Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E 7.5, Avaya Aura® Session Manager 6.2, Acme Packet 3820 Net-Net® Session Director 6.3.0 with CenturyLink SIP Trunk Service (Legacy Qwest) – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk Service (Legacy Qwest) using Sonus NBS version 7.3.5R6 and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E, Avaya Aura® Session Manager, and various Avaya endpoints.

CenturyLink is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted 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 Acme Packet 3820 Net-Net Session Director 6.3.0 (Acme Packet 3820) integration with CenturyLink SIP Trunk Service (Legacy Qwest) using Sonus NBS version 7.3.5R6. CenturyLink can offer SIP trunk service using several different platform technologies in the CenturyLink network. These Application Notes correspond to the SIP trunk service offered using a Sonus platform in the network.

In the sample configuration, the Acme Packet 3820 is used as an edge device between Avaya Customer Premise Equipment (CPE) and CenturyLink SIP Trunk. The Acme Packet 3820 performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the CenturyLink SIP Trunk access method.

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

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

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

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya Communication Server 1000E (CS1000E), Session Manager, and Acme Packet 3820 to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to CenturyLink SIP Trunk service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

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

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

Items not supported or not tested included the following:

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

2.2. Test Results

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

- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/CenturyLink SIP Trunk solution. It is listed here simply as an observation.
- **Mobile-X**: Mobile-X extended calls does not contain the original called party number in the FROM or PAI headers. CenturyLink requires a valid phone number in the FROM, PAI or Diversion headers to allow the call to go through. A header manipulation rule was created in the Acme Packet 3820 to add a valid Diversion header for Mobile-X calls. See **Section 7.9** and **Appendix A**.

CenturyLink SIP Trunk (Legacy Qwest) passed compliance testing.

2.3. Support

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

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the CenturyLink SIP Trunks to East and West servers. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an Acme Packet 3820 provides NAT functionality and SIP header manipulation. The Acme Packet 3820 receives traffic from CenturyLink SIP Trunk on port 5060 and sends traffic to the CenturyLink SIP Trunk 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.

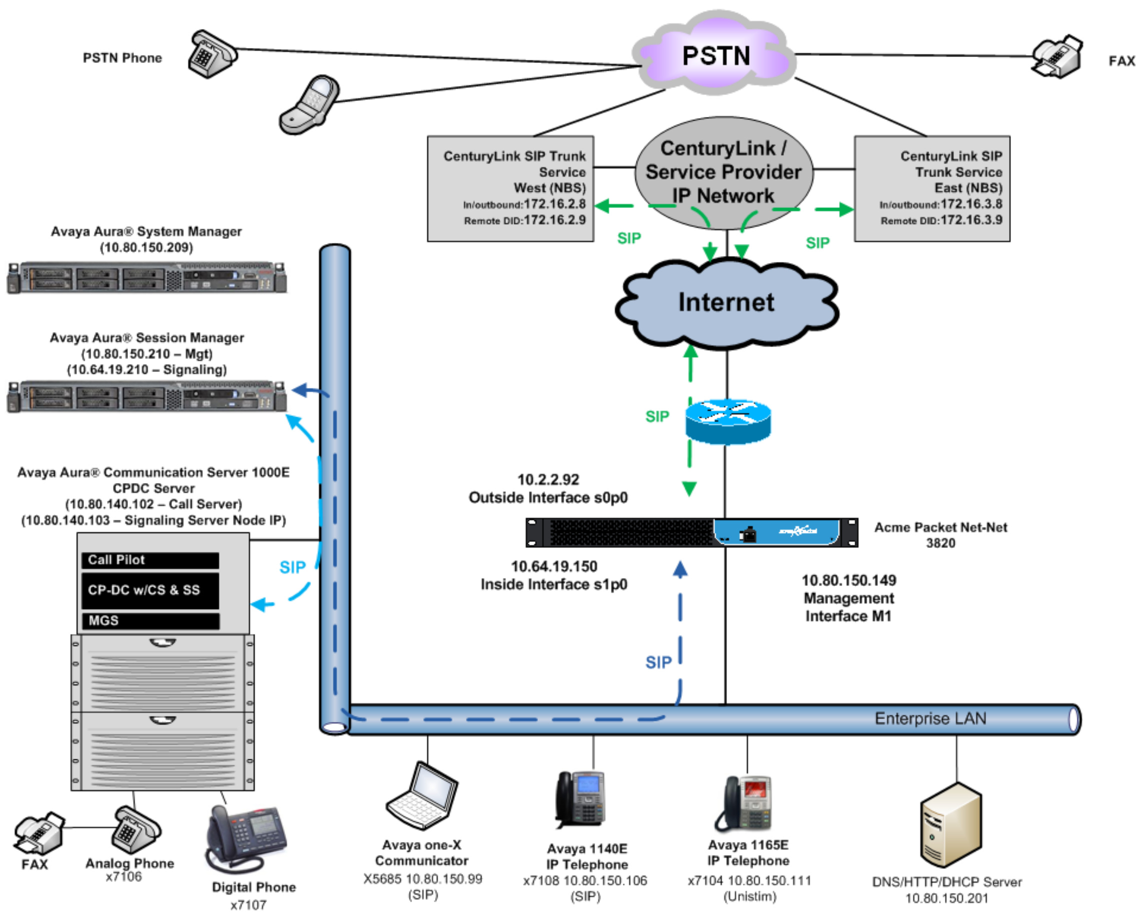


Figure 1: Avaya Interoperability Test Lab Configuration

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_20120110 • SSG Server: 7.50.17 GA • SLG Server: 7.50.17 GA
Communication Server 1000E Media Gateway	CSP Version: MGCC CD02 MSP Version: MGCM AB01 APP Version: MGCA BA15 FPGA Version: MGCF AA19 BOOT Version: MGCB BA15 DSP1 Version: DSP4 AB01 BCSP Version: MGCC CD01
Acme Packet Net-Net Session Director 3820	6.3.0 MR-1
Avaya 1165E (UNIStim)	0626C8A
Avaya 1140E (SIP)	04.03.09.00
Avaya one-X Communicator (SIP)	CS6.1.1.02
Avaya M3904 (Digital)	n/a
Avaya 6210 Analog Telephone	n/a
CenturyLink (Legacy Qwest) SIP Trunking Solution Components	
Component	Release
Sonus Network Border Switch (NBS)	07.03.05 R006

Table 1: Equipment and Software Tested

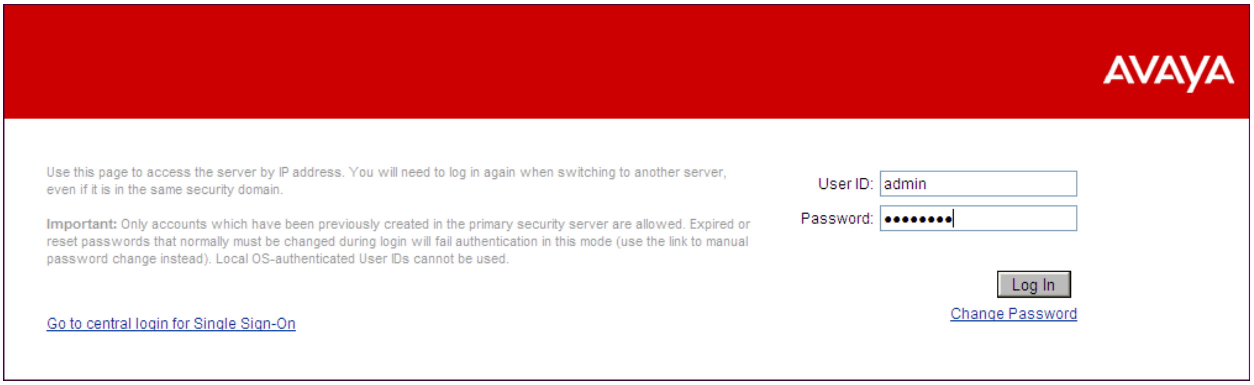
The specific configuration above was used for the compatibility testing.

5. Configure Avaya Communication Server 1000E

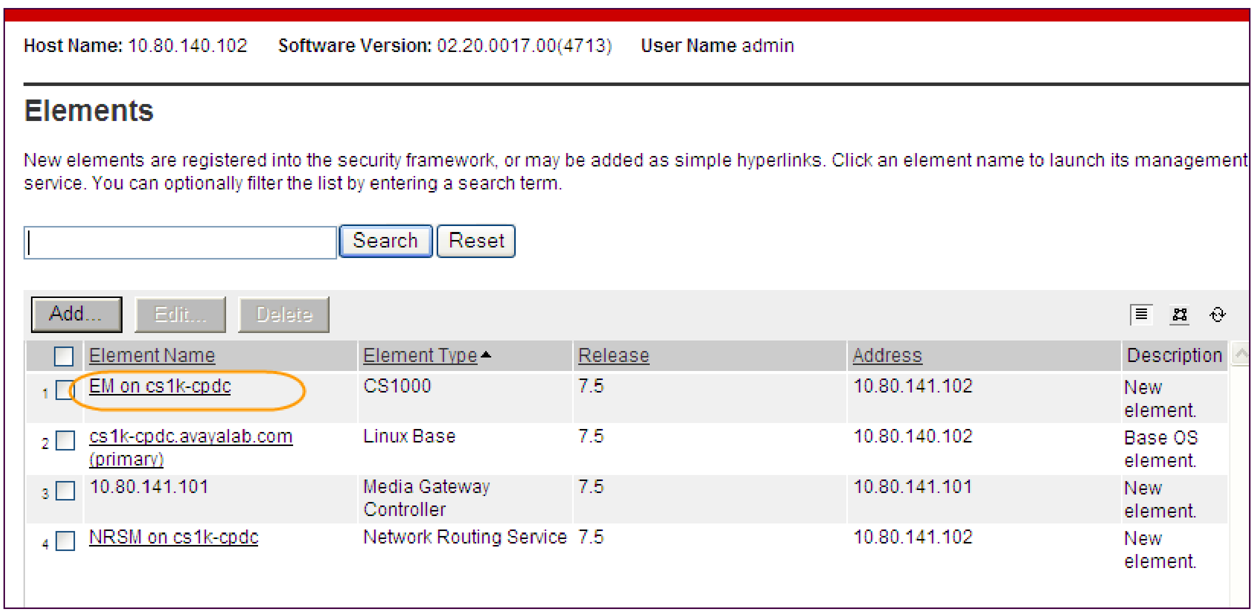
This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to CenturyLink over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed as a co-resident system with the SIP Signaling Server, and Call Server applications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



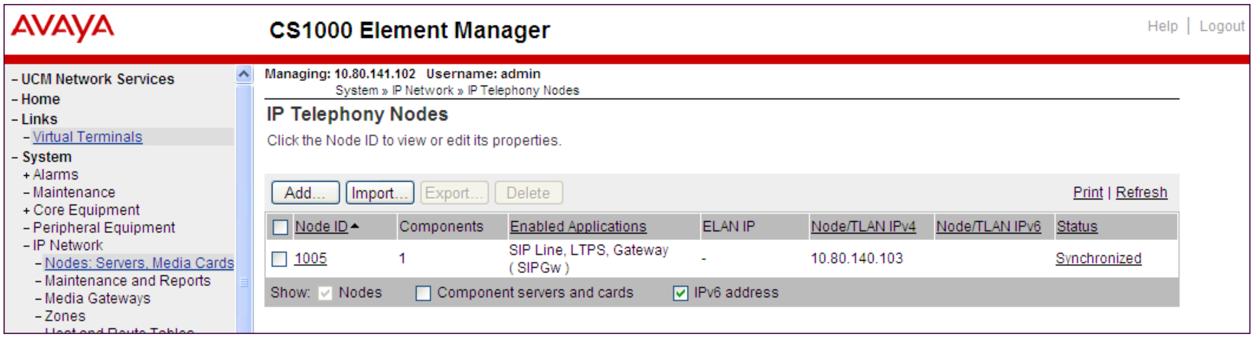
5.1. Administer an IP Telephony Node

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

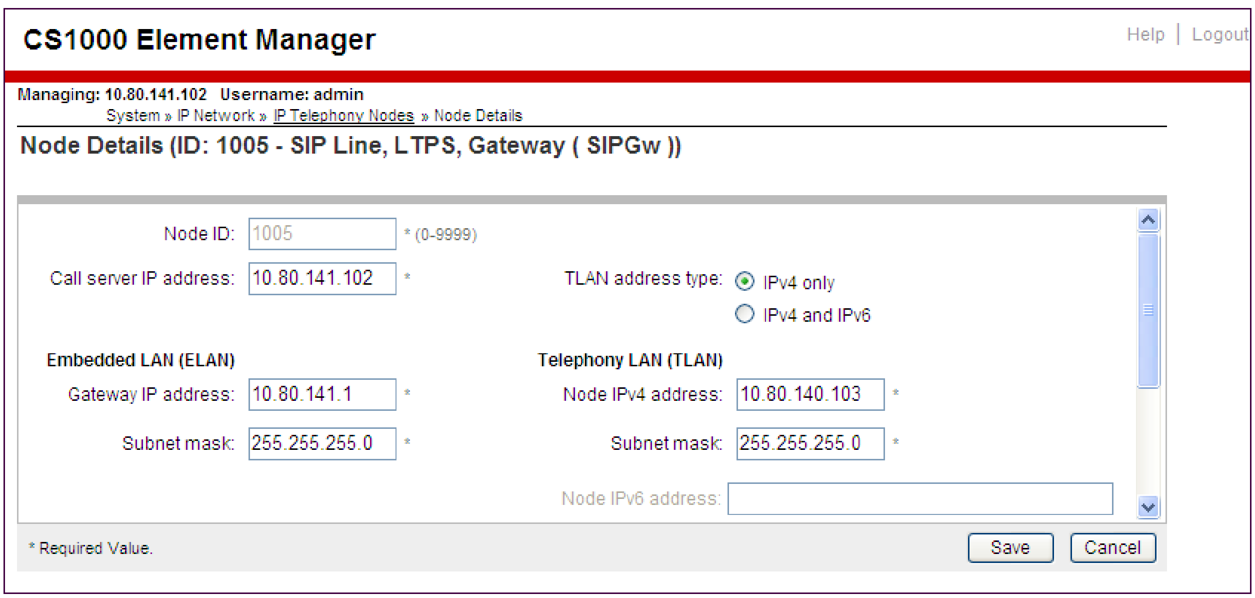
5.1.1. Obtain Node IP Address

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

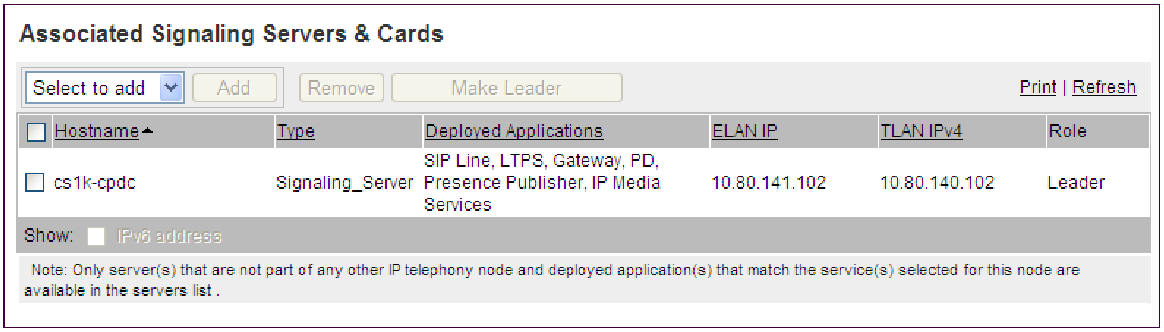
The **IP Telephony Nodes** page is displayed as shown below. Click **<Node id>** in the Node ID column to view details of the node. In the sample configuration, **Node ID 1005** was used.



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 6.6**.

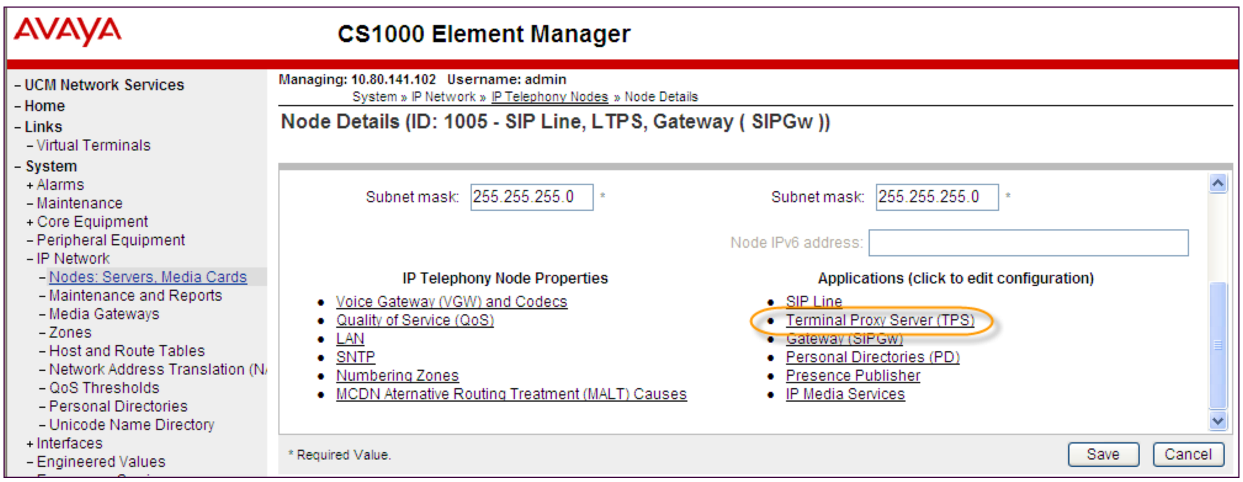


The following screen shows the **Associated Signaling Servers & Cards** heading at the bottom of the screen, simply to document the configuration.

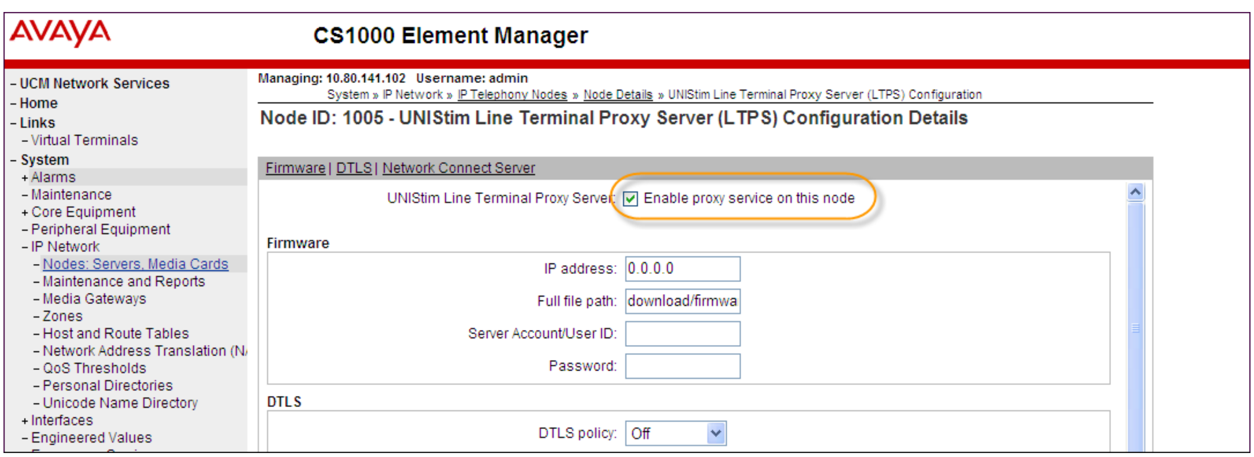


5.1.2. Terminal Proxy Server (TPS)

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

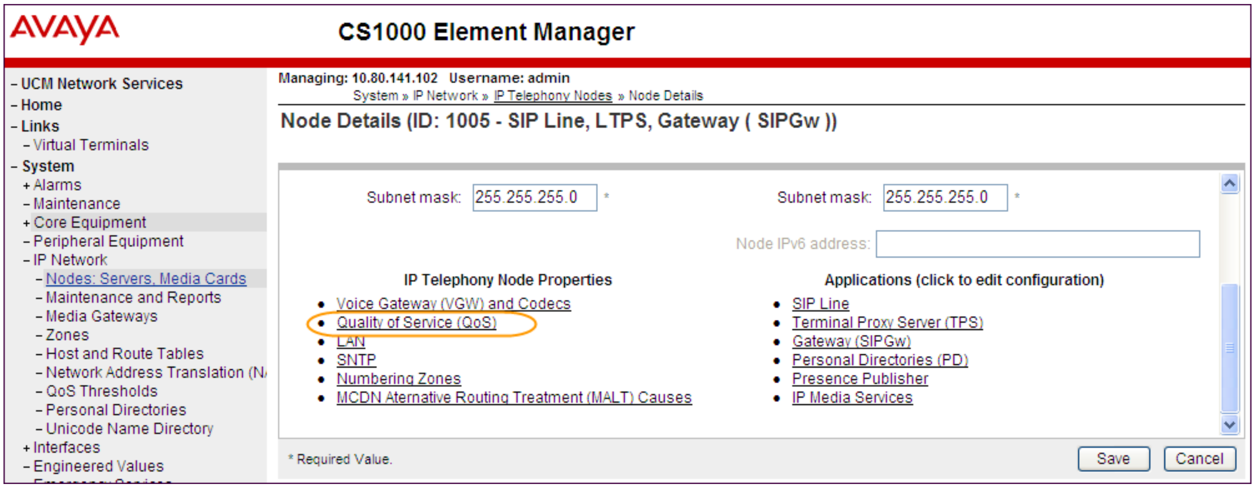


Check the **UNIStim Line Terminal Proxy Server** check box and then click the **Save** button (not shown).

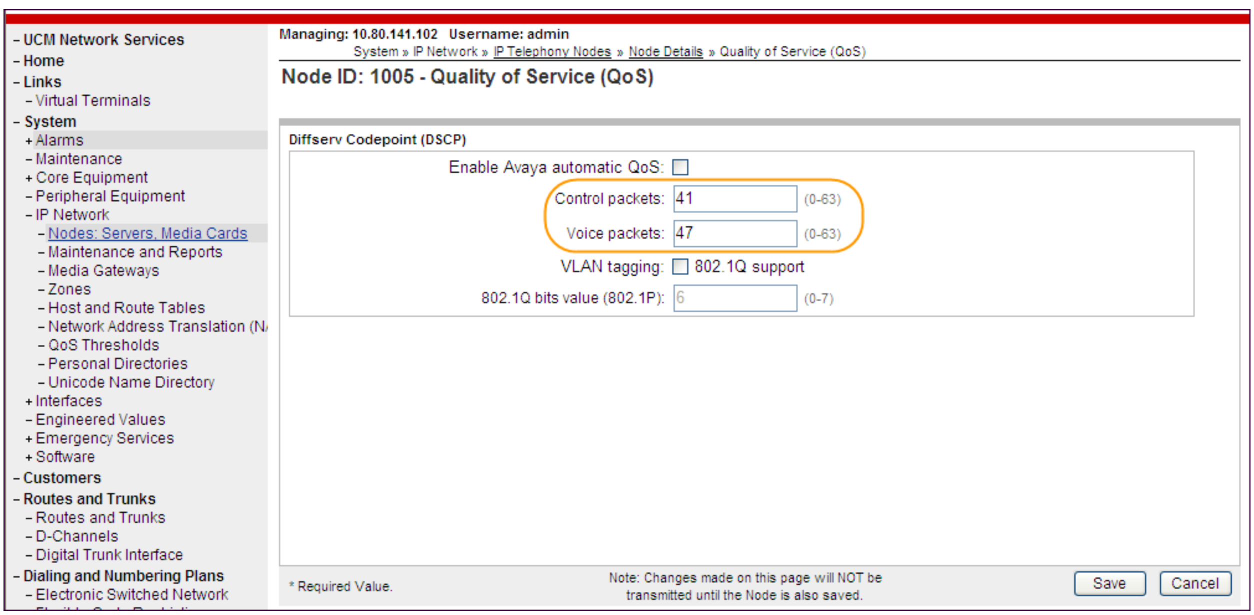


5.1.3. Quality of Service (QoS)

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

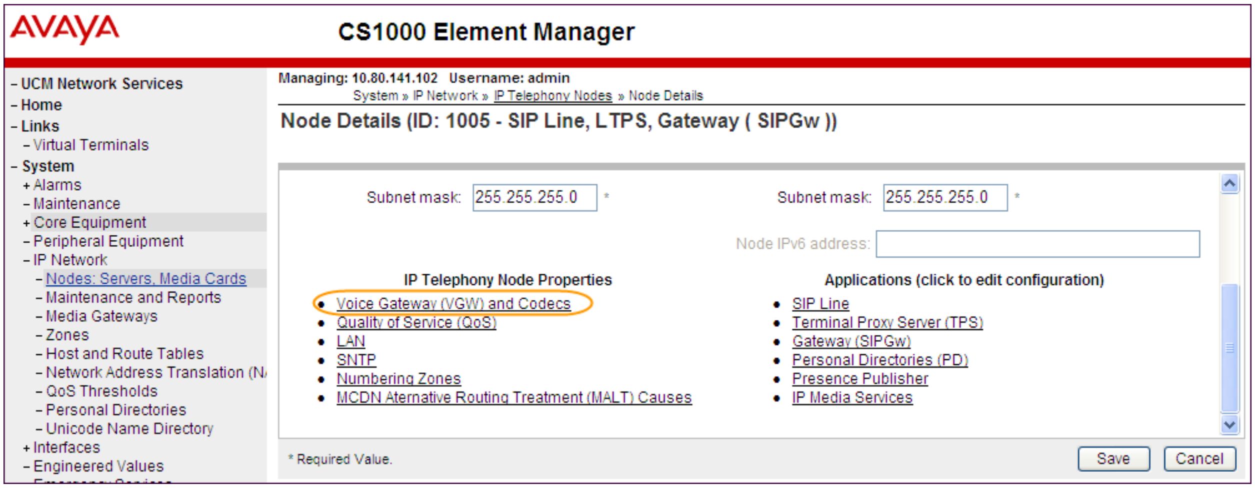


Set the **Control packets** and **Voice packets** values to the desired Diffserv settings required on the internal network. The default Diffserv values are shown below. Click on the **Save** button.

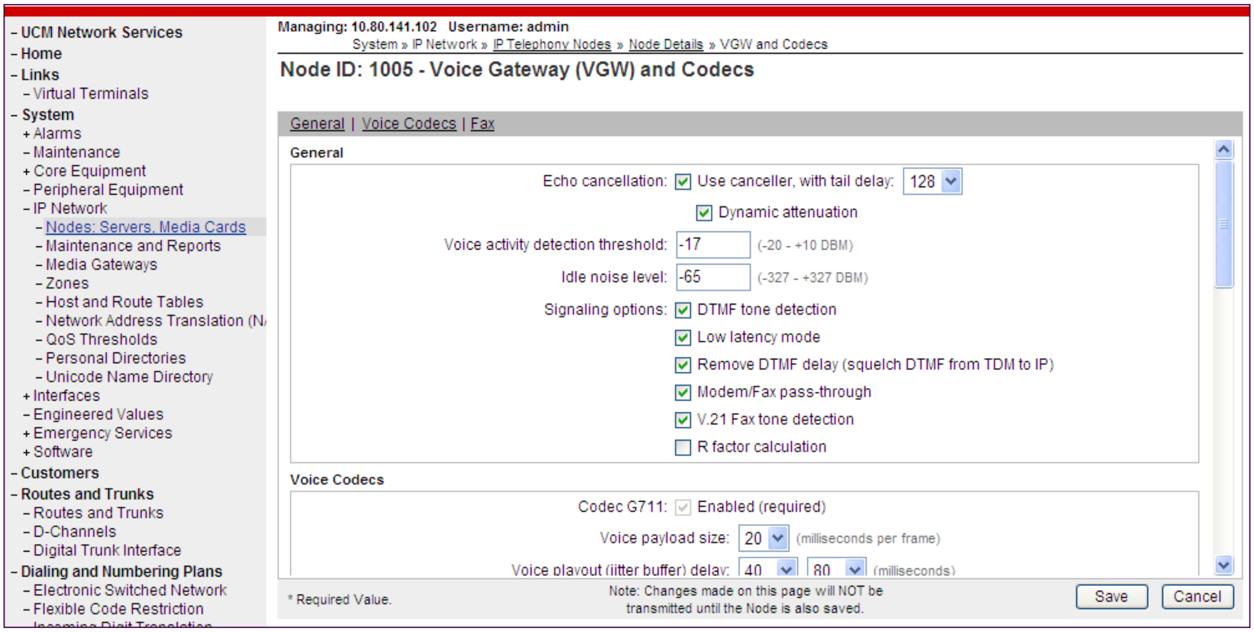


5.1.4. Voice Gateway and Codecs

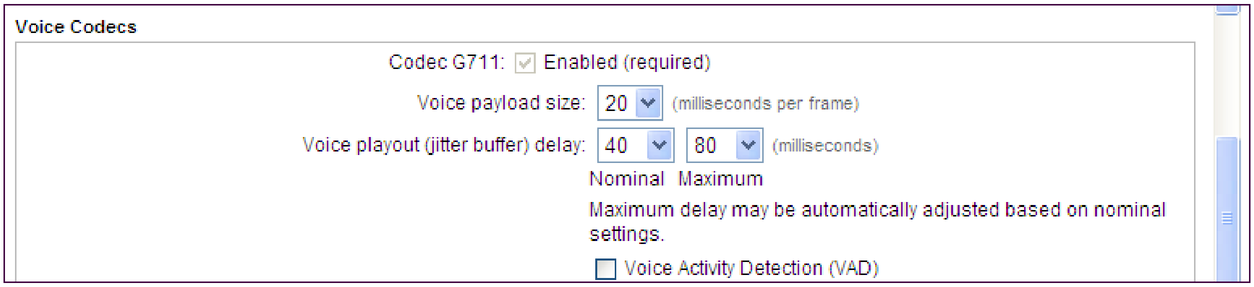
On the **Node Details** screen, scroll down in the top window and select the **Voice Gateway (VGW) and Codecs** link as shown below.



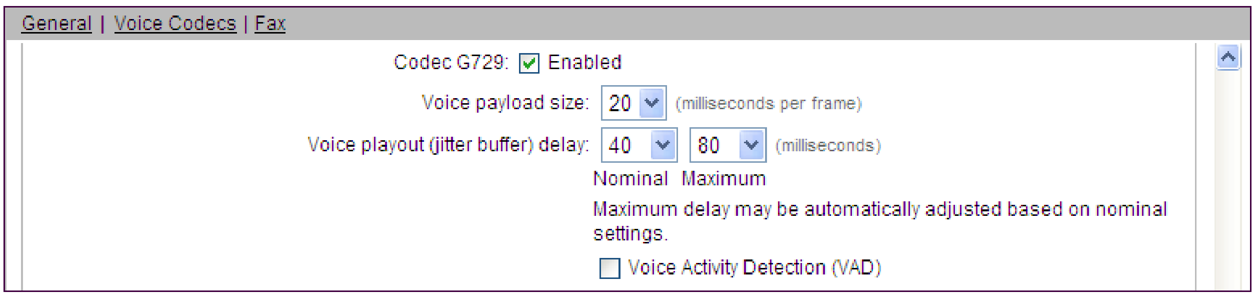
The following screen shows the General parameters used in the sample configuration.



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.

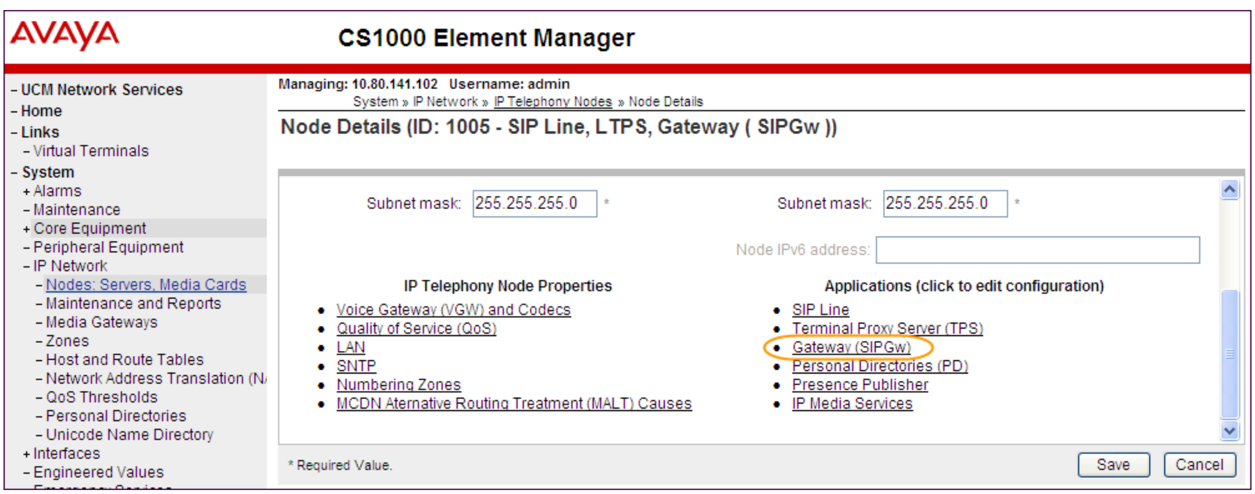


For the **Codec G.729**, ensure that the **Enabled** box is checked, and the **Voice Activity Detection (VAD)** box is un-checked. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order. During compliance testing, the G.729B codec was also tested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



5.1.5. SIP Gateway

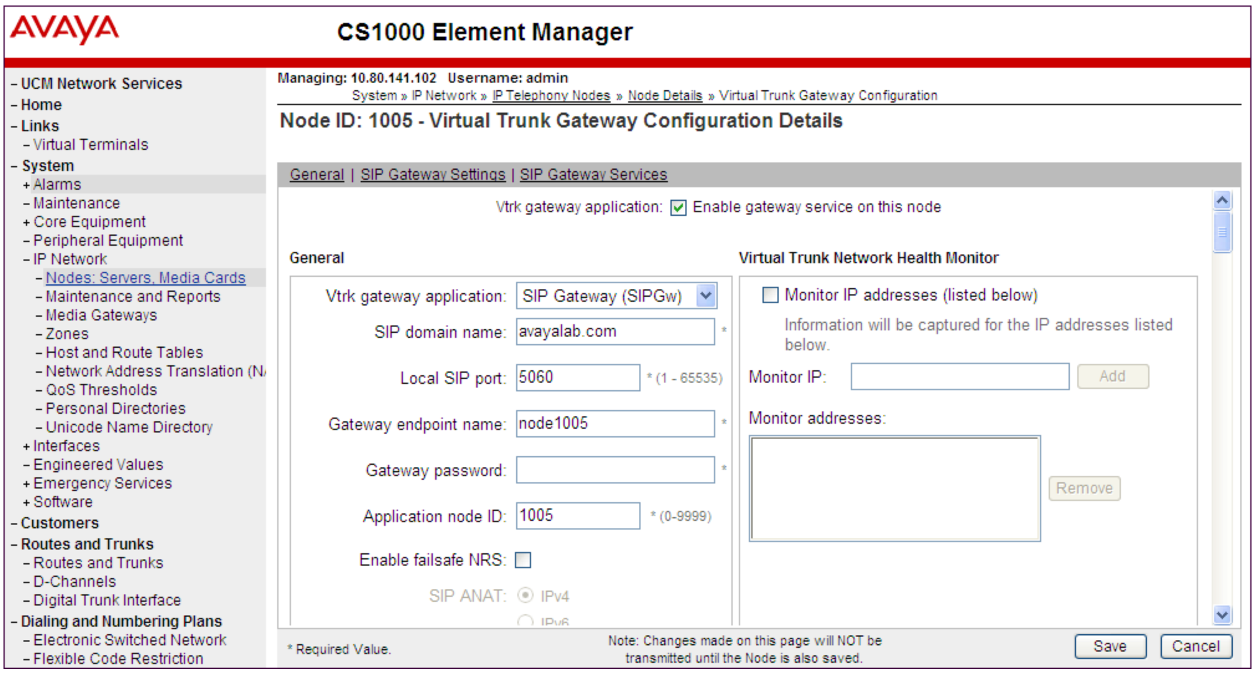
The SIP Gateway is the SIP trunk between the CS1000E and Session Manager. On the **Node Details** screen, scroll down in the top window and select the **Gateway (SIPGw)** link as show below.



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 shown in **Section 5.1.1**.

The values defined for the sample configuration are shown below.

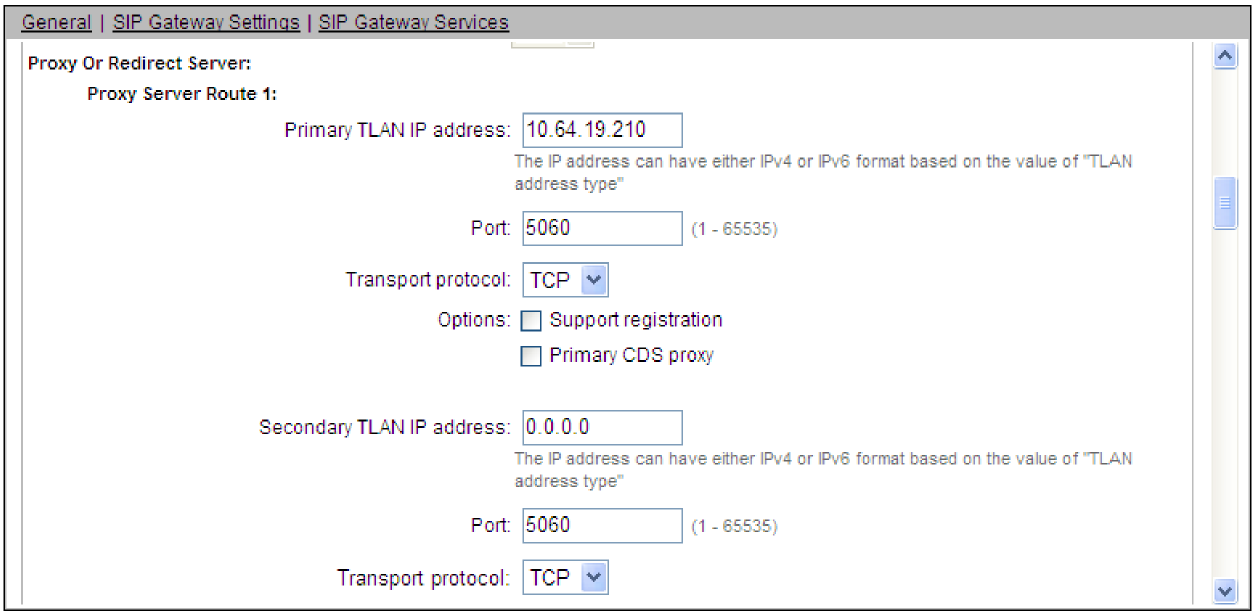


Scroll down to the **SIP Gateway Settings → Proxy or Redirect Server:** section.

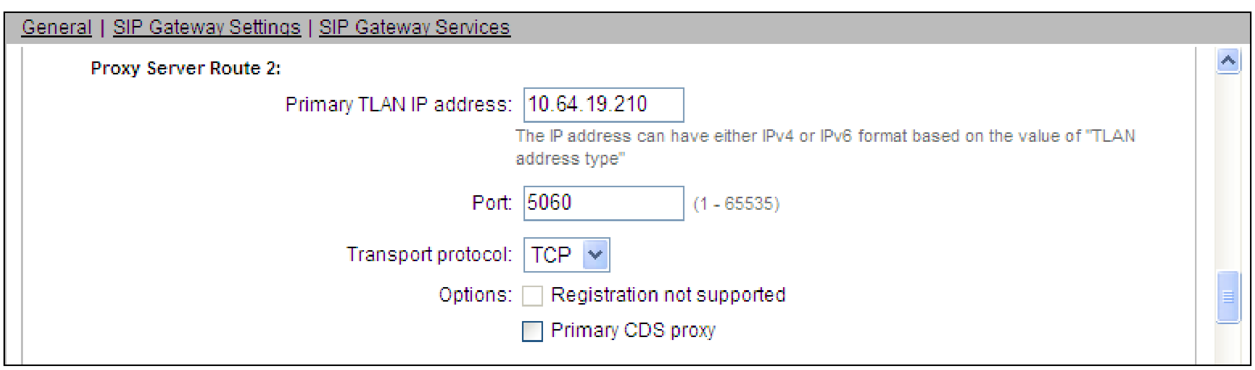
Under **Proxy Server Route 1**, enter the following and use default values for remaining fields.

- **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**

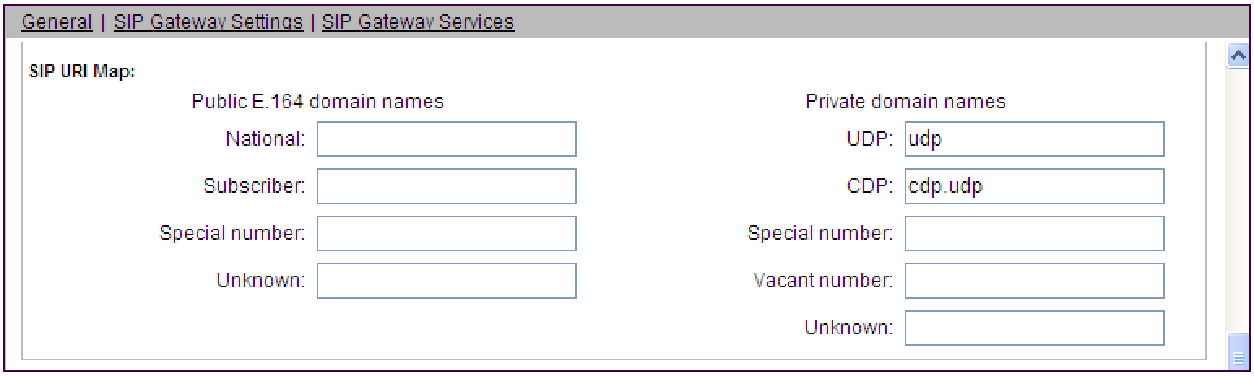
The values defined for the sample configuration are shown below.



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



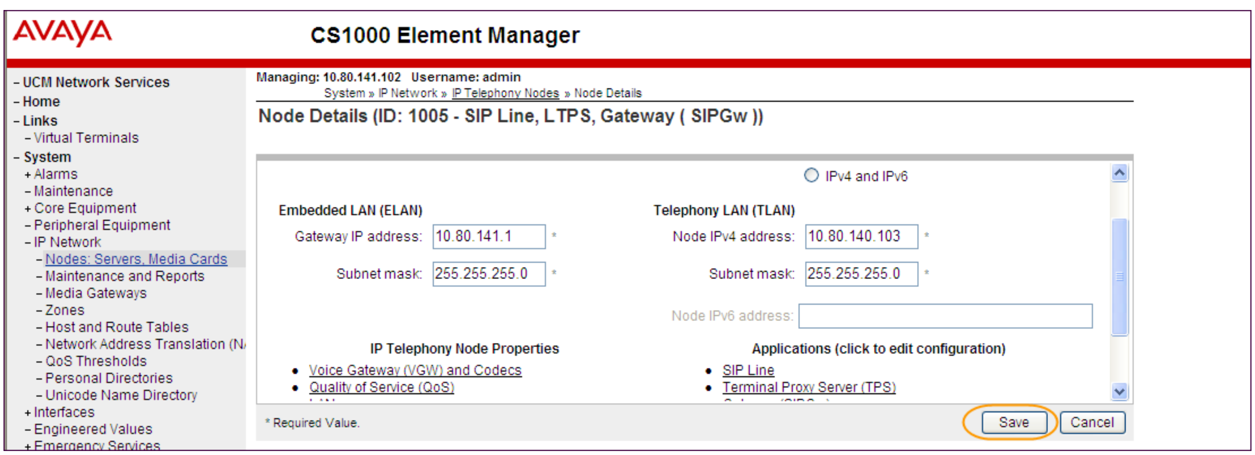
Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. The Avaya CS1000E will put the “string” entered in the **SIP URI Map** in the “phone-context=<string>” parameter in SIP headers such as the To and From headers. If the value is configured to blank,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



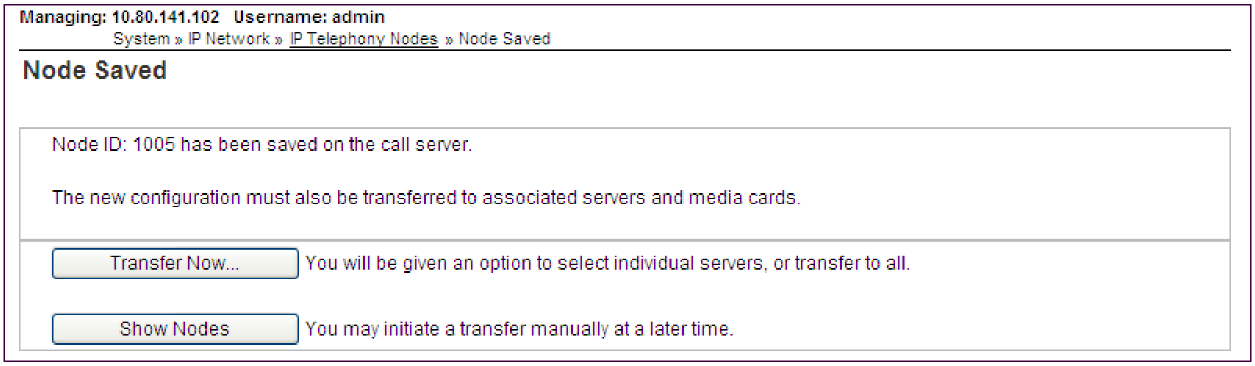
Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen.

5.1.6. Synchronize Node Configuration

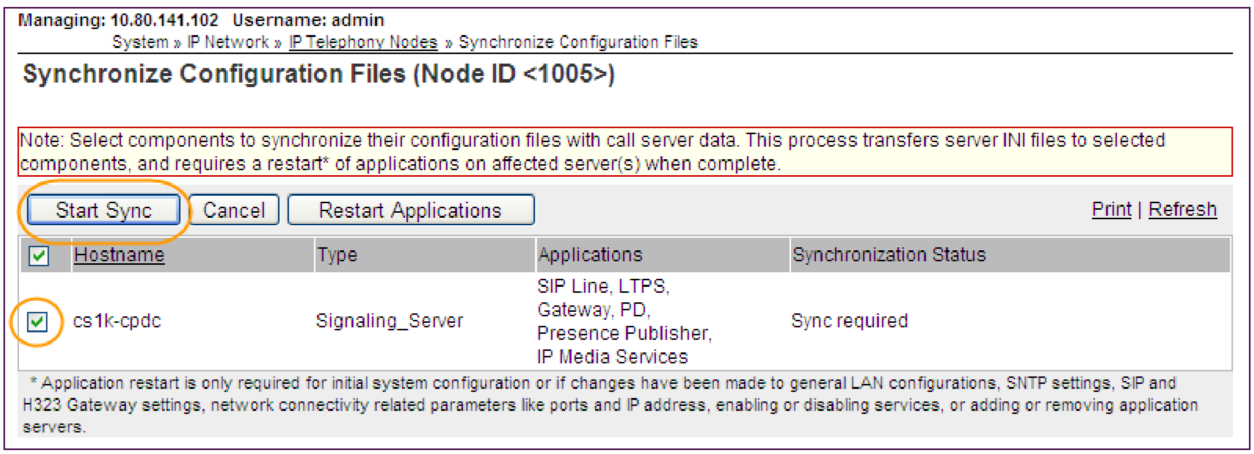
On the **Node Details** screen click **Save** as shown below.



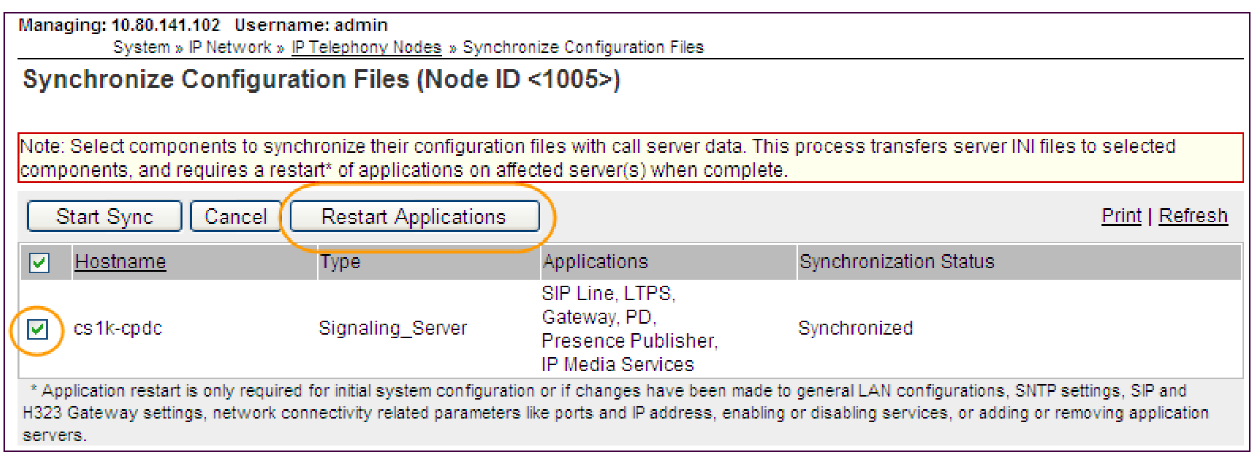
Select **Transfer Now** on the **Node Saved** page as show below.



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.

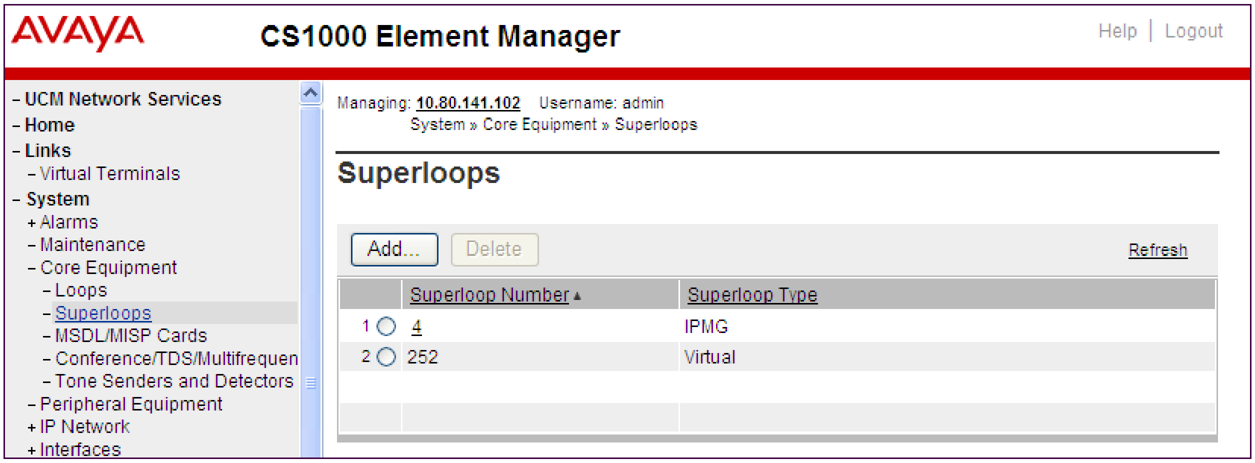


The **Synchronization Status** field will update from **Sync required** (as shown above) to **Synchronized** (as shown below). After synchronization completes, place a check mark next to the appropriate Hostname and click **Restart Applications**.



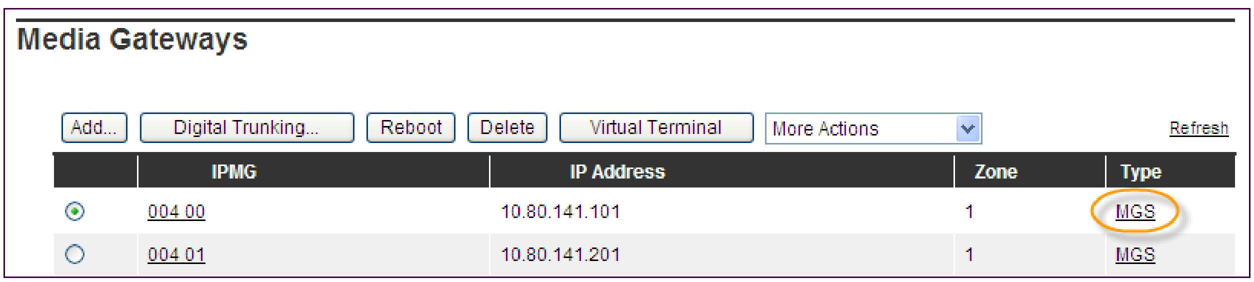
5.2. Virtual Superloops

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.

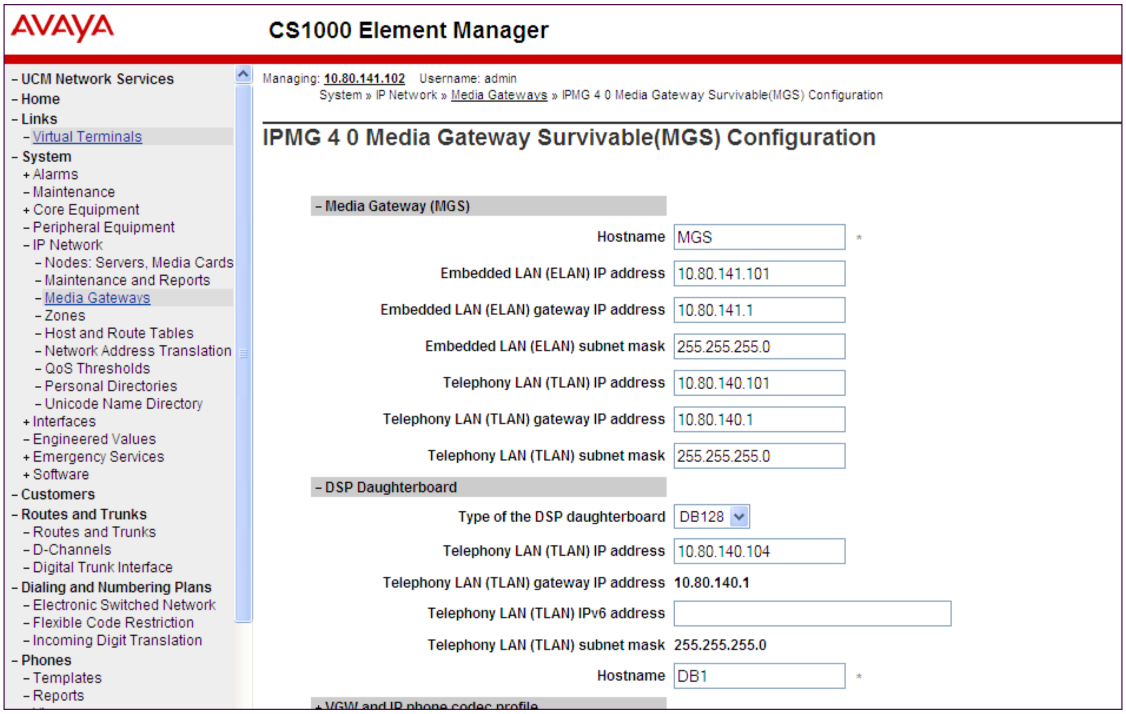


5.3. Media Gateway

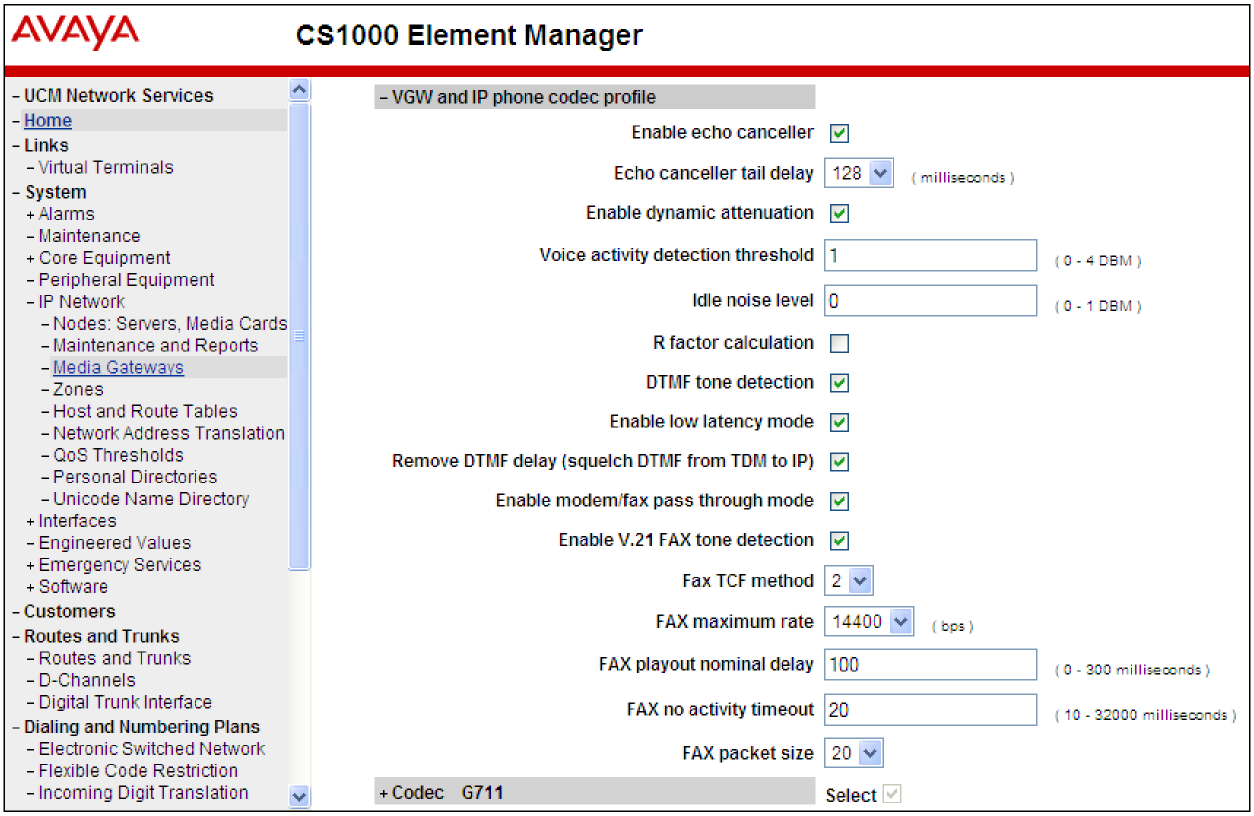
Expand **System → IP Network** on the left panel and select **Media Gateways**. Click the link in the **Type** column for the appropriate Media Gateway to be modified as shown below.



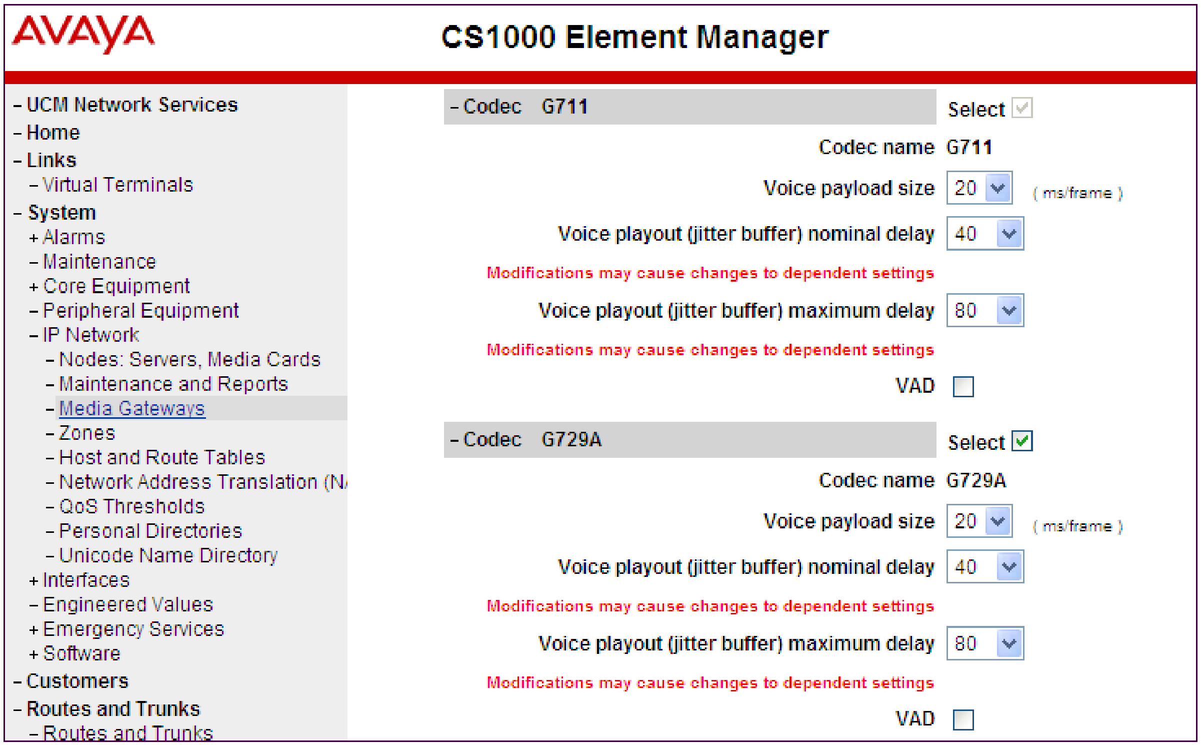
The **IPMG 4 0 Media Gateway Survivable(MGS) Configuration** window appears. The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard 1** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for a call from a digital telephone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



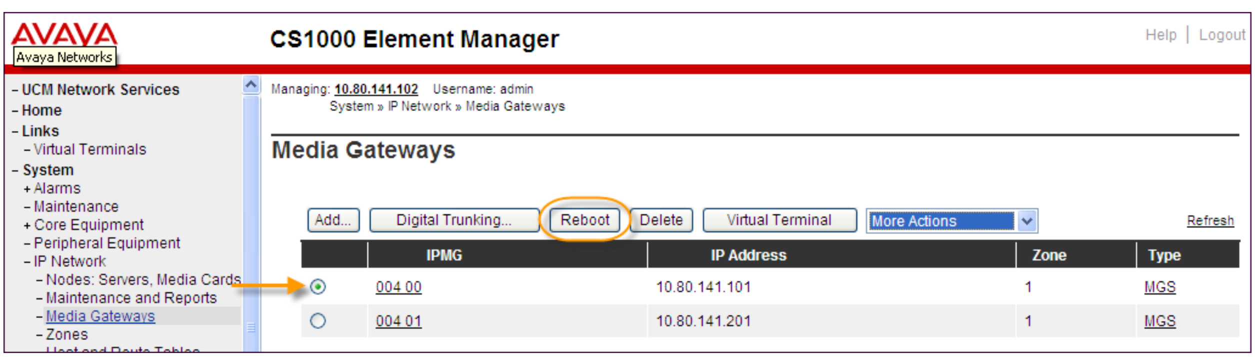
Scroll down to the area of the screen containing **VGW and IP phone codec profile** and expand it. The fax T.38 settings used for compliance testing is shown below.



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



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

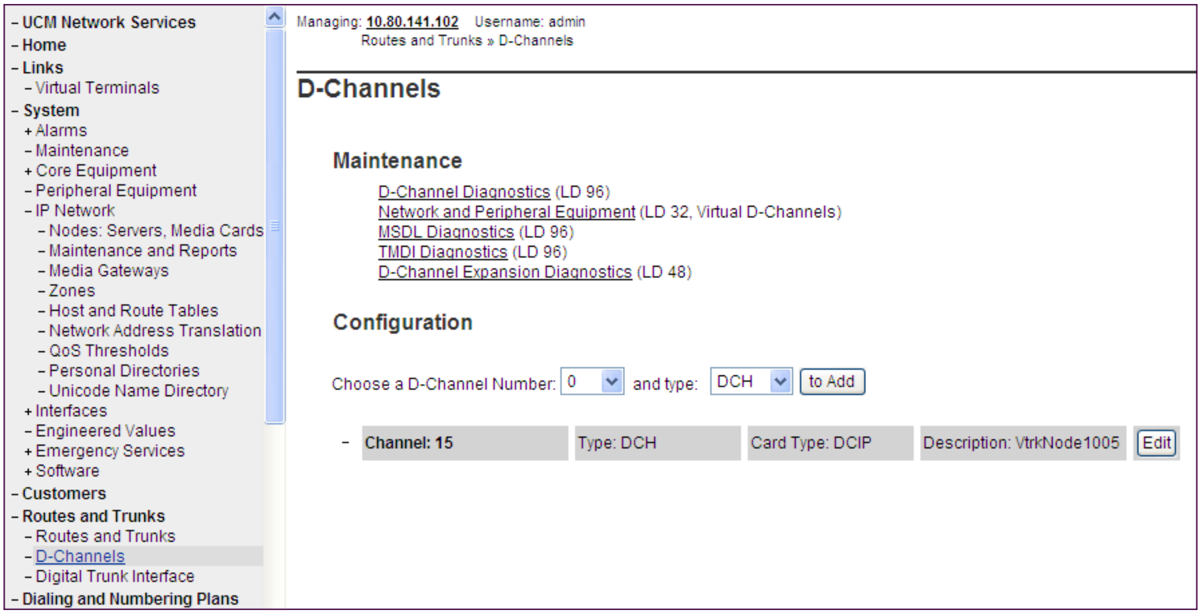


5.4. Virtual D-Channel, Routes and Trunks

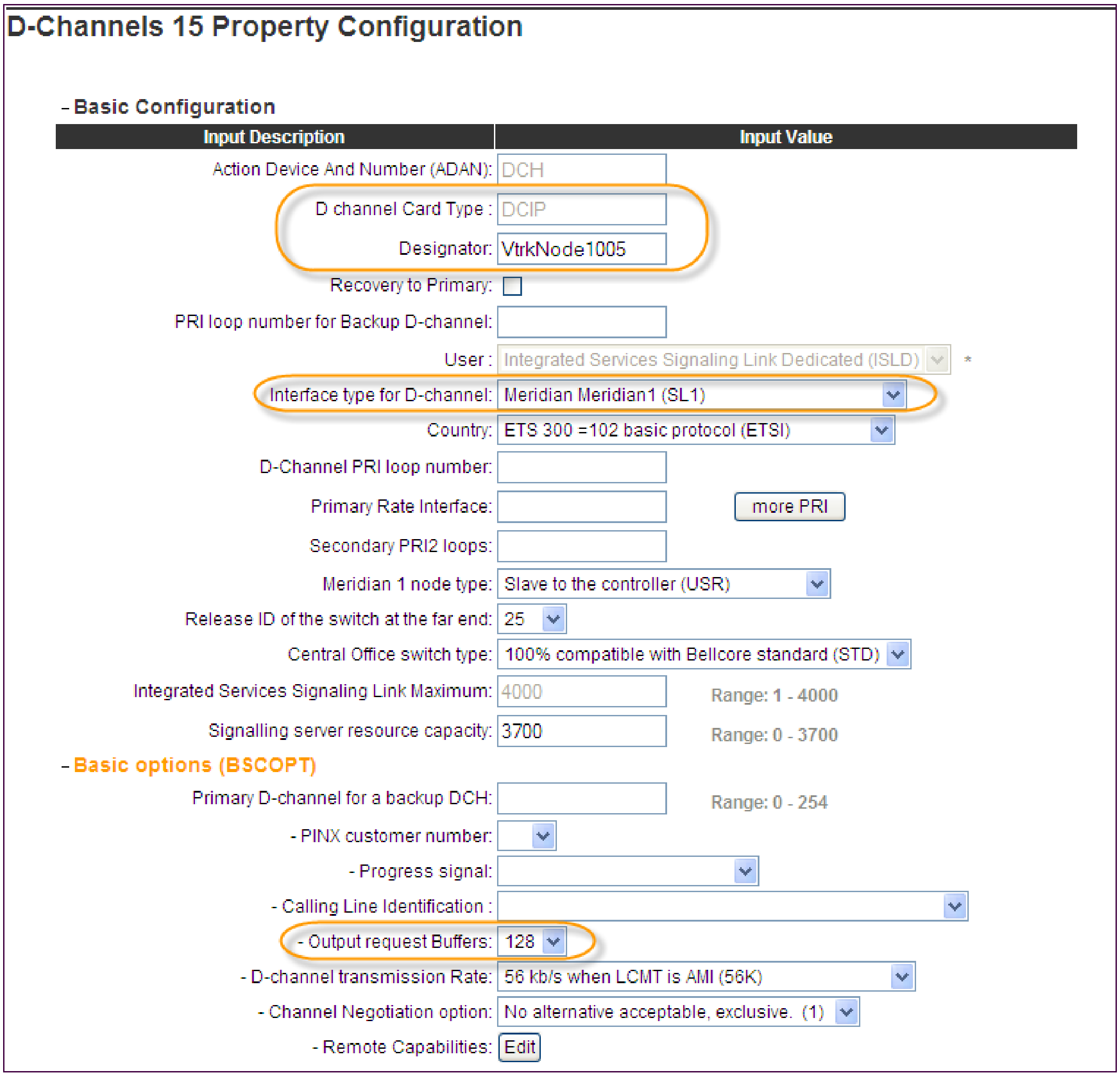
Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server.

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.

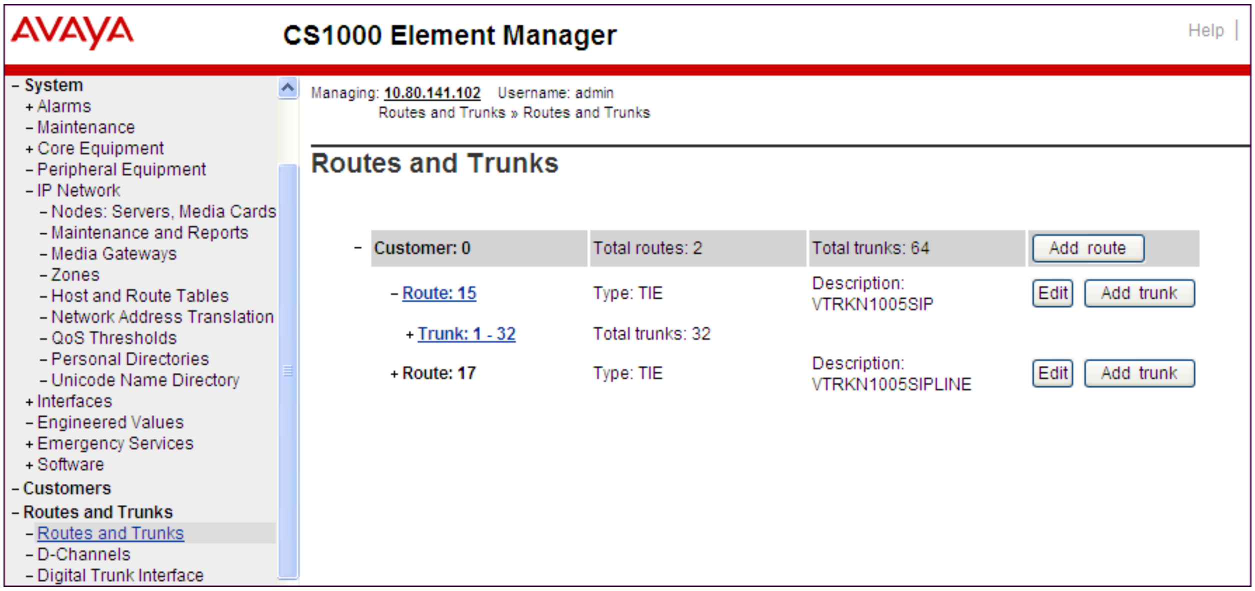


Select **Edit** to verify the configuration, as shown below. Verify **DCIP** has been selected for **D Channel Card Type** field and the **Interface type for D-Channel** is set to **Meridian Meridian 1(SL1)**. Under the Basic Options section, verify **128** is selected for the **Output request Buffers**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

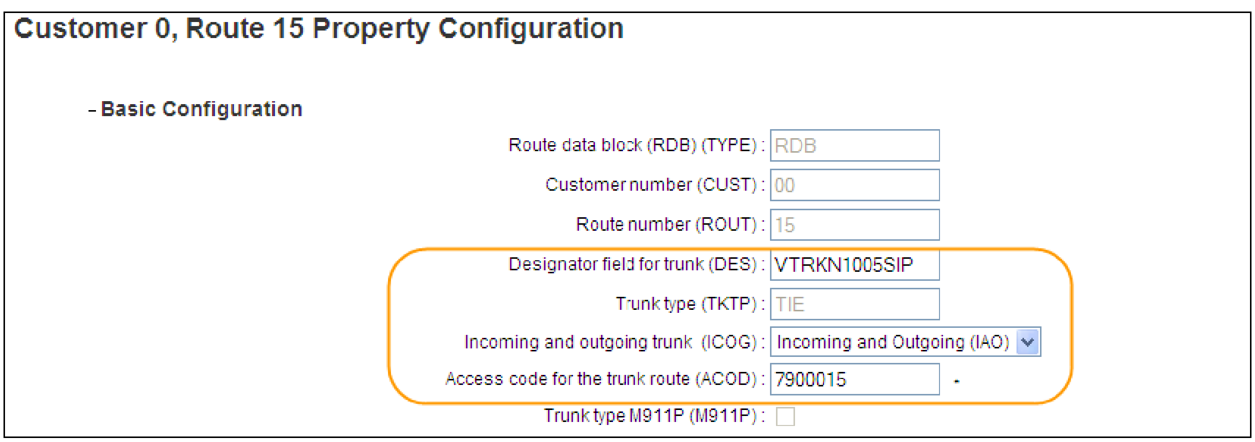


5.4.2. Routes and Trunks Configuration

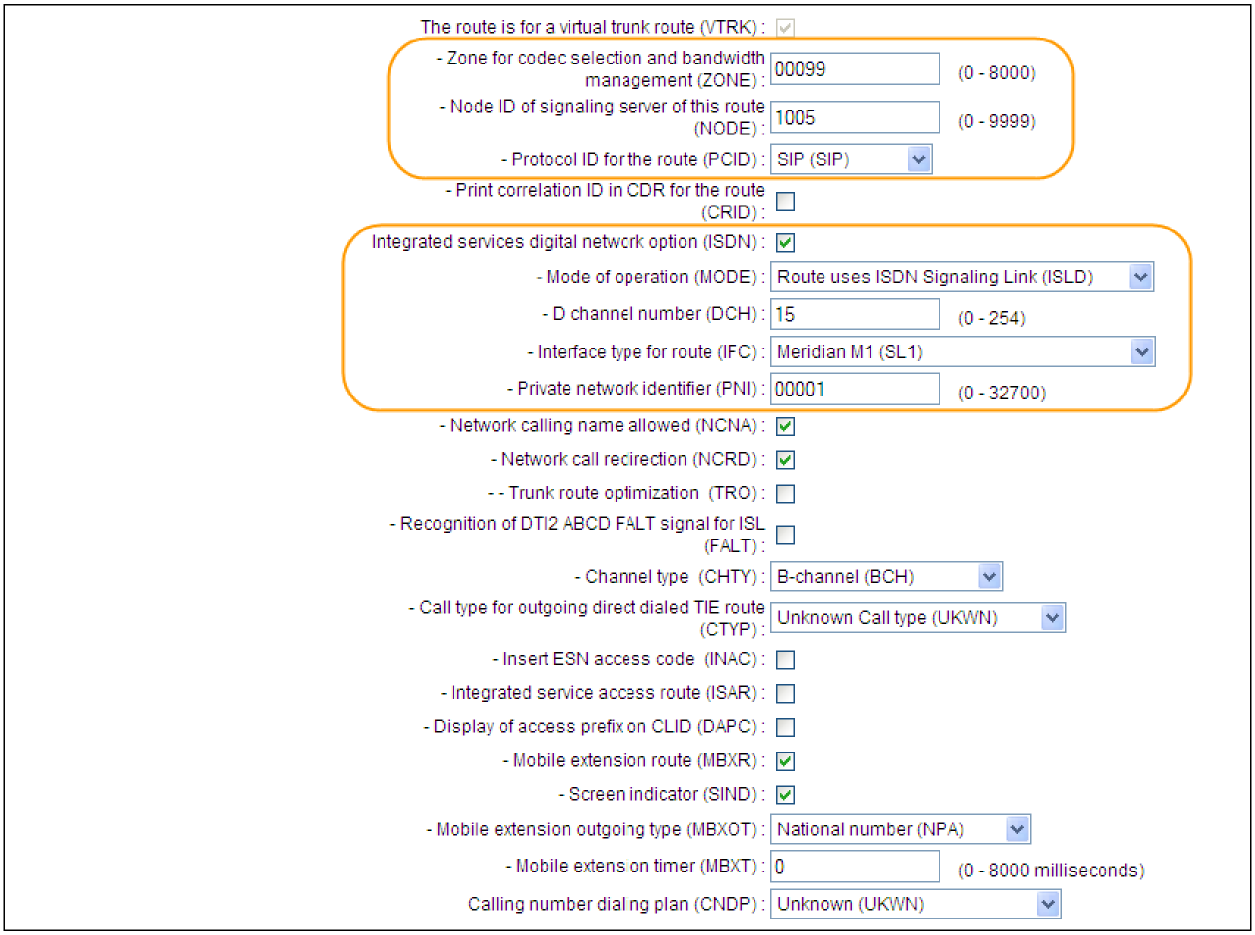
In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured. Expand **Routes and Trunks** on the left panel and expand the customer number. In the example screen that follows, it can be observed that Route 15 has 32 trunks in the sample configuration.



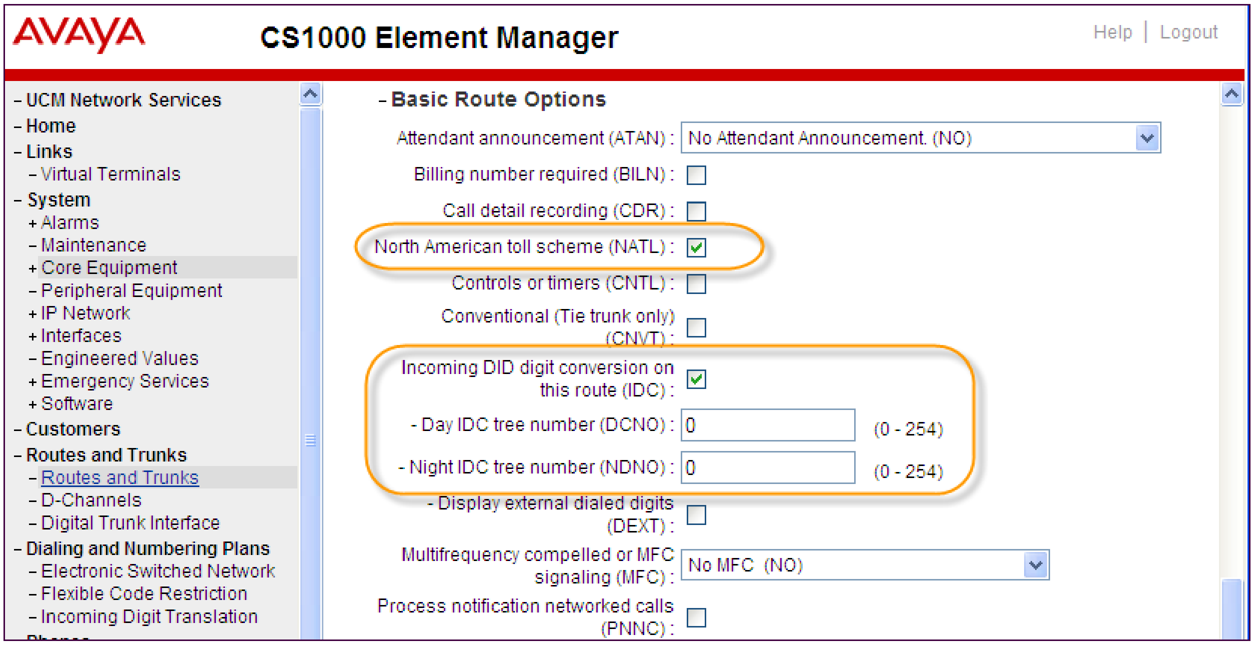
Select **Edit** to verify the configuration, as shown below. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may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

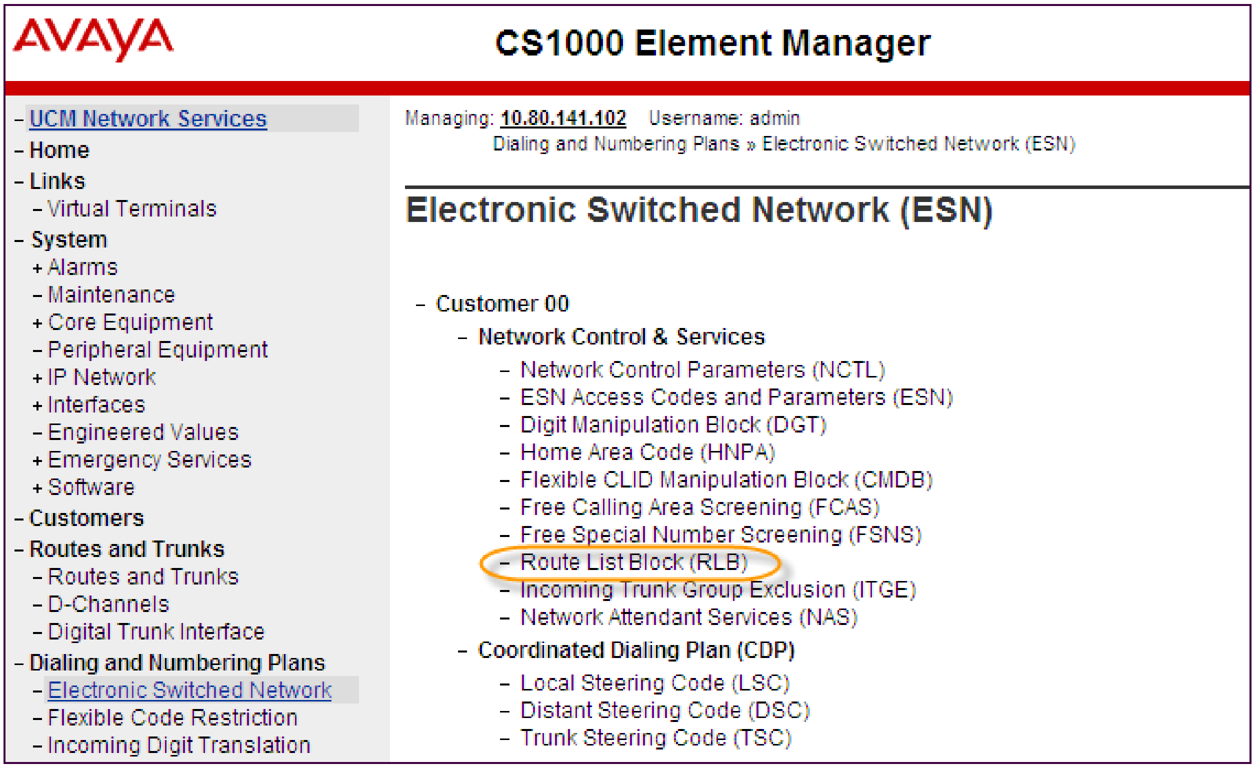


5.5. Dialing and Numbering Plans

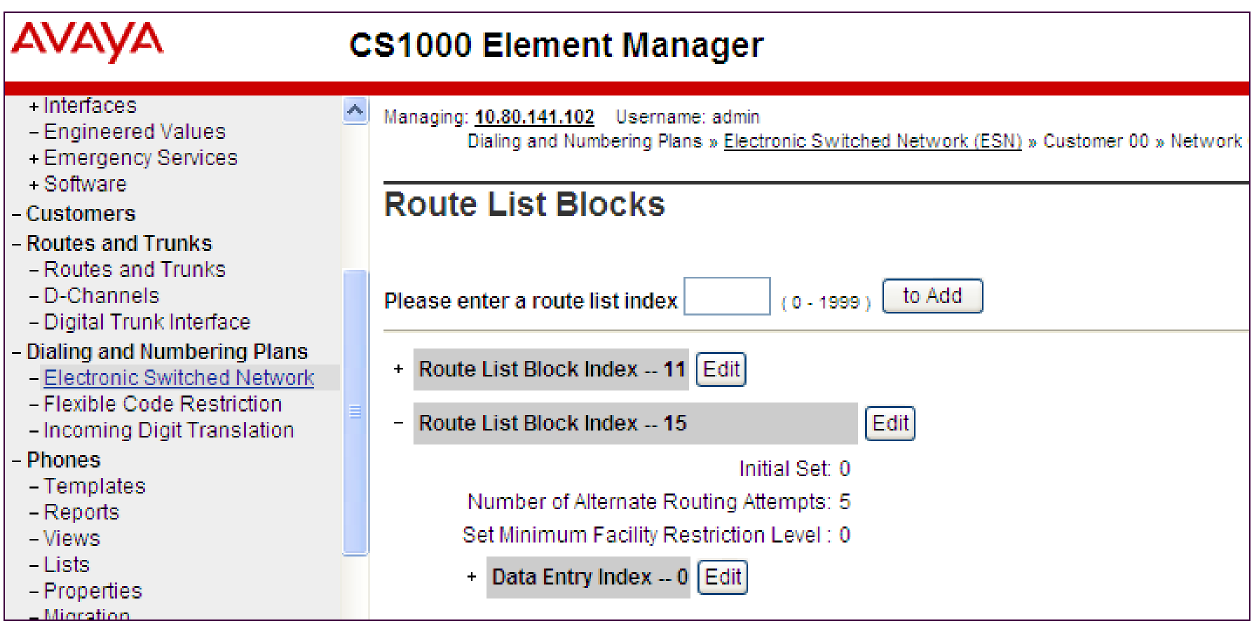
This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Session Manager for calls destined for the CenturyLink SIP Trunk. The routing defined in this section is simply an example and not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

5.5.1. Route List Block

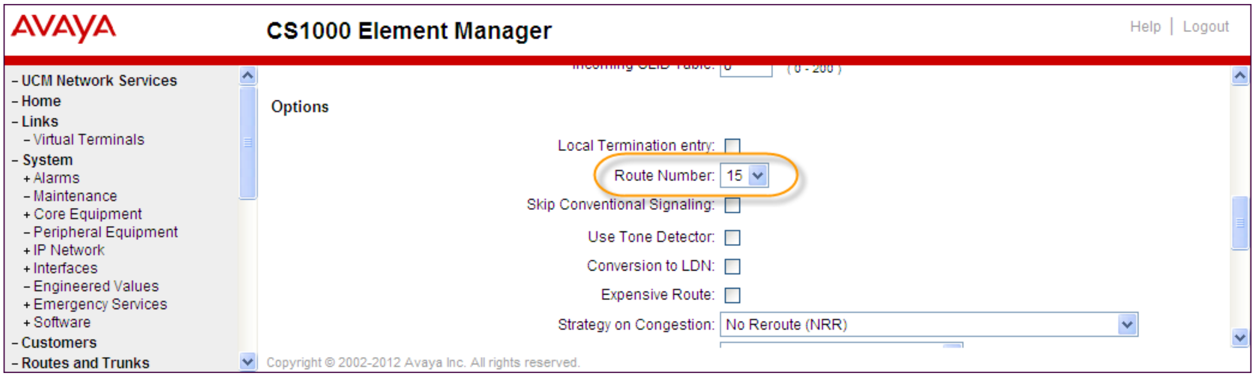
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown on the following page.



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.

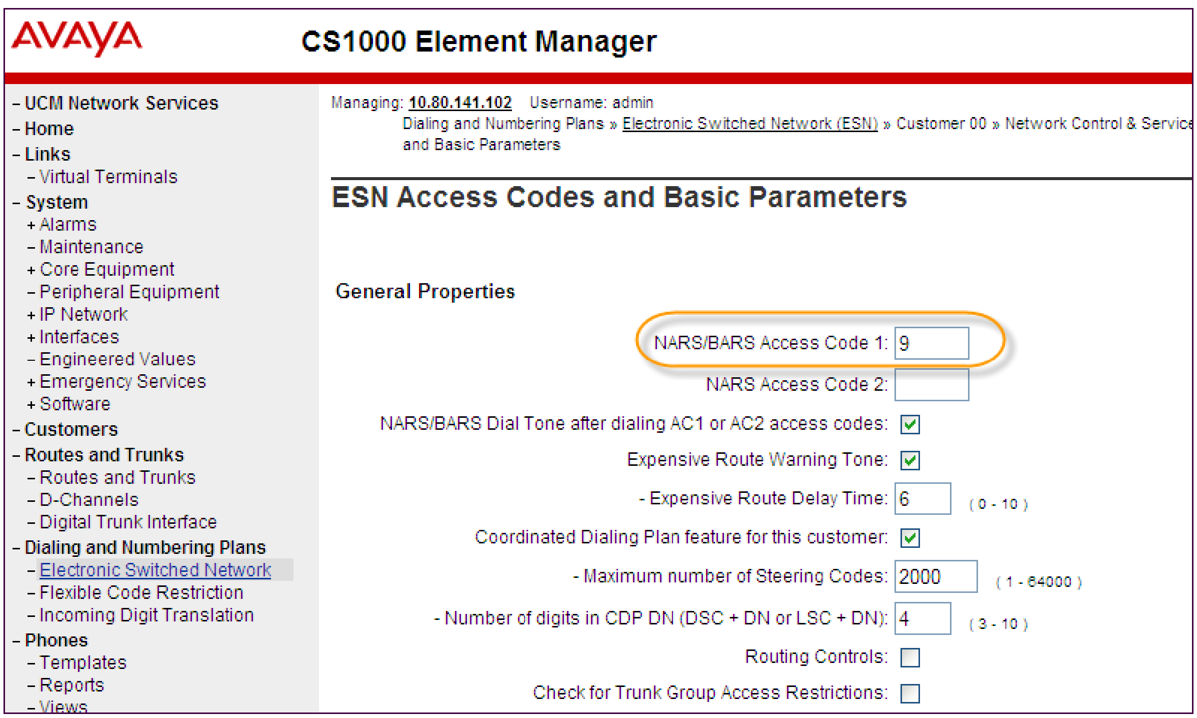


Under the **Options** section, select **<Route id>** in the **Route Number** field. In the sample configuration route number **15** was used. Default values may be retained for remaining fields.



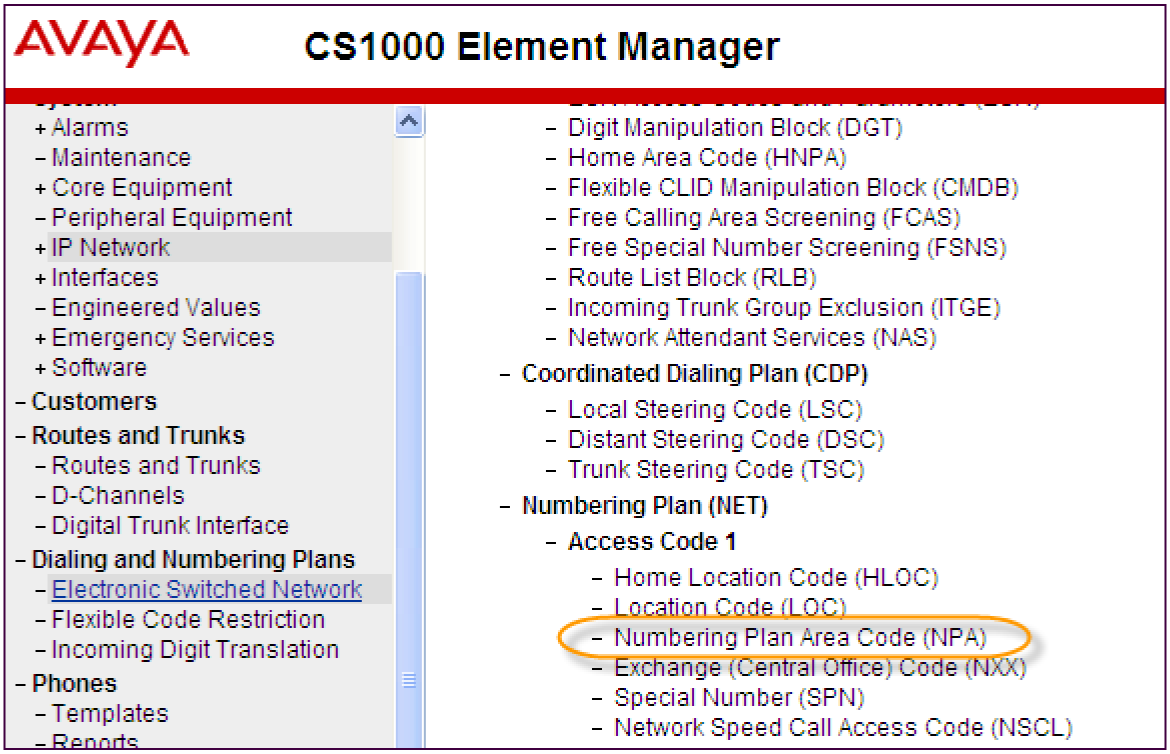
5.5.2. NARS Access Code

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.

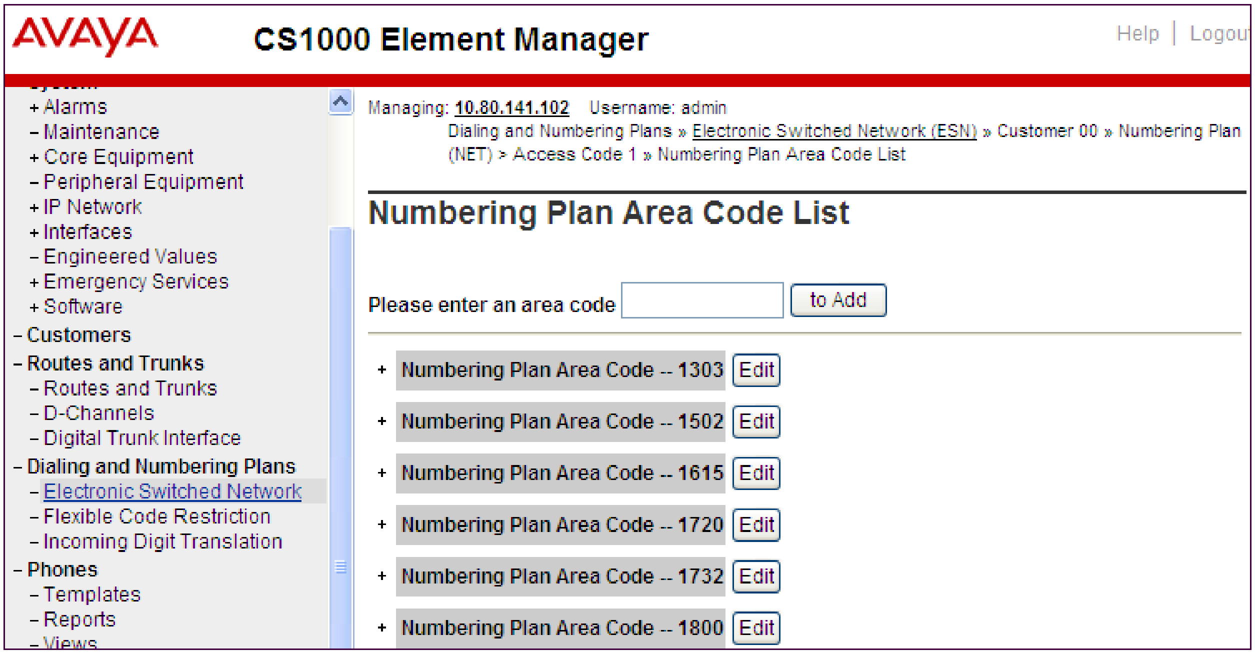


5.5.3. Numbering Plan Area Codes

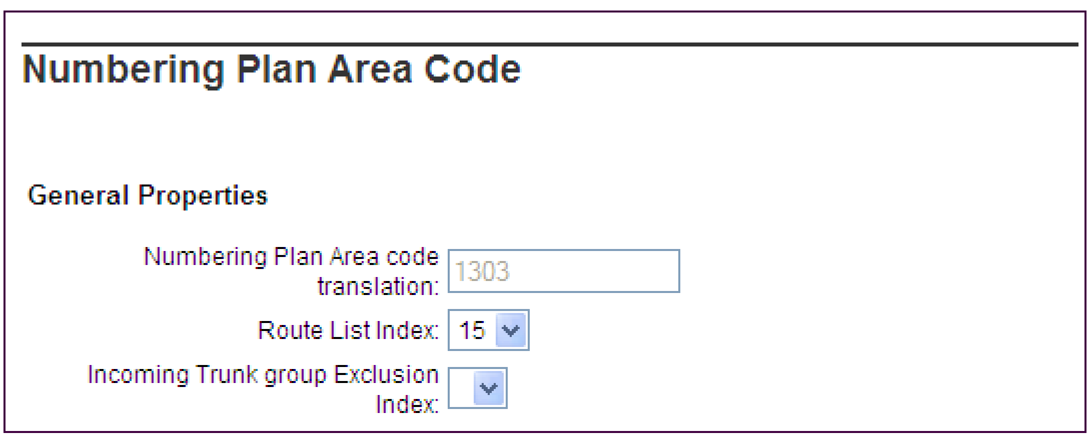
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Numbering Plan Area Code (NPA)** under the appropriate access code heading. In the sample configuration, this is **Access Code 1**, as shown below.



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.

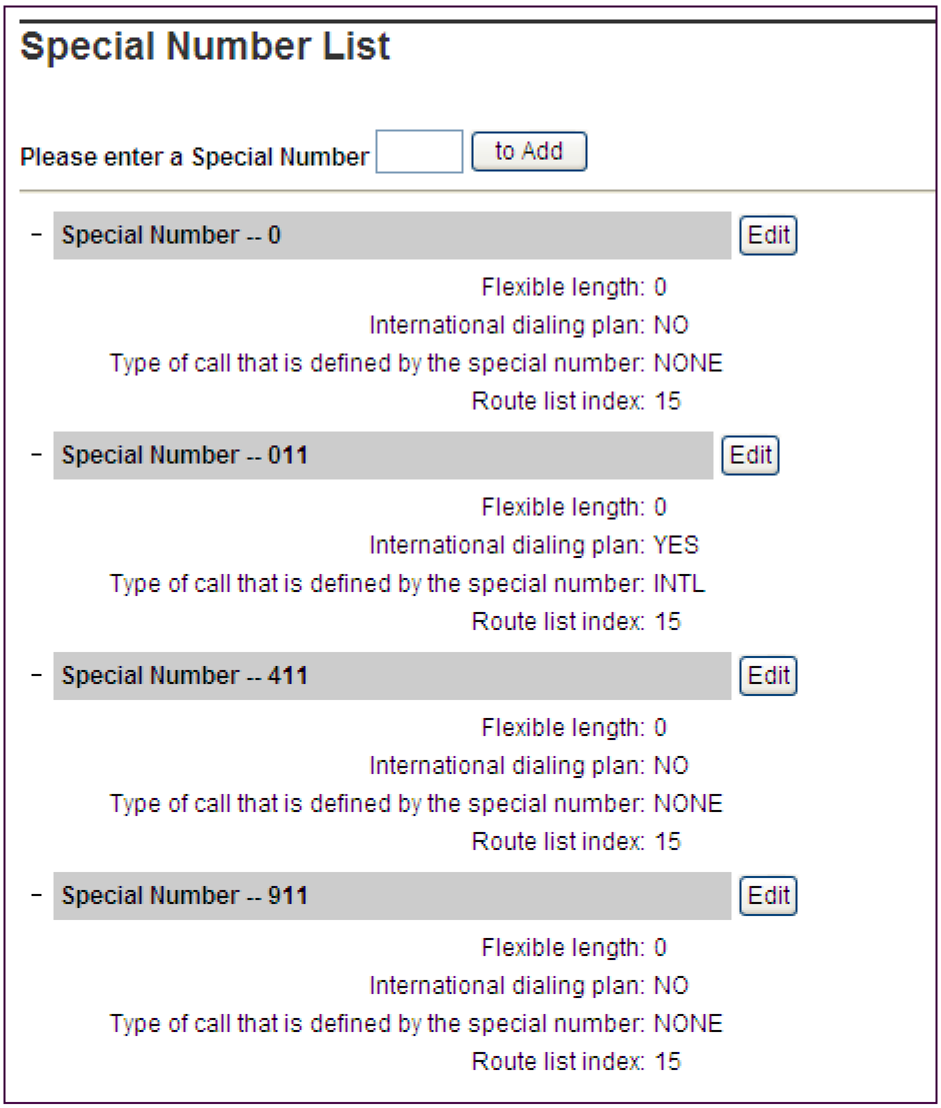


5.5.4. Special Numbers to Route to Session Manager

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 CenturyLink SIP Trunk. Although not intended to be prescriptive, one approach to such routing is summarized in this section.

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Special Number (SPN)** under the appropriate access code heading (as can be observed in the first screen in **Section 5.5.3**).

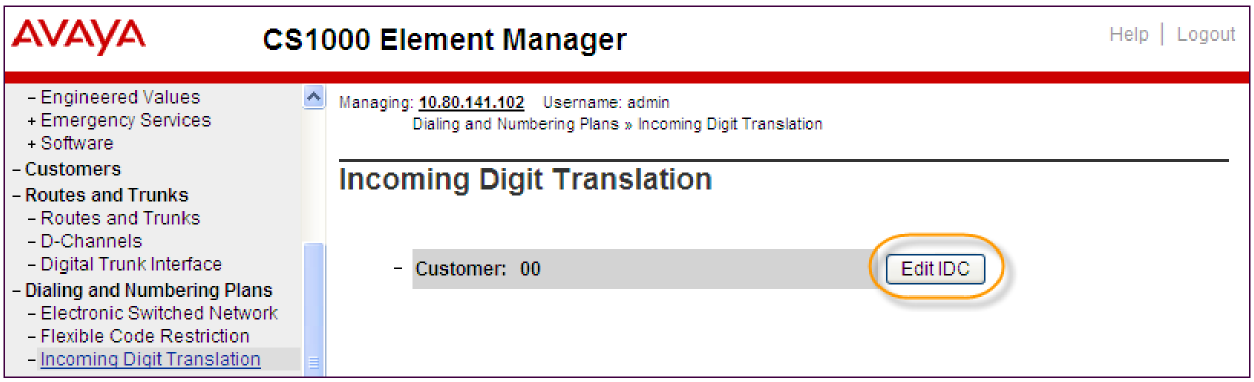
Add a new number by entering it in the **Please enter a Special Number** box and click **to Add** or click **Edit** to view or change a special number that has been previously configured. In the screen below, it can be observed that various dial strings such as **0**, **011**, **411** and **911** calls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



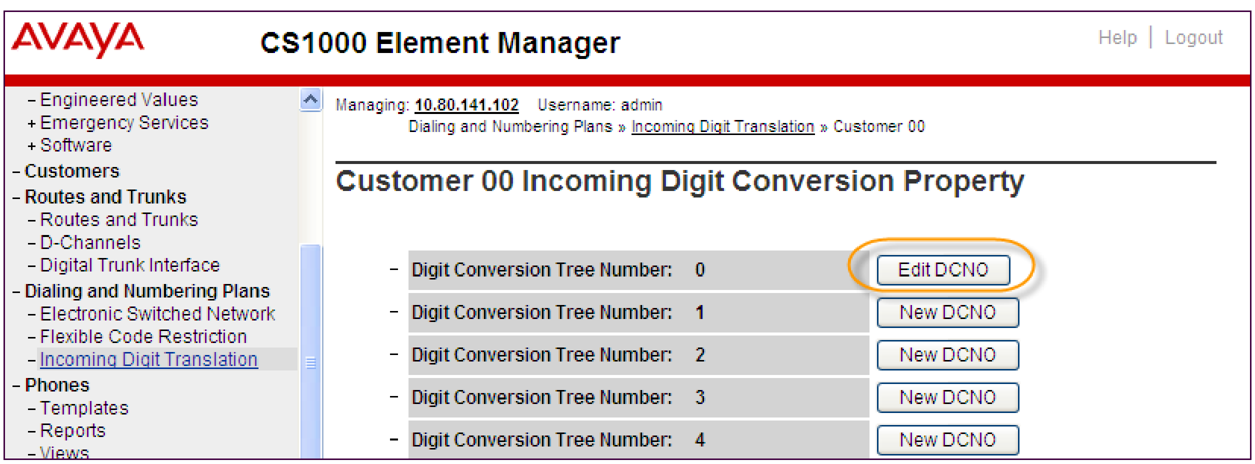
5.5.5. Incoming Digit Translation

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, and digit manipulation via the CS1000E Incoming Digit Translation table may not be necessary. If the DID number sent by CenturyLink 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.

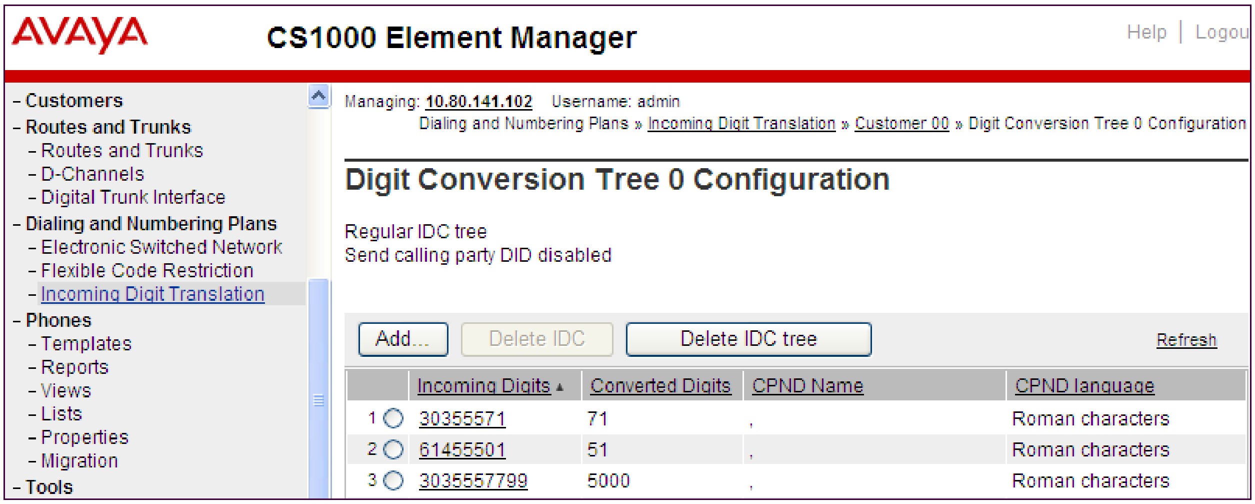


Click on the **New DCNO** to create the digit translation mechanism or if editing an existing one, select the **Edit DCNO** button next to the appropriate Digit Conversion Tree Number. In this example, **Digit Conversion Tree Number (DCNO) 0** has been created as shown below.



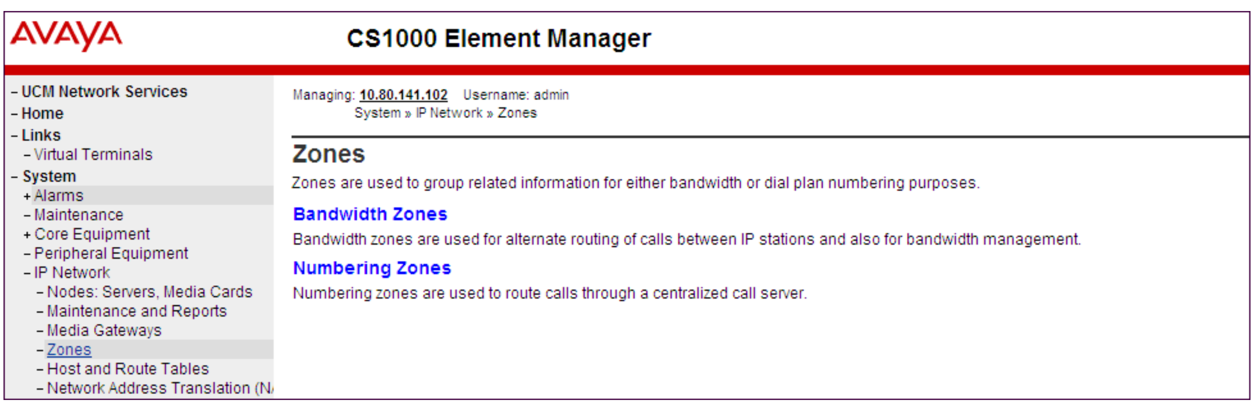
Detail configuration of the **DCNO** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000E system phones DN. This **DCNO** has been assigned to route 15 as shown in **Section 5.4.2**.

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

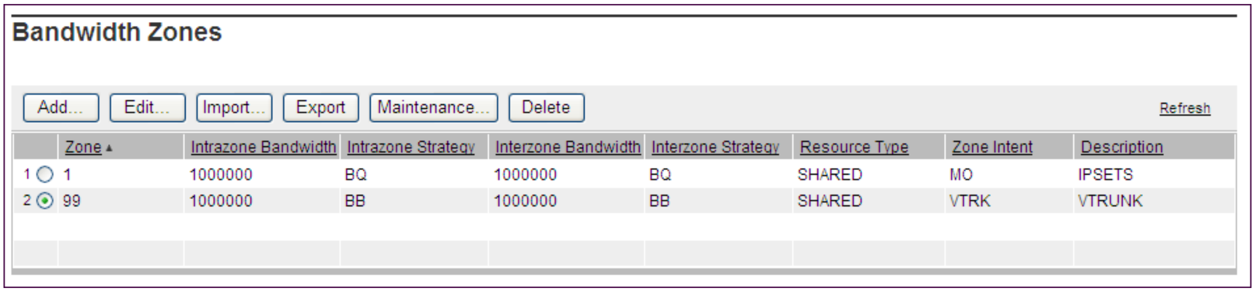


5.6. Zones and Bandwidth

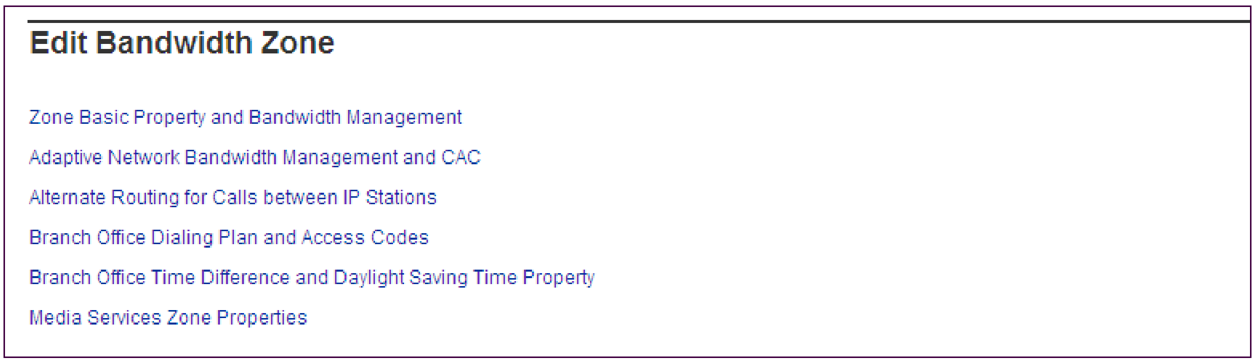
Zone configuration can be used to control codec selection and for bandwidth management. To configure, expand **System → IP Network** on the left panel and select **Zones** as shown below.



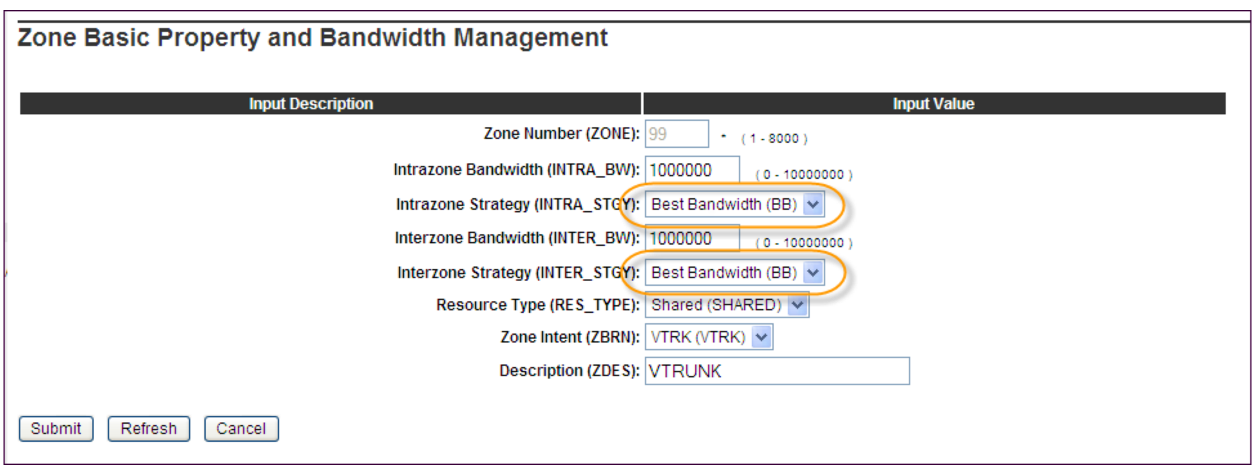
Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured. In production environments, it is likely that more zones will be required. Select the zone associated with the virtual trunk to Session Manager and click **Edit** as shown below. In the sample configuration, this is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

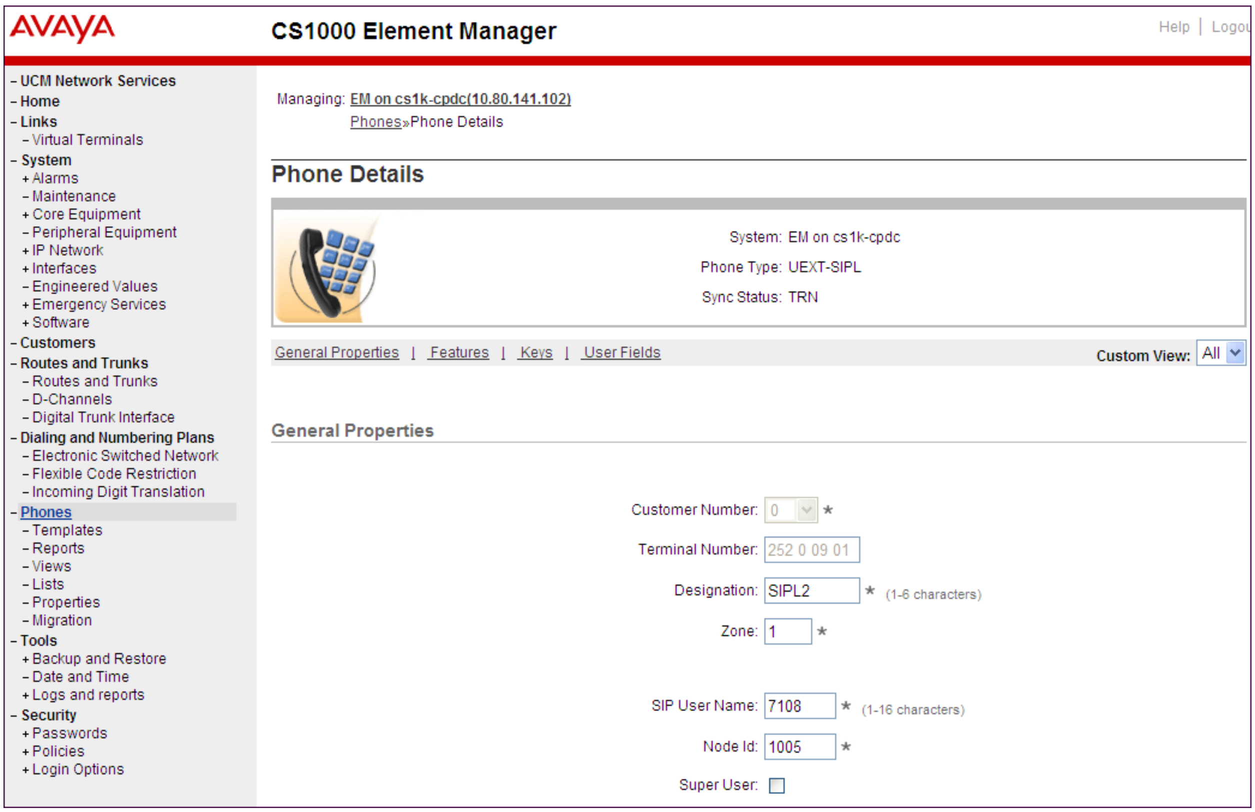


5.7. Example CS1000E Telephone Users

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

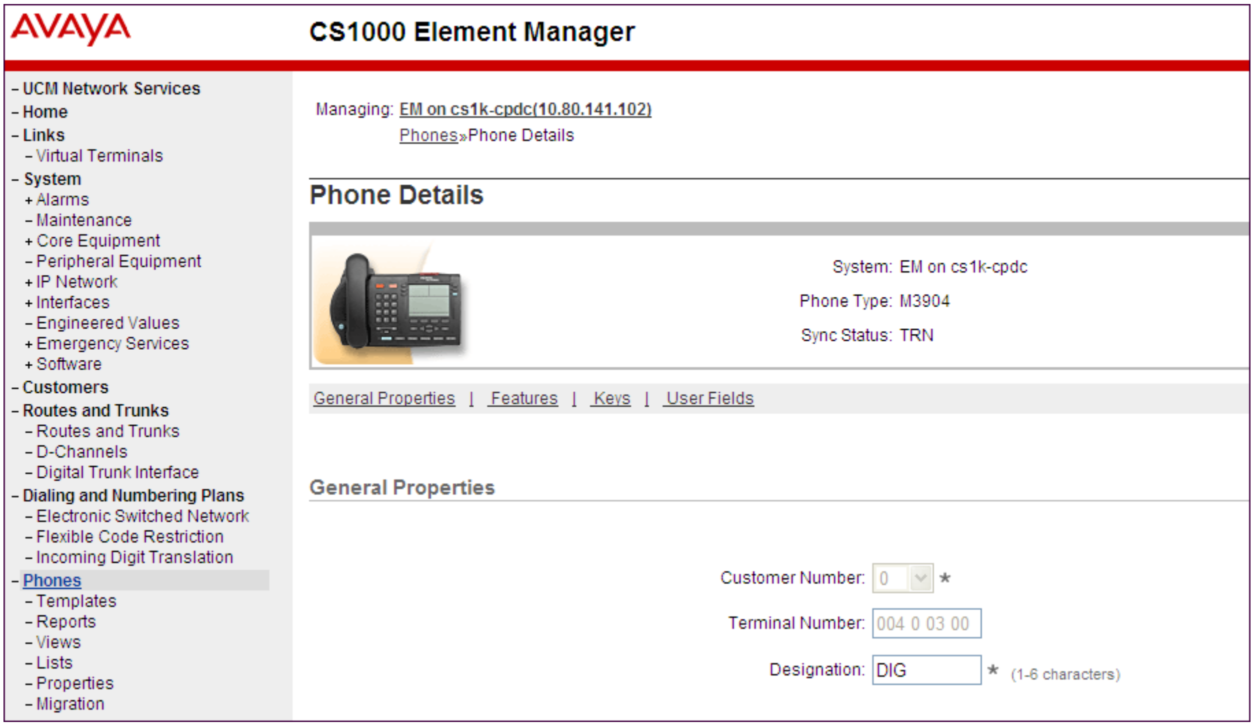
5.7.1. Example SIP Phone DN 7108, Codec Considerations

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 CenturyLink SIP Trunk, the call would use a **best bandwidth** strategy, and the call would use G.729A.

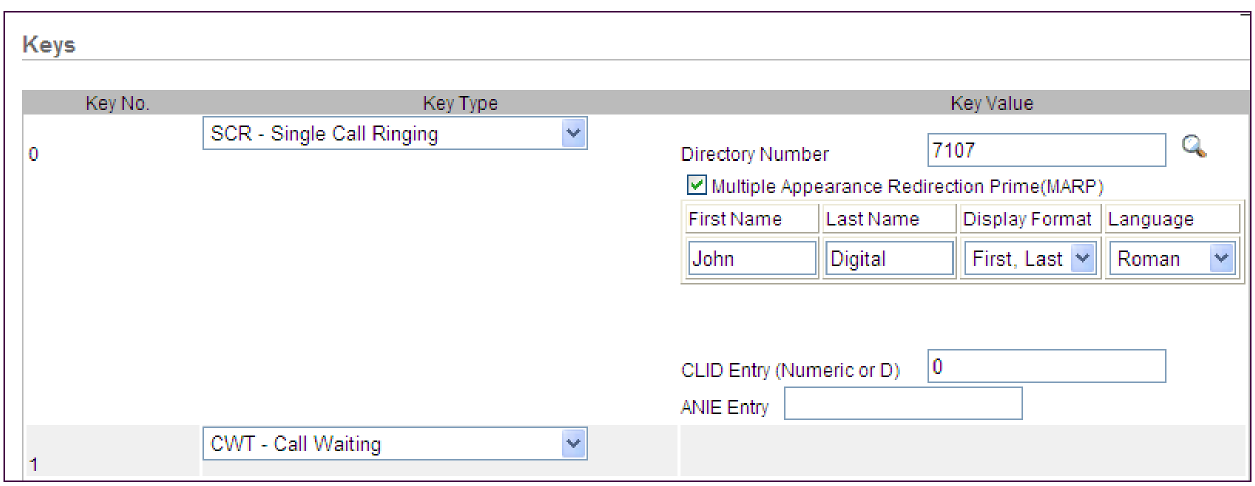


5.7.2. Example Digital Phone DN 7107 with Call Waiting

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

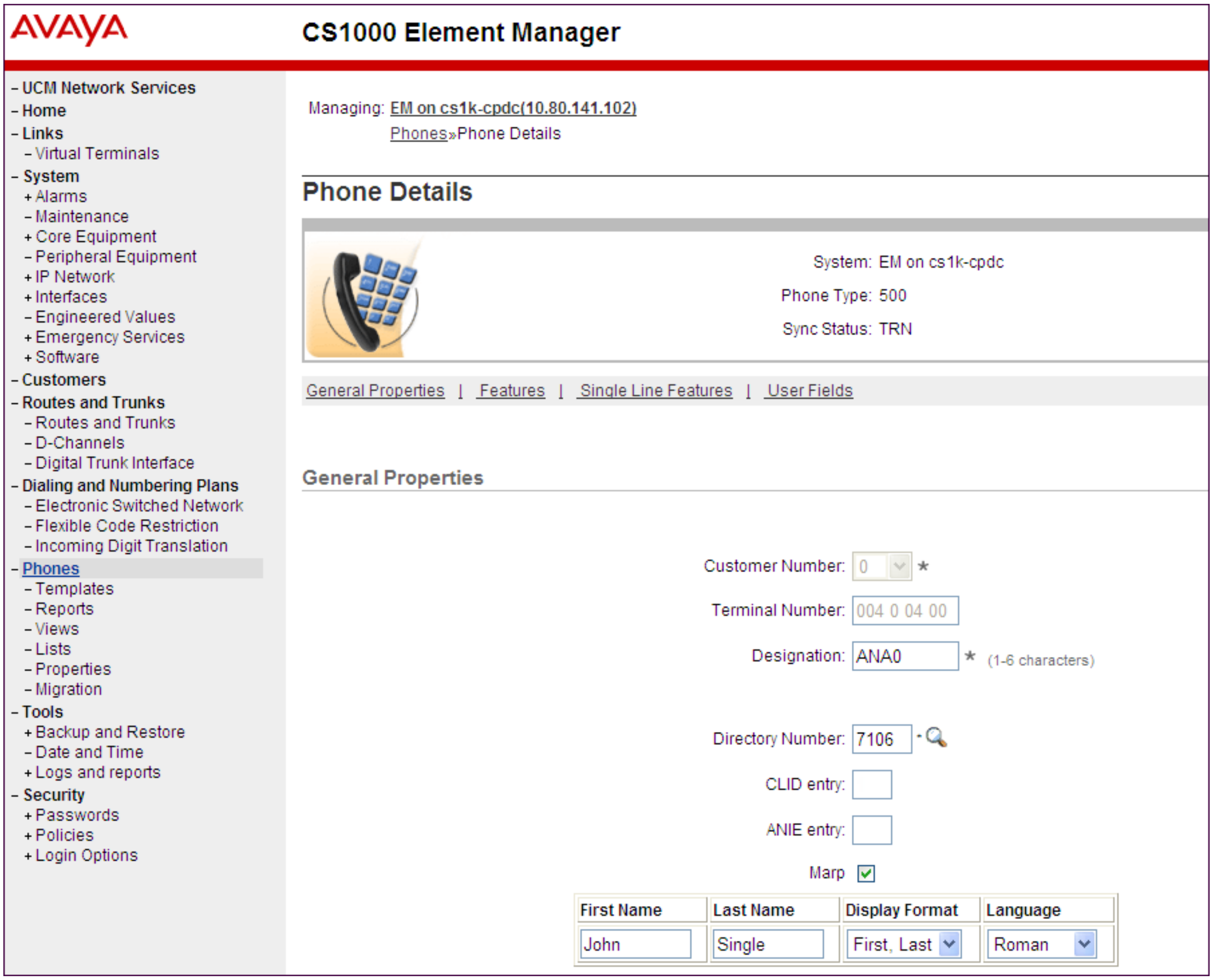


The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone. Although not shown in detail below, to use call waiting with tone, assign a key **CWT – Call Waiting**, set the feature **SWA – Call waiting from a Station** to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



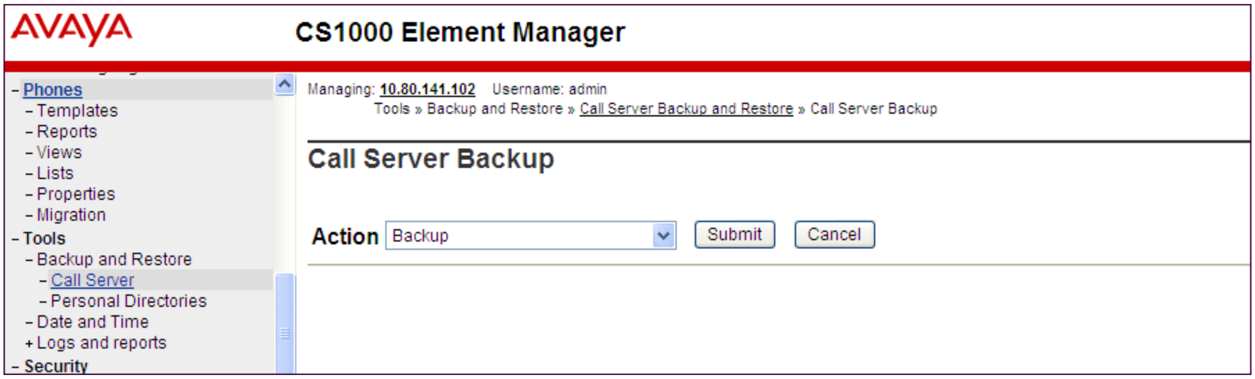
5.7.3. Example Analog Port with DN 7106, Fax

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.



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

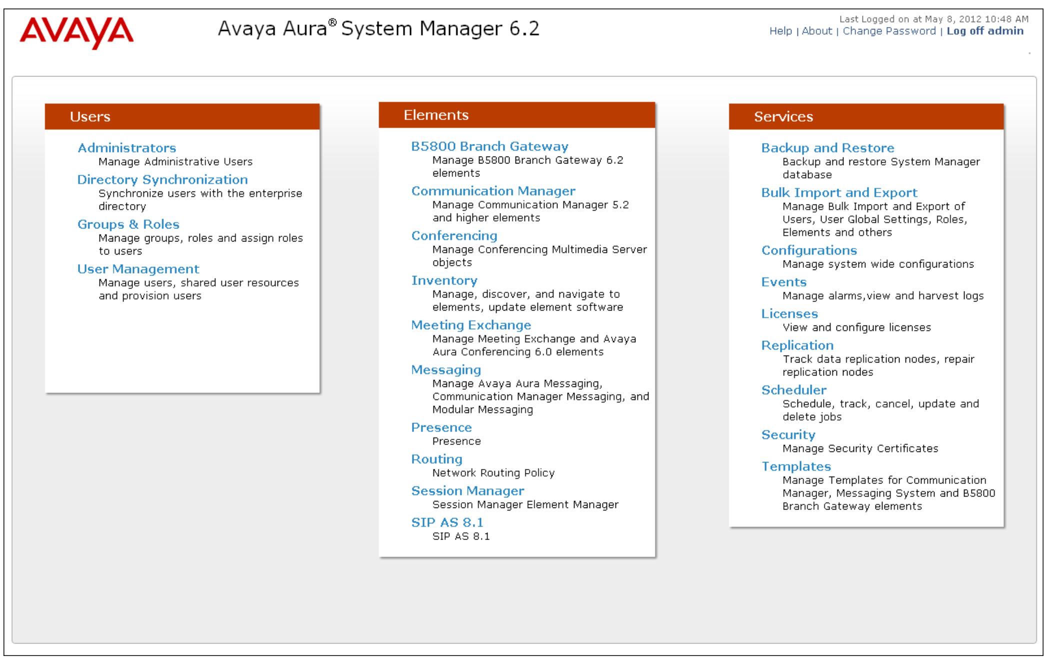
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to CS1000E, Acme Packet 3820 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.

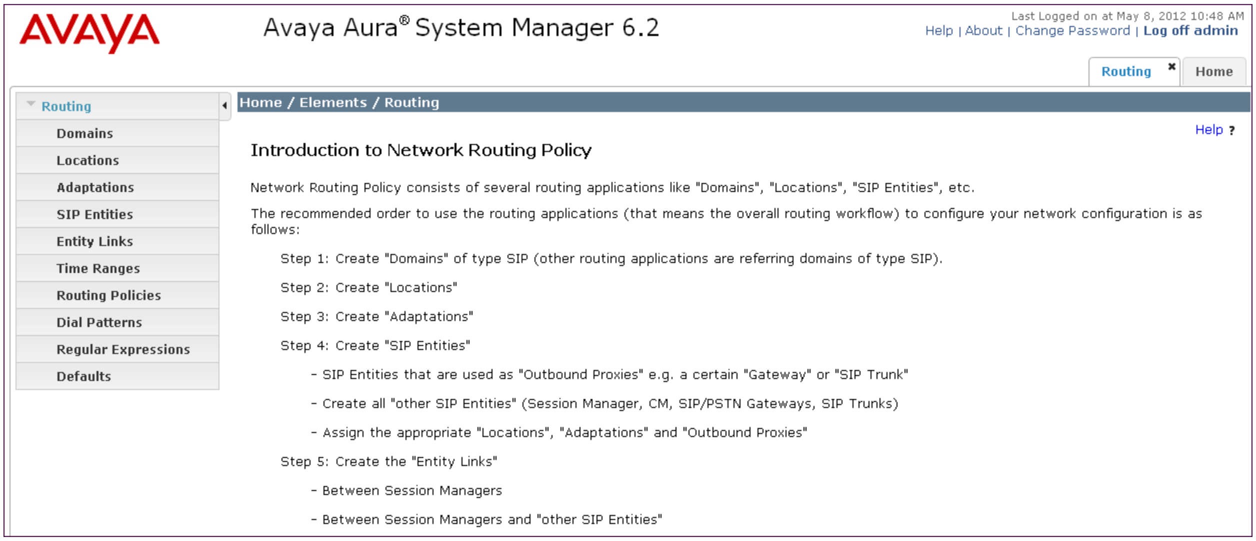
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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



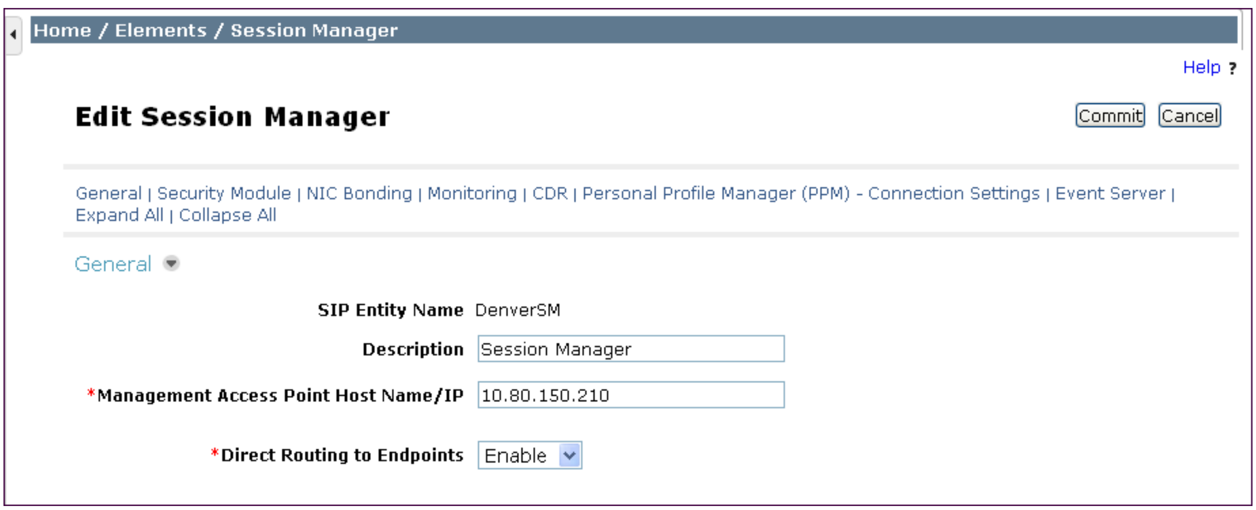
6.2. Add/View Avaya Aura® Session Manager Instance

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.

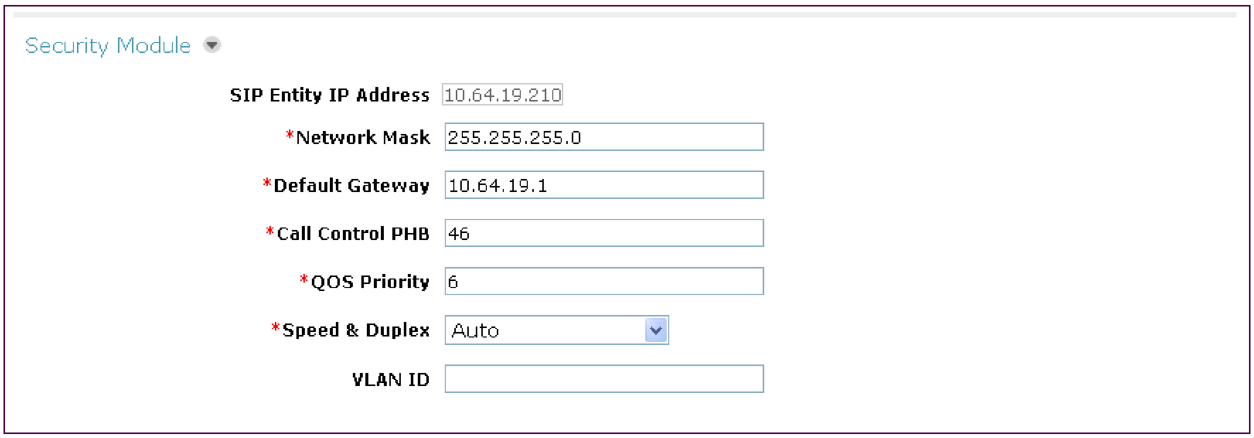
The screen below shows the Session Manager values used for the compliance test.



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.

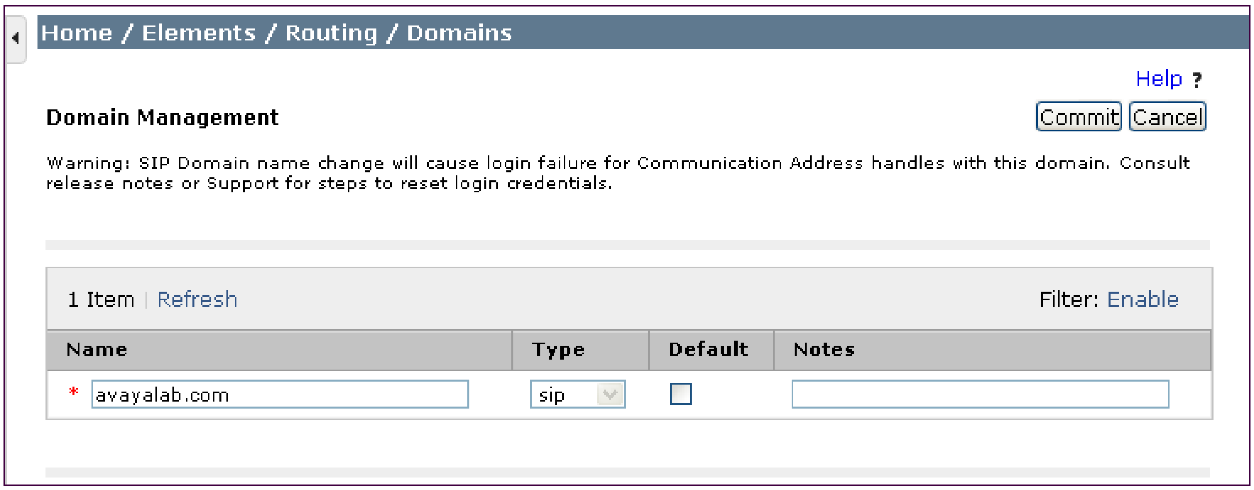


6.3. Specify SIP Domain

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.



6.4. Add Location

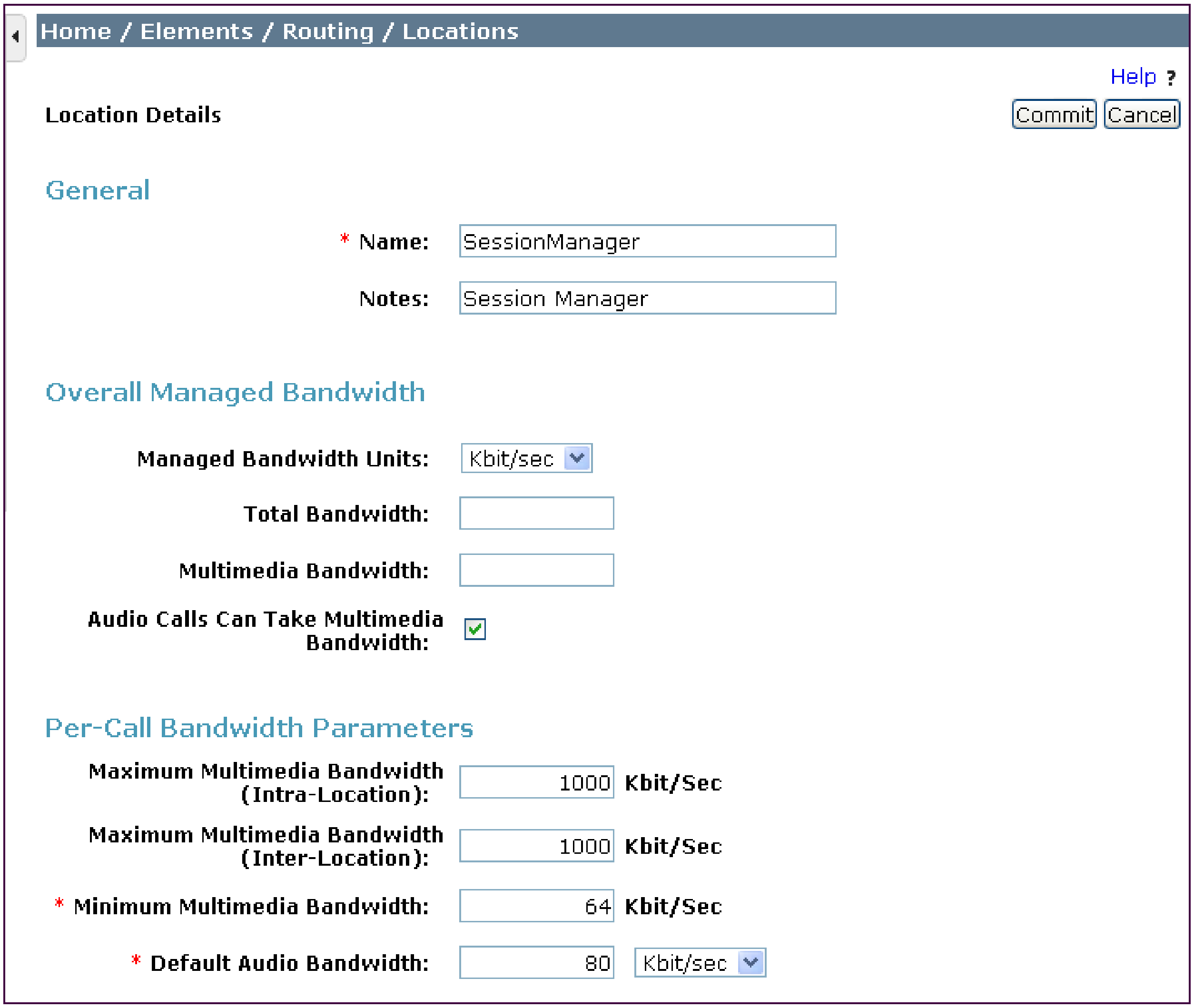
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

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).

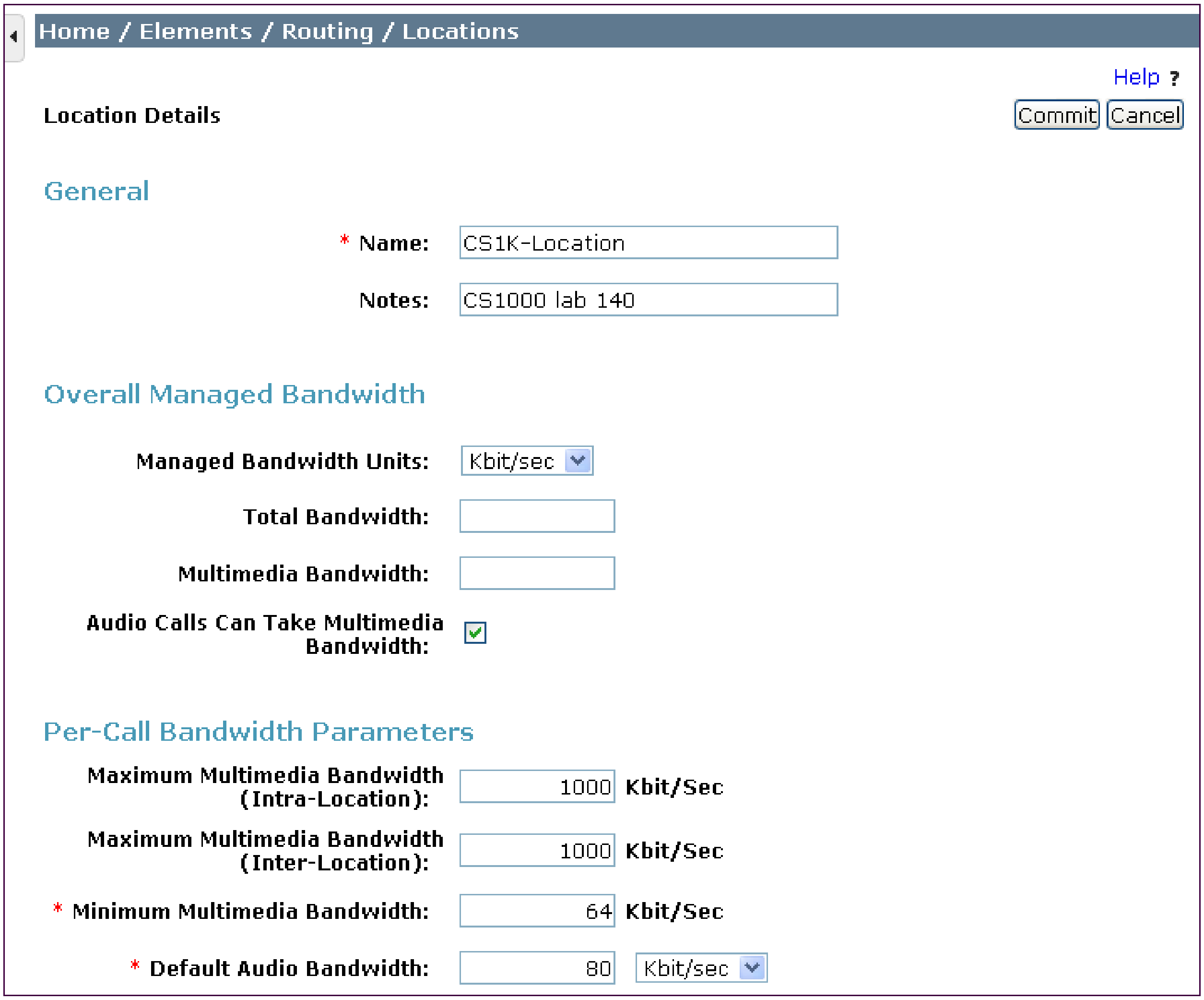
The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.6**), 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.

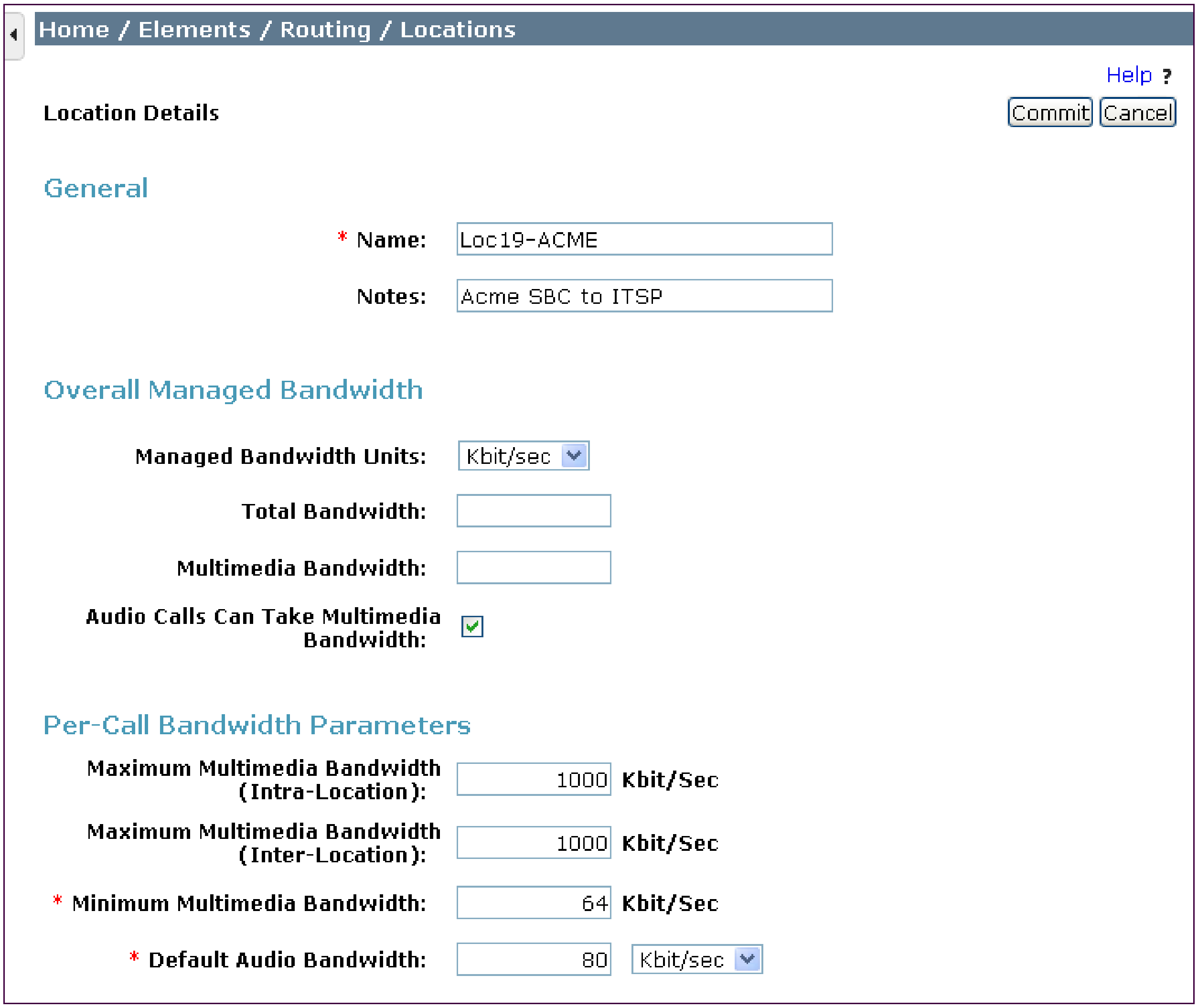


Note: Call bandwidth management parameters should be set per customer requirement.

Repeat the preceding procedure to create a separate Location for CS1000E and Acme Packet 3820. Displayed below is the screen for **CS1K-Location** used for CS1000E.



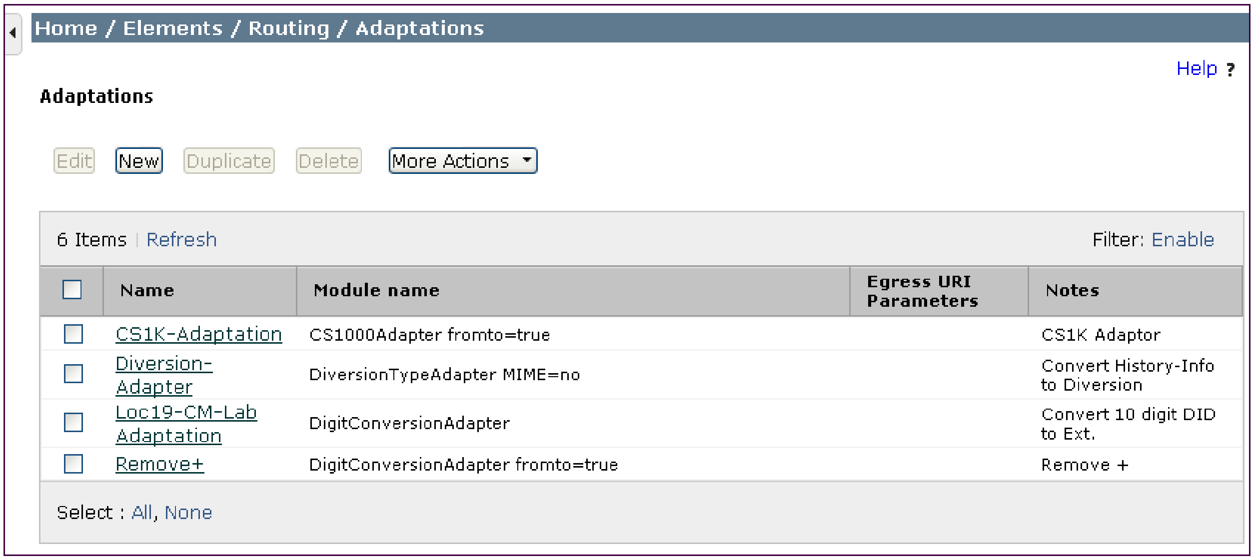
Below is the screen for **Loc19-ACME** used for Acme Packet 3820.



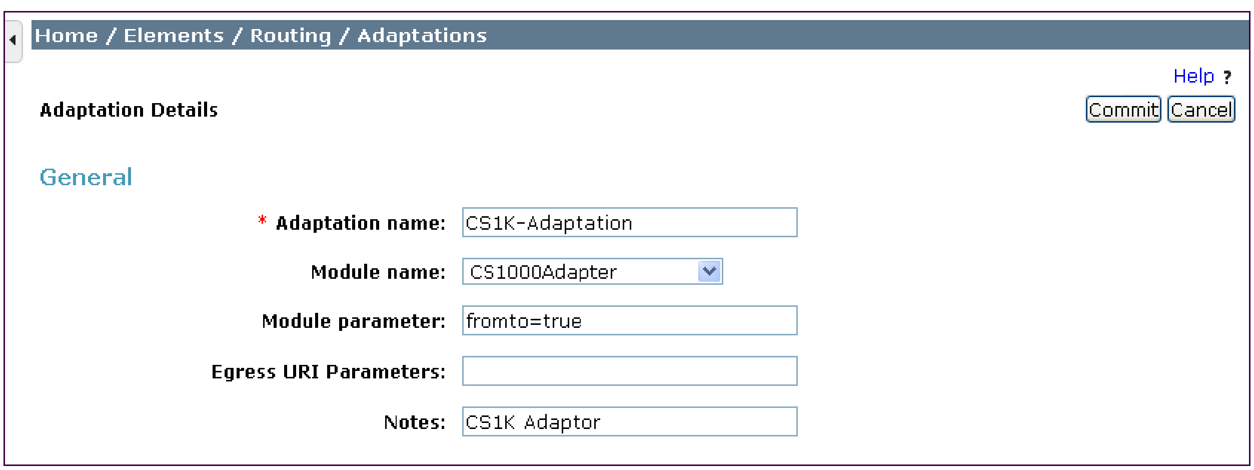
6.5. Adaptations

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.

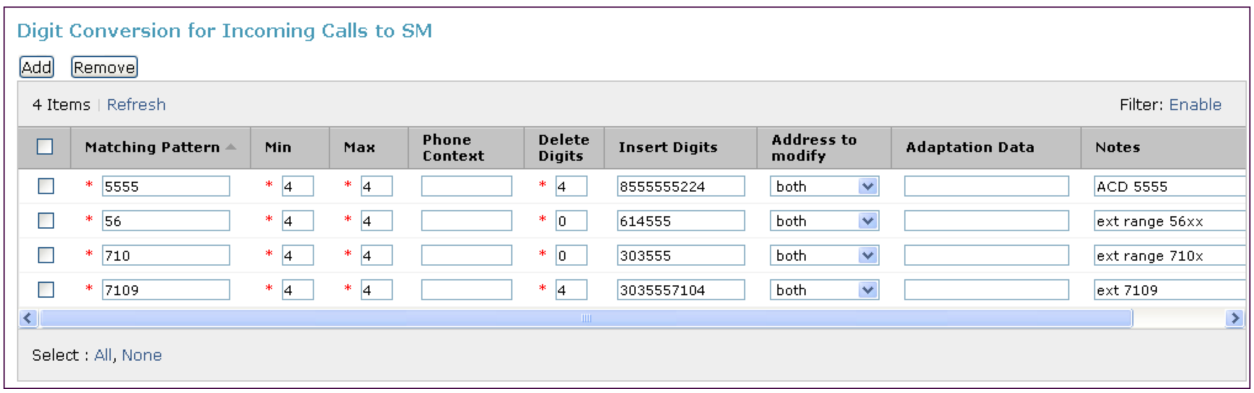


The adapter named **CS1K-Adaptation** will later be assigned to the SIP Entity linking Session Manager to CS1000E for calls involving CenturyLink SIP Trunking. This adaptation uses the **CS1000Adapter** to convert digits between CS1000E and CenturyLink. The **Module parameter fromto=true** will include 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 CenturyLink. The text below and the screen example that follows explain how to use Session Manager to convert between CS1000E directory numbers and the corresponding CenturyLink 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 CenturyLink DID, enter the number of digits in the extension to remove all digits.
- **Insert Digits:** Enter the CenturyLink 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

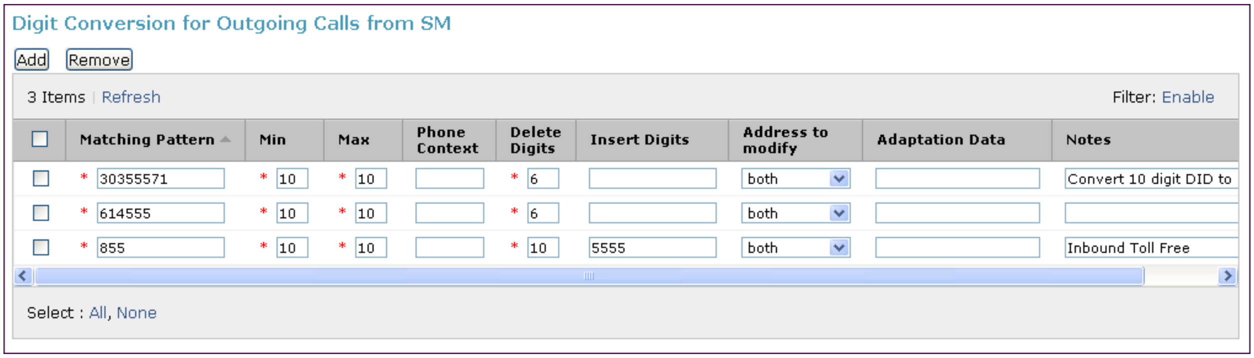
4 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	* 5555	* 4	* 4		* 4	8555555224	both		ACD 5555
	* 56	* 4	* 4		* 0	614555	both		ext range 56xx
	* 710	* 4	* 4		* 0	303555	both		ext range 710x
	* 7109	* 4	* 4		* 4	3035557104	both		ext 7109

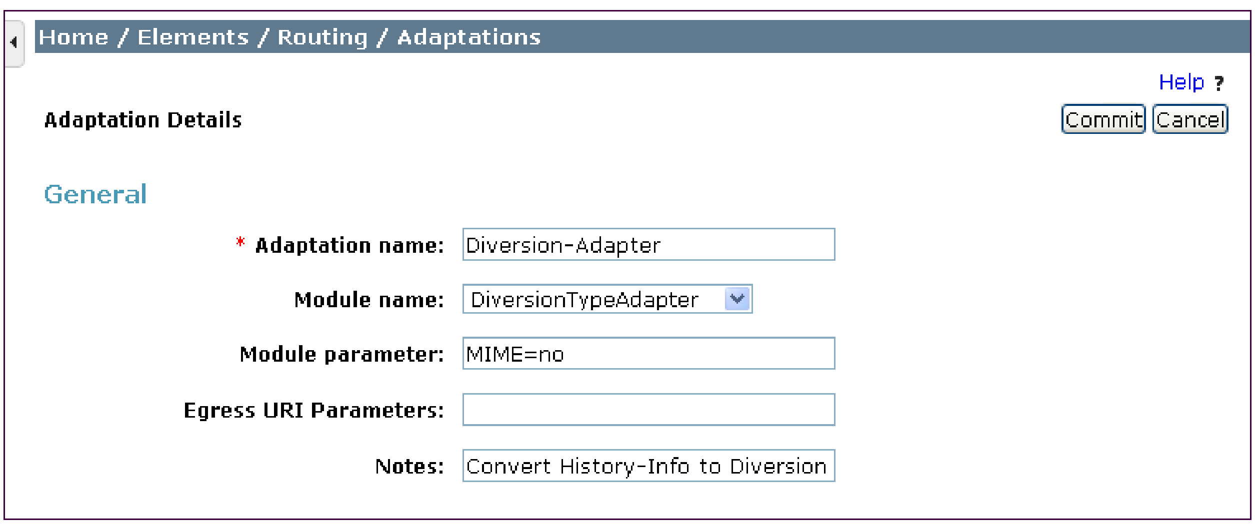
Select : All, None

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 CenturyLink.

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.



The adapter named **Diversion-Adapter** will later be assigned to the SIP Entity linking Session Manager to the Acme Packet 3820. This adaptation uses the **DiversionTypeAdapter** to convert History-Info headers to Diversion headers. This is necessary to support call forwarding of inbound calls back to the PSTN. Also, **MIME=no** was entered as a **Module Parameter** to have Session Manager strip MIME message bodies on egress to the Acme Packet 3820, such that only SDP is present in the message body.



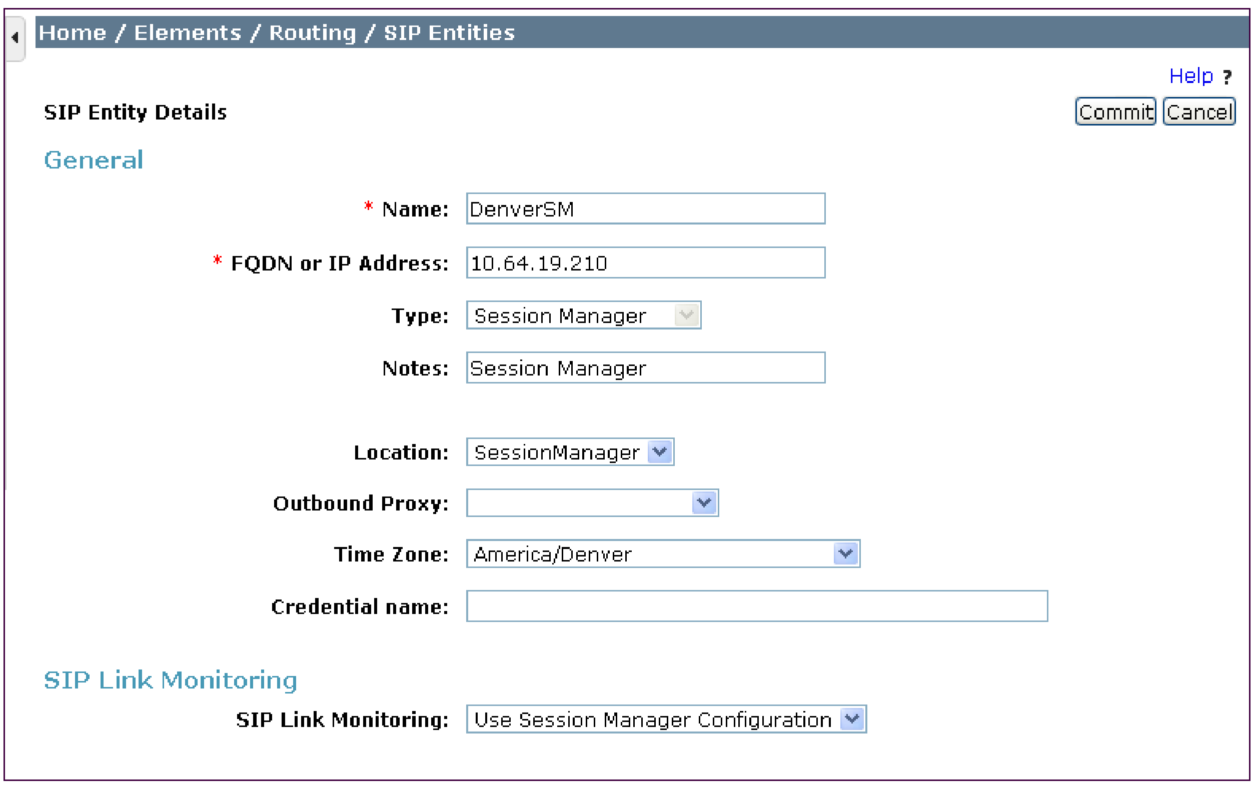
6.6. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes CS1000E and Acme Packet 3820. 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 Acme Packet 3820.
- **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**.



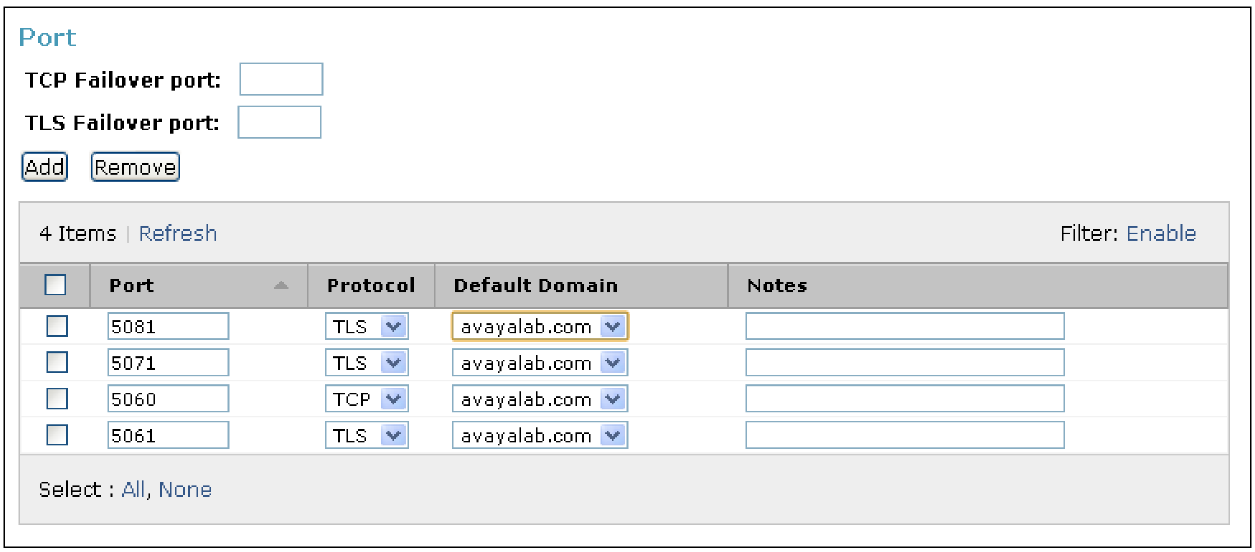
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from 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 6.7**.

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

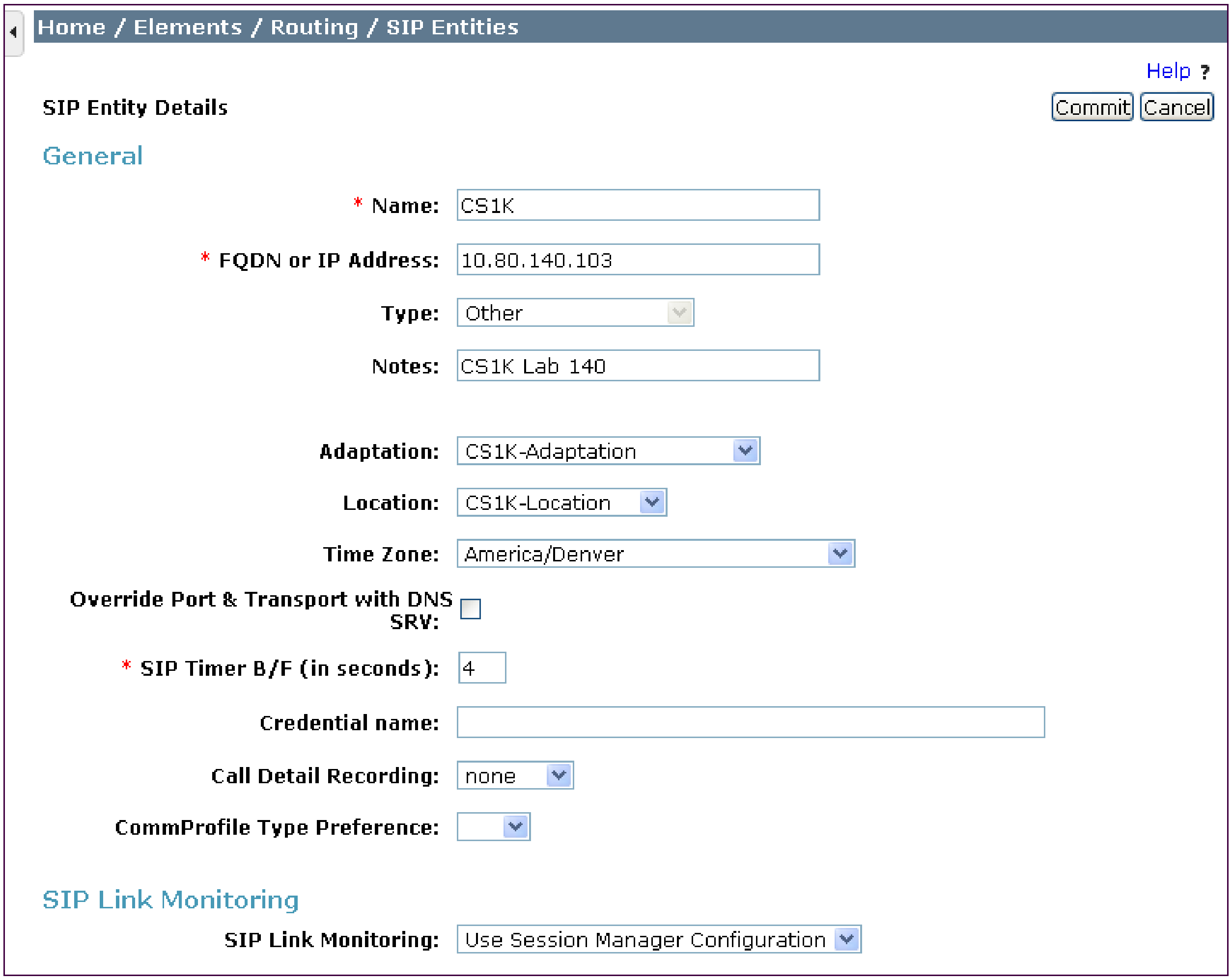
- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

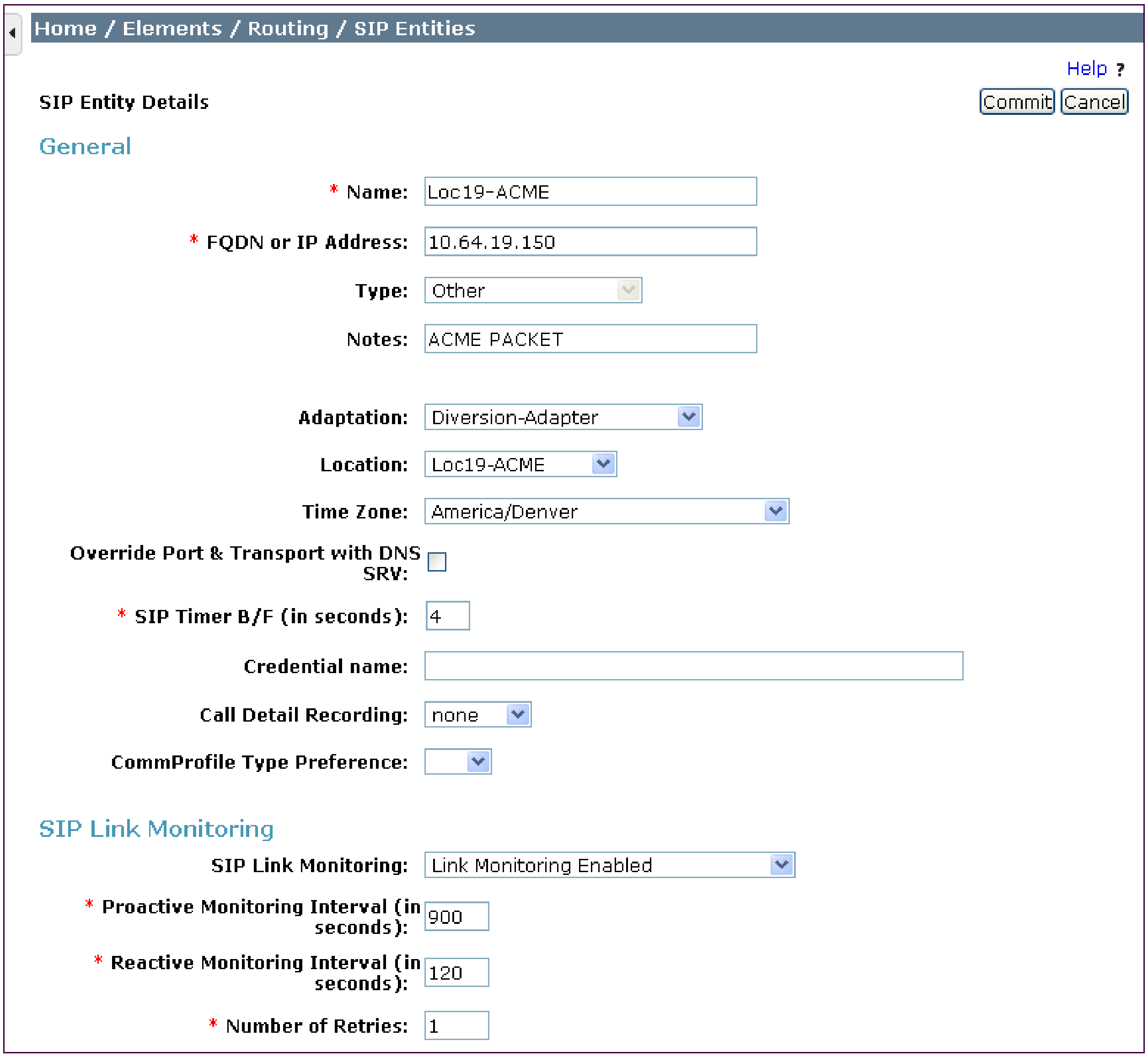
For the compliance test, four **Port** entries were added.



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 6.5** and the Location is set to the one defined for CS1000E in **Section 6.4**.



The following screen shows the addition of Acme Packet 3820 SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The **Adaptation** field is set to the **Diversion-Adapter** created in **Section 6.5** and the Location is set to the one defined for Acme Packet 3820 in **Section 6.4**. **Link Monitoring Enabled** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements.



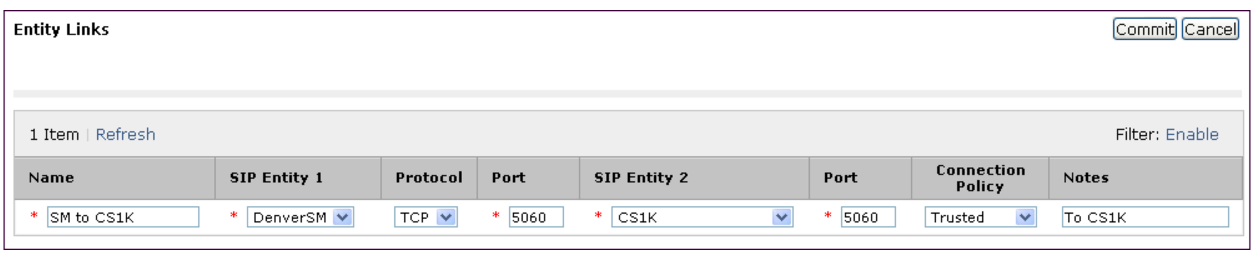
6.7. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to CS1000E for use only by service provider traffic and one to Acme Packet 3820. 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:

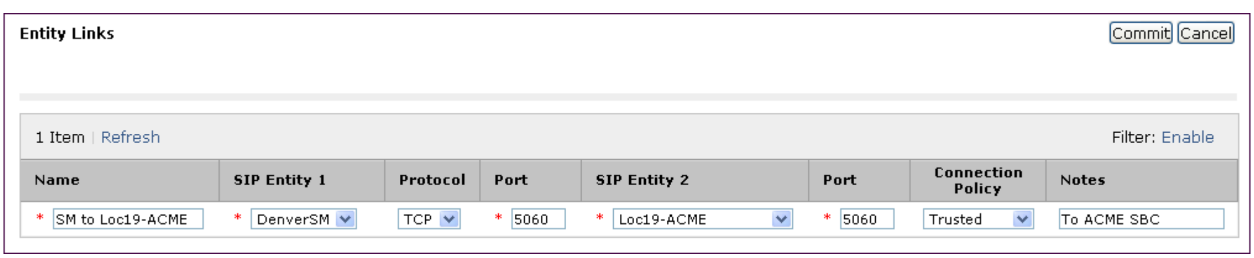
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system. For CS1000E, select the CS1000E SIP Entity defined in **Section 6.6**.
- **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 6.6** will be denied.

Click **Commit** to save. The following screens illustrate the Entity Links to CS1000E and Acme Packet 3820.

Entity Link to CS1000E:



Entity Link to Acme Packet 3820:



6.8. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.6**. Two routing policies must be added; one for CS1000E and one for

Acme Packet 3820. 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:

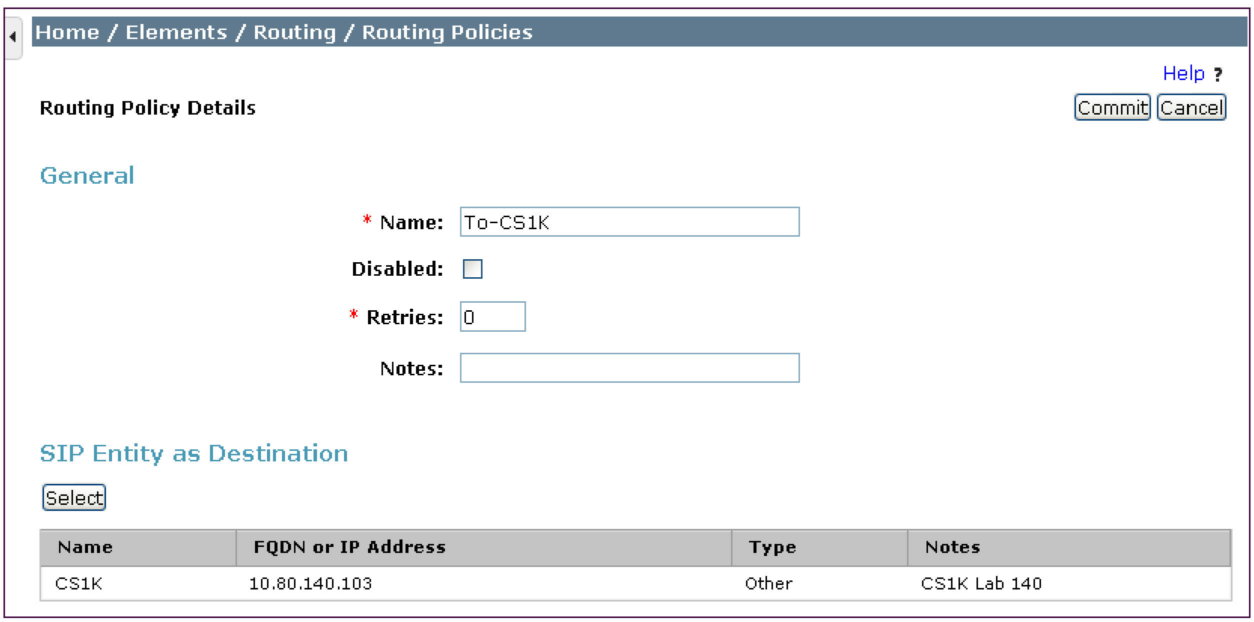
In the **General** section, enter the following values. Use default values for all remaining fields:

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

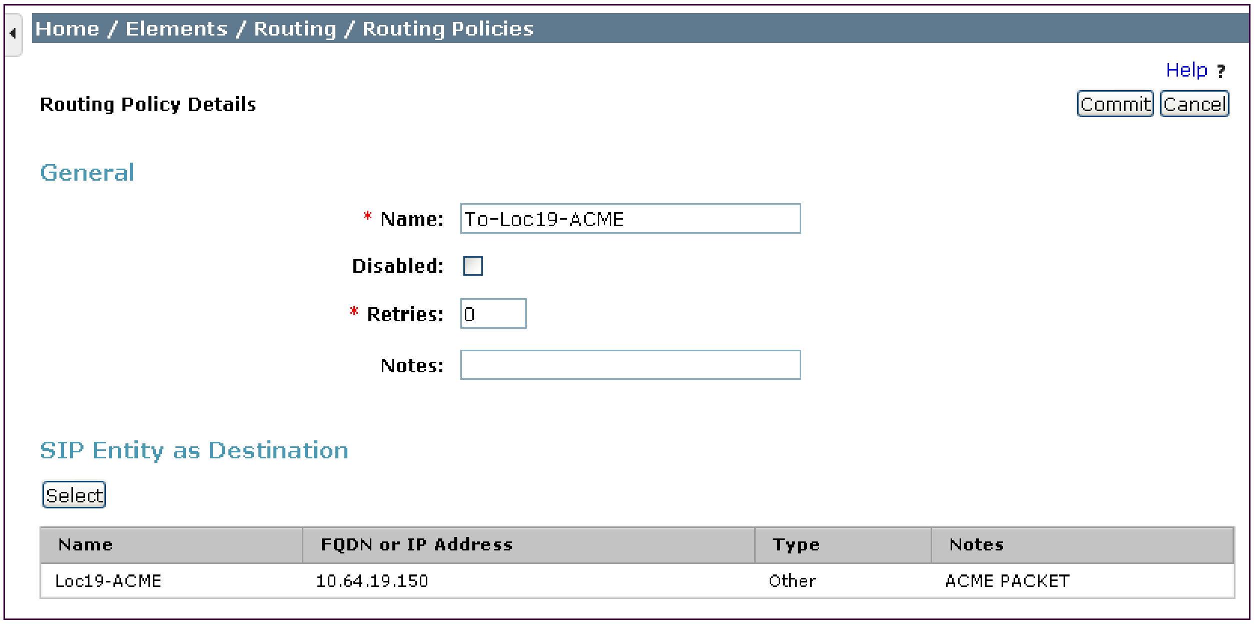
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select** (not shown)**.** The selected SIP Entity displays on the **Routing Policy Details** page as shown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

The following screens show the Routing Policies for CS1000E and Acme Packet 3820.

Routing Policy for CS1000E:



Routing Policy for Acme Packet 3820:



6.9. 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 CenturyLink and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

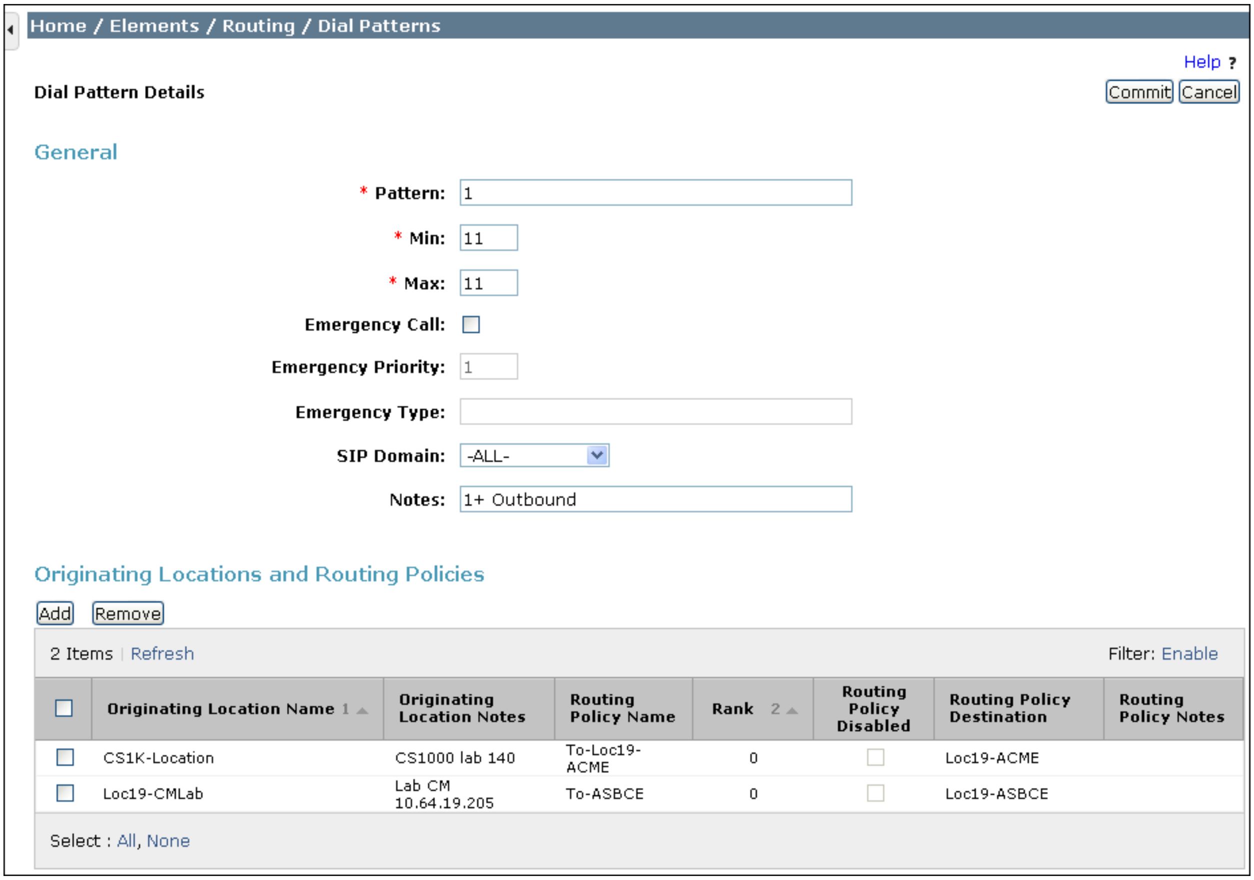
In the **General** section, enter the following values. Use default values for all remaining fields:

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

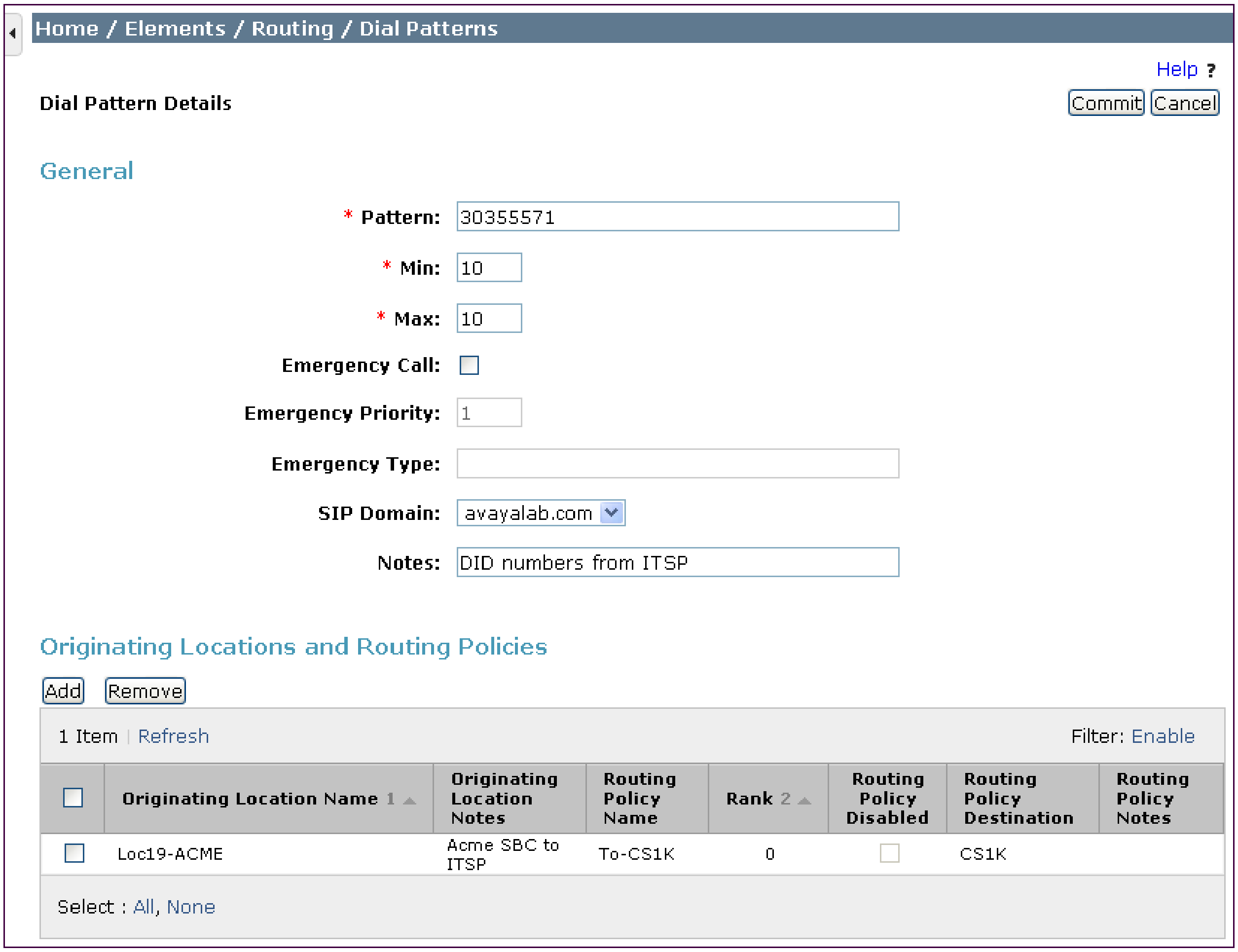
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

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-Loc19-ACME**.



The second example shows that a **10** digit number starting with **30355571** and originating from **Loc19-ACME** uses route policy **To-CS1K**. This is a DID range 303-555-7100 through 303-555-7199 assigned to the enterprise from CenturyLink.

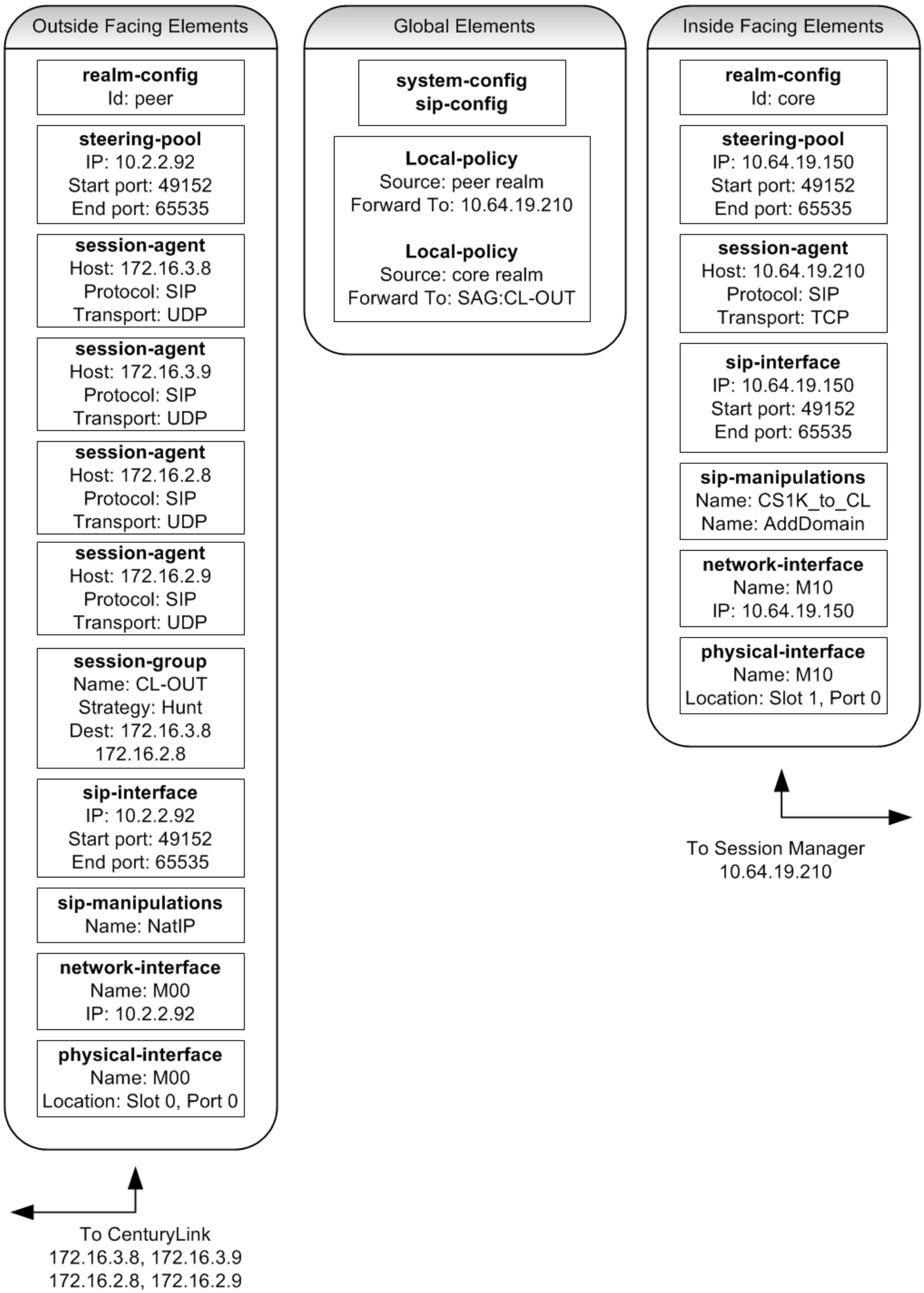


7. Configure Acme Packet 3820 Net-Net® Session Director

This section describes the configuration of the Acme Packet 3820 necessary for interoperability with CenturyLink and Session Manager. The Acme Packet 3820 is configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet 3820.

A pictorial view of this configuration is shown below. It shows the internal components needed for the compliance test. Each of these components is defined in the Acme Packet 3820 configuration file contained in **Appendix A**. However, this section does not cover standard Acme Packet 3820 configurations that are not directly related to the interoperability test. The details of these configuration elements can be found in **Appendix A**.

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes and the direct connection to CenturyLink and Session Manager. These same fields are highlighted in **Appendix A**. The remaining fields are generally the default/standard value used by the Acme Packet 3820 for that field. For additional details on the administration of the Acme Packet 3820, see **Reference [12]**.


Outside Facing Elements
realm-config
Id: peer
steering-pool
IP: 10.2.2.92
Start port: 49152
End port: 65535
session-agent
Host: 172.16.3.8
Protocol: SIP
Transport: UDP
session-agent
Host: 172.16.3.9
Protocol: SIP
Transport: UDP
session-agent
Host: 172.16.2.8
Protocol: SIP
Transport: UDP
session-agent
Host: 172.16.2.9
Protocol: SIP
Transport: UDP
session-group
Name: CL-OUT
Strategy: Hunt
Dest: 172.16.3.8
172.16.2.8
sip-interface
IP: 10.2.2.92
Start port: 49152
End port: 65535
sip-manipulations
Name: NatIP
network-interface
Name: M00
IP: 10.2.2.92
physical-interface
Name: M00
Location: Slot 0, Port 0
To CenturyLink
172.16.3.8, 172.16.3.9
172.16.2.8, 172.16.2.9
Global Elements
system-config
sip-config
Local-policy
Source: peer realm
Forward To: 10.64.19.210
Local-policy
Source: core realm
Forward To: SAG:CL-OUT
Inside Facing Elements
realm-config
Id: core
steering-pool
IP: 10.64.19.150
Start port: 49152
End port: 65535
session-agent
Host: 10.64.19.210
Protocol: SIP
Transport: TCP
sip-interface
IP: 10.64.19.150
Start port: 49152
End port: 65535
sip-manipulations
Name: CS1K_to_CL
Name: AddDomain
network-interface
Name: M10
IP: 10.64.19.150
physical-interface
Name: M10
Location: Slot 1, Port 0
To Session Manager
10.64.19.210

7.1. Acme Packet Command Line Interface Summary

The Acme Packet 3820 is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements.

1. Access the console port of the Acme Packet 3820 using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the 3820 for cable connection). Use the following settings for the serial port on the PC.
    - Bits per second: 115200
    - Data bits: 8
    - Parity : None
    - Stop bits: 1
    - Flow control: None

2. Log in to the Acme Packet 3820 with the user password.
3. Enable the Superuser mode by entering the **enable** command and then the superuser password. The command prompt will change to include a “#” instead of a “>” while in Superuser mode. This level of system access (i.e. at the “acmesystem#” prompt) will be referred to as the **main** level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific elements and specific parameters of those elements.
4. In Superuser mode, enter the **configure terminal** command. The **configure terminal** command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the **configuration** level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface**).
7. Enter the name of an element parameter followed by its value (e.g., **name M00**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat **Steps 5 - 9** to configure all the elements.
11. Enter **exit** to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration.

After accessing different levels of the ACLI to configure elements and parameters, it is necessary to return to the main level in order to run certain tasks such as saving the configuration, activating the configuration, and rebooting the system.

7.2. System Configuration

The system configuration defines system-wide parameters for the Acme Packet 3820.

The key system configuration (**system-config**) field is:

- **default-gateway**: The IP address of the default gateway for the management network (10.80.150.0/24) from **Figure 1**. In this case, the default gateway is **10.80.150.1**.

```
system-config
       hostname
       description
       location
       mib-system-contact
       mib-system-name

< text removed for brevity >

       call-trace                      disabled
       internal-trace                  disabled
       log-filter                      all
       default-gateway                 10.80.150.1
       restart                         enabled
       exceptions
       telnet-timeout                  0
       console-timeout                 0
       remote-control                  enabled
       cli-audit-trail                 enabled
       link-redundancy-state           disabled
       source-routing                  disabled
       cli-more                        disabled
       terminal-height                 24
       debug-timeout                   0
```

7.3. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface slot 0 / port 0 of the Acme Packet 3820 was connected to the external untrusted network. Ethernet slot 1 / port 0 was connected to the internal corporate LAN. A network interface was defined for each physical interface to assign it a routable IP address.

The key physical interface (**phy-interface**) fields are:

- **name**: A descriptive string used to reference the Ethernet interface.
- **operation-type**: Media indicates both signaling and media packets are sent on this interface.
- **slot / port**: The identifier of the specific Ethernet interface used.

```
phy-interface
        name                           M00
        operation-type                 Media
        port                           0
        slot                           0
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        overload-protection            disabled
        last-modified-by               admin@console
        last-modified-date             2011-11-01 09:59:56
phy-interface
        name                           M10
        operation-type                 Media
        port                           0
        slot                           1
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        overload-protection            disabled
        last-modified-by               admin@console
        last-modified-date             2011-11-01 10:00:38
```

The key network interface (**network-interface**) fields are:

- **name**: The name of the physical interface (defined previously) that is associated with this network interface.
- **description**: A descriptive name to help identify the interface.
- **ip-address**: The IP address on the interface connected to the network on which the CenturyLink SIP trunk service resides. In the compliance test, the IP address **10.2.2.92** was assigned to the public interface and **10.64.19.150** was assigned to the private interface.
- **netmask**: Subnet mask for the IP subnet.
- **gateway**: The subnet gateway address.
- **hip-ip-list**: The list of virtual IP addresses assigned to the Acme Packet 3820 on this interface. If a single virtual IP address is used, this value would be the same as the value entered for the **ip-address** field above.
- **icmp-address**: The list of IP addresses to which the Acme Packet 3820 will answer ICMP requests on this interface.

```
network-interface
       name                           M00
       sub-port-id                    0
       description                    PUBLIC
       hostname
       ip-address                     10.2.2.92
       pri-utility-addr
       sec-utility-addr
       netmask                        255.255.255.128
       gateway                        10.2.2.1
       sec-gateway
       gw-heartbeat
              state                          disabled
              heartbeat                      0
              retry-count                    0
              retry-timeout                  1
              health-score                   0
       dns-ip-primary
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                    11
       hip-ip-list                    10.2.2.92
       ftp-address
       icmp-address
       snmp-address
       telnet-address
       ssh-address
       last-modified-by               admin@10.80.150.38
       last-modified-date             2011-11-01 12:52:08
```

The settings for the private side network interface are shown below.

```
network-interface
       name                           M10
       sub-port-id                    0
       description                    PRIVATE
       hostname
       ip-address                     10.64.19.150
       pri-utility-addr
       sec-utility-addr
       netmask                        255.255.255.0
       gateway                        10.64.19.1
       sec-gateway
       gw-heartbeat
              state                          disabled
              heartbeat                      0
              retry-count                    0
              retry-timeout                  1
              health-score                   0
       dns-ip-primary
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                    11
       hip-ip-list                    10.64.19.150
       ftp-address
       icmp-address                   10.64.19.150
       snmp-address
       telnet-address
       ssh-address
       last-modified-by               admin@10.80.150.38
       last-modified-date             2011-11-01 12:16:22
```

7.4. Realm

A realm represents a group of related Acme Packet 3820 components. Two realms were defined for the compliance test. The **peer** realm was defined for the external network and the **core** realm was defined for the internal network.

The key realm (**realm-config**) fields are:

- **identifier**: A string used as a realm reference. This will be used in the configuration of other components.
- **network interfaces**: The network interfaces located in this realm.
- **In-manipulationid**: For the **core** realm **CS1K_To_CL** was used. This name refers to a set of sip-manipulations that is performed on inbound traffic to the Acme Packet 3820.
- **out-manipulationid**: For the **peer** realm **NatIP** was used and for the **core** realm **AddDomain** was used. These names refer to a set of sip-manipulations (defined in **Section 7.9**) that are performed on outbound traffic from the Acme Packet 3820. These sip-manipulations are specified in each realm. Thus, these sip-manipulations are applied to outbound traffic from the public side (**peer**) of the Acme Packet 3820 as well as to outbound traffic from the private side (**core**) of the Acme Packet 3820.

```
realm-config
        identifier                      peer
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M00:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled

< text removed for brevity >

        out-translationid
        in-manipulationid
        out-manipulationid              NatIP
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0

< text removed for brevity >

realm-config
        identifier                      core
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M10:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled

< text removed for brevity >

        out-translationid
        in-manipulationid               CS1K_To_CL
        out-manipulationid              AddDomain
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0

< text removed for brevity >
```

7.5. SIP Configuration

The SIP configuration (**sip-config**) defines the global system-wide SIP parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

The key SIP configuration (**sip-config**) fields are:

- **state: enabled**
- **home-realm-id**: The name of the realm on the private side of the Acme Packet 3820.
- **egress-realm-id**: The name of the realm on the private side of the Acme Packet 3820.
- **options**: **max-udp=length=0**. This option was used to prevent errors about the packet size being too large.

```
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  core
        egress-realm-id                core
        nat-mode                       None
        registrar-domain
        registrar-host
        registrar-port                 0
        register-service-route         always
        init-timer                     500
        max-timer                      4000
        trans-expire                   32
        invite-expire                  180

< text removed for brevity >

        options                        max-udp-length=0
        refer-src-routing              disabled
        add-ucid-header                disabled
        proxy-sub-events

< text removed for brevity >
```

7.6. SIP Interface

The SIP interface (**sip-interface**) defines the receiving characteristics of the SIP interfaces on the Acme Packet 3820. Two SIP interfaces were defined; one for each realm.

The key SIP interface (**sip-interface**) fields are:

- **realm-id**: The name of the realm to which this interface is assigned.
- **sipport**
  - **address**: The IP address assigned to this sip-interface.
  - **port**: The port assigned to this sip-interface. Port 5060 is used for both UDP and TCP.
  - **transport-protocol**: The transport method used for this interface.
  - **allow-anonymous**: Defines from whom SIP requests will be allowed. On the peer side, the value of **agents-only** is used. Thus, SIP requests will only be accepted from session agents (as defined in **Section 7.7**) on this interface. On the core side, the value of **all** is used. Thus, SIP requests will be accepted from anyone on this interface.

```
sip-interface
      state                             enabled
      realm-id                          peer
      description
      sip-port
            address                           10.2.2.92
            port                              5060
            transport-protocol                UDP
            tls-profile
            allow-anonymous                   agents-only
            ims-aka-profile
      carriers
      trans-expire                      0
      invite-expire                     0

< text removed for brevity >

sip-interface
      state                             enabled
      realm-id                          core
      description
      sip-port
            address                           10.64.19.150
            port                              5060
            transport-protocol                TCP
            tls-profile
            allow-anonymous                   all
            ims-aka-profile
      carriers
      trans-expire                      0
      invite-expire                     0

< text removed for brevity >
```

7.7. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet 3820 such as Session Manager and CenturyLink SIP Trunk service.

The key session agent (**session-agent**) fields are:

- **hostname**: Fully qualified domain name or IP address of this SIP peer.
- **ip-address**: The IP address of this SIP peer.
- **port**: The port used by the peer for SIP traffic.
- **app-protocol**: **SIP**
- **transport-method**: UDP
- **realm-id**: The realm id where this peer resides.
- **description**: A descriptive name for the peer.
- **ping-method**: **OPTIONS;hops=70** This setting defines that the SIP OPTIONS message will be sent to the peer to verify that the SIP connection is functional. In addition, this parameter causes the Acme Packet 3820 to set the SIP "Max-Forward" field to 70 in outbound SIP OPTIONS pings generated by the Acme Packet 3820 to this session agent.
- **ping-interval**: Specifies the interval (in seconds) between each ping attempt.

The settings for the session agent used for CenturyLink East Inbound/Outbound peer:

```
session-agent
       hostname                         172.16.3.8
       ip-address                       172.16.3.8
       port                             5060
       state                            enabled
       app-protocol                     SIP
       app-type
       transport-method                 UDP
       realm-id                         peer
       egress-realm-id
       description
       carriers
       allow-next-hop-lp                enabled
       constraints                      disabled
       max-sessions                     0

< text removed for brevity >

       response-map
       ping-method                      OPTIONS;hops=70
       ping-interval                    60

< text removed for brevity >
```

The settings for the session agent used for CenturyLink East Remote DID peer:

```
session-agent
       hostname                         172.16.3.9
       ip-address                       172.16.3.9
       port                             5060
       state                            enabled
       app-protocol                     SIP
       app-type
       transport-method                 UDP
       realm-id                         peer
       egress-realm-id
       description
       carriers
       allow-next-hop-lp                enabled
       constraints                      disabled
       max-sessions                     0

< text removed for brevity >

       response-map
       ping-method                      OPTIONS;hops=70
       ping-interval                    60

< text removed for brevity >
```

The settings for the session agent used for CenturyLink West Inbound/Outbound peer:

```
session-agent
       hostname                         172.16.2.8
       ip-address                       172.16.2.8
       port                             5060
       state                            enabled
       app-protocol                     SIP
       app-type
       transport-method                 UDP
       realm-id                         peer
       egress-realm-id
       description
       carriers
       allow-next-hop-lp                enabled
       constraints                      disabled
       max-sessions                     0

< text removed for brevity >

       response-map
       ping-method                      OPTIONS;hops=70
       ping-interval                    60

< text removed for brevity >
```

The settings for the session agent used for CenturyLink West Remote DID peer:

```
session-agent
        hostname                        172.16.2.9
        ip-address                      172.16.2.9
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0

< text removed for brevity >

        response-map
        ping-method                     OPTIONS;hops=70
        ping-interval                   60

< text removed for brevity >
```

The settings for the session agent used for Session Manager:

```
session-agent
        hostname                        10.64.19.210
        ip-address                      10.64.19.210
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                TCP
        realm-id                        core
        egress-realm-id
        description
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0

< text removed for brevity >

        response-map
        ping-method                     OPTIONS;hops=70
        ping-interval                   60

< text removed for brevity >
```

7.8. Session Agent Group

Session agents can be configured in a session agent group (SAG), so multiple session agents can be assigned to a route policy for fail-over or load balancing purposes. For compliance testing CenturyLink had four session agents assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound traffic. Only the two session agents allocated for outbound traffic were added to the SAG.

The key session agent group (**session-group**) fields are:

- **group-name**: A descriptive string used to reference the session agent group.
- **state**: **enabled**
- **app-protocol**: **SIP**
- **strategy**: **Hunt** This strategy will route to the secondary session agent only if the primary fails. An alternative is to use a strategy of **RoundRobin**. This strategy will alternatively select between session agents.
- **dest**: The list of session agents to be added to the group by hostname. For compliance testing **172.16.3.8** and **172.16.2.8** were used.
- **sag-recursion**: **enabled** This allows Acme Packet 3820 to select a different session agent in the SAG if a failure occurs to the first session agent.

```
session-group
        group-name                     CL-OUT
        description
        state                          enabled
        app-protocol                   SIP
        strategy                       Hunt
        dest
                                       172.16.3.8
                                       172.16.2.8
        trunk-group
        sag-recursion                  enabled
        stop-sag-recurse               401,407
        last-modified-by               admin@10.80.150.38
        last-modified-date             2012-06-18 10:27:19
```

7.9. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. In **Section 7.4**, it was defined that the set of sip-manipulations named **NatIP** would be performed on outbound traffic in the **peer** realm and **AddDomain** would be performed on outbound traffic in the **core** realm. The sip-manipulation named **CS1K_To_CL** would be performed on inbound traffic in the **core** realm. For the complete configuration of these rules refer to **Appendix A**.

The key SIP manipulation (sip-manipulation) fields are:

- **name**: The name of this set of SIP header rules.
- **header-rule**
  - **name**: The name of this individual header rule.
  - **header-name**: The SIP header to be modified.
  - **action**: The action to be performed on the header.
  - **comparison-type**: The type of comparison performed when determining a match.
  - **msg-type**: The type of message to which this rule applies.
  - **element-rule**
    - **name**: The name of this individual element rule.
    - **type**: Defines the particular element in the header to be modified.
    - **action**: The action to be performed on the element.
    - **match-val-type**: Element matching criteria on the data type (if any) in order to perform the defined action.
    - **comparison-type**: The type of comparison performed when determining a match.
    - **match-value**: Element matching criteria on the data value (if any) in order to perform the defined action.
    - **new-value**: New value for the element (if any).

In the configuration file in **Appendix A**, the **NatIP** sip manipulation has many modifications (or header-rules) defined. These header manipulations were added to hide the private IP address and enterprise domain name which appear in the “To”, “From”, “Request-URI”, “Diversion” and “PAI” SIP headers for outbound calls. As well as remove unwanted headers going to the SIP service provider.

Similarly the **AddDomain** sip manipulation was used towards Session Manager to hide the public IP addresses and to add the enterprise domain to the “From” and “PAI” SIP headers.

The **CS1K_To_CL** sip manipulation was used to add a “Diversion” header for Mobile X calls from CS1000E. This was added to the inbound traffic to the Acme Packet 3820 so that it could be further modified by the **NatIP** sip manipulation to remove the “History-Info” header and to hide the enterprise domain name.

The example below shows the **natFROM header-rule** in the **NatIP** sip manipulation. It specifies that the "From" header in SIP request messages will be manipulated based on the element rule defined. The element rule **natHost** will match any value in the host part of the URI and replace it with the value of **$LOCAL_IP**. The value of **$LOCAL_IP** is the outside IP address of the Acme Packet 3820.

```
sip-manipulation
        name                                    NatIP
        description
        split-headers
        join-headers
        header-rule
                name                                    natFROM
                header-name                             From
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value
                element-rule
                        name                                    natHost
                        parameter-name
                        type                                    uri-host
                        action                                  replace
                        match-val-type                          any
                        comparison-type                         case-sensitive
                        match-value
                        new-value                               $LOCAL_IP

< text removed for brevity >
```

The example below shows the **FromDomain header-rule** in the **AddDomain** sip manipulation. It specifies that the "From" header in SIP request messages will be manipulated based on the element rule defined. The element rule **From** will match any value in the host part of the URI and replace it with the value of **avayalab.com**. The value of **avayalab.com** is the domain name used in the enterprise. This value should match the Domain set in Session Manager (**Section 6.2**) and the CS1000E signaling group Far-end Domain (**Section 5.7**).

```
sip-manipulation
        name                                 AddDomain
        description
        split-headers
        join-headers
        header-rule
                name                                 FromDomain
                header-name                          From
                action                               manipulate
                comparison-type                      case-sensitive
                msg-type                             request
                methods
                match-value
                new-value
                element-rule
                        name                                 From
                        parameter-name
                        type                                 uri-host
                        action                               replace
                        match-val-type                       any
                        comparison-type                      case-sensitive
                        match-value
                        new-value                            avayalab.com

< text removed for brevity >
```

The example below shows the **CS1K_To_CL** sip manipulation. This manipulation specifies that if the P-Asserted-Identity header does not have a phone number within the range 303-555-7100 to 303-5557199 (the DID range specified by CenturyLink) and does not have a Reason parameter in the "History-Info" header, a static Diversion header will be created.

```
sip-manipulation
        name                          CS1K_To_CL
        description
        split-headers
        join-headers
        header-rule
                name                          PAIRegex
                header-name                   P-Asserted-Identity
                action                        store
                comparison-type               pattern-rule
                msg-type                      any
                methods                       INVITE
                match-value
                new-value
                element-rule
                        name                          chkUser
                        parameter-name
                        type                          header-value
                        action                        store
                        match-val-type                any
                        comparison-type               pattern-rule
                        match-value                   (.*)(30355571)(.*)
                        new-value
        header-rule
                name                          HistRegex
                header-name                   History-Info
                action                        store
                comparison-type               pattern-rule
                msg-type                      any
                methods
                match-value
                new-value
                element-rule
                        name                          GetReason
                        parameter-name
                        type                          header-value
                        action                        store
                        match-val-type                any
                        comparison-type               pattern-rule
                        match-value                   (.*)(reason)(.*)
                        new-value
        header-rule
                name                          AddDiversion
                header-name                   Diversion
                action                        add
                comparison-type               boolean
                msg-type                      request
                methods                       INVITE
                match-value                   (!$PAIRegex[0].$chkUser)&!$HistRegex[0].$GetReason
                new-value                     "<sip:3035557104@avayalab.com;user=phone>"
```

7.10. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools were defined; one for each realm.

The key steering pool (**steering-pool**) fields are:

- **ip-address**: The address of the interface on the Acme Packet 3820.
- **start-port**: An even number of the port that begins the range.
- **end-port**: An odd number of the port that ends the range.
- **realm-id**: The realm to which this steering pool is assigned

```
steering-pool
       ip-address                      10.2.2.92
       start-port                      49152
       end-port                        65535
       realm-id                        peer
       network-interface
       last-modified-by                admin@console
       last-modified-date              2012-06-06 15:07:34
steering-pool
       ip-address                      10.64.19.150
       start-port                      49152
       end-port                        65535
       realm-id                        core
       network-interface
       last-modified-by                admin@console
       last-modified-date              2012-06-06 15:08:02
```

7.11. Local Policy

Local policy controls the routing of SIP calls from one realm to another.

The key local policy (**local-policy**) fields are:

- **from-address**: A policy filter indicating the originating IP address to which this policy applies. An asterisk (*) indicates any IP address.
- **to-address**: A policy filter indicating the terminating IP address to which this policy applies. An asterisk (*) indicates any IP address.
- **source-realm**: A policy filter indicating the matching realm in order for the policy rules to be applied.
- **policy-attribute**:
    - **next-hop**: The IP address where the message should be sent when the policy rules match.
    - **realm**: The realm associated with the next-hop IP address.

In this case, the first policy provides a simple routing rule indicating that messages originating from the **peer** realm are to be sent to the **core** realm via IP address **10.80.150.206** (Session Manager at the enterprise). The second policy indicates that messages originating from the **core** realm are to be sent to the **peer** realm via the session agent group **CL-OUT** created in **Section 7.8**.

```
local-policy
      from-address
                                        *
      to-address
                                        *
      source-realm
                                        peer
      description
      activate-time                     N/A

< text removed for brevity >

      policy-attribute
            next-hop                          10.64.19.210
            realm                             core
            action                            none

< text removed for brevity >

local-policy
      from-address
                                        *
      to-address
                                        *
      source-realm
                                        core
      description
      activate-time                     N/A

< text removed for brevity >

      policy-attribute
            next-hop                          SAG:CL-OUT
            realm                             peer

< text removed for brevity >
```

8. CenturyLink SIP Trunk Service Configuration

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

9. Verification

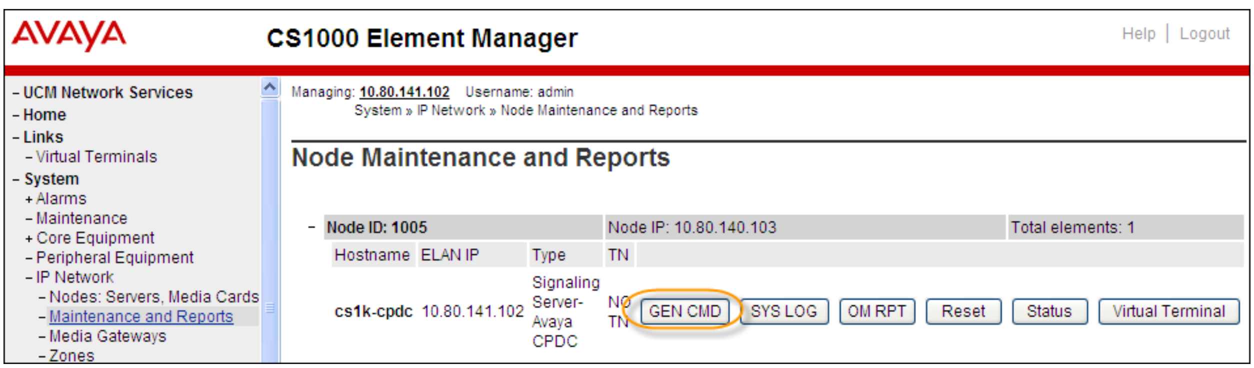
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

9.1. Avaya Communication Server 1000E Verifications

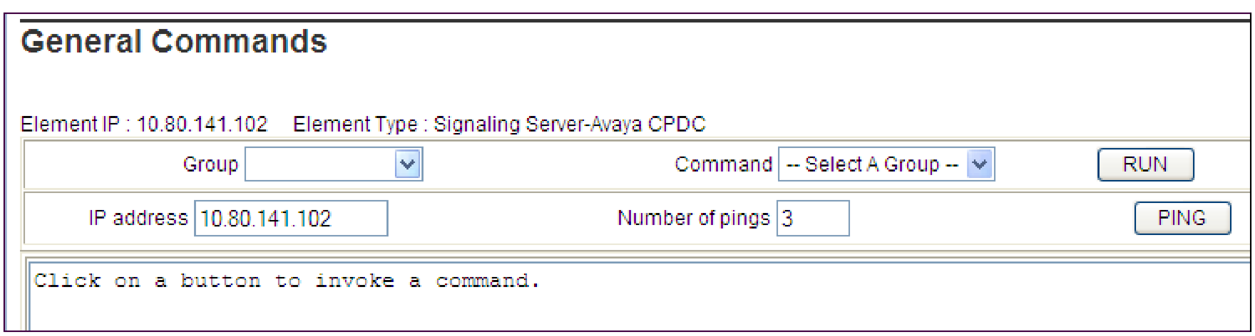
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

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.

General Commands

Element IP : 10.80.141.102 Element Type : Signaling Server-Avaya CPDC

Group: Sip | Command: SIPGwShow | Sip | RUN

IP address: 10.80.141.102 | Number of pings: 3 | PING

```
SIPNPM Status                 : Active
Primary   Proxy IP address    : 10.64.19.150
Primary   Proxy port          : 5060
Primary   Proxy Transport     : TCP
Secondary Proxy IP address    : 0.0.0.0
Secondary Proxy port          : 5060
Secondary Proxy Transport     : TCP
Primary Proxy2 IP address     : 10.64.19.250
Primary Proxy2 port           : 5060
Primary Proxy2 Transport      : TCP
Active    Proxy               : Primary  :Register Not Supported
Time To Next Registration     : 0 Seconds
Channels Busy / Idle / Total  : 0 / 32 / 32
Stack version                     : 5.5.0.13
TLS Security Policy           : Security Disabled
```

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

General Commands

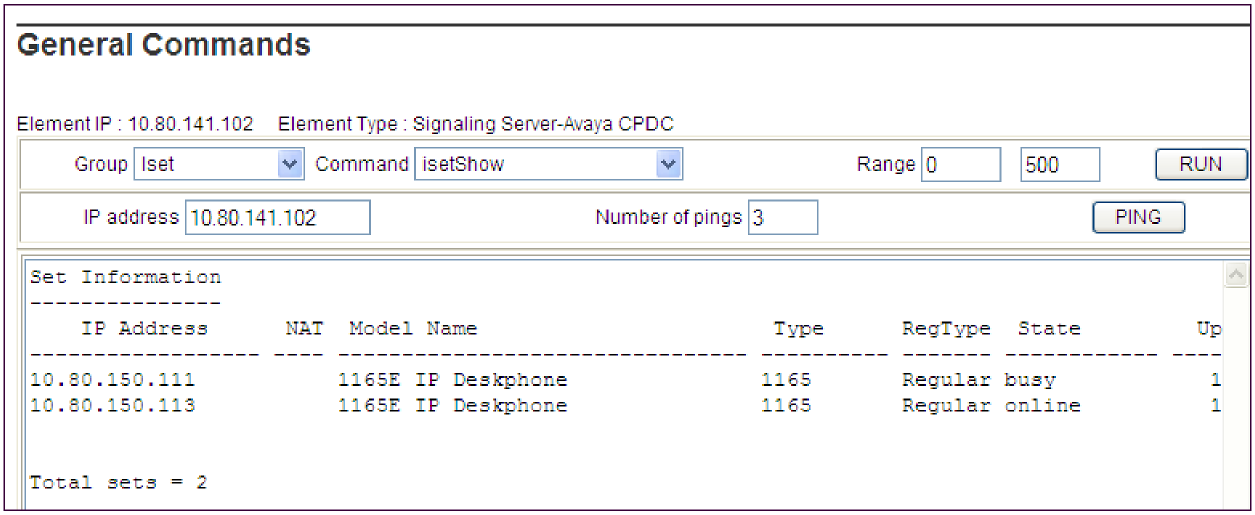
Element IP : 10.80.141.102 Element Type : Signaling Server-Avaya CPDC

Group: SipLine | Command: slgSetShowAll | RUN

IP address: 10.80.141.102 | Number of pings: 3 | PING

```
UserID          AuthId      TN              Clients  Calls  SetHandle  Pos ID   SIPL Type
--------------- ----------  --------------- -------  -----  ---------  -------  ---------
--------------- IPV4 Endpoints   --------------------------
          7108        7108     252-00-09-01        1      1  0x8d155f8          SIP Lines
          5685        5685     252-00-09-02        1      0  0xb7e16e58          SIP Lines
Total User Registered = 2   V4 Registered = 2  V6 Registered = 0
```

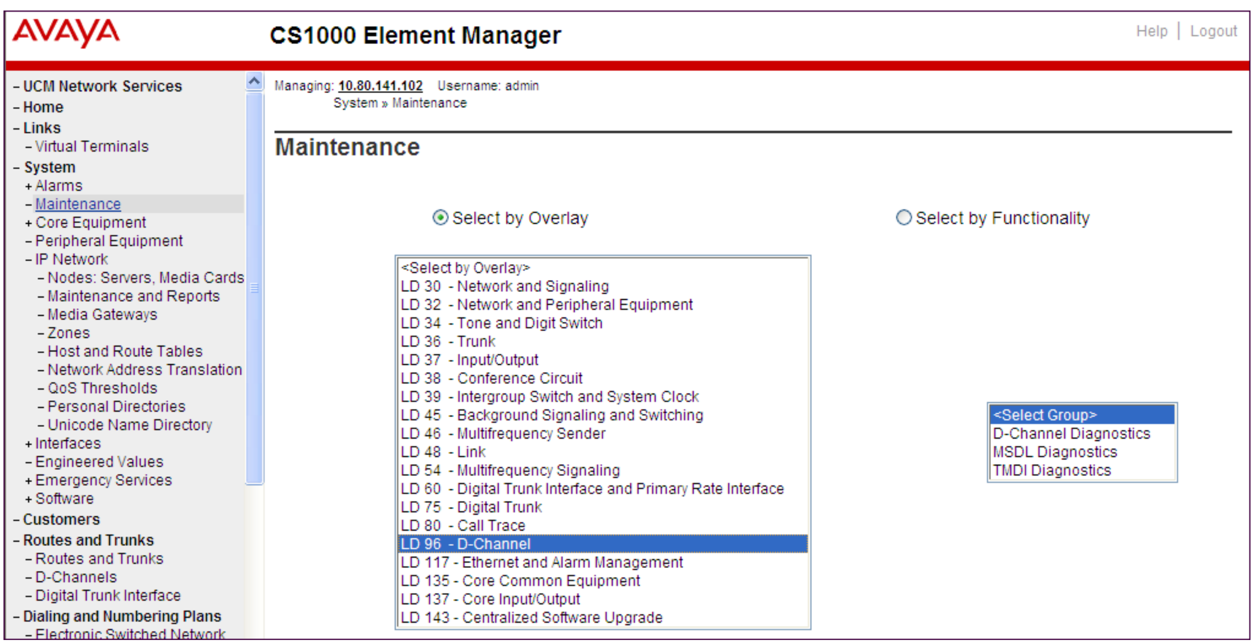
The following screen shows a means to view IP UNIStim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**. At the time this screen was captured, the UNIStim telephone with IP address **10.80.150.111** was involved in an active call with the CenturyLink SIP Trunk service.



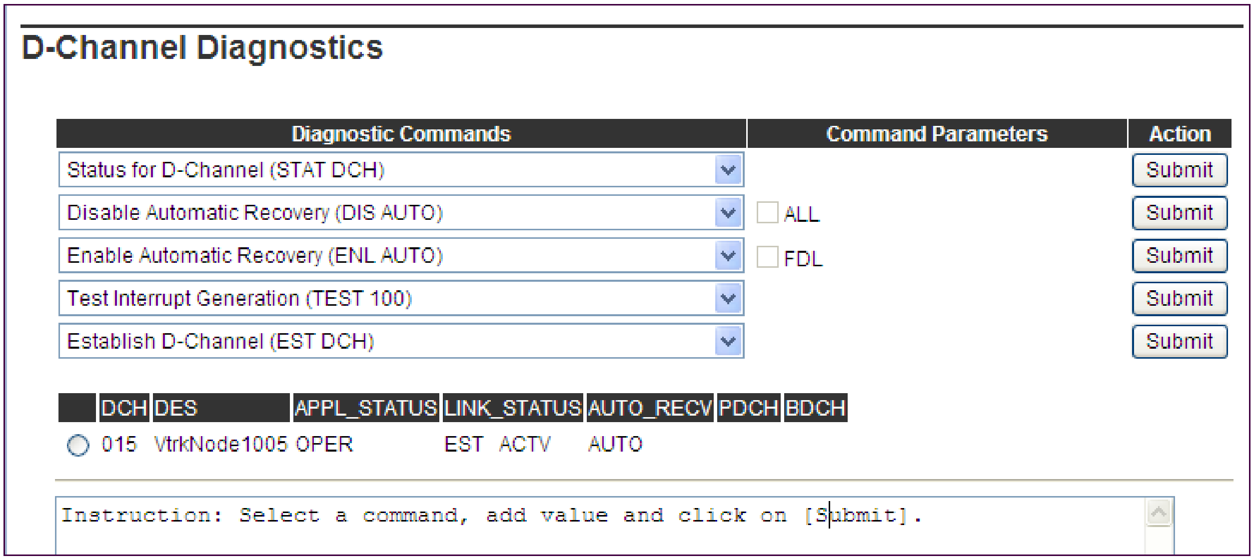
9.1.2. System Maintenance Commands

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.



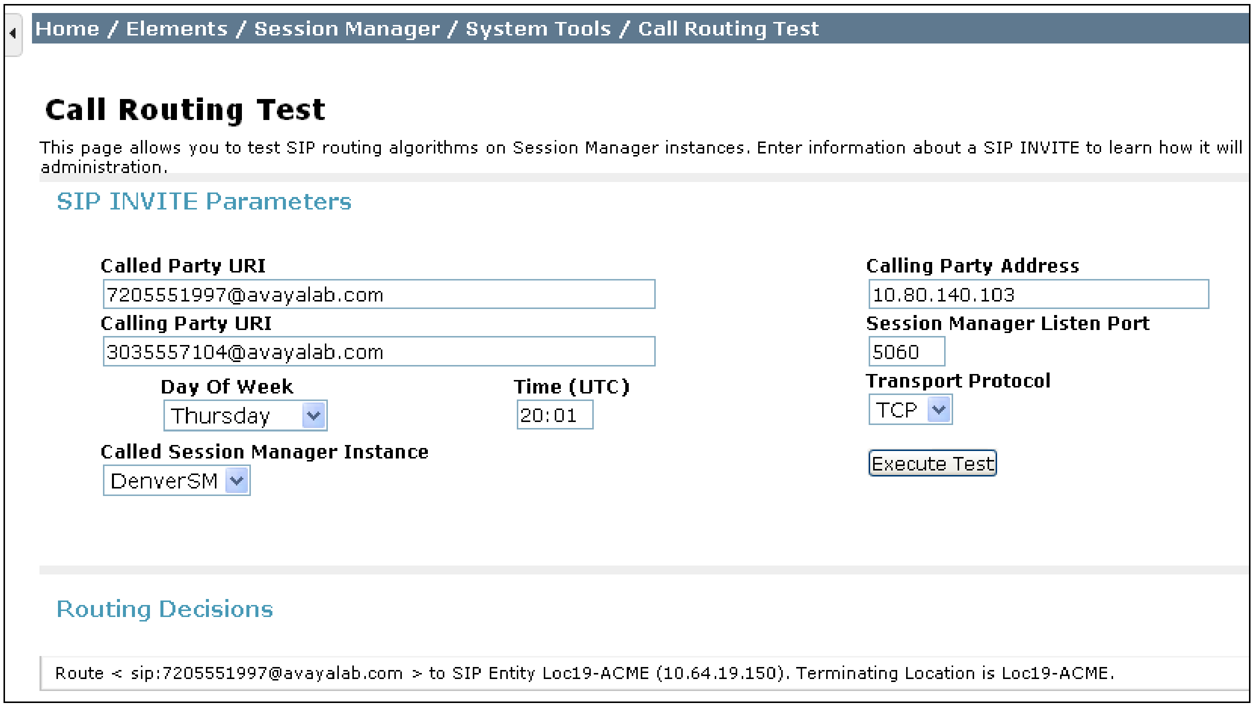
On the preceding screen, **if D-Channel Diagnostics** is selected on the right, a screen such as the following is displayed. D-Channel number 15, which is used in the sample configuration, is established **EST** and active **ACTV**.



9.2. Avaya Aura® Session Manager Verifications

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 CenturyLink. Under **Routing Decisions**, observe the call will rout via Acme Packet 3820 to CenturyLink. 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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E, Avaya Aura® Session Manager, and Acme Packet 3820 Net-Net Session Director to the CenturyLink SIP Trunk (Legacy Qwest) Service. The CenturyLink SIP Trunk is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The CenturyLink SIP Trunk provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

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

[12] *Acme Packet, "Net-Net 4000 S-CX6.3.0 ACLI Configuration Guide",* 400-0061-62, Nov 2009

[13] *Acme Packet, "Net-Net 3800 Series And Net-Net 4500 SSM2 Installation Guide",* 400-0114-20, Apr 2010

[14] *Acme Packet, "Net-Net 3820 Hardware Installation Guide",* 400-0134-10, Mar 2011

Appendix A: Acme Packet 3820 Configuration

Included below is the Acme Packet 3820 configuration used during the compliance testing. The contents of the configuration can be shown by using the ACLI command **show running-config** at the Acme Packet 3820.

```
ACMESYSTEM# show running-config
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       peer
        description
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@10.80.150.50
        last-modified-date             2012-06-06 14:48:12
        policy-attribute
                next-hop                       10.64.19.210
                realm                          core
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol                   SIP
                state                          enabled
                methods
                media-profiles
                lookup                         single
                next-key
                eloc-str-lkup                  disabled
                eloc-str-match
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       core
        description
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@10.80.150.38
        last-modified-date             2011-11-03 17:39:11
        policy-attribute
                next-hop                       SAG:CL-OUT
                realm                          peer
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol                   SIP
                state                          enabled
                methods
```

```
            media-profiles
            lookup                          single
            next-key
            eloc-str-lkup                   disabled
            eloc-str-match
media-manager
        state                           enabled
        latching                        enabled
        flow-time-limit                 86400
        initial-guard-timer             300
        subsq-guard-timer               300
        tcp-flow-time-limit             86400
        tcp-initial-guard-timer         300
        tcp-subsq-guard-timer           300
        tcp-number-of-ports-per-flow    2
        hnt-rtcp                        disabled
        algd-log-level                  NOTICE
        mbcd-log-level                  NOTICE
        red-flow-port                   1985
        red-mgcp-port                   1986
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        media-policing                  enabled
        max-signaling-bandwidth         10000000
        max-untrusted-signaling         100
        min-untrusted-signaling         30
        app-signaling-bandwidth         0
        tolerance-window                30
        rtcp-rate-limit                 0
        trap-on-demote-to-deny          disabled
        syslog-on-demote-to-deny        disabled
        syslog-on-demote-to-untrusted   disabled
        anonymous-sdp                   disabled
        arp-msg-bandwidth               32000
        fragment-msg-bandwidth          0
        rfc2833-timestamp               disabled
        default-2833-duration           100
        rfc2833-end-pkts-only-for-non-sig enabled
        translate-non-rfc2833-event     disabled
        media-supervision-traps         disabled
        dnsalg-server-failover          disabled
        last-modified-by                admin@10.80.150.38
        last-modified-date              2011-11-01 12:25:41
network-interface
        name                            M00
        sub-port-id                     0
        description                     PUBLIC
        hostname
        ip-address                      10.2.2.92
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         10.2.2.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
         hip-ip-list                     10.2.2.92
        ftp-address
         icmp-address                    10.2.2.92
        snmp-address
```

```
        telnet-address
        ssh-address
        signaling-mtu                   0
        last-modified-by                admin@10.80.150.50
        last-modified-date              2012-06-06 14:40:39
network-interface
        name                            M10
        sub-port-id                     0
        description                     PRIVATE
        hostname
        ip-address                      10.64.19.150
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.0
        gateway                         10.64.19.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary                  10.80.150.201
        dns-ip-backup1
        dns-ip-backup2
        dns-domain                      avayalab.com
        dns-timeout                     11
         hip-ip-list                     10.64.19.150
        ftp-address
         icmp-address                    10.64.19.150
        snmp-address
        telnet-address
        ssh-address
        signaling-mtu                   0
        last-modified-by                admin@10.80.150.50
        last-modified-date              2012-06-06 14:42:37
phy-interface
        name                            M00
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2011-11-01 09:59:56
phy-interface
        name                            M10
        operation-type                  Media
        port                            0
        slot                            1
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2011-11-01 10:00:38
realm-config
        identifier                      peer
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M00:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
```

```
mm-same-ip                    enabled
mm-in-system                  enabled
bw-cac-non-mm                 disabled
msm-release                   disabled
qos-enable                    disabled
generate-UDP-checksum         disabled
max-bandwidth                 0
fallback-bandwidth            0
max-priority-bandwidth        0
max-latency                   0
max-jitter                    0
max-packet-loss               0
observ-window-size            0
parent-realm
dns-realm
media-policy
media-sec-policy
srtp-msm-passthrough          disabled
in-translationid
out-translationid
in-manipulationid
out-manipulationid            NatIP
manipulation-string
manipulation-pattern
class-profile
average-rate-limit            0
access-control-trust-level    none
invalid-signal-threshold      0
maximum-signal-threshold      0
untrusted-signal-threshold    0
nat-trust-threshold           0
deny-period                   30
cac-failure-threshold         0
untrust-cac-failure-threshold 0
ext-policy-svr
diam-e2-address-realm
symmetric-latching            disabled
pai-strip                     disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching           none
restriction-mask              32
accounting-enable             enabled
user-cac-mode                 none
user-cac-bandwidth            0
user-cac-sessions             0
icmp-detect-multiplier        0
icmp-advertisement-interval   0
icmp-target-ip
monthly-minutes               0
net-management-control        disabled
delay-media-update            disabled
refer-call-transfer           disabled
refer-notify-provisional      none
dyn-refer-term                disabled
codec-policy
codec-manip-in-realm          disabled
constraint-name
call-recording-server-id
xnq-state                     xnq-unknown
hairpin-id                    0
stun-enable                   disabled
stun-server-ip                0.0.0.0
stun-server-port              3478
stun-changed-ip               0.0.0.0
stun-changed-port             3479
match-media-profiles
qos-constraint
```

```
        sip-profile
        sip-isup-profile
        block-rtcp                     disabled
        hide-egress-media-update       disabled
        last-modified-by               admin@10.80.150.38
        last-modified-date             2011-11-01 13:03:09
realm-config
        identifier                     core
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M10:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
        generate-UDP-checksum          disabled
        max-bandwidth                  0
        fallback-bandwidth             0
        max-priority-bandwidth         0
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        srtp-msm-passthrough           disabled
        in-translationid
        out-translationid
        in-manipulationid              CS1K_To_CL
        out-manipulationid             AddDomain
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        cac-failure-threshold          0
        untrust-cac-failure-threshold  0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        refer-notify-provisional       none
```

```
        dyn-refer-term                 disabled
        codec-policy
        codec-manip-in-realm           disabled
        constraint-name
        call-recording-server-id
        xnq-state                      xnq-unknown
        hairpin-id                     0
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
        stun-server-port               3478
        stun-changed-ip                0.0.0.0
        stun-changed-port              3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                     disabled
        hide-egress-media-update       disabled
        last-modified-by               admin@10.80.150.50
        last-modified-date             2012-06-21 12:20:52
session-agent
        hostname                       10.64.19.210
        ip-address                     10.64.19.210
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       core
        egress-realm-id
        description
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action                Proxy
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS;hops=70
        ping-interval                  60
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
        load-balance-dns-query         hunt
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
```

```
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        refer-notify-provisional       none
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        kpml-interworking              inherit
        last-modified-by               admin@10.80.150.50
        last-modified-date             2012-06-06 14:45:58
session-agent
        hostname                       172.16.2.8
        ip-address                     172.16.2.8
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS;hops=70
        ping-interval                  60
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
```

```
        load-balance-dns-query         hunt
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        refer-notify-provisional       none
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        kpml-interworking              inherit
        last-modified-by               admin@10.80.150.38
        last-modified-date             2011-11-01 12:39:40
session-agent
        hostname                       172.16.2.9
        ip-address                     172.16.2.9
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
```

```
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS;hops=70
        ping-interval                  60
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
        load-balance-dns-query         hunt
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        refer-notify-provisional       none
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        kpml-interworking              inherit
        last-modified-by               admin@10.80.150.38
        last-modified-date             2011-11-01 12:39:46
session-agent
        hostname                       172.16.3.8
        ip-address                     172.16.3.8
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
```

```
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS;hops=70
        ping-interval                  60
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
        load-balance-dns-query         hunt
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        refer-notify-provisional       none
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        kpml-interworking              inherit
        last-modified-by               admin@10.80.150.50
        last-modified-date             2012-06-18 10:23:25
session-agent
        hostname                       172.16.3.9
        ip-address                     172.16.3.9
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       peer
        egress-realm-id
        description
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
```

```
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS;hops=70
        ping-interval                  60
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
        load-balance-dns-query         hunt
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        refer-notify-provisional       none
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        kpml-interworking              inherit
        last-modified-by               admin@10.80.150.50
        last-modified-date             2012-06-18 10:23:57
session-group
        group-name                     CL-OUT
        description
        state                          enabled
        app-protocol                   SIP
        strategy                       Hunt
        dest
                                       172.16.3.8
                                       172.16.2.8
        trunk-group
```

```
        sag-recursion                   enabled
        stop-sag-recurse                401,407
        last-modified-by                admin@10.80.150.50
        last-modified-date              2012-06-18 10:27:19
sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   core
        egress-realm-id                 core
        nat-mode                        None
        registrar-domain
        registrar-host
        registrar-port                  0
        register-service-route          always
        init-timer                      500
        max-timer                       4000
        trans-expire                    32
        invite-expire                   180
        inactive-dynamic-conn           32
        enforcement-profile
        pac-method
        pac-interval                    10
        pac-strategy                    PropDist
        pac-load-weight                 1
        pac-session-weight              1
        pac-route-weight                1
        pac-callid-lifetime             600
        pac-user-lifetime               3600
        red-sip-port                    1988
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        add-reason-header               disabled
        sip-message-len                 4096
        enum-sag-match                  disabled
        extra-method-stats              disabled
        registration-cache-limit        0
        register-use-to-for-lp          disabled
        options                         max-udp-length=0
        refer-src-routing               disabled
        add-ucid-header                 disabled
        proxy-sub-events
        allow-pani-for-trusted-only     disabled
        pass-gruu-contact               disabled
        sag-lookup-on-redirect          disabled
        set-disconnect-time-on-bye      disabled
        last-modified-by                admin@10.80.150.38
        last-modified-date              2011-11-21 17:43:22
sip-interface
        state                           enabled
        realm-id                        peer
        description
        sip-port
                address                         10.2.2.92
                port                            5060
                transport-protocol              UDP
                tls-profile
                multi-home-addrs
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
```

```
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                disabled
        subscribe-reg-event            disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                 0
        register-keep-alive            none
        kpml-interworking              disabled
        tunnel-name
        last-modified-by               admin@10.80.150.50
        last-modified-date             2012-06-06 15:06:55
sip-interface
        state                          enabled
        realm-id                       core
        description
        sip-port
                address                        10.64.19.150
                port                           5060
                transport-protocol             TCP
                tls-profile
                multi-home-addrs
                allow-anonymous                all
                ims-aka-profile
        carriers
        trans-expire                   0
```

```
        invite-expire                   0
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        trust-mode                      all
        max-nat-interval                3600
        nat-int-increment               10
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        subscribe-reg-event             disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                  none
        implicit-service-route          disabled
        rfc2833-payload                 101
        rfc2833-mode                    transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                 disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                   none
        add-sdp-invite                  disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                  0
        register-keep-alive             none
        kpml-interworking               disabled
        tunnel-name
        last-modified-by                admin@10.80.150.50
        last-modified-date              2012-06-18 10:34:11
sip-manipulation
        name                            NatIP
        description
        split-headers
        join-headers
        header-rule
                name                            natFROM
```

```
        header-name                   From
        action                        manipulate
        comparison-type               case-sensitive
        msg-type                      request
        methods
        match-value
        new-value
        element-rule
               name                          natHost
               parameter-name
               type                          uri-host
               action                        replace
               match-val-type                any
               comparison-type               case-sensitive
               match-value
               new-value                     $LOCAL_IP
 header-rule
        name                          natTO
        header-name                   To
        action                        manipulate
        comparison-type               case-sensitive
        msg-type                      request
        methods
        match-value
        new-value
        element-rule
               name                          natHost
               parameter-name
               type                          uri-host
               action                        replace
               match-val-type                any
               comparison-type               case-sensitive
               match-value
               new-value                     $REMOTE_IP
 header-rule
        name                          natPAI
        header-name                   P-Asserted-Identity
        action                        manipulate
        comparison-type               case-sensitive
        msg-type                      any
        methods
        match-value
        new-value
        element-rule
               name                          natHost
               parameter-name
               type                          uri-host
               action                        replace
               match-val-type                any
               comparison-type               case-sensitive
               match-value
               new-value                     $LOCAL_IP
 header-rule
        name                          removePL
        header-name                   P-Location
        action                        delete
        comparison-type               case-sensitive
        msg-type                      any
        methods
        match-value
        new-value
 header-rule
        name                          remoteAlrtInfo
        header-name                   Alert-Info
        action                        delete
        comparison-type               case-sensitive
        msg-type                      any
        methods
        match-value
        new-value
```

```
header-rule
        name                            natRequest
        header-name                     Request-URI
        action                          manipulate
        comparison-type                 case-sensitive
        msg-type                        request
        methods
        match-value
        new-value
        element-rule
                name                            natHost
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       $REMOTE_IP
header-rule
        name                            natDiversion
        header-name                     Diversion
        action                          manipulate
        comparison-type                 case-sensitive
        msg-type                        request
        methods
        match-value
        new-value
        element-rule
                name                            natHost
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       $LOCAL_IP
header-rule
        name                            natREFER
        header-name                     Refer-To
        action                          manipulate
        comparison-type                 case-sensitive
        msg-type                        request
        methods
        match-value
        new-value
        element-rule
                name                            refer
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       $REMOTE_IP
header-rule
        name                            removeHist
        header-name                     History-Info
        action                          delete
        comparison-type                 case-sensitive
        msg-type                        any
        methods
        match-value
        new-value
header-rule
        name                            removeRPI
        header-name                     Remote-Party-ID
        action                          delete
        comparison-type                 case-sensitive
        msg-type                        any
        methods
```

```
            match-value
            new-value
        header-rule
            name                            removeXNTe164
            header-name                     X-nt-e164-clid
            action                          delete
            comparison-type                 case-sensitive
            msg-type                        any
            methods
            match-value
            new-value
        last-modified-by                admin@10.80.150.50
        last-modified-date              2012-06-18 15:26:21
sip-manipulation
        name                            AddDomain
        description
        split-headers
        join-headers
        header-rule
            name                            FromDomain
            header-name                     From
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods
            match-value
            new-value
            element-rule
                name                            From
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       avayalab.com
        header-rule
            name                            PaiDomain
            header-name                     P-Asserted-Identity
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods
            match-value
            new-value
            element-rule
                name                            Pai
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
                match-value
                new-value                       avayalab.com
        header-rule
            name                            natTO
            header-name                     To
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods
            match-value
            new-value
            element-rule
                name                            To
                parameter-name
                type                            uri-host
                action                          replace
                match-val-type                  any
                comparison-type                 case-sensitive
```

```
                match-value
                new-value                       $REMOTE_IP
        last-modified-by                admin@10.80.150.50
        last-modified-date              2012-06-21 12:09:39
sip-manipulation
        name                            CS1K_To_CL
        description
        split-headers
        join-headers
        header-rule
                name                            PAIRegex
                header-name                     P-Asserted-Identity
                action                          store
                comparison-type                 pattern-rule
                msg-type                        any
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            chkUser
                        parameter-name
                        type                            header-value
                        action                          store
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     (.*)(30355571)(.*)
                        new-value
        header-rule
                name                            HistRegex
                header-name                     History-Info
                action                          store
                comparison-type                 pattern-rule
                msg-type                        any
                methods
                match-value
                new-value
                element-rule
                        name                            GetReason
                        parameter-name
                        type                            header-value
                        action                          store
                        match-val-type                  any
                        comparison-type                 pattern-rule
                        match-value                     (.*)(reason)(.*)
                        new-value
        header-rule
                name                            AddDiversion
                header-name                     Diversion
                action                          add
                comparison-type                 boolean
                msg-type                        request
                methods                         INVITE
                match-value                     (!$PAIRegex[0].$chkUser)&!$HistRegex[0].$GetReason
                new-value                       "<sip:3035557104@avayalab.com;user=phone>"
        last-modified-by                admin@10.80.150.50
        last-modified-date              2012-06-22 11:06:09
steering-pool
        ip-address                      10.2.2.92
        start-port                      49152
        end-port                        65535
        realm-id                        peer
        network-interface
        last-modified-by                admin@10.80.150.50
        last-modified-date              2012-06-06 15:07:34
steering-pool
        ip-address                      10.64.19.150
        start-port                      49152
        end-port                        65535
        realm-id                        core
        network-interface
```

```
        last-modified-by               admin@10.80.150.50
        last-modified-date             2012-06-06 15:08:02
system-config
        hostname
        description
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                   enabled
        enable-snmp-auth-traps         disabled
        enable-snmp-syslog-notify      disabled
        enable-snmp-monitor-traps      disabled
        enable-env-monitor-traps       disabled
        snmp-syslog-his-table-length   1
        snmp-syslog-level              WARNING
        system-log-level               WARNING
        process-log-level              NOTICE
        process-log-ip-address         0.0.0.0
        process-log-port               0
        collect
                sample-interval                5
                push-interval                  15
                boot-state                     disabled
                start-time                     now
                end-time                       never
                red-collect-state              disabled
                red-max-trans                  1000
                red-sync-start-time            5000
                red-sync-comp-time             1000
                push-success-trap-state        disabled
        call-trace                     disabled
        internal-trace                 disabled
        log-filter                     all
        default-gateway                10.80.150.1
        restart                        enabled
        exceptions
        telnet-timeout                 0
        console-timeout                0
        remote-control                 enabled
        cli-audit-trail                enabled
        link-redundancy-state          disabled
        source-routing                 disabled
        cli-more                       disabled
        terminal-height                24
        debug-timeout                  0
        trap-event-lifetime            0
        default-v6-gateway             ::
        ipv6-signaling-mtu             1500
        ipv4-signaling-mtu             1500
        cleanup-time-of-day            00:00
        snmp-engine-id-suffix
        snmp-agent-mode                v1v2
task done
ACMESYSTEM#
```

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.