Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2 with Verizon Business IP Trunk SIP Trunk Service – Issue 1.1

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and the Avaya Session Border Controller for Enterprise Release 6.2, with the Verizon Business Private IP (PIP) IP Trunk service.

The Verizon Business IP Trunk service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

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., utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration of Avaya Communication Server 1000E Release 7.6 (CS1000E), Avaya Aura® Session Manager Release 6.3.2, and Avaya Session Border Controller for Enterprise Release 6.2 (Avaya SBCE), with the Verizon Business Private IP (PIP) IP Trunk service. The Verizon Business IP Trunk service provides local and/or long-distance calls via standards-based SIP trunks.

Customers using Avaya CS1000E with the Verizon Business IP Trunk SIP Trunk service are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

Verizon Business IP Trunk service offer can be delivered to the customer premise via either a Private IP (PIP) or Internet Dedicated Access (IDA) IP network terminations. Although the configuration documented in these Application Notes used Verizon's IP Trunk service terminated via a IDA network connection, the solution validated in this document also applies to IP Trunk services delivered via IDA service terminations.

For more information on the Verizon Business IP Trunking service, including access alternatives, visit http://www.verizonbusiness.com/us/products/voip/trunking/.

2. General Test Approach and Test Results

The Avaya CS1000E location was connected to the Verizon Business IP Trunk Service, as depicted in **Figure 1**. The Avaya equipment was configured to use the commercially available SIP Trunking solution provided by the Verizon Business IP Trunk SIP Trunk Service. This allowed Avaya CS1000E users to make calls to the PSTN and receive calls from the PSTN via the Verizon Business IP Trunk SIP Trunk Service.

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

2.1. Interoperability Compliance Testing

The testing included the following successful SIP trunk interoperability compliance testing:

- DNS SRV to determine the Verizon IP Trunk SIP signaling information, using UDP for SIP signaling and full SIP headers. The use of DNS SRV is optional, and the configuration was tested with static configuration of the Verizon SIP signaling IP Address and port as well as with the DNS SRV configuration.
- Incoming calls from the PSTN were routed to the DID numbers assigned by Verizon Business to the Avaya CS1000E location. These incoming PSTN calls arrived via the SIP

Trunk and were answered by Avaya SIP telephones, Avaya IP UNIStim telephones, Avaya digital telephones, and analog telephones and fax machines. The display of caller ID on display-equipped Avaya CS1000E telephones was verified. Avaya CS1000E sends 180 Ringing (without SDP) for calls ringing to an Avaya CS1000E telephone user.

- Outgoing calls from the Avaya CS1000E location to the PSTN were routed via the SIP Trunk to Verizon Business. These outgoing PSTN calls were originated from Avaya SIP telephones, Avaya IP UNIStim telephones, Avaya digital telephones, and analog telephones and fax machines. The display of caller ID on display-equipped PSTN telephones was verified. Outbound calls using "fast answer" (Verizon 200 OK without a preceding 18x) were also tested successfully.
- Proper disconnect when the caller abandoned a call before answer for both inbound and outbound calls.
- Proper disconnect when the Avaya CS1000E party or the PSTN party terminated an active call.
- Proper busy tone heard when an Avaya CS1000E user called a busy PSTN user, or a PSTN user called a busy Avaya CS1000E user (i.e., if no redirection was configured for user busy conditions).
- Various outbound PSTN call types were tested including long distance, international, toll-free, operator assisted, directory assistance, and non-emergency x11 calls.
- Requests for privacy (i.e., caller anonymity) for Avaya CS1000E outbound calls to the PSTN were verified. That is, when privacy is requested by Avaya CS1000E, outbound PSTN calls were successfully completed while withholding the caller ID from the displays of display-equipped PSTN telephones.
- Privacy requests for inbound calls from the PSTN to Avaya CS1000E users were verified. That is, when privacy is requested by a PSTN caller, the inbound PSTN call was successfully completed to an Avaya CS1000E user while presenting an "anonymous" display to the Avaya CS1000E user.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Both Verizon Business and the Avaya Session Border Controller for Enterprise (SBCE) were able to monitor health using SIP OPTIONS. The Avaya Aura® SBC configurable control of SIP OPTIONS timing was exercised successfully.
- Incoming and outgoing voice calls using the G.729(a) and G.711 ULAW codecs, and proper protocol procedures related to media.
- DTMF transmission for incoming and outgoing calls.
- Inbound and outbound long holding time call stability.
- Telephony features such as call waiting hold transfer using re-INVITE and conference. Note that Avaya CS1000E will not send REFER to the Verizon network.
- Inbound calls from Verizon IP Trunk Service that were call forwarded back to PSTN destinations via Verizon IP Trunk Service, presenting true calling party information to the destination PSTN telephone.
- Proper DiffServ markings for SIP signaling and RTP media.
- Inbound fax and outbound fax calls.
- Inbound and outbound G.729a voice calls for which intentionally induced ambient fax tone "noise" played to the voice call causes Verizon to issue a re-INVITE to G.711.

Items not supported or not tested included the following:

- Emergency 911/E911 Services Limitations and Restrictions - Although Verizon provides 911/E911 calling capabilities 911 capabilities were not tested, it is Customer's responsibility to ensure proper operation with its equipment/software vendor.
- Verizon Business IP Trunking service does not support G.729B codec.
- SIP REFER method is not supported by Avaya CS1000E.
- CS1000E Mobile-X features were not tested.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results. The following observations were noted:

- **T.38 Fax:** Verizon has implemented T.38 Fax in their network; however Verizon sends a re-Invite to G.711 instead of T.38 after the detection of fax tone. This resulted in outbound fax transmission using G.711.

- **Avaya CS1000E does not support sending REFER:** Incoming Verizon IP Trunk calls that are transferred back out to the PSTN via the Verizon IP Trunk Service will continue to traverse the enterprise site (i.e., will not be released via a REFER-based transfer).

- **Max-Forwards header:** The Invite message from the Avaya CS1000E would sometimes contain a Max-Forwards value of 20. Verizon recommends a Max-Forwards value of 70 be sent with all SIP requests from the CPE. A SigMa Script on the Avaya SBCE was used to change the Max-Forwards value to 70. See **Section 7.5**.

- **Transfer from PSTN to PSTN:** Assume a call is active between a CS1000E telephone user and a PSTN user "A". To allow the CS1000E user to transfer the call using the Verizon IP Trunk Service to another PSTN user "B" before user B has answered the call, CS1000E plug-in 501 must be enabled as show in **Section 5.7**.

- **Blind transfer off-net, calling party on PSTN does not hear ringback tone when the called PSTN is ringing:** This limitation is encountered when performing a work around to support a blind transfer call without an UPDATE/SDP method. Before completing the transferred call, the CS1000 uses an UPDATE/SDP method to anchor ring back tone on the 2nd leg to the 1st leg. However, Verizon does not support this method, it rejects the UPDATE/SDP with a "500 Internal Server Error" response. A workaround has been made to eliminate the UPDATE method on inbound signaling, that makes the CS1000 automatically disable UPDATE from being sent to Verizon. This is achieved by the SigMa Script on the Avaya SBCE in **Section 7.5** and by enabling plug-in 501 for the CS1000 in **Section 5.7**.

Note: The Avaya CS1000E requires support of UPDATE, but Verizon does not support this method. Not supporting UPDATE may result in significant service degradation and feature breakage.

2.3. The SIP Trunk Redundant (2-CPE) Architecture Option

Verizon Business and Avaya developed the SIP Trunk Redundant (2-CPE) architecture to ensure that SIP trunk calls can be automatically rerouted to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described in these Application Notes is based on a customer location having two Avaya Session Border Controllers for Enterprise. One Avaya SBCE is designated as Primary and one as Secondary. The Avaya SBCEs reside at the edge of the customer network.

Session Manager is provisioned to attempt outbound calls to the Primary Avaya SBCE first. If that attempt fails, the Secondary Avaya SBCE is used. Similarly, the Verizon Business Private IP Trunk service node will send inbound calls to the Primary Avaya SBCE. If there is no response then the call will be sent to the Secondary Avaya SBCE.

2.4. Support

2.4.1. Avaya

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

2.4.2. Verizon

For technical support on Verizon Business IP Trunk service offer, visit the online support site at http://www.verizonbusiness.com/us/customer/.

3. Reference Configuration

Figure 1 illustrates an example Avaya CS1000E solution connected to the Verizon Business IP Trunk SIP Trunk service. The Avaya equipment is located on a private IP network. An enterprise edge router provides access to the Verizon Business IP Trunk service network via a Verizon Business T1 circuit. This circuit is provisioned for the Verizon Business Private IP (PIP) service. The optional Verizon "unscreened ANI" feature is not needed by the Avaya CS1000E.

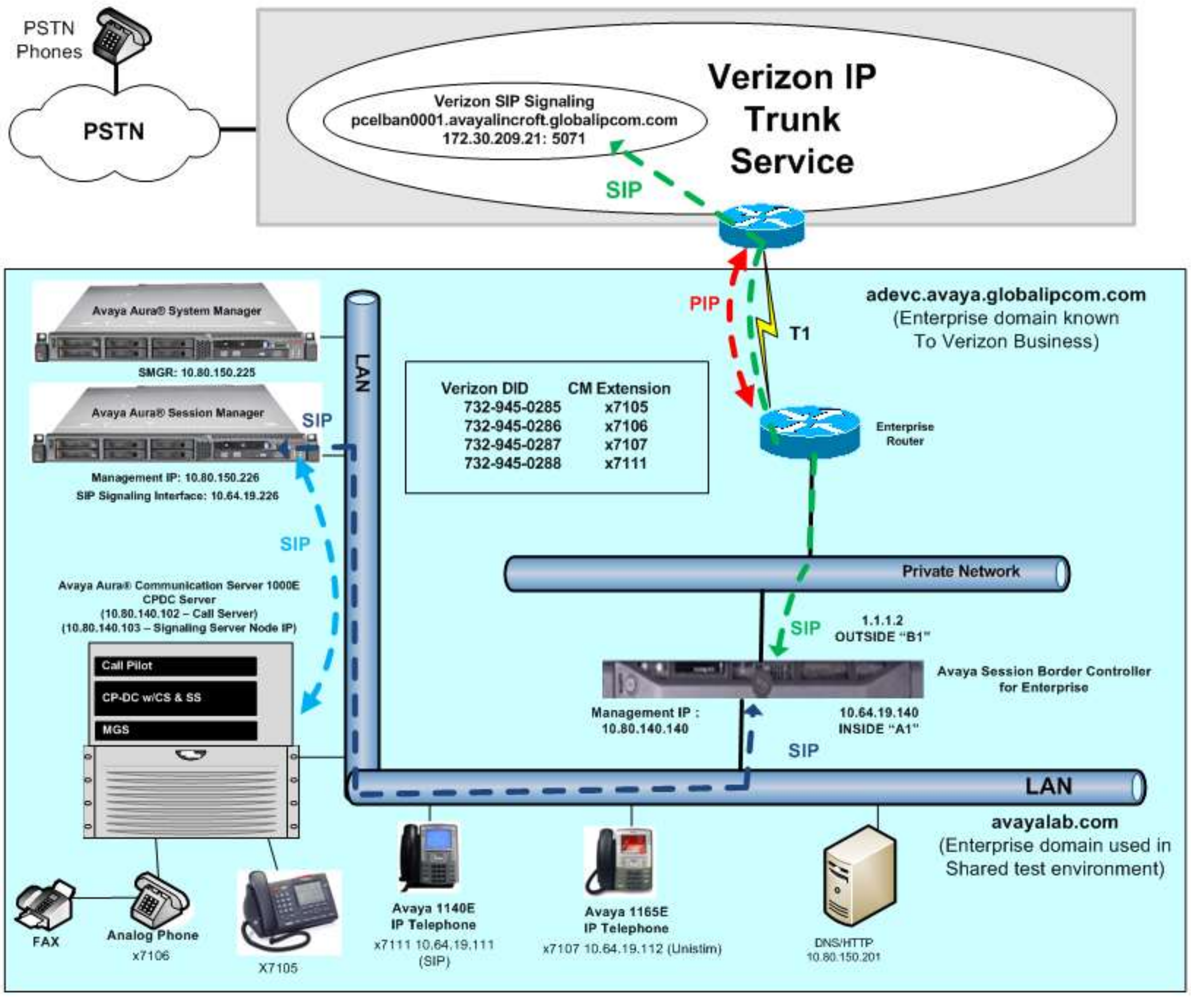


Figure 1: Avaya Interoperability Test Lab Configuration

In the sample configuration, the Avaya SBCE receives traffic from the Verizon Business IP Trunk service on port 5060. When the Avaya SBCE is installed, a static IP Address for the Verizon SIP signaling address and port can be entered. If DNS SRV is preferred, the Avaya SBCE can be configured to use DNS SRV, using UDP for transport, to determine the IP Address and port to be used to send SIP signaling to Verizon. In the sample configuration, the DNS process will result in SIP signaling being sent to IP Address 172.30.209.21 and port 5071.

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunk Service as FQDN *adevc.avaya.globalipcom.com*. For efficiency, the Avaya environment utilizing Session Manager Release 6.3 and Communication Server Release 7.6 was shared among many ongoing test efforts at the Avaya Solution and Interoperability Test lab. Access to the Verizon Business IP Trunk service was added to a configuration that already used domain "avayalab.com" at the enterprise. The Avaya SBCE is used to adapt the "avayalab.com" domain to the domains known to Verizon. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in CS1000E and Session Manager match the CPE domain known to the Verizon Business IP Trunk service.

The Verizon Business IP Trunk service provided Direct Inward Dial (DID) numbers that terminated at the Avaya CS1000E location. These DID numbers were mapped to Avaya CS1000E users via a Session Manager adaptation. **Table 1** shows a sample mapping of Verizon-provided DID numbers to Avaya CS1000E telephone users.

Verizon Provided DID	Avaya CS1000E Destination	Notes
732-945-0285	x7105	Avaya M3904 Digital Telephone
732-945-0286	x7106	Analog telephone / fax
732-945-0287	x7107	Avaya 1165-Series IP Deskphone (UNIStim)
732-945-0288	x7111	Avaya 1140E-Series IP Deskphone (SIP)

Table 1: Sample Verizon DID to CS1000E Telephone Mappings

The following components were used in the sample configuration:

Note – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the sample configuration shown in **Figure 1**. Verizon Business customers will use different FQDNs and IP addressing as required.

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
  - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN)
  - *adevc.avaya.globalipcom.com*
- Avaya Session Border Controller for Enterprise(SBC-E) 6.2.0Q36
- Avaya Communication Server 1000E Release 7.6
- Avaya Aura® System Manager Release 6.3.2
- Avaya Aura® Session Manager Release 6.3.2
- Avaya 1100-Series IP Deskphones using UNIStim software
- Avaya 1140E IP Deskphones using SIP software, registered to the CS1000E
- Avaya M3900-Series Digital phones
- Analog telephones and fax machines

Note – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

3.1. History-Info and Diversion Headers

The Verizon Business IP Trunk service does not support SIP History-Info Headers. Instead, the Verizon Business IP Trunk service requires that SIP Diversion Header be sent for redirected calls. The Avaya Communication Server 1000E includes History-Info header in messaging sent to Session Manager. Session Manager can convert the History Info header into the Diversion Header required by Verizon. This is performed by specifying the "*VerizonAdapter*" adaptation in Session Manager. See **Section 6.3.2**.

The Avaya Communication Server 1000E call forwarding feature may be used for call scenarios testing Diversion Header.

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: 7.65.16 GA (CoRes) Service Pack 2
Communication Server 1000E Media Gateway	CSP Version: MGCC DC01 MSP Version: MGCM AB02 APP Version: MGCA BA18 FPGA Version: MGCF AA22 BOOT Version: MGCB BA18 DSP1 Version: DSP4 AB07 BCSP Version: MGCC DC01
Avaya Aura® System Manager	6.3.0 –FP2
Avaya Aura® Session Manager	6.3.2.0.632023
Avaya Session Border Controller for Enterprise	6.2.0Q36
Avaya 1165E (UNIStim)	0626C8Q
Avaya 1140E (SIP)	04.03.12.00
Avaya M3904 (Digital)	n/a
Avaya 6210 Analog Telephone	n/a

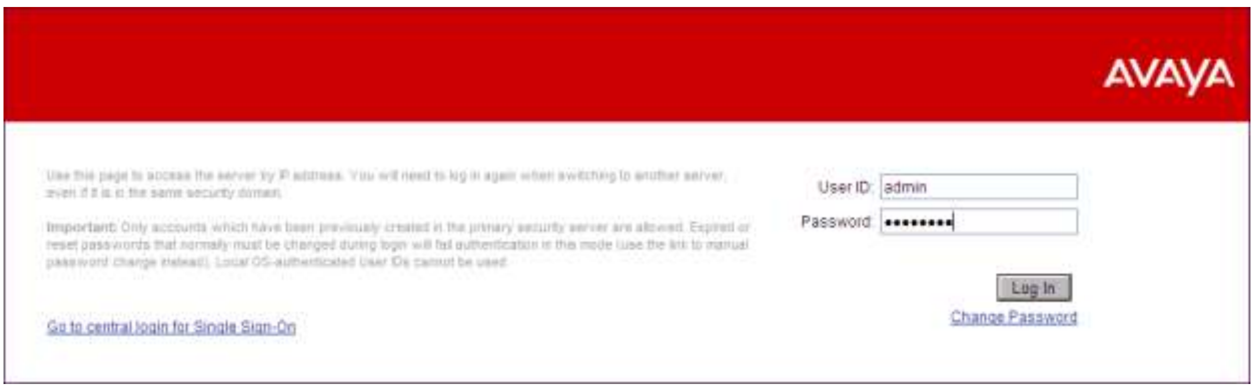
Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Communication Server 1000E

This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to Verizon over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.6 (CS1000E) 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.

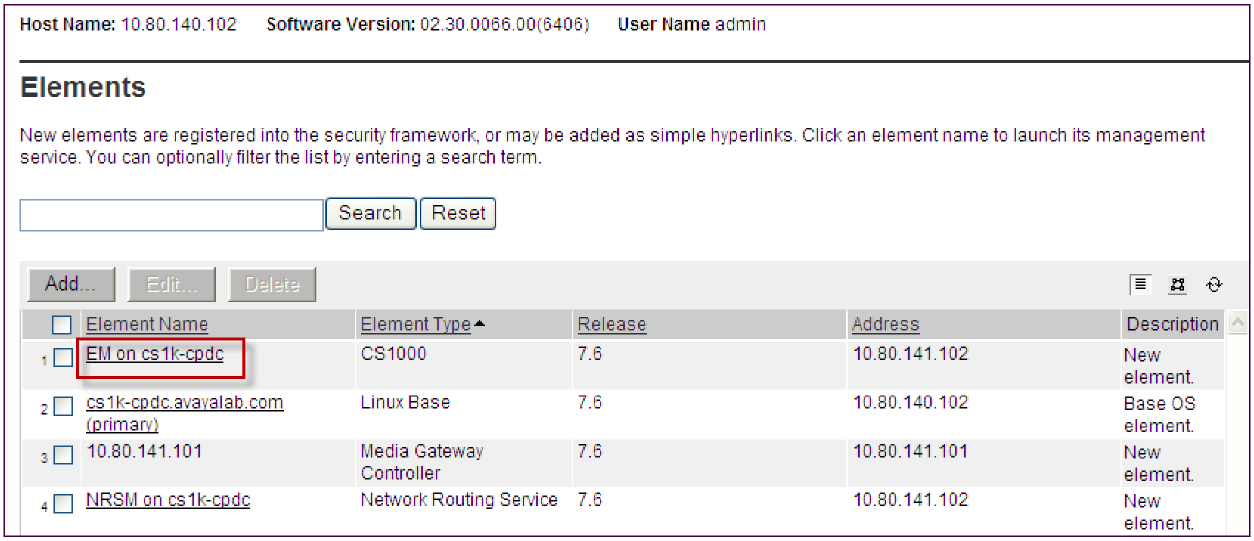
This section focuses on the SIP Trunking configuration. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the Call Server and SIP Signaling Server applications has been completed, and that the Avaya CS1000E is configured to support analog, digital, UNIStim, and SIP telephones. For references on how to administer these functions of Avaya CS1000E, 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.



Alternatively, if System Manager has been configured as the Primary Security Server for the Avaya Unified Communications Management application and Avaya CS1000E is registered as a member of the System Manager Security framework, the Element Manager may be accessed via System Manager. In this case, access the web based GUI of Avaya Aura® System Manager by using the URL http://<ip-address>/SMGR, where <ip-address> is the IP address of System Manager. Log in with appropriate credentials. The System Manager Home Page will be displayed. Under the **Elements** category on the right side of the page, click the **Communication Server 1000** link (not shown).

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

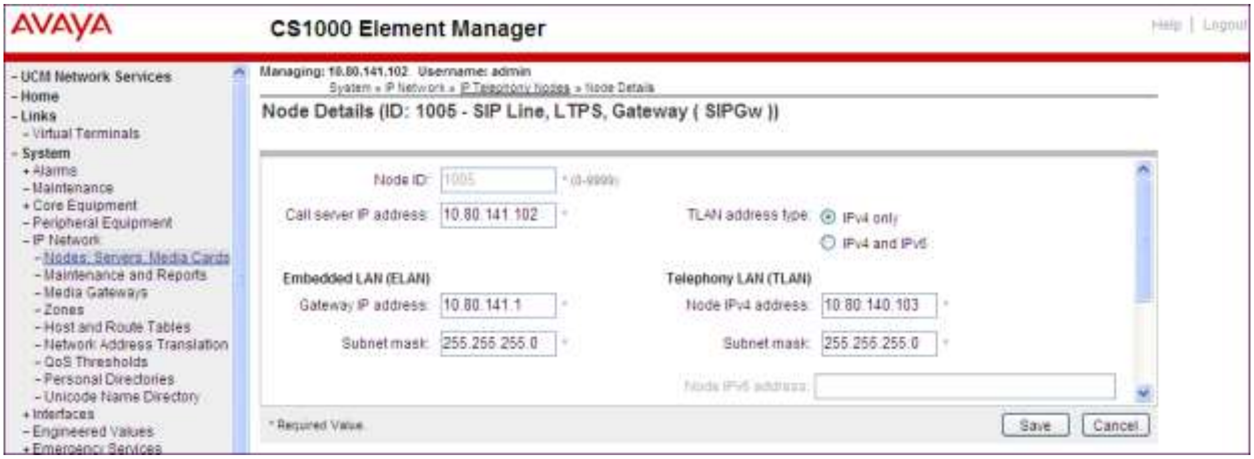
This section describes how to configure an IP Telephony Node on the Avaya CS1000E.

5.1.1. Obtain Node IP Address

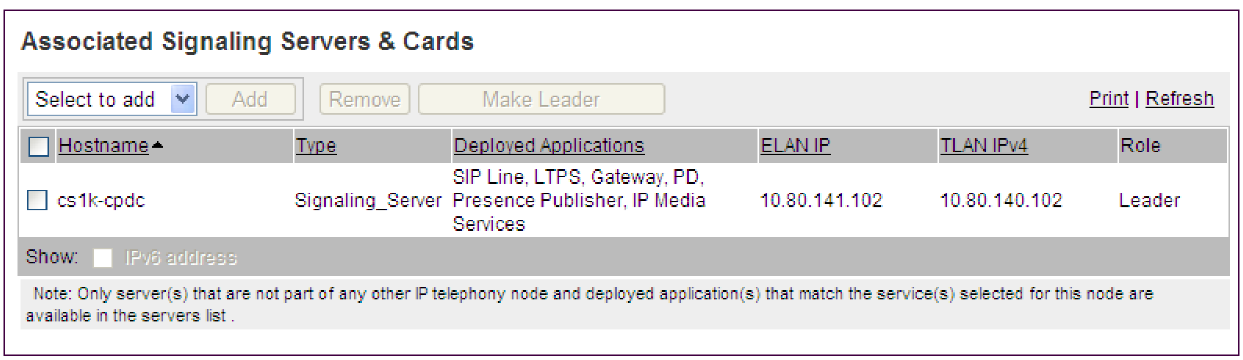
Expand **System → IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

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 Avaya CS1000E in **Section 6.4.1**.

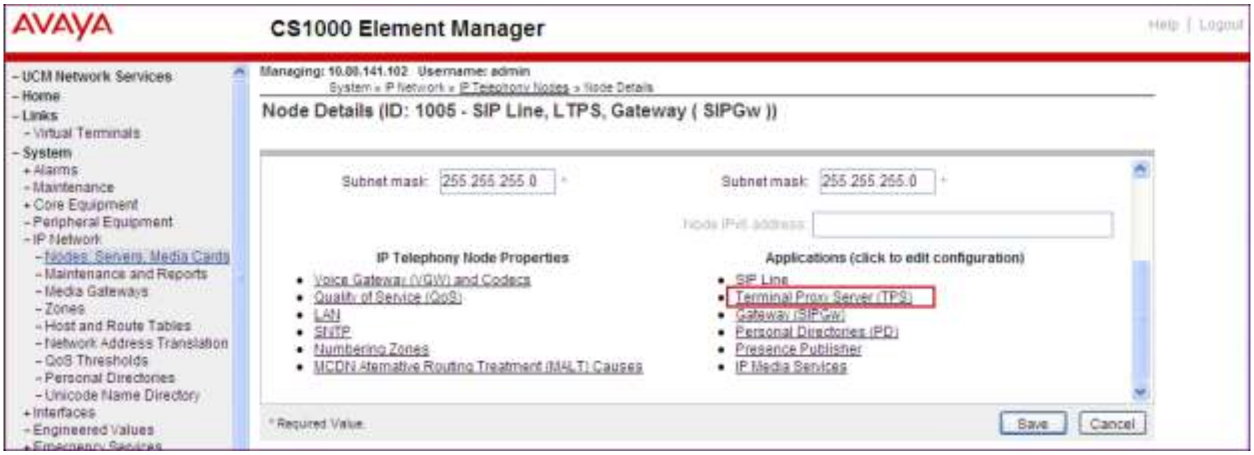


The following screen shows the **Associated Signaling Servers & Cards** heading at the bottom of the screen, simply to document the configuration.

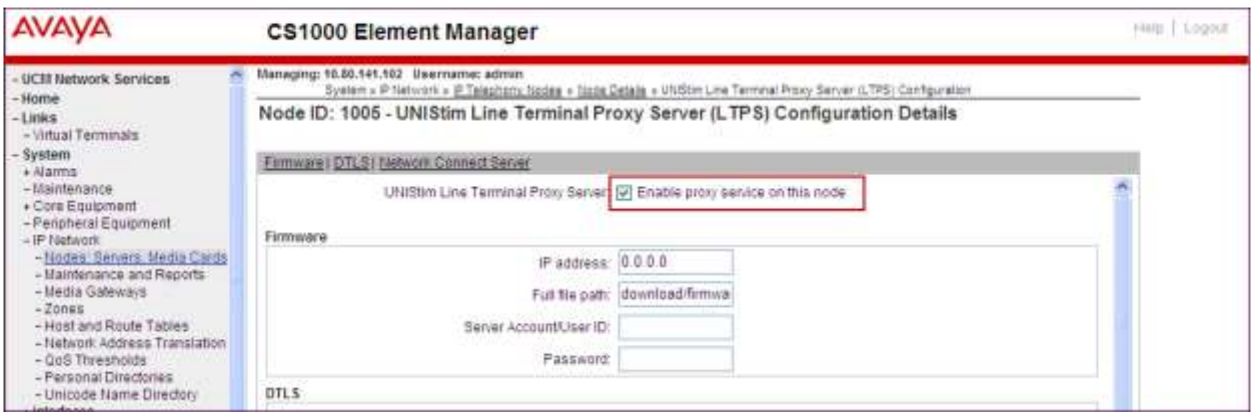


5.1.2. Terminal Proxy Server (TPS)

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

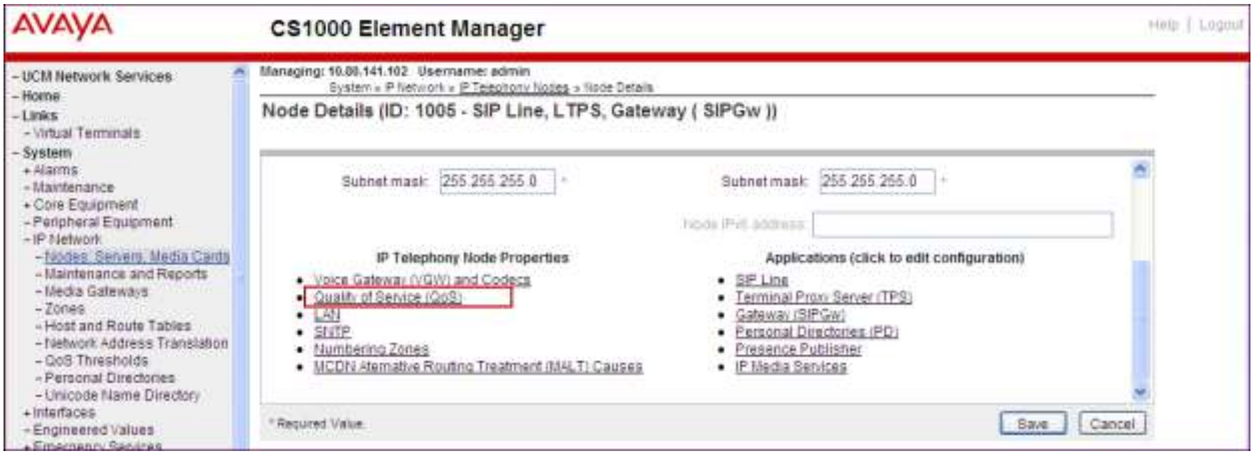


Check the **UNIStim Line Terminal Proxy Server** check box and then click **Save** (not shown).

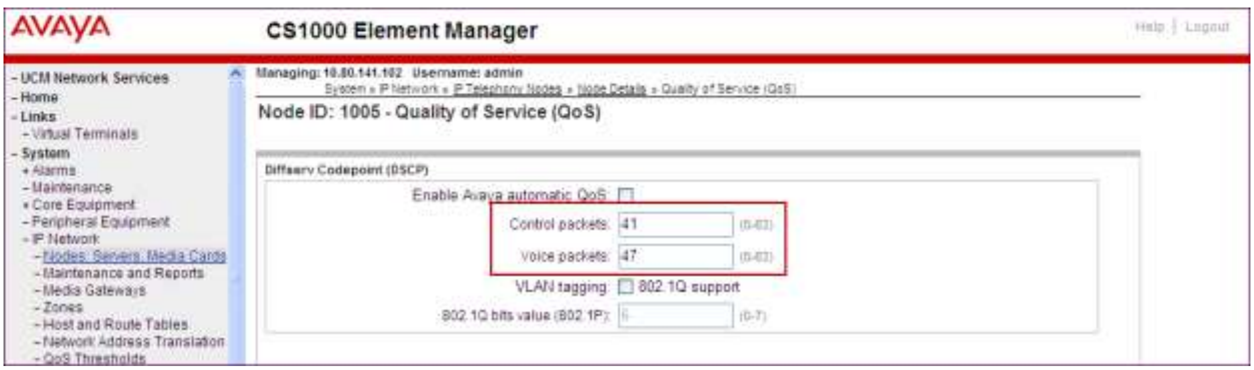


5.1.3. Quality of Service (QoS)

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

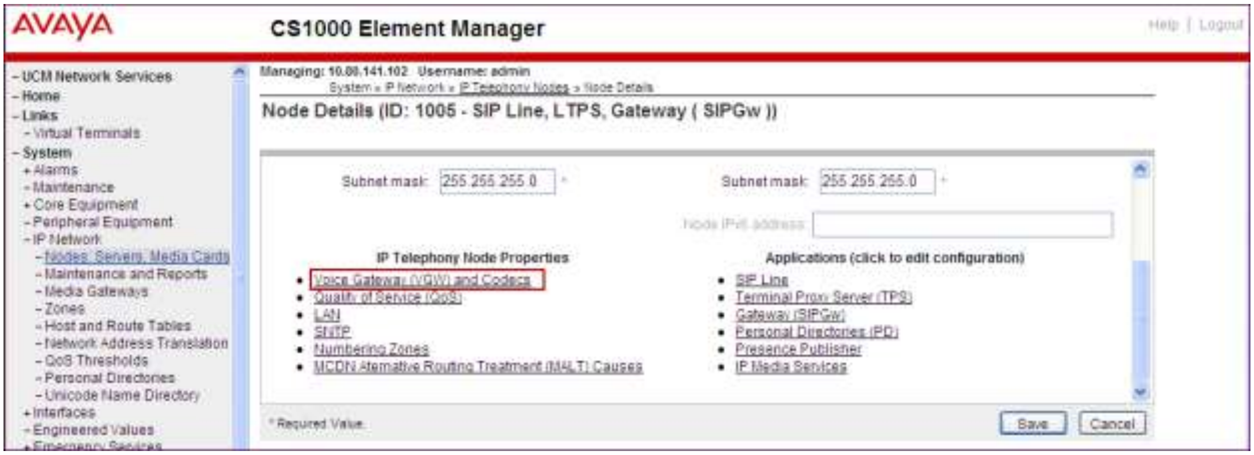


Set the **Control packets** and **Voice packets** values to the desired Diffserv settings required on the internal network. The default Diffserv values are shown below. Click **Save**.

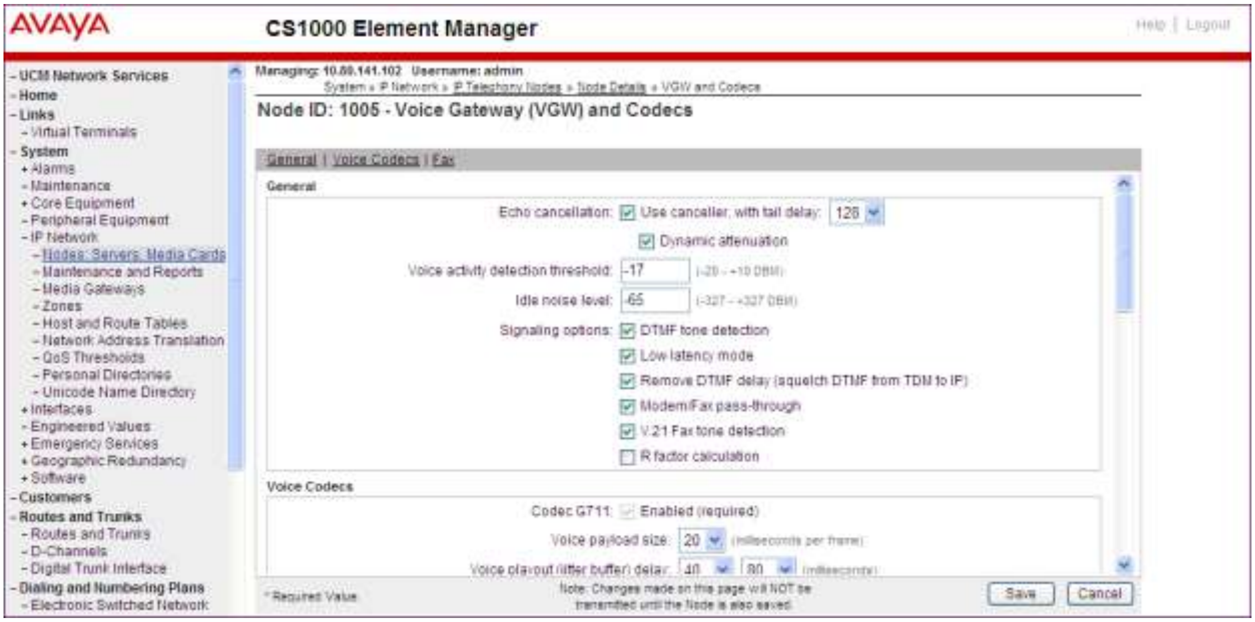


5.1.4. Voice Gateway and Codecs

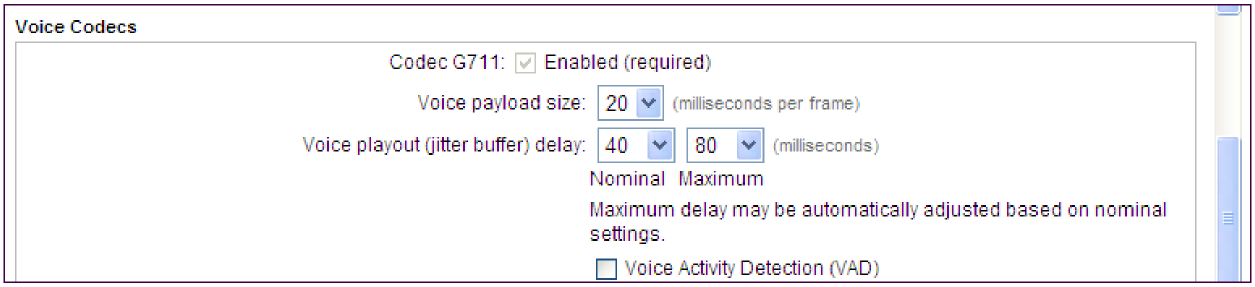
On the **Node Details** screen, scroll down in the top window and select the **Voice Gateway (VGW) and Codecs** link as shown below.



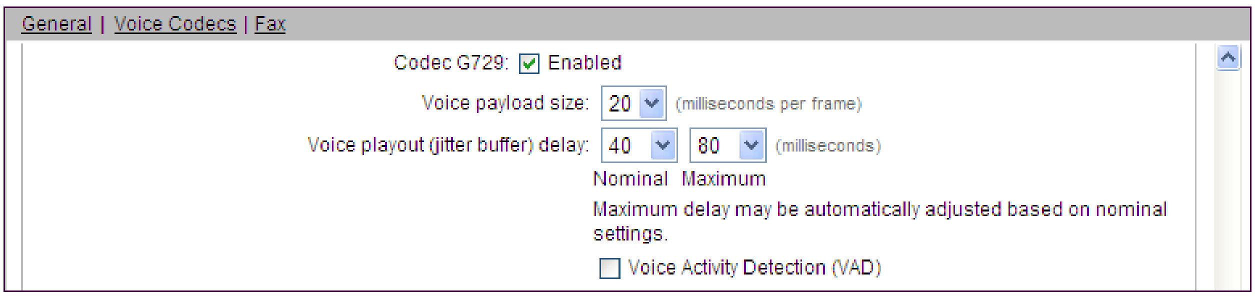
The following screen shows the General parameters used in the sample configuration.



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.

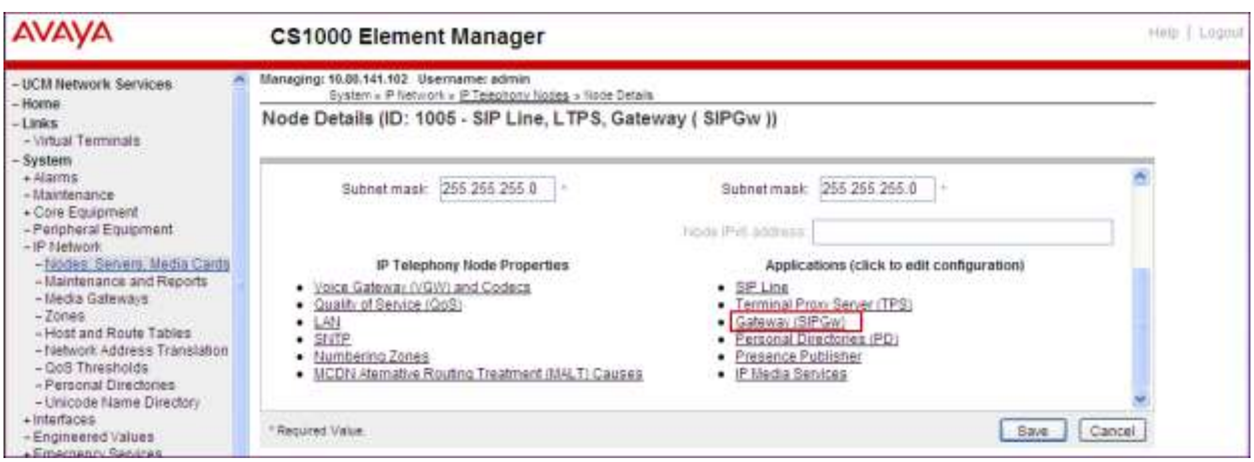


For the **Codec G.729**, ensure that the **Enabled** box is checked, and the **Voice Activity Detection (VAD)** box is un-checked. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order.



5.1.5. SIP Gateway

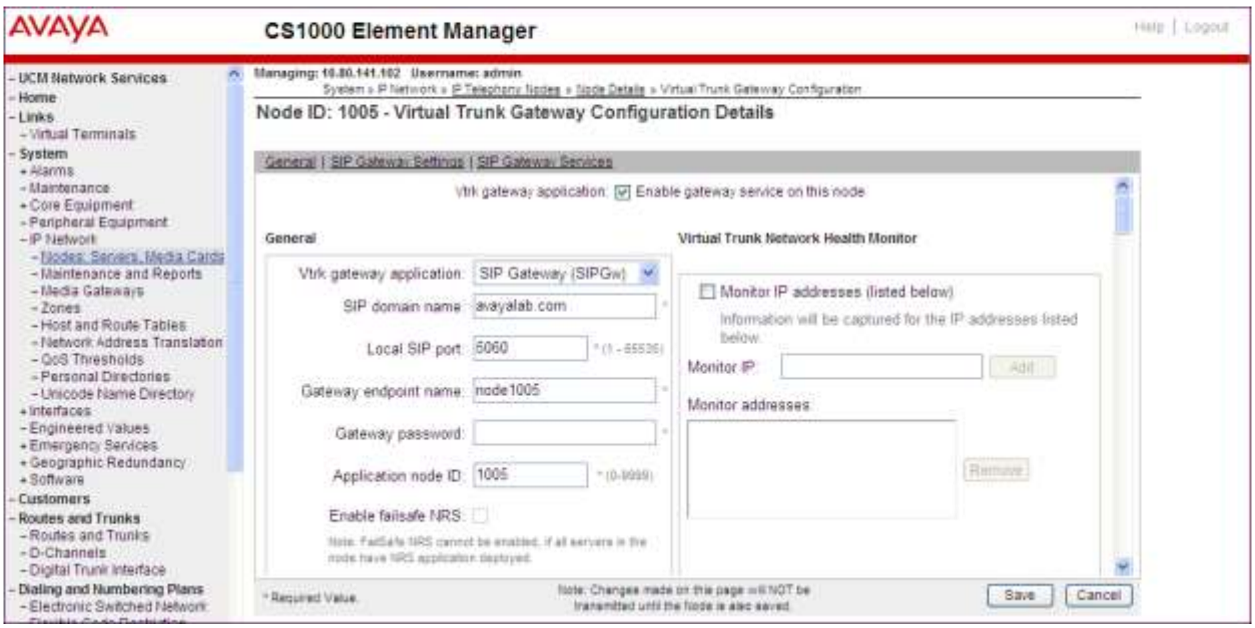
The SIP Gateway is the SIP trunk between the Avaya CS1000E and Session Manager. On the **Node Details** screen, scroll down in the top window and select the **Gateway (SIPGw)** link as show below.



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. The SIP domain for the enterprise known to Verizon is "**adevc.avaya.globalipcom.com**", and the SIP domain will be adapted by Avaya SBCE for calls to and from the Avaya CS1000E.
- **Local SIP port:** Enter "**5060**".
- **Gateway endpoint name:** Enter a descriptive name.
- **Application node ID:** Enter **<Node id>**. In the sample configuration, Node "**1005**" was used matching the node show in **Section 5.1.1**.

The values defined for the sample configuration are shown below.

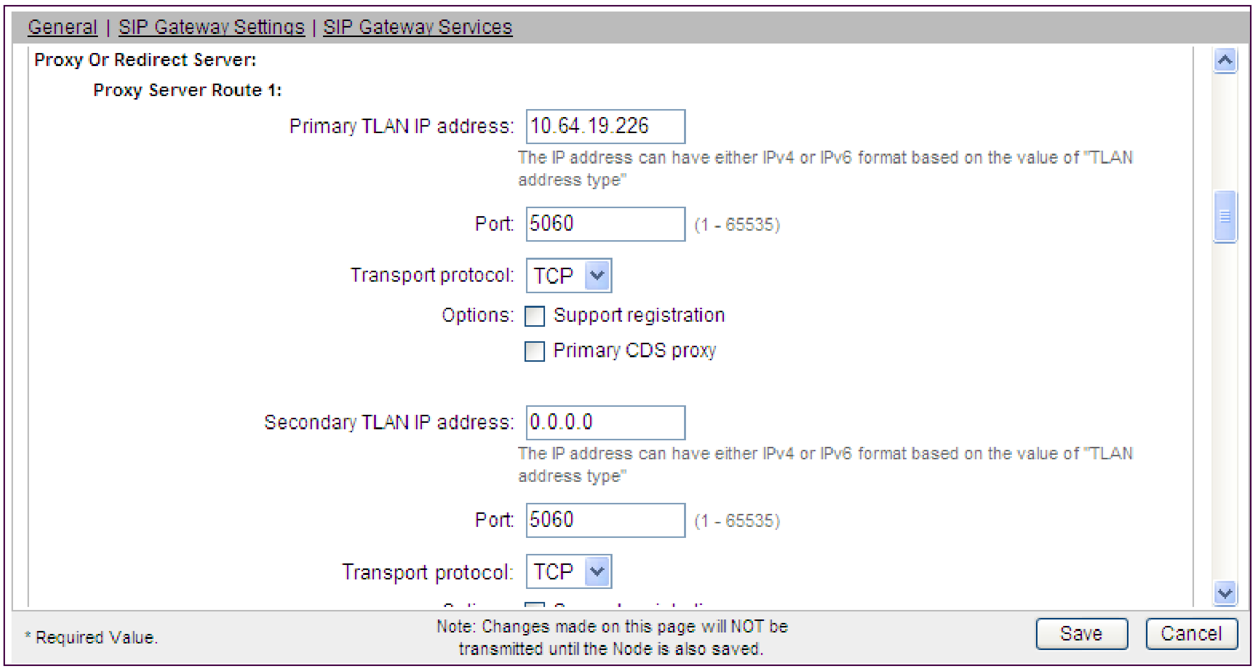


Scroll down to the **SIP Gateway Settings → Proxy or Redirect Server:** section.

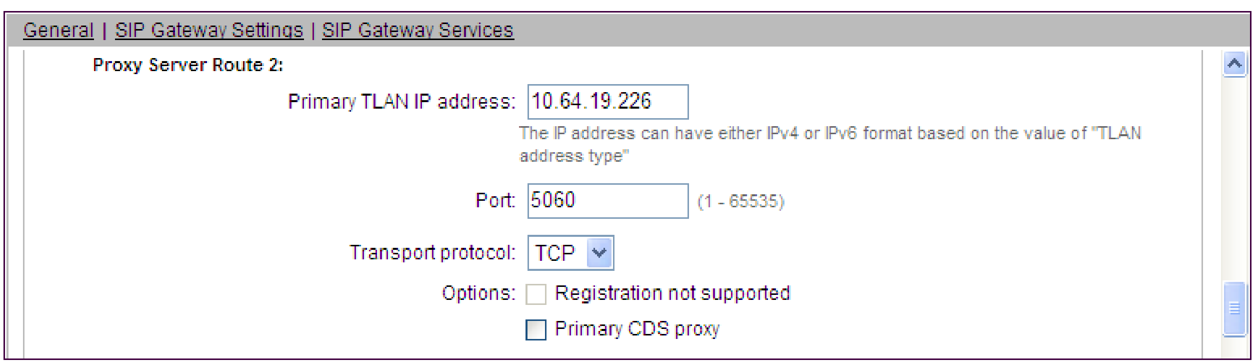
Under **Proxy Server Route 1**, enter the following and use default values for remaining fields.

- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface. In the sample configuration "**10.64.19.226**" was used.
- **Port:** Enter "**5060**"
- **Transport protocol:** Select "**TCP**"

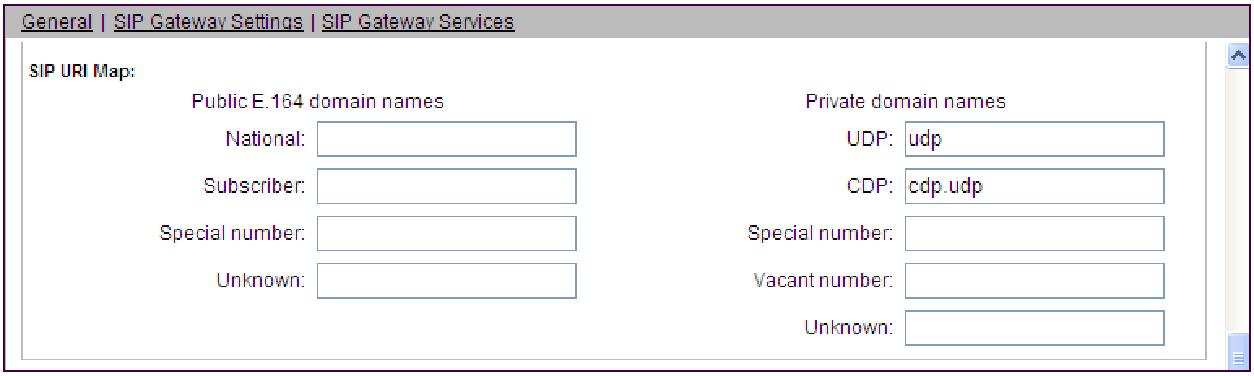
The values defined for the sample configuration are shown below.



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.

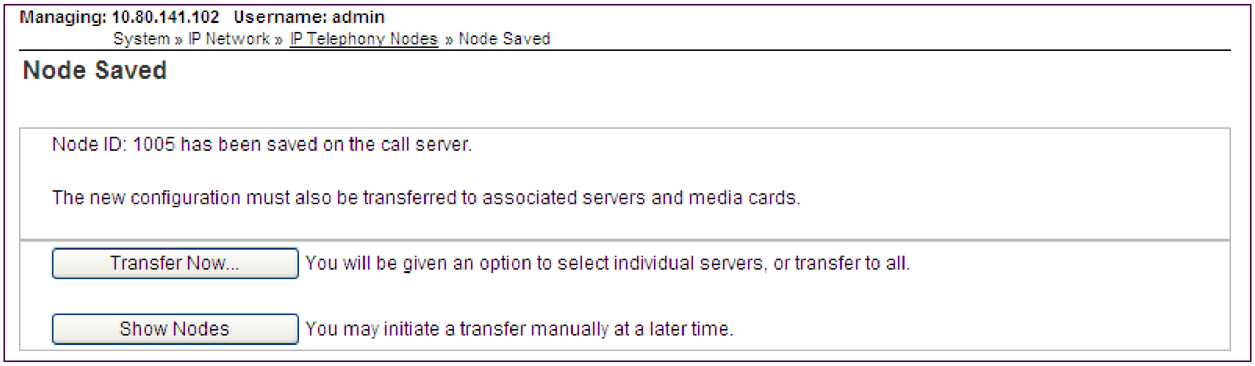


Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen.

5.1.6. Synchronize Node Configuration

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

Select **Transfer Now** on the **Node Saved** page.

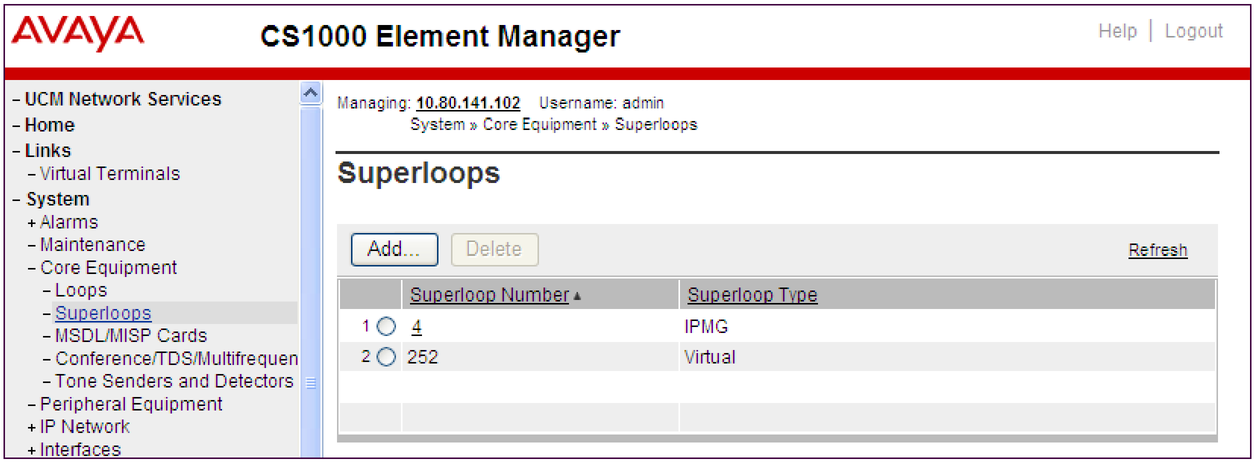


Once the transfer is complete, the **Synchronize Configurations Files (NODE ID <id>)** page is displayed. Place a check mark next to the appropriate **Hostname** and click **Start Sync**. The screen will automatically refresh until the synchronization is finished.

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

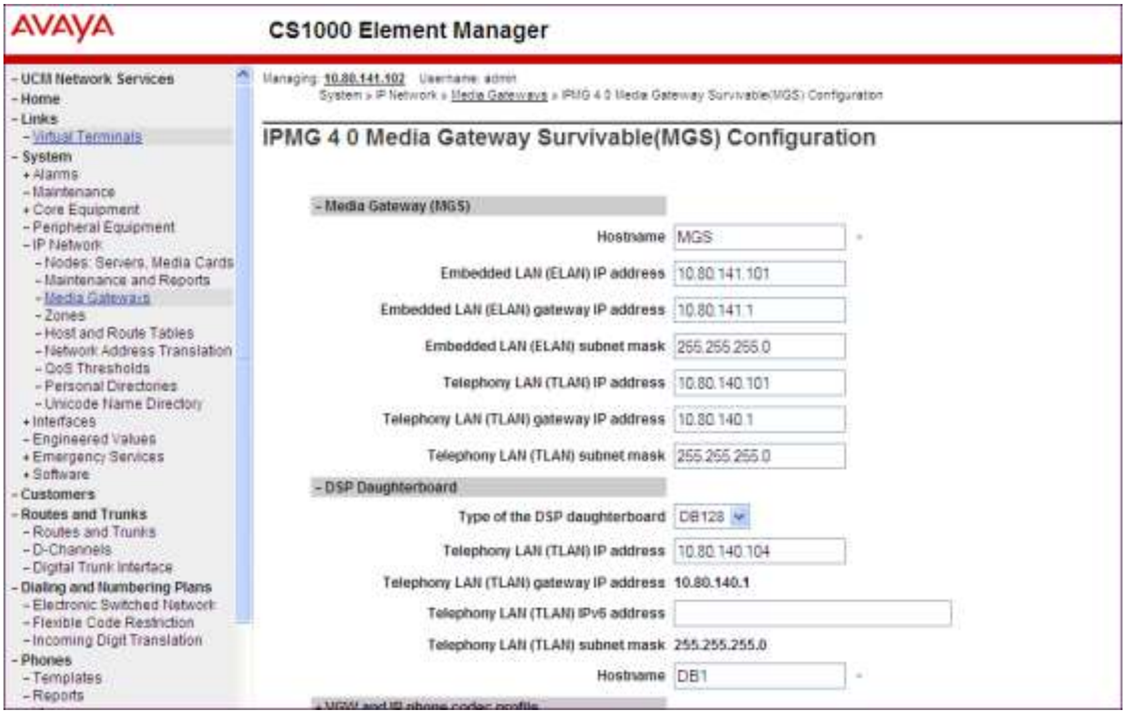
Expand **System → Core Equipments** on the left panel and select **Superloops**. In the sample configuration, Superloop "**4**" is for the Media Gateway and Superloop "**252**" is the virtual Superloop used by the IP phones and SIP trunks.



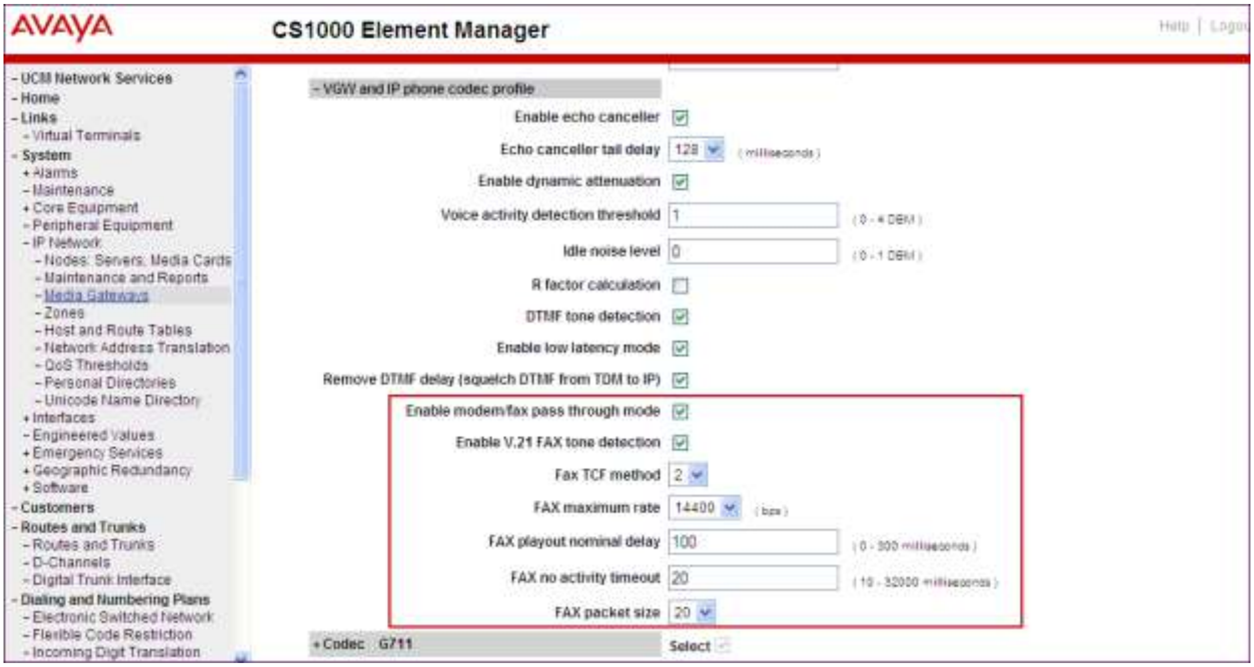
5.3. Media Gateway

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.

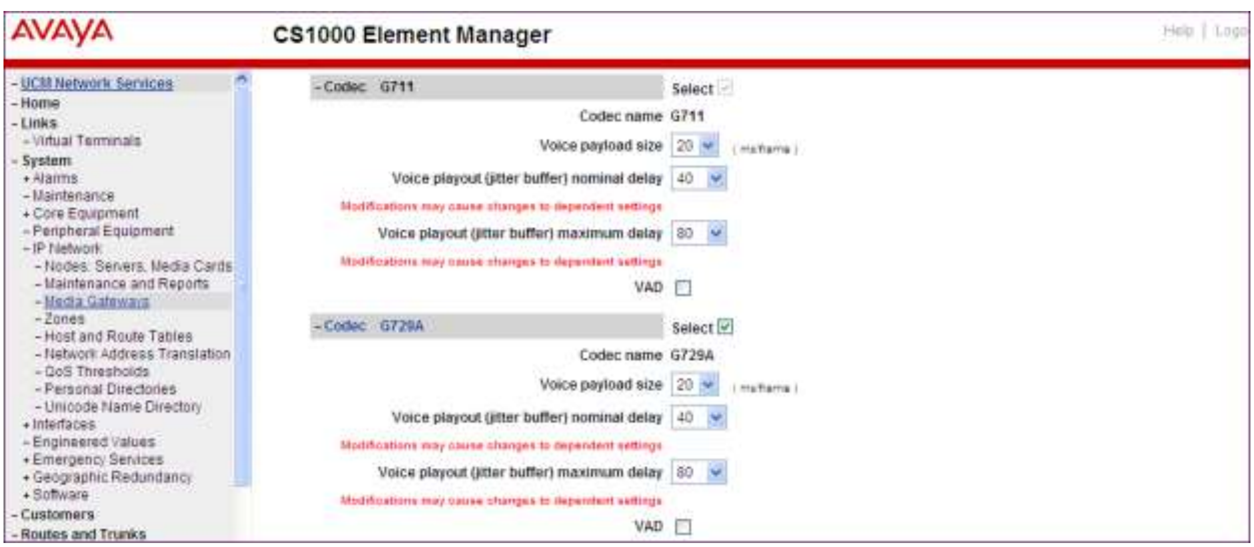
The **IPMG 4 0 Media Gateway Survivable (MGS) Configuration** window appears. The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard 1** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for a call from a digital telephone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



Scroll down to the area of the screen containing **VGW and IP phone codec profile** and expand it. The fax T.38 settings used for compliance testing are 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 Verizon IP Trunk Service for both G.729A and G.711. Click **Save** (not shown) at the bottom of the window. Then click **OK** in the dialog box (not shown) to save the IPMG configuration. Scroll down and click **Save** and then click **OK** on the new dialog box that appears to save the configuration.



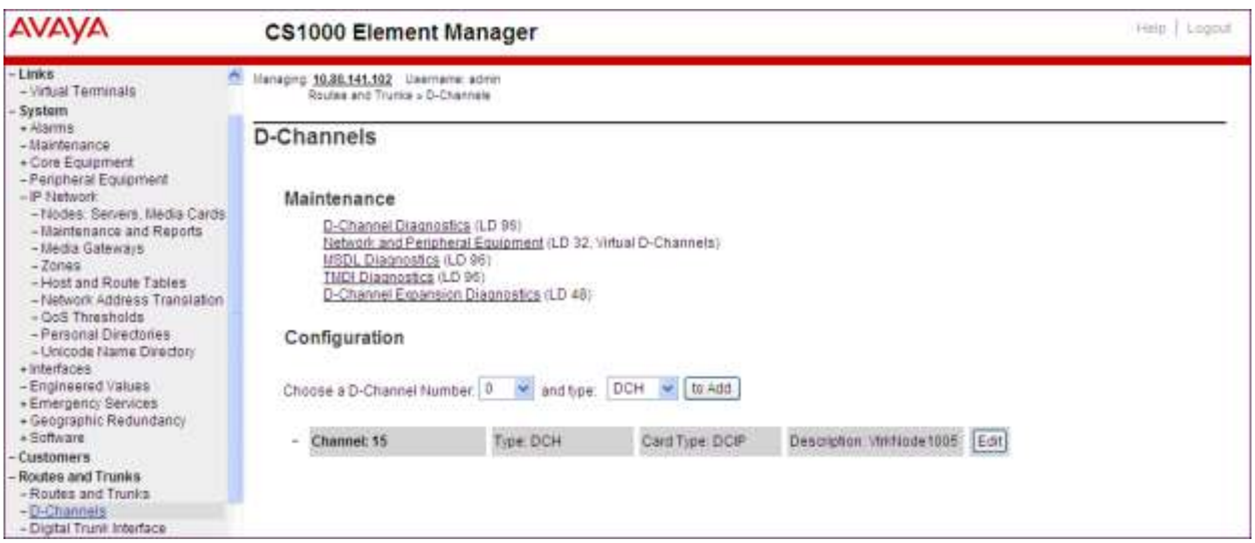
After the configuration is saved, the **Media Gateways** page is displayed. Select the appropriate Media Gateway and click **Reboot** to load the new configuration.

5.4. Virtual D-Channel, Routes and Trunks

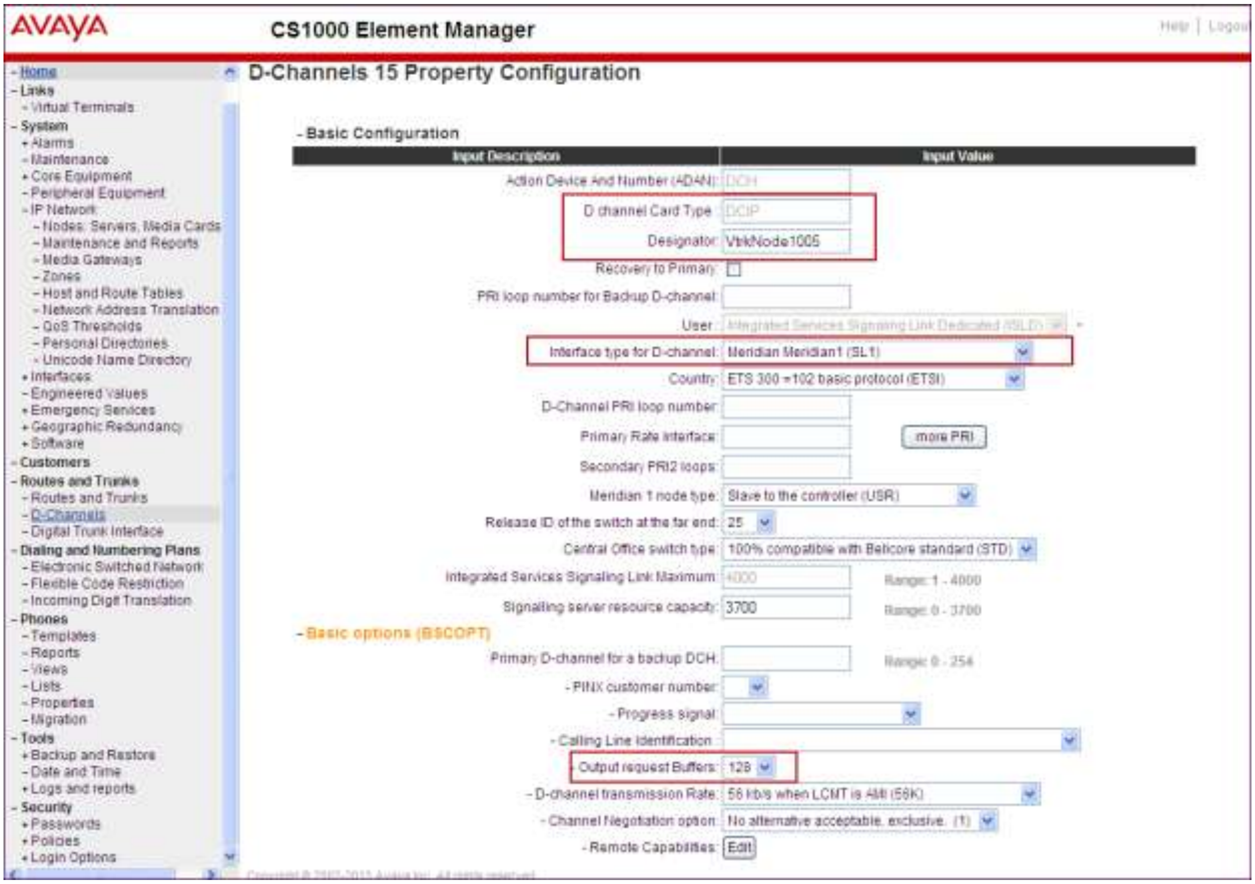
Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server.

5.4.1. Virtual D-Channel Configuration

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

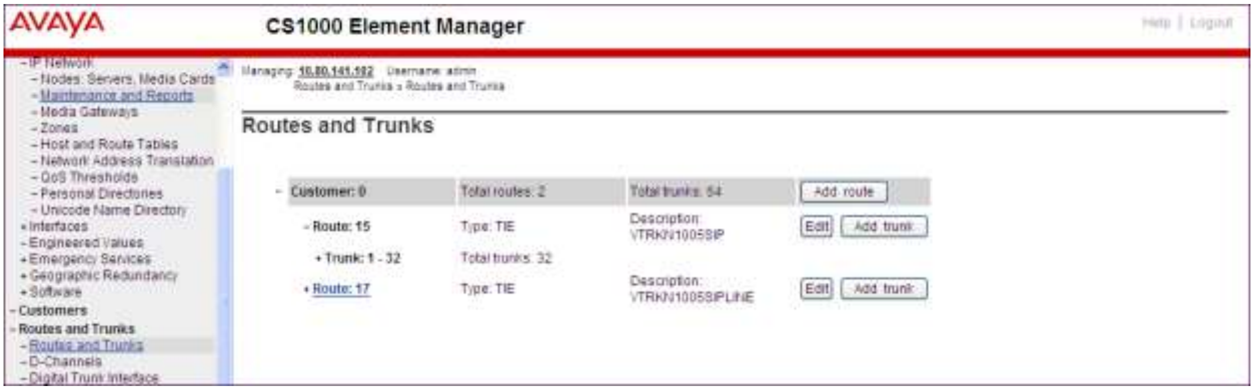


Select **Edit** to verify the configuration, as shown below. Verify “**DCIP**” has been selected for **D Channel Card Type** field and the **Interface type for D-Channel** is set to “**Meridian Meridian 1(SL1)**”. Under the Basic Options section, verify “**128**” is selected for the **Output request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



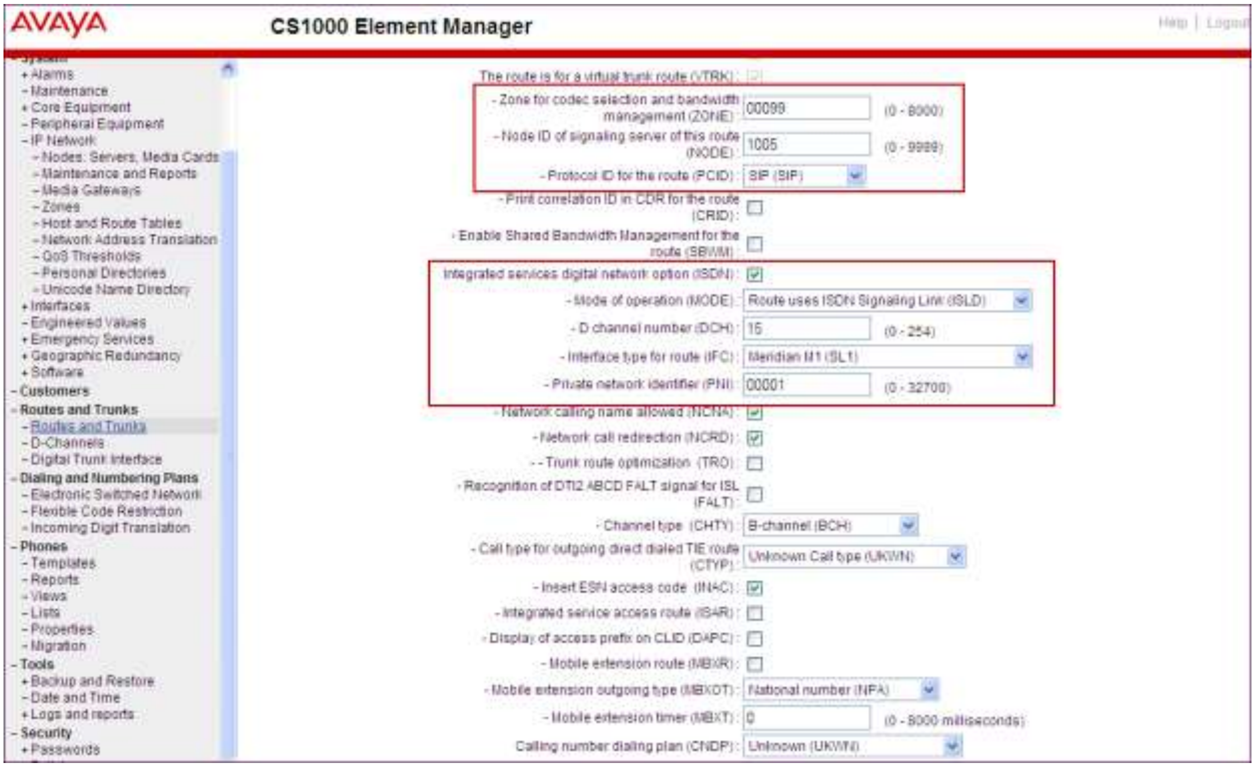
5.4.2. Routes and Trunks Configuration

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

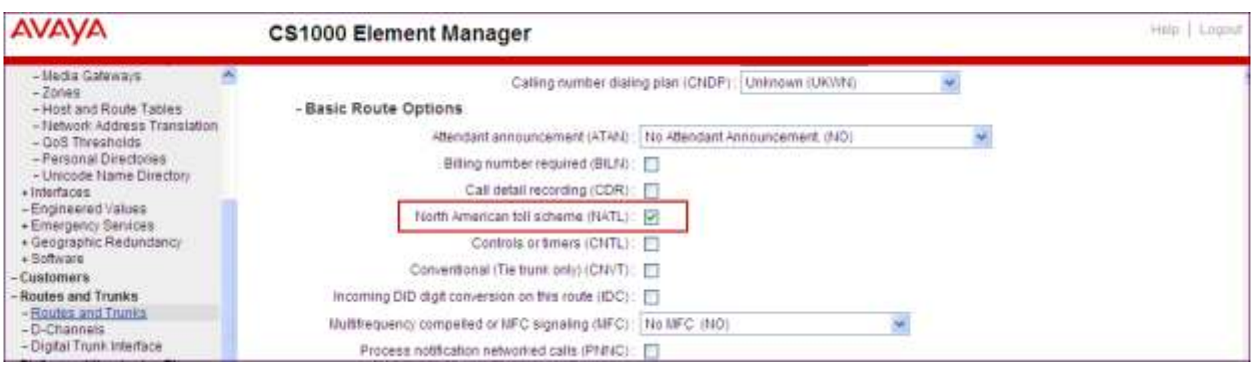


Select **Edit** to verify the configuration, as shown below. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may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

Further down in the **Basic Configuration** section verify the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.1.1**. Also verify “**SIP (SIP)**” has been selected for **Protocol ID for the route (PCID)** field. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging. The **D channel number (DCH)** field must match the D-Channel number shown in **Section 5.4.1**.



Scroll down and expand the **Basic Route Options** section. Check the **North American toll scheme (NATL)**.



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 Verizon IP Trunk Service. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks.

5.5.1. Route List Block

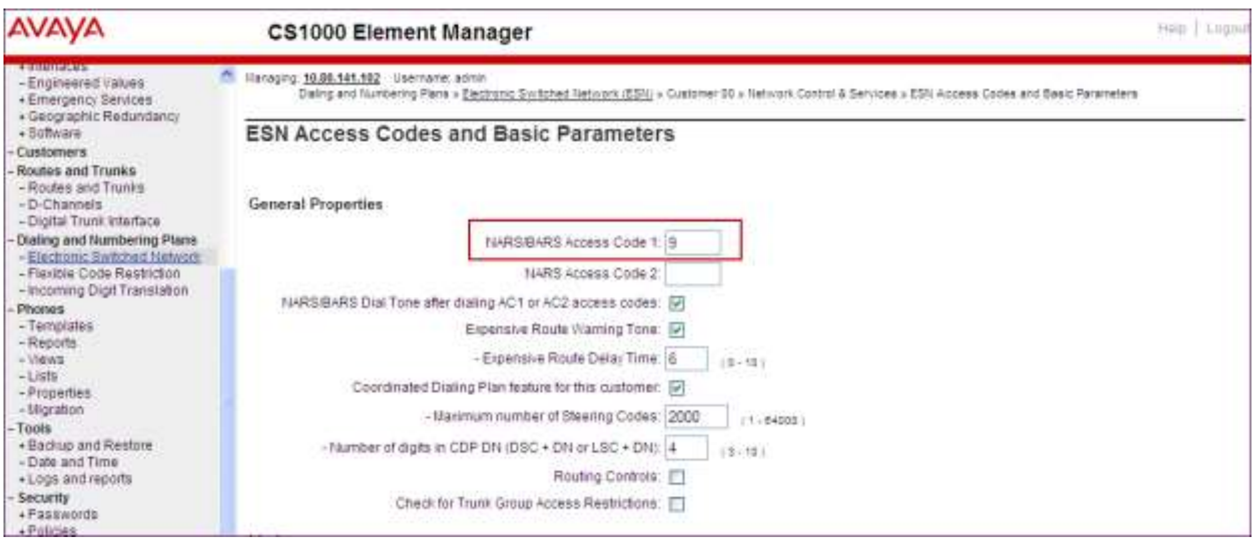
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown below.

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

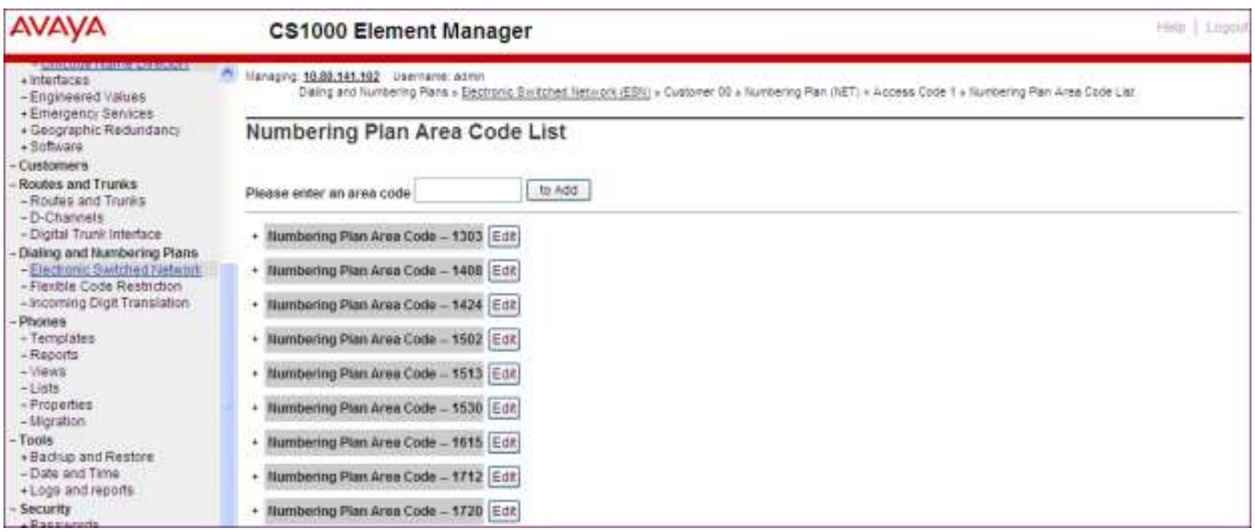
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **ESN Access Codes and Parameters (ESN)**. Although not repeated below, this link can be observed in the first screen in **Section 5.5.1**. In the **NARS/BARS Access Code 1** field, enter the number the user will dial before the target PSTN number. In the sample configuration, the single digit "**9**" was used.



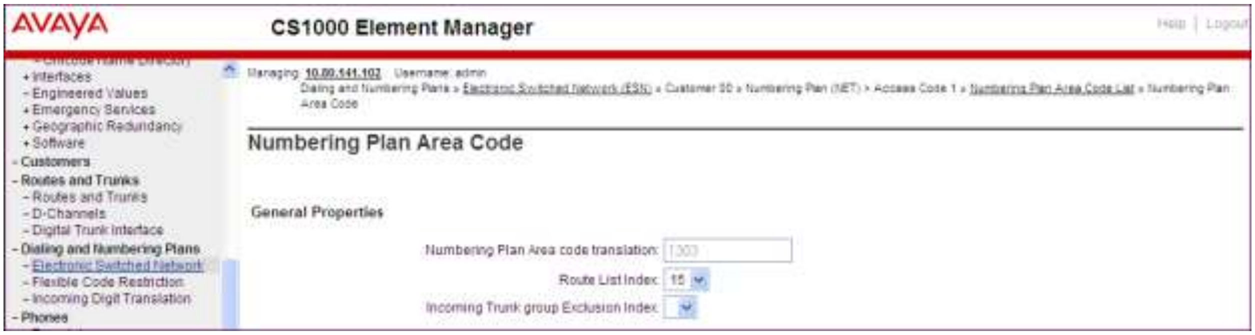
5.5.3. Numbering Plan Area Codes

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 **1408** 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.

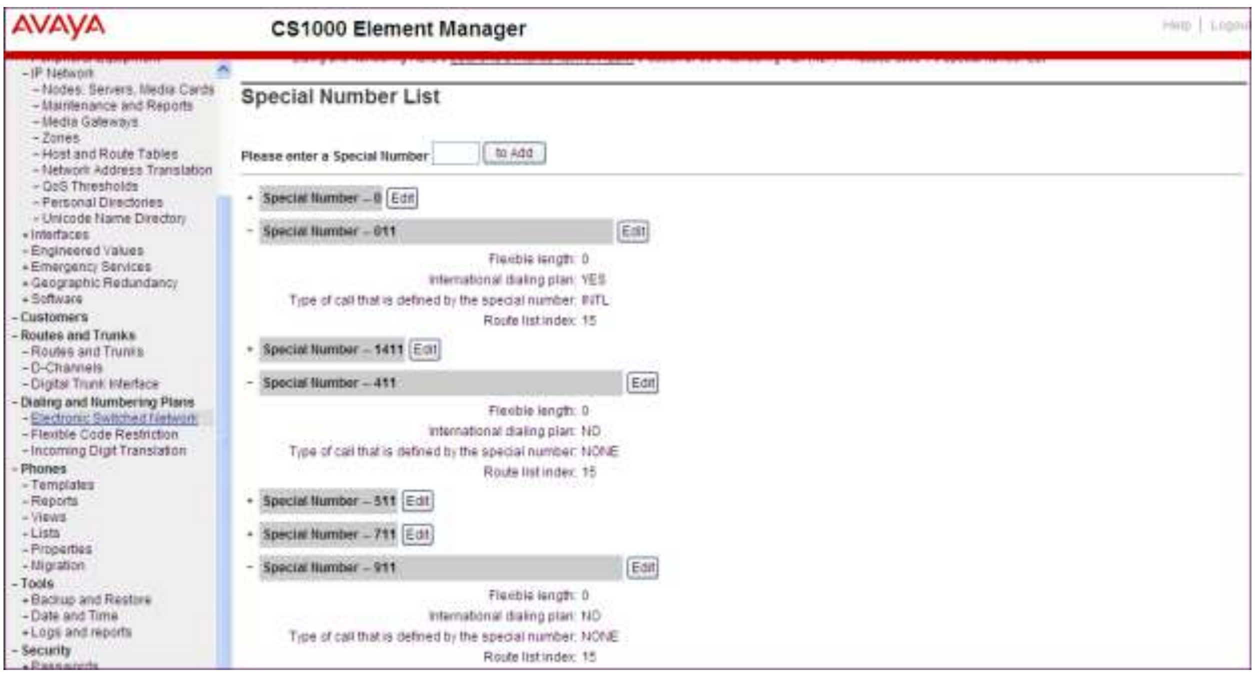


5.5.4. Special Numbers to Route to Session Manager

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 Verizon IP Trunk Service. Although not intended to be prescriptive, one approach to such routing is summarized in this section.

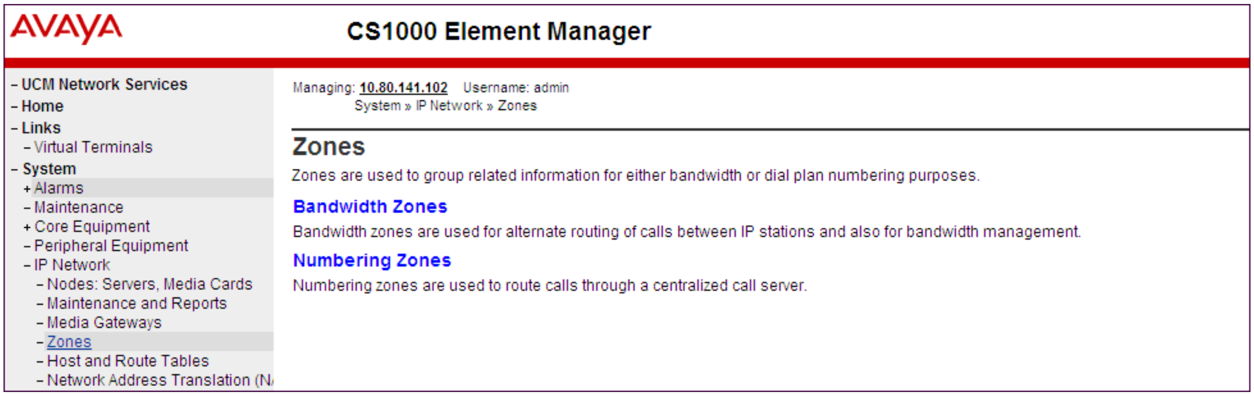
Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Special Number (SPN)** under the appropriate access code heading (as can be observed in the first screen in **Section 5.5.3**).

Add a new number by entering it in the **Please enter a Special Number** box and click **to Add** or click **Edit** to view or change a special number that has 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 for each Special Number in the same manner as shown for the NPAs in the prior section.

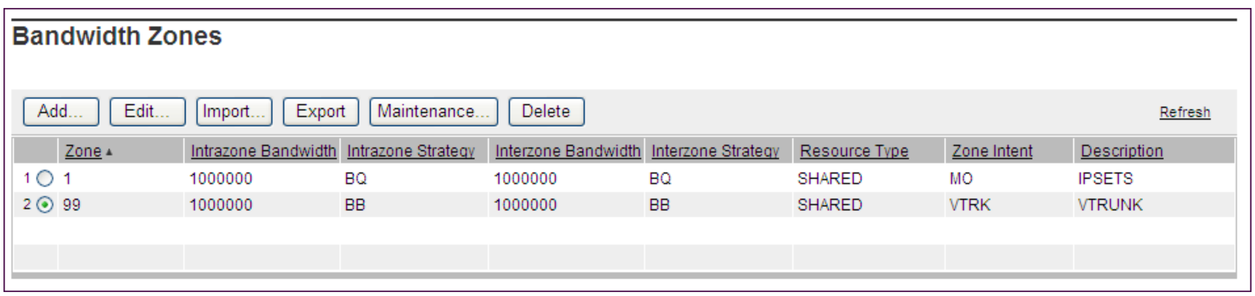


5.6. Zones and Bandwidth

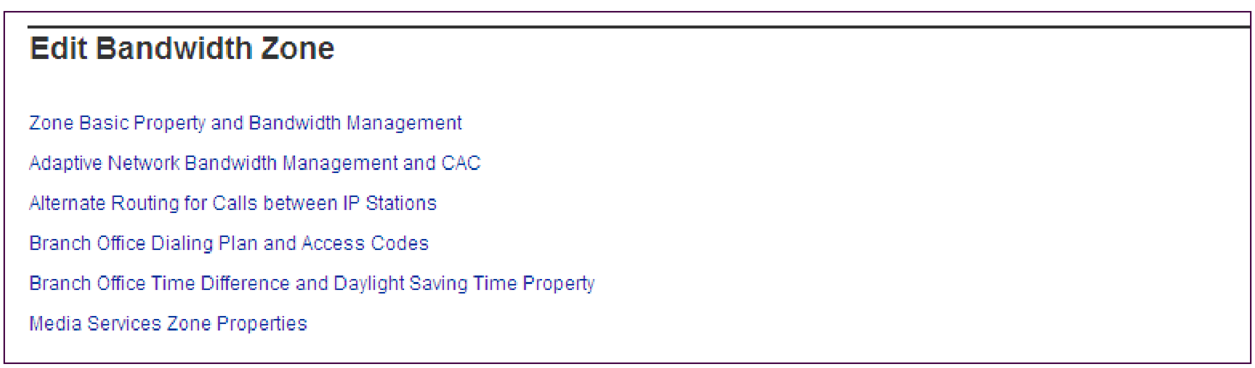
Zone configuration can be used to control codec selection and for bandwidth management. To configure, expand **System → IP Network** on the left panel and select **Zones** as shown below.



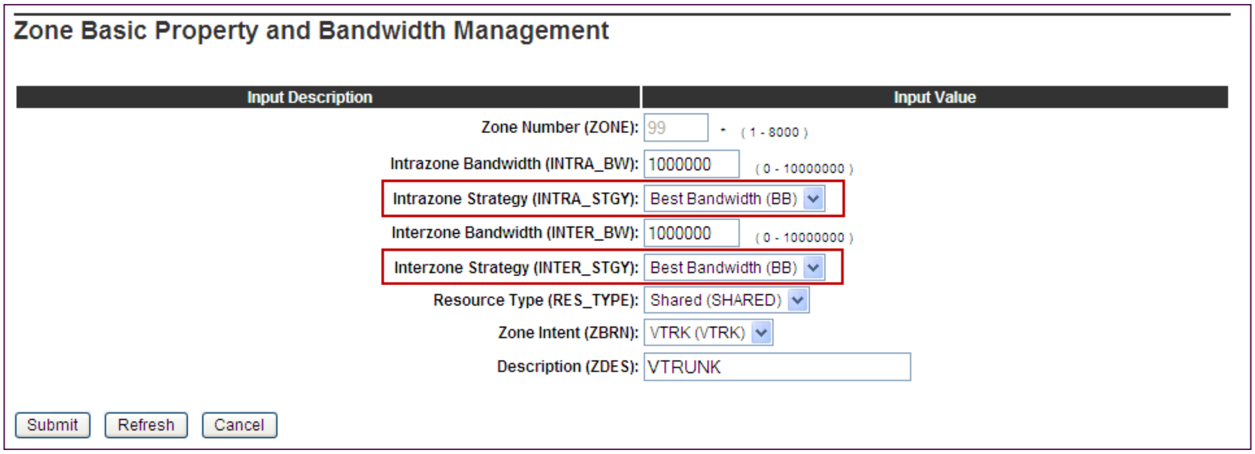
Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured. In production environments, it is likely that more zones will be required. Select the zone associated with the virtual trunk to Session Manager and click **Edit** as shown below. In the sample configuration, this is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



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



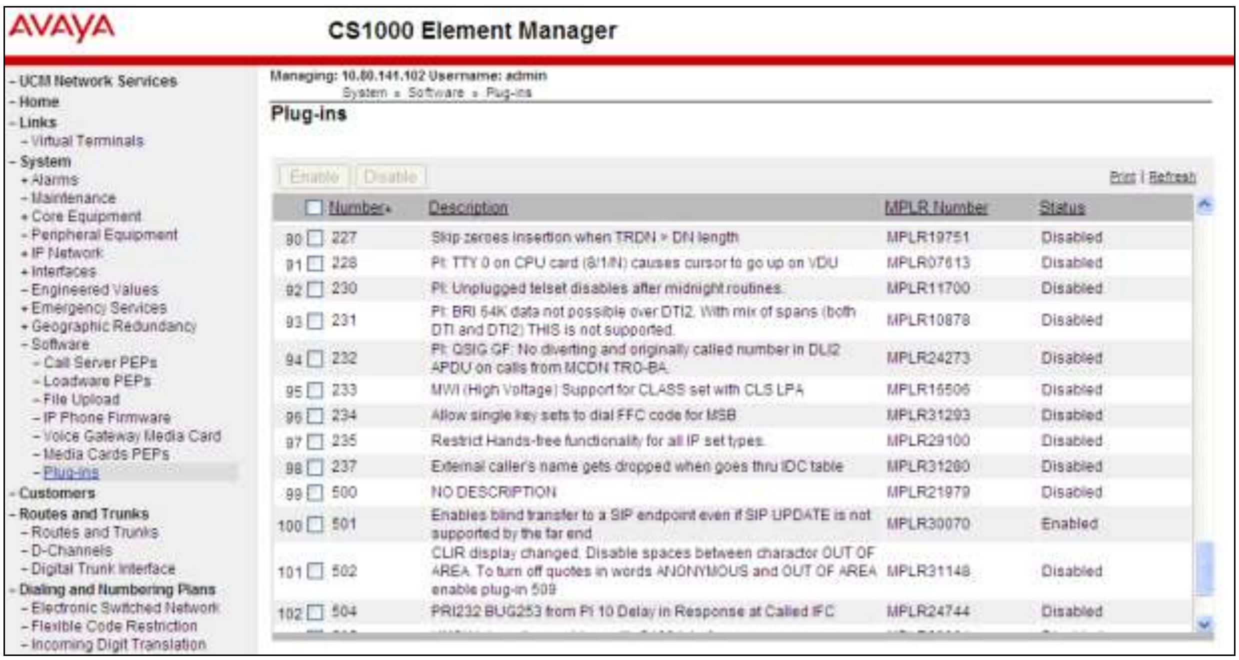
The following screen shows the Zone 99 configuration. Note that "**Best Bandwidth (BB)"** is selected for the zone strategy parameters so that codec G.729A is preferred over codec G.711MU for calls with Verizon IP Trunk Service.



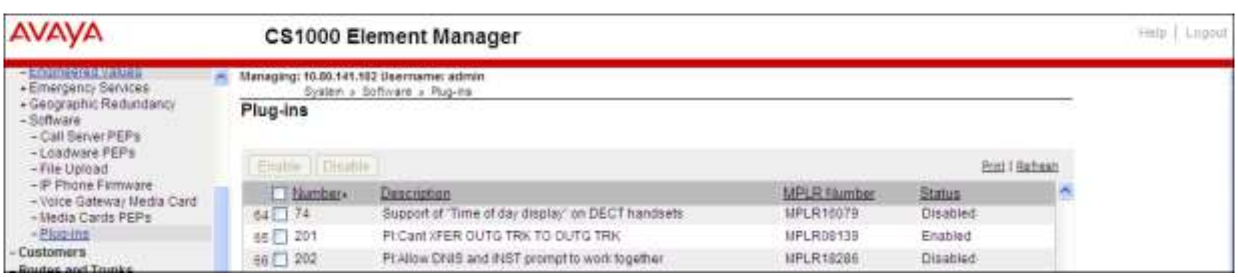
5.7. Enabling Plug-Ins for Call Transfer Scenarios

Plug-ins allow specific CS1000E software feature behaviors to be changed. In the testing associated with these Application Notes, two plug-ins were enabled as shown in this section.

To view or enable a plug-in, from the left navigation menu, expand **System → Software**, and select **Plug-ins**. In the right side screen, a list of available plug-ins will be displayed along with the associated MPLR Number and Status. Use the scroll bar on the right to scroll down so that Plug-in 501 is displayed as shown in the screen below. If the **Status** is "**Disabled**", select the check-box next to Number 501 and click **Enable** at the top, if it is desirable to allow CS1000E users to complete a call transfer to PSTN destinations via the Verizon IP Trunk Service before the call has been answered by the PSTN user. Note that enabling plug-in 501 will allow the user to complete the transfer while the call is in a ringing state, but no audible ring back tone will be heard after the transfer is complete.



The same procedure may be used to enable plug-in 201 if desired. Plug-in 201 will allow a CS1000E user to make a call to the PSTN using the Verizon IP Trunk Service, and then subsequently perform an attended transfer of the call to another PSTN destination via the Verizon IP Trunk Service.

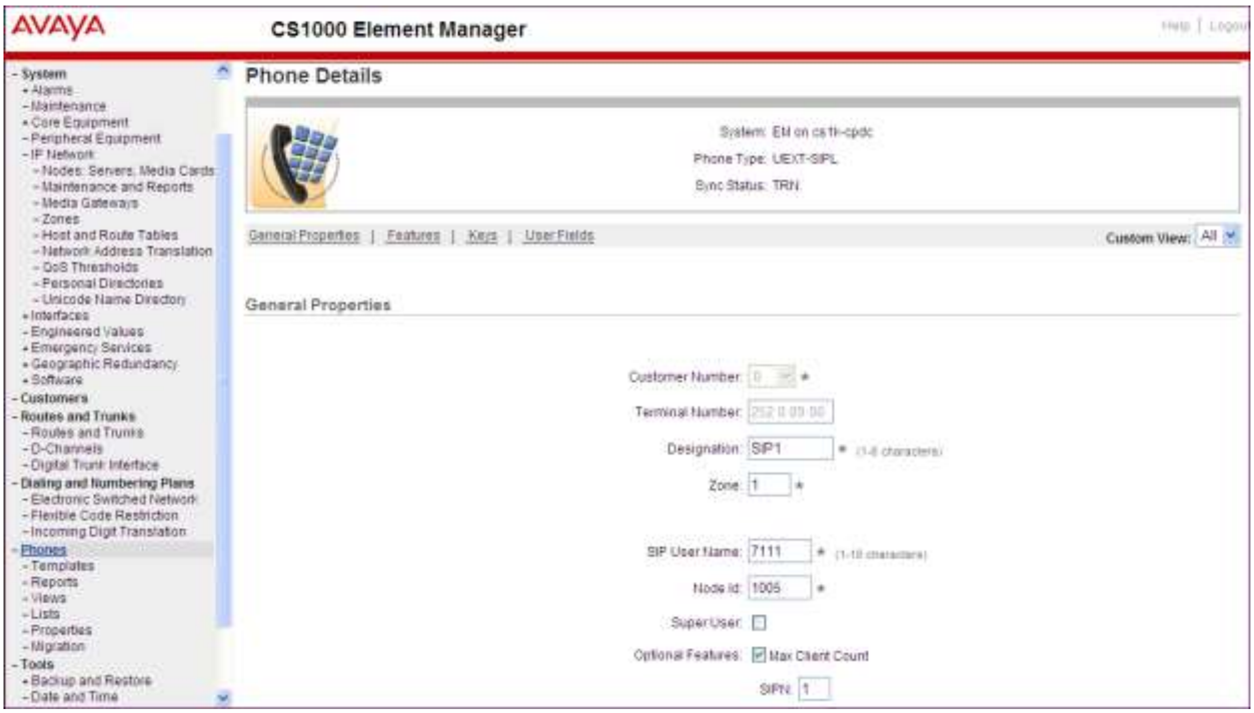


5.8. Example CS1000E Telephone Users

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

5.8.1. Example SIP Phone DN 7111, Codec Considerations

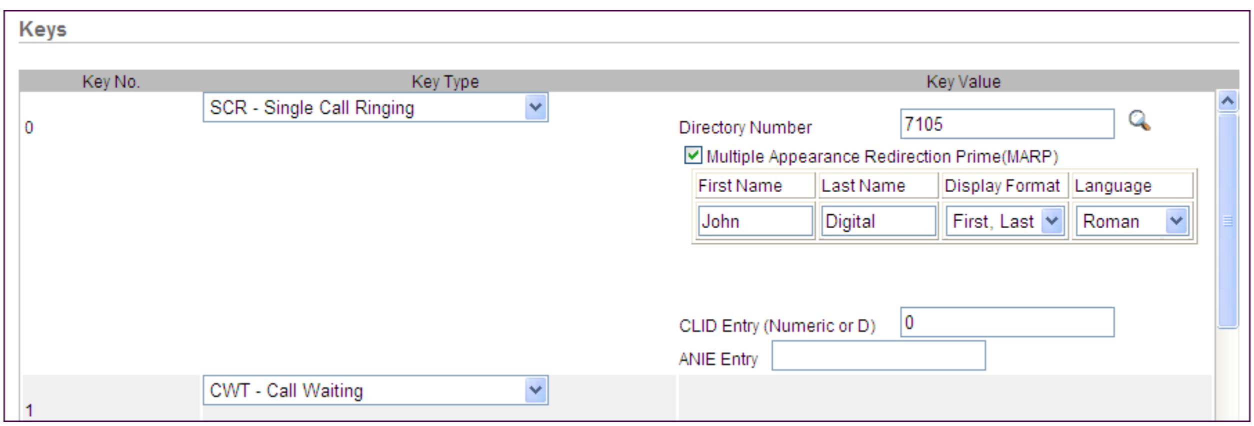
The following screen shows basic information for a SIP phone in the configuration. The telephone is configured as Directory Number 7111. Note that the telephone is in Zone 1 and is associated with Node 1005 (see **Section 5.1**). A call between this telephone and another telephone in Zone 1 will use 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 Verizon IP Trunk Service, the call would use a **best bandwidth** strategy, and the call would use G.729A.



5.8.2. Example Digital Phone DN 7105 with Call Waiting

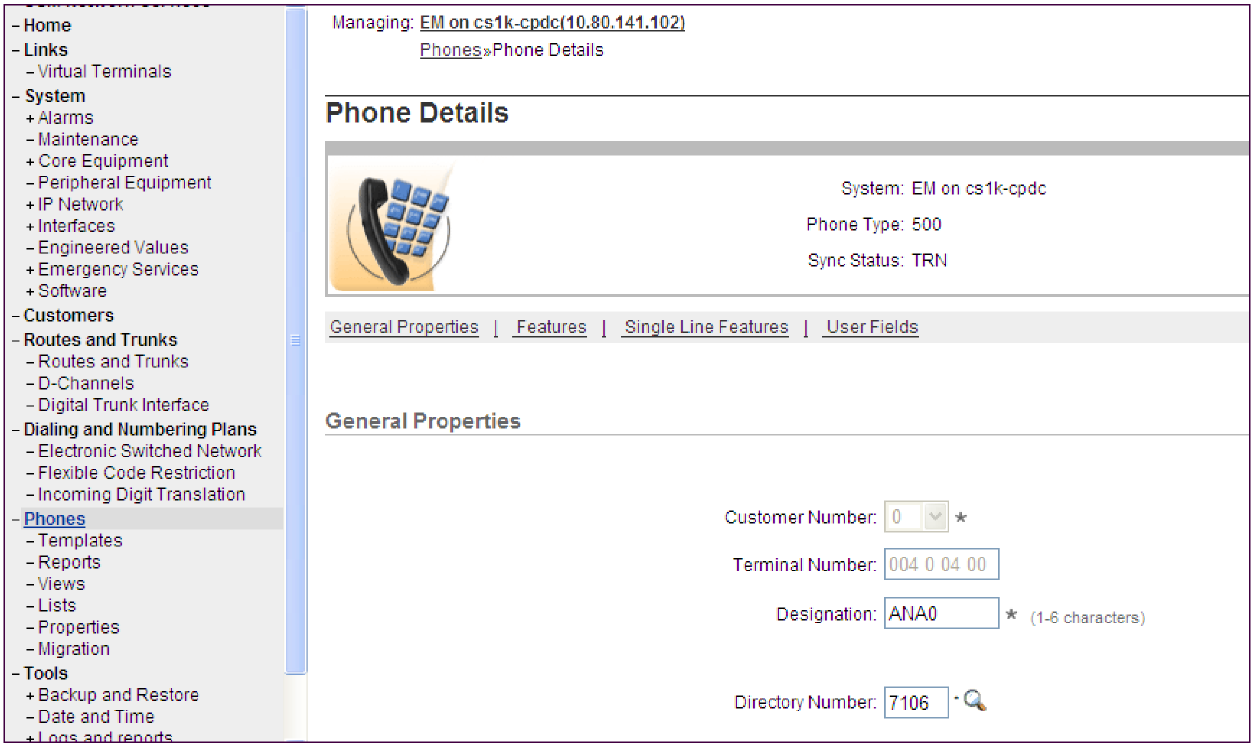
The following screen shows basic information for a digital phone in the configuration. The telephone is configured as Directory Number 7105.

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**".



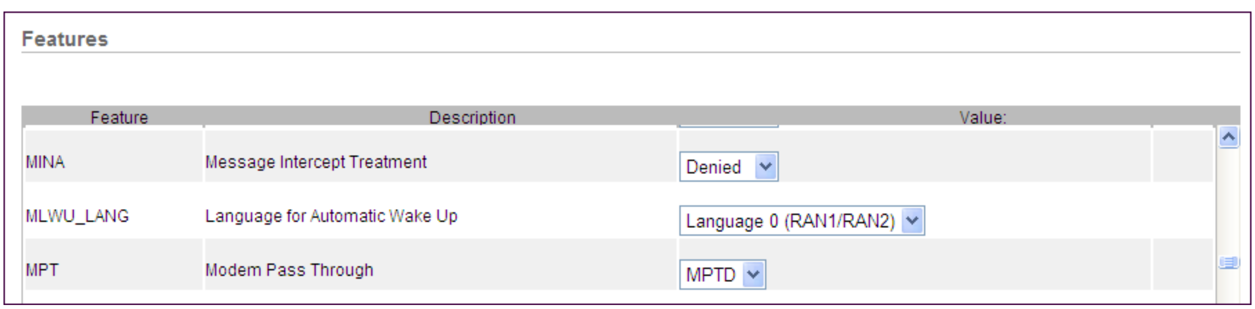
5.8.3. Example Analog Port with DN 7106, Fax

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



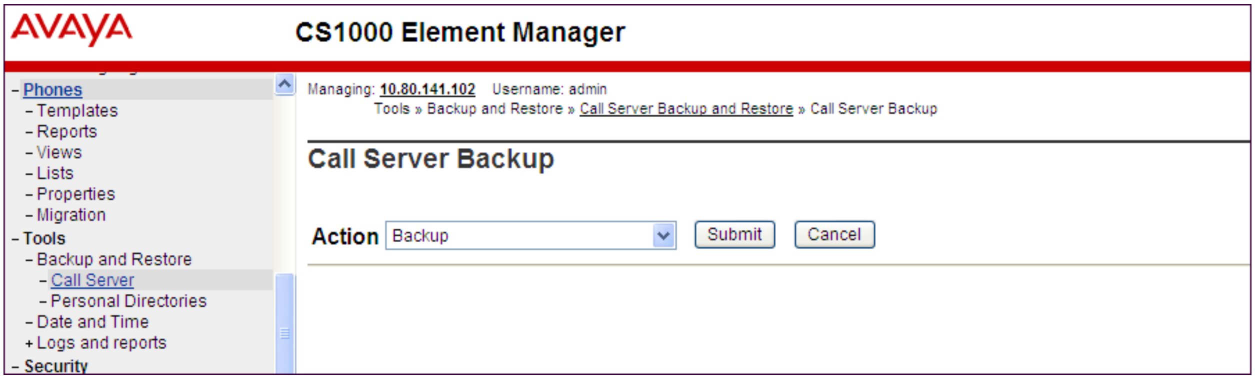
When an analog port is used for a fax machine, Modem Pass Through Allowed (MPTA) can be set to cause G.711 to be used instead of T.38 for fax calls, even if the zone configuration would otherwise have resulted in G.729. For example, if MPTA is configured, and an inbound call arrives from Verizon IP Trunk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

In the sample configuration, **MPTD** was selected to allow for T.38 to be used for outbound fax calls. As noted in **Section 2.2**, Verizon sends a re-Invite to G.711 instead of T.38 after the detection of fax tone. This resulted in outbound fax transmission using G.711.



5.9. Save Configuration

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

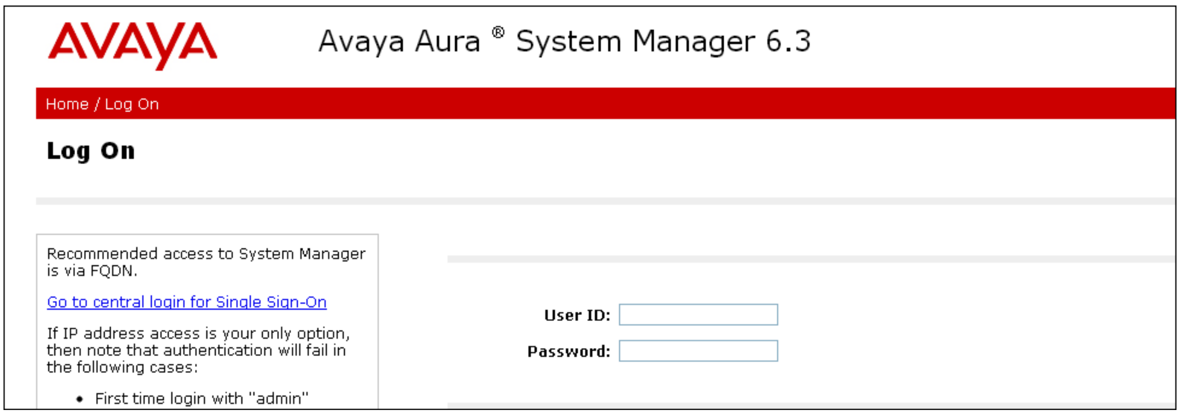


6. Configure Avaya Aura® Session Manager

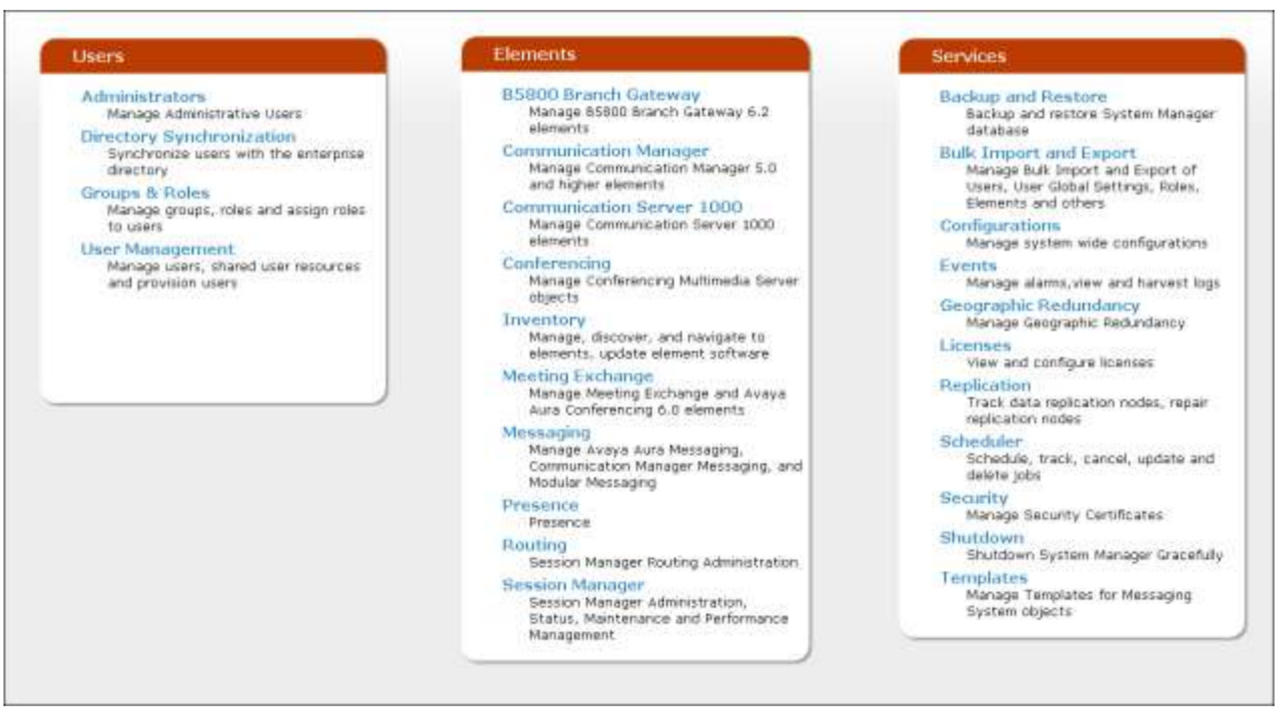
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between System Manager and Session Manager.

Session Manager is managed via System Manager. Using a web browser, access "https://<ip-addr of System Manager>/SMGR". In the **Log On** screen, enter appropriate **User ID** and **Password** and click **Log On** (not shown).



Once logged in, a **Home Screen** is displayed. An abridged **Home Screen** is shown below.

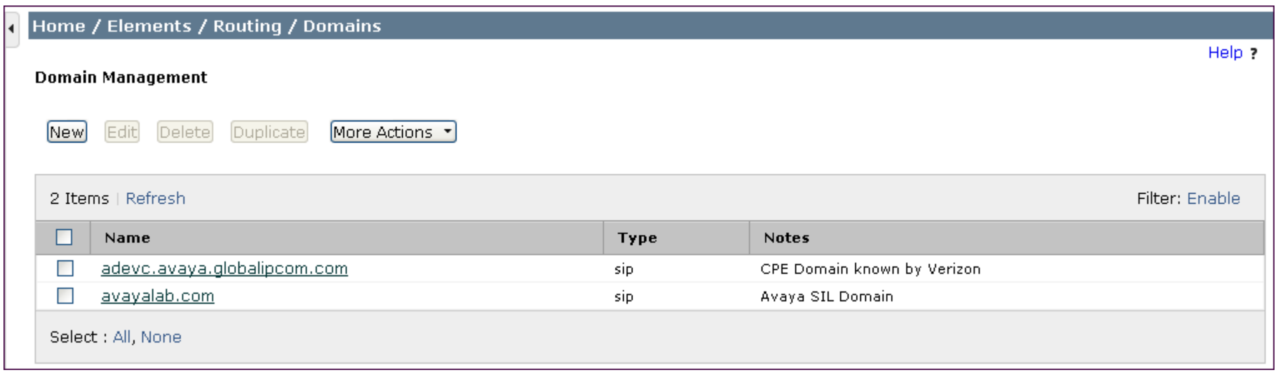


6.1. SIP Domain

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or **New** to add a domain. Click **Commit** (not shown) to save.

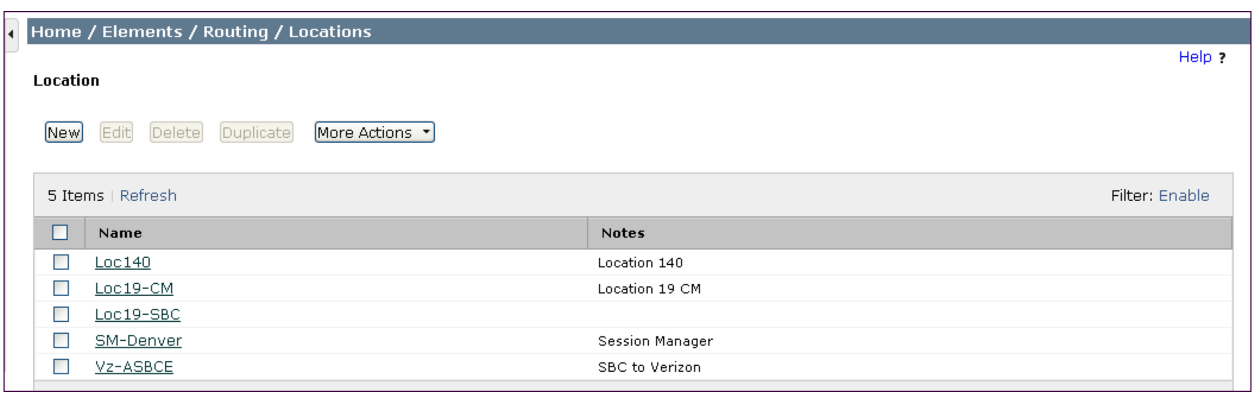
The following screen shows a list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among other Avaya interoperability test efforts. The domain "**avayalab.com**" was used for communication with Avaya SIP Telephones and other Avaya systems and applications. The domain "**avayalab.com**" is not known to the Verizon production service.

The domain "**adevc.avaya.globalipcom.com**" is the domain known to Verizon as the enterprise SIP domain. For example, for calls from the enterprise site to Verizon, this domain can appear in the From and P-Asserted-Identity headers in the INVITE message sent to Verizon.



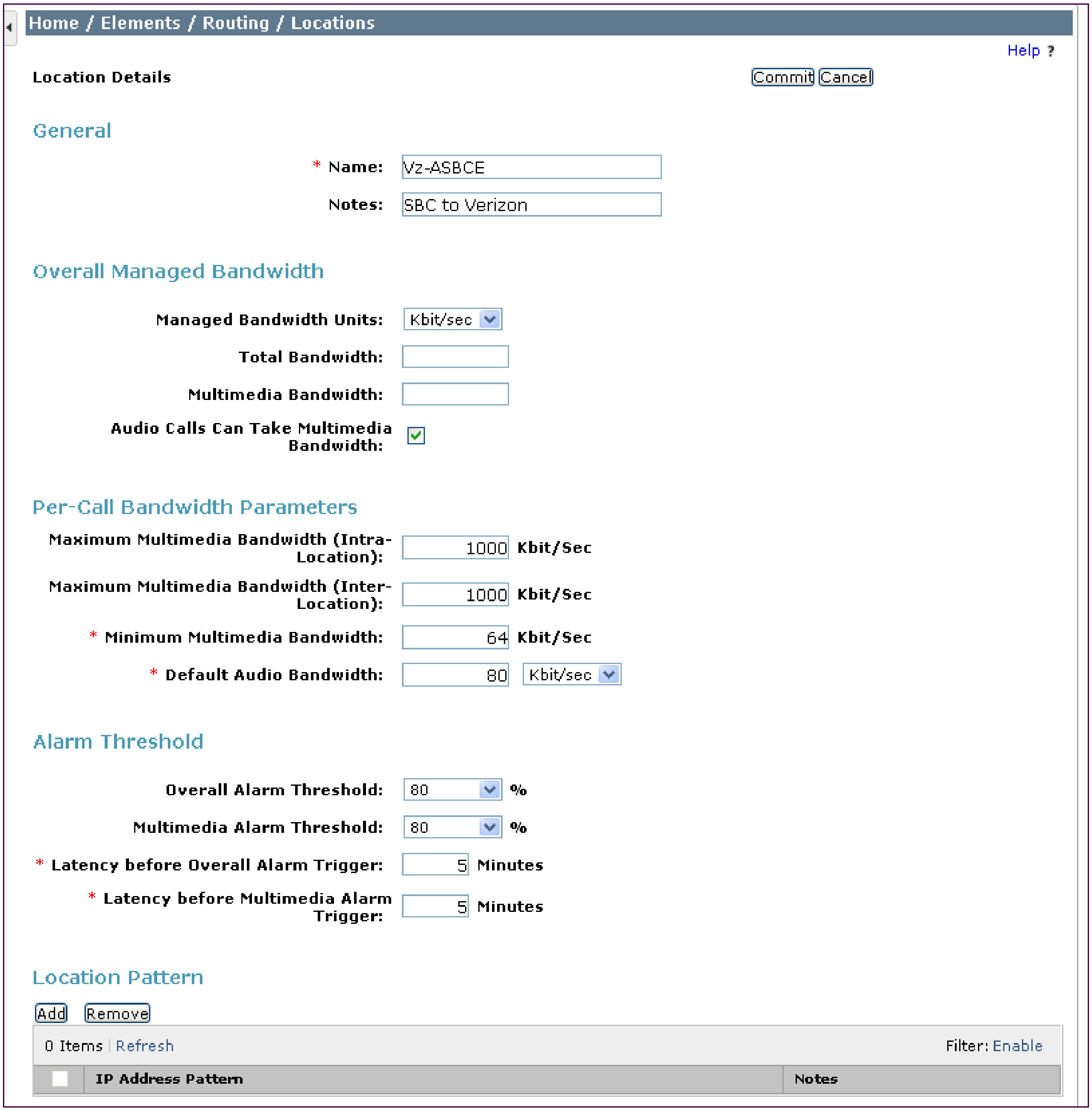
6.2. Locations

To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or **New** to add a location. Click **Commit** save. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.

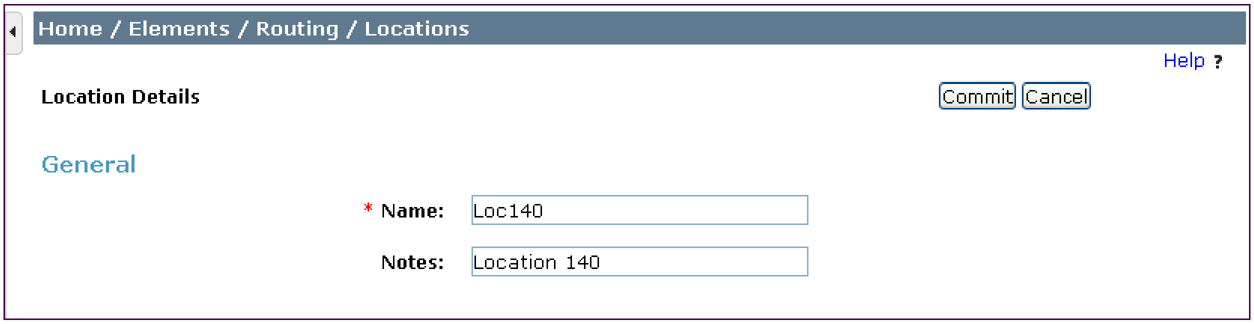


The following screen shows the location details for the location named "**Vz-ASBCE**", corresponding to the Avaya SBCE relevant to these Application Notes. Later, the location with name "**Vz-ASBCE**" will be assigned to the corresponding Avaya SBCE SIP Entity.

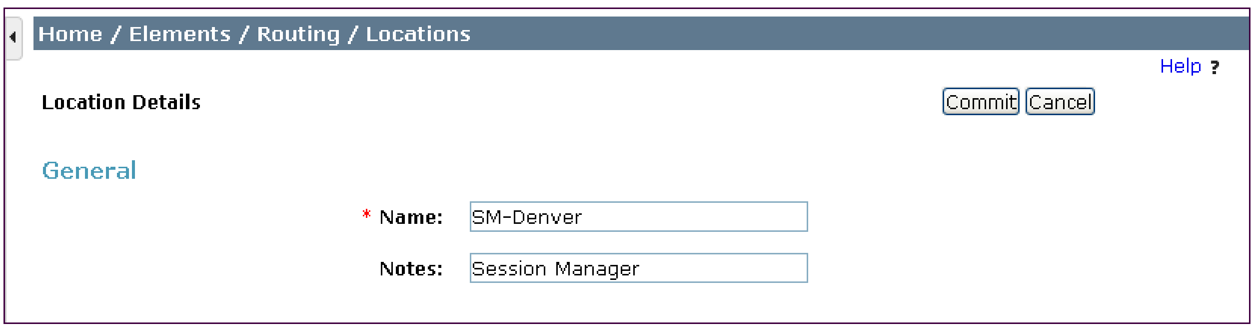
The **Location Pattern** is used to identify call routing based on IP Address. Session Manager matches the IP Address of SIP Entities against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP Address pattern then Session Manager uses the Location administered in the SIP Entity form. In this sample configuration Locations are added to SIP Entities in **Section 6.4**, so it is not necessary to add a pattern.



The following screen shows the location details for the location named "**Loc140**", corresponding to CS1000E. Later, the location with name "**Loc140**" will be assigned to the corresponding CS1000E SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.



The following screen shows the location details for the location named "**SM-Denver**", corresponding to Session Manager. This location was created during the installation of Session Manager and was assigned to the Session Manager SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.



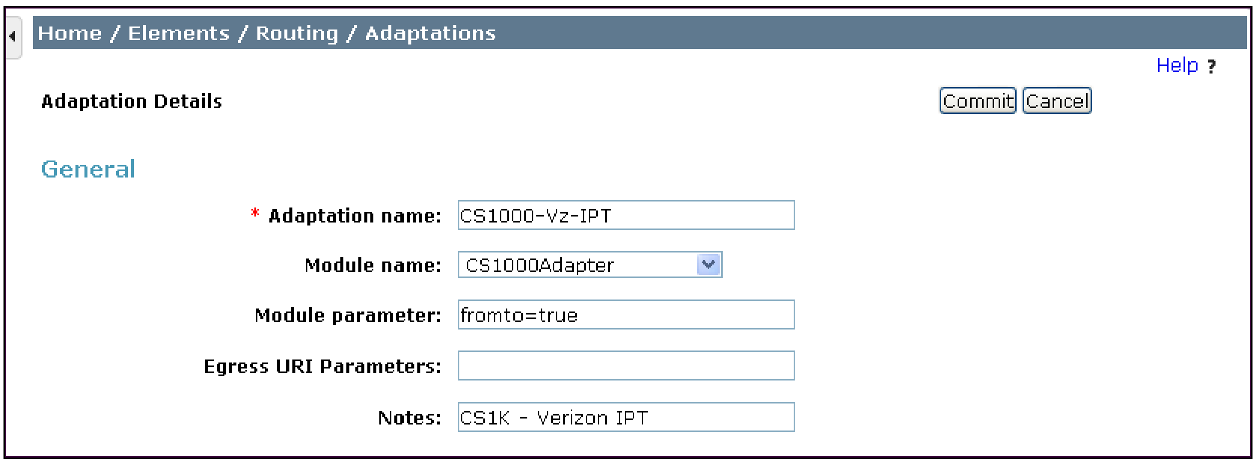
6.3. Adaptations

Session Manager can be configured to use an Adaptation Module designed for CS1000E to convert SIP headers in messages sent by CS1000E to the format used by other Avaya products and endpoints.

6.3.1. Adaptation for Avaya Communication Server 1000E Entity

Navigate to **Routing → Adaptations** 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 and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., "**CS1000-Vz-IPT**")
- **Module Name:** Select "**CS1000Adapter**" from drop-down menu (or add an adapter with name "CS1000Adapter" if not previously defined)
- **Module parameter:** Enter "**fromto=true**" to allow the From and To headers to be modified by Session Manager



Scrolling down, in the **Digit Conversion for Outgoing Calls to SM** section, click **Add** to configure entries for calls from Verizon to CS1000E users. The text below and the screen example that follows explain how to use Session Manager to convert between Verizon DID numbers and corresponding CS1000E directory numbers.

- **Matching Pattern:** Enter Verizon DID number (or number ranges via wildcard pattern matching)
- **Min:** Enter minimum number of digits (e.g., 10)
- **Max:** Enter maximum number of digits (e.g., 10)
- **Delete Digits:** Enter "**10**", as digits should be removed from dialed number before routing by Session Manager
- **Insert Digits:** Enter the CS1000E extension corresponding to the matched extension
- **Address to modify** Select "**destination**"

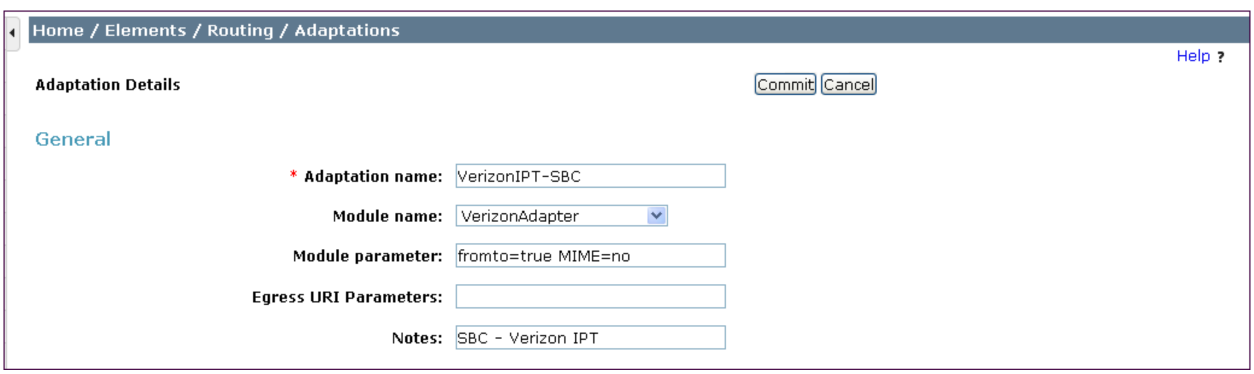
Click **Commit** to save the adaptation.

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	7329450239	10	10		10	7109	destination		
	7329450285	10	10		10	7105	destination		
	7329450286	10	10		10	7106	destination		
	7329450287	10	10		10	7107	destination		
	7329450288	10	10		10	7111	destination		

6.3.2. Adaptation for Avaya SBCE Entity

Navigate to **Routing → Adaptations** 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 and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., "**VerizonIPT-SBC**")
- **Module Name:** Select "**VerizonAdapter**" from drop-down menu (or add an adapter with name "VerizonAdapter" if not previously defined)
- **Module parameter:** Enter "**fromto=true**" to allow the From and To headers to be modified by Session Manager, and "**MIME=no**" to have Session Manager strip MIME message bodies on egress to the SBC

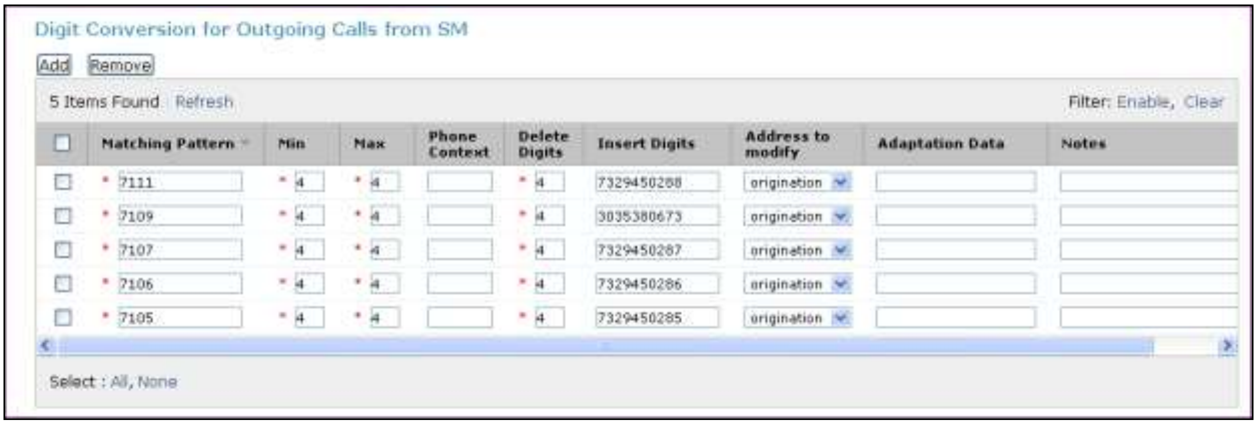


Scrolling down, in the **Digit Conversion for Outgoing Calls to SM** section, click **Add** to configure entries for calls from CS1000E users to Verizon. The text below and the screen example that follows explain how to use Session Manager to convert between CS1000E directory numbers and corresponding Verizon DID numbers.

- **Matching Pattern:** Enter CS1000E extensions (or extension ranges via wildcard pattern matching)
- **Min:** Enter minimum number of digits (e.g., 4)

- **Max:** Enter maximum number of digits (e.g., 4)
- **Delete Digits:** Enter the number of digits in the extension to remove all digits (e.g., 4)
- **Insert Digits:** Enter the Verizon DID corresponding to the matched extension
- **Address to modify:** Select “**origination**”

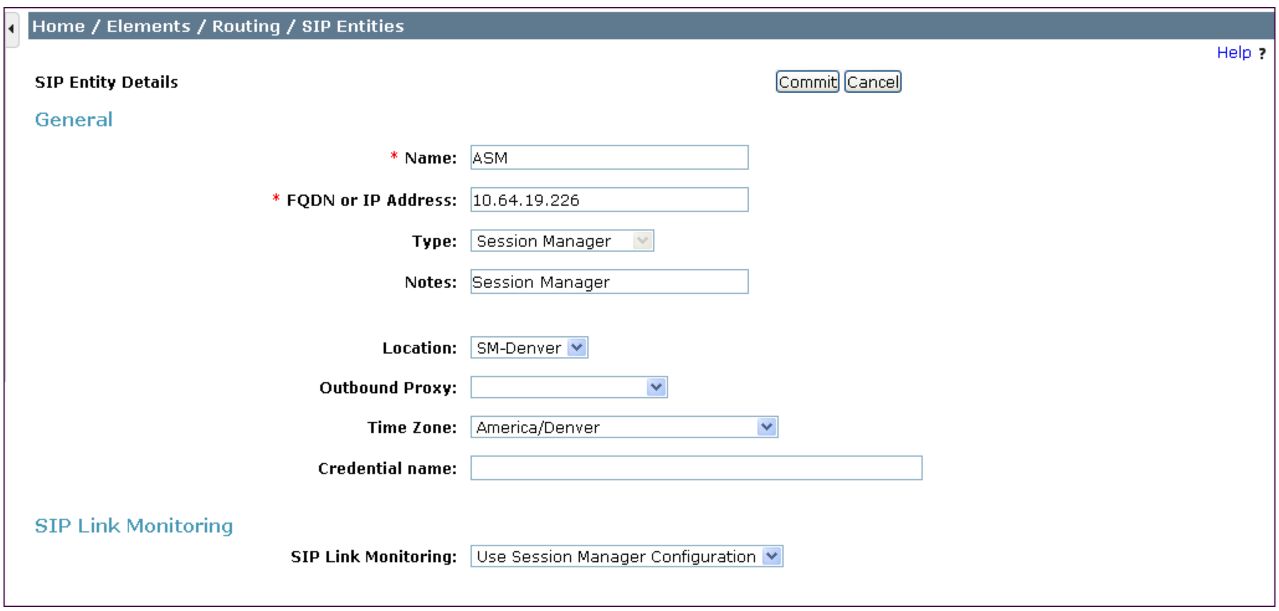
Click **Commit** to save the adaptation.



6.4. SIP Entities

To view or change SIP entities, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or **New** to add an entity. Click **Commit** to save.

The following screen shows the upper portion of the **SIP Entity Details** corresponding to "**ASM**". The **FQDN or IP Address** field for "**ASM**" is the Session Manager Security Module IP Address (**10.64.19.226**), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP entity is "**Session Manager**". Select an appropriate location for the Session Manager from the **Location** drop-down menu. In the shared test environment, the Session Manager used location "**SM-Denver**". The default **SIP Link Monitoring** parameters may be used. Unless changed elsewhere, links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers, configurable at the Session Manager level. If desired, these timers may be customized for each entity.



6.4.1. SIP Entity for Avaya Communication Server 1000E

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:

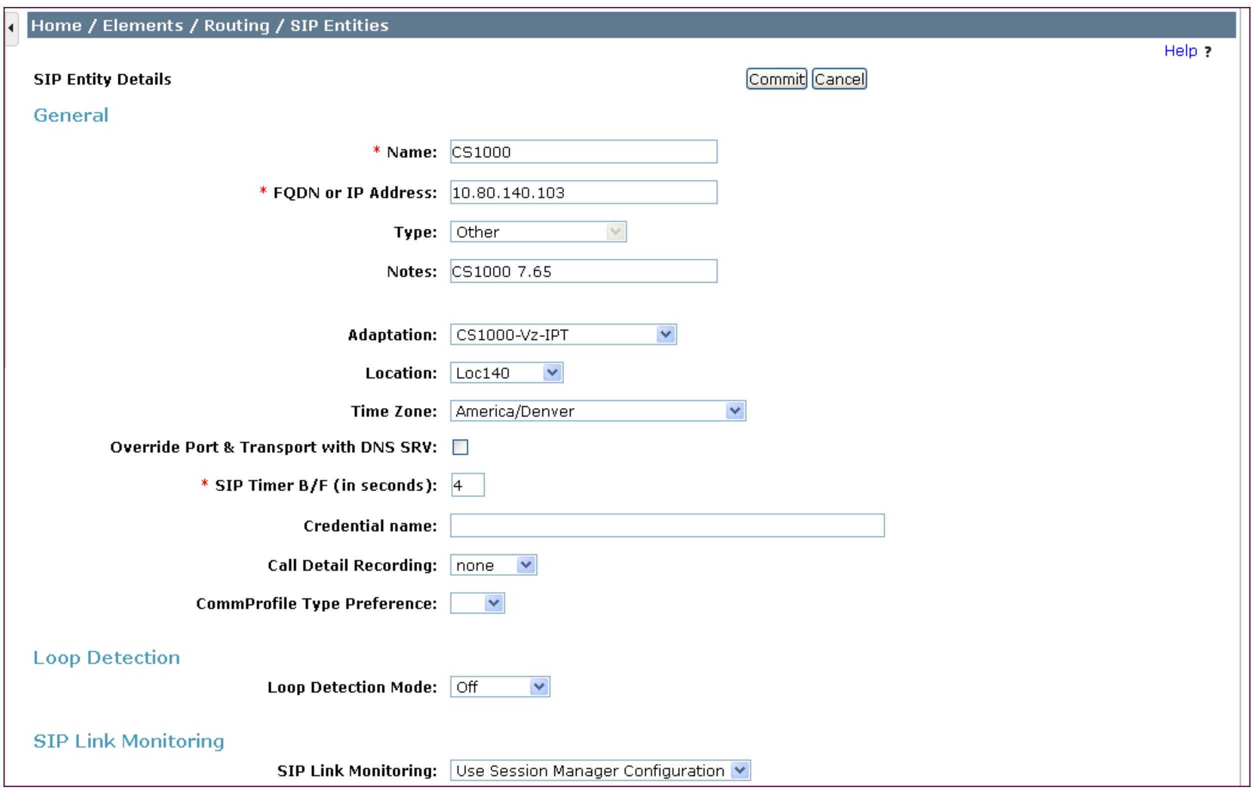
- **Name:** Enter a descriptive name
- **FQDN or IP Address:** Enter the TLAN IP Address of the CS1000E Node
- **Type:** Select "**Other**"
- **Adaptation:** Select the Adaptation Module for the CS1000E
- **Location:** Select the Location for the CS1000E

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Use Session Manager Configuration**" (or choose an alternate Link Monitoring approach for this entity, if desired)

Click **Commit** to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for CS1000E in the sample configuration.



6.4.2. SIP Entity for Avaya SBCE

Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

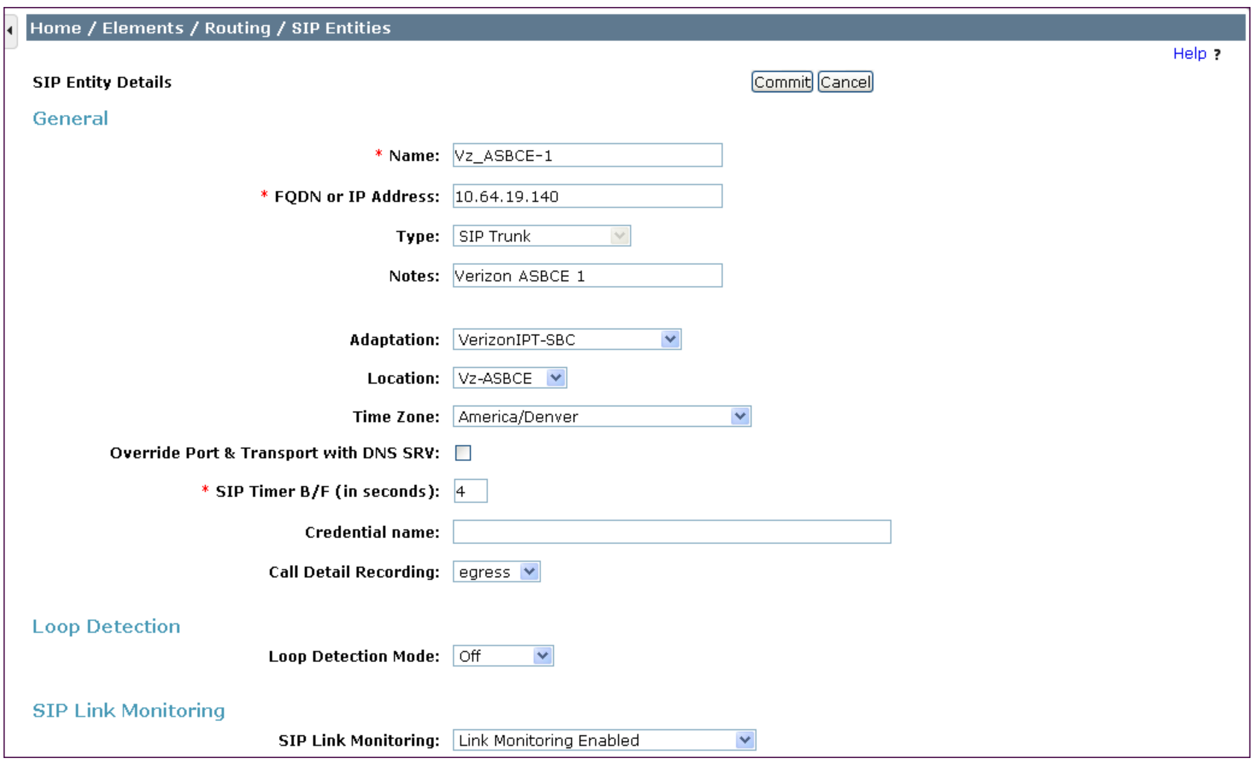
- **Name:** Enter a descriptive name
- **FQDN or IP Address:** Enter the inside IP Address of the Avaya SBCE
- **Type:** Select "**SIP Trunk**"
- **Adaptation:** Select the Adaptation Module for the Avaya SBCE
- **Location:** Select the Location for the Avaya SBCE

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Link Monitoring Enabled**" (or choose an alternate Link Monitoring approach for this entity, if desired)

Click **Commit** to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for Avaya SBCE in the sample configuration.

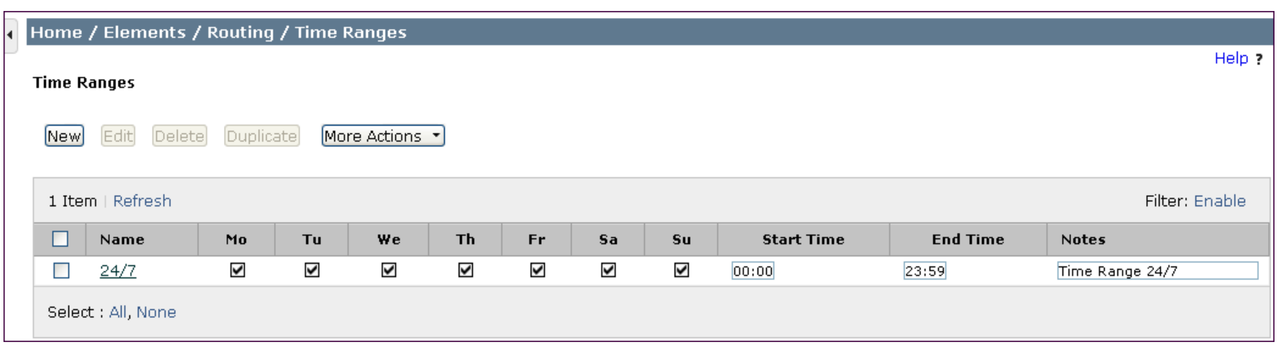


6.5. Entity Links

The SIP trunk between Session Manager and CS1000E is described by an Entity Link, as is the SIP trunk between Session Manager and Avaya SBCE. The following screen shows the two configured links, "**ASM to CS1000**" and "**ASM to Vz_ASBCE-1**". Each link uses the entity named "**ASM**" as **SIP Entity 1**, and the appropriate entity, such as "**CS1000**", for **SIP Entity 2**.

6.6. Time Ranges

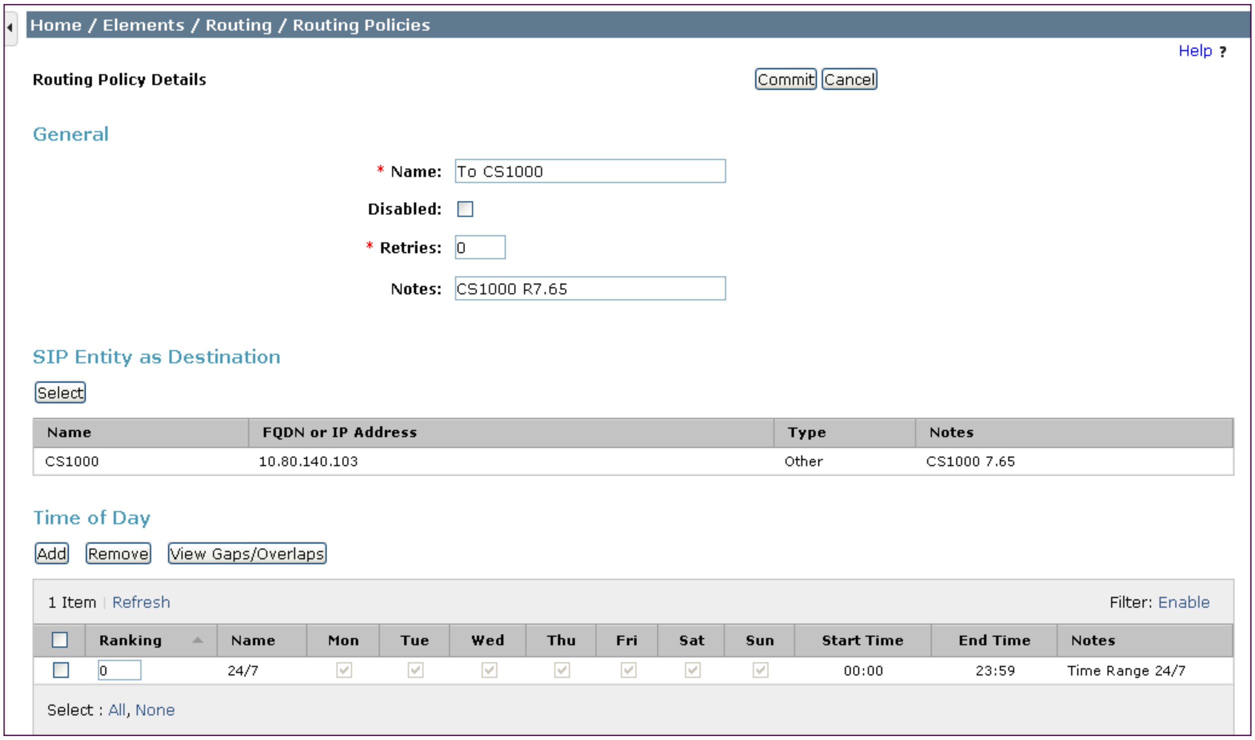
To view or change Time Ranges, select **Routing → Time Ranges**. The Routing Policies shown subsequently will use the "**24/7**" range since time-based routing was not the focus of these Application Notes.



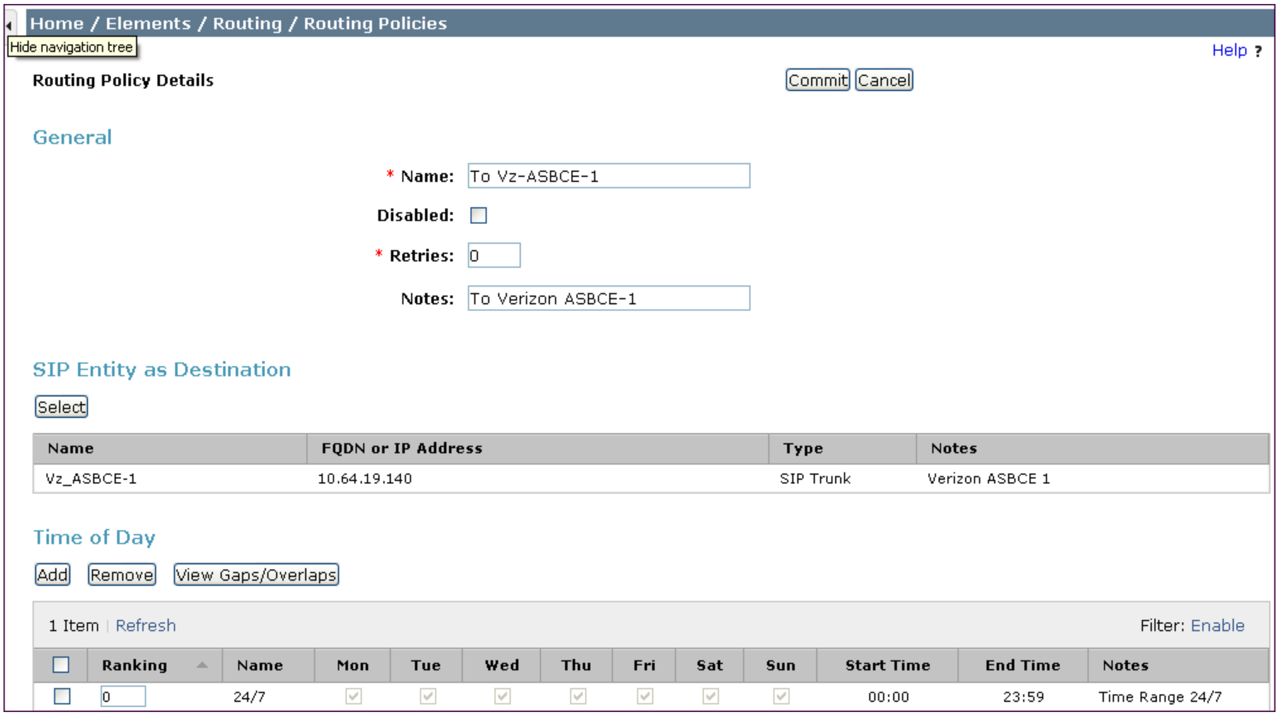
6.7. Routing Policies

To view or change routing policies, select **Routing → Policies**. Click on the checkbox corresponding to the name of a policy and **Edit** to edit an existing policy, or **New** to add a policy. Click **Commit** to save the Routing Policy definition.

The following screen shows the **Routing Policy Details** for the policy named “**To CS1000**” associated with incoming PSTN calls from Verizon to CS1000E. Observe the **SIP Entity as Destination** is the entity named “**CS1000**” that was created in **Section 6.4.1**.



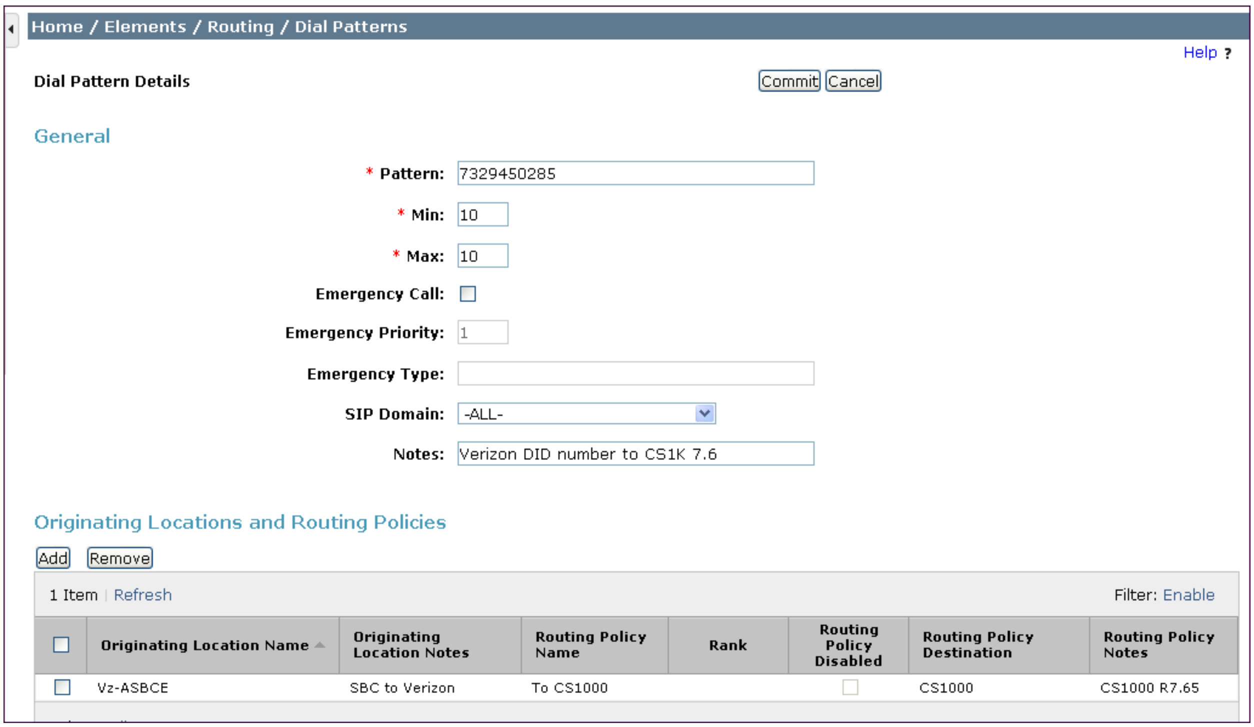
The following screen shows the **Routing Policy Details** for the policy named "**To Vz-ASBCE-1**" associated with outgoing calls from CS1000E to the PSTN via Verizon through Avaya SBCE. Observe the **SIP Entity as Destination** as the entity named "**Vz_ASBCE-1**" that was created in **Section 6.4.2**.



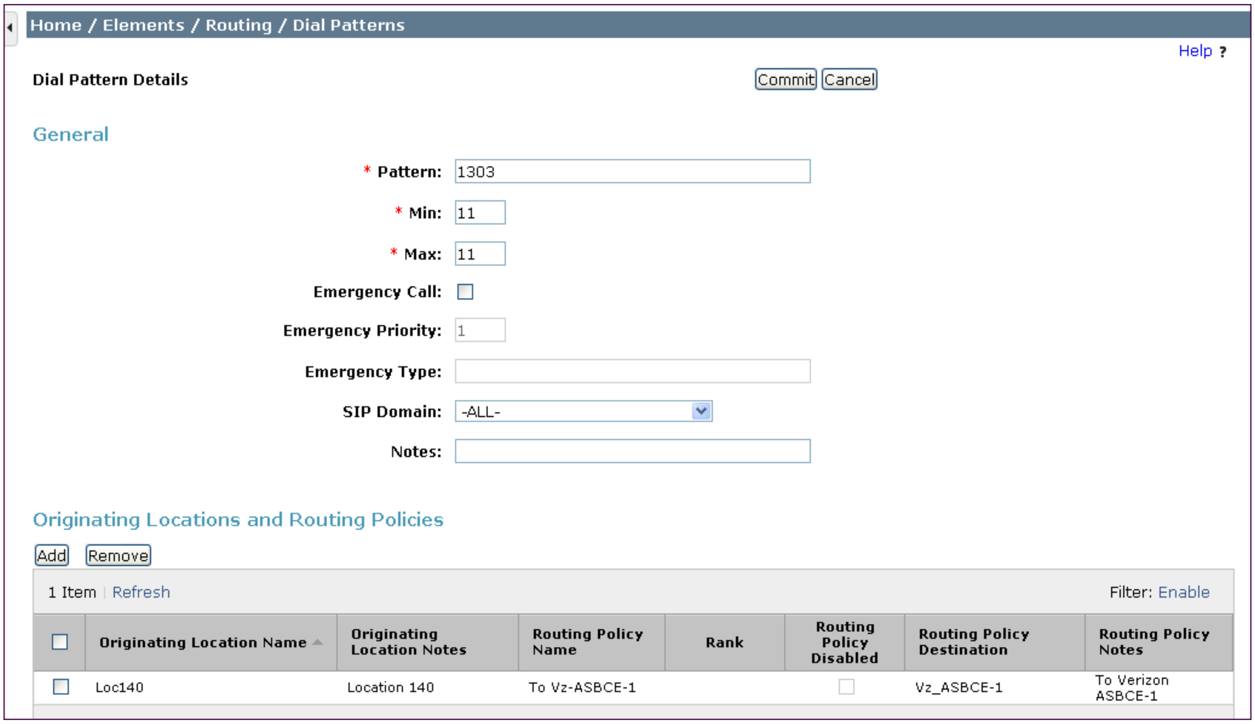
6.8. Dial Patterns

To view or change dial patterns, select **Routing → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern. Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a number assigned to the Verizon IP Trunk Service, such as 732-945-0285, Verizon delivers the number to the enterprise, and the Avaya SBCE sends the call to Session Manager. The pattern below matches on 732-945-0285 specifically. Dial patterns can alternatively match on ranges of number (e.g., a DID block). Under **Originating Locations and Routing Policies**, the routing policy named "**To CS1000**" is chosen when the call originates from **Originating Location Name** "**Vz-ASBCE**".



The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a CS1000E user dials a PSTN number such as 9-1303-XXX-XXXX, CS1000E sends the call to Session Manager. Session Manager will match the dial pattern shown below and send the call to the Avaya SBCE via the **Routing Policy Name** "**To Vz-ASBCE-1**".



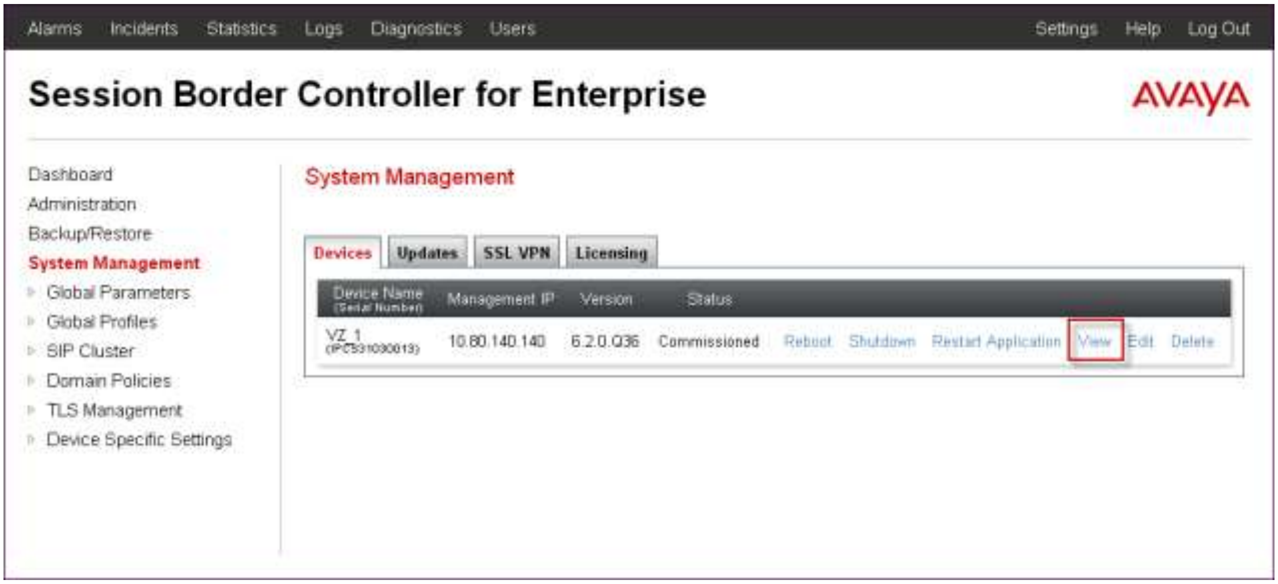
7. Configure Avaya Session Border Controller for Enterprise

These Application Notes assume that the installation of the Avaya SBCE and the assignment of all IP Addresses have already been completed, including the management IP Address.

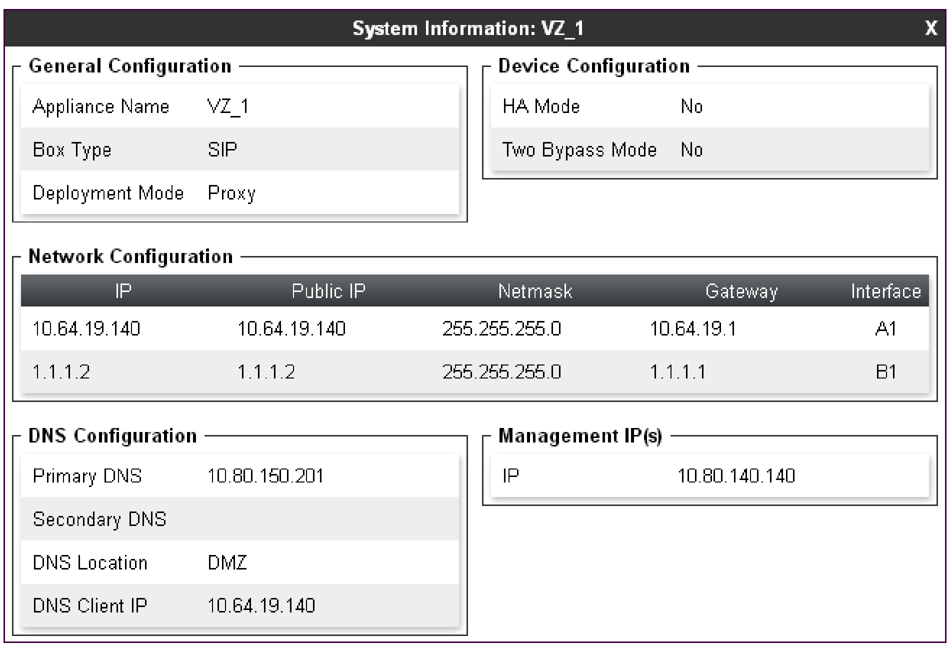
Access the web management interface by entering https://<ip-address> where <ip-address> is the management IP Address assigned during installation. In the sample configuration, the management IP is 10.80.140.140. Log in with the appropriate credentials. Click **Log In**.

The main page of the Avaya SBCE will appear.

To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named "**VZ_1**" is shown. To view the configuration of this device, click **View** as highlighted below.



The **System Information** screen shows the **Network Settings**, **DNS Configuration**, and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to "**SIP**" and the **Deployment Mode** was set to "**Proxy**". Default values were used for all other fields. Note that the **Management IP** must be on a separate subnet from the IP interfaces designated for SIP traffic.



7.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the internal interface is assigned to **A1** and the external interface is assigned to **B1**.

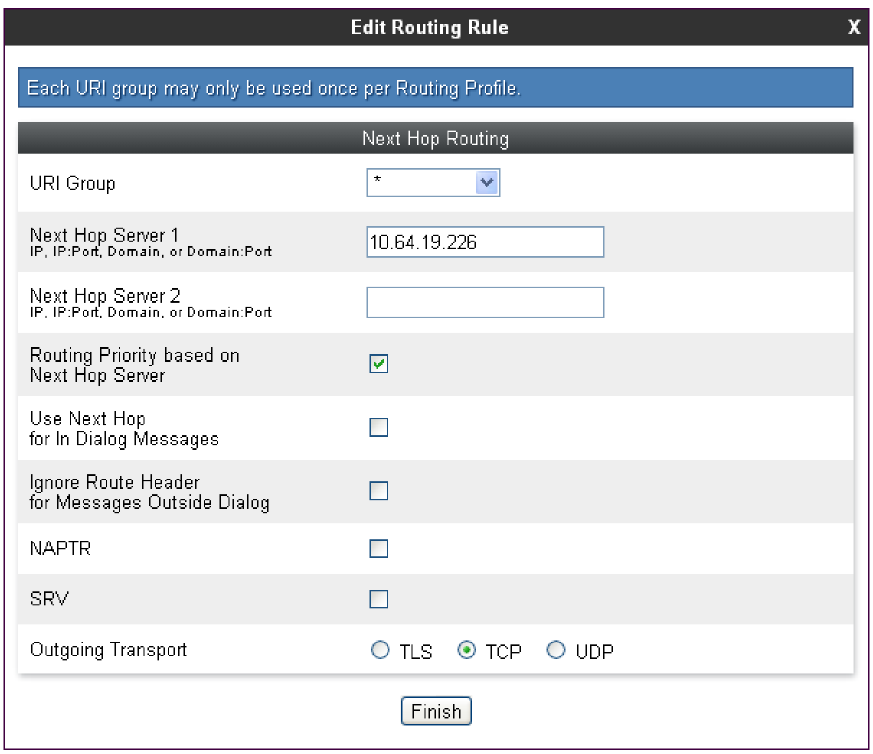
The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click the corresponding **Toggle State** button.

7.2. Routing Profile

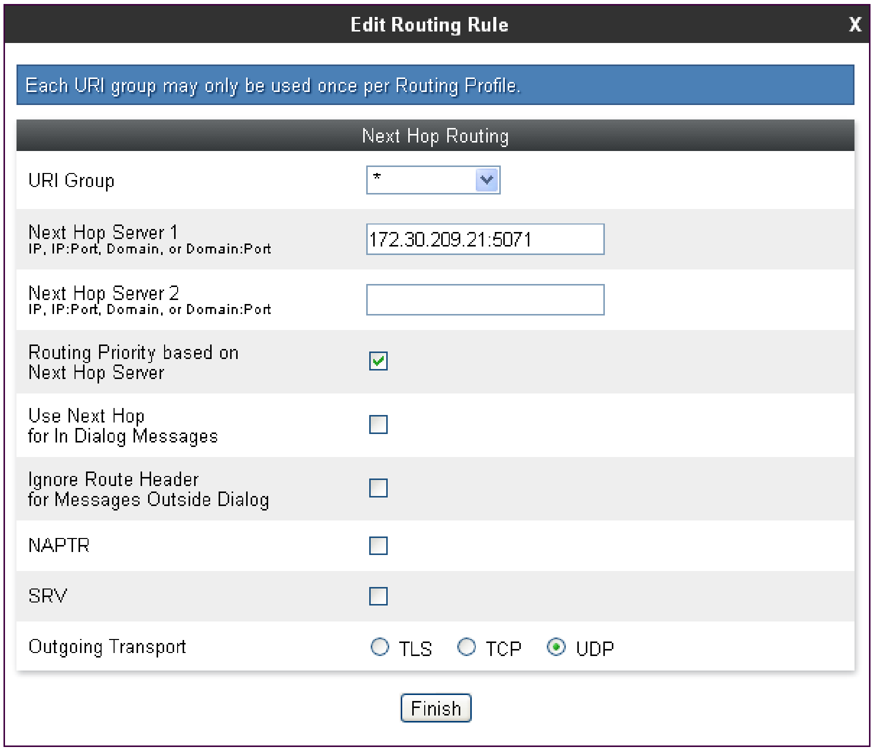
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

Create a Routing Profile for Session Manager and Verizon IP Trunk Service. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.

In the shared test environment the following screen shows Routing Profile "**Route to SM6.3**" created for Session Manager. The **Next Hop Server 1** IP address must match the IP address of Session Manager Entity, as shown in **Section 6.4**. The **Outgoing Transport** is set to **TCP** and matched the **Protocol** set in the Session Manager Entity Link for Avaya SBCE in **Section 6.5**.



The following screen shows Routing Profile “**Route To Vz_IPT**” created for Verizon. Enter the IP address and port of the Verizon SIP signaling interface as **Next Hop Server 1**, as shown below. It is only necessary to include the port after the IP address when it is not the default SIP port. Choose **UDP** for **Outgoing Transport**, and click **Finish**.



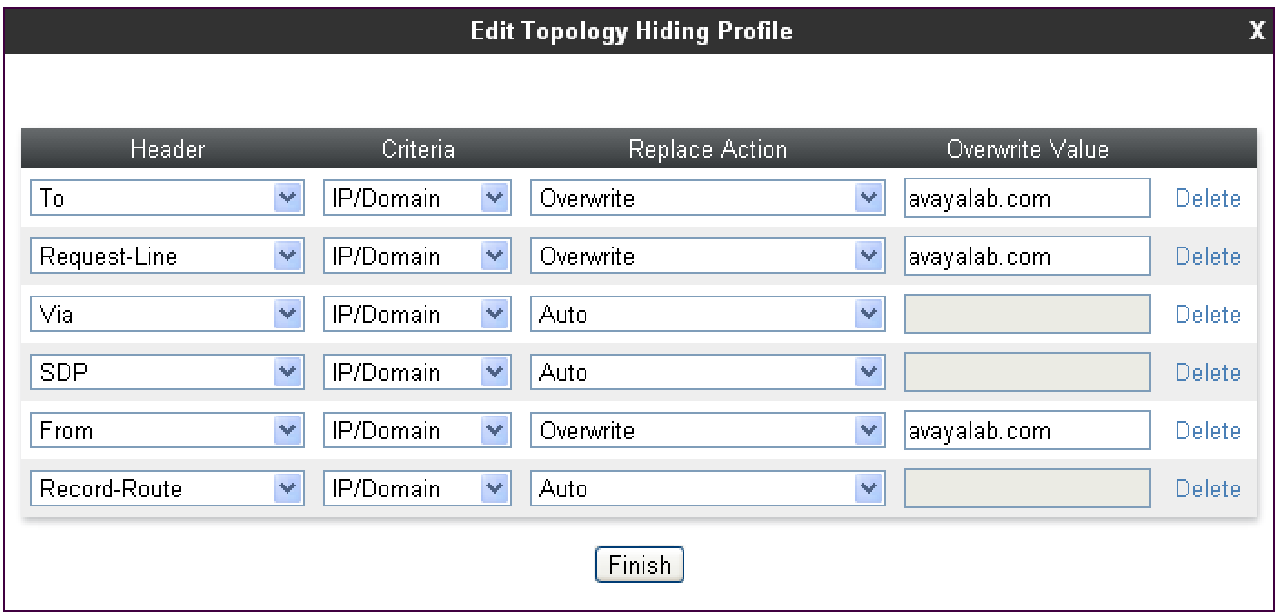
7.3. Topology Hiding Profile

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

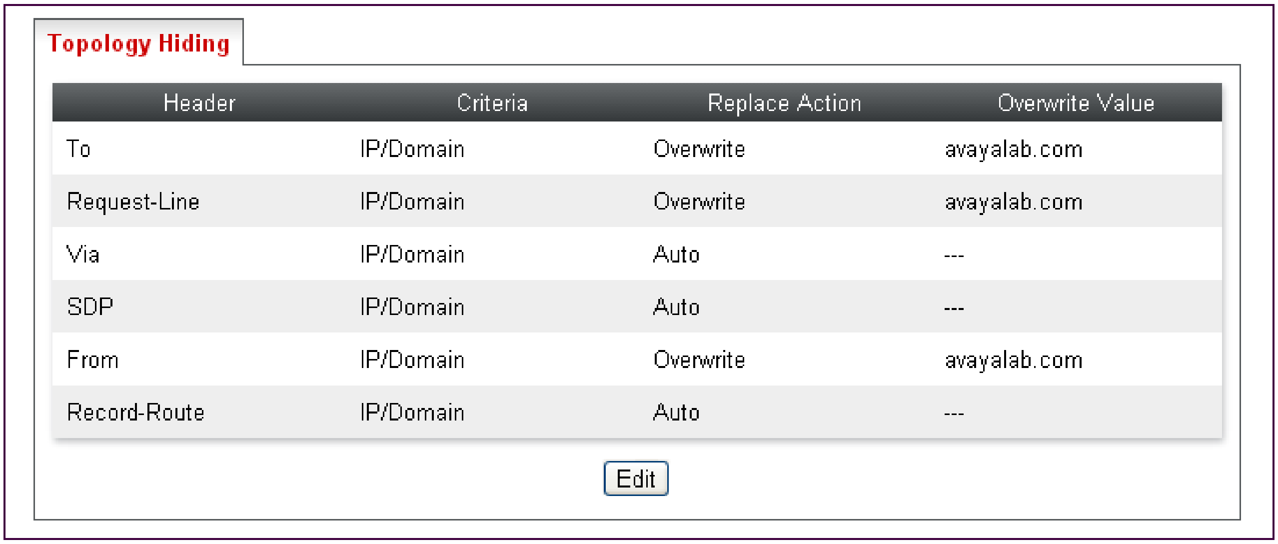
Click **Add** (not shown) to create a new profile, or select an existing topology hiding profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as “**Avaya**” shown below. Click **Next**.

In the resultant screen, click **Add Header** in the upper right multiple times to reveal additional headers.

In the **Replace Action** column an action of "**Auto**" will replace the header field with the IP address of the Avaya SBCE interface and the "**Overwrite**" will use the value in the **Overwrite Value**. In the example shown, this profile will later be applied in the direction of the Session Manager and "**Overwrite**" has been selected for the To/From and Request-Line headers and the shared Interop Lab domain of "**avayalab.com**" has been inserted. Click **Finish**.



After configuration is completed, the Topology Hiding for profile "**Avaya**" will appear as follows. This profile will later be applied to the Server Flow for Avaya.

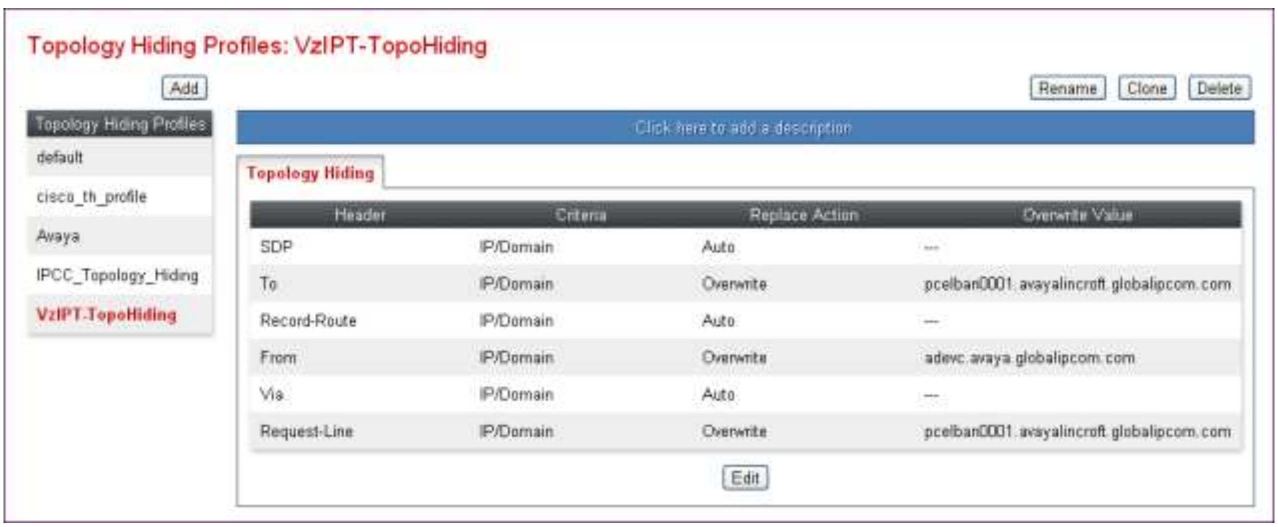


Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	avayalab.com
Request-Line	IP/Domain	Overwrite	avayalab.com
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
From	IP/Domain	Overwrite	avayalab.com
Record-Route	IP/Domain	Auto	---

Edit

Similarly, create a Topology Hiding profile for Verizon. The following screen shows Topology Hiding profile "**VzIPT-TopoHiding**" created for Verizon with the proper Verizon domains inserted in the **Overwrite Value**. This profile will later be applied to the Server Flow for Verizon.



Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	adevc.avaya.globalipcom.com
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com

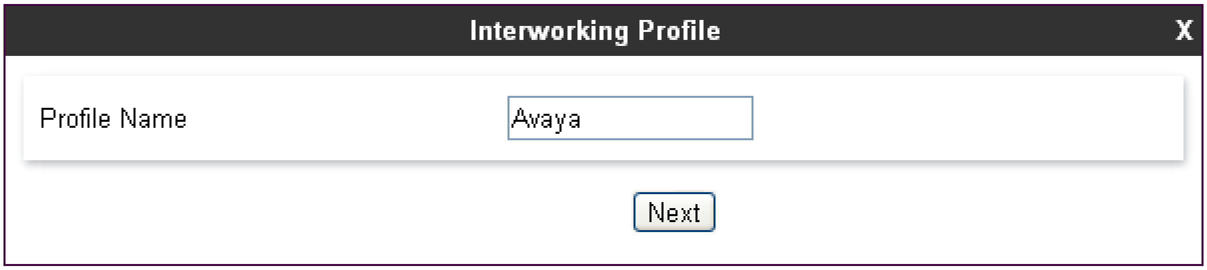
7.4. Server Interworking Profile

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

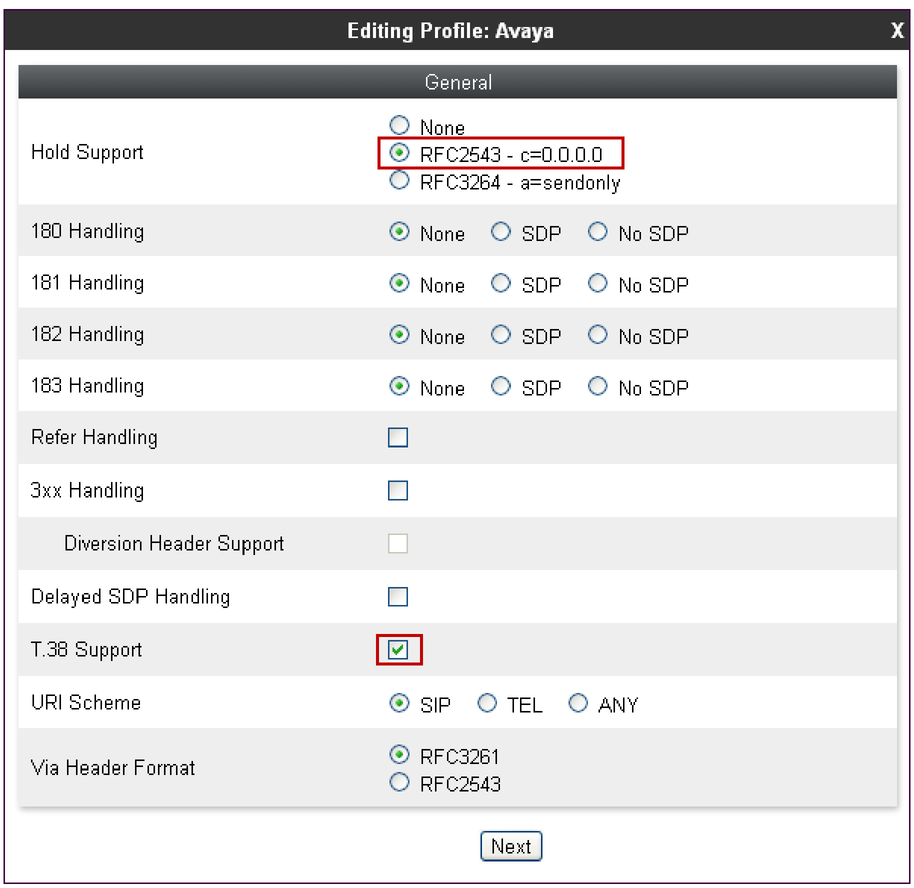
In the sample configuration, separate Server Interworking Profiles were created for Avaya and Verizon IP Trunk.

7.4.1. Server Interworking– Avaya

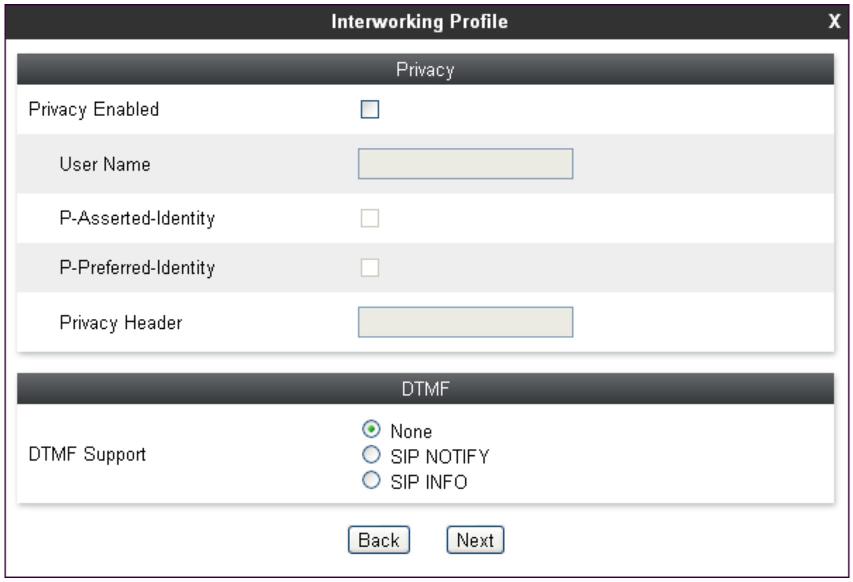
Navigate to **Global Profiles → Server Interworking** and click the **Add** button (not shown) to create a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as "**Avaya**" shown below. Click **Next**.

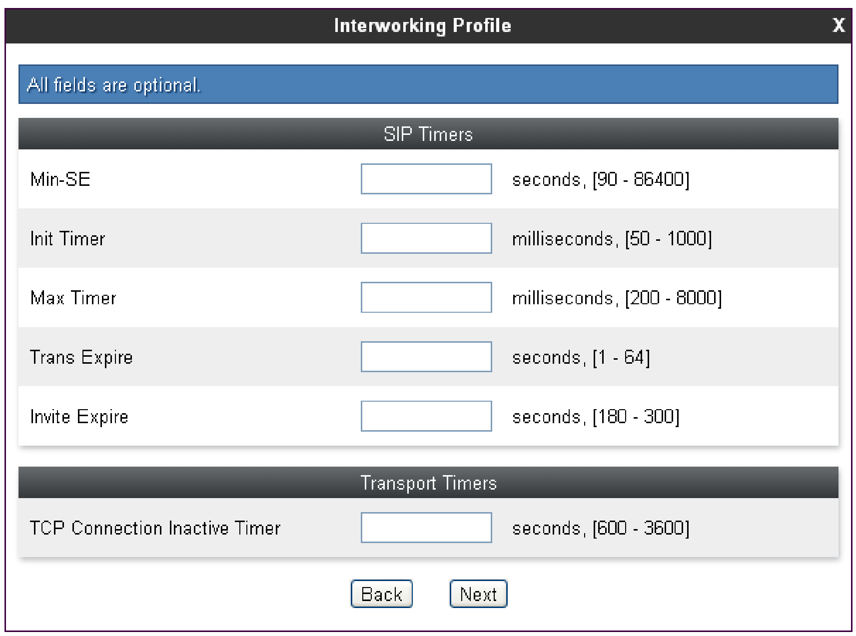


The following screens illustrate the **General** parameters used in the sample configuration for the Interworking Profile named "**Avaya**". Most parameters retain default values. In the sample configuration, **RFC2543 – c=0.0.0.0** is selected and **T.38 support** is checked.

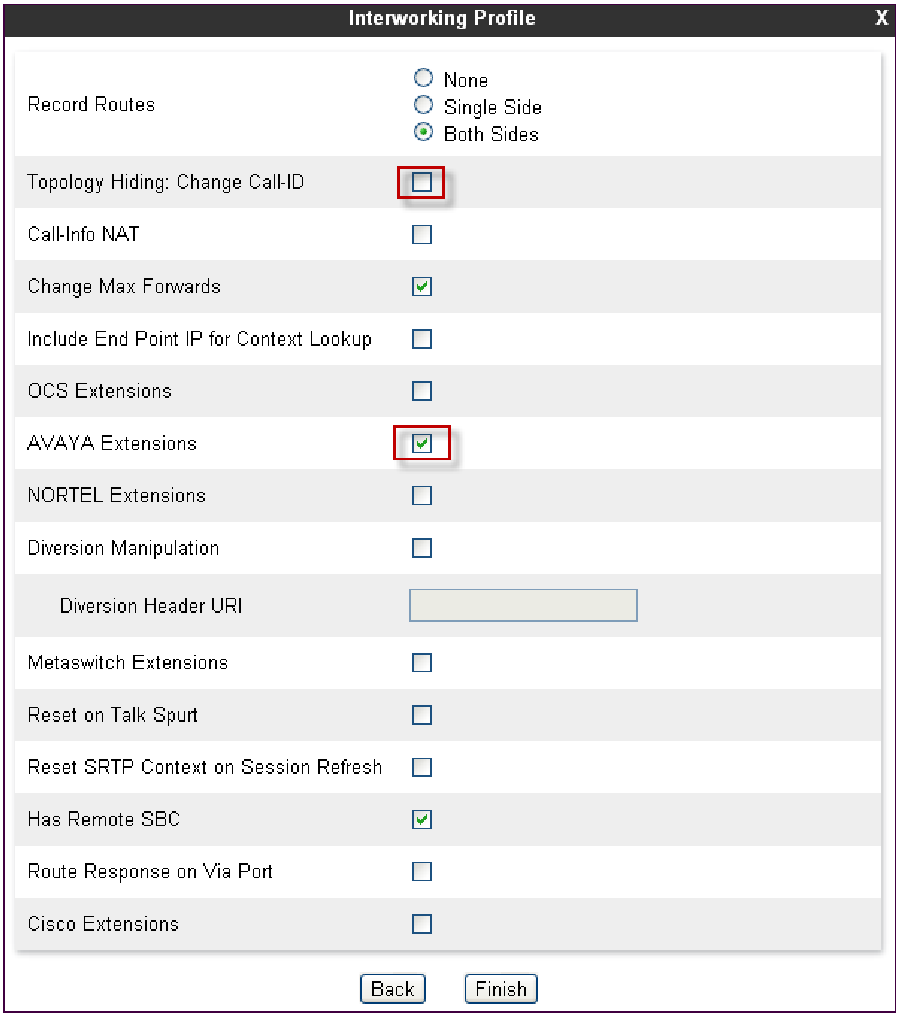


Click **Next** to advance to through both the Privacy / DTMF parameters screen, and the SIP / Transport Timers parameters screen, which may retain default values.



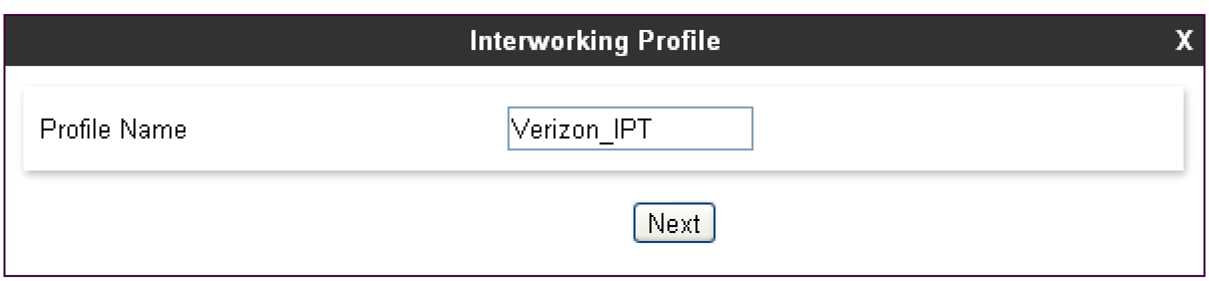


The following screen illustrates the **Advanced Settings** configuration. The **Topology Hiding: Change Call-ID** is unchecked and the **AVAYA Extensions** is checked. All other parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

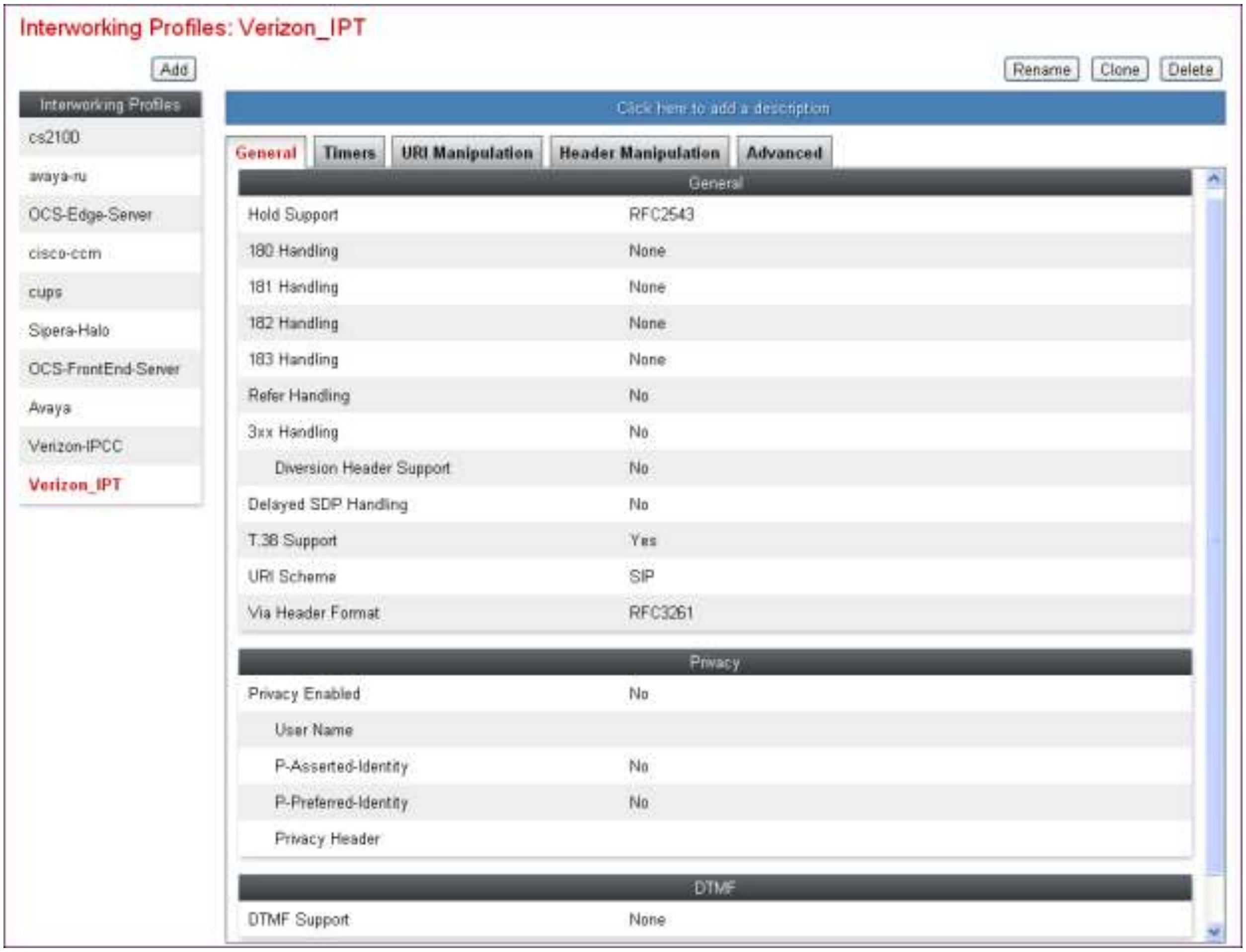


7.4.2. Server Interworking – Verizon IP Trunk

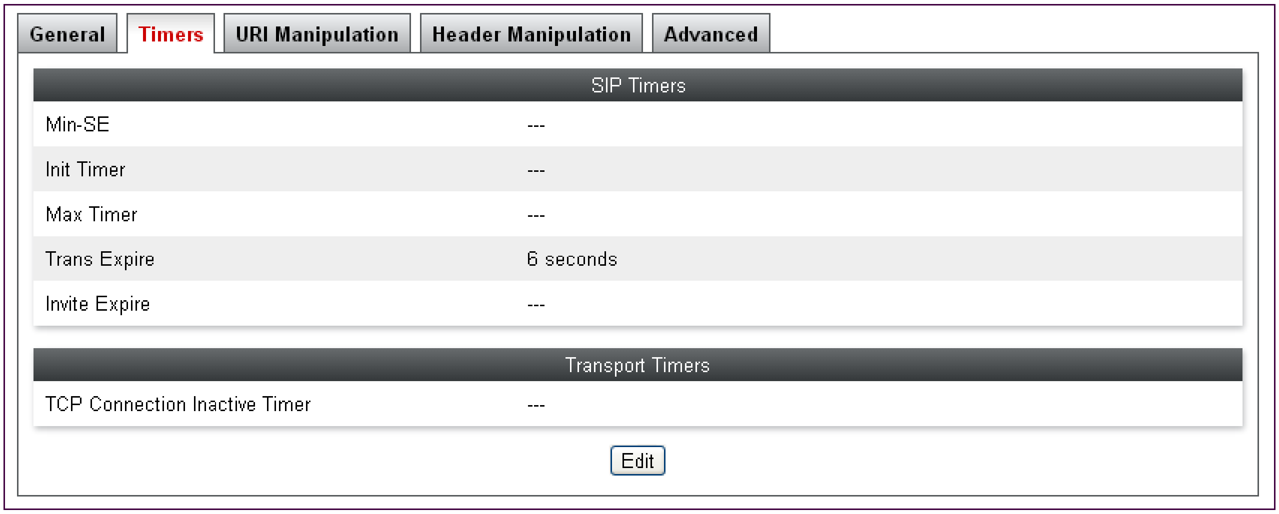
Click the **Add** button (not shown) to create a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as “**Verizon_IPT**” shown below. Click **Next**.



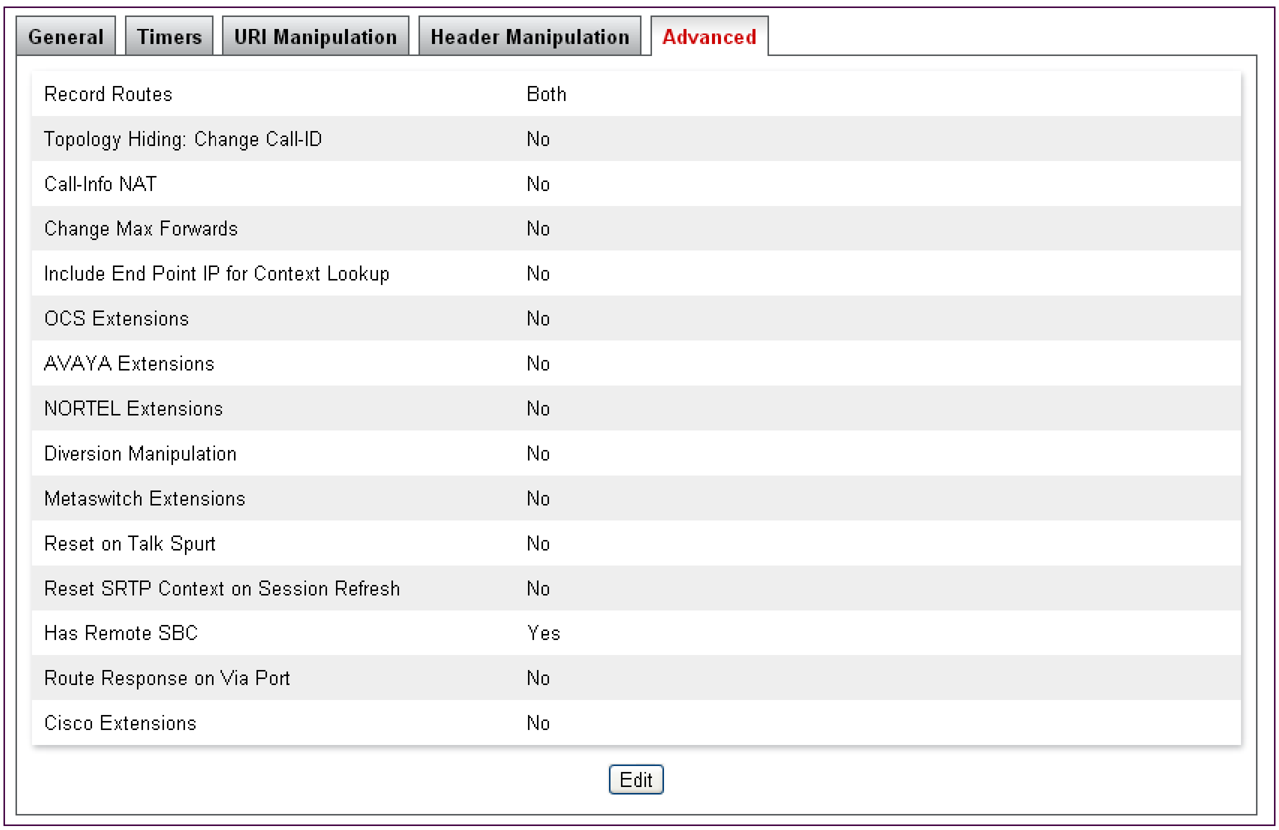
The following screens illustrate the **General** parameters used in the sample configuration for the Interworking Profile named "**Verizon_IPT**". Most parameters retain default values. In the sample configuration, **T.38 support** is set to "**Yes**", **Hold Support** is set for "**RFC2543**", and all other fields retained default values.



On the Timers tab, select 6 seconds for the **Trans Expire** timer as shown below.



The following screen illustrates the **Advanced Settings** configuration. The **Topology Hiding: Change Call-ID** and **Change Max Forwards** defaults were changed to "**No**". All other parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.



7.5. Signaling Manipulation

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

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

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing. The sample script is used to change the "Max-Forwards" header value to "70" and to remove the "UPDATE" value in the "Allow" header from Verizon.

To create a new Signaling Manipulation, navigate to **Global Profiles → Signaling Manipulation** and click **Add**. A new blank SigMa Editor window will pop up.

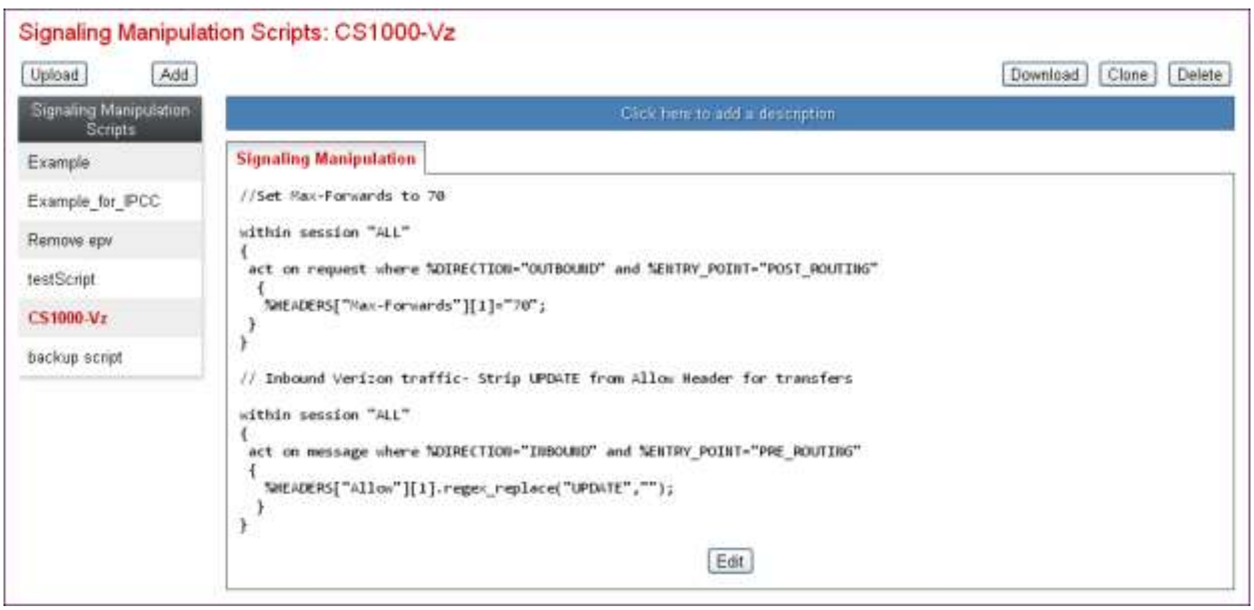
The following screens illustrate the "**CS1000-Vz**" script separated into two segments. In the Signaling Manipulation script segment below, the statement **act on request where %DIRECTION="OUTBOUND" and%ENTRY_POINT="POST_ROUTING"** specifies the portion of the script that will take effect on outbound SIP request messages to Verizon and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

```
//Set Max-Forwards to 70

within session "ALL"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
   %HEADERS["Max-Forwards"][1]="70";
 }
}
```

In the following segment of the Signaling Manipulation script, the statement **act on message where %DIRECTION="INBOUND" and%ENTRY_POINT="PRE_ROUTING"** specifies the portion of the script that will take effect on inbound SIP messages from Verizon, and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement.

```
// Inbound Verizon traffic- Strip UPDATE from Allow Header for transfers

within session "ALL"
{
 act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
 {
   %HEADERS["Allow"][1].regex_replace("UPDATE","");
  }
}
```

The following screen shows the complete Signaling Manipulation Script "**CS1000-Vz**" used during compliance testing. This script will later be applied to the Verizon Server Configuration in **Section 7.6.2**.



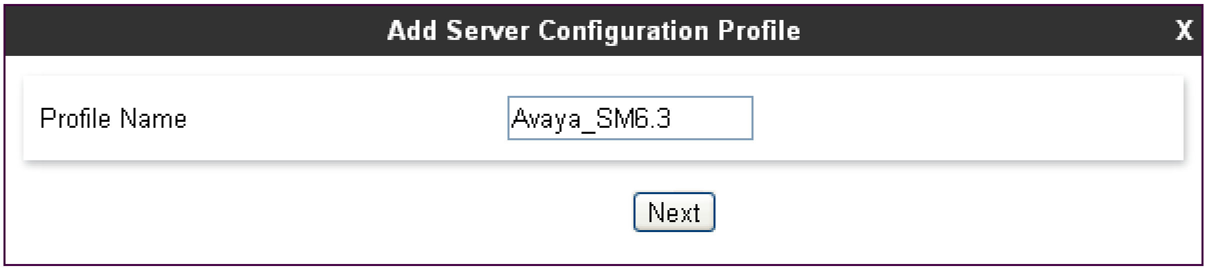
7.6. Server Configuration

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

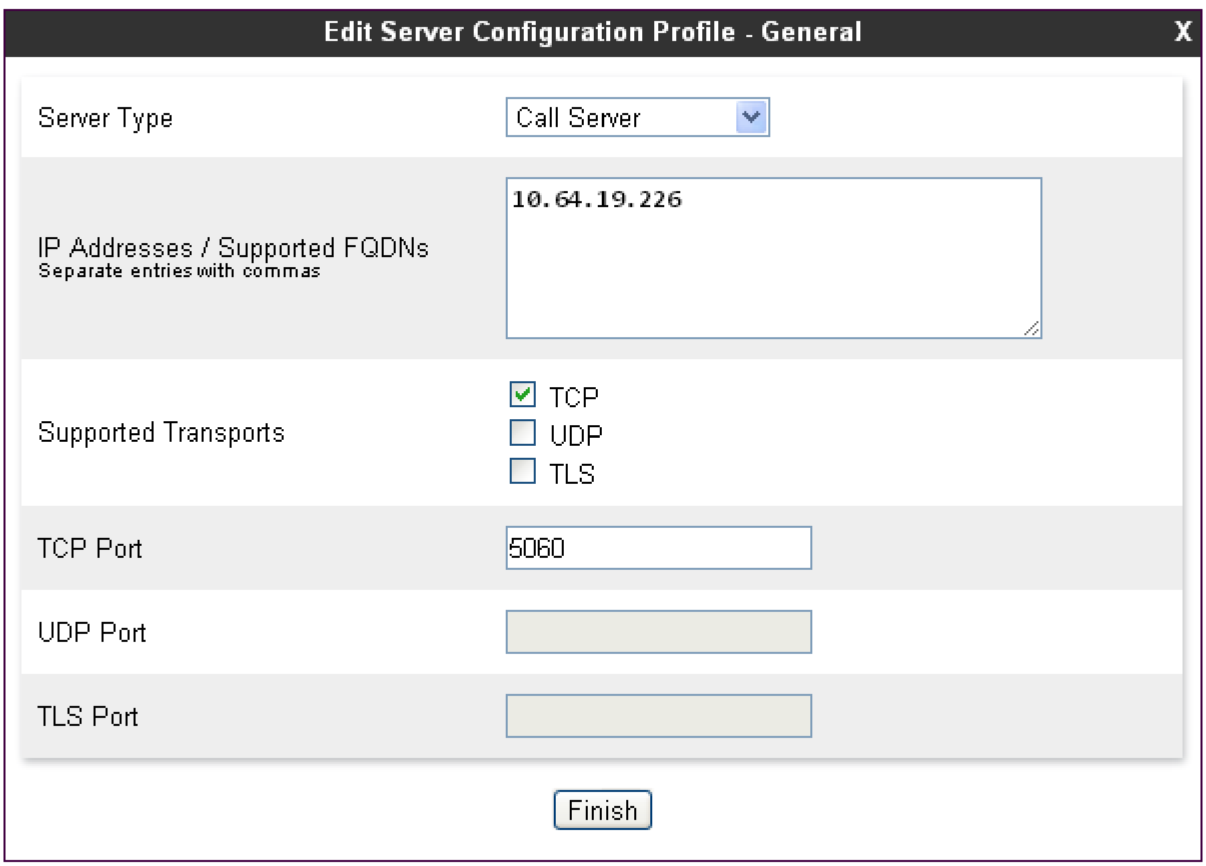
In the sample configuration, separate Server Configuration Profiles were created for Session Manager and Verizon IP Trunk.

7.6.1. Server Configuration for Session Manager

Click the **Add** button (not shown) to create a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as "**Avaya_SM6.3**" shown below. Click **Next**.

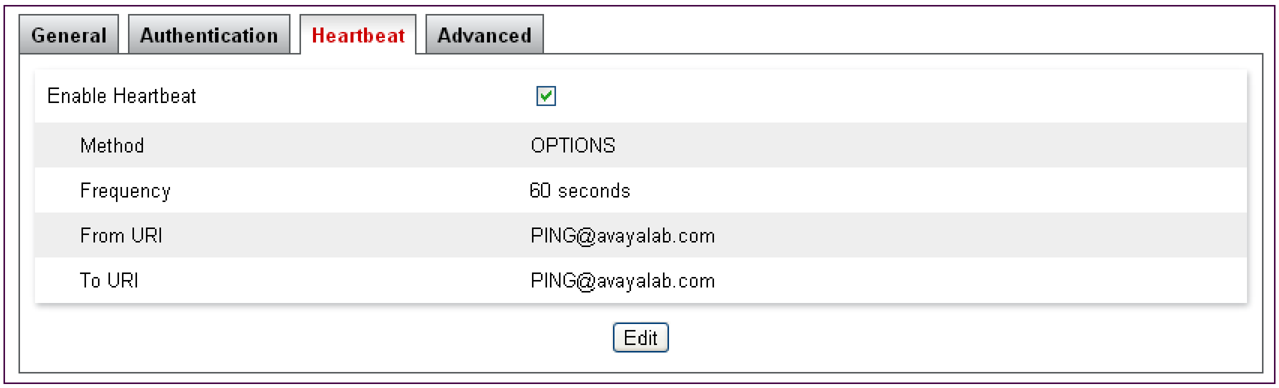


The following screens illustrate the Server Configuration for the Profile name "**Avaya_SM6.3**". On the **General** tab, select "**Call Server**" from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the IP Address of the Session Manager SIP signaling interface is entered. In the sample configuration, this IP Address is "**10.64.19.226**". In the **Supported Transports** area, **TCP** is selected, and the **TCP Port** is set to "**5060**". This configuration corresponds with the Session Manager Entity Link configuration for the Entity Link to the Avaya SBCE created in **Section 6.5**. If adding a new profile, click **Next** (not shown). If editing an existing profile, click **Finish**.

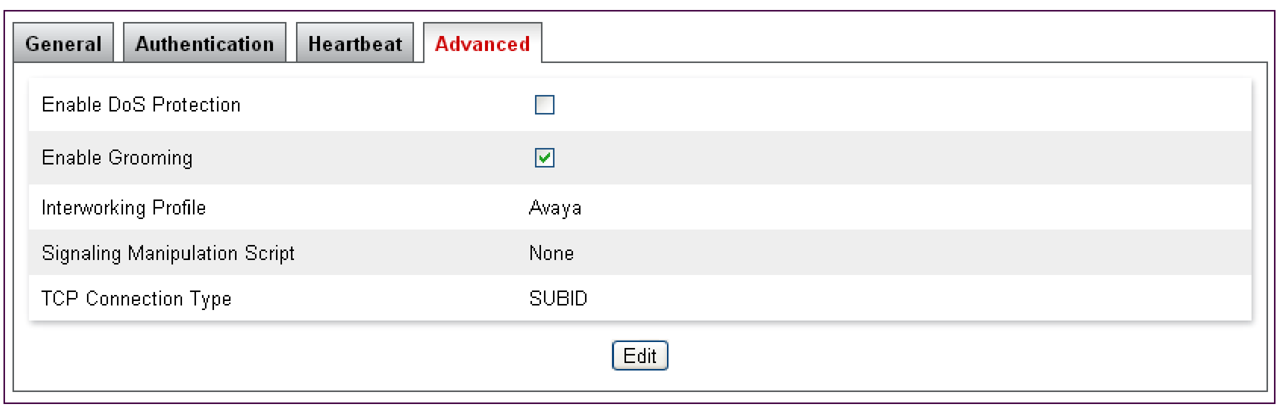


If adding the profile, click **Next** to accept default parameters for the Authentication tab (not shown), and advance to the Heartbeat area. If editing an existing profile, select the **Heartbeat** tab and click **Edit**.

Avaya SBCE can be configured to source "heartbeats" in the form of SIP OPTIONS. In the sample configuration, with one Session Manager, this configuration is optional. If Avaya SBCE-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select "**OPTIONS**" from the **Method** drop-down menu. Select the desired frequency that the Avaya SBCE will source OPTIONS to this server. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE towards Session Manager. If adding a new profile, click **Next** (not shown). If editing an existing profile, click **Finish** (not shown).

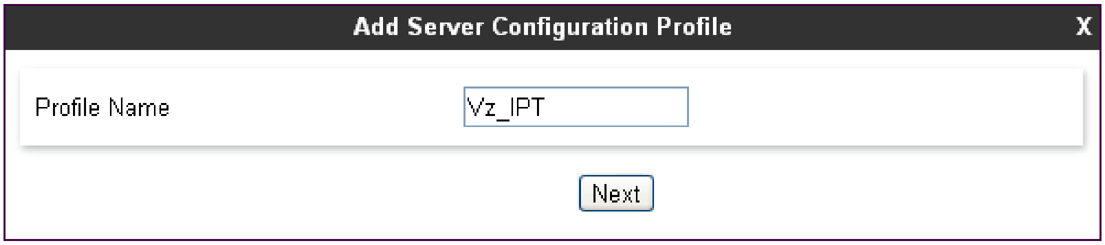


If adding a profile, click **Next** to continue to the **Advanced** settings (not shown). If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select **Enable Grooming** to allow the same TCP connection to be used for all SIP messages from this device. Select the **Interworking Profile** "**Avaya**" created previously. Click **Finish** (not shown).

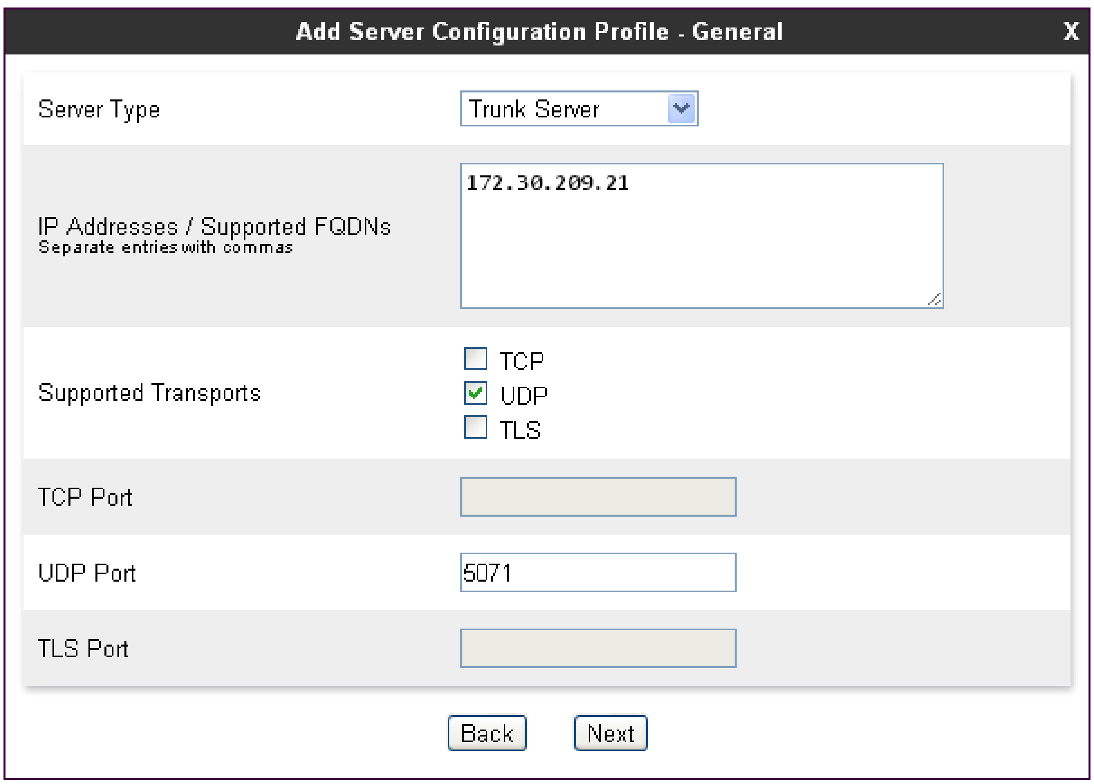


7.6.2. Server Configuration for Verizon IP Trunk

Click the **Add** button (not shown) to create a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as "**Vz_IPT**" shown below. Click **Next**.



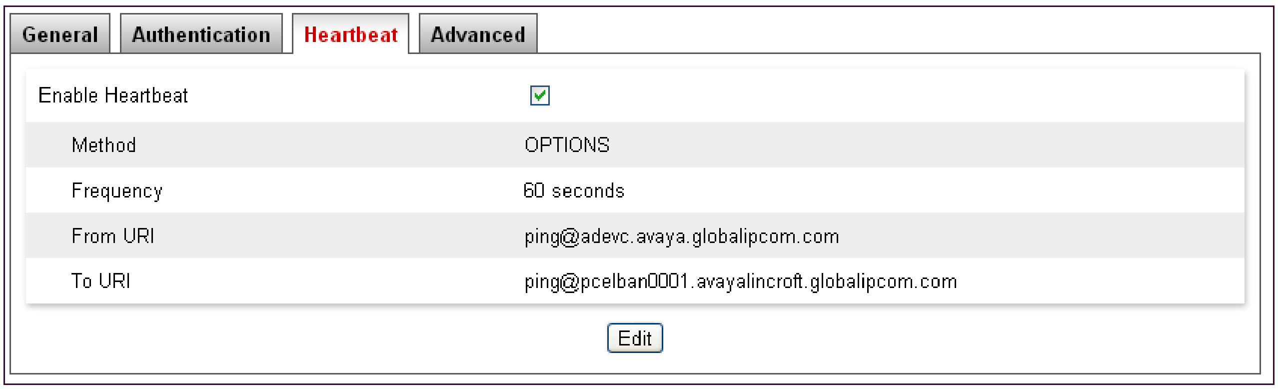
The following screens illustrate the Server Configuration with Profile name "**Vz_IPT**". On the **General** tab, select "**Trunk Server**" from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Verizon-provided IP Trunk IP Address is entered. This IP Address is "**172.30.209.21**". In the **Supported Transports** area, **UDP** is selected, and the **UDP Port** is set to "**5071**". Click **Next** to proceed to the **Authentication** Tab.



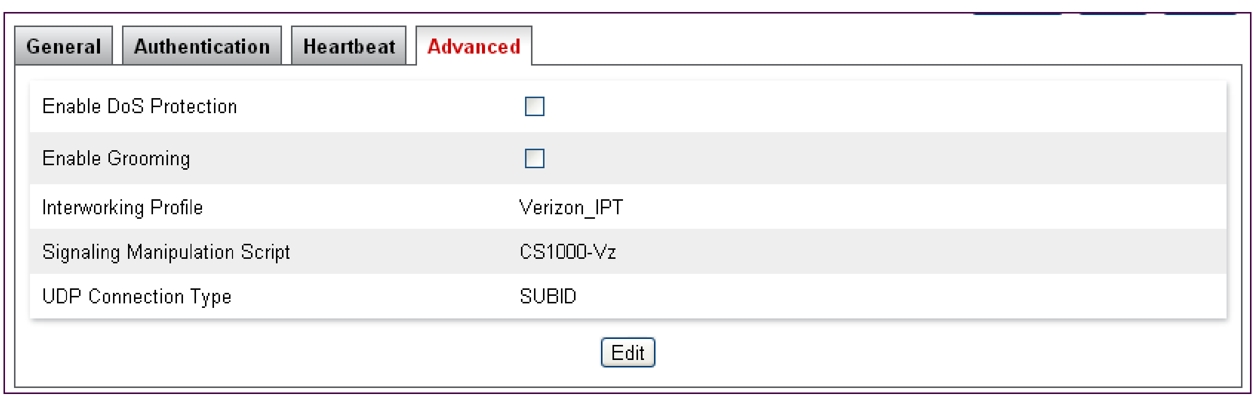
If adding the profile, click **Next** to accept default parameters for the Authentication tab (not shown), and advance to the Heartbeat area. If editing an existing profile, select the **Heartbeat** tab and click **Edit**.

The Avaya SBCE can be configured to source "heartbeats" in the form of SIP OPTIONS towards Verizon. This configuration is optional. Independent of whether the Avaya SBCE is configured to source SIP OPTIONS towards Verizon, Verizon will receive OPTIONS from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. When Session Manager sends SIP OPTIONS to the inside private IP Address of the Avaya SBCE, the Avaya SBCE will send SIP OPTIONS to Verizon. When Verizon responds, the Avaya SBCE will pass the response to Session Manager.

Select "**OPTIONS**" from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If adding a new profile, click **Next** to continuing to the "Advanced" settings. If editing an existing profile, click Finish (not shown).



If editing an existing profile, highlight the desired profile and select the **Advanced** tab and then click **Edit**. In the resultant screen, **Enable Grooming** is not used for UDP connections and left unchecked. Select the **Interworking Profile** "**Verizon_IPT**" created previously, and **Signaling Manipulation Script** will be the script shown in the previous section titled "**CS1000-Vz**". Click **Finish** (not shown).

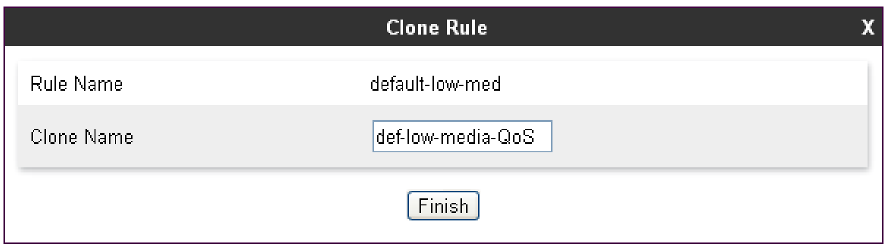


7.7. Media Rule

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

In the sample configuration, a single media rule is created by cloning the default rule called "**default-low-med**". Select the default-low-med rule and click the **Clone** button.

Enter a name in the **Clone Name** field, such as "**def-low-media-QoS**" as shown below. Click **Finish**.



Select the newly created rule, select the **Media QoS** tab and click the **Edit** button (not shown). In the resulting screen below, check the **Media QoS Marking Enabled** checkbox. Select **DSCP** and select "**EF**" for Expedited Forwarding as shown below. Click **Finish**.

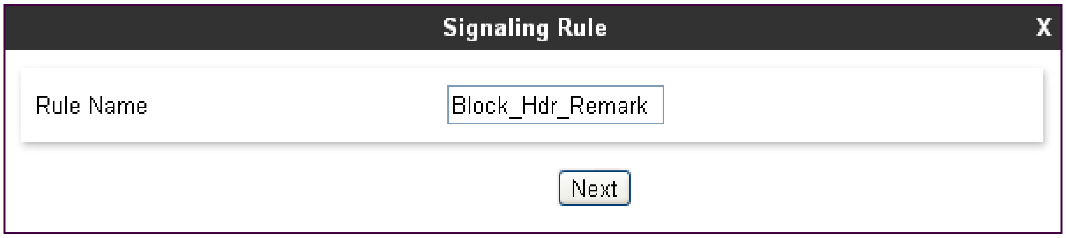
When configuration is completed, the “**default-low-media-QoS**” media rule **Media QoS** tab appears as follows.

7.8. Signaling Rule

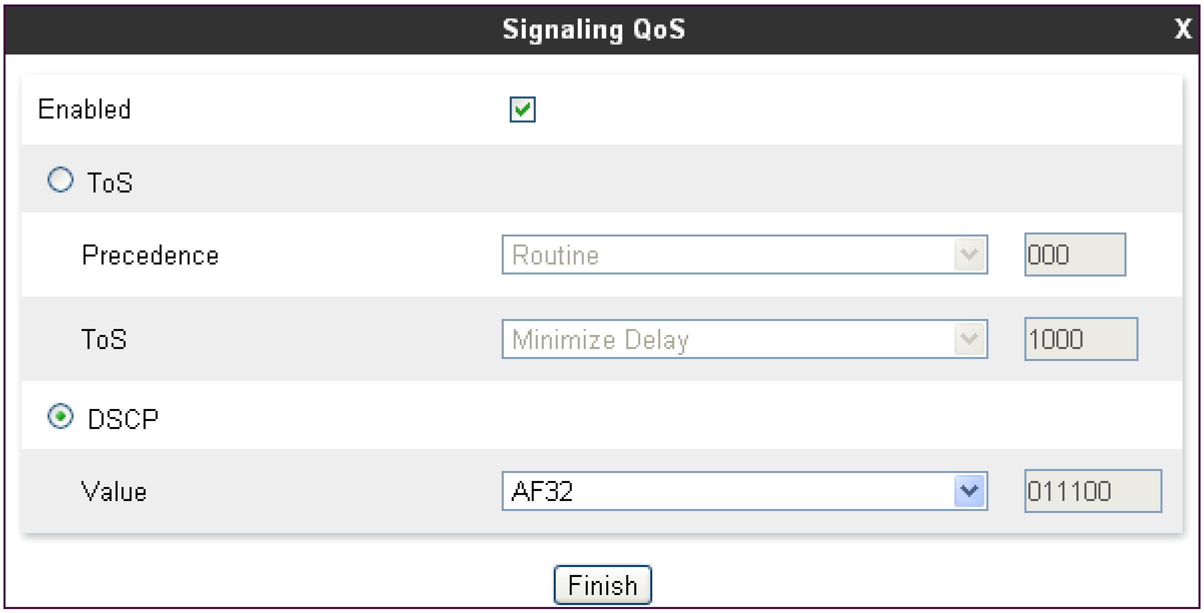
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To add a signaling rule, navigate to **Domain Policies → Signaling Rules**. Click the **Add** button to create a new signaling rule.

In the **Rule Name** field, enter an appropriate name, such as “**Block_Hdr_Remark**” and click **Next**.

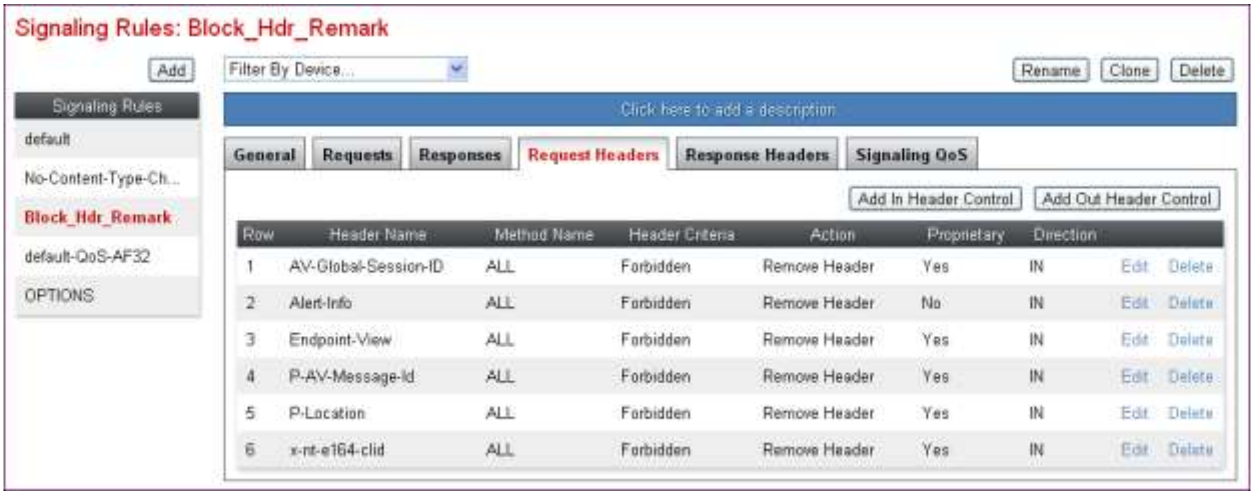


In the subsequent screen (not shown), click **Next** to accept defaults. In the **Signaling QoS** screen below, select **DSCP** and select the desired **Value** for Signaling QoS from the drop-down box. In the sample configuration, "**AF32**" is selected for Assured Forwarding 32. Click **Finish**.



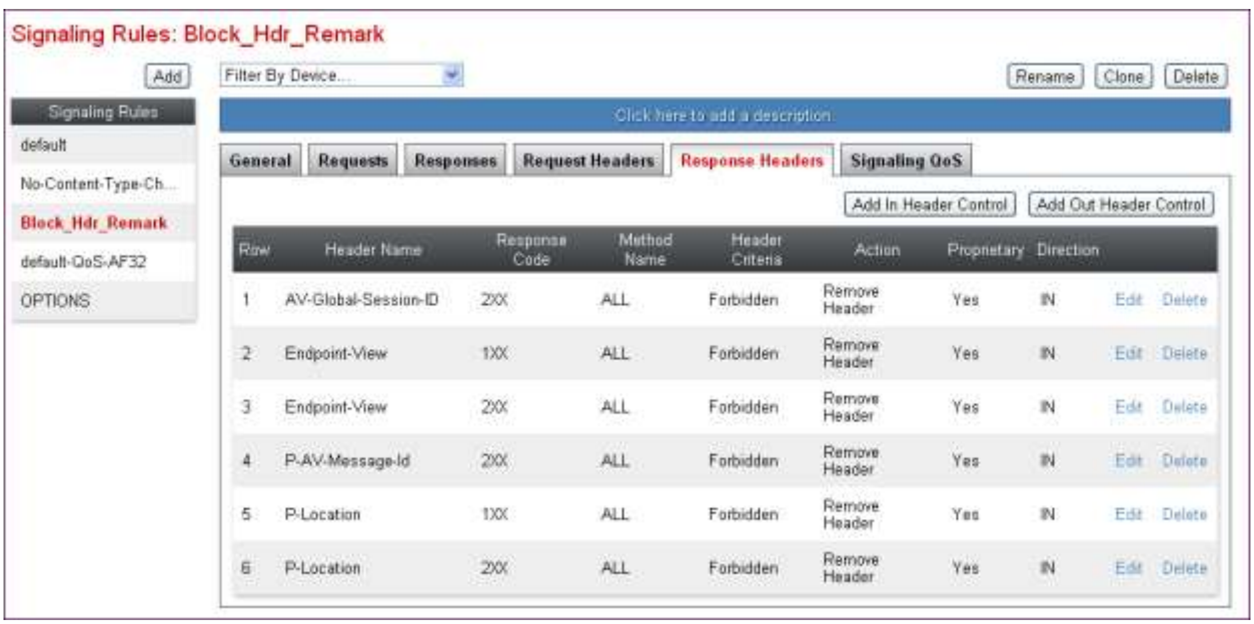
After this configuration, the new "**Block_Hdr_Remark**" will appear as follows.

Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on the request messages such as the initial INVITE message. The following screen shows the "**Alert-Info**", "**x-nt-e164-clid**", "**P-Location**" and other proprietary headers removed during the compliance test. This configuration is optional in that these headers do not cause any user-perceivable problems if presented to Verizon.



Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	x-nt-e164-clid	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

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



Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.9. Application Rule

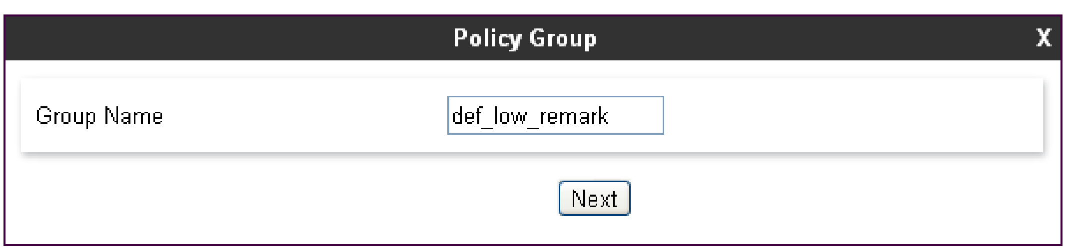
Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, user can determine the maximum number of concurrent voice and video sessions the network will process in order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

Select **Domain Policies → Application Rules** from the left-side menu as shown below. In the sample configuration, a single default application rule "**default-trunk**" is used and will be applied to the Endpoint Policy Group in the next section.

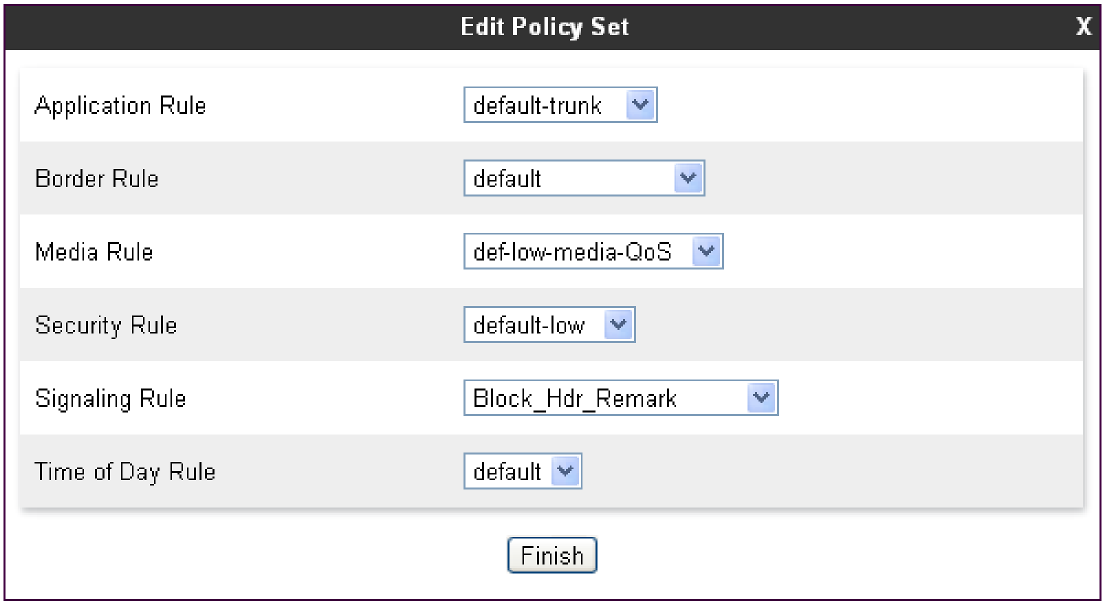
7.10. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section** Error! Reference source not found.. Create a separate Endpoint Policy Group for the enterprise and the Verizon IP Trunk. To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups**. Click the **Add** button.

Enter a name in the **Group Name** field, such as "**def_low_remark**" as shown below. Click **Next**.



In the sample configuration, defaults were selected for all fields, with the exception of the **Application Rule** which is set to "**default-trunk**", **Media Rule** which is set to "**default-low-media-QoS**", and the **Signaling Rule**, which is set to "**Block_Hdr_Remark**" as shown below. The selected non-default media rule and signaling rule chosen were created in previous sections. Click **Finish**.



Once configuration is completed, the "**default-low-remark**" policy group will appear as follows.

7.11. Media Interface

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

To create a new Signaling Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**. The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces.

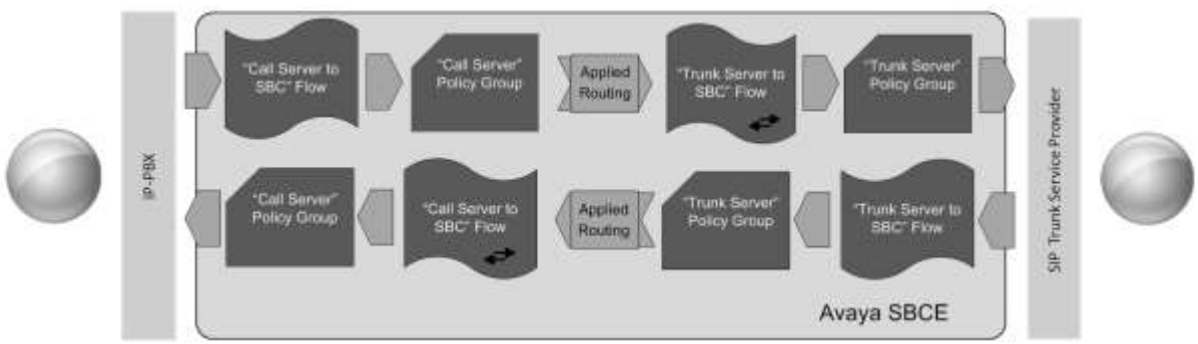
7.12. Signaling Interface

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

To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add**. The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

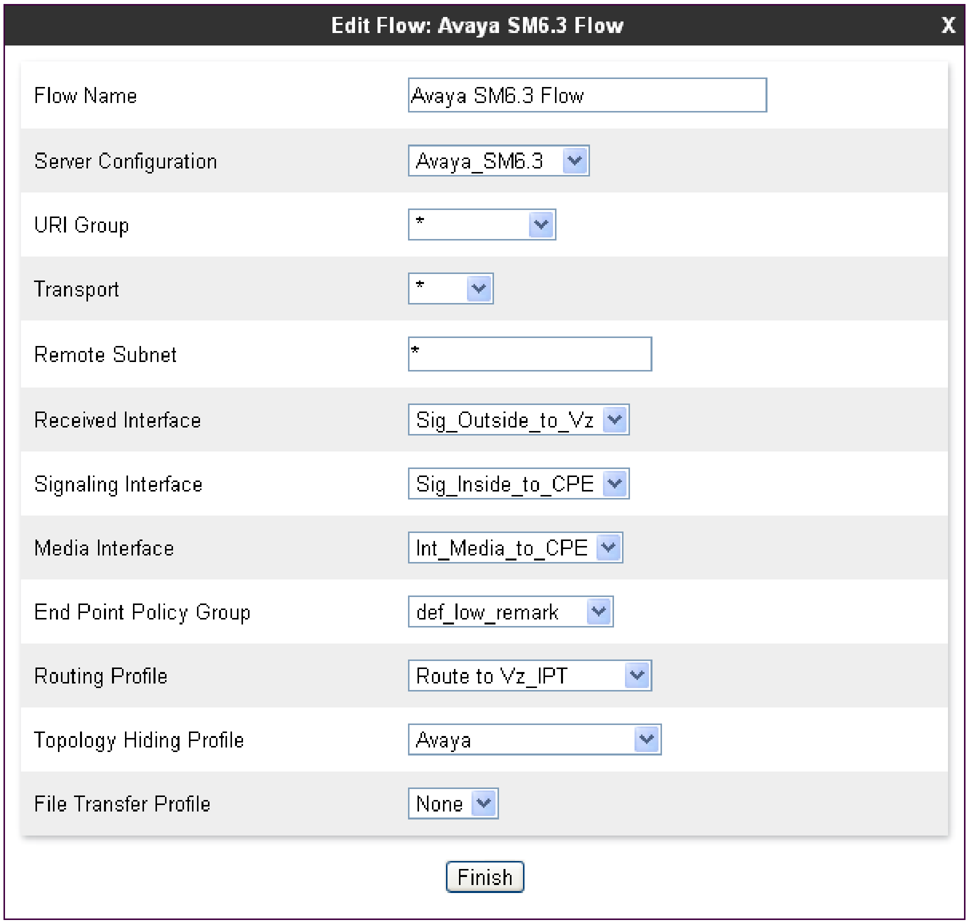
7.13. End Point Flows - Server Flow

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

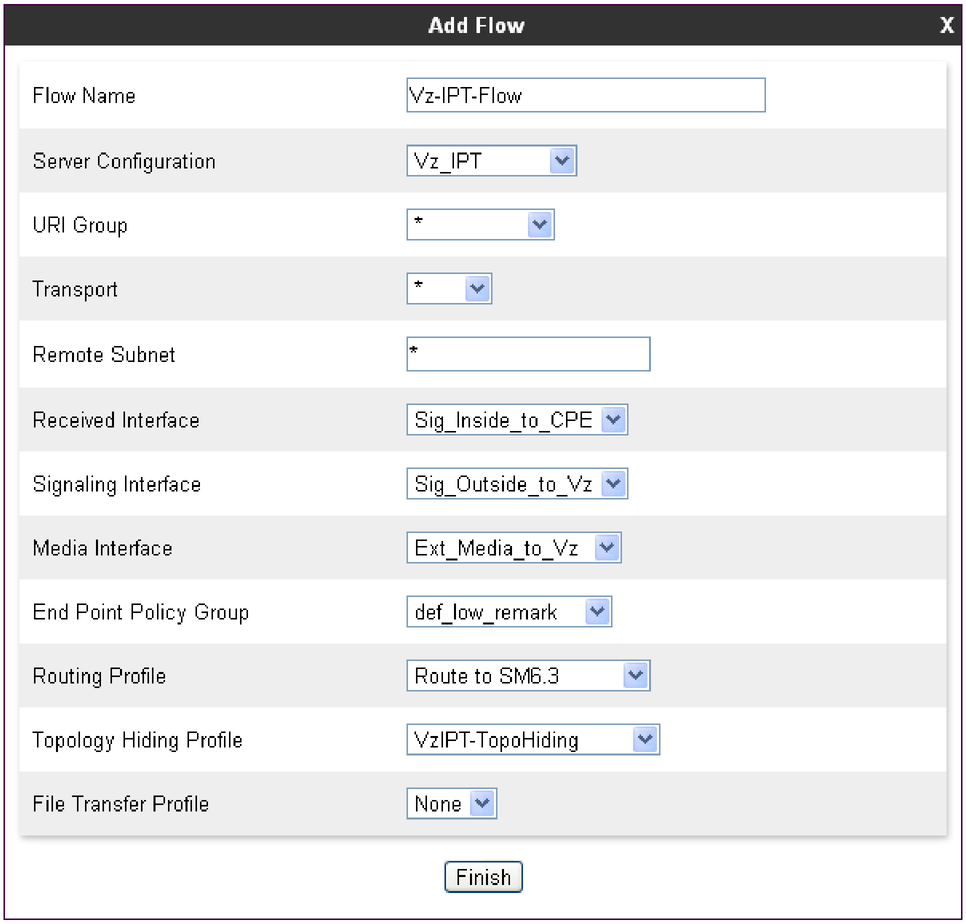


Create a Server Flow for Session Manager and the Verizon IP Trunk. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** as shown in below.

The following screen shows the flow named "**Avaya SM6.3 Flow**" used in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.



The following screen shows the flow named “**Vz-IPT-Flow**” used in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.



8. Verizon Business IP Trunk Service Offer Configuration

Information regarding Verizon Business IP Trunk service offer can be found at http://www.verizonbusiness.com/us/products/voip/trunking/ or by contacting a Verizon Business sales representative.

The sample configuration described in these Application Notes was located in the Avaya Solutions and Interoperability Test Lab. The Verizon Business IP trunk service was accessed via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

8.1. Fully Qualified Domain Name (FQDN)s

The following Fully Qualified Domain Names (FQDN)s were provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
adevc.avaya.globalipcom.com	*pcelban0001.avayalincroft.globalipcom.com*

8.2. DID Numbers Assigned by Verizon

Verizon provided DID numbers that could be called from the PSTN. These Verizon-provided DID numbers terminated to the Avaya CS1000E location via the Verizon IP Trunk Service. **Table 1** in **Section 3** shows example Verizon DID numbers and the configurable association of the Verizon DID numbers with Avaya CS1000E users.

9. Verification

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

9.1. Avaya Communication Server 1000E Verification

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

9.1.1. IP Network Maintenance and Reports Commands

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

The **General Commands** page is displayed. 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 (10.64.19.226, port 5060, TCP) has **SIPNPM Status** "**Active**".

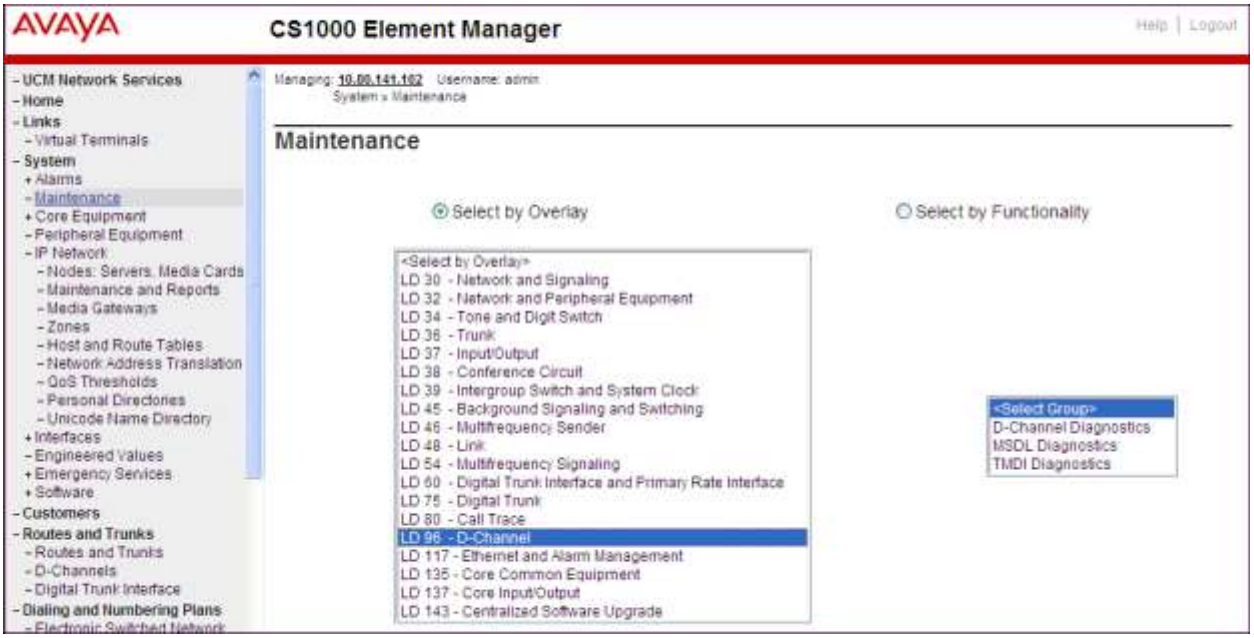
The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command sigSetShowAll** in **Group SipLine**. At the time this screen was captured, the SIP telephone with DN 7111 was involved in an active call with the Verizon IPCC.

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 "**10.64.19.112**" was involved in an active call with the Verizon IP Trunk Service.

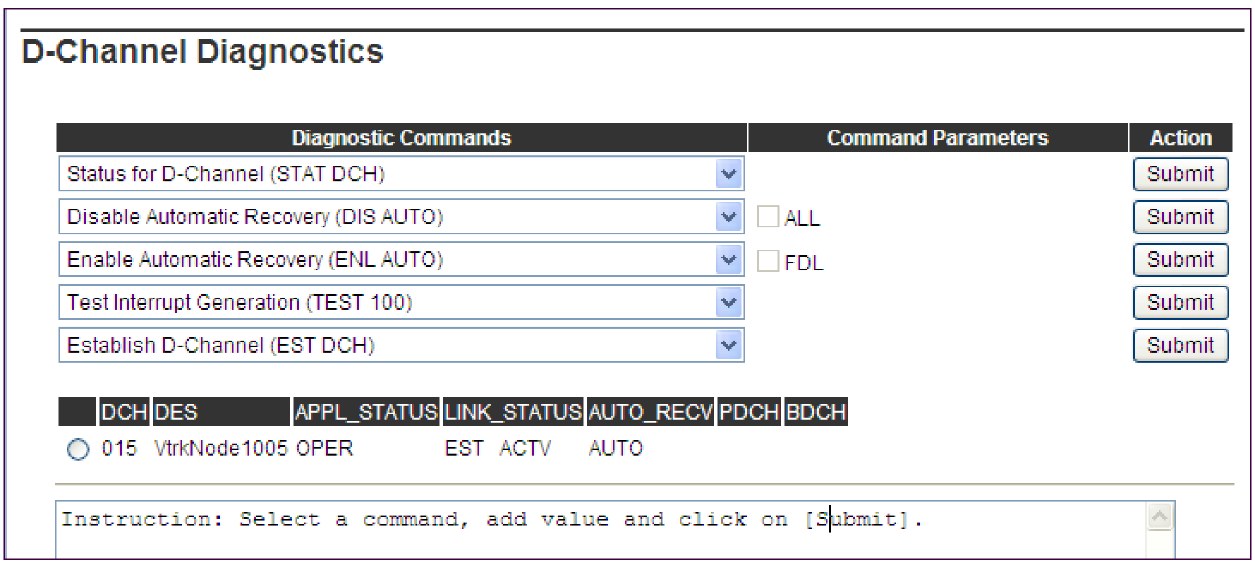
9.1.2. System Maintenance Commands

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**).

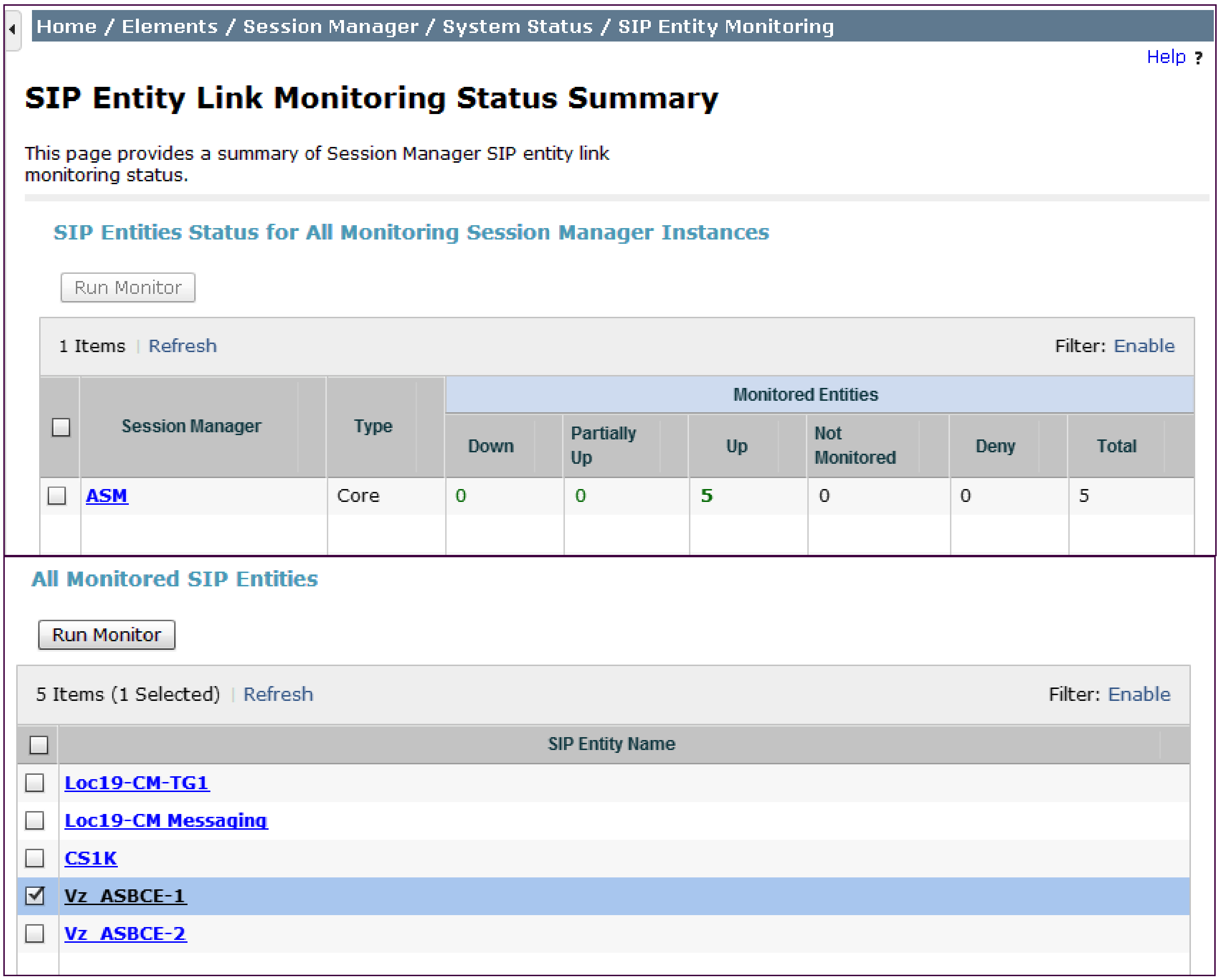


9.2. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

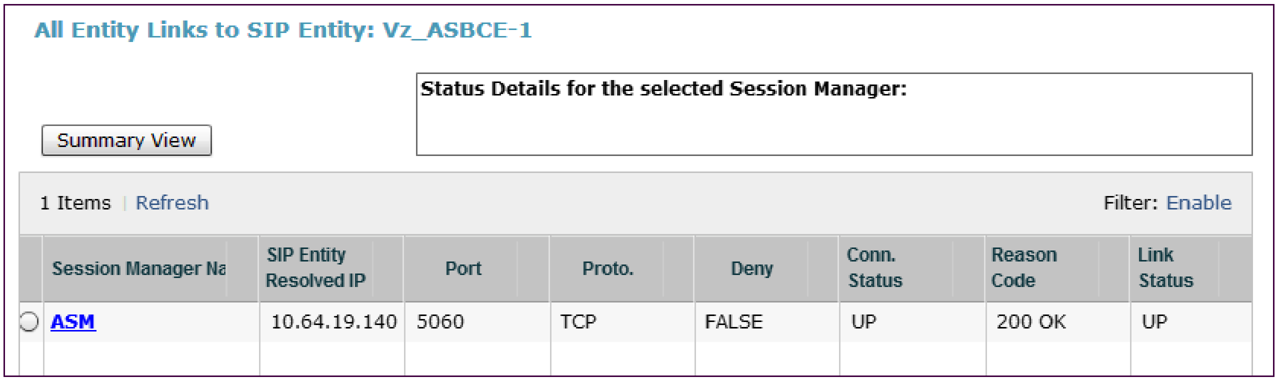
This section contains verification steps that may be performed using System Manager for Session Manager.

9.2.1. Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**.



From the list of monitored entities, select an entity of interest, such as "**Vz_ASBCE-1**". Under normal operating conditions, the **Link Status** should be "UP" as shown in the example screen below.


All Entity Links to SIP Entity: Vz_ASBCE-1

Status Details for the selected Session Manager:

Summary View

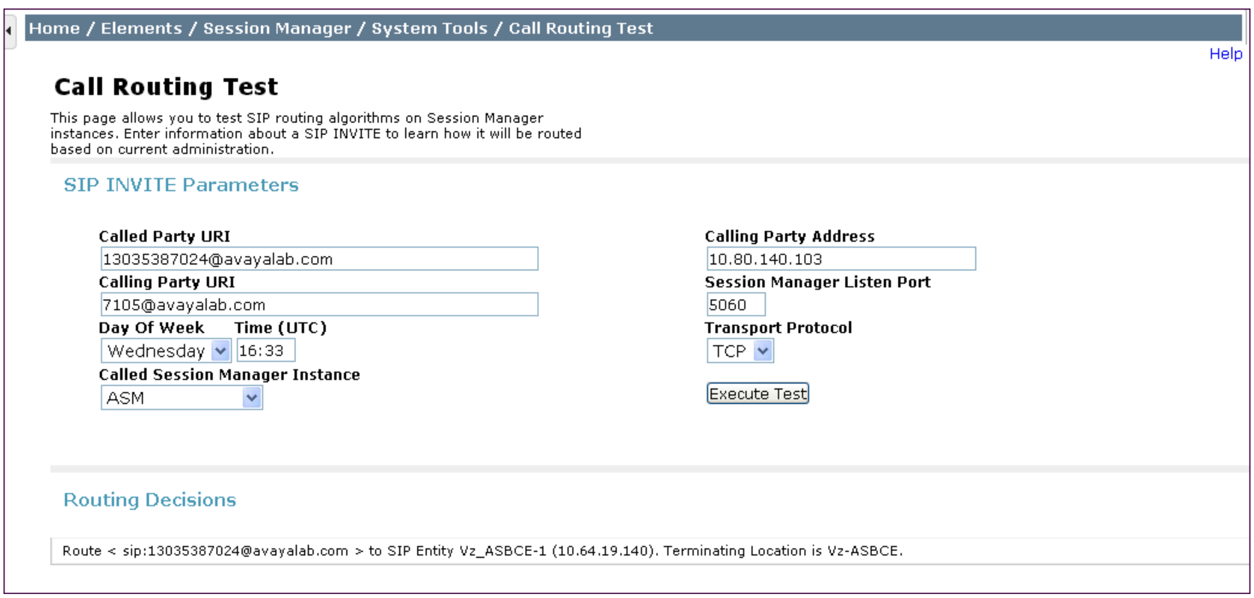
1 Items | Refresh Filter: Enable

Session Manager Na	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
ASM	10.64.19.140	5060	TCP	FALSE	UP	200 OK	UP

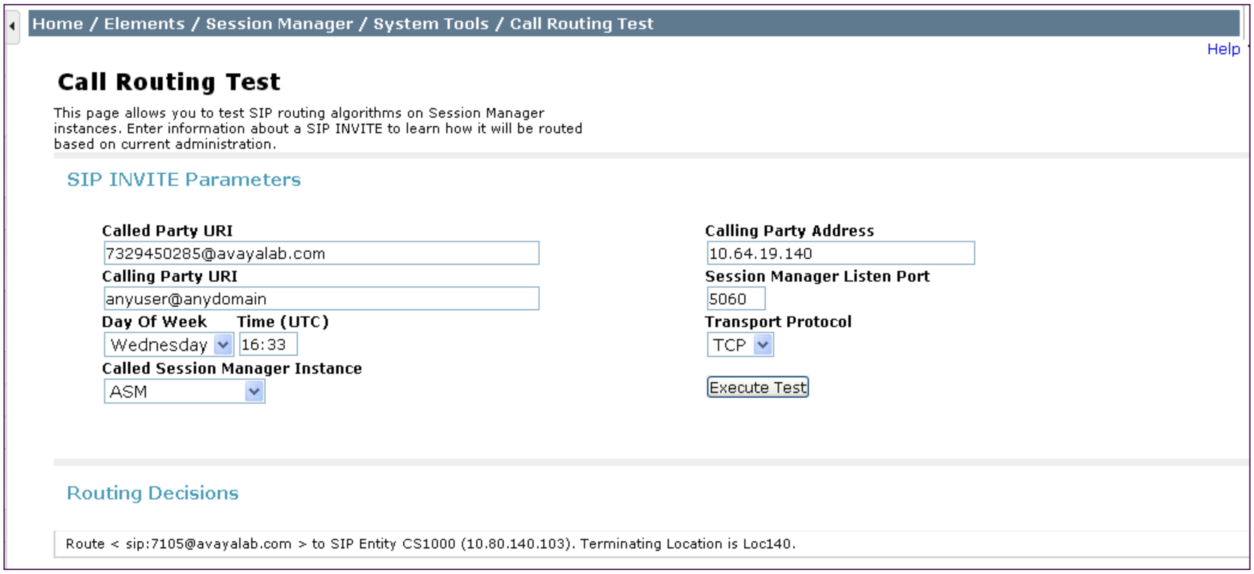
9.2.2. Call Routing Test

The **Call Routing Test** verifies the routing for a particular source and destination. To run the routing test, expand **Elements → Session Manager → System Tools → Call Routing Test**.

Populate the fields for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to the PSTN via Verizon. Under **Routing Decisions**, observe that the call will route via an Avaya SBCE on the path to Verizon. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



Another example shows an inbound call to one of Verizon assigned DID numbers. Observe that the DID number 732-945-0285 has been converted to CS1000E extension 7105 under **Routing Decisions** and will be routed to CS1000E.



9.3. Avaya Session Border Controller for Enterprise Verification

The welcome screen shows alarms, incidents, and the status of all managed Avaya SBCEs at a glance.

9.3.1. Alarms

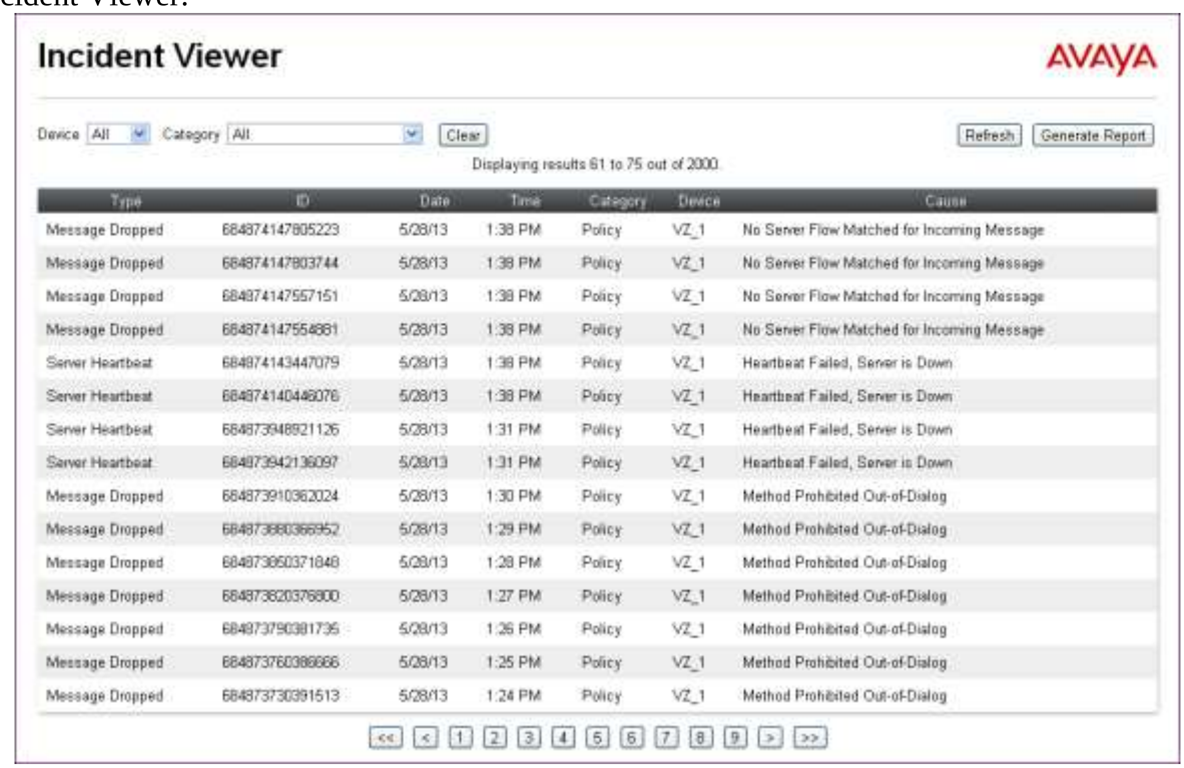
A list of the most recent alarms can be found under the **Alarms** tab on the top left bar.

Alarm Viewer:

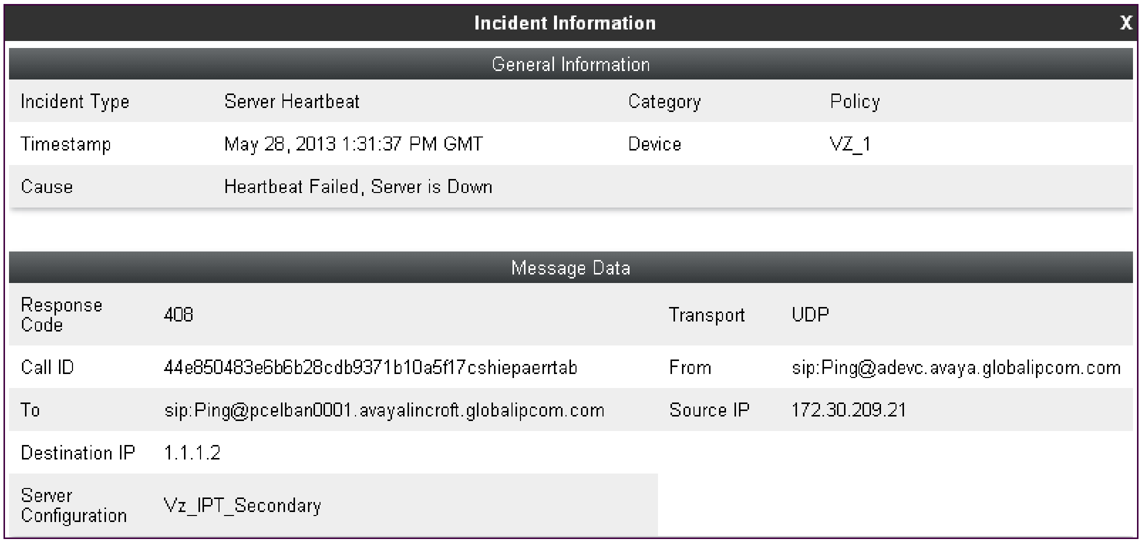
9.3.2. Incidents

A list of all recent incidents can be found under the **Incidents** tab at the top left next to the Alarms.

Incident Viewer:



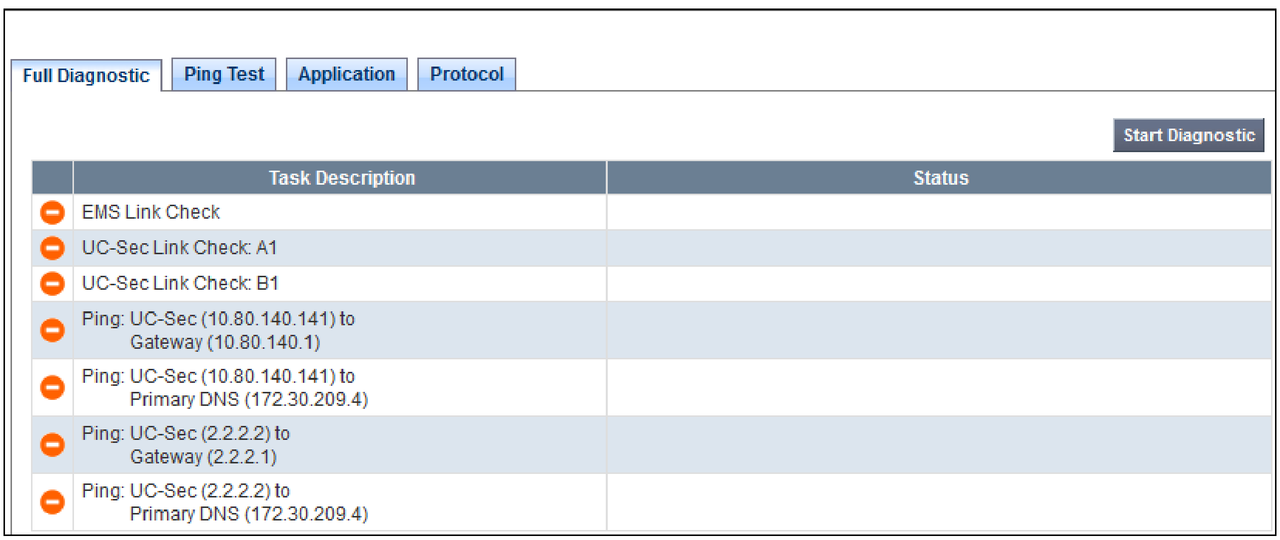
Further Information can be obtained by clicking on an incident in the incident viewer.



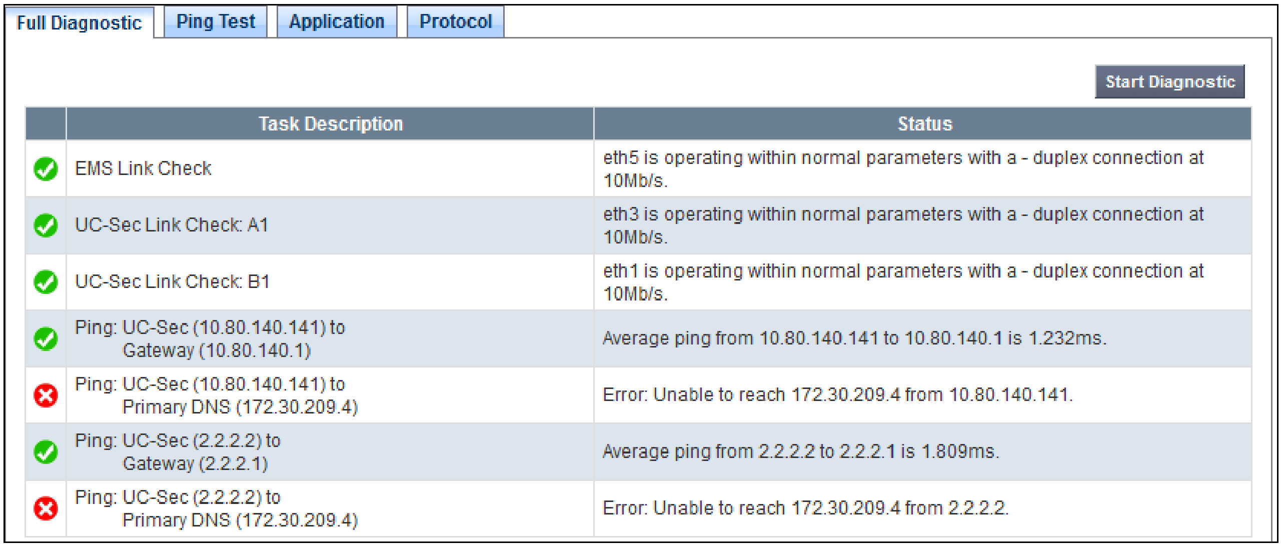
9.3.3. Diagnostics

The full diagnostics check that can be run can run line checks in both directions.

Click on **Diagnostics** on the top bar, select the Avaya SBCE from the list of devices and then click “Start Diagnostics”.



A green check mark or a red x will indicate success or failure.



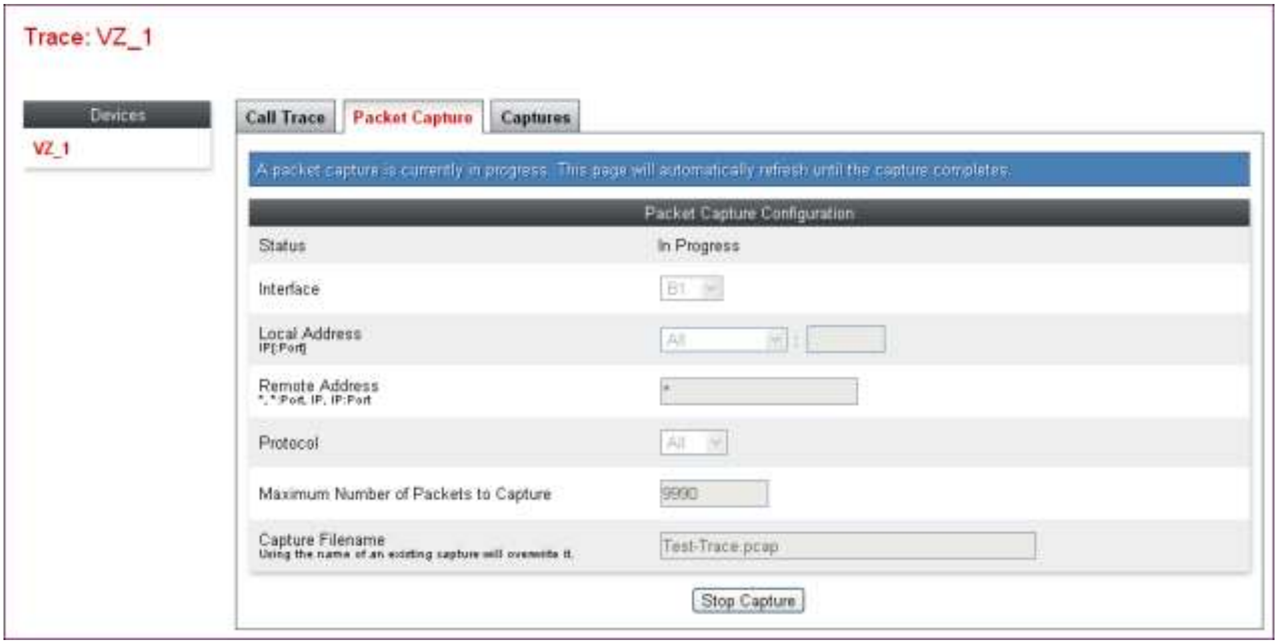
	Task Description	Status
✓	EMS Link Check	eth5 is operating within normal parameters with a - duplex connection at 10Mb/s.
✓	UC-Sec Link Check: A1	eth3 is operating within normal parameters with a - duplex connection at 10Mb/s.
✓	UC-Sec Link Check: B1	eth1 is operating within normal parameters with a - duplex connection at 10Mb/s.
✓	Ping: UC-Sec (10.80.140.141) to Gateway (10.80.140.1)	Average ping from 10.80.140.141 to 10.80.140.1 is 1.232ms.
✗	Ping: UC-Sec (10.80.140.141) to Primary DNS (172.30.209.4)	Error: Unable to reach 172.30.209.4 from 10.80.140.141.
✓	Ping: UC-Sec (2.2.2.2) to Gateway (2.2.2.1)	Average ping from 2.2.2.2 to 2.2.2.1 is 1.809ms.
✗	Ping: UC-Sec (2.2.2.2) to Primary DNS (172.30.209.4)	Error: Unable to reach 172.30.209.4 from 2.2.2.2.

9.3.4. Tracing

To take a call trace, Select **Device Specific Settings → Troubleshooting → Tracing** from the left-side menu as shown below.

Select the Packet Capture tab and set the desired configuration for a call trace and click **Start Capture**.

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, click the **Stop Capture** button at the bottom.



Select the **Captures** tab at the top and the capture will be listed; select the File Name and choose to open it with an application like Wireshark.

10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager 6.3.2, and the Avaya Session Border Controller for Enterprise Release 6.2 can be configured to interoperate successfully with Verizon Business IP Trunk service. This solution allows Avaya CS1000E users access to the PSTN using a Verizon Business IP Trunk public SIP trunk service connection.

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] *Implementing Avaya Aura® Session Manager*, Release 6.3
[2] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3
[3] *Upgrading Avaya Aura® Session Manager,* Release 6.3
[4] *Maintaining and Troubleshooting Avaya Aura® Session Manager Release 6.3*
[5] *Installing and Configuring Avaya Aura® System Platform Release 6.3*, June 2013
[6] *Implementing Avaya Aura® System Manager Release 6.3*, June 2013
[7] *Upgrading Avaya Aura® System Manager to 6.3.2*, July 2013
[8] *Avaya Communication Server 1000E Installation and Commissioning*, April 2012, Document Number NN43041-310.
[9] *Feature Listing Reference Avaya Communication Server 1000*, November 2010, Document Number NN43001-111, 05.01.
[10] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, April 2013, Document Number NN43001-315
[11] *Unified Communications Management Common Servers Fundamentals Avaya Communication Server 1000*, February 2013, Document Number NN43001-116
[12] *Software Input Output Reference – Maintenance Avaya Communication Server 1000*, April 2012, Document Number NN43001-711
[13] *Signaling Server IP Line Applications Fundamentals Avaya Communication Server 1000*, October 2011, Document Number NN43001-125
[14] *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, December 2011, Document Number NN43170-600
[15] RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/

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