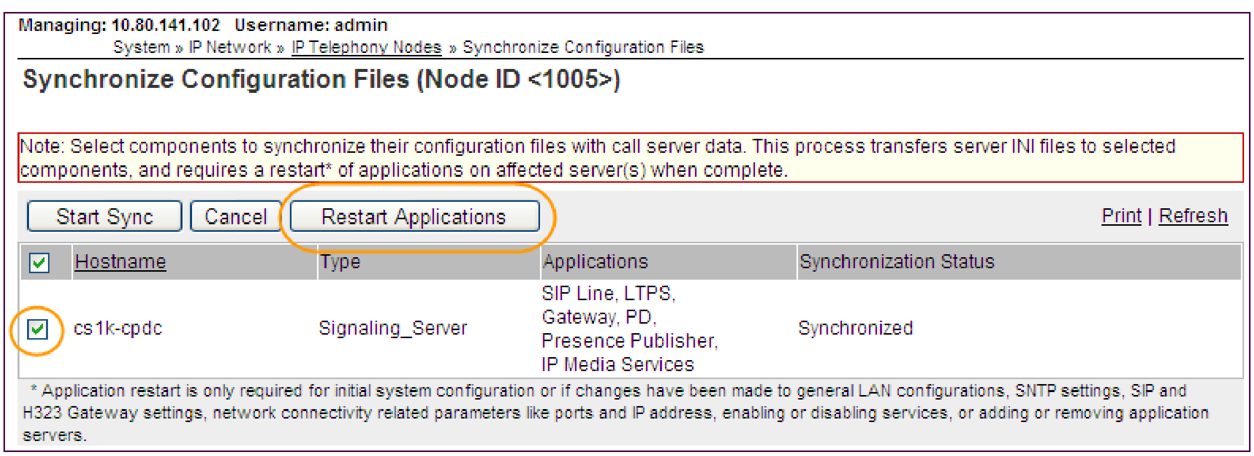
Select **Transfer Now** on the **Node Saved** page as show below.



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.

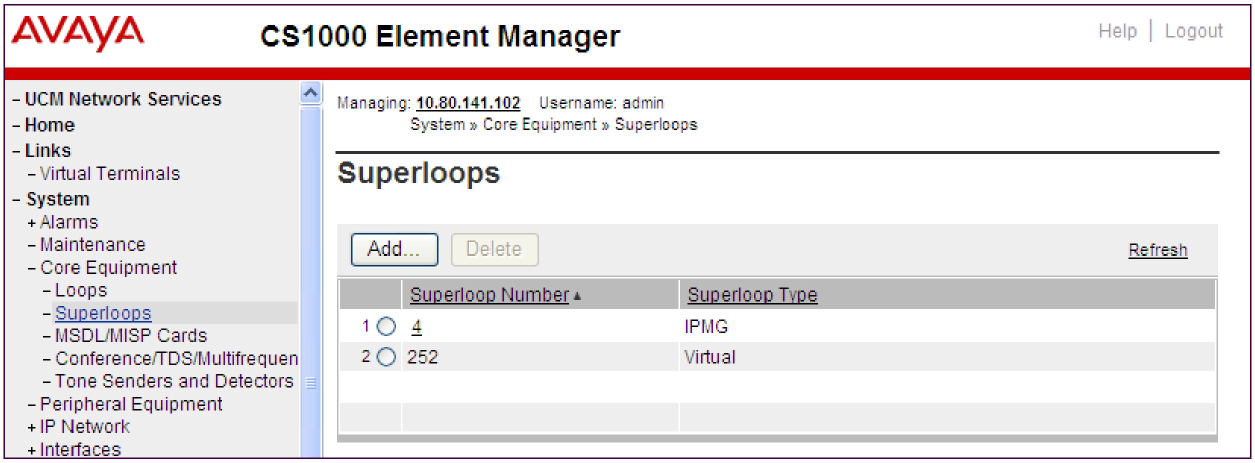


The **Synchronization Status** field will update from **Sync required** (as shown above) to **Synchronized** (as shown below). After synchronization completes, place a check mark next to the appropriate Hostname and click **Restart Applications**.



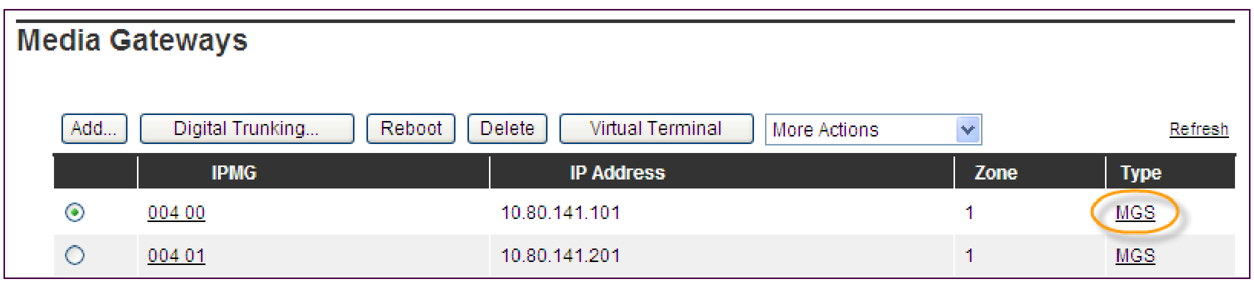
5.2. Virtual Superloops

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.

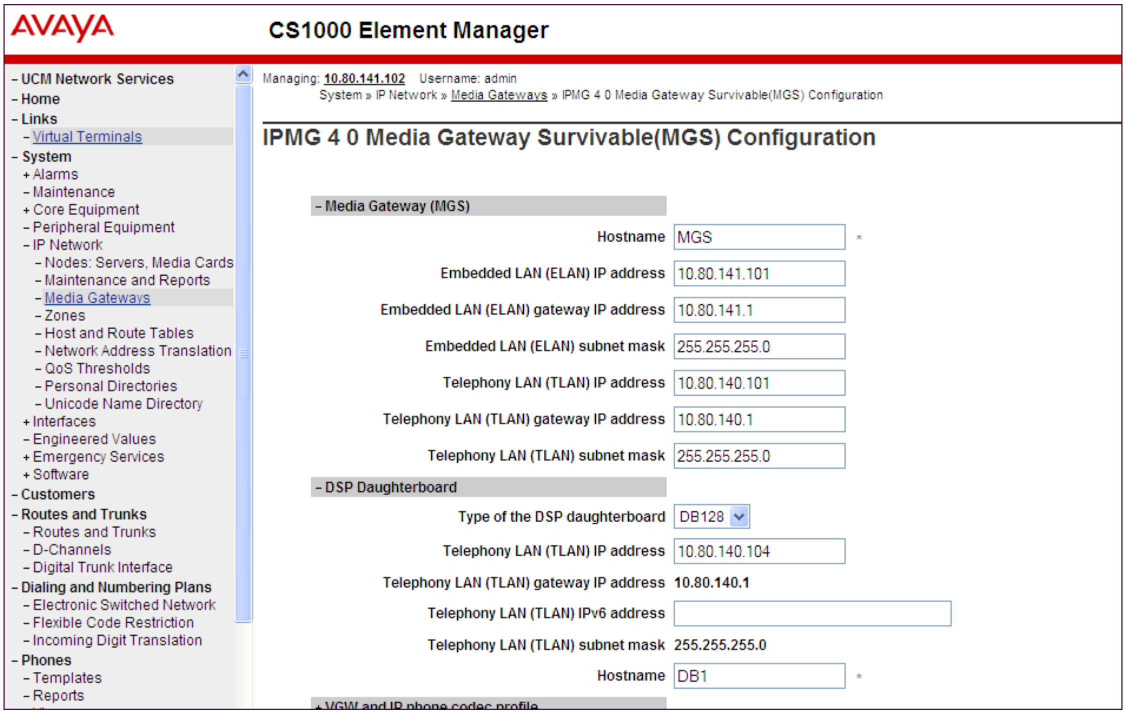


5.3. Media Gateway

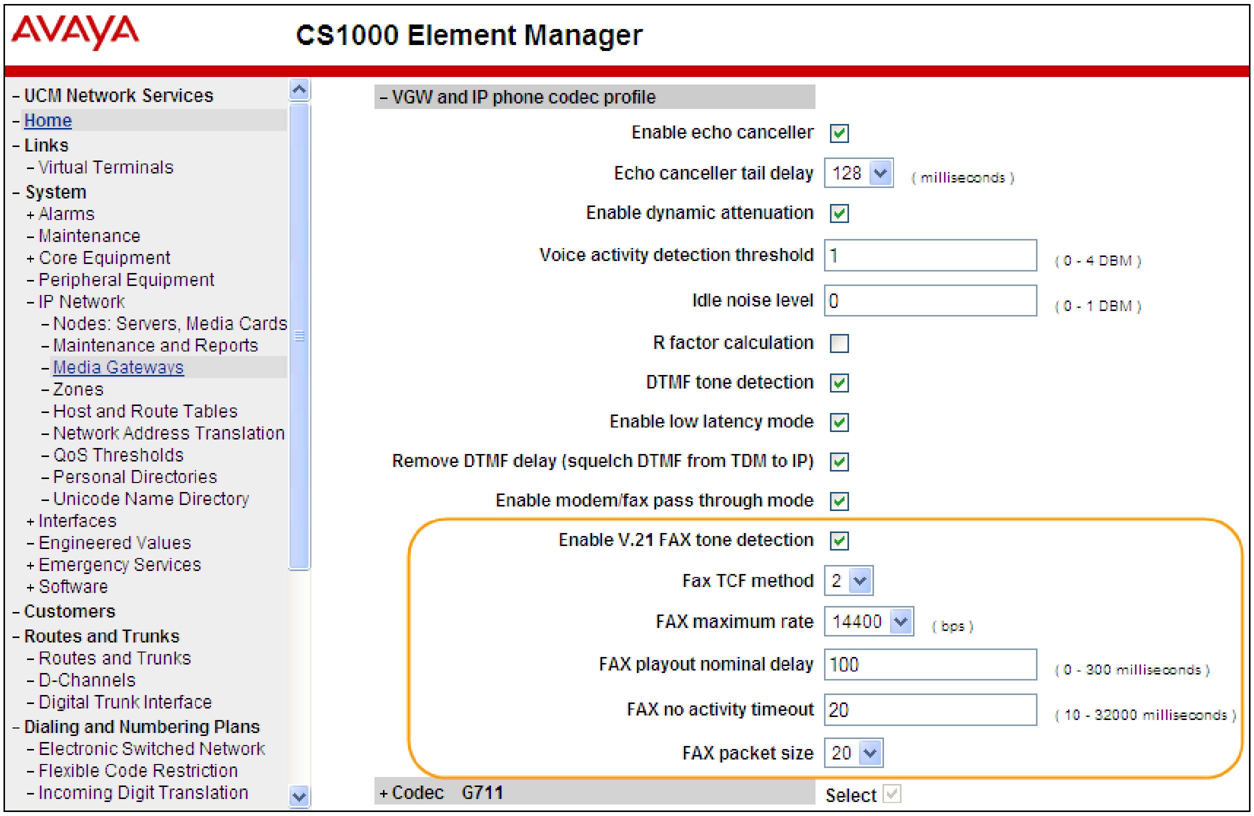
Expand **System → IP Network** on the left panel and select **Media Gateways**. Click the link in the **Type** column for the appropriate Media Gateway to be modified as shown below.



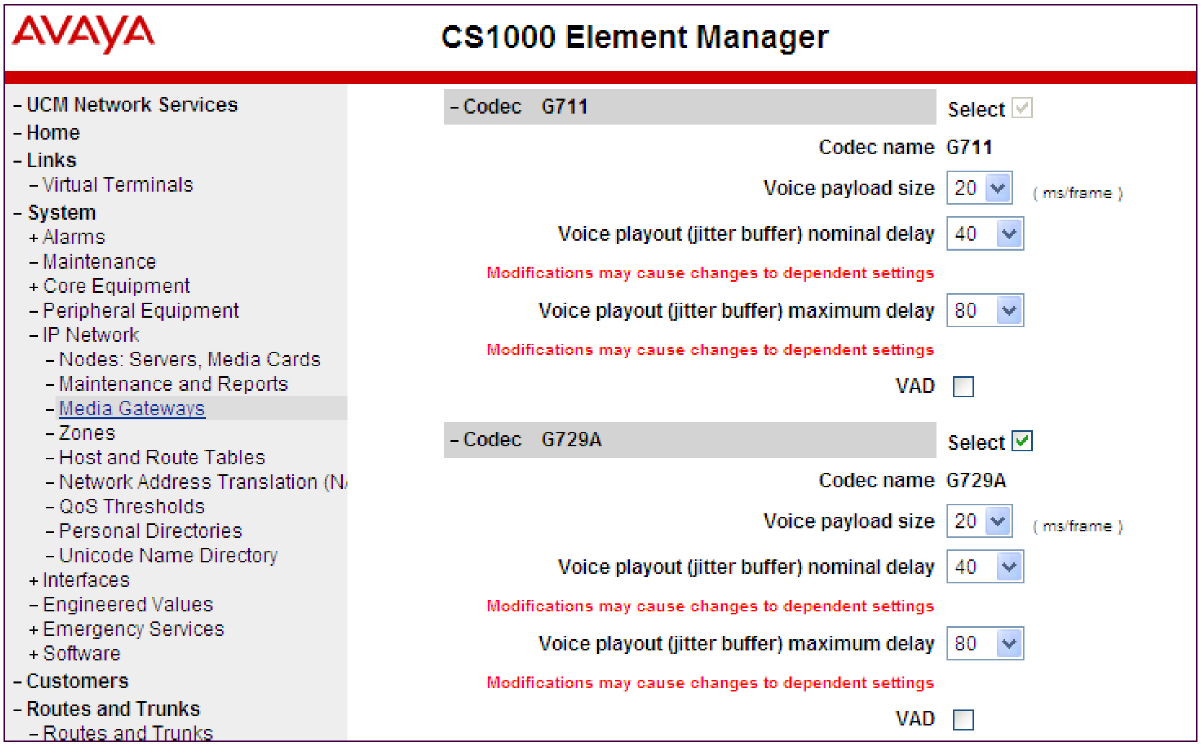
The **IPMG 4 0 Media Gateway Survivable (MGS) Configuration** window appears. The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard 1** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for a call from a digital telephone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



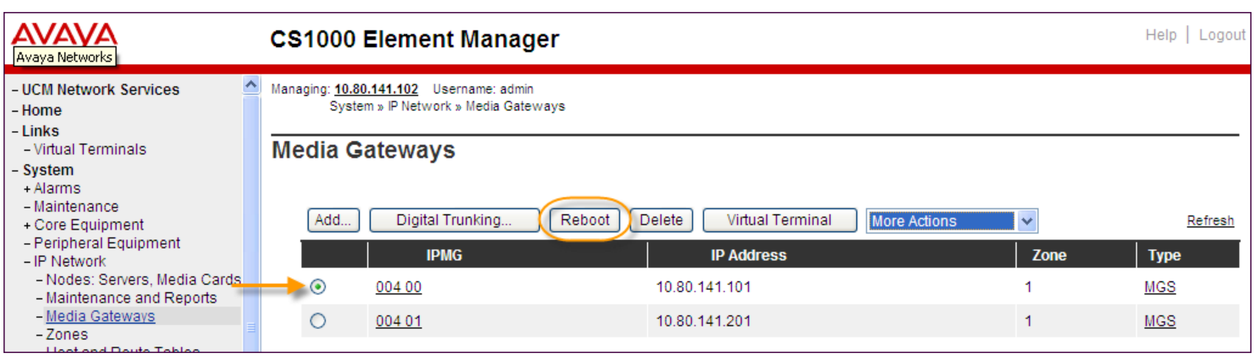
Scroll down to the area of the screen containing **VGW and IP phone codec profile** and expand it. The fax T.38 settings used for compliance testing is shown below.



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 Cincinnati Bell eVantage IP Service 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 Detection (VAD)** box. Scroll down and click **Save** and then click **OK** on the new dialog box that appears to save the configuration.



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

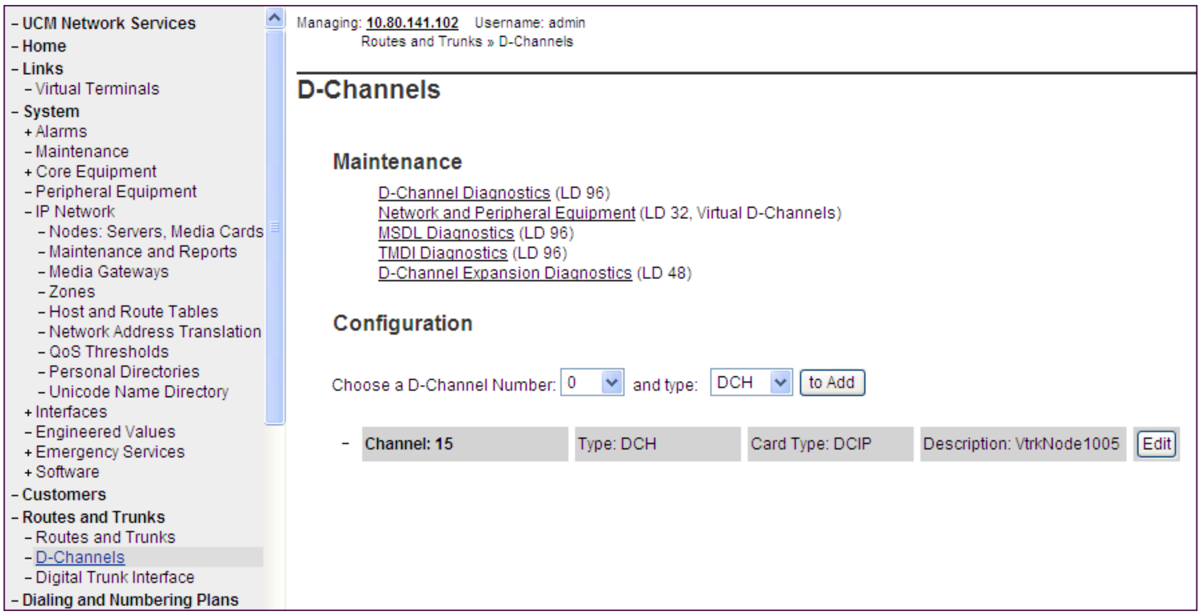


5.4. Virtual D-Channel, Routes and Trunks

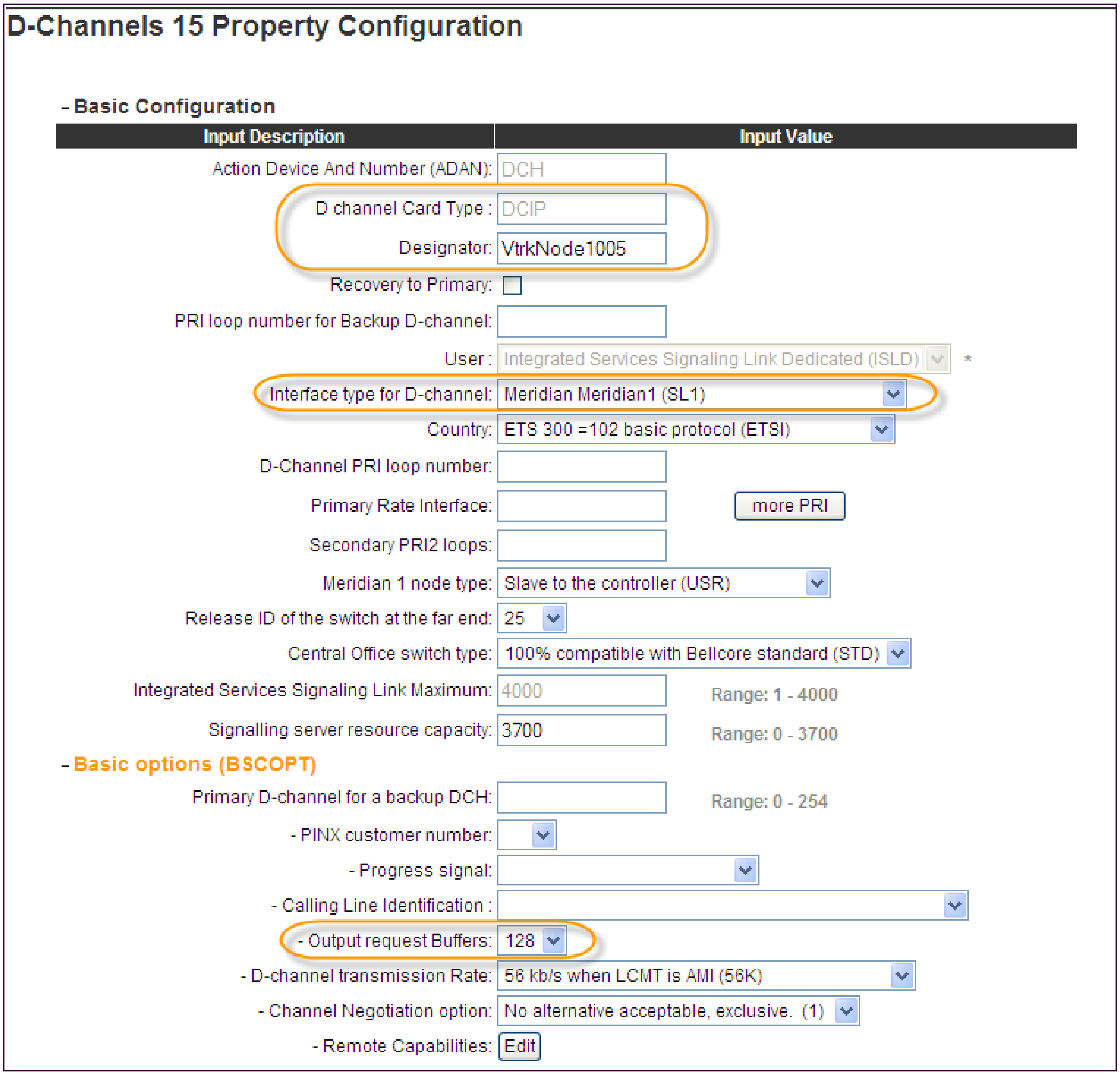
Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server.

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.

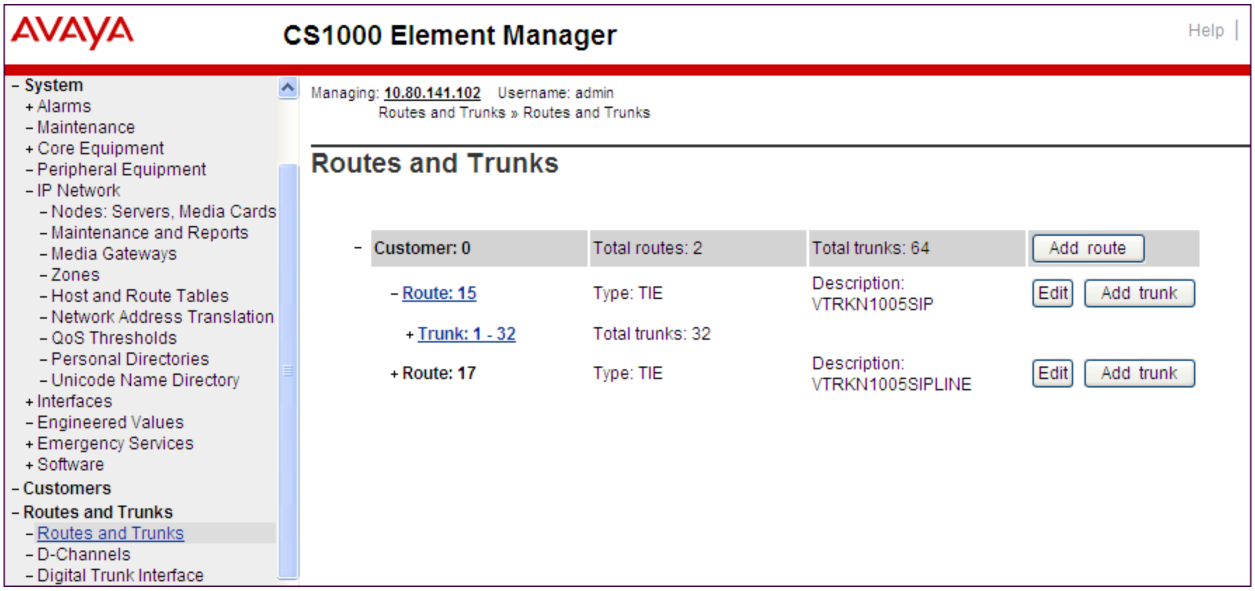


Select **Edit** to verify the configuration, as shown below. Verify **DCIP** has been selected for **D Channel Card Type** field and the **Interface type for D-Channel** is set to **Meridian Meridian 1(SL1)**. Under the Basic Options section, verify **128** is selected for the **Output request Buffers**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

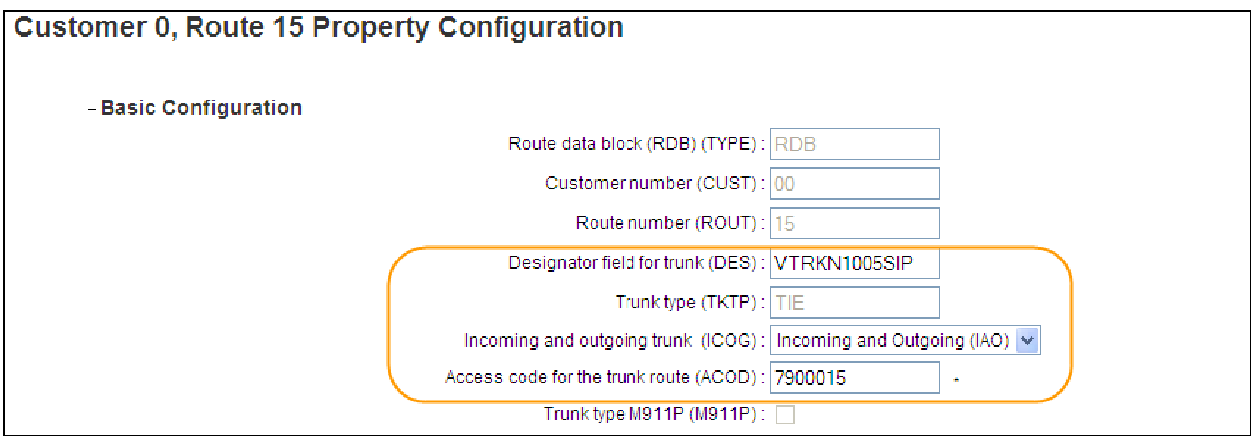


5.4.2. Routes and Trunks Configuration

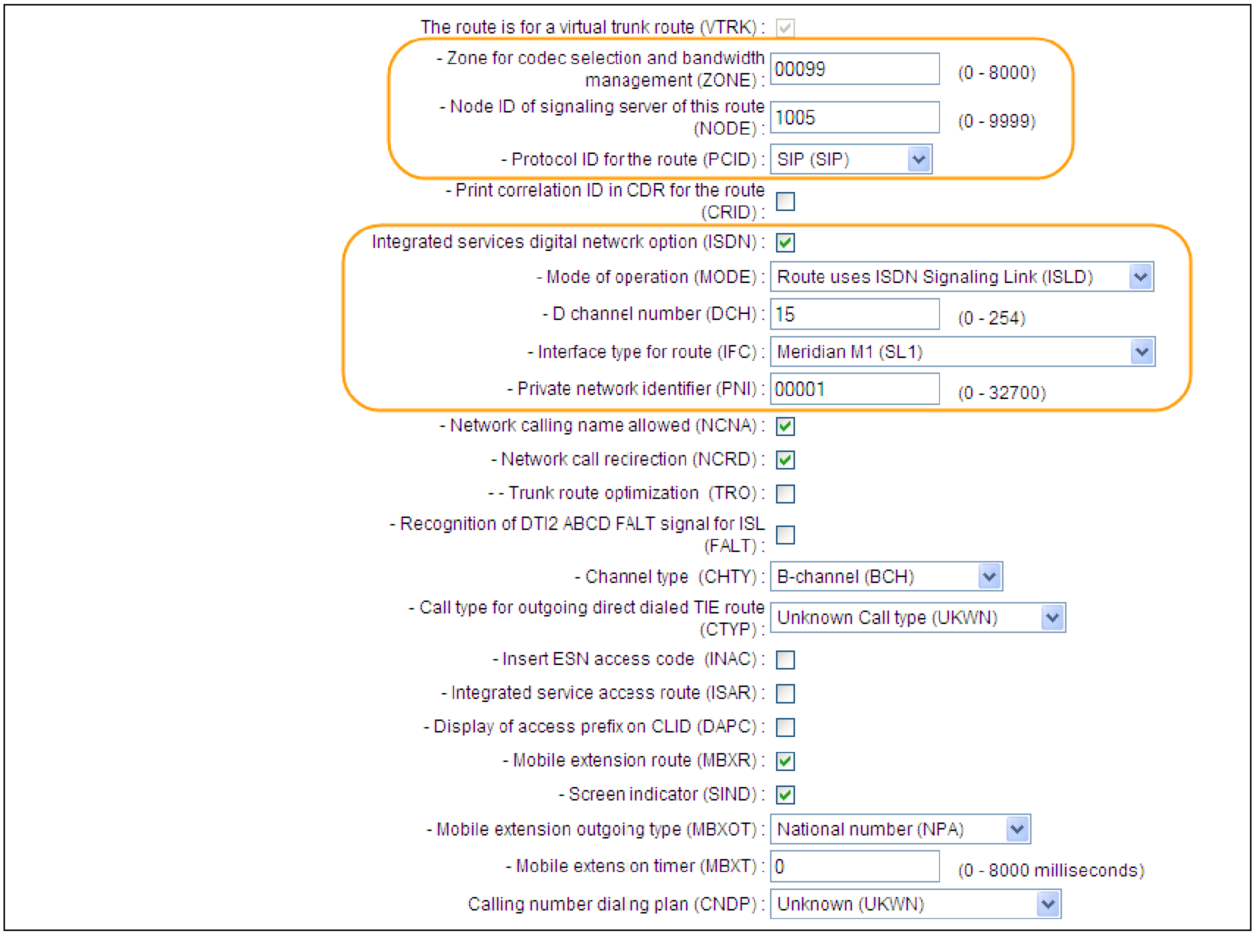
In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured. Expand **Routes and Trunks** on the left panel and expand the customer number. In the example screen that follows, it can be observed that Route 15 has 32 trunks in the sample configuration.



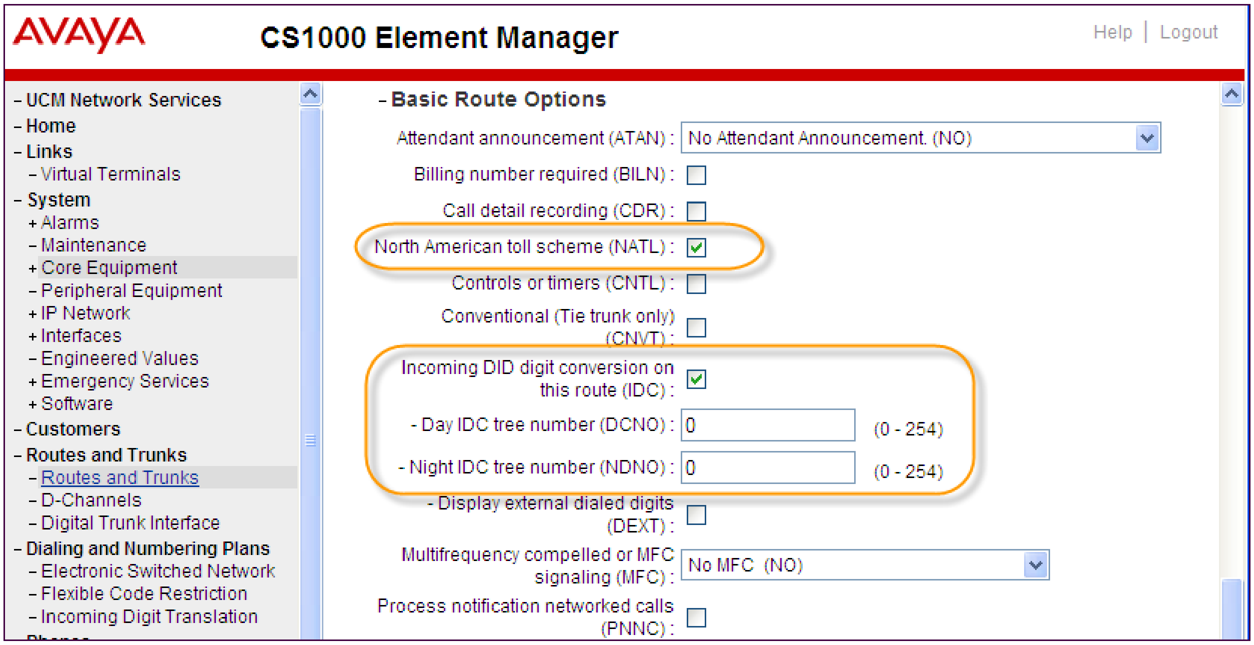
Select **Edit** to verify the configuration, as shown below. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may 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 5.1.1**. 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 5.5.5**.

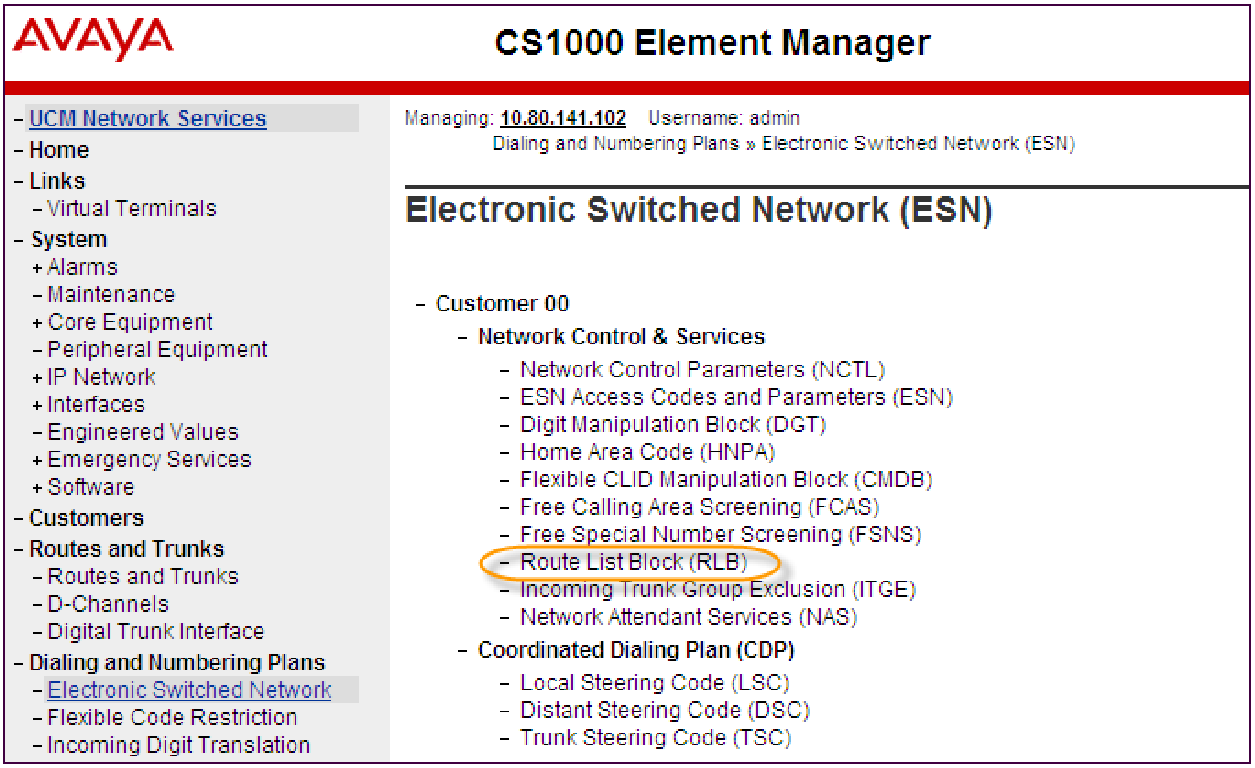


5.5. Dialing and Numbering Plans

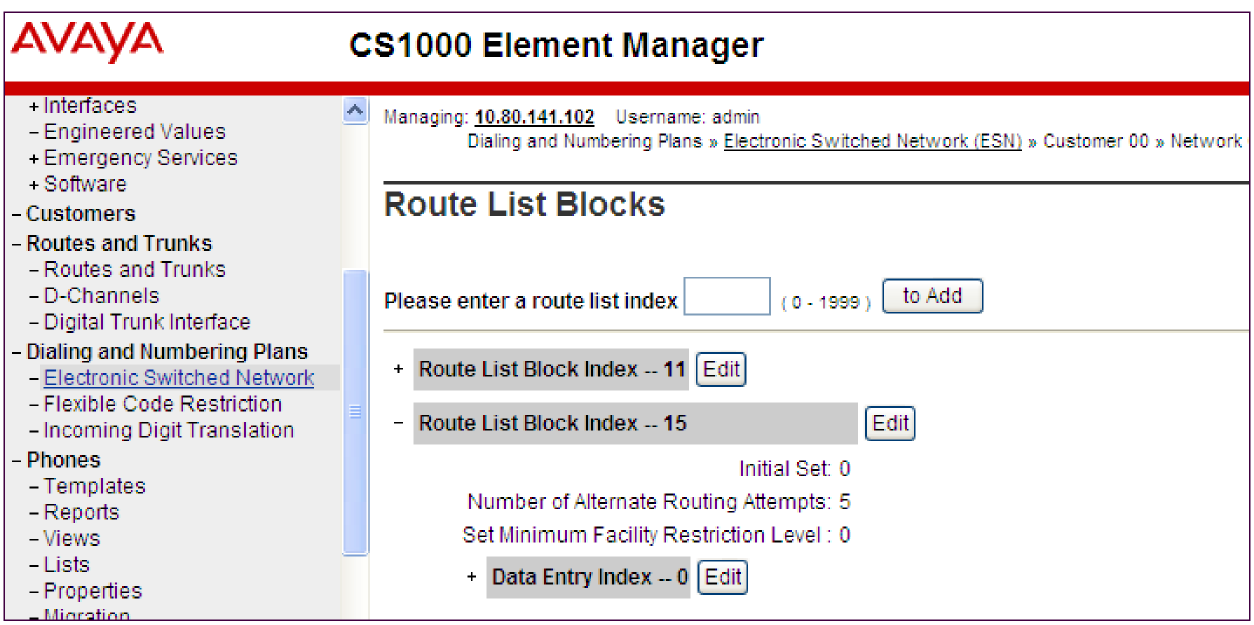
This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Session Manager for calls destined for the Cincinnati Bell eVantage IP Service. The routing defined in this section is simply an example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

5.5.1. Route List Block

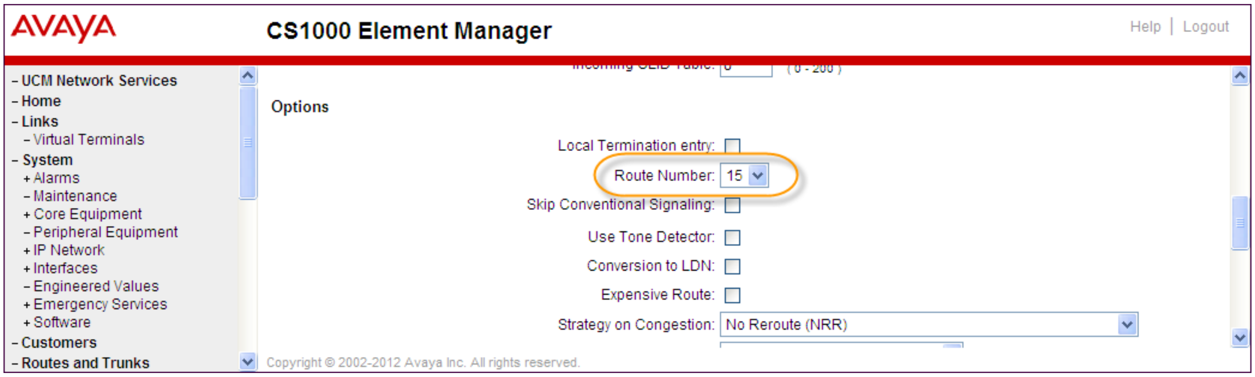
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown on the following page.



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.

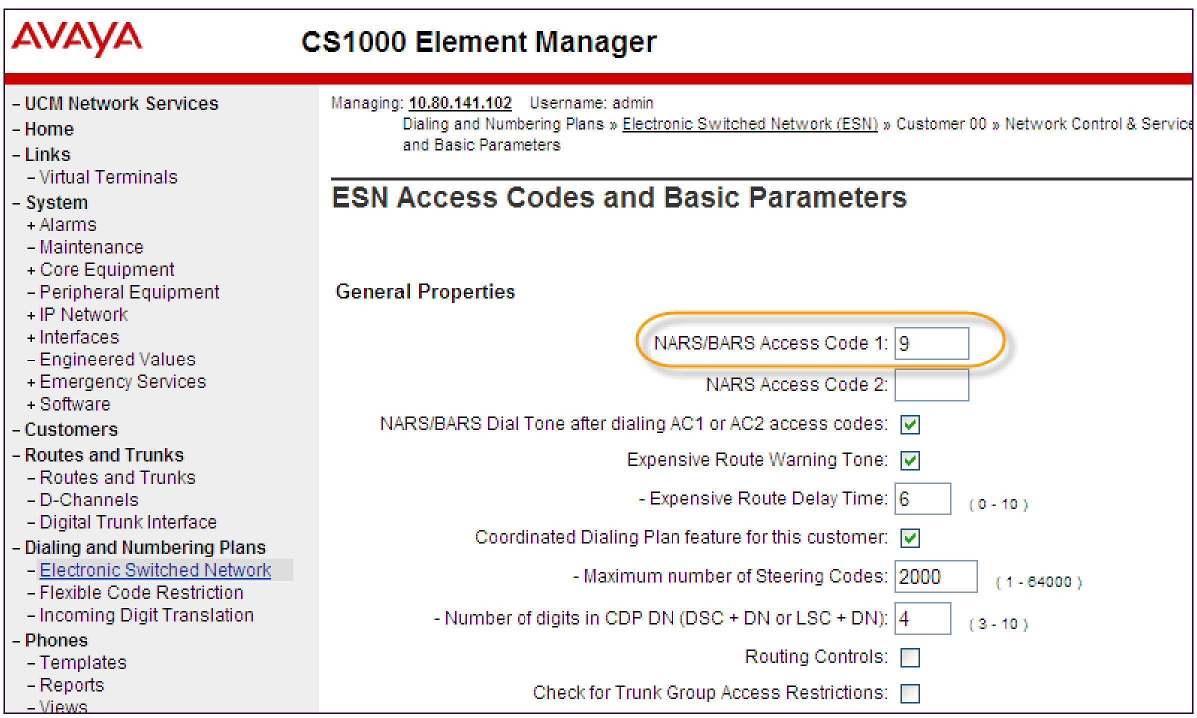


Under the **Options** section, select **<Route id>** in the **Route Number** field. In the sample configuration route number **15** was used. Default values may be retained for remaining fields.



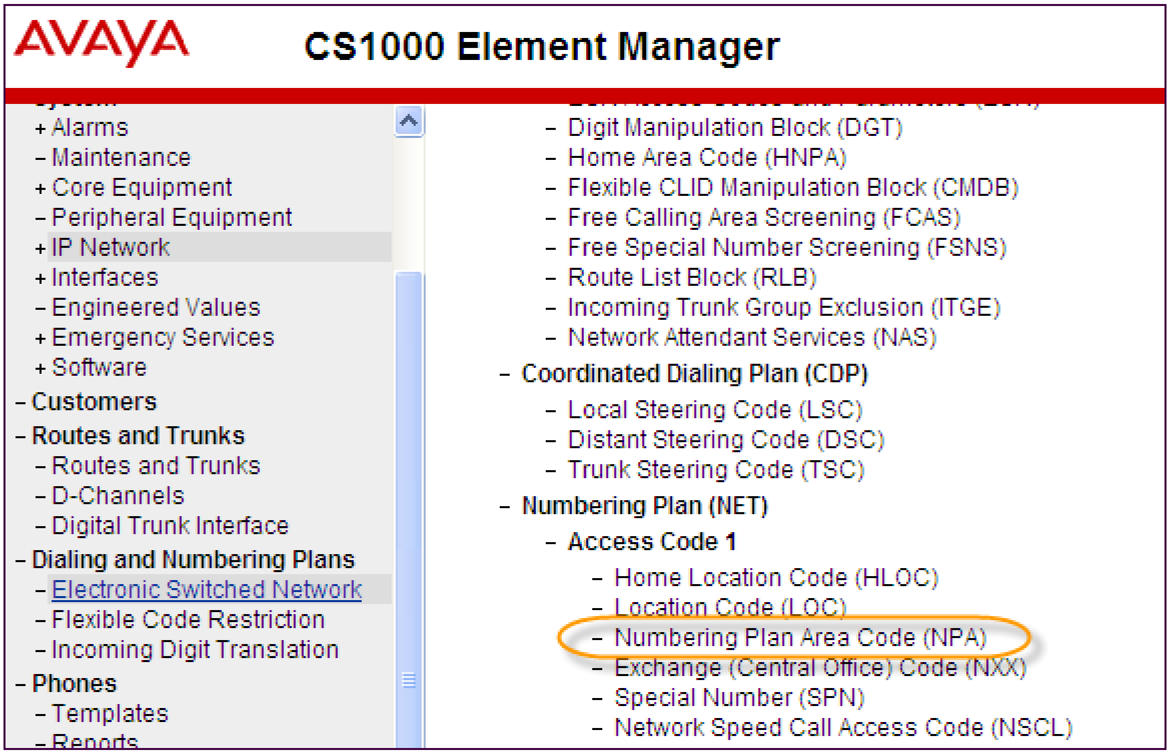
5.5.2. NARS Access Code

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 5.5.1**. 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.

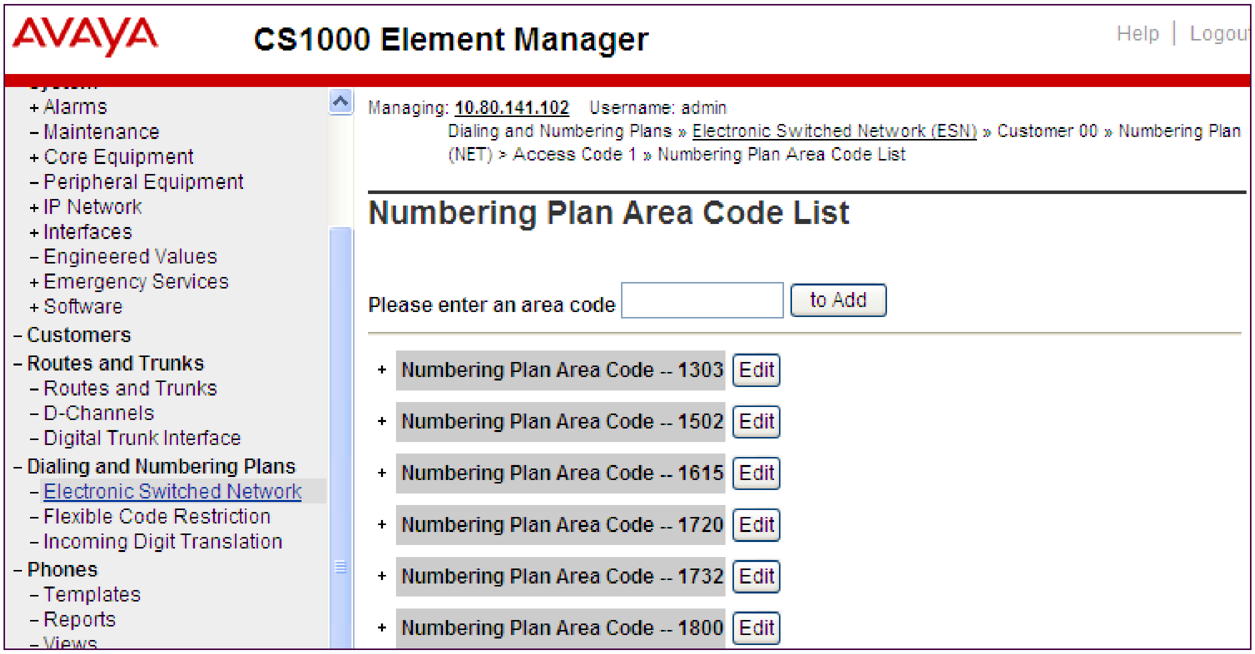


5.5.3. Numbering Plan Area Codes

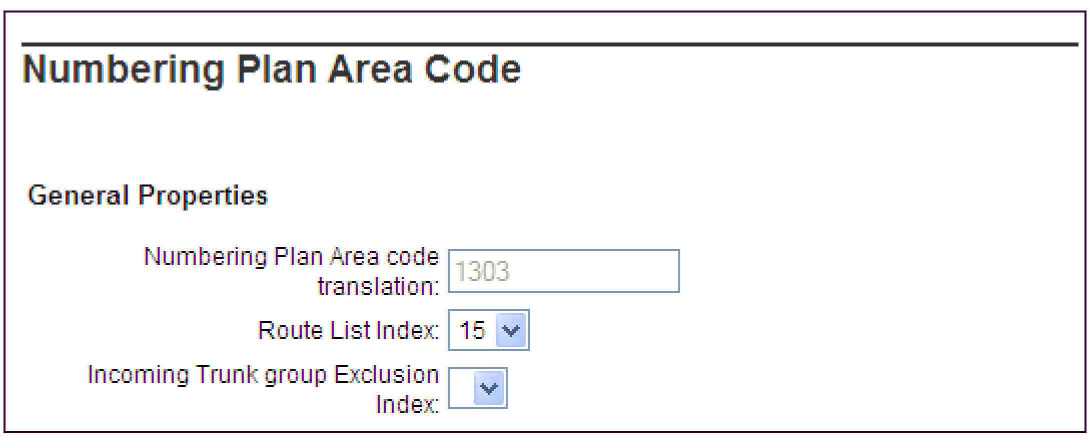
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Numbering Plan Area Code (NPA)** under the appropriate access code heading. In the sample configuration, this is **Access Code 1**, as shown below.



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 Session Manager 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 Session Manager.

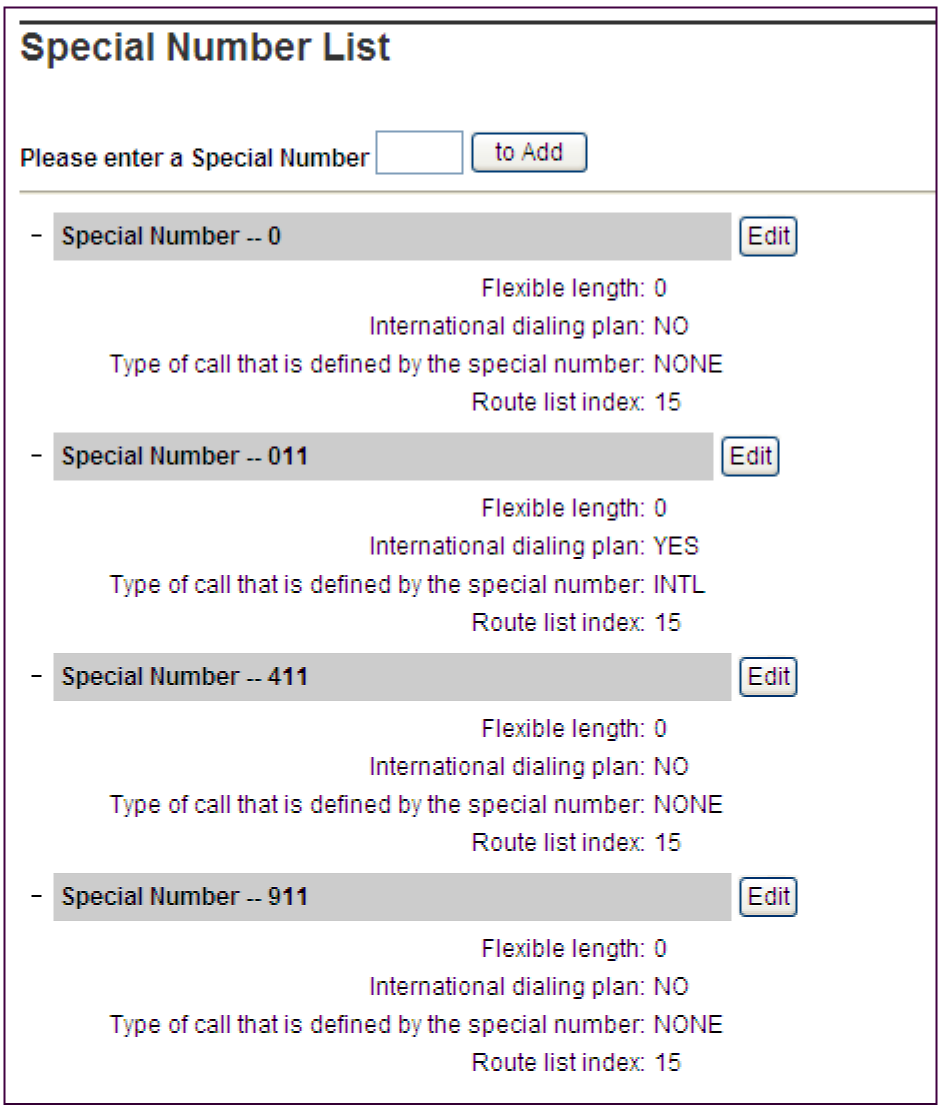


5.5.4. Special Numbers to Route to Session Manager

In the testing associated with these Application Notes, special service numbers such as x11, international calls, and operator assisted calls were also routed to Session Manager and ultimately to the Cincinnati Bell eVantage IP Service. 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 5.5.3**).

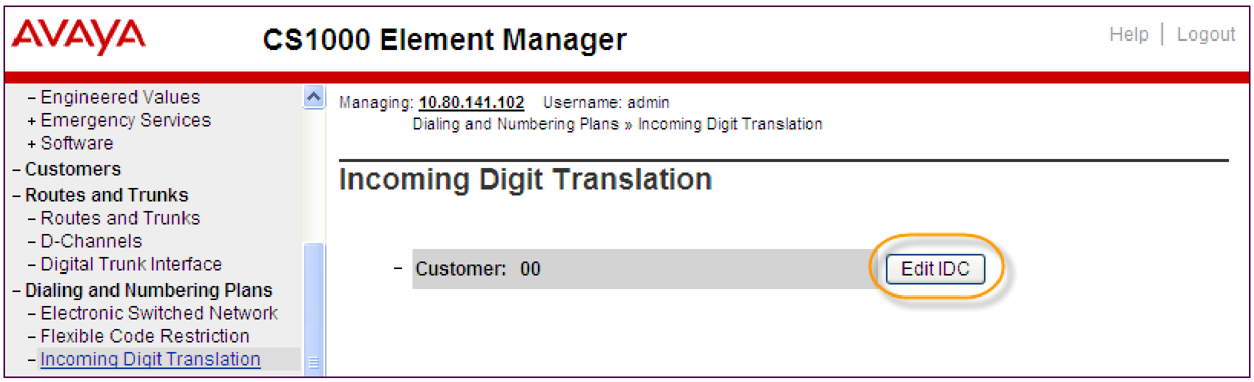
Add a new number by entering it in the **Please enter a Special Number** box and click **to Add** or click **Edit** to view or change a special number that has previously configured. In the screen below, it can be observed that various dial strings such as **0**, **011**, **411** and **911** calls are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



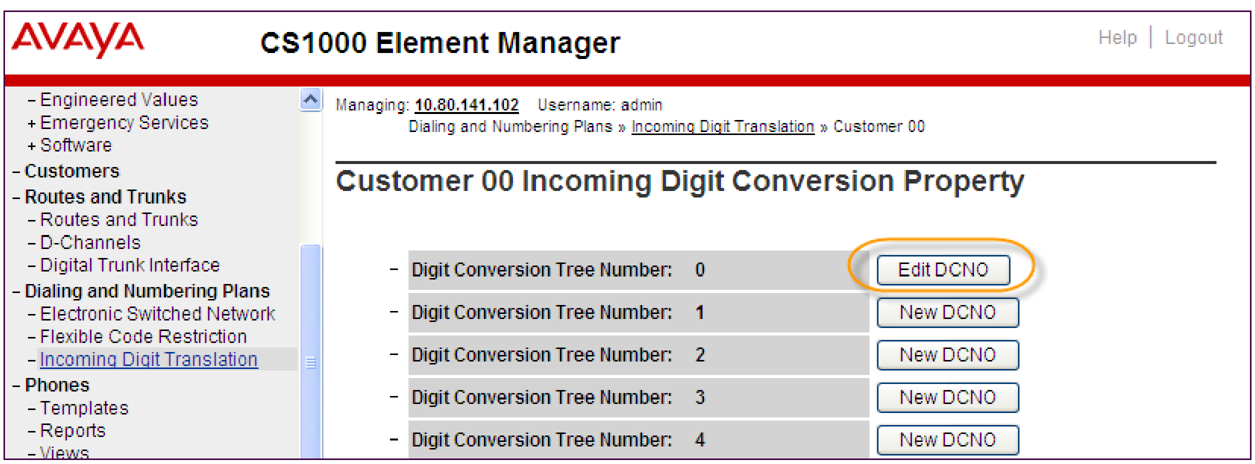
5.5.5. Incoming Digit Translation

In general, the incoming digit translation can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation as shown in **Section 6.4**, and digit manipulation via the CS1000E Incoming Digit Translation table may not be necessary. If the DID number sent by Cincinnati Bell is unchanged by Session Manager, then the DID number can be mapped to an extension using the Incoming Digit Translation. Both Session Manager digit conversion and CS1000E incoming digit translation methods were tested successfully.

Expand **Dialing and Numbering Plans** on the left panel and select **Incoming Digit Translation**. Click on the **Edit IDC** button as shown below.

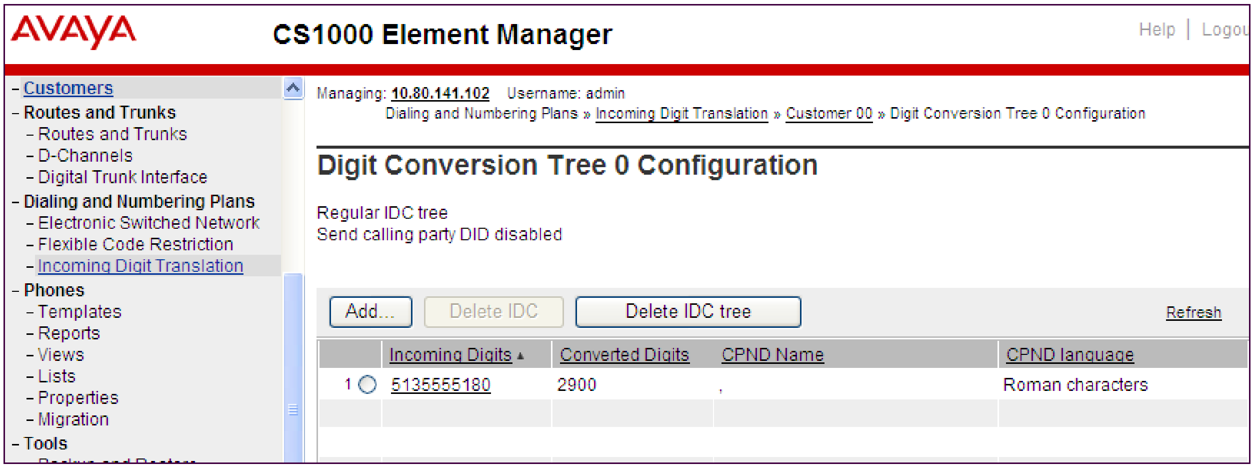


Click on the **New DCNO** to create the digit translation mechanism or if editing an existing one, select the **Edit DCNO** button next to the appropriate Digit Conversion Tree Number. In this example, **Digit Conversion Tree Number (DCNO) 0** has been created as shown below.



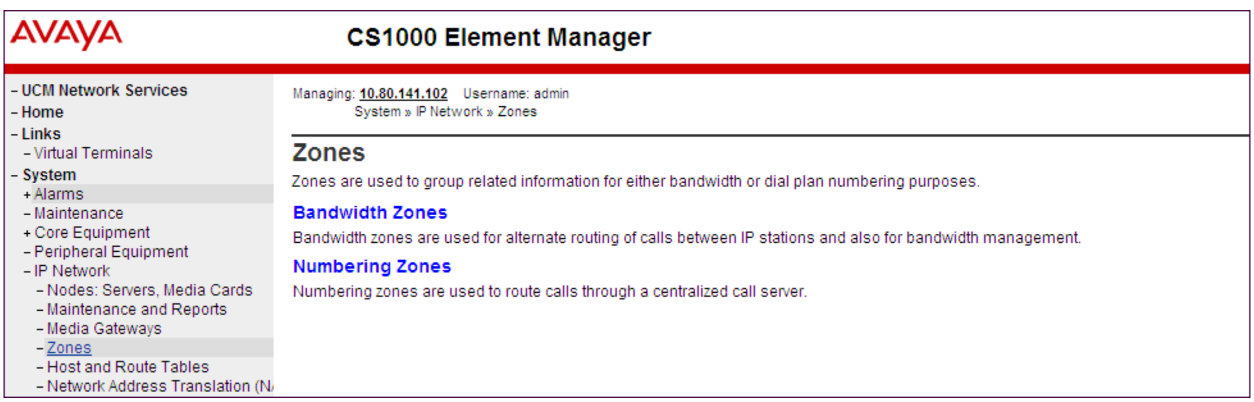
Detail configuration of the **DCNO** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000E system phones DN. This **DCNO** has been assigned to route 15 as shown in **Section 5.4.2**.

In the following configuration, the incoming DID 5135555180 will be translated to CS1000E DN 2900.

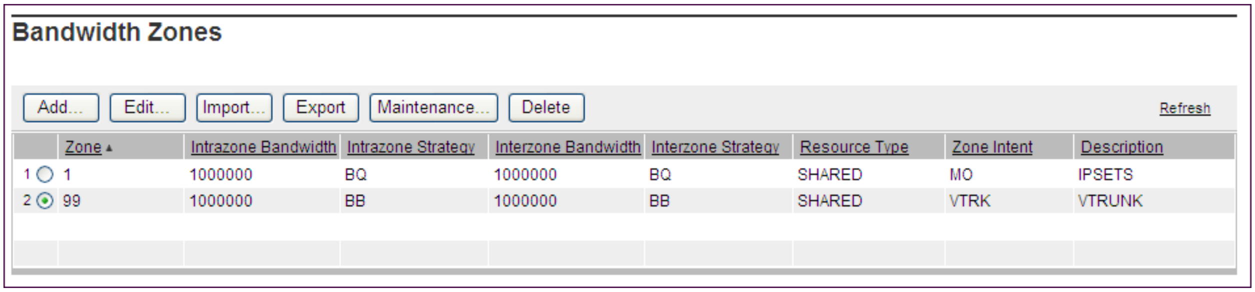


5.6. Zones and Bandwidth

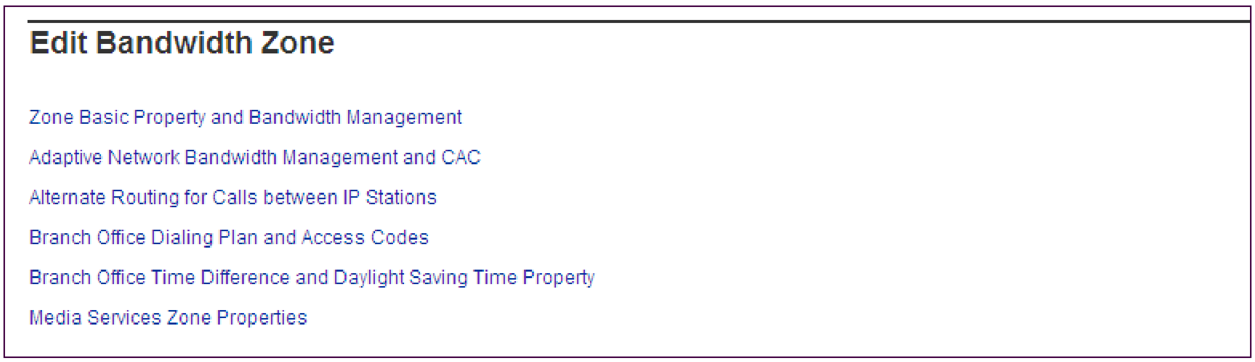
Zone configuration can be used to control codec selection and for bandwidth management. To configure, expand **System → IP Network** on the left panel and select **Zones** as shown below.



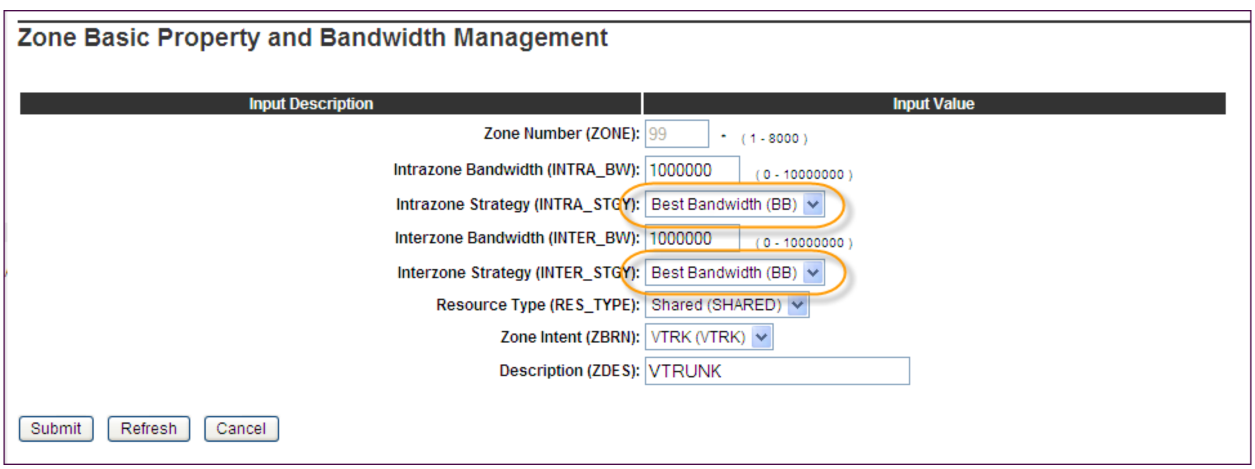
Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured. In production environments, it is likely that more zones will be required. Select the zone associated with the virtual trunk to Session Manager and click **Edit** as shown below. In the sample configuration, this is 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 Cincinnati Bell eVantage IP Service.

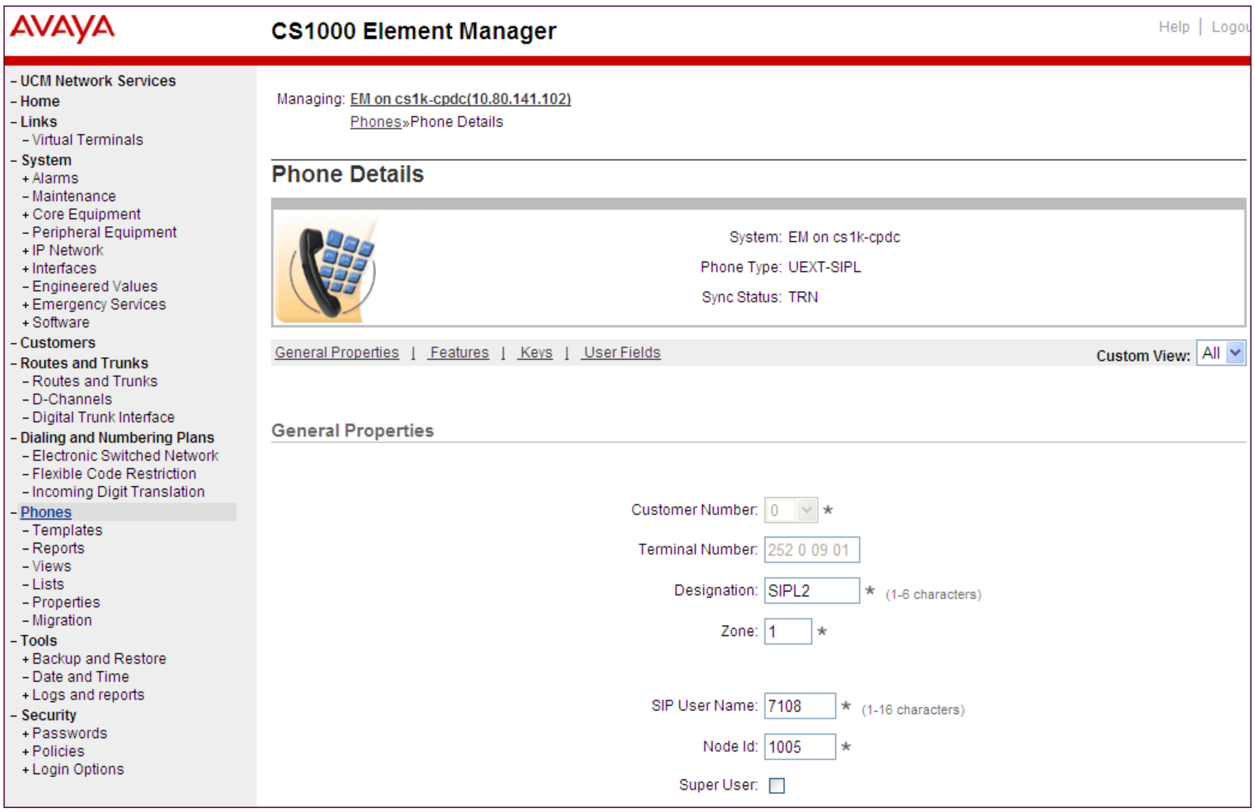


5.7. Example CS1000E Telephone Users

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

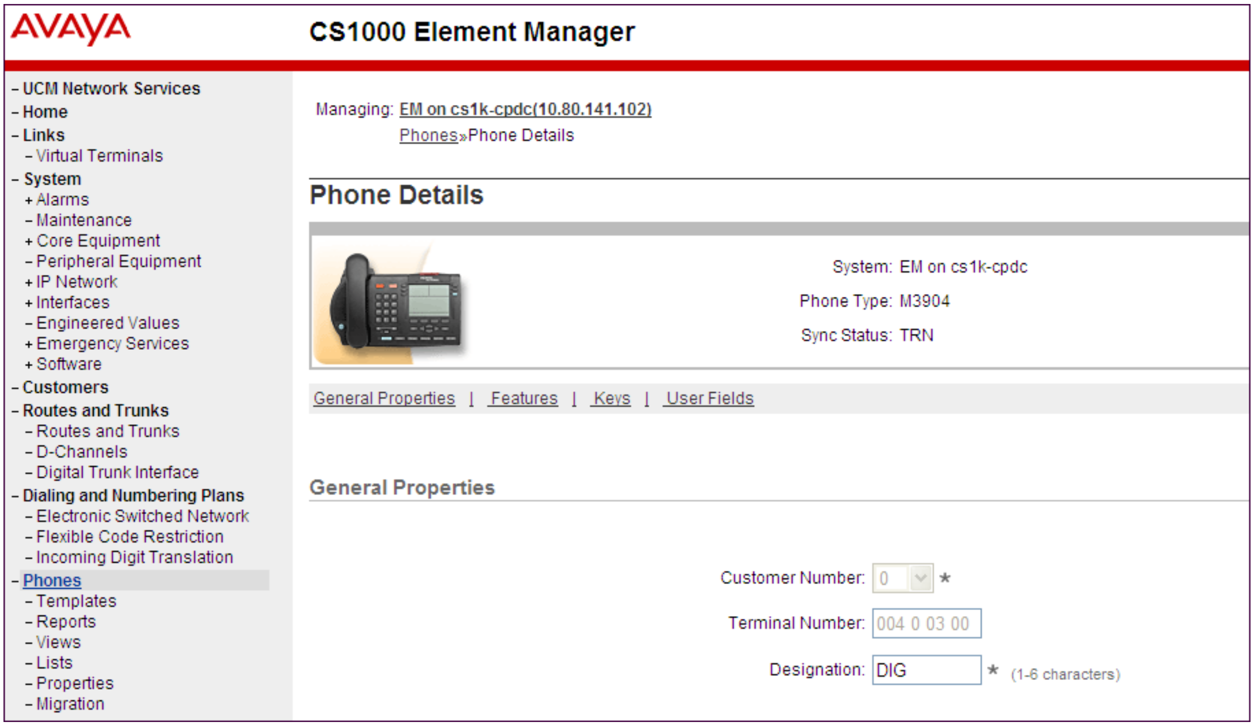
5.7.1. Example SIP Phone DN 7108, Codec Considerations

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 Cincinnati Bell eVantage IP Service, the call would use a **best bandwidth** strategy, and the call would use G.729A.

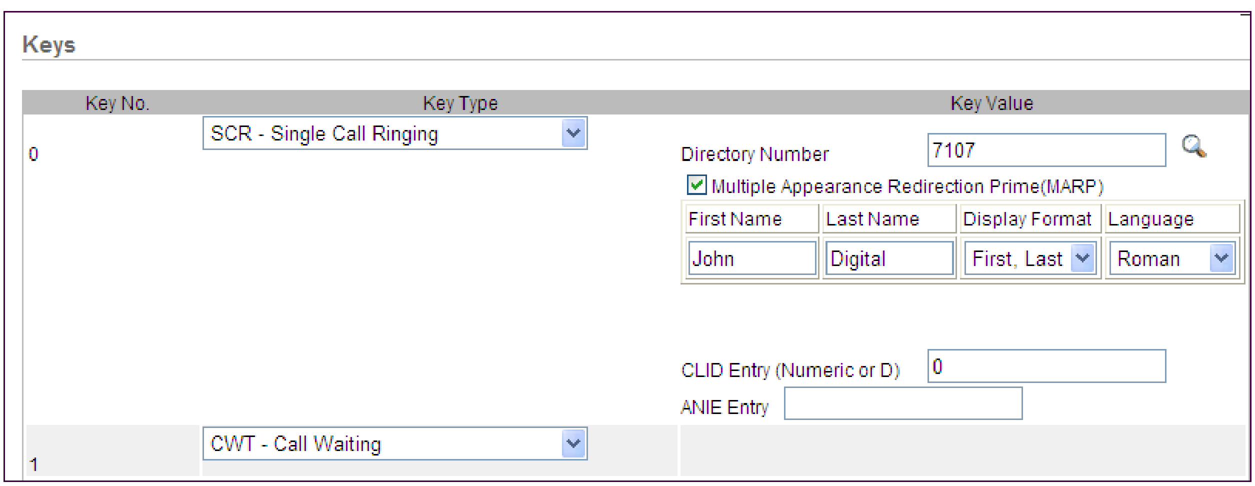


5.7.2. Example Digital Phone DN 7107 with Call Waiting

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

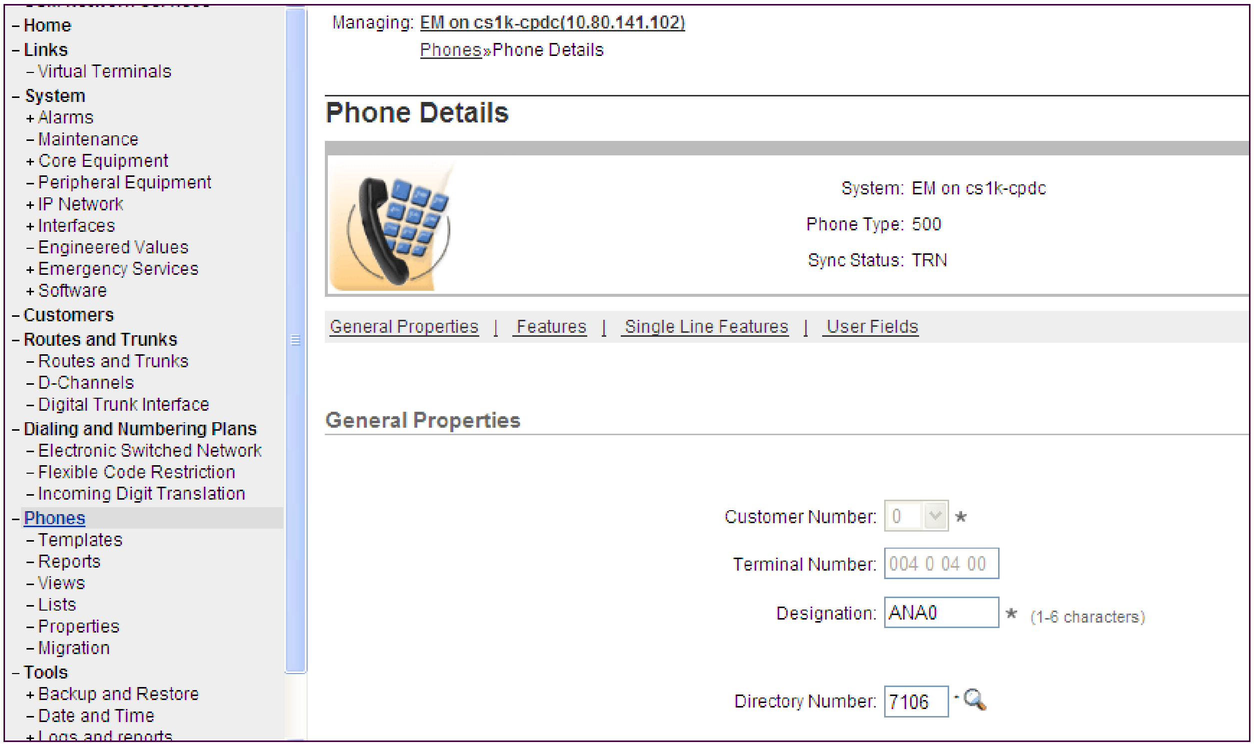


The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone. Although not shown in detail below, to use call waiting with tone, assign a key **CWT – Call Waiting**, set the feature **SWA – Call waiting from a Station** to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



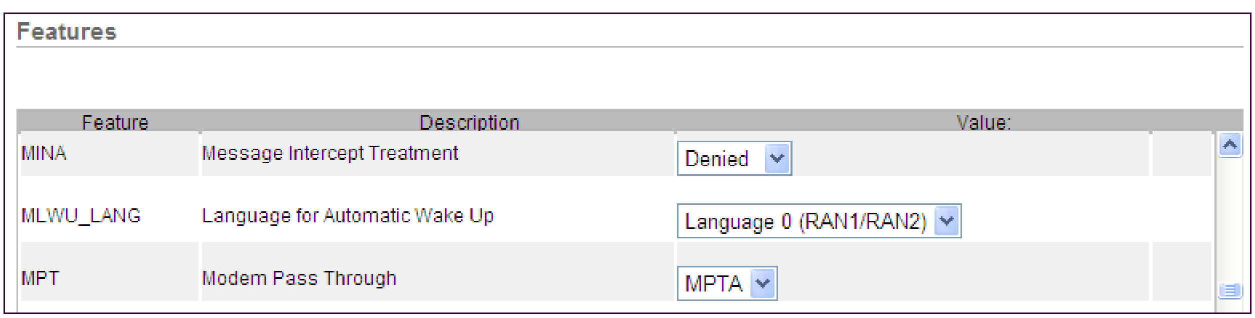
5.7.3. Example Analog Port with DN 7106, Fax

The following screen shows basic information for an analog port in the configuration that may be used with a telephone or fax machine. The port is configured as Directory Number 7106.



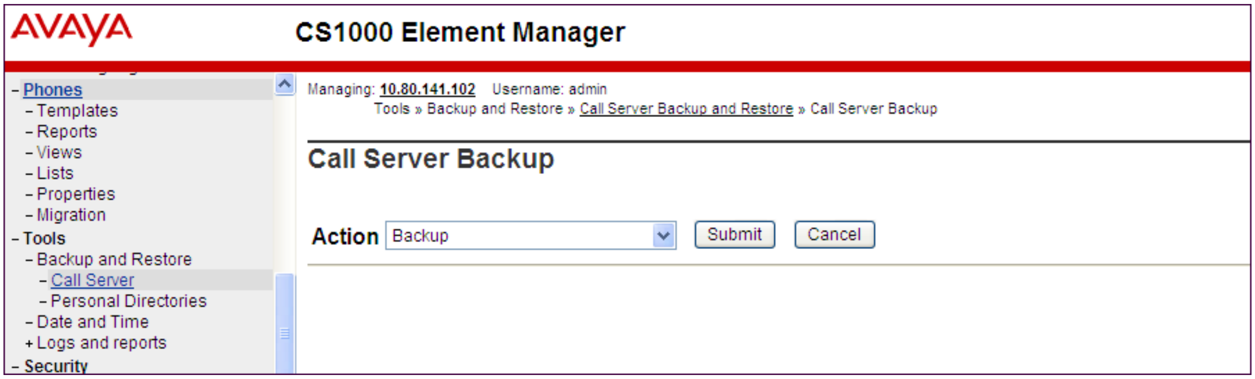
When an analog port is used for a fax machine, Modem Pass Through Allowed (MPTA) can be set to cause G.711 to be used instead of T.38 for fax calls, even if the zone configuration would otherwise have resulted in G.729. For example, if MPTA is configured, and an inbound call arrives from Cincinnati Bell eVantage IP Service, the CS1000E will respond with a 200 OK, selecting G.711 for the call in the SDP answer, even if the SDP offer from Cincinnati Bell listed G.729 before G.711. Similarly, for an outbound call with MPTA configured, the CS1000E will send the INVITE with an SDP offer for G.711. See **Section 2.2** for T.38 limitations with the Cincinnati Bell eVantage IP Service.

To configure MPTA, scroll down to the **Features** area and locate the feature with description **Modem Pass Through**. From the drop-down menu, select **MPTA** as shown below.



5.8. 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.



6. Configure Avaya Aura® Session Manager

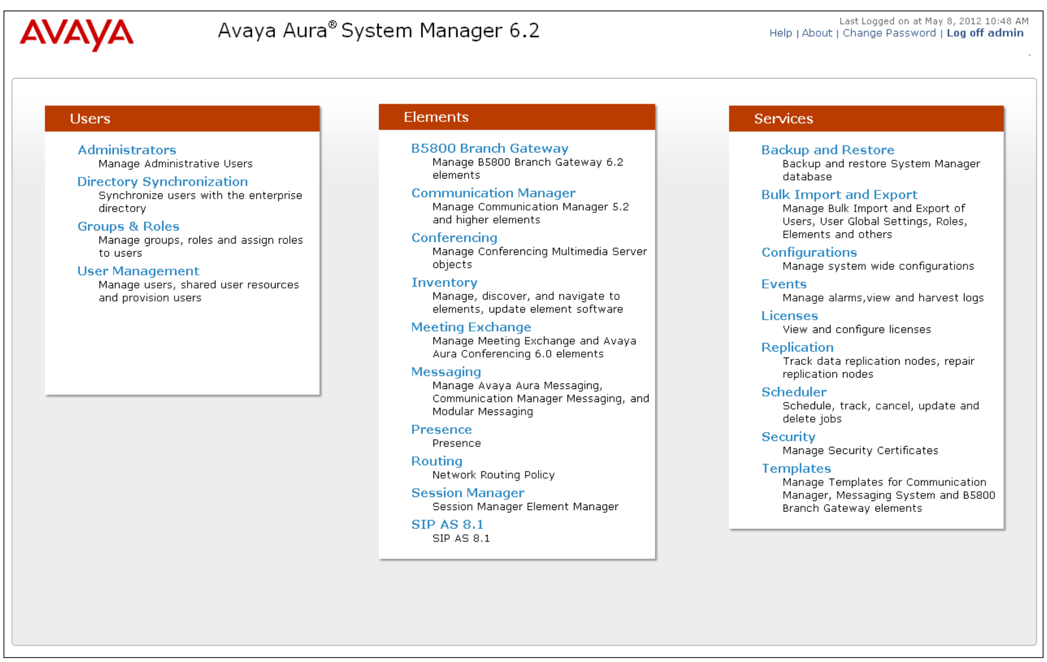
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to CS1000E, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager Instance, corresponding to the Session Manager server to be administered in System Manager.

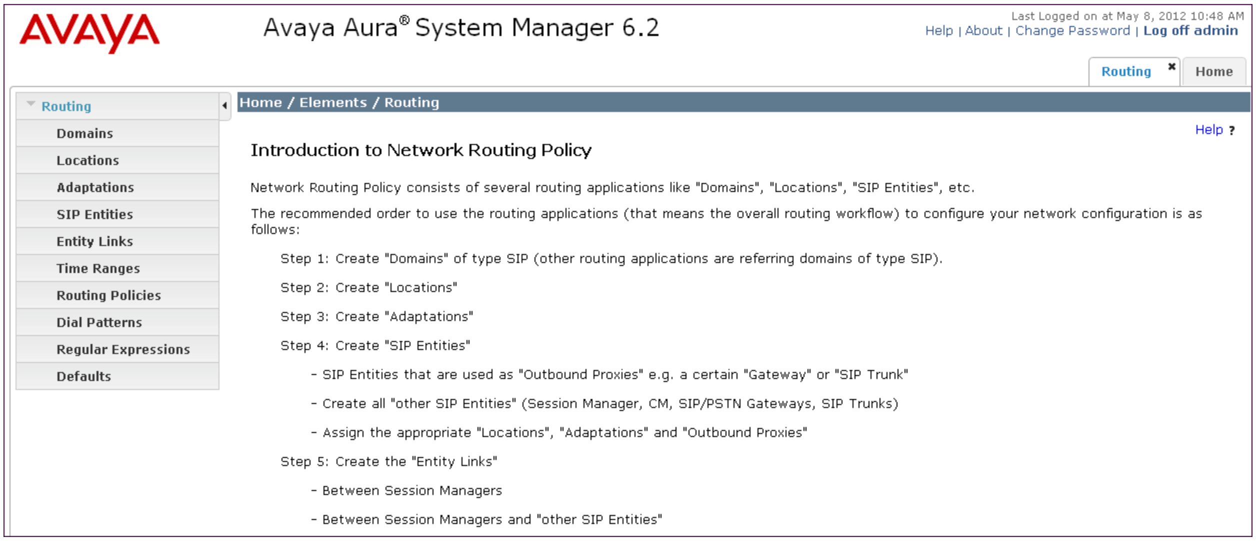
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Avaya Aura® System Manager Login and Navigation

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



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the **Introduction to Network Routing Policy** screen.

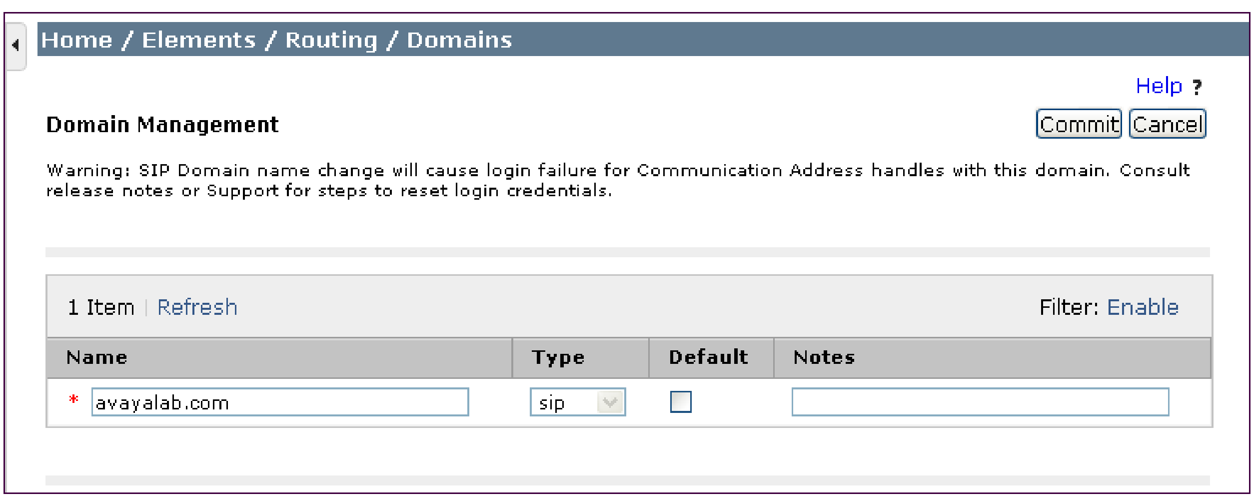


6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**). Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, fill in the following:

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

Click **Commit**. The screen below shows the entry for the **avayalab.com** domain.



6.3. Add Location

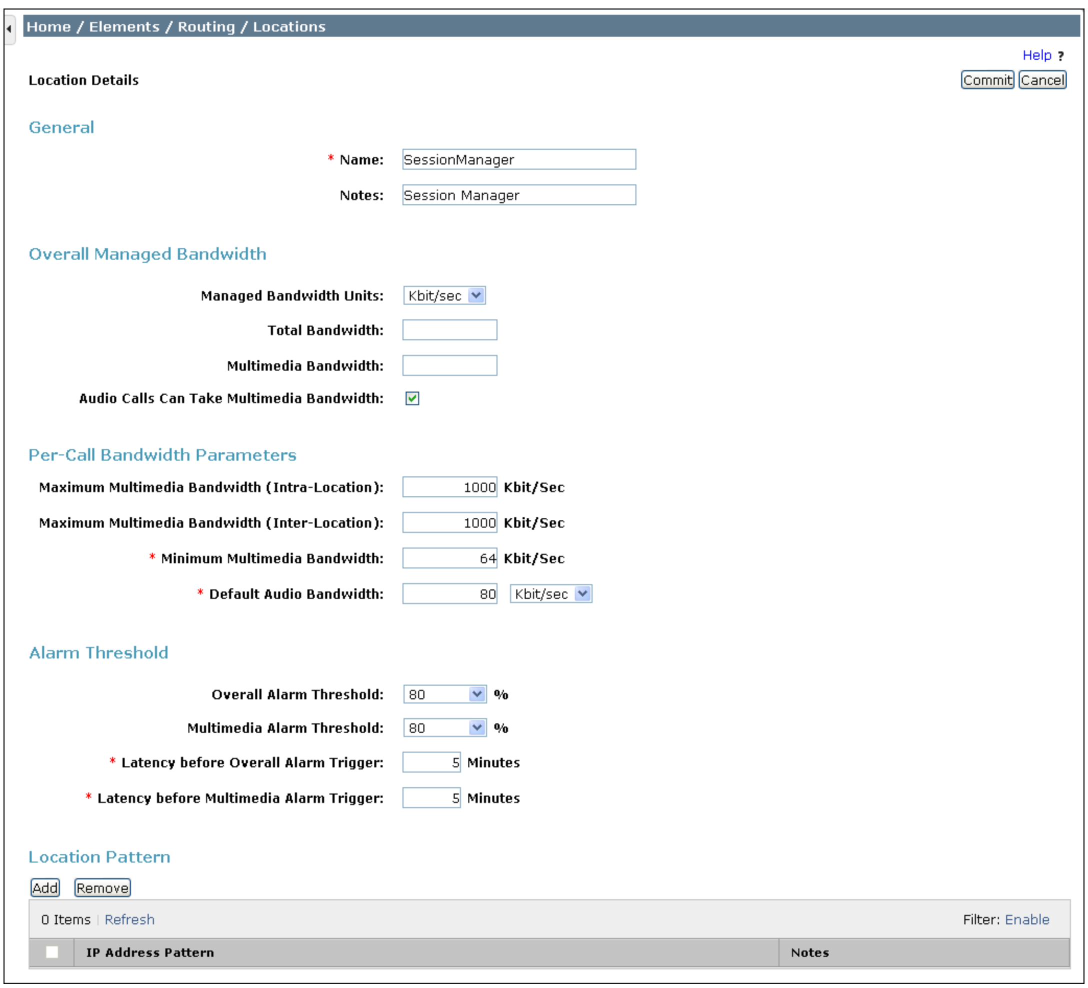
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

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

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

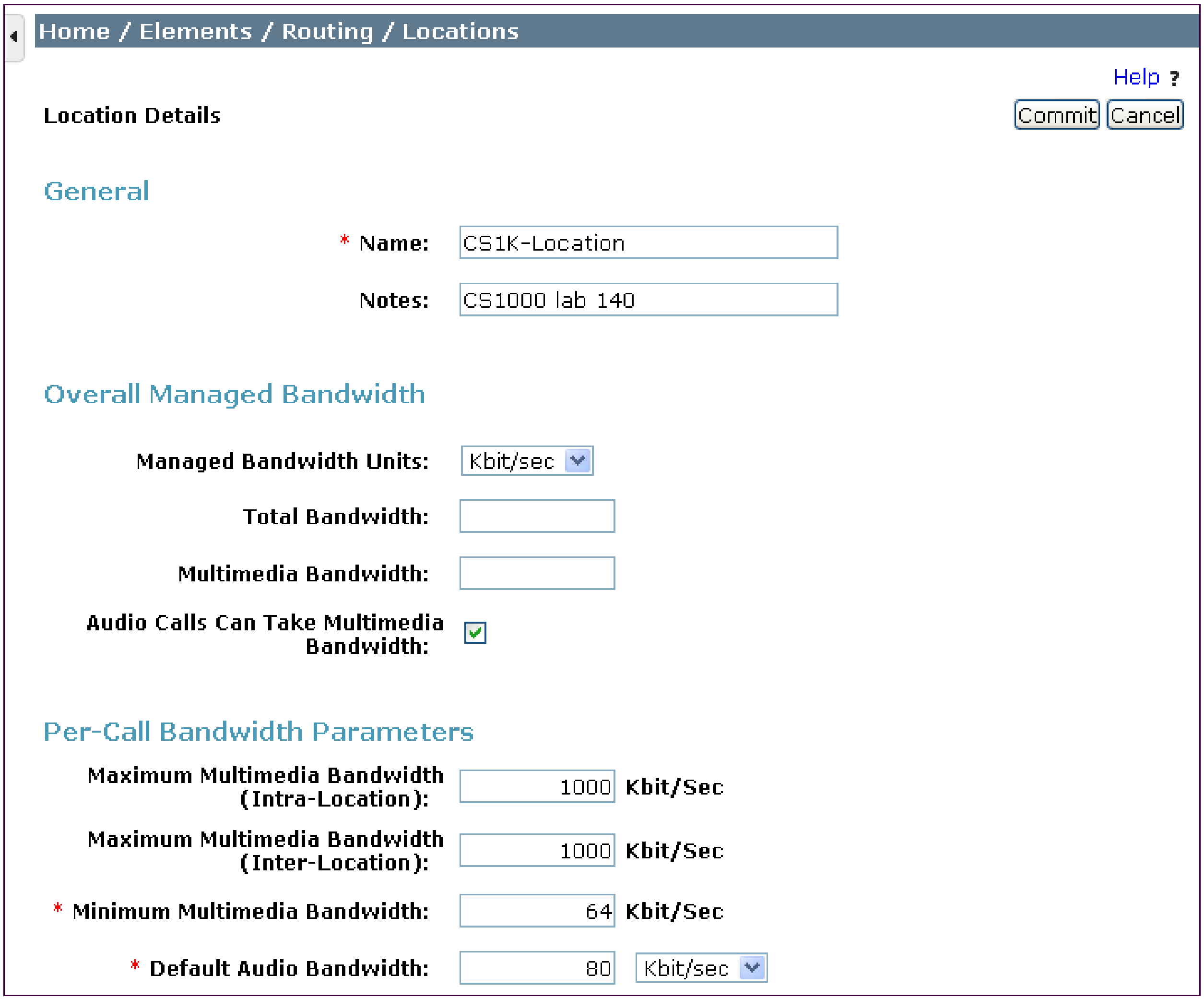
The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.5**), so it was not necessary to add a pattern.

The following screen shows the addition of **SessionManager**, this location will be used for Session Manager. Click **Commit** to save.

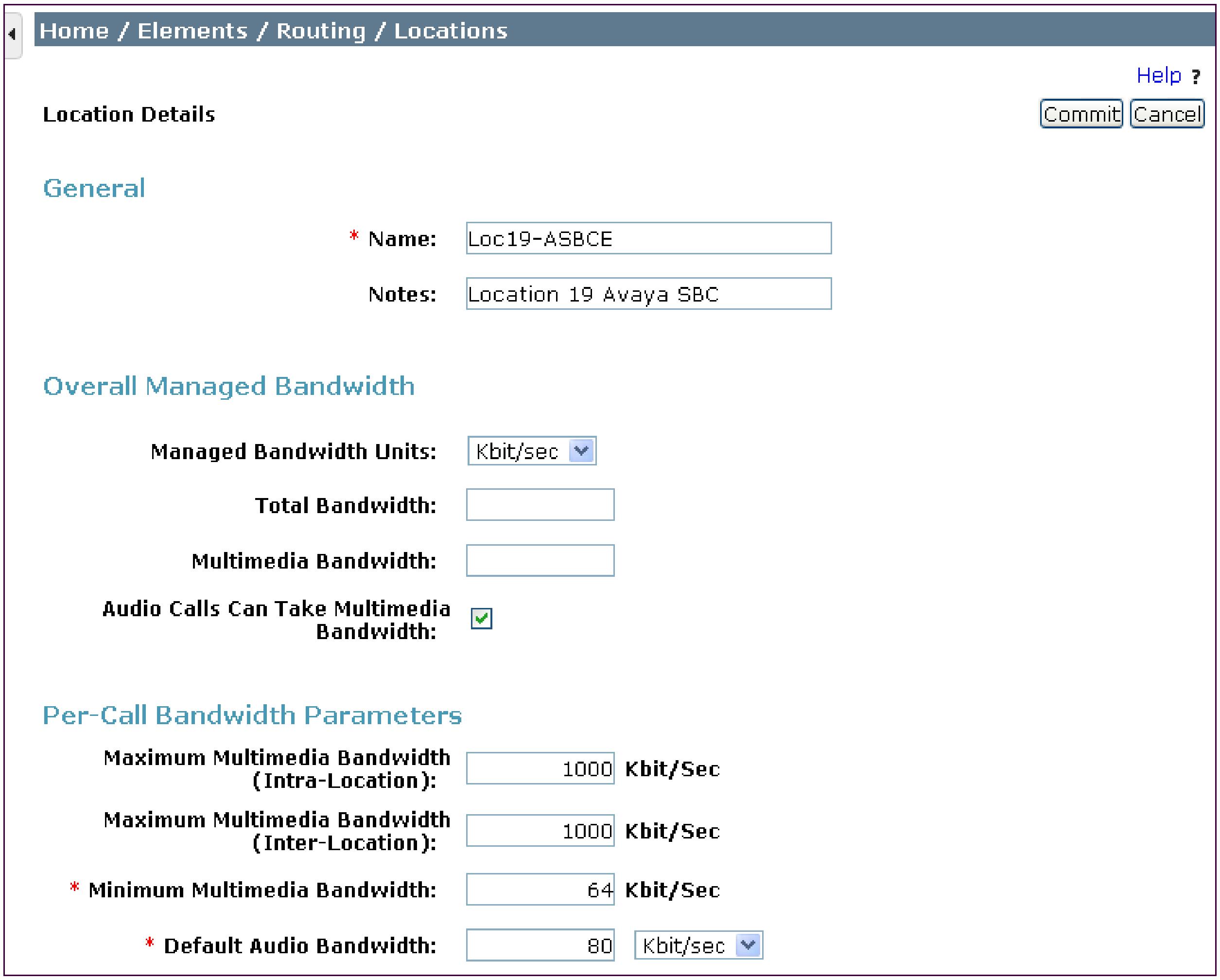


Note: Call bandwidth management parameters should be set per customer requirement.

Repeat the preceding procedure to create a separate Location for CS1000E and Avaya SBCE. Displayed below is the screen for **CS1K-Location** used for CS1000E.



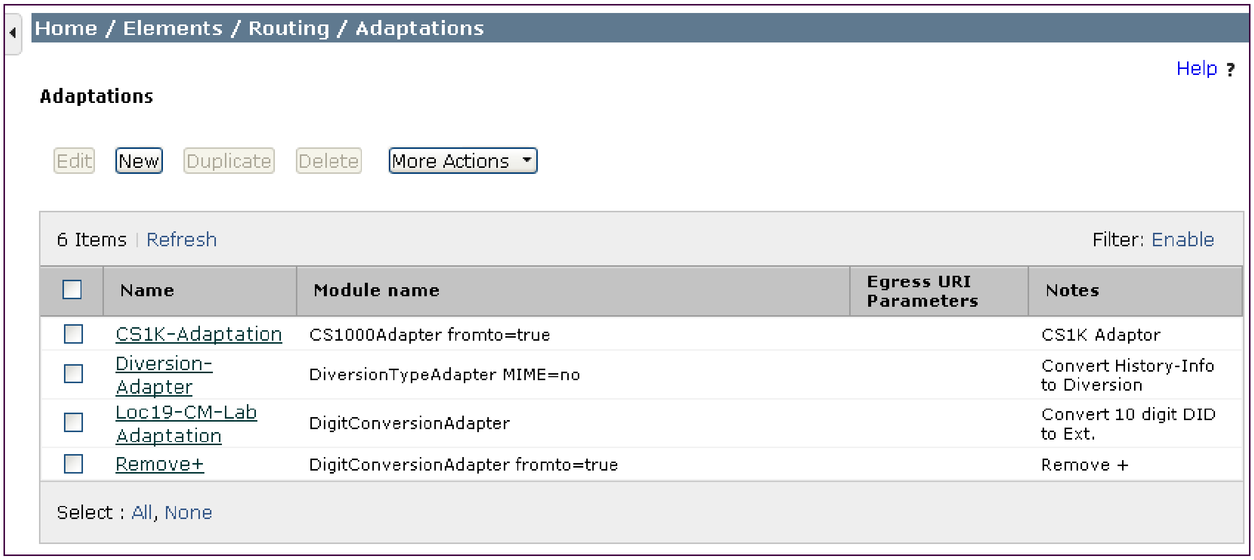
Below is the screen for **Loc19-ASBCE** used for Avaya SBCE.



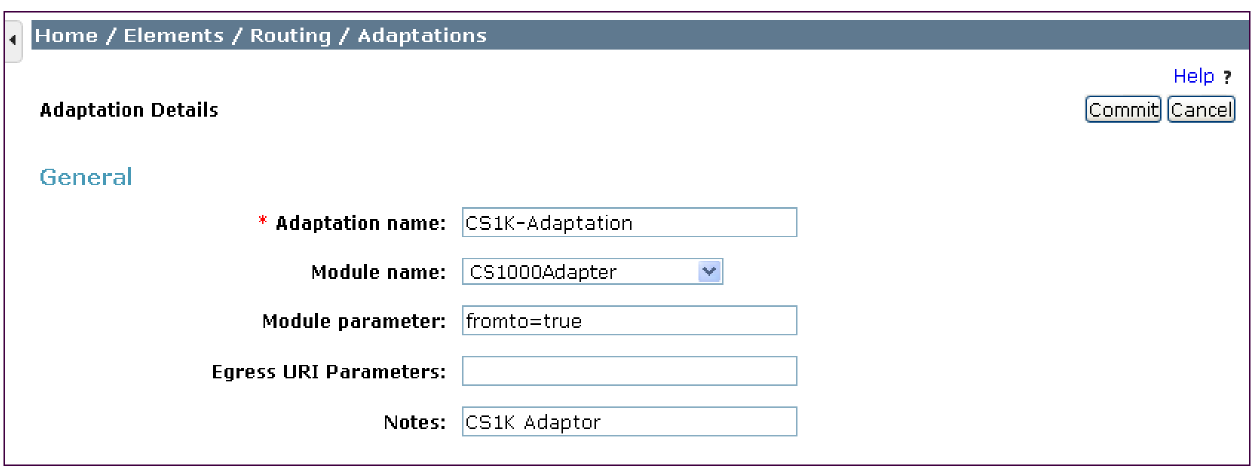
6.4. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

The following screen shows the adaptations that were available in the sample configuration.

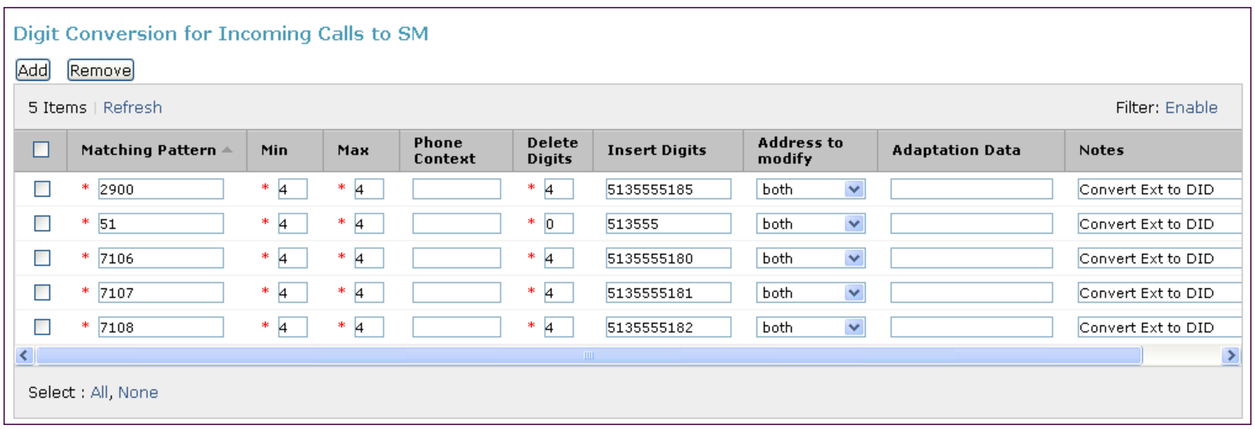


The adapter named **CS1K-Adaptation** will later be assigned to the SIP Entity linking Session Manager to CS1000E for calls involving Cincinnati Bell eVantage IP Service. This adaptation uses the **CS1000Adapter** to convert digits between CS1000E and Cincinnati Bell. The **Module parameter fromto=true** will include the FROM and TO headers in the digit conversion.



Scrolling down, in the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for calls from CS1000E users to Cincinnati Bell. The text below and the screen example that follows explain how to use Session Manager to convert the CS1000E directory numbers that are in the From and P-Asserted-Identity headers to the corresponding Cincinnati Bell DID numbers.

- **Matching Pattern** Enter Avaya CS1000E extensions (or extension ranges via wildcard pattern matching). For other entries, enter the dialed prefix for any SIP endpoints registered to Session Manager (if any).
- **Min** Enter minimum number of digits (e.g., 4).
- **Max** Enter maximum number of digits (e.g., 4).
- **Delete Digits** Enter **0**, unless digits should be removed from dialed number before routing by Session Manager. For CS1000E extensions that do not match the last digits of the Cincinnati Bell DID, enter the number of digits in the extension to remove all digits.
- **Insert Digits** Enter the Cincinnati Bell DID corresponding to the matched extension or DID prefix for a range of extensions.
- **Address to modify** Select **both**.


Digit Conversion for Incoming Calls to SM

Add Remove

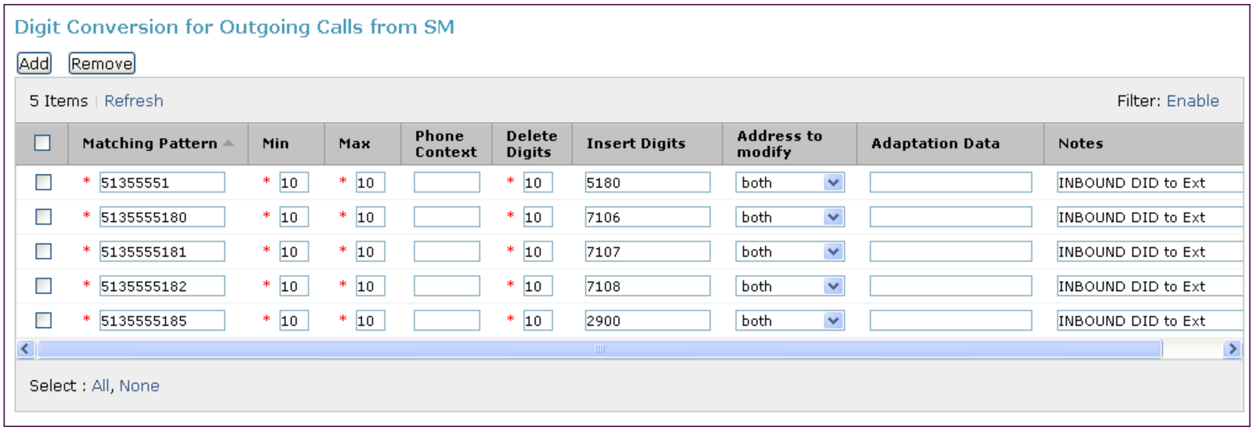
5 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	* 2900	* 4	* 4		* 4	5135555185	both		Convert Ext to DID
	* 51	* 4	* 4		* 0	513555	both		Convert Ext to DID
	* 7106	* 4	* 4		* 4	5135555180	both		Convert Ext to DID
	* 7107	* 4	* 4		* 4	5135555181	both		Convert Ext to DID
	* 7108	* 4	* 4		* 4	5135555182	both		Convert Ext to DID

Select : All, None

Scrolling down, the following screen shows a portion of the **CS1K-Adaptation** adapter that can be used to convert digits between the CS1000E extension numbers and the DID numbers assigned by Cincinnati Bell.

An example portion of the settings for **Digit Conversion for Outgoing Calls from SM** (i.e., inbound to CS1000E) is shown below. It can be observed that the first two entries are used to match a range of numbers while the last entry is used to match on a specific number.



Digit Conversion for Outgoing Calls from SM

Add Remove

5 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	* 51355551	* 10	* 10		* 10	5180	both		INBOUND DID to Ext
	* 5135555180	* 10	* 10		* 10	7106	both		INBOUND DID to Ext
	* 5135555181	* 10	* 10		* 10	7107	both		INBOUND DID to Ext
	* 5135555182	* 10	* 10		* 10	7108	both		INBOUND DID to Ext
	* 5135555185	* 10	* 10		* 10	2900	both		INBOUND DID to Ext

Select : All, None

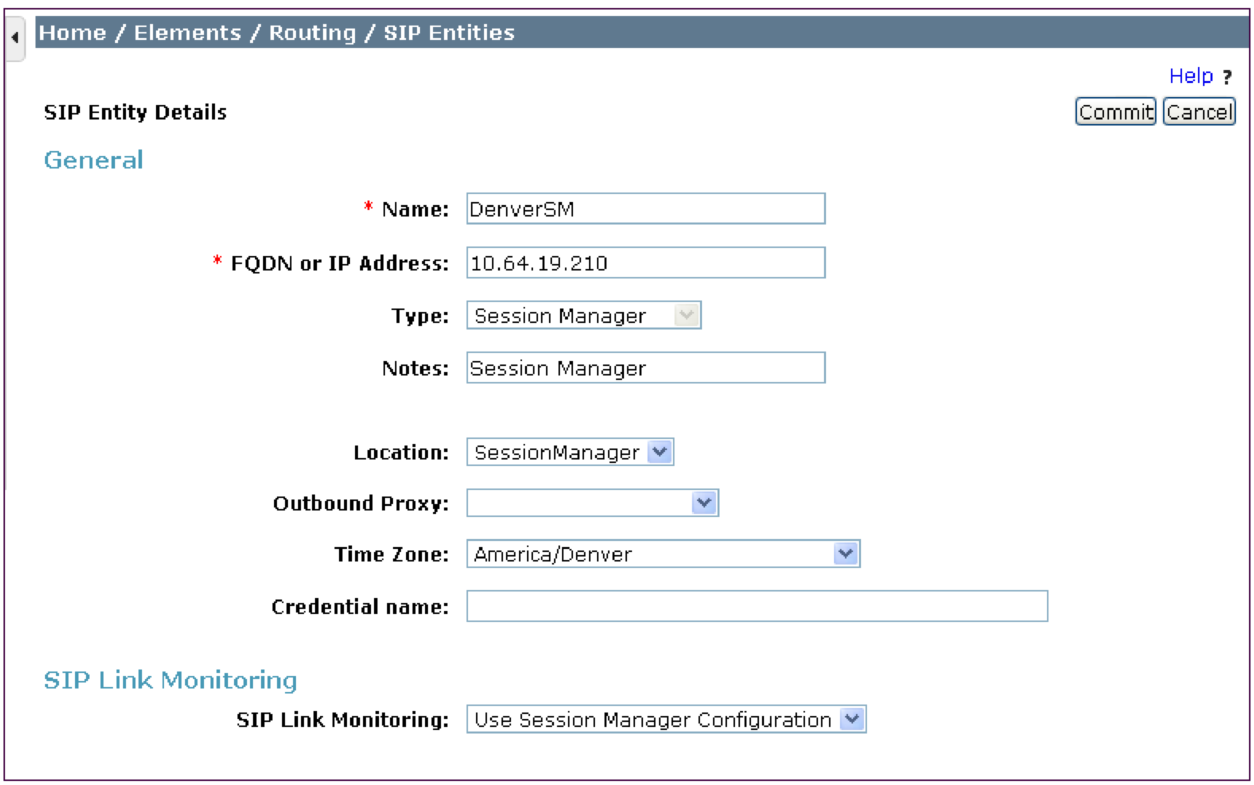
6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes CS1000E and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for CS1000E and **SIP Trunk** for Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.



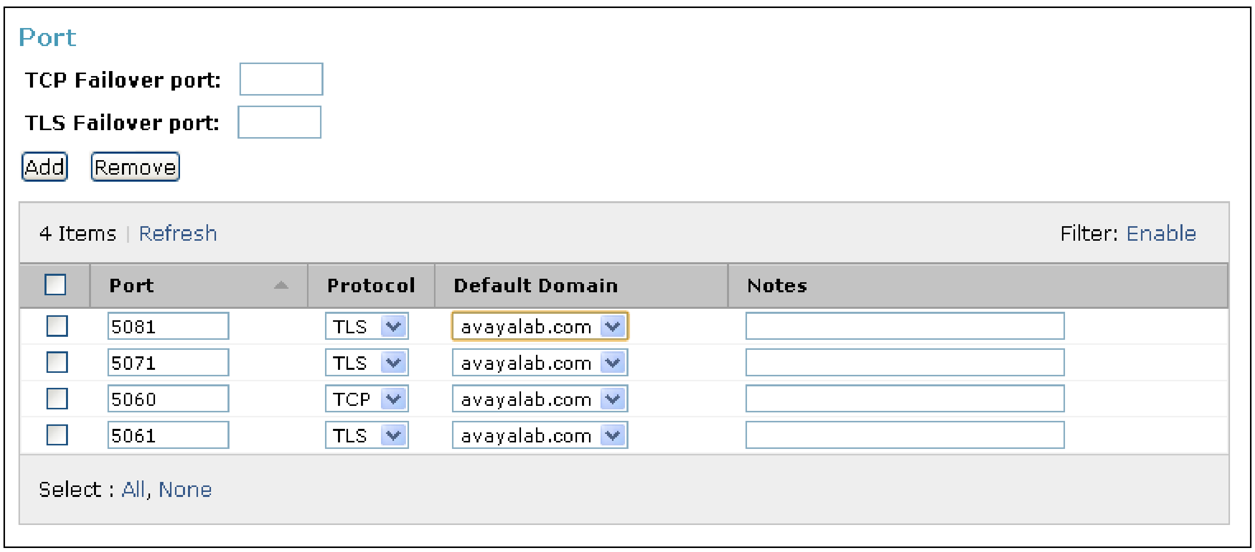
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.6**.

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

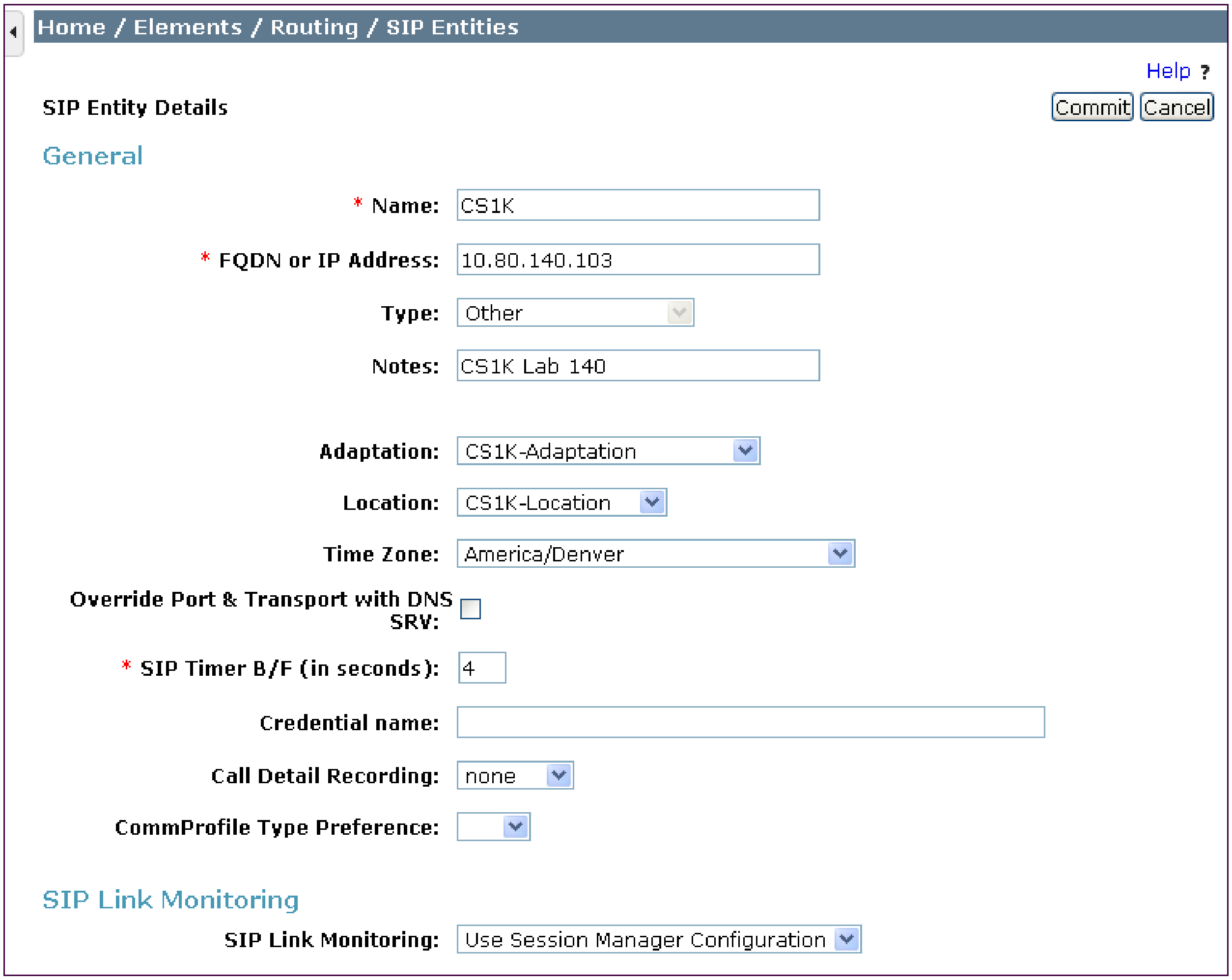
- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

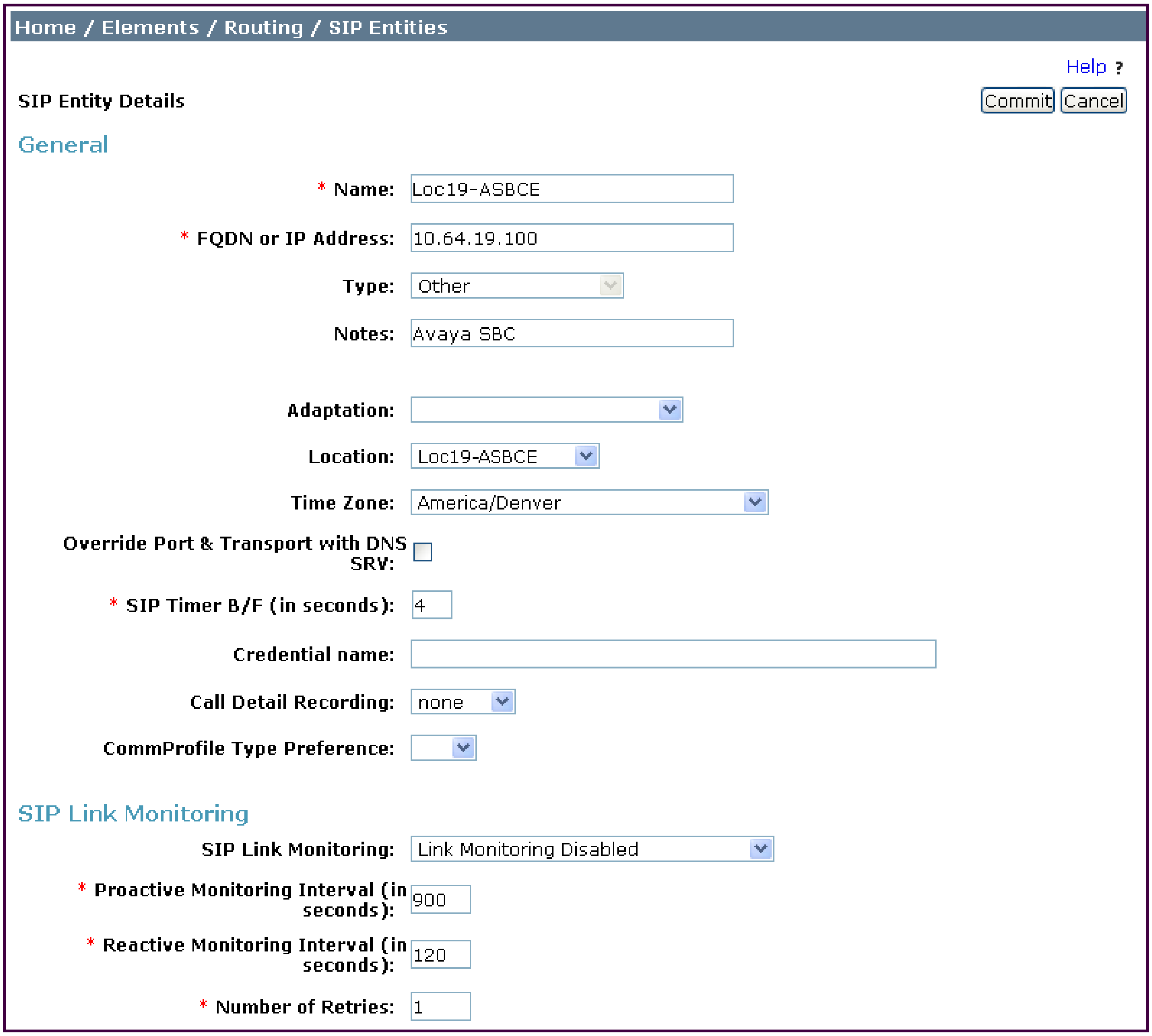
For the compliance test, four **Port** entries were added.



The following screen shows the addition of CS1000E. The **FQDN or IP Address** field is set to the IP address of the Node IP on CS1000E defined in **Section 5.1.1**. The **Adaptation** field is set to the **CS1K-Adaptation** created in **Section 6.4** and the Location is set to the one defined for CS1000E in **Section 6.3**.



The following screen shows the addition of Avaya SBCE SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The Location is set to the one defined for Avaya SBCE in **Section 6.3**. **Link Monitoring Disabled** was selected for **SIP Link Monitoring**.



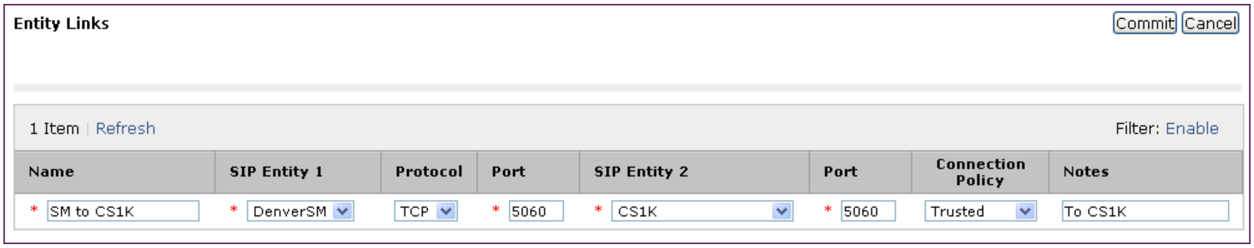
6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to CS1000E and one to Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system. For CS1000E, select the CS1000E SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Trusted:** Check this box. **Note**: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

Click **Commit** to save. The following screens illustrate the Entity Links to CS1000E and Avaya SBCE.

Entity Link to CS1000E:

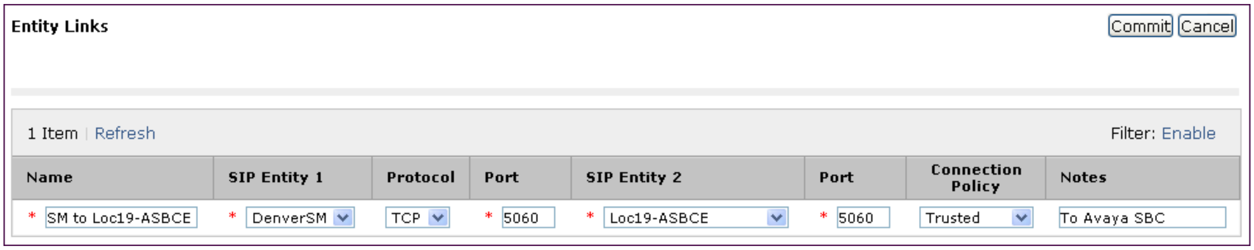

Entity Links

Commit Cancel

1 Item | Refresh — Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to CS1K	* DenverSM	TCP	* 5060	* CS1K	* 5060	Trusted	To CS1K

Entity Link to Avaya SBCE:


Entity Links

Commit Cancel

1 Item | Refresh — Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to Loc19-ASBCE	* DenverSM	TCP	* 5060	* Loc19-ASBCE	* 5060	Trusted	To Avaya SBC

6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added; one for CS1000E and one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

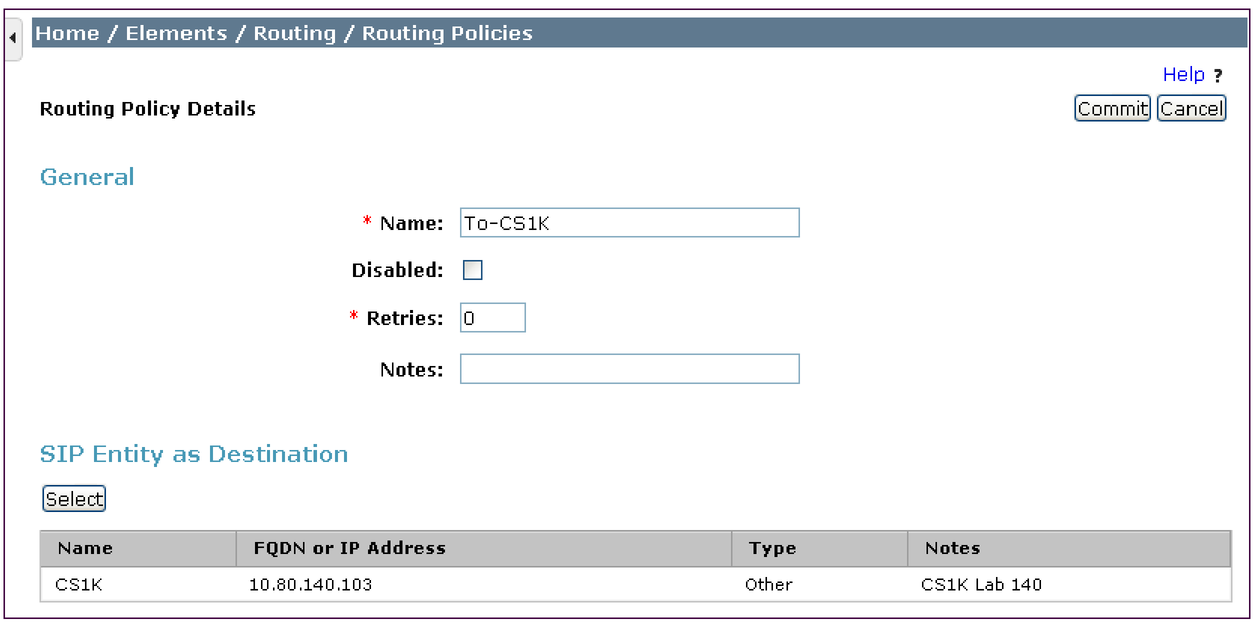
In the **General** section, enter the following values. Use default values for all remaining fields:

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

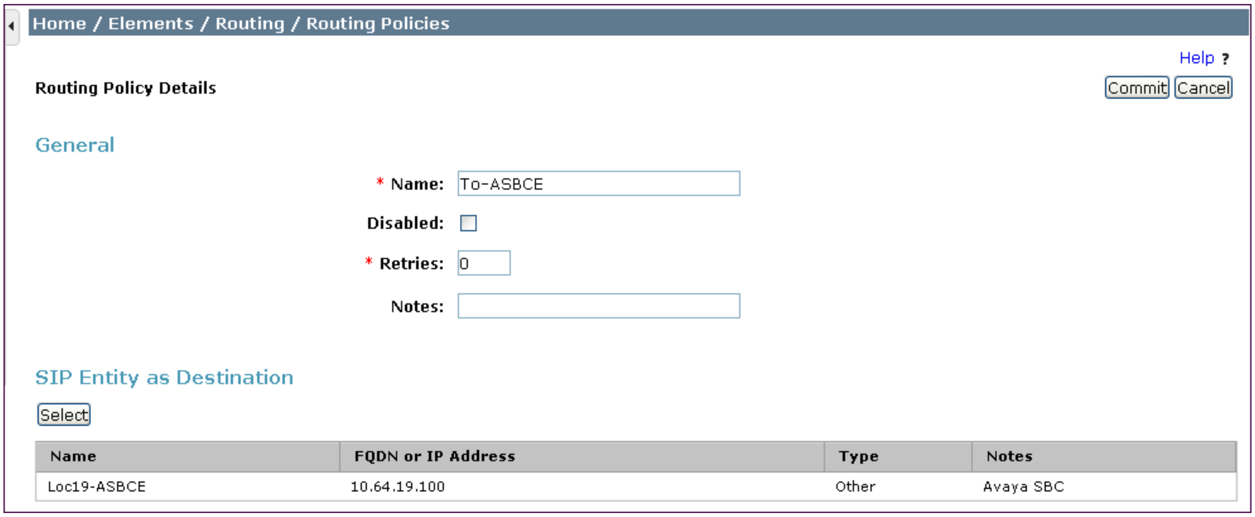
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select** (not shown)**.** The selected SIP Entity displays on the **Routing Policy Details** page as shown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

The following screens show the Routing Policies for CS1000E and Avaya SBCE.

Routing Policy for CS1000E:



Routing Policy for Avaya SBCE:



6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from CS1000E to Cincinnati Bell and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

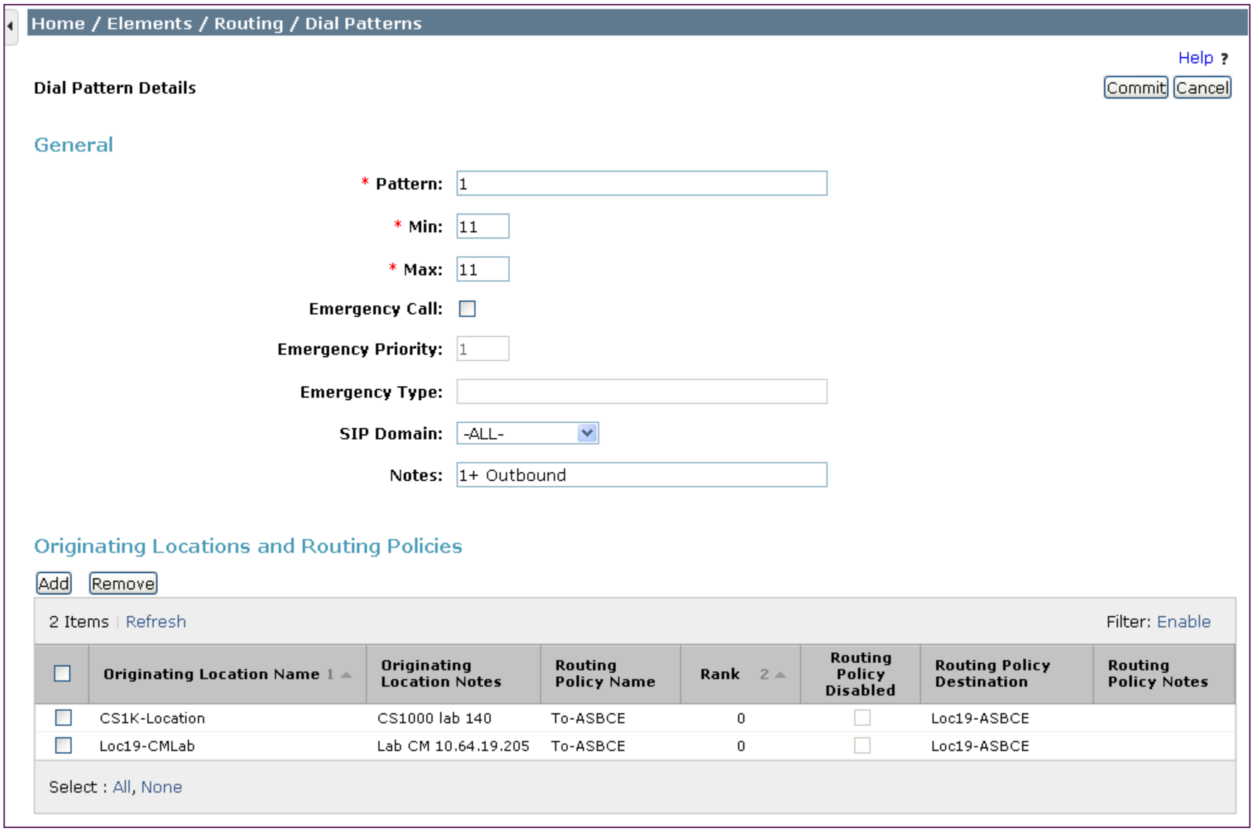
In the **General** section, enter the following values. Use default values for all remaining fields:

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

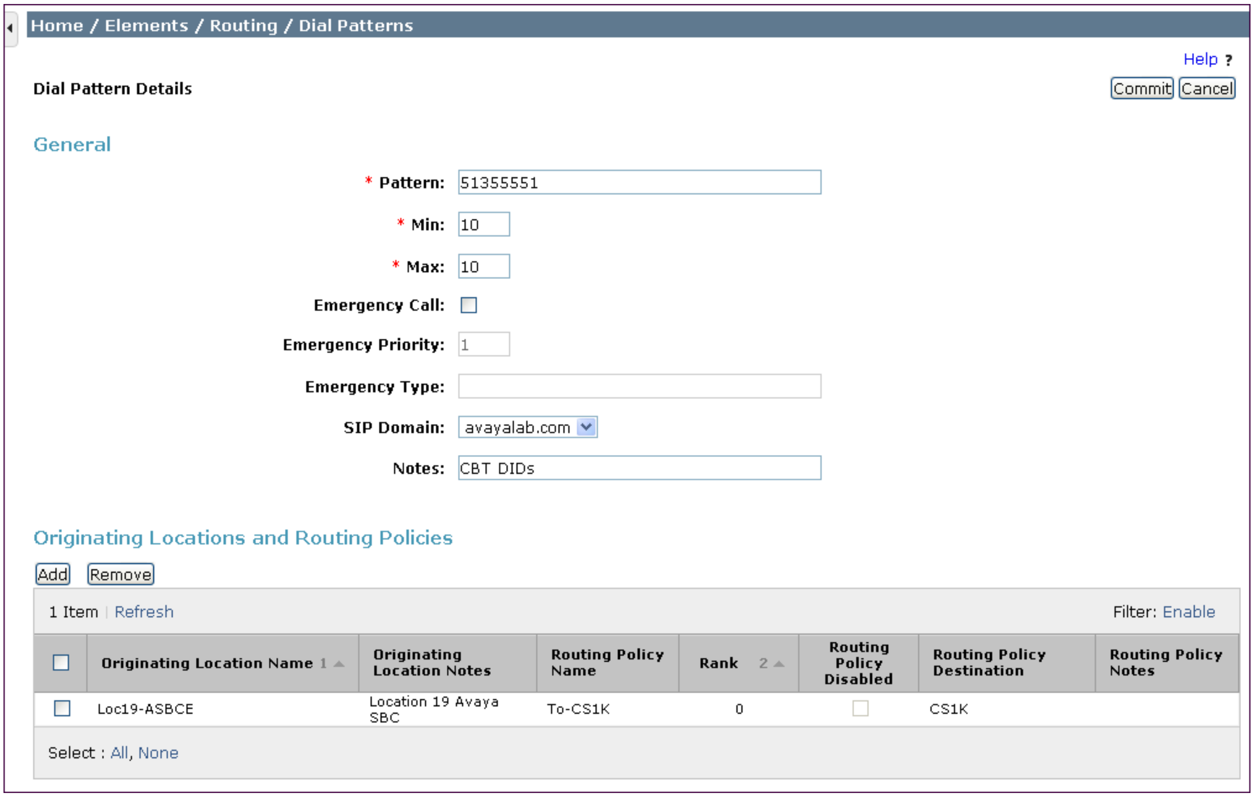
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that that in the shared test environment, 11 digit dialed numbers that begin with **1** originating from **CS1K-Location** uses route policy **To-ASBCE**.



The second example shows that a **10** digit number starting with **51355551** and originating from **Loc19-ASBCE** uses route policy **To-CS1K**. This is a DID range 513-555-5100 through 513-555-5199 assigned to the enterprise from Cincinnati Bell.



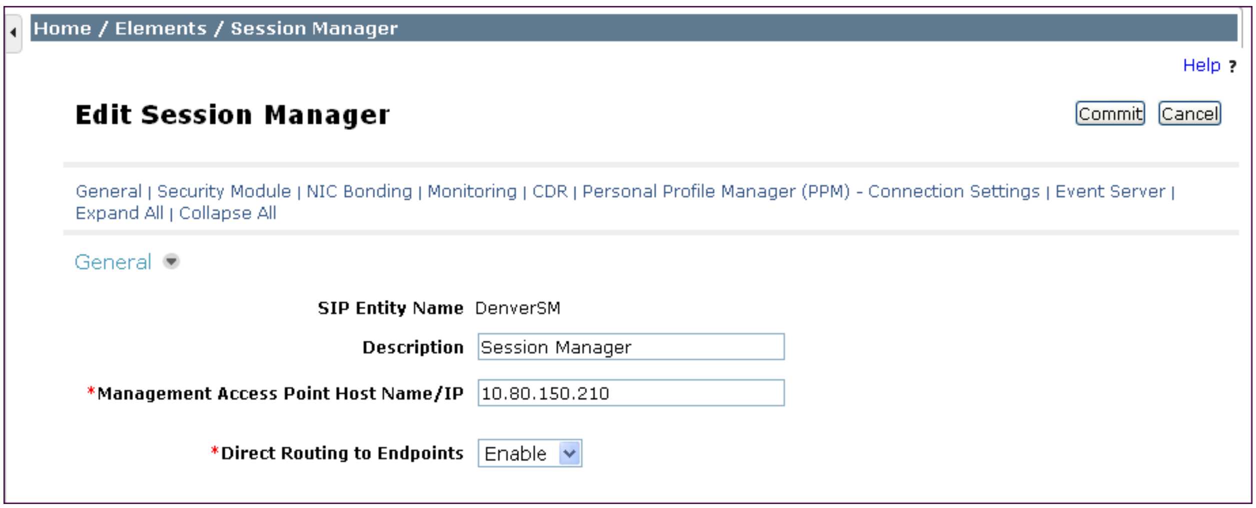
6.9. Add/Verify Avaya Aura® Session Manager Instance

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

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

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

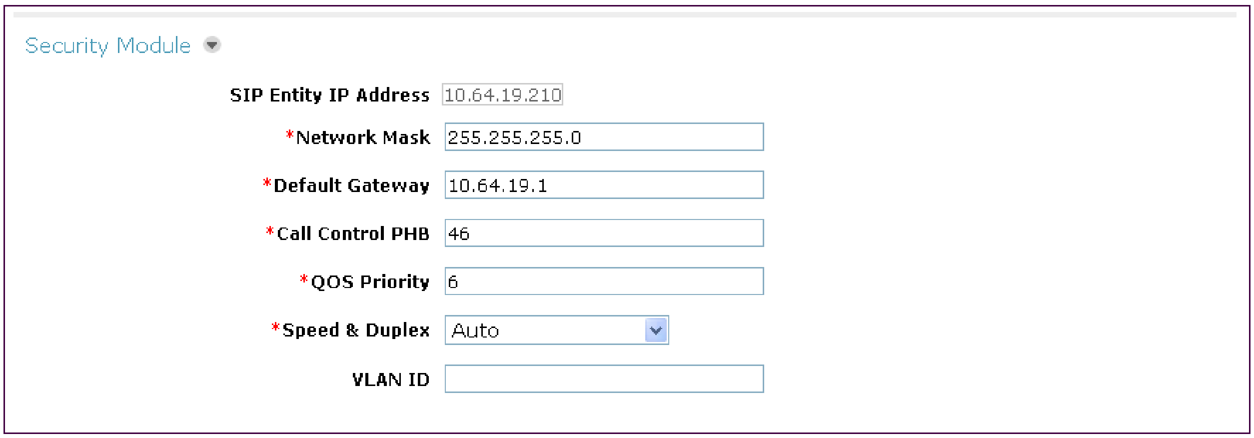
The screen below shows the Session Manager values used for the compliance test.



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

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

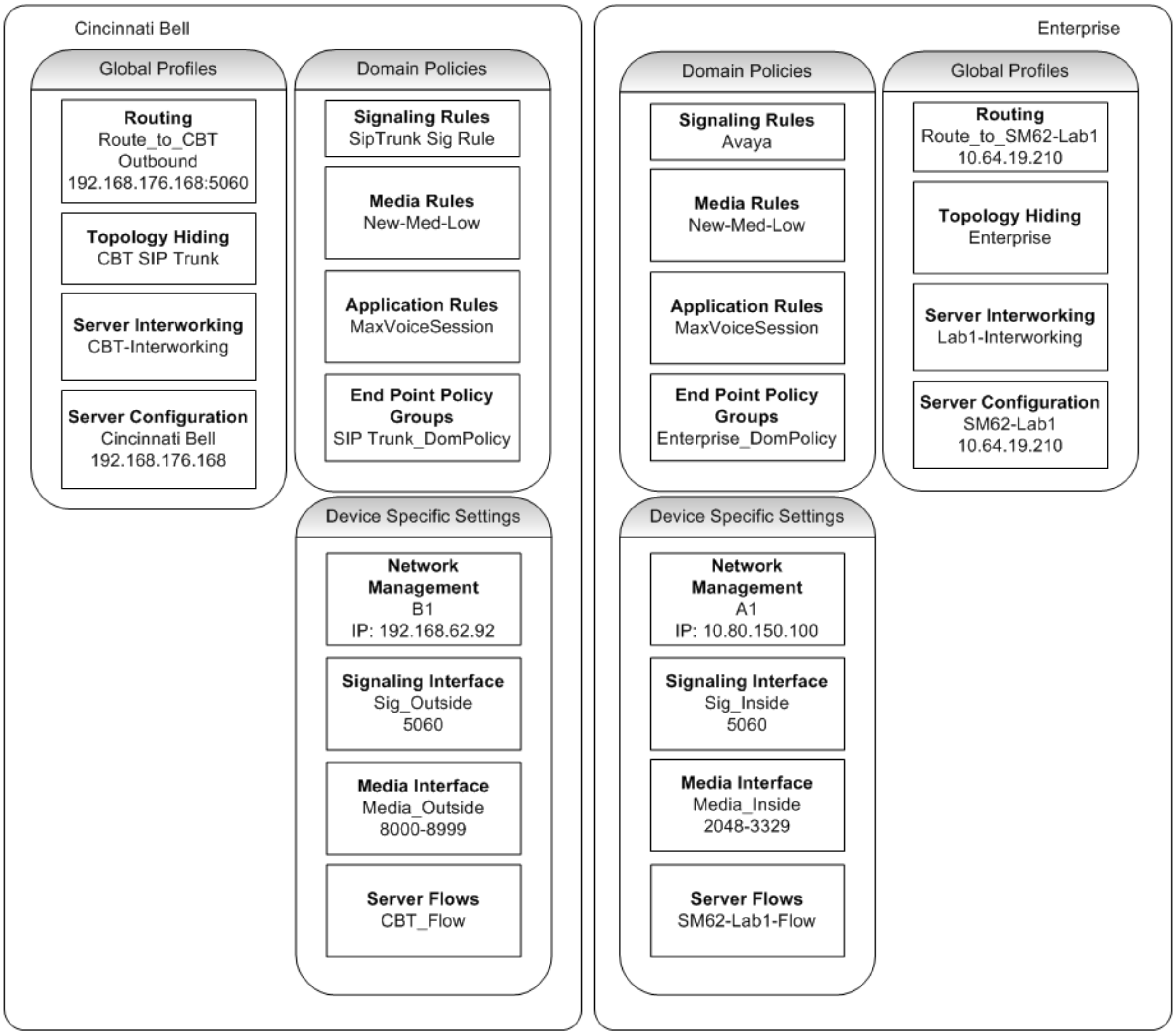
Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.



7. Configure Avaya Session Border Controller for Enterprise

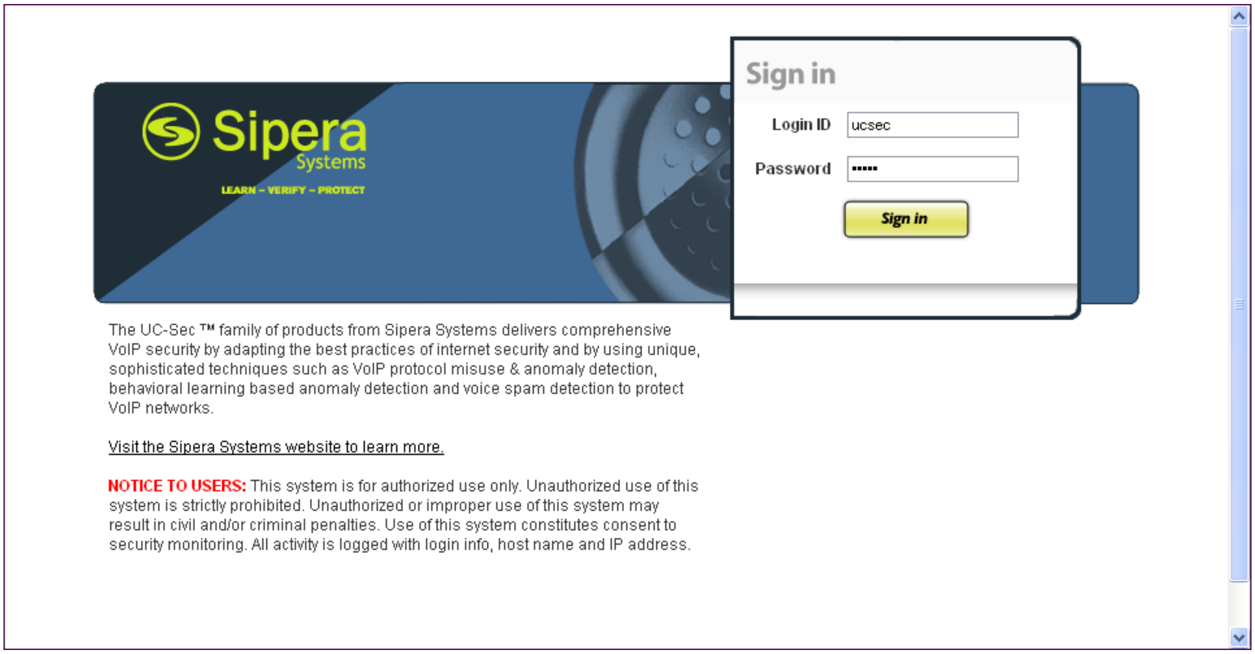
This section covers the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed.

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.

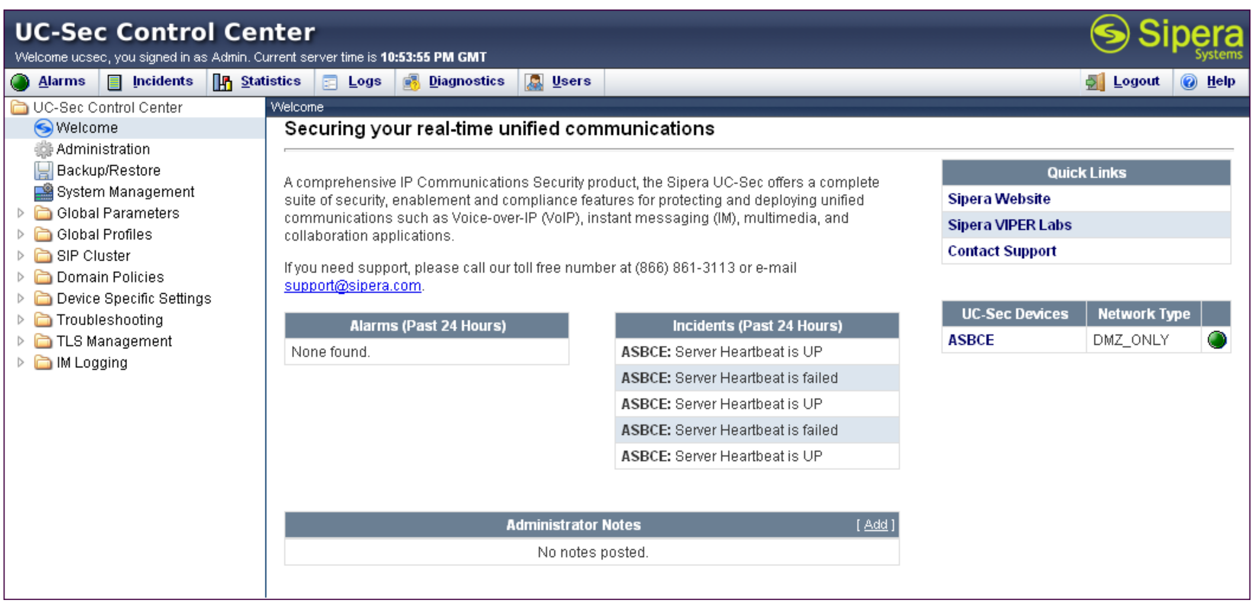


Use a WEB browser to access the Element Management Server (EMS) web interface, and enter https://<ip-addr>/ucsec in the address field of the web browser, where <ip-addr> is the management LAN IP address of the Avaya SBCE.

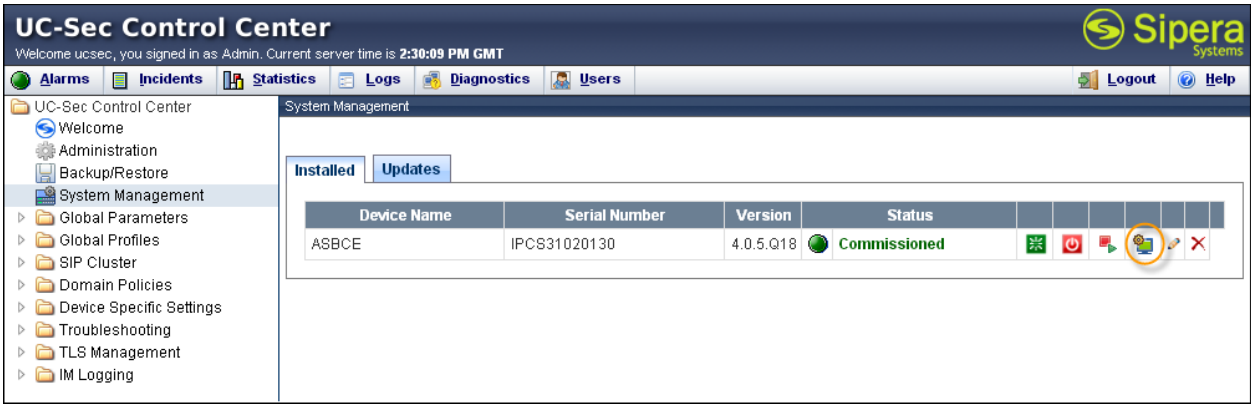
Log in with the appropriate credentials. Click **Sign In**.



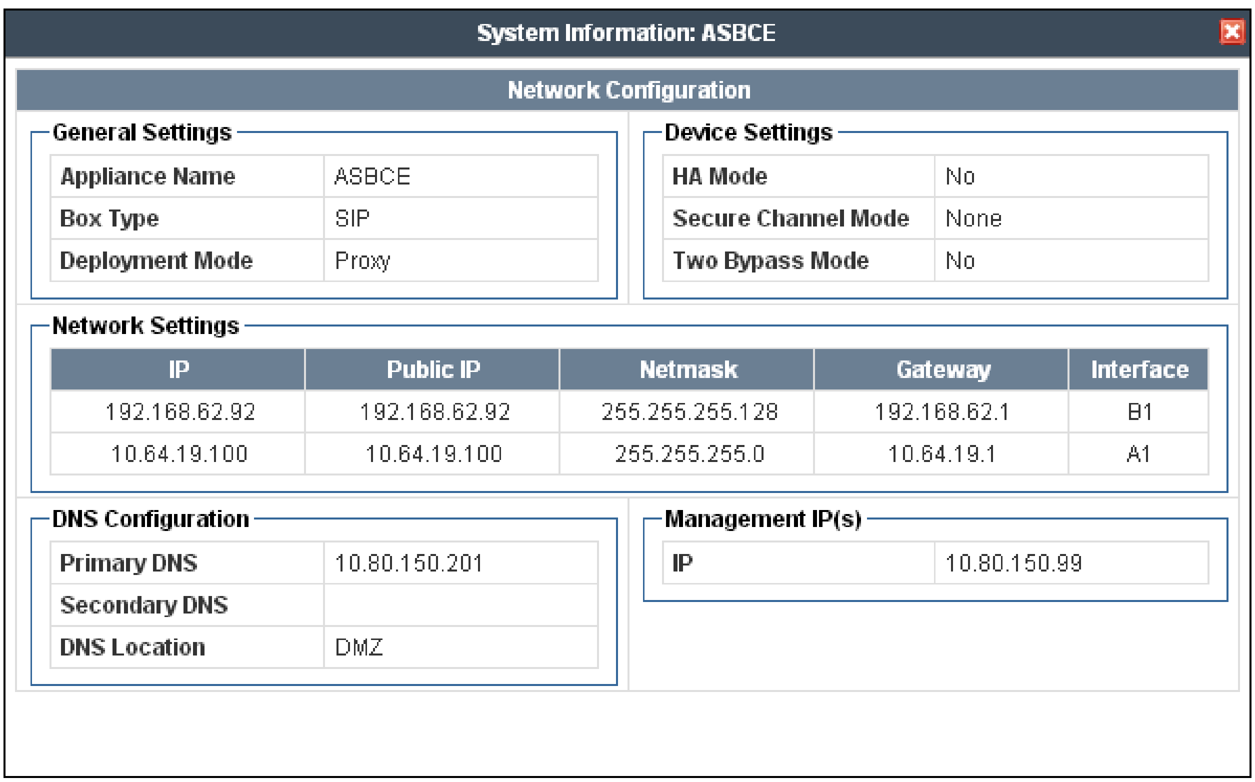
The main page of the UC-Sec Control Center will appear.



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.

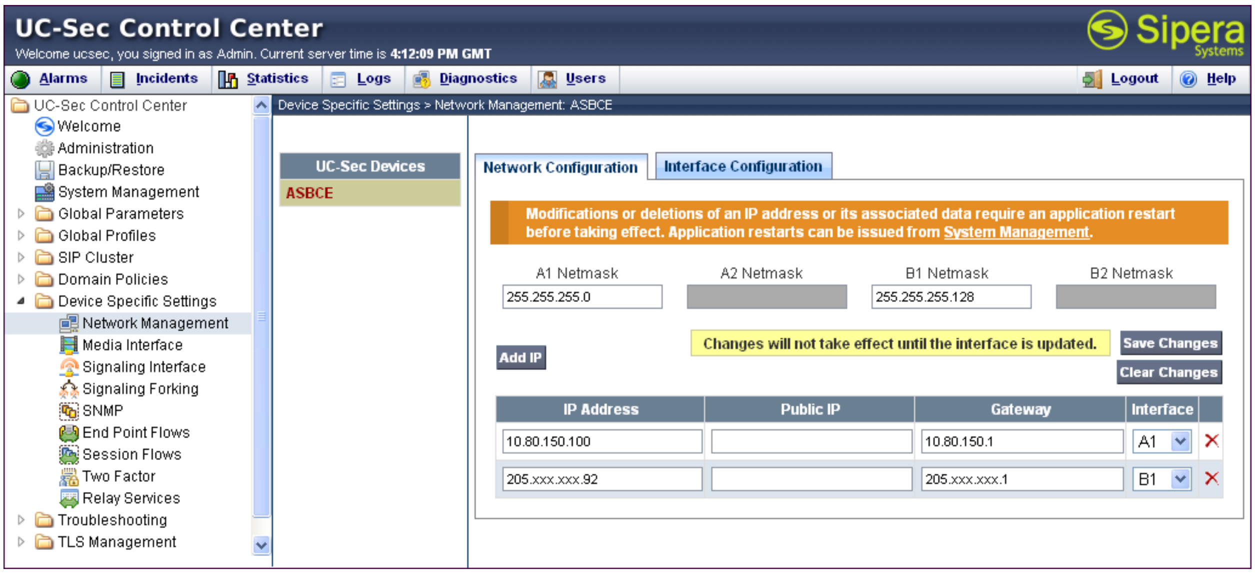


The **System Information** screen shows the **Network Settings, DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other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

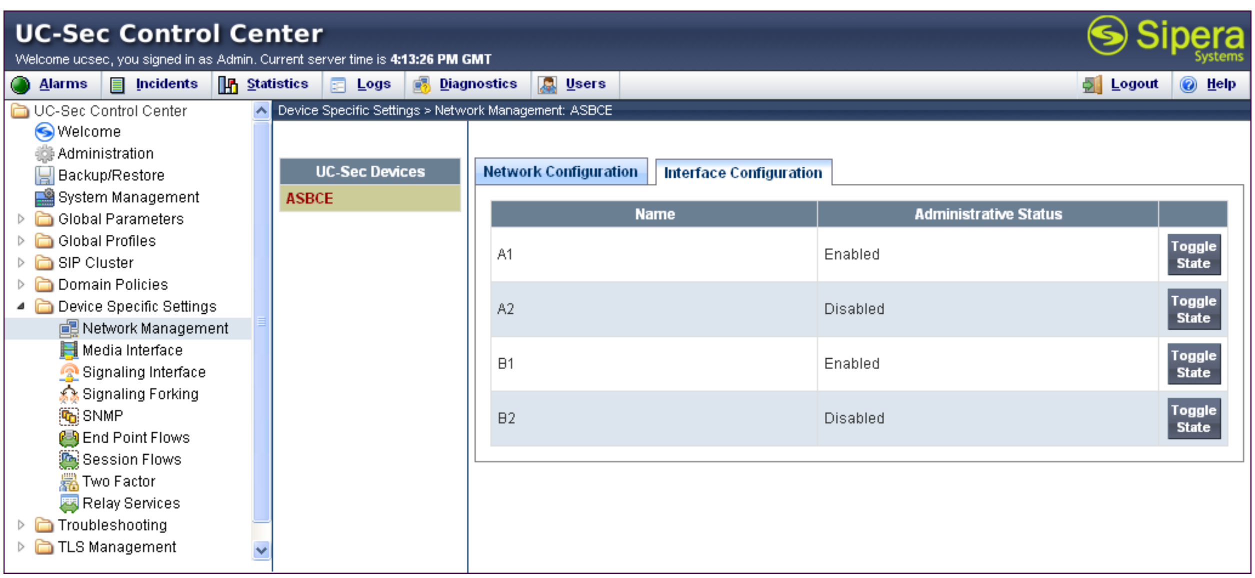


7.1. Network Management

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**.



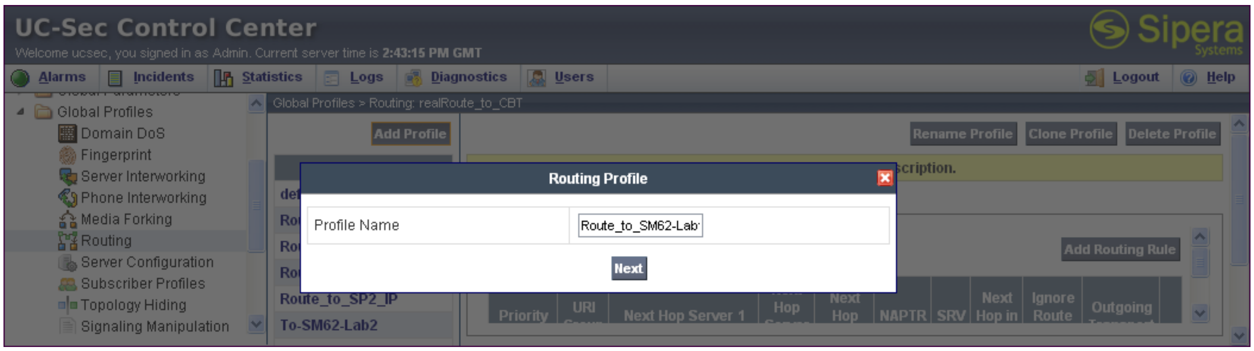
The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click its **Toggle State** button.



7.2. 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 Session Manager and Cincinnati Bell eVantage IP Service. 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.

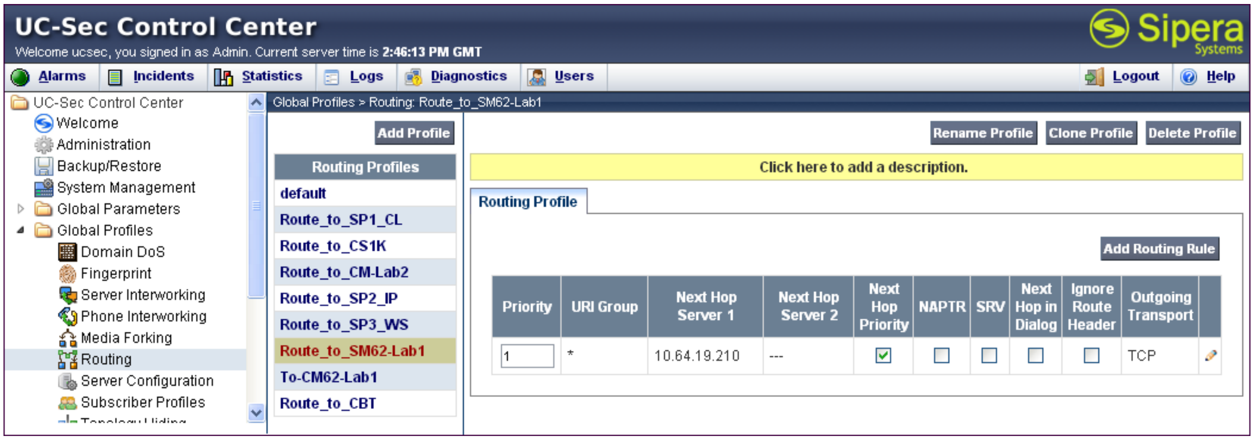


In the new window that appears, enter the following values (not shown). Use default values for all remaining fields:

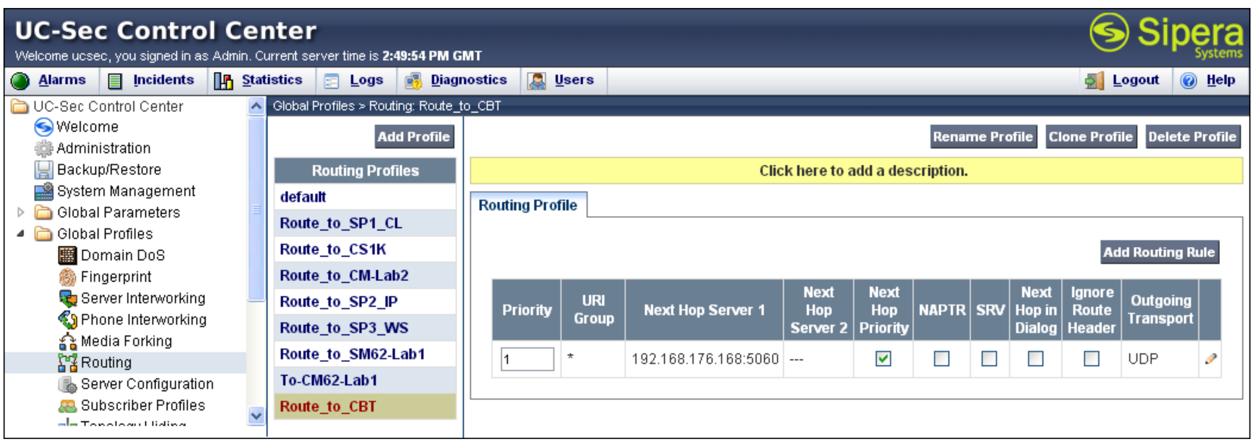
- **URI Group:** Select "*****" from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server**: 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 Session Manager. The **Next Hop Server 1** IP address must match the IP address of Session Manager Entity created in **Section 6.5**. The **Outgoing Transport** is set to **TCP** and matched the **Protocol** set in the Session Manager Entity Link for Avaya SBCE in **Section 6.6**.



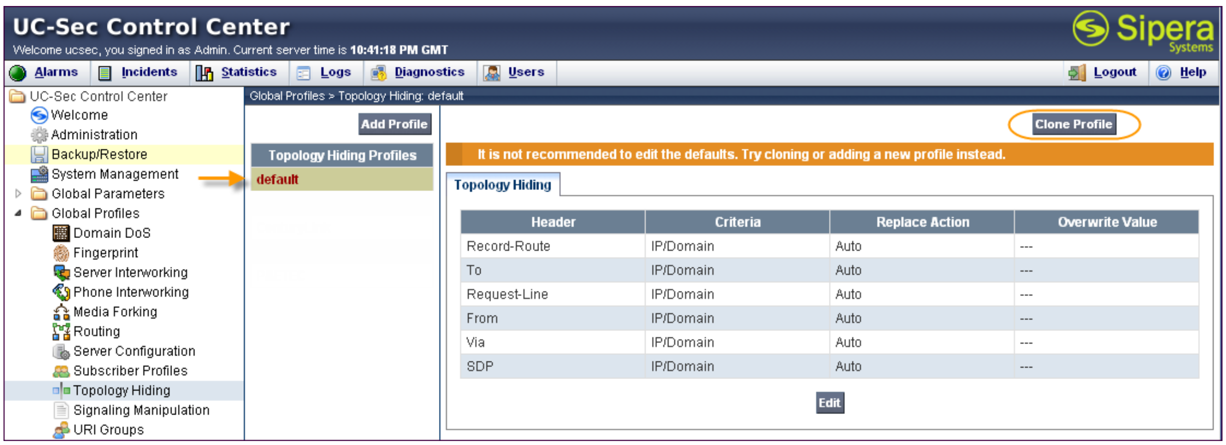
The following screen shows the Routing Profile to Cincinnati Bell. In the **Next Hop Server 1** field enter the IP address and port that Cincinnati Bell uses to listen for SIP traffic. Enter **UDP** for the **Outgoing Transport field**.



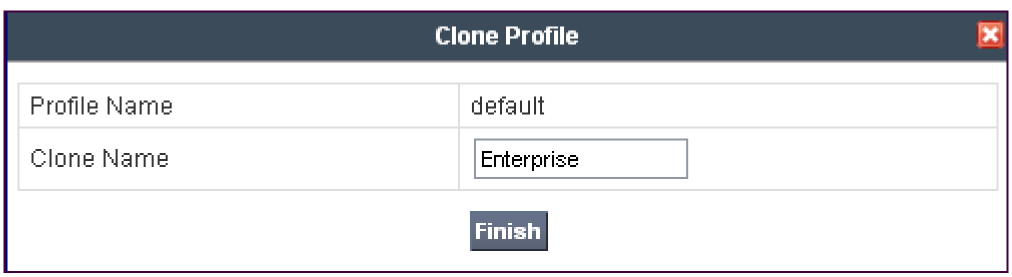
7.3. Topology Hiding Profile

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.

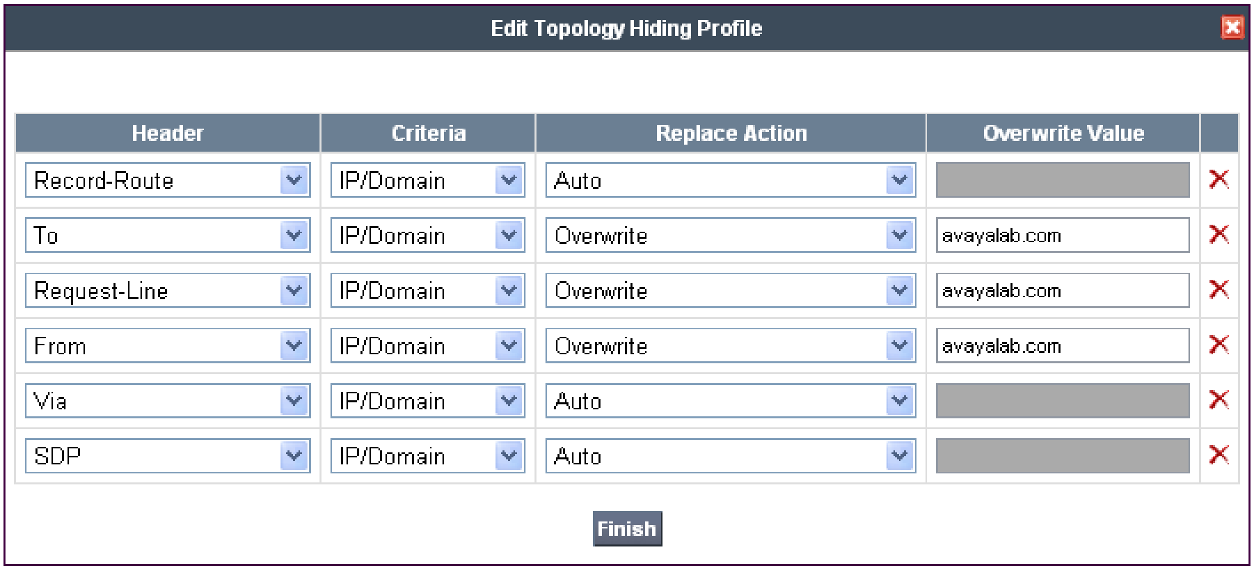
Create a Topology Hiding Profile for the enterprise and Cincinnati Bell eVantage IP Service. In the sample configuration, the **Enterprise** and **CBT SIP Trunk** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center → Global Profiles → Topology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



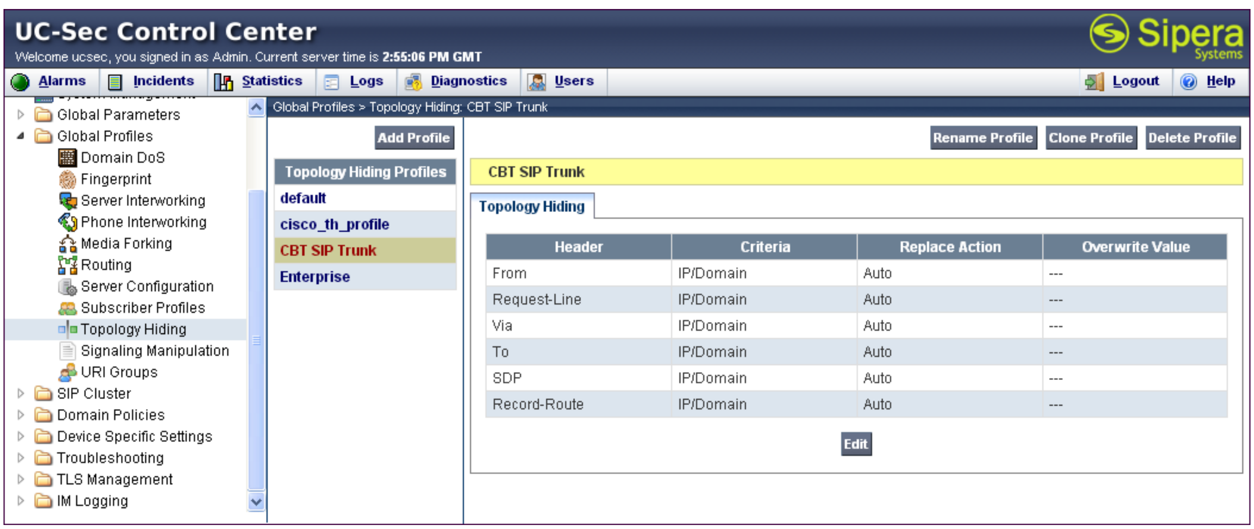
Enter a descriptive name for the new profile and click **Finish**.



Edit the **Enterprise** profile to overwrite the headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager (**Section 6.2**). Click **Finish** to save the changes.



It is not necessary to modify the **CBT SIP Trunk** profile from the default values. The following screen shows the Topology Hiding Policy created for Cincinnati Bell.



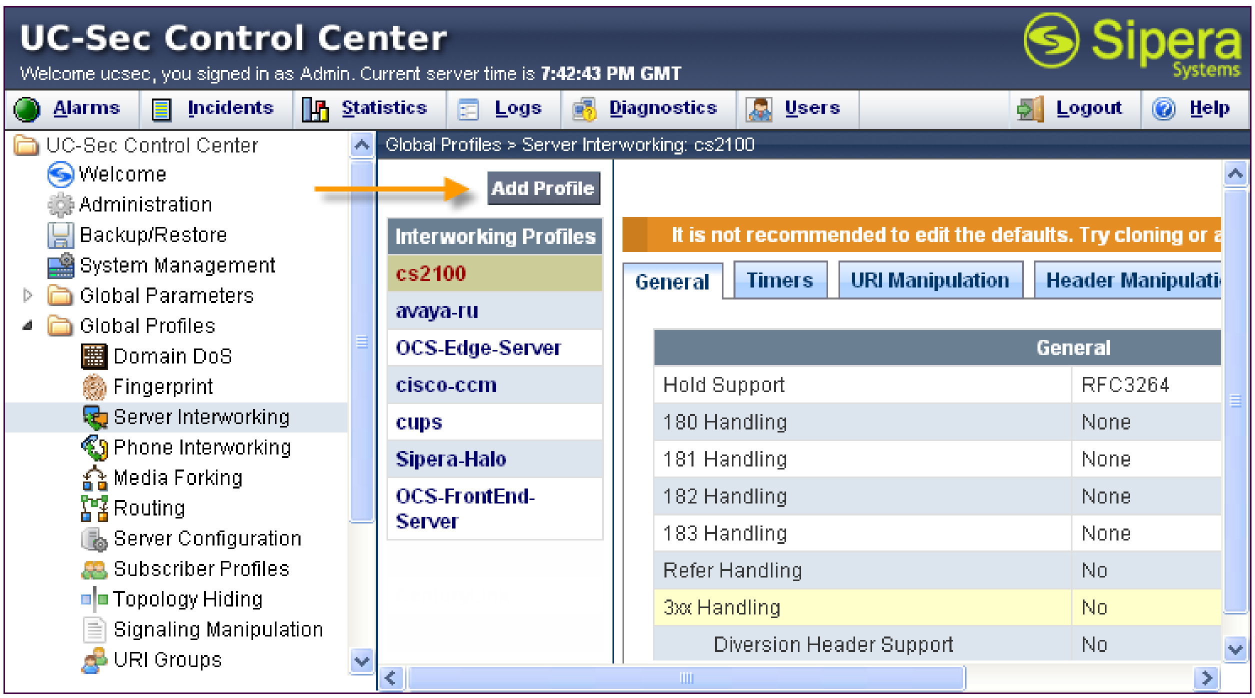
7.4. Server Interworking Profile

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.

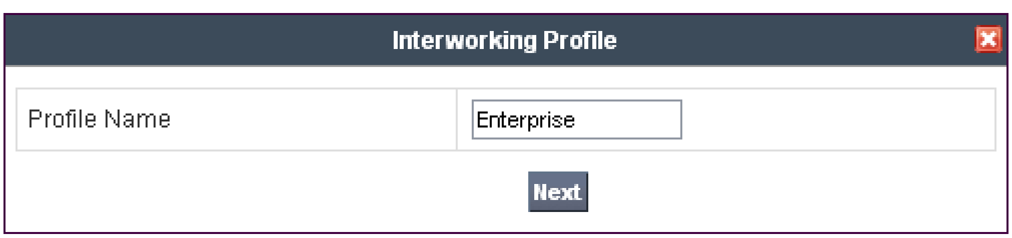
In the sample configuration, separate Server Interworking Profiles were created for Enterprise and Cincinnati Bell.

7.4.1. 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.



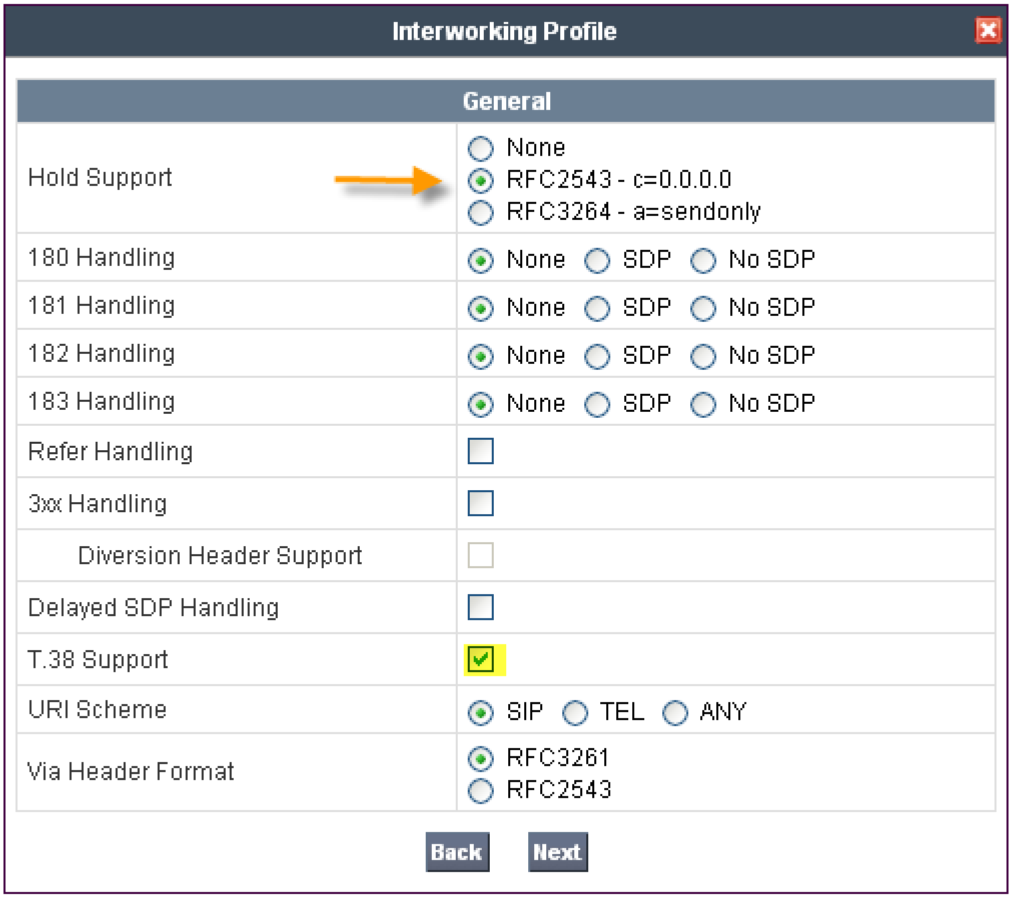
Enter a descriptive name for the new profile and click **Next** to continue.



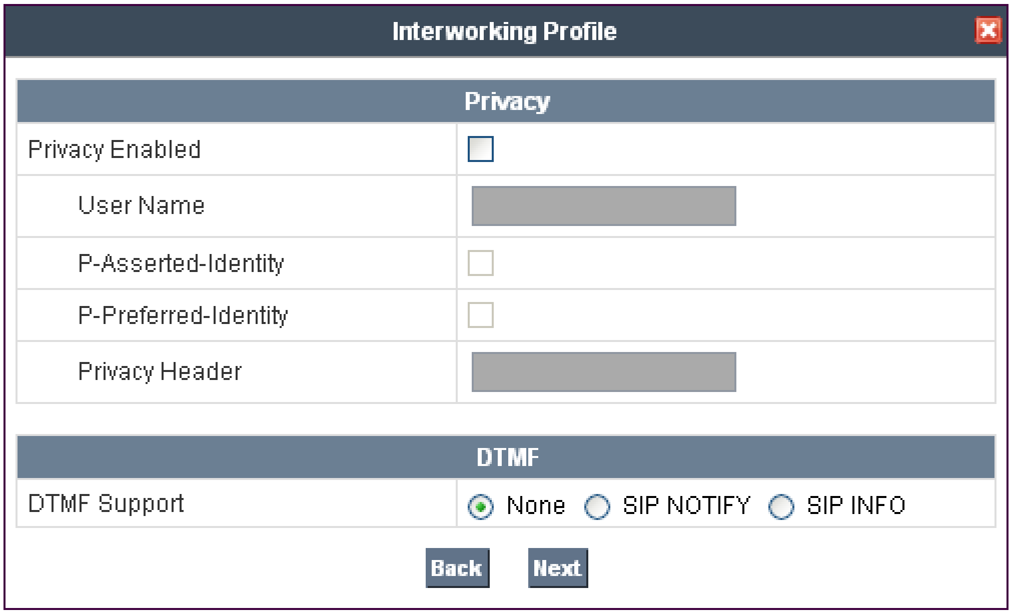
In the new window that appears, enter the following values. Use default values for all remaining fields:

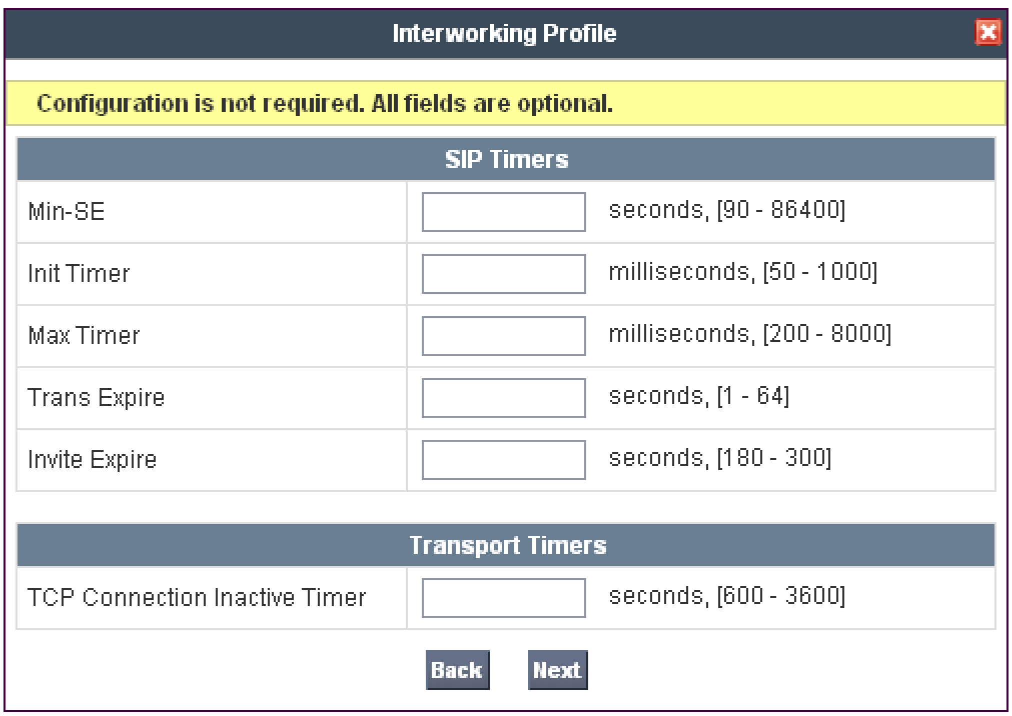
- **Hold Support:** Select **RFC2543 - c=0.0.0.0**.
- **T.38 Support:** Checked.

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



Default values can be used for the next two windows that appear. Click **Next** to continue.

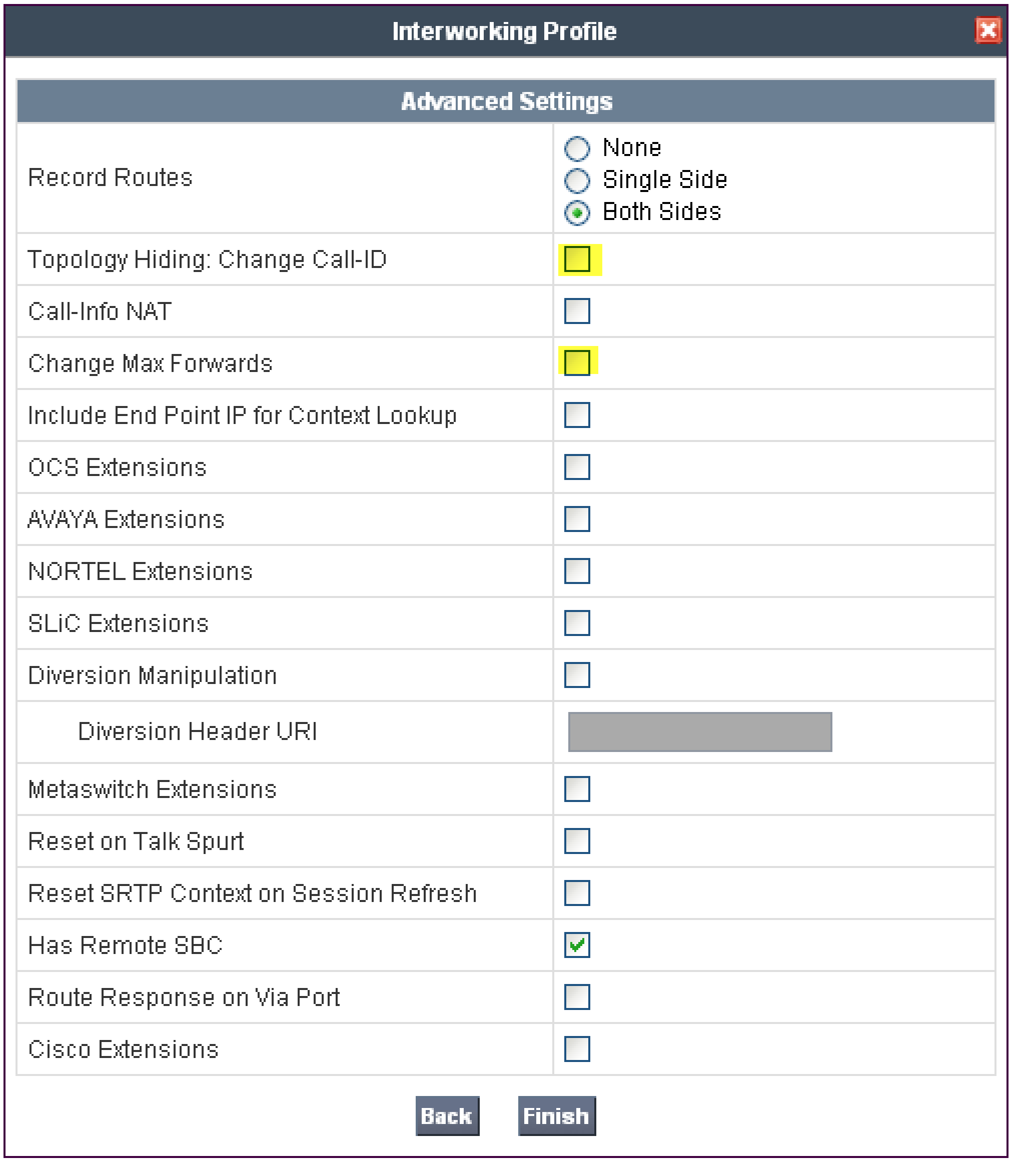




On the **Advanced Settings** window uncheck the following default settings:

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

Click **Finish** to save changes.



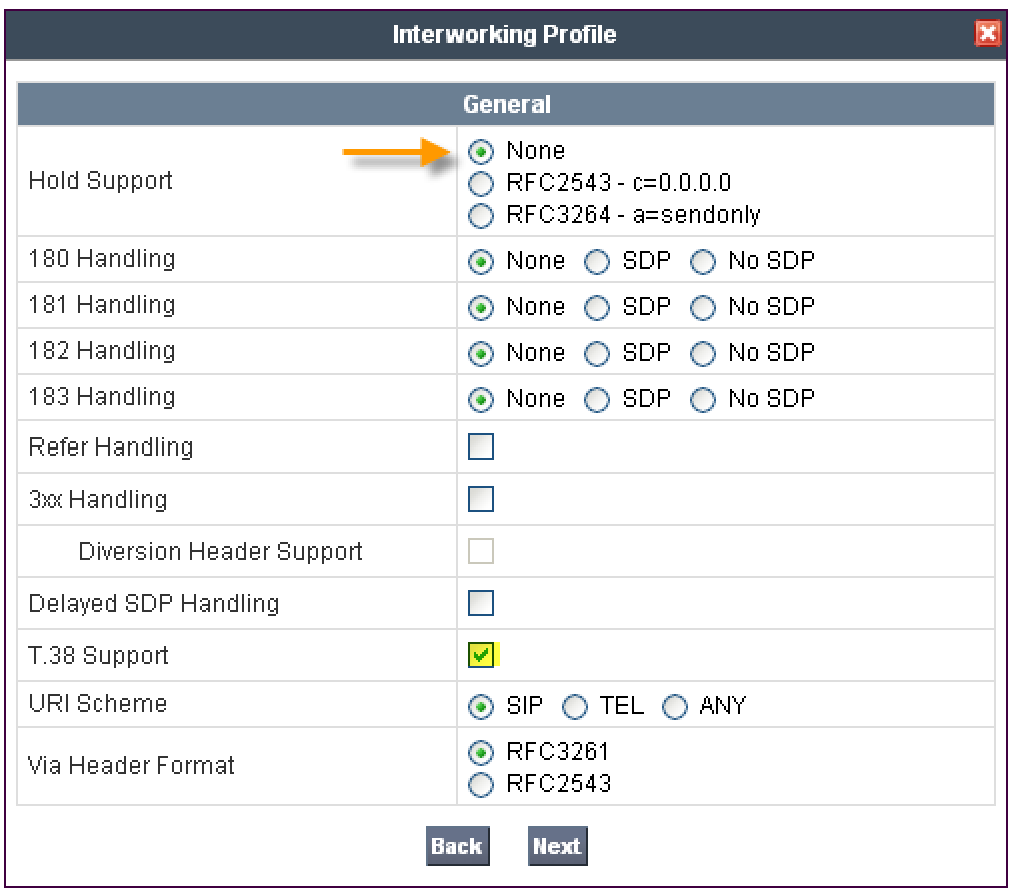
7.4.2. Server Interworking Profile – Cincinnati Bell

To create a new Server Interworking Profile for Cincinnati Bell, 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.

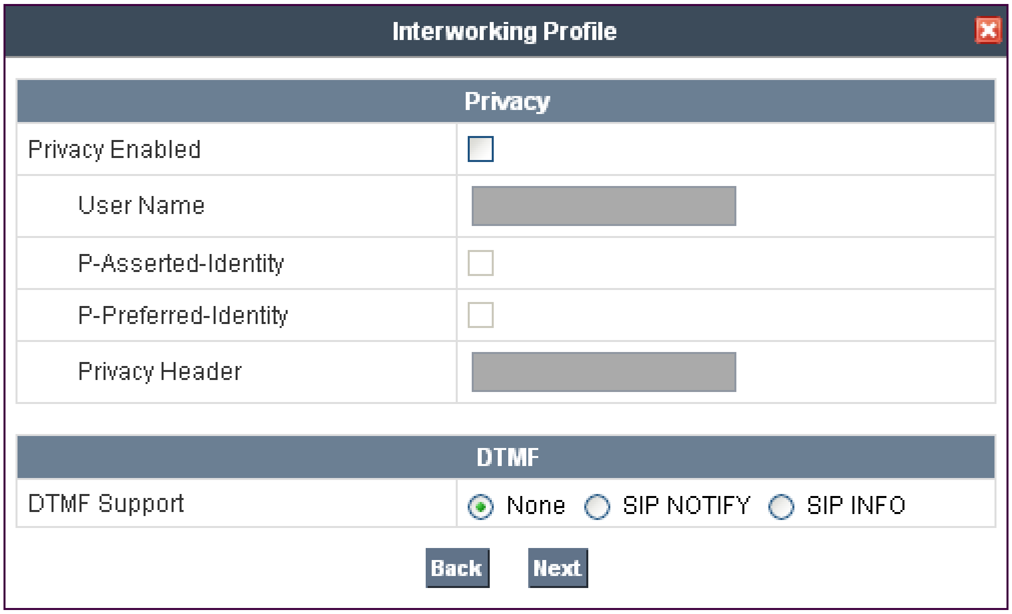
In the new window that appears, enter the following values. Use default values for all remaining fields:

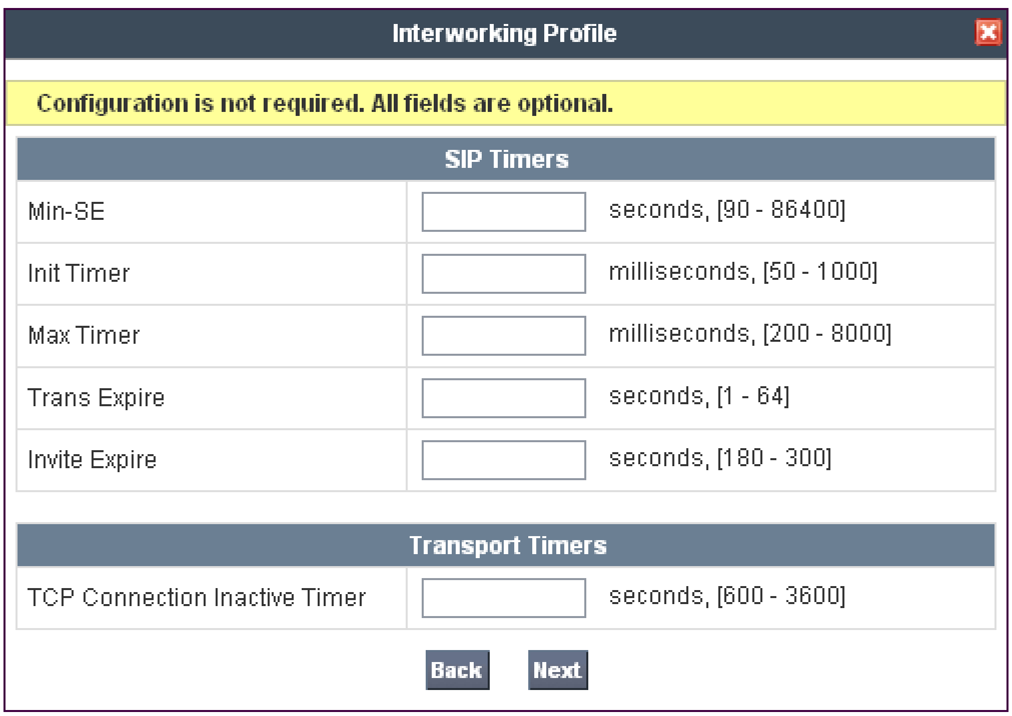
- **Hold Support:** **None**
- **T.38 Support:** Checked.

Click **Next** to continue.



Default values can be used for the next two windows that appear. Click **Next** to continue.

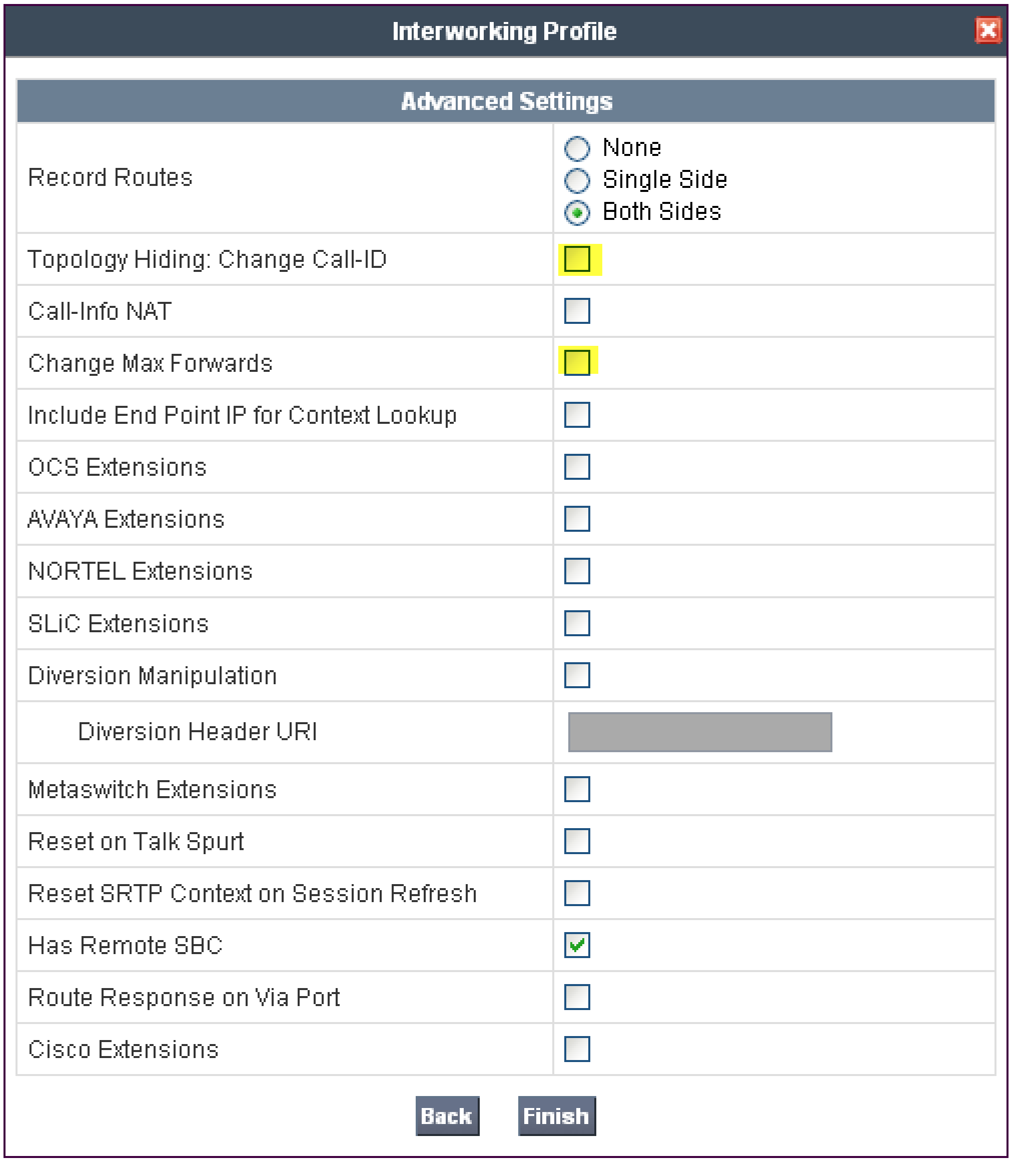




On the **Advanced Settings** window uncheck the following default settings:

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

Click **Finish** to save changes.



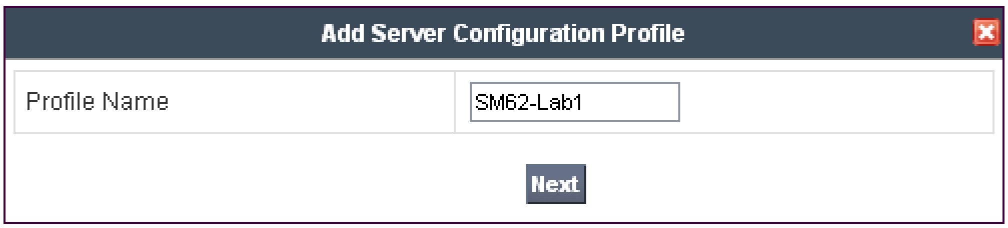
7.5. Server Configuration

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 Session Manager and Cincinnati Bell.

7.5.1. Server Configuration – Session Manager

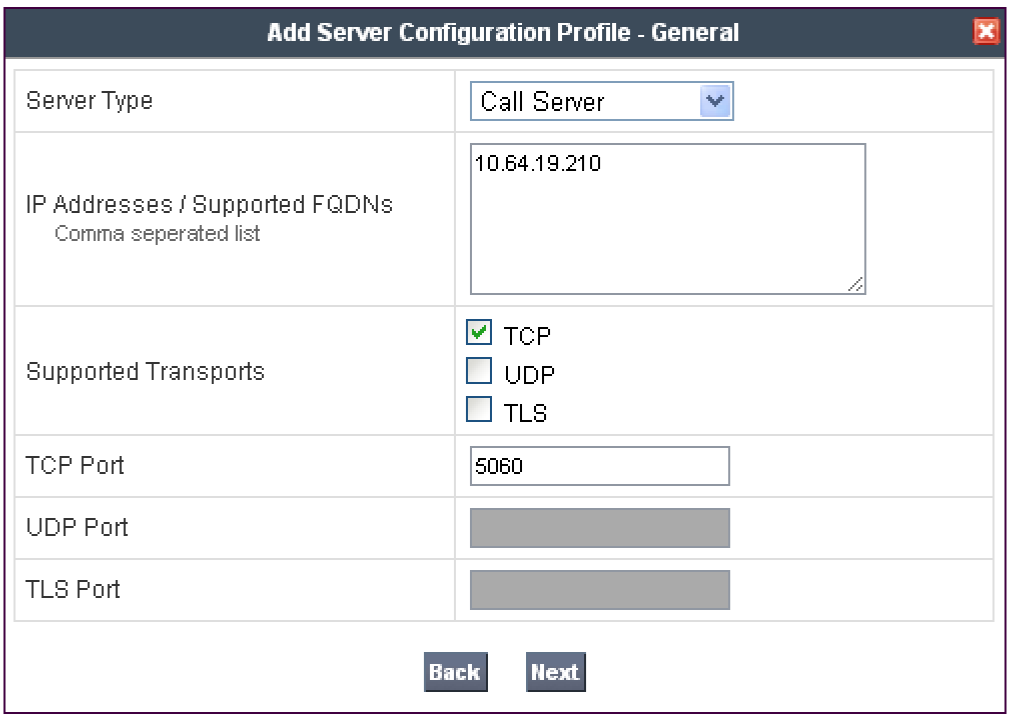
To add a Server Configuration Profile for Session Manager, navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** (not shown). Enter a descriptive name for the new profile and click **Next**.



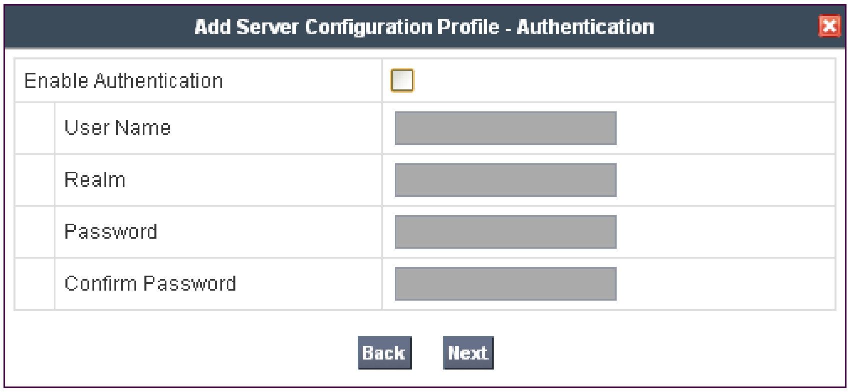
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Call Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of Session Manager. This should match the IP address of the SIP Entity for Session Manager in **Section 6.5**.
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Entity Link in Session Manager in **Section 6.6**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Entity Link in Session Manager in **Section 6.6**.

Click **Next** to continue.



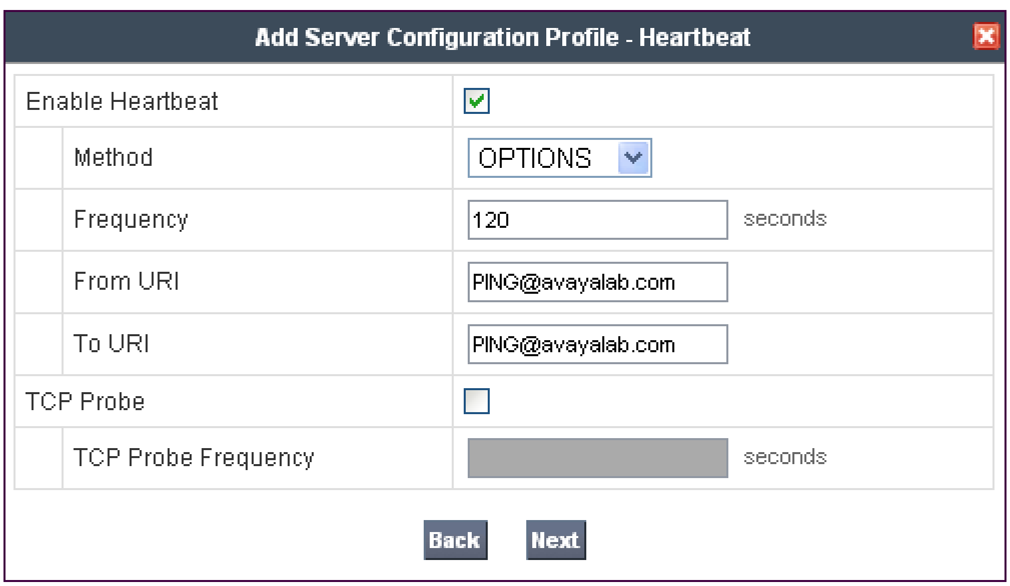
Verify **Enable Authentication** is unchecked as Session Manager does not require authentication. Click **Next** to continue.



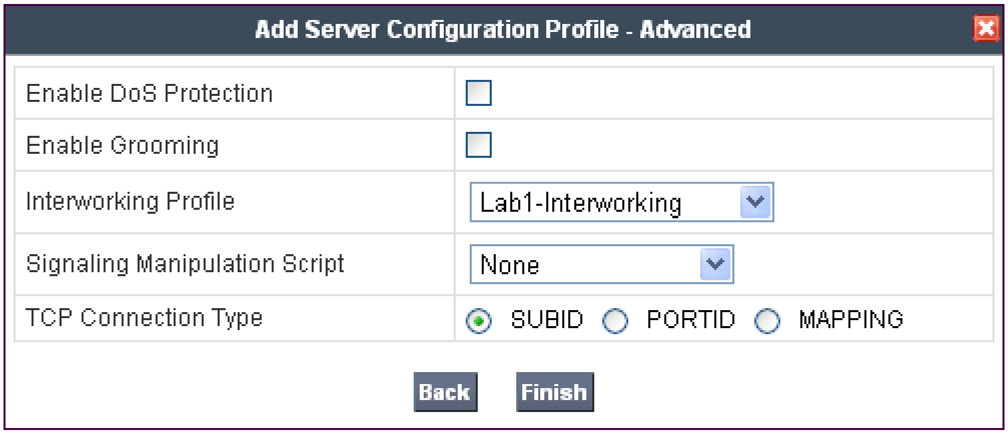
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **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 Session Manager. For compliance testing **120** 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.

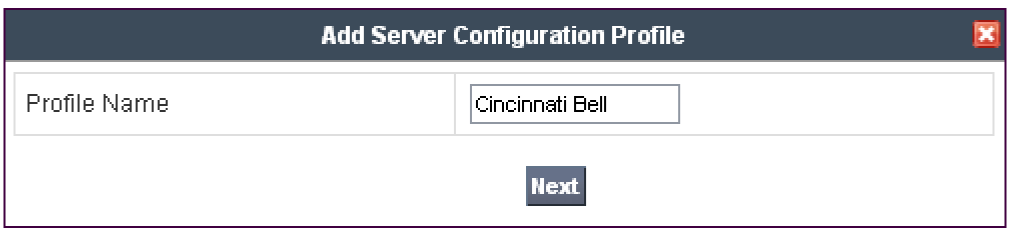


In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.4.1**. Use default values for all remaining fields. Click **Finish** to save the configuration.



7.5.2. Server Configuration - Cincinnati Bell

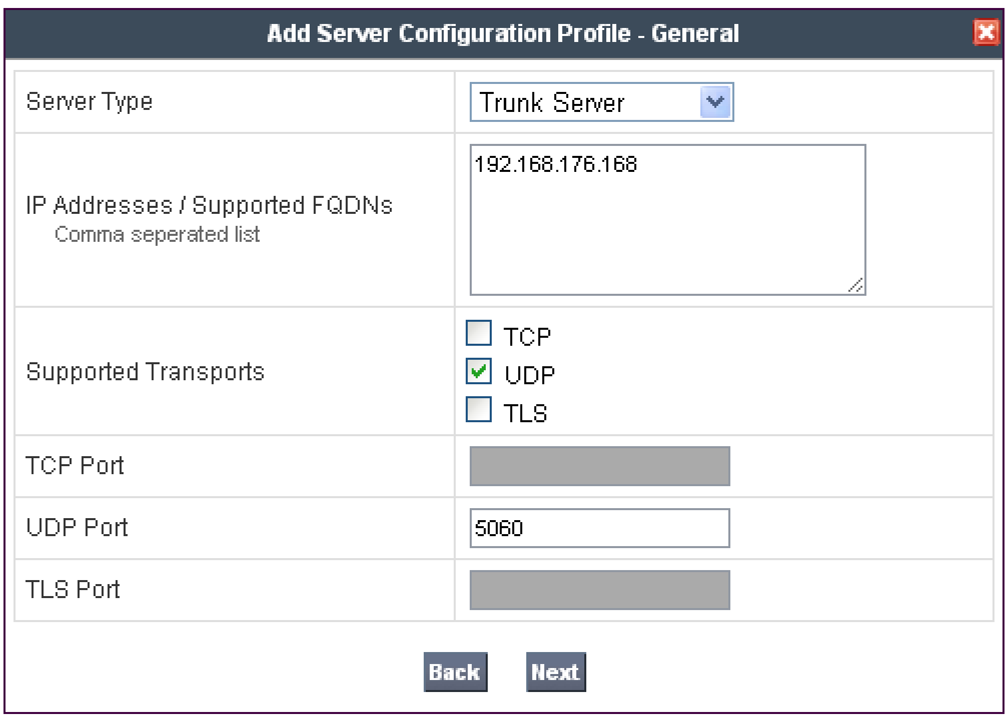
To add a Server Configuration Profile for Cincinnati Bell, navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** (not shown). Enter a descriptive name for the new profile and click **Next**.



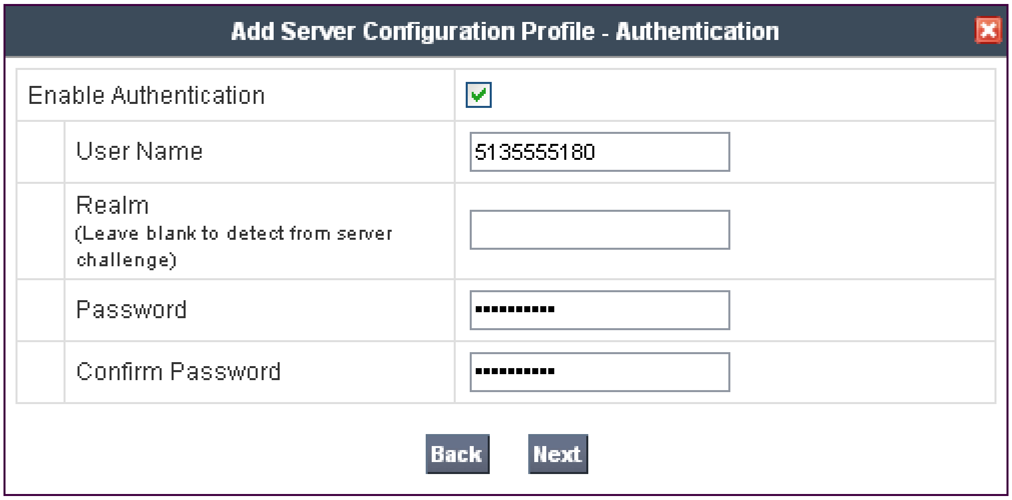
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Trunk Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address(es) of the SIP proxy(ies) of the service provider. In the case of the compliance test, this is the IP address of the Cincinnati Bell eVantage IP Service. This will associate the inbound SIP messages from Cincinnati Bell to this Sever Configuration.
- **Supported Transports:** Select the transport protocol to be used for SIP traffic between Avaya SBCE and Cincinnati Bell. For compliance testing **UDP** was used.
- **UDP Port:** Enter the port number that Cincinnati Bell uses to send SIP traffic. For compliance testing **5060** was used.

Click **Next** to continue.



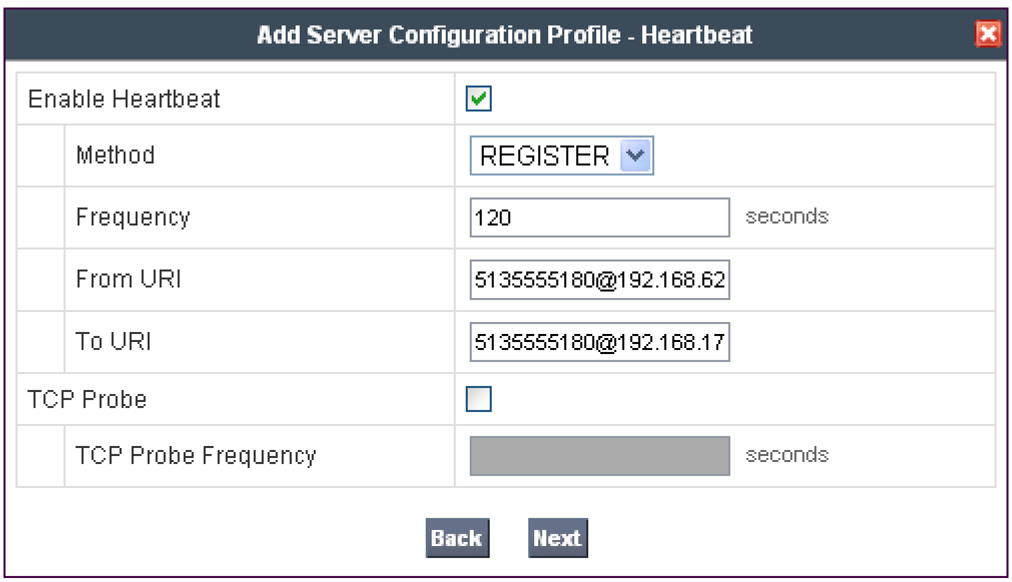
If using trunk registration, select **Enable Authentication**. Enter the user name provided by Cincinnati Bell in the **User Name** field. Leave the **Realm** blank to have it detected from the server challenge. Enter the password provided by Cincinnati Bell in the **Password** field. Click **Next** to continue.



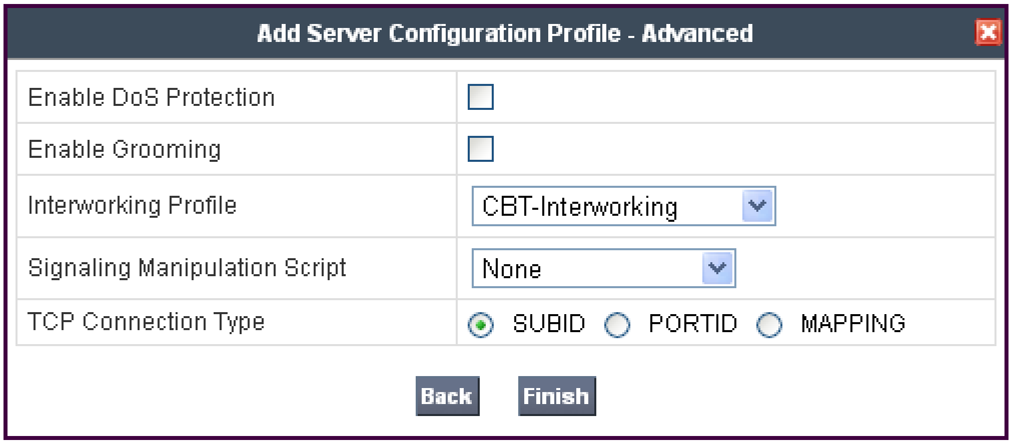
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Enabled Heartbeat:** Checked.
- **Method:** If using trunk registration, select **REGISTER** from the drop-down box. Otherwise, select **OPTIONS**.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send REGISTER/OPTIONS messages to Cincinnati Bell. For compliance testing **120** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP REGISTER/OPTIONS. In the example below **5135555180@192.168.62.92** was used.
- **TO URI:** Enter an URI to be sent in the TO header for SIP REGISTER/OPTIONS. In the example below **5135555180@192.168.176.168** was used.

Click **Next** to continue.



In the new window that appears, select the **Interworking Profile** created for Cincinnati Bell in **Section 7.4.2**. Use default values for all remaining fields. Click **Finish** to save the configuration.

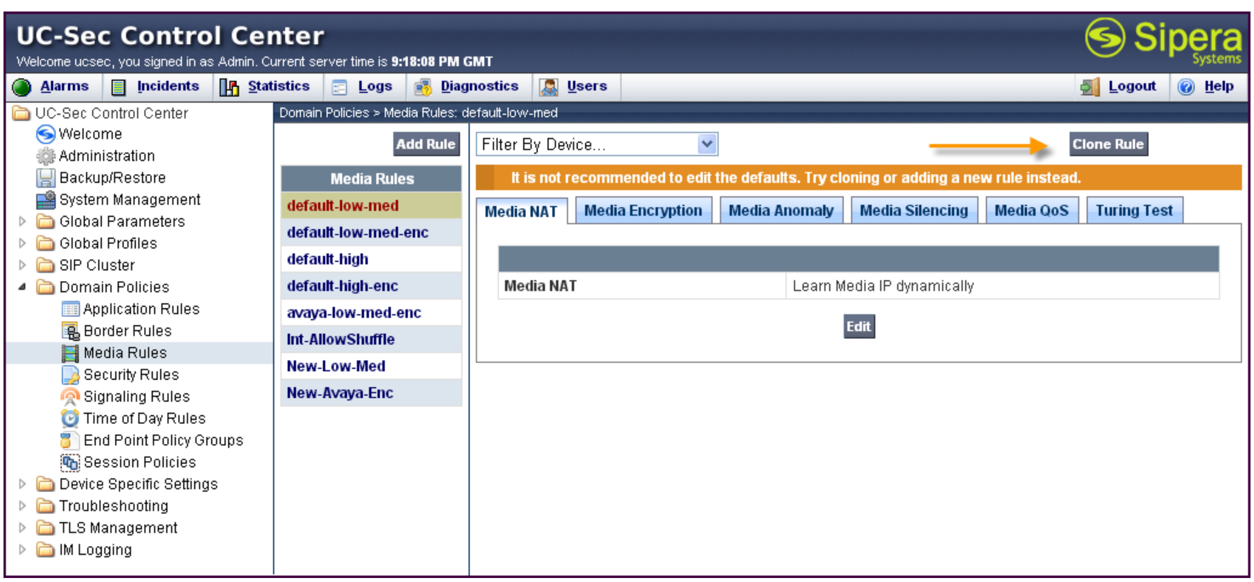


7.6. Media Rule

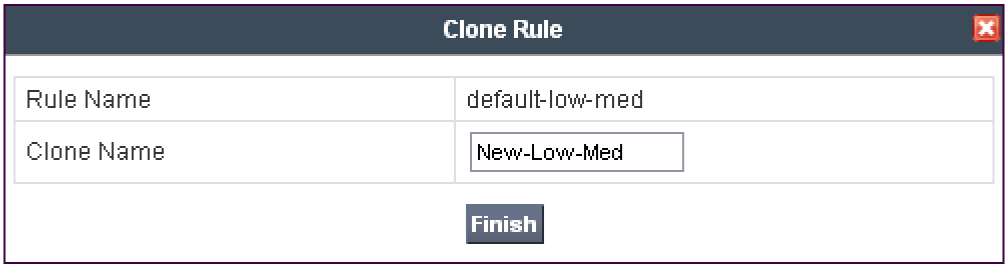
Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be 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 Cincinnati Bell eVantage IP Service and the enterprise.

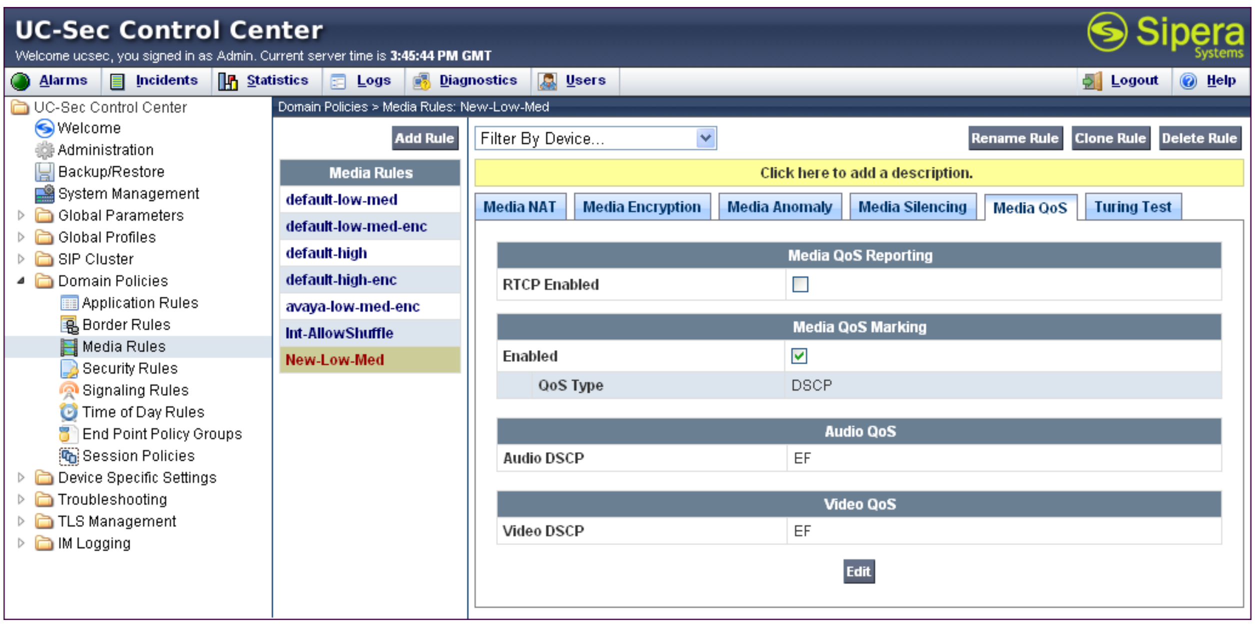
To create a custom Media Rule, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**. With **default-low-med** selected, click **Clone Rule** as shown below.



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



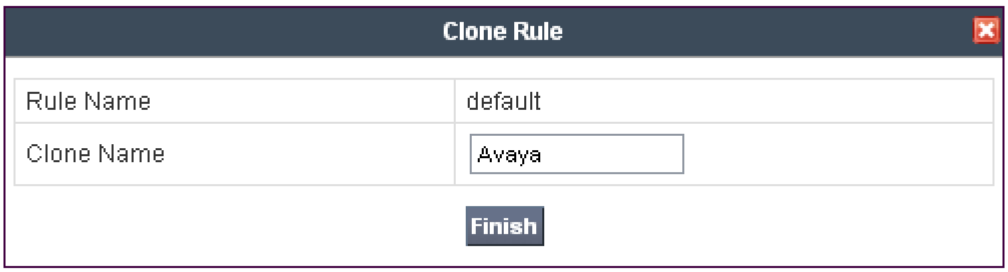
On the **Media QoS** tab select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies for the media. The following screen shows the QoS values used for compliance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



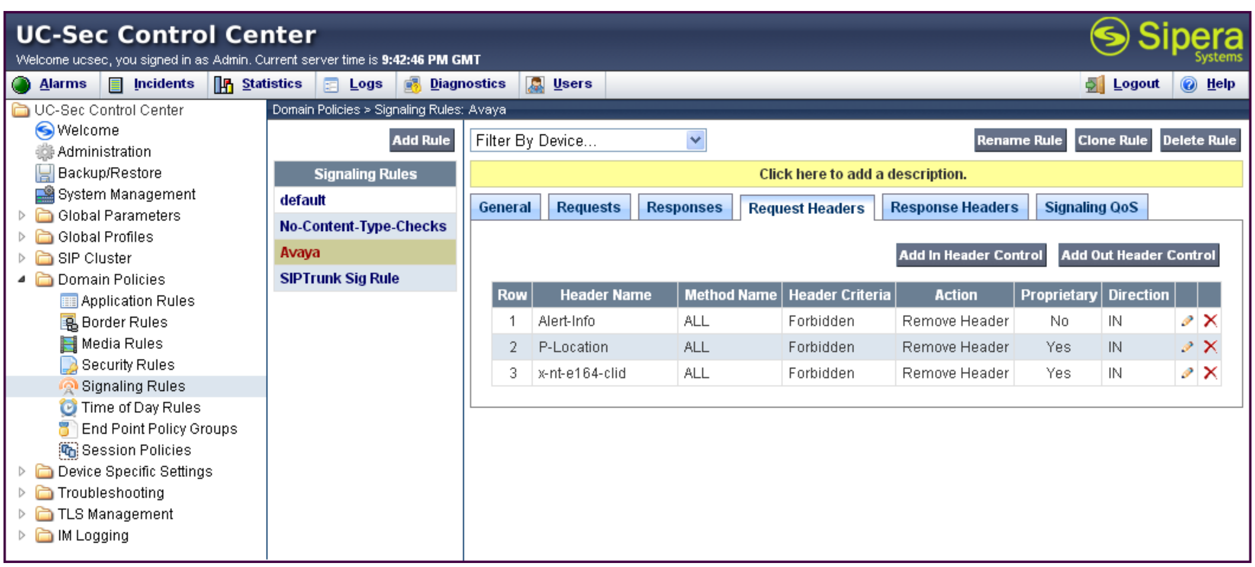
7.7. Signaling Rule

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.

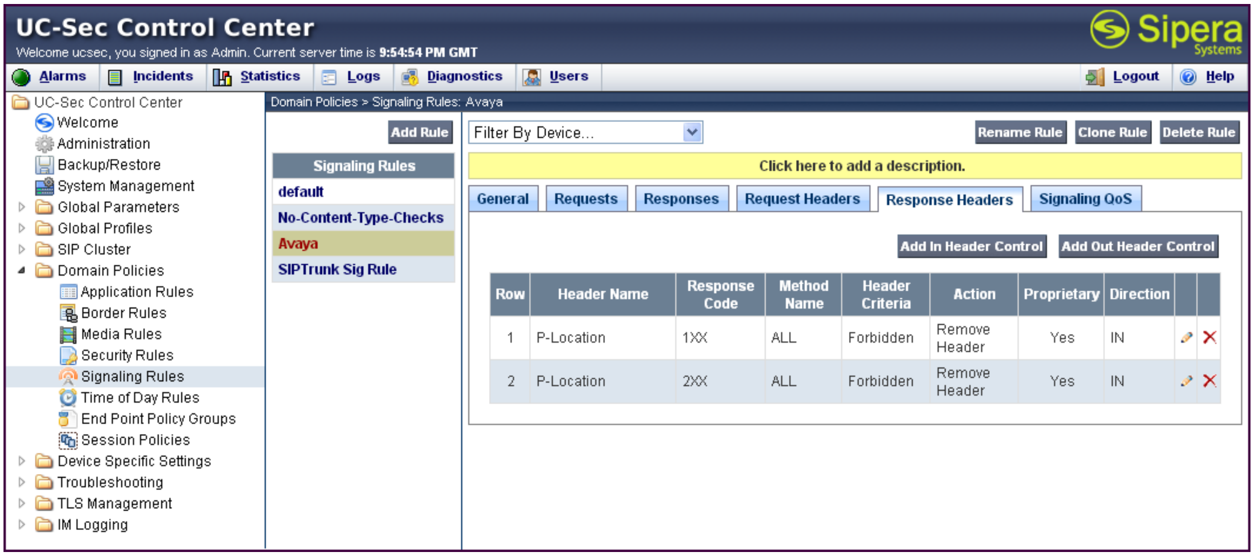
Clone and modify the default signaling rule to remove unnecessary SIP headers and add the proper quality of service to the SIP message. To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** (not shown). Enter a descriptive name for the new rule and click **Finish**.



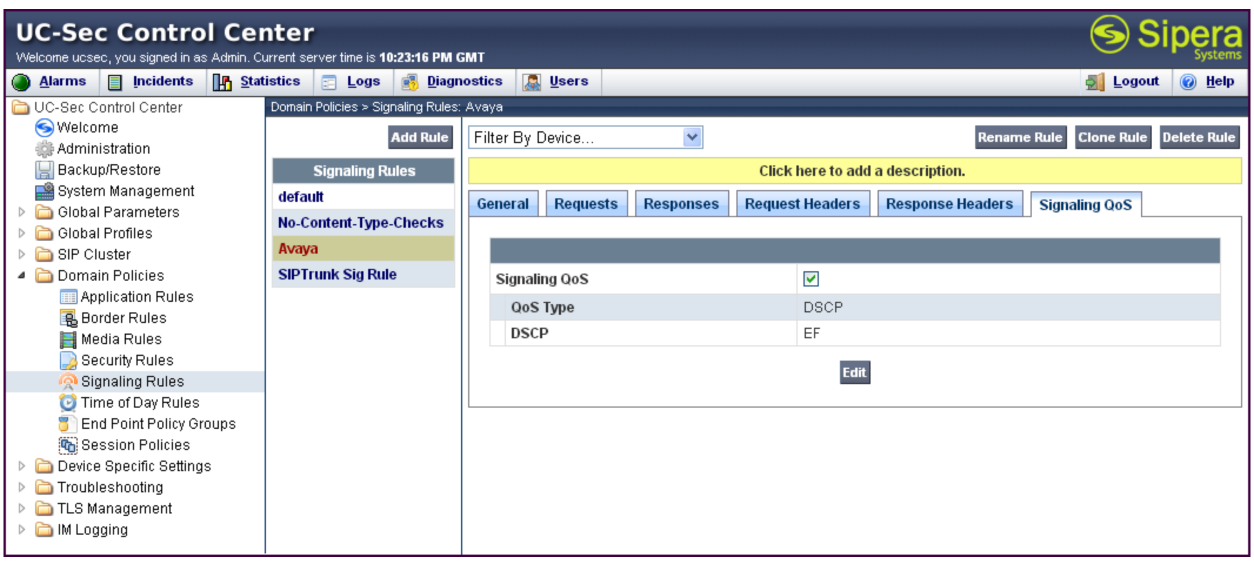
In the sample configuration, signaling rule **Avaya** was created for Session Manager to prevent certain headers in the SIP messages sent from the CS1000E and Session Manager from being propagated to Cincinnati Bell. Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on the request messages such as the initial INVITE or UPDATE message. The following screen shows the **Alert-Info**, **P-Location**, and **x-nt-e164-clid** headers removed during the compliance test.



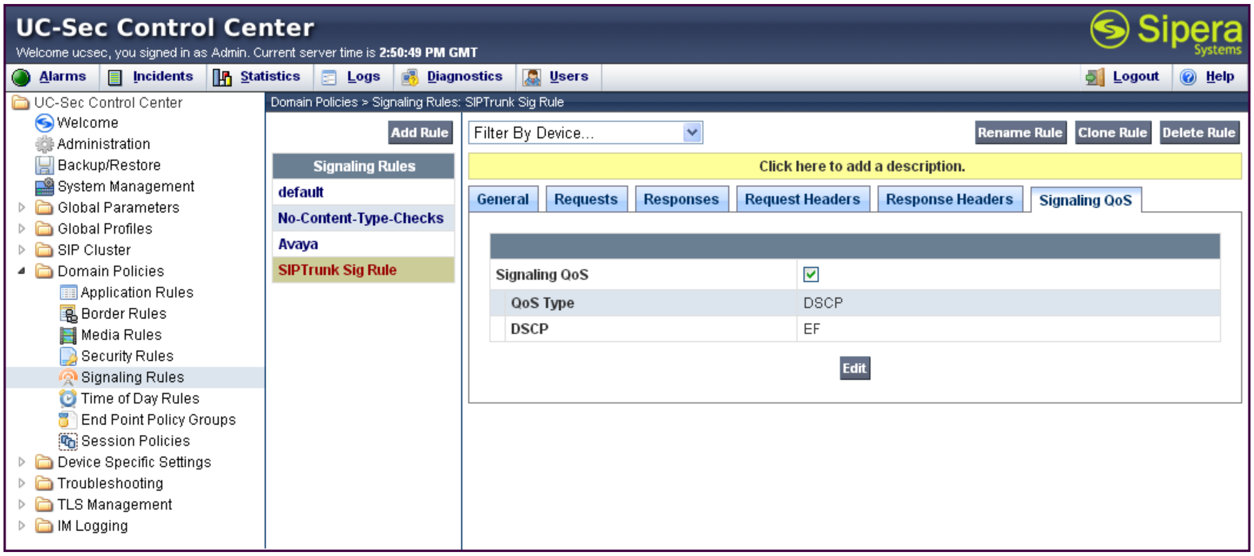
Similarly, manipulations can be performed on the SIP response messages. These can be viewed by selecting the **Response Headers** tab as shown below.



On the **Signaling QoS** tab select the proper Quality of Service (QoS). The 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 signaling. The following screen shows the QoS values used for compliance testing.



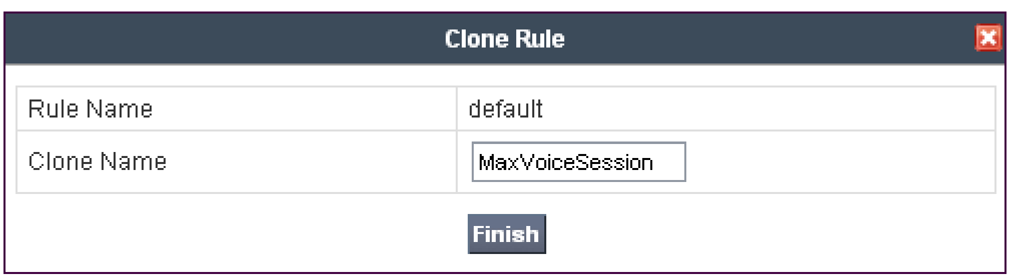
A separate signaling rule **SIPTrunk Sig Rule** was created for Cincinnati Bell eVantage IP Service by cloning the **default** signaling rule and changing the **Signaling QoS** parameters as shown below.



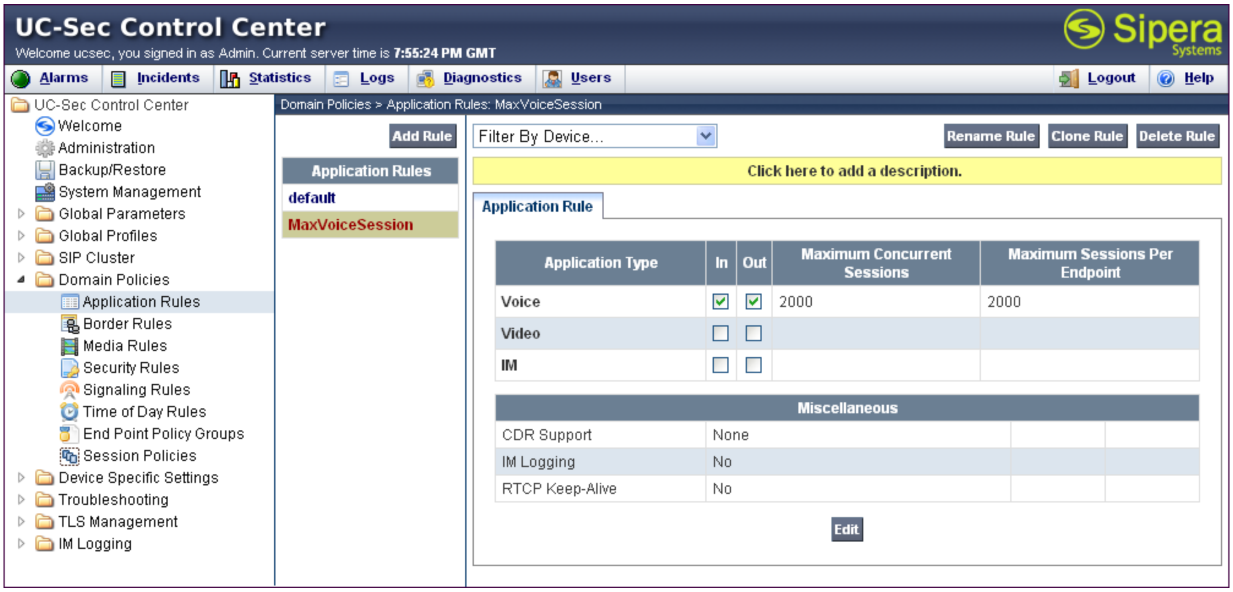
7.8. Application Rule

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** (not shown). Enter a descriptive name for the new rule and click **Finish**.



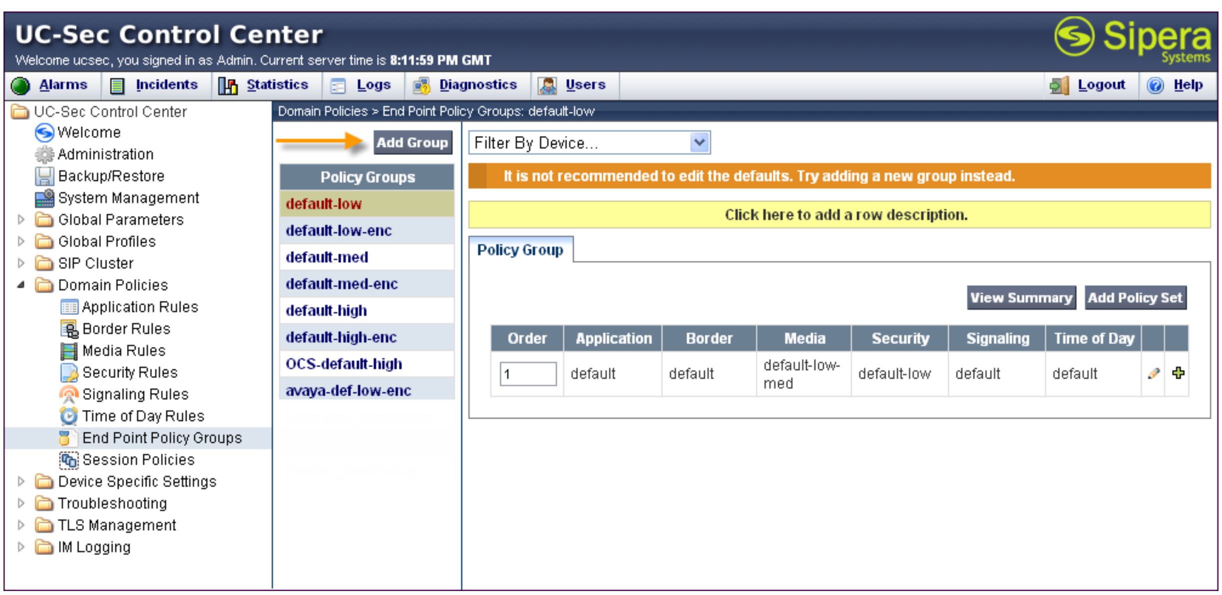
Modify the rule by clicking the **Edit** button. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. Set the values high enough for the amount of traffic the network is able process. Keep in mind Avaya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



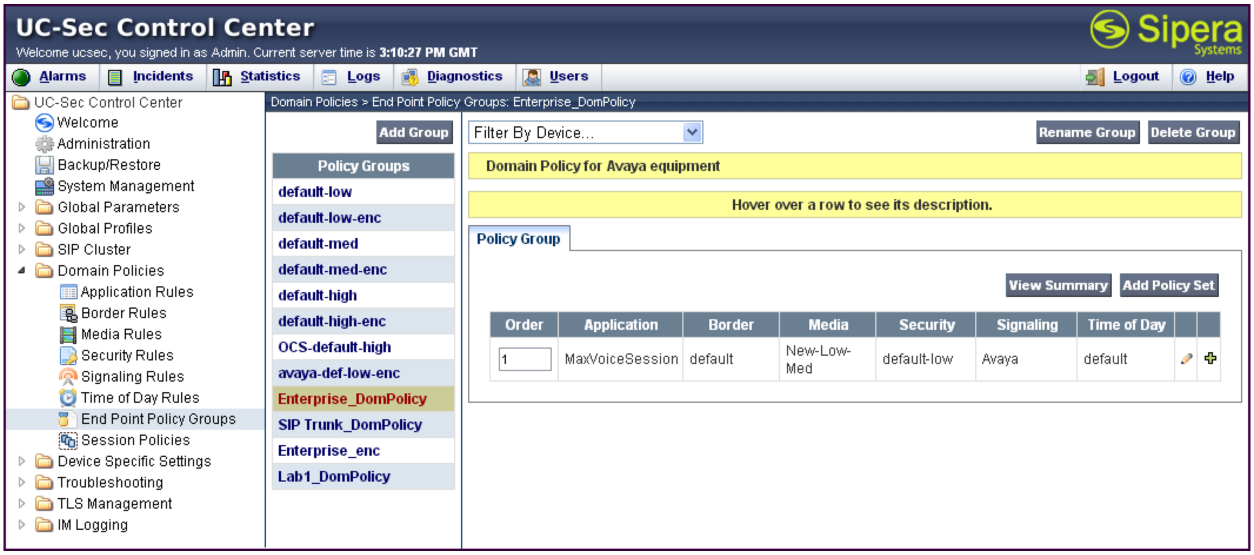
7.9. Endpoint Policy Group

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 7.12**. Create a separate Endpoint Policy Group for the enterprise and the Cincinnati Bell eVantage IP Service.

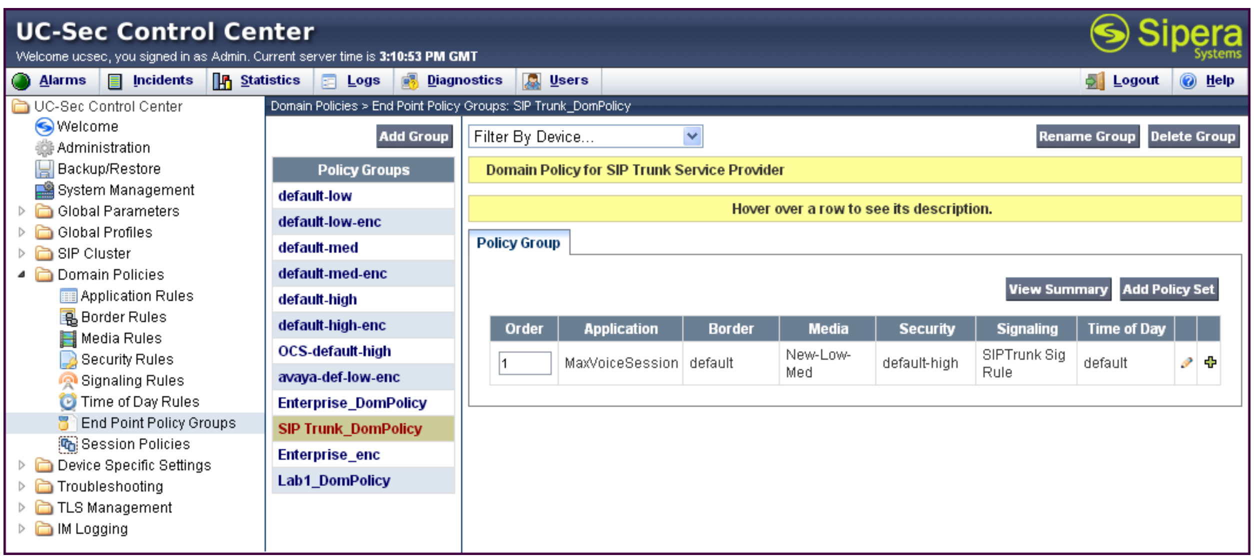
To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** as shown below.



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



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

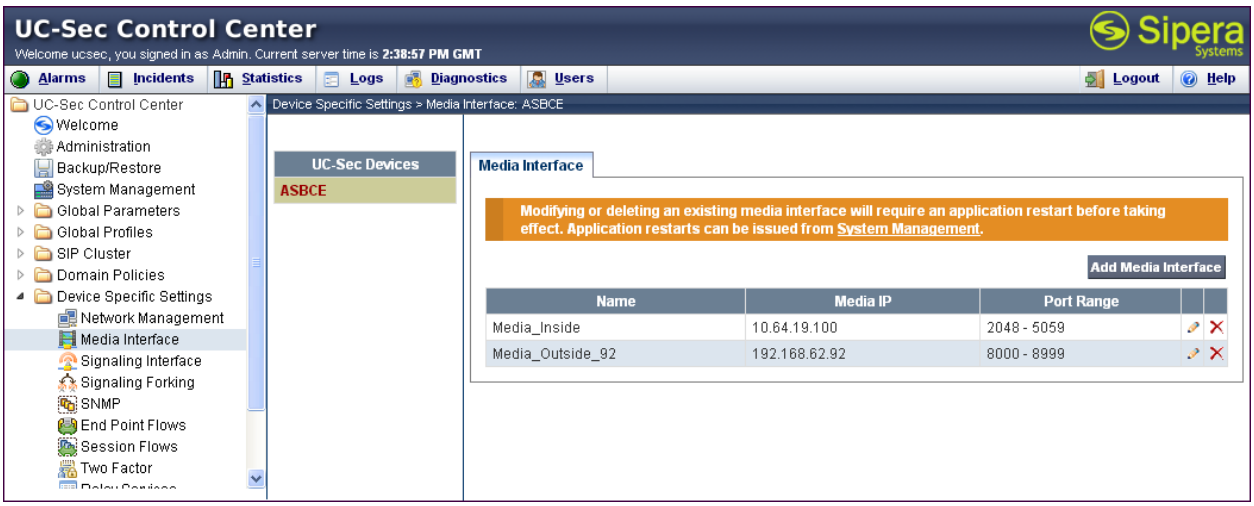


7.10. Media Interface

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.

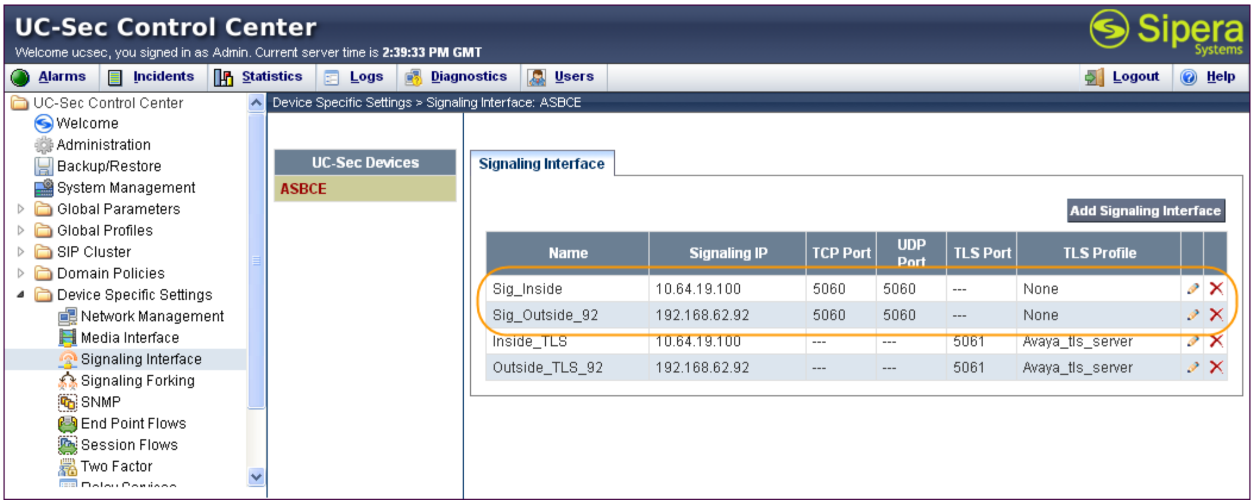


After the media interfaces are created, an application restart is necessary before the changes will take effect. Navigate to **UC-Sec Control Center → System Management** and click the forth icon from the right to restart the applications as highlighted below.

7.11. Signaling Interface

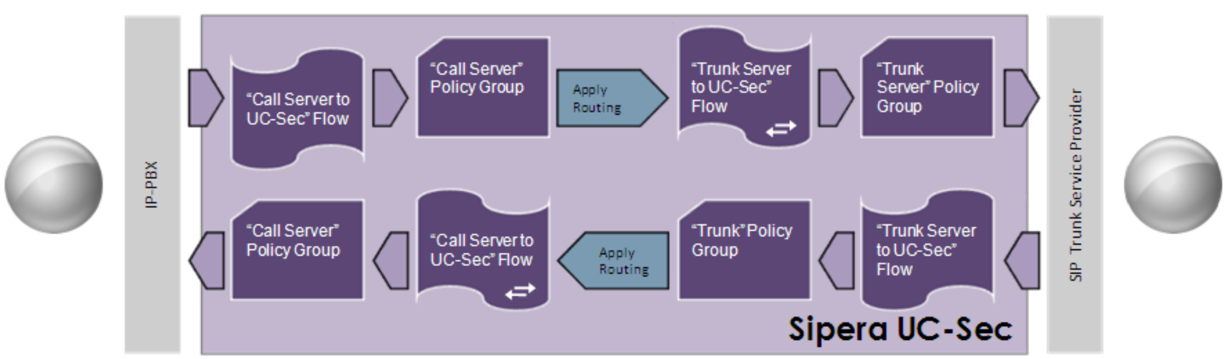
The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific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

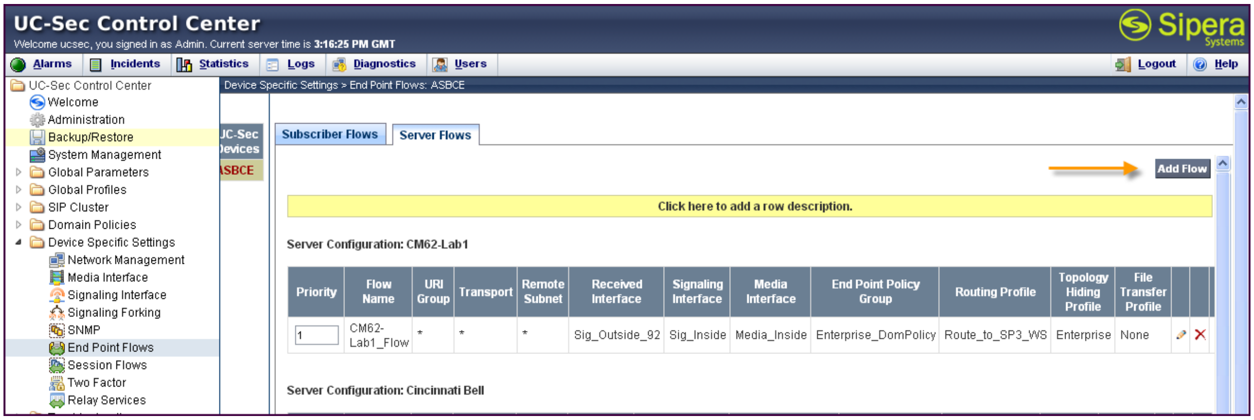


7.12. End Point Flows - Server Flow

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 Avaya SBCE to secure a SIP Trunk call.



Create a Server Flow for Session Manager and Cincinnati Bell eVantage IP Service. 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.

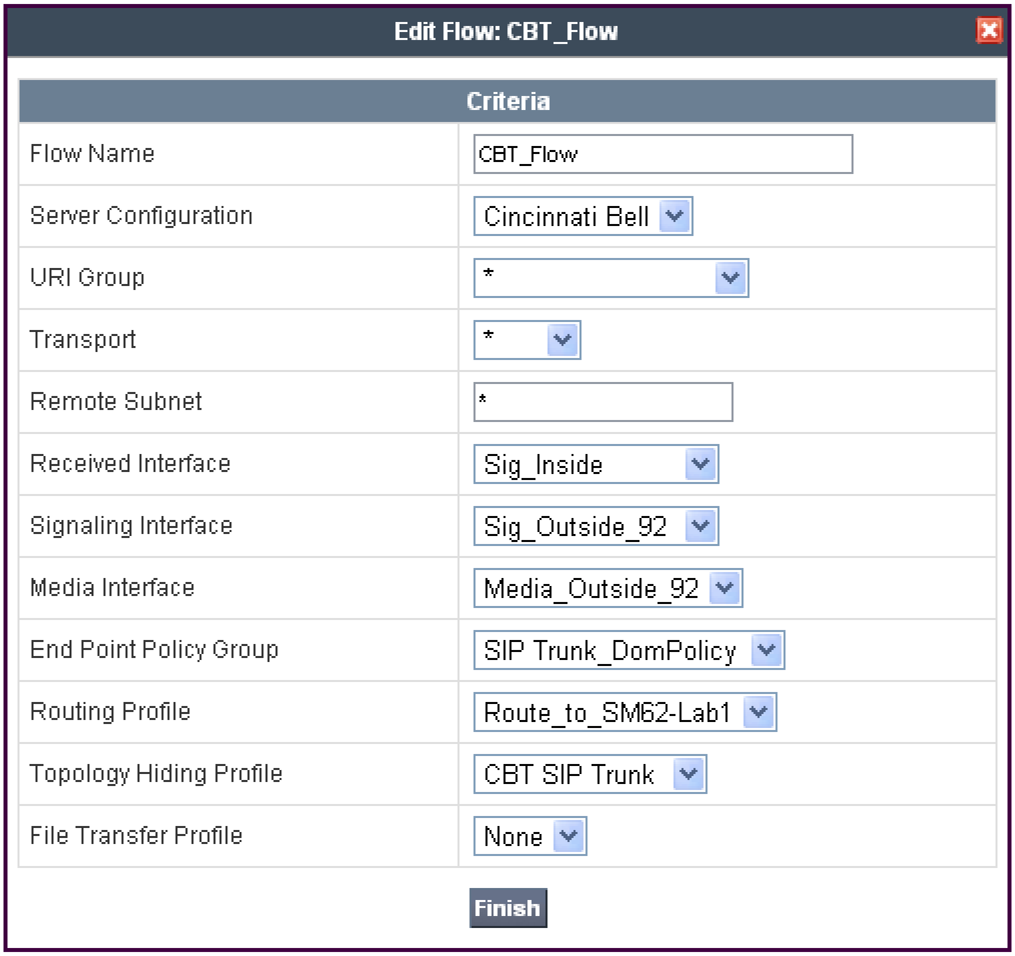


In the new window that appears, enter the following values. Use default values for all remaining fields:

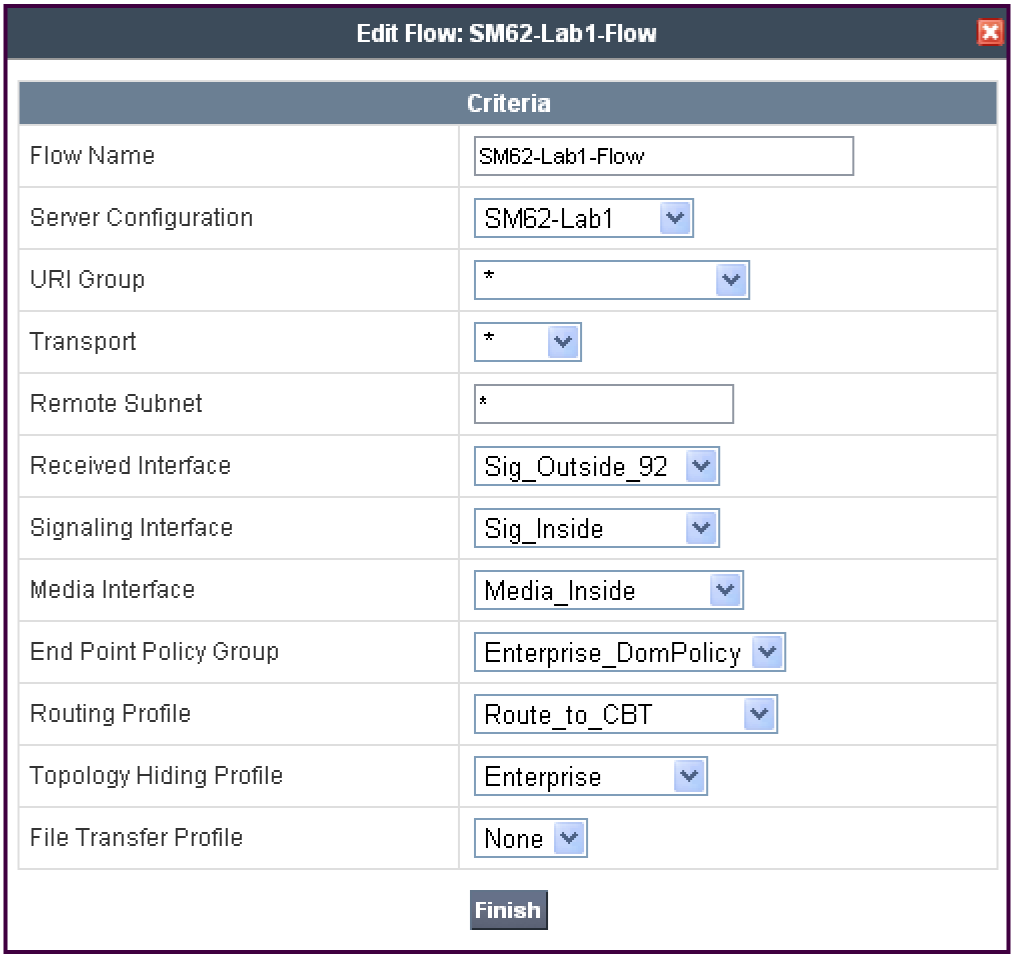
- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.5** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface created in **Section 7.11** the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.11** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 7.10** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy created in **Section 7.9** assigned to the Server Configuration.
- **Routing Profile:** Select the profile created in **Section 7.2** the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile created in **Section 7.3** to apply toward the Server Configuration.

Click **Finish** to save and exit.

The following screen shows the Sever Flow for Cincinnati Bell eVantage IP Service:



The following screen shows the Sever Flow for Session Manager:



8. Cincinnati Bell eVantage IP Service Configuration

To use Cincinnati Bell eVantage IP Service, a customer must request the service from Cincinnati Bell using their sales processes. This process can be initiated by contacting Cincinnati Bell via the corporate web site at www.cincinnatibell.com and requesting information via the online sales links or telephone numbers.

9. Verification

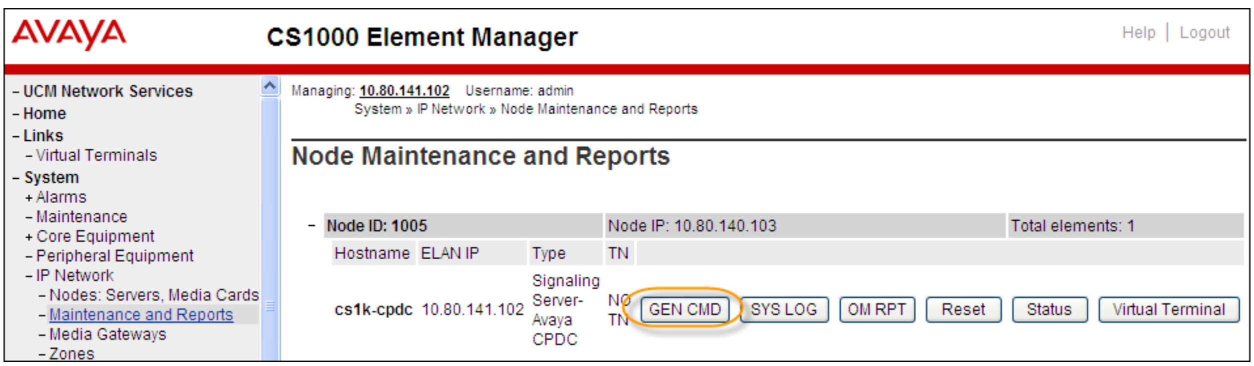
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

9.1. Avaya Communication Server 1000E Verification

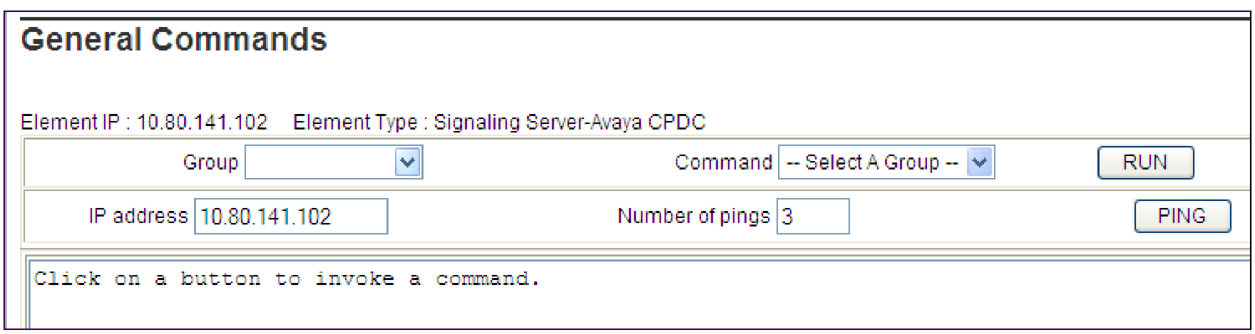
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

9.1.1. 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.

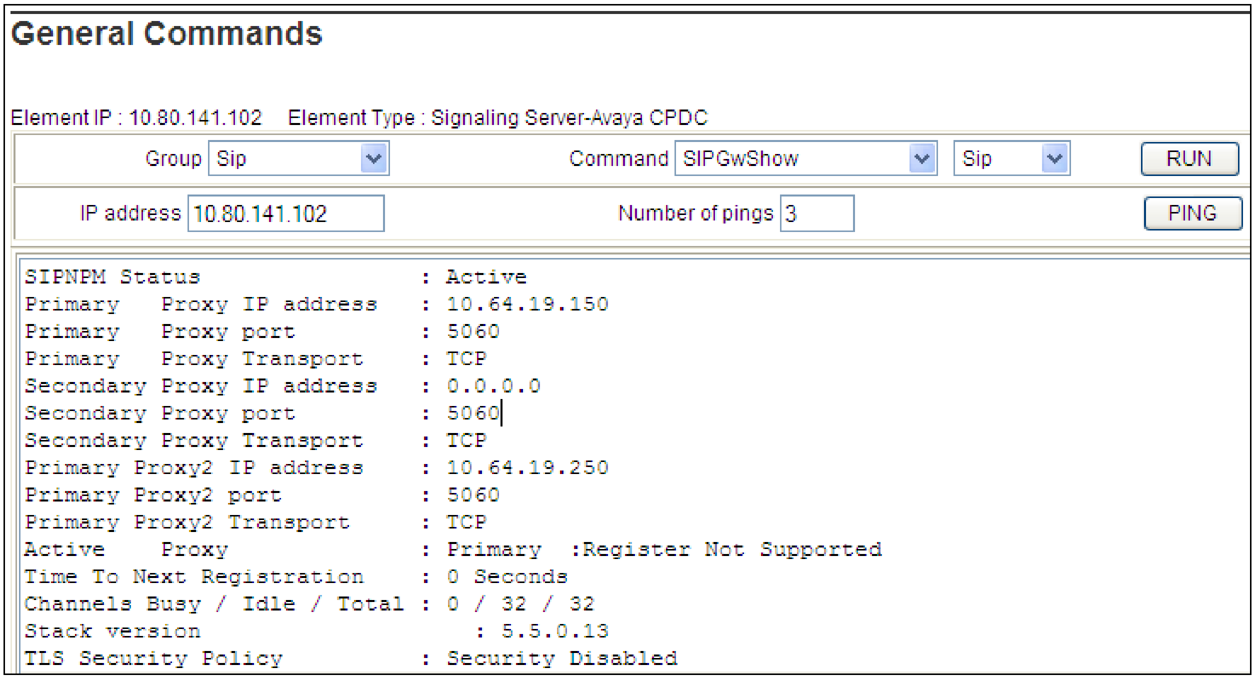


The **General Commands** page is displayed as shown below.

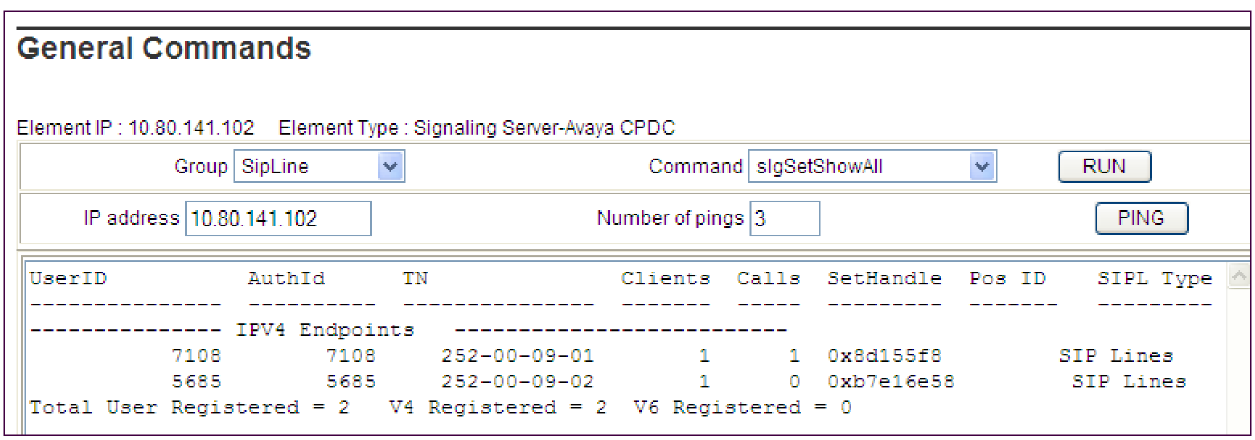


A variety of commands are available by selecting an appropriate Group and Command from the drop-down menus, and selecting Run.

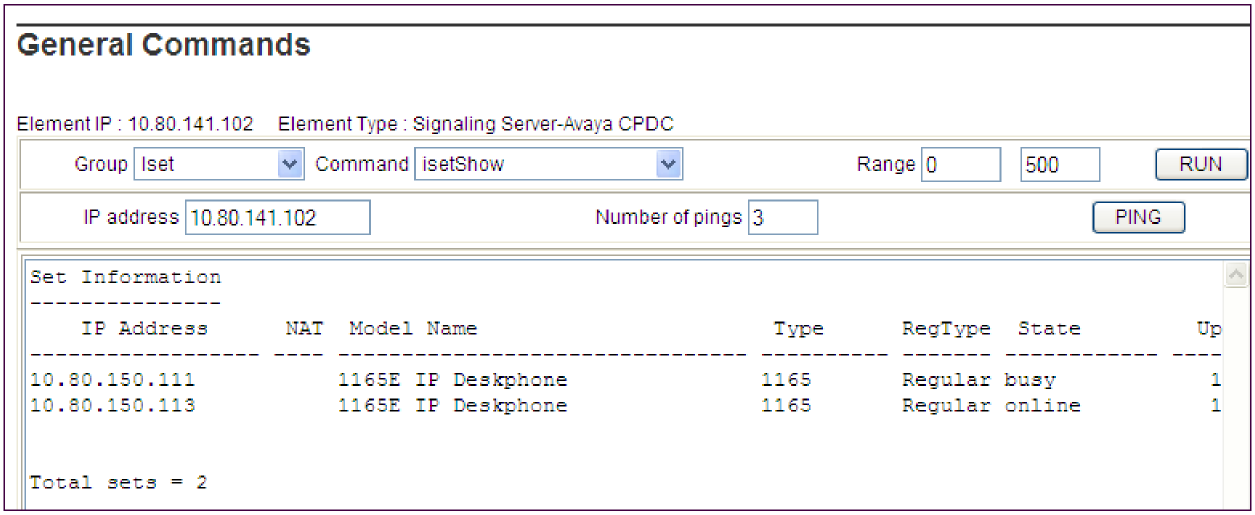
To check the status of the SIP Gateway to Session Manager in the sample configuration, select **Sip** from the Group menu and **SIPGwShow** from the **Command** menu. Click Run. The example output below shows that Session Manager (10.64.19.150, port 5060, TCP) has **SIPNPM Status** Active.



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 Cincinnati Bell eVantage IP Service.



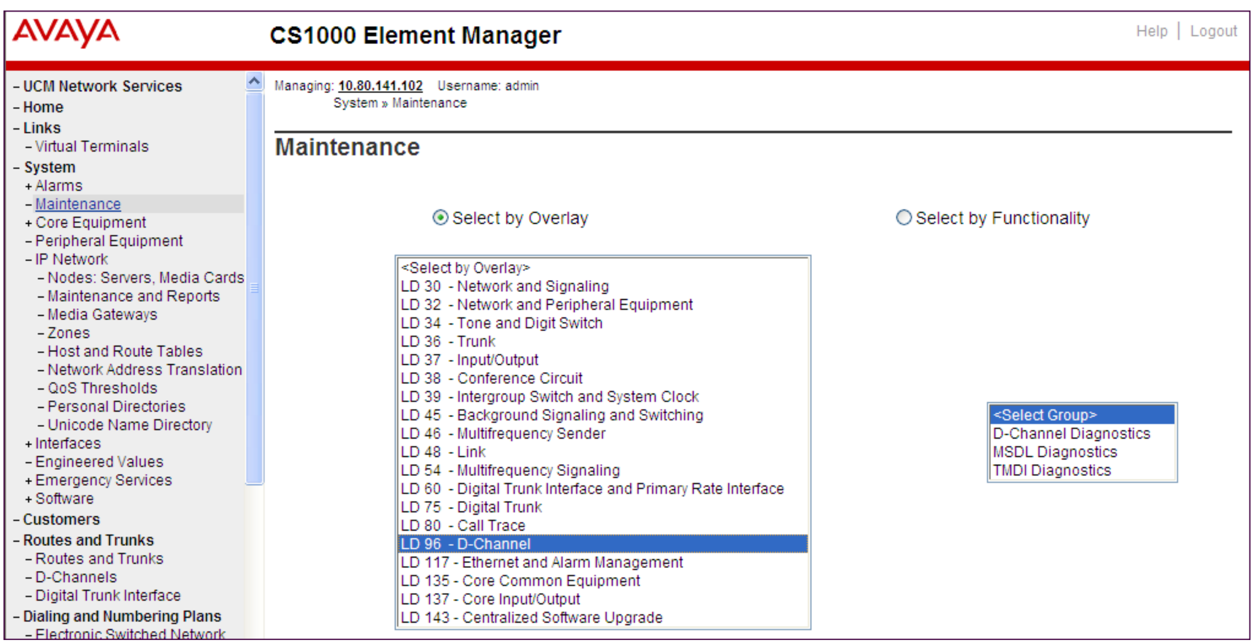
The following screen shows a means to view IP UNIStim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**. At the time this screen was captured, the UNIStim telephone with IP address **10.80.150.111** was involved in an active call with the Cincinnati Bell eVantage IP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



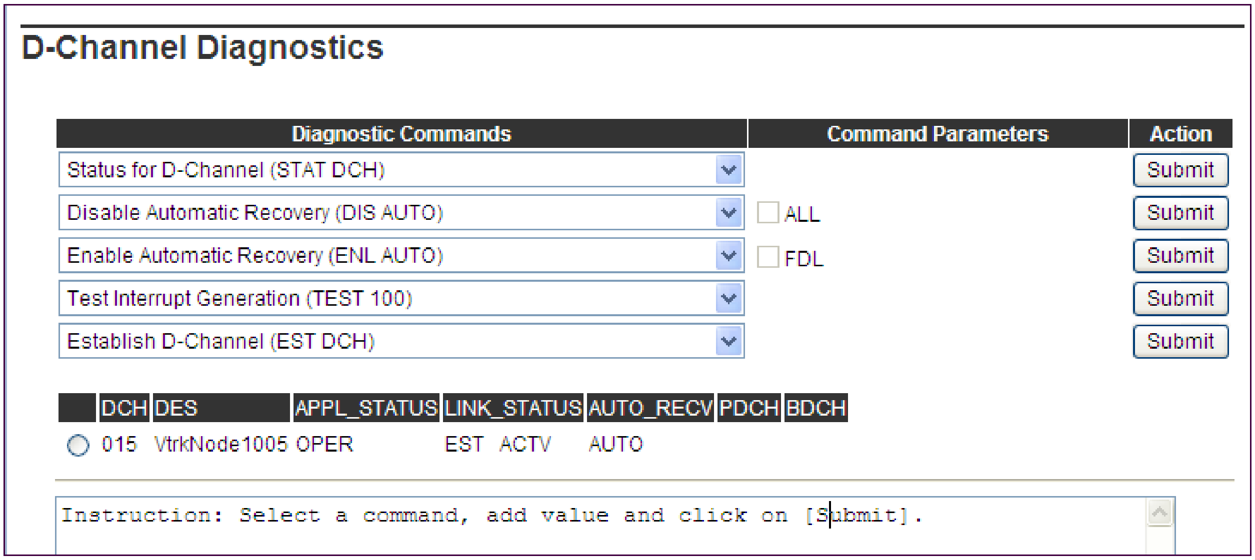
9.1.2. System Maintenance Commands

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.



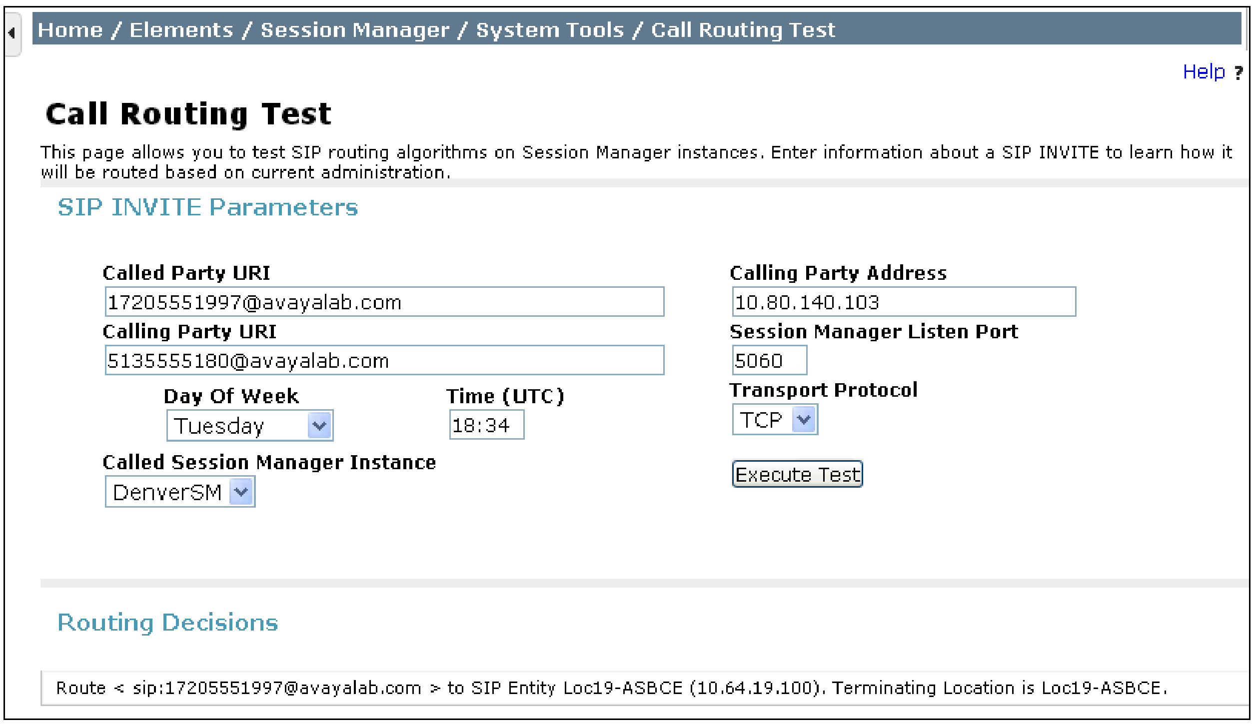
On the preceding screen, **if D-Channel Diagnostics** is selected on the right, a screen such as the following is displayed. D-Channel number 15, which is used in the sample configuration, is established **EST** and active **ACTV**.



9.2. Avaya Aura® Session Manager Verification

The following steps may be used to verify the Session Manager configuration:

1. Verify the call routing administration on Session Manager by logging in to System Manager and executing the Call Routing Test. Expand **Elements → Session Manager → System Tools → Call Routing Test**. 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 Cincinnati Bell. Under **Routing Decisions**, observe the call will rout via Avaya SBCE to Cincinnati Bell. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



2. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
3. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
4. Verify that the user on the PSTN can end an active call by hanging up.
5. Verify that an endpoint at the enterprise site can end an active call by hanging up

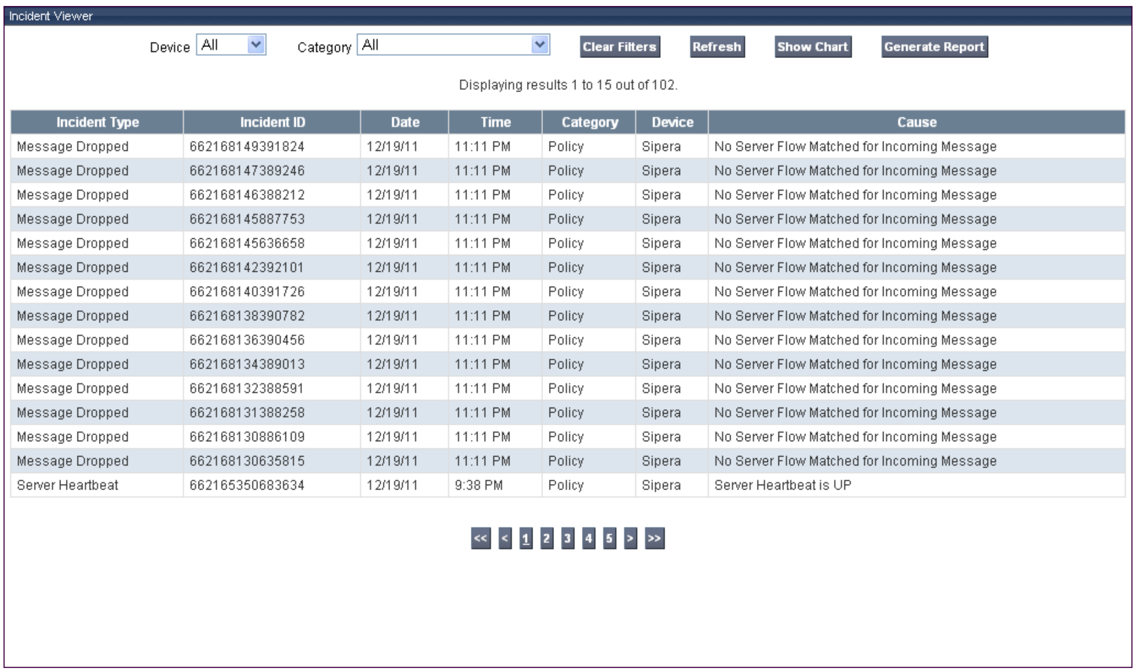
9.3. Avaya Session Border Controller for Enterprise Verification

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

9.3.1. Incidents

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

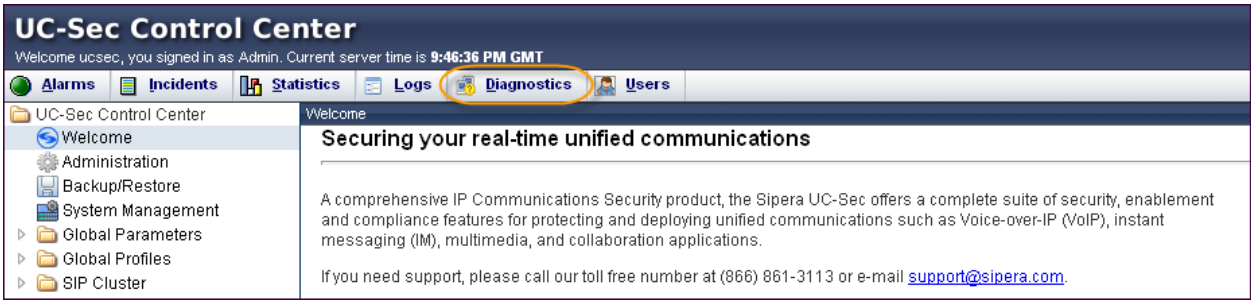
The following screen shows an example SIP messages that do not match a Server Flow for an incoming message.



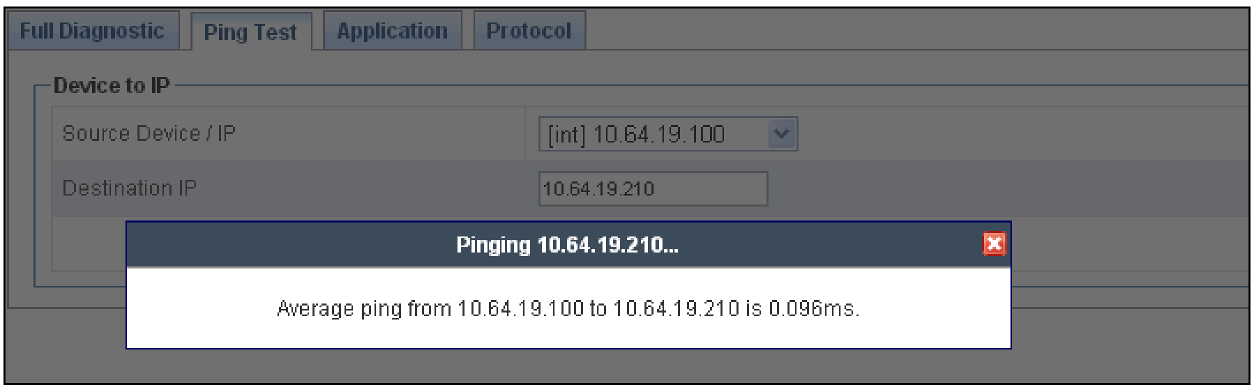
Incident Type	Incident ID	Date	Time	Category	Device	Cause
Message Dropped	662168149391824	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168147389246	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168146388212	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145887753	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145636658	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168142392101	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168140391726	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168138390782	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168136390456	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168134389013	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168132388591	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168131388258	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130886109	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130635815	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Server Heartbeat	662165350683634	12/19/11	9:38 PM	Policy	Sipera	Server Heartbeat is UP

9.3.2. Diagnostics

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

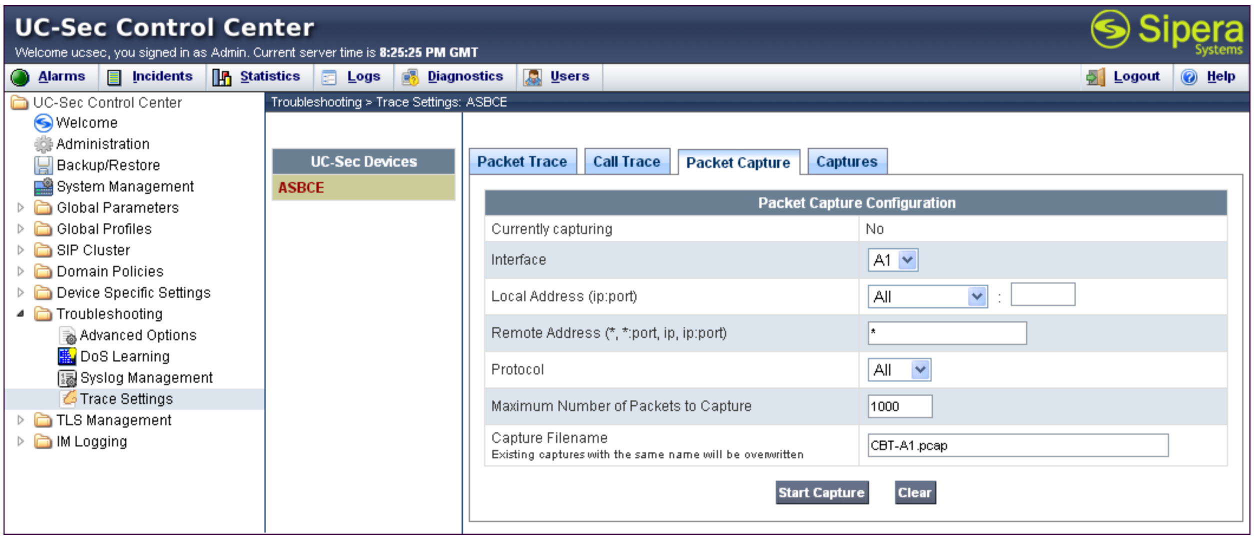


The following screen shows an example PING to Session Manager from the internal signaling interface of the Avaya SBCE.

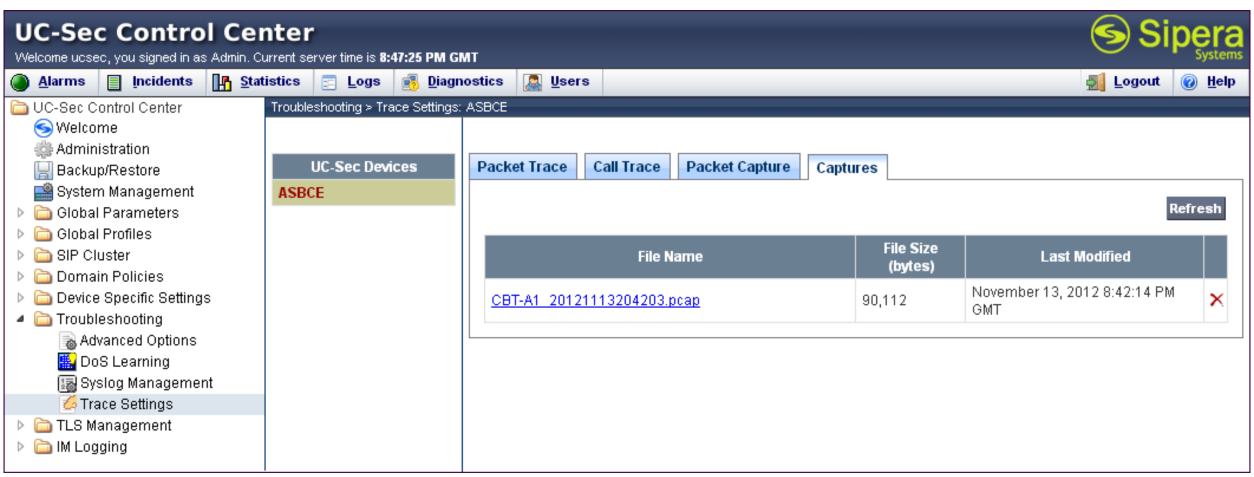


9.3.3. Trace Settings

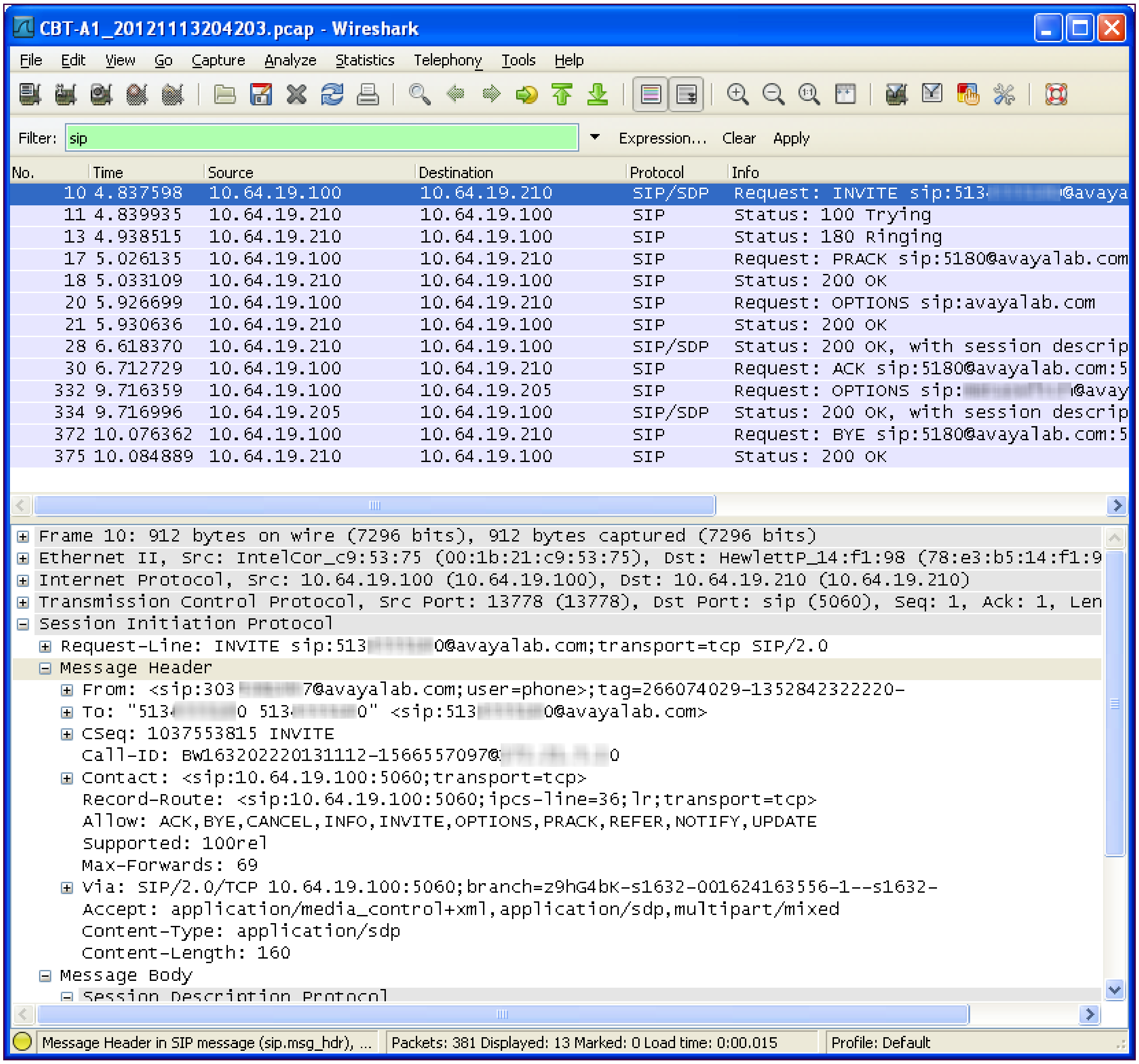
The Trace Settings tool is for configuring and displaying call traces and packet captures for the Avaya SBCE. Navigate to **Troubleshooting → Trace Settings** as shown below. The following screen shows an example packet capture on interface **A1** with a **Maximum Number of Packets to Capture** set to **1000**. The **Capture Filename CBT-A1.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:



10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise to the Cincinnati Bell eVantage IP Service. The Cincinnati Bell eVantage IP Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The Cincinnati Bell eVantage IP Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.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] *Installing and Configuring Avaya Aura® System Platform, Release 6.2.0,* March 2012.

[6] *Administering Avaya Aura® System Platform, Release 6.2.0,* February 2012.

[7] *Implementing Avaya Aura ® System Manager*, Release 6.2, March 2012

[8] *Installing Service Packs for Avaya Aura® Session Manager*, February 2012, Document Number 03-603863

[9] *Implementing Avaya Aura® Session Manager,* February 2012, Document Number 03-603473.

[10] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315, 05.18 January 2012

[11] *SIP Software for Avaya 1100 Series IP Deskphones-Administration* , Document Number NN43170-600, Standard 04.02 December 2011

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.