Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Session Border Controller for Enterprise. The enterprise equipment is integrated with the Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite is comprised of the IP Toll Free VoIP Inbound and IP-IVR SIP trunk service offers. This service suite provides toll free inbound calling via standards-based SIP trunks. Using the sample configuration, PSTN callers may dial toll-free numbers associated with the IP Toll Free and IP-IVR services to reach Avaya Communication Server 1000E telephone users.

Avaya Communication Server 1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon Labs independent certification.

Verizon Business is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab, utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IPCC Services.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E (CS1000E) Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Session Border Controller for Enterprise (ASBCE). The enterprise equipment is integrated with the Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite is comprised of the IP Toll Free VoIP Inbound and IP-IVR SIP trunk service offers. This service suite provides toll free inbound calling via standards-based SIP trunks. Using the sample configuration, PSTN callers may dial toll-free numbers associated with the IP Toll Free and IP-IVR services to reach Avaya Communication Server 1000E telephone users.

Avaya CS1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon Labs independent certification.

Access to the IPCC Services suite may use Internet Dedicated Access (IDA) or Private IP (PIP). The configuration documented in these Application Notes used the Verizon IPCC service terminated via a PIP network connection, but the solution validated in this document can also be applied to IPCC services delivered via IDA service terminations. IP Toll Free VoIP Inbound is the base service offering that offers core call routing and termination features. IP-IVR is an enhanced service offering that includes features such as menu-routing, custom transfer, and additional media capabilities.

In the sample configuration, an Avaya Session Border Controller for Enterprise (ASBCE) is used as an edge device between the Avaya Customer Premise Equipment(CPE) and Verizon Business. The ASBCE performs SIP header manipulation and topology hiding to convert the private Avaya CPE IP addressing to IP addressing appropriate for the Verizon access method.

Customers using Avaya Communication Server 1000E with the Verizon Business IP Contact Center services are able to receive inbound toll-free calls from the PSTN via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

For more information on the Verizon Business IP Contact Center service, including access alternatives, visit http://www.verizonbusiness.com/products/contactcenter/ip/

2. General Test Approach and Test Results

Avaya CS1000E location was connected to the Verizon Business IPCC Service, as depicted in **Figure 1.** Avaya equipment was configured to use the commercially available IP Toll Free VoIP Inbound and IP-IVR services that comprise the Verizon Business IPCC Services suite.

2.1. Interoperability Compliance Testing

The SIP trunk interoperability testing included the following:

- Incoming calls from the PSTN were routed to the toll-free numbers assigned by Verizon Business to the Avaya CS1000E location. These incoming were answered by Avaya IP-UNIStim telephones, Avaya SIP telephones, and Avaya digital telephones. The display of caller ID on display-equipped Avaya telephones was verified.
- Proper disconnect when the PSTN caller abandons a call before answer.
- Proper disconnect when either party hangs up an active call.
- Proper busy tone heard when a PSTN user calls a toll-free number directed to a busy CS1000E user (i.e., if no redirection is configured for user busy conditions).
- Privacy requests for inbound toll-free calls from the PSTN were verified. That is, when privacy is requested by a PSTN caller (e.g., dialing *67 from a mobile phone), the inbound toll-free call can be successfully completed to a CS1000E user while presenting an anonymous display to the CS1000E user.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Both Verizon Business and the enterprise SBC can monitor health using SIP OPTIONS.
- Calls using the G.729A (IP Toll Free) and G.711 ULAW (IP-IVR) codecs, and proper protocol procedures related to media.
- DTMF transmission using RFC 2833.
- Inbound toll-free calls with long holding times and call stability
- Long duration calls.
- Telephony features such as call waiting, hold, transfer, and conference. Note that CS1000E will not send REFER to the Verizon network.
- Proper DiffServ markings for SIP signaling and RTP media sent to Verizon.

2.2. Test Results

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

1. The Verizon IPCC Service does not support fax.

2. Although the Verizon Business IP Contact Center service supports transfer using the SIP REFER method, Avaya CS1000E does not support sending REFER to Verizon.

3. The SIP protocol allows sessions to be refreshed for calls that remain active for some time. In the tested configuration, neither Verizon nor CS1000E send re-INVITE or UPDATE messages to refresh a session. In the tested configuration, this is transparent to the users that are party to the call in that the media paths remain established.

2.3. Support

2.3.1 Avaya

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

2.3.2 Verizon

For technical support on Verizon Business IPCC 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 IPCC service. Avaya equipment is located on a private IP network. An enterprise edge router provides access to the Verizon IPCC service network via a T1 circuit provisioned for the Verizon Business Private IP (PIP) service. At the edge of the Avaya CPE location, an Avaya Session Border Controller for Enterprise (ASBCE) provides topology hiding and SIP header manipulation. The ASBCE receives traffic from Verizon Business IPCC Services on port 5060 and sends traffic to the Verizon Business IPCC Services using destination port 5071, using the UDP protocol.

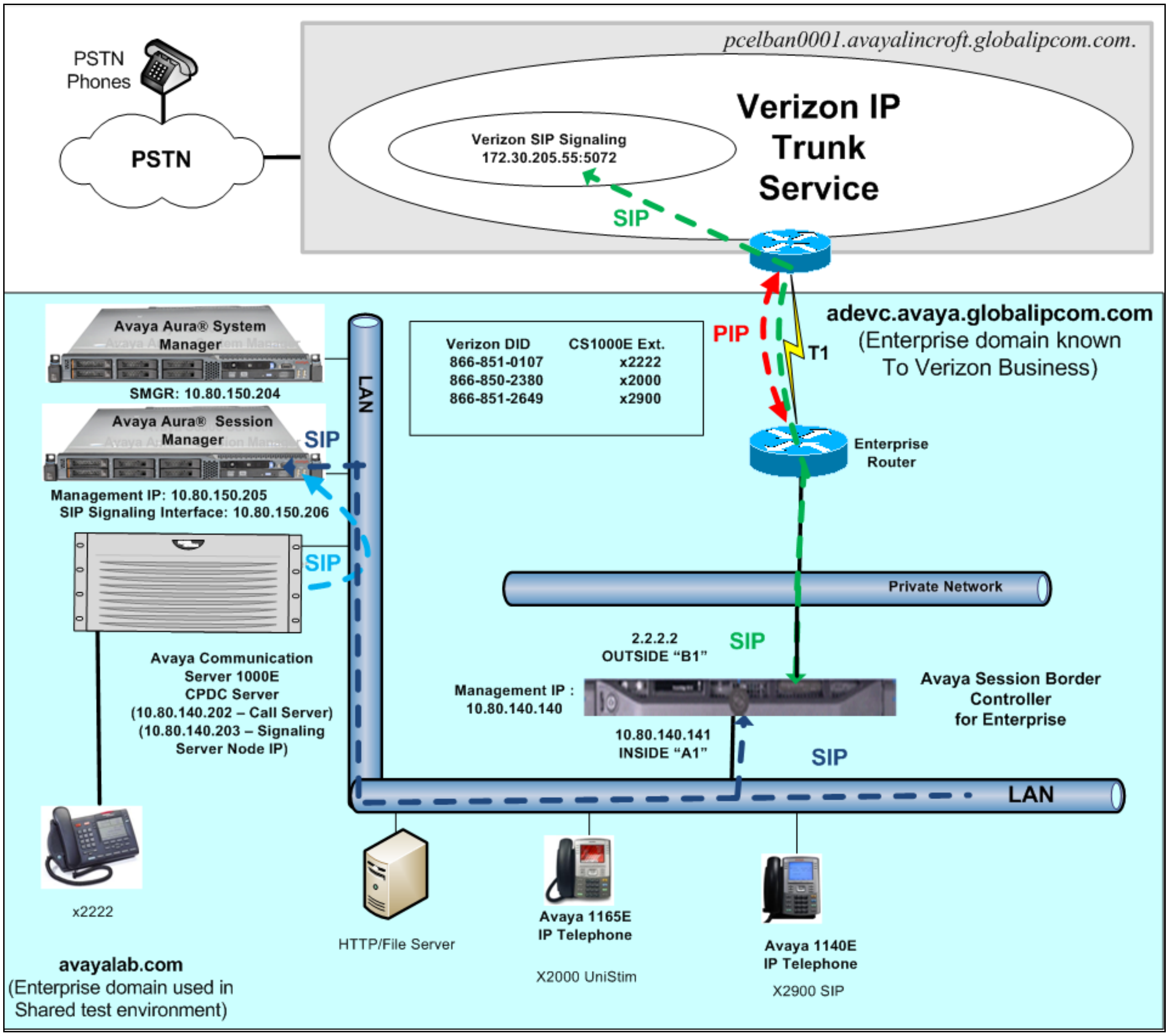


Figure 1: Avaya Interoperability Test Lab Configuration

The Avaya CPE was known to Verizon Business as FQDN *adevc.avaya.globalipcom.com*. For efficiency, the Avaya environment utilizing Avaya Aura® Session Manager Release 6.1 and Communication Server 1000E Release 7.5 was shared among many ongoing test efforts at the Avaya Solution and Interoperability Test lab. Access to the Verizon Business IPCC service was added to a configuration that already used domain “avayalab.com” at the enterprise. Session Manager is used to adapt the “avayalab.com” domain to the domains known to Verizon, defined in **Section 8.1**. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Server 1000E and Session Manager match the CPE domain known to Verizon.

Table 1 lists a sampling of Verizon Business IP Toll-Free numbers that terminated at the Avaya CS1000E location. These toll-free numbers were mapped to Avaya CS1000E users via an Avaya Aura® Session Manager adaptation.

Verizon Provided Toll-Free	Avaya CS1000E Destination	Notes
866-851-0107	x2222	Avaya M3904 Digital Telephone
866-850-2380	x2000	Avaya 1165E IP Deskphone (UNIStim)
866-851-2649	x2900	Avaya 1140E IP Deskphone (SIP)

Table 1: Sample Verizon IP Toll Free Number 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.

- Avaya CPE Fully Qualified Domain Name (FQDN)
    - *adevc.avaya.globalipcom.com*
- Avaya Session Border Controller for Enterprise(ASBCE) 4.0.5Q09
- Avaya Communication Server 1000E Release 7.5
- Avaya Aura® System Manager Release 6.1
- Avaya Aura® Session Manager Release 6.1
- Avaya 1100-Series IP Deskphones using UNIStim software
- Avaya 1140E IP Deskphones using SIP software, registered to the CS1000E
- Avaya M3900-Series Digital phones

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment/Software	Release/Version
Avaya Communication Server 1000E running on CP+DC server as co-resident configuration	Release 7.5, Version 7.50.17 (with latest Patches and Deplist) Plug-in 201 Enabled Plug-in 501 Enabled
Avaya Aura® System Manager running on HP Common Server	Release 6.1.0 (Build Number 6.1.0.0.7345 Patch 6.1.5.502)
Avaya Aura® Session Manager running on HP Common Server	Release 6.1 (Load 6.1.5.0.615006)
Avaya Session Border Controller for Enterprise running on Dell R210 V2 server	4.0.5Q09
Avaya 1100-Series IP Deskphones (UNIStim)	FW 0626C8A
Avaya 1140E IP Deskphones (SIP)	SIP 04.03.09.00

Table 2: Equipment and Software Used in the Sample Configuration

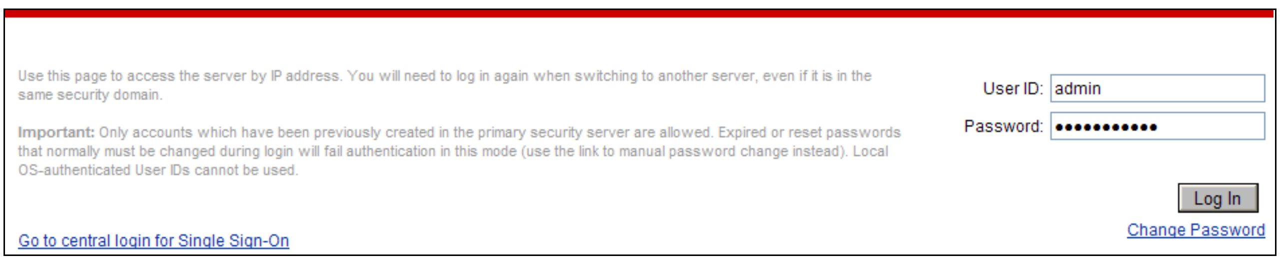
5. Configure Avaya Communication Server 1000E

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

Avaya Aura® Session Manager Release 6.1 provides all the SIP Proxy Service (SPS) and Network Connect Services (NCS) functions previously provided by the Network Routing Service (NRS). As a result, the NRS application is not required to configure a SIP trunk between Avaya Communication Server 1000E and Session Manager.

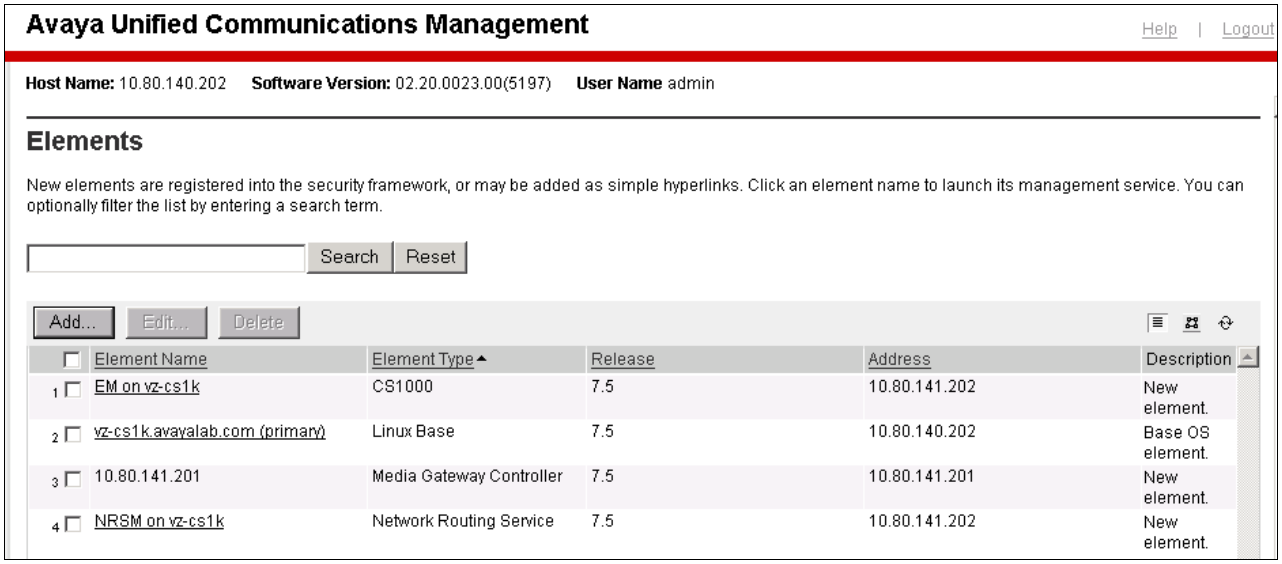
This section focuses on the SIP Trunking configuration. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the Call Server and SIP Signaling Server applications has been completed, and that the Avaya Communication Server 1000E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

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://<ip-address>** where the relevant <ipaddress> in the sample configuration is 10.80.140.202.
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 Communication Server 1000E 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 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 **Services** category on the right side of the page, click the **UCM Services** link (not shown). For more information on configuring System Manager as Primary Security Server, see **Reference [2].**

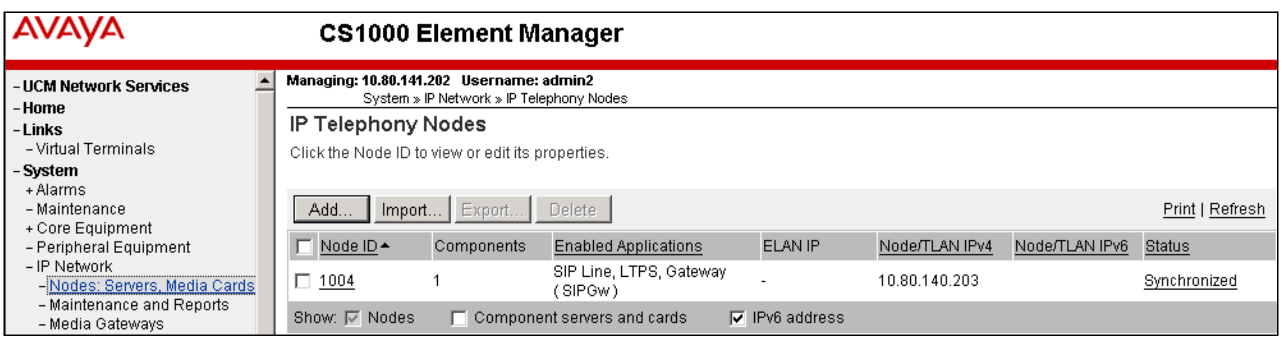
The Avaya Unified Communications Management **Elements** page will be used for configuration. Click on the **Element Name** corresponding to "CS1000" in the **Element Type** column. In the abridged screen below, the user would click on the **Element Name** "EM on vz_cs1k".



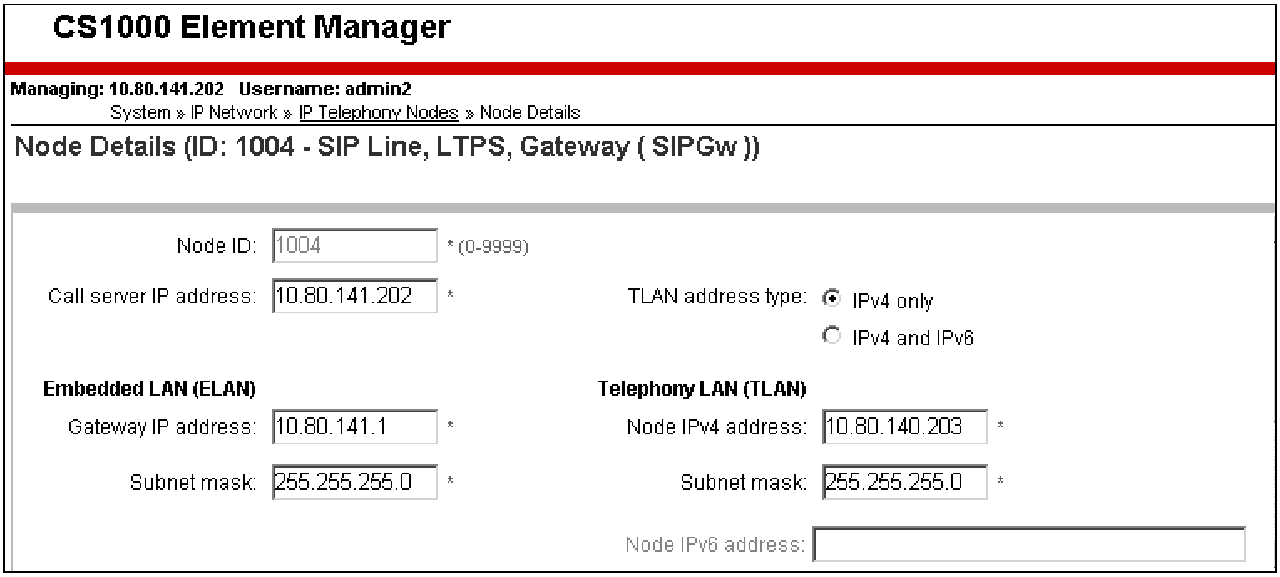
5.1. Node and Key IP Addresses

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

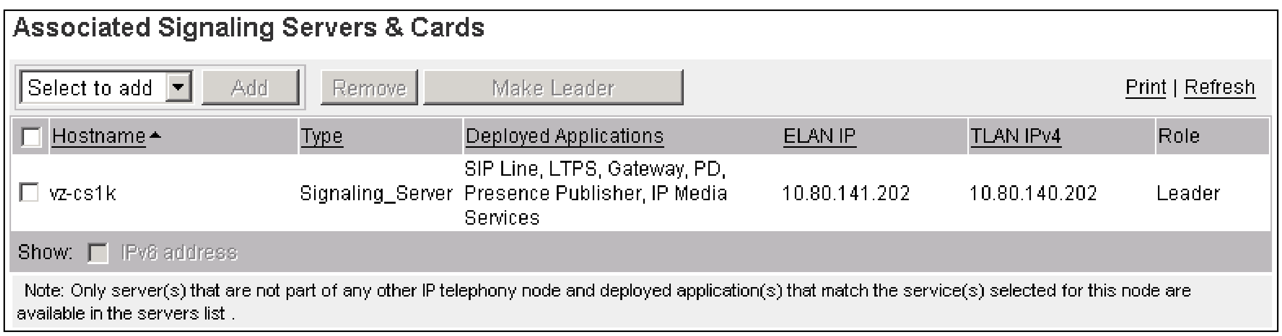
The **IP Telephony Nodes** page is displayed as shown below. Click "**<Node id>**" in the **Node ID** column to view details of the node. In the sample configuration, **Node ID** "**1004**" was used.



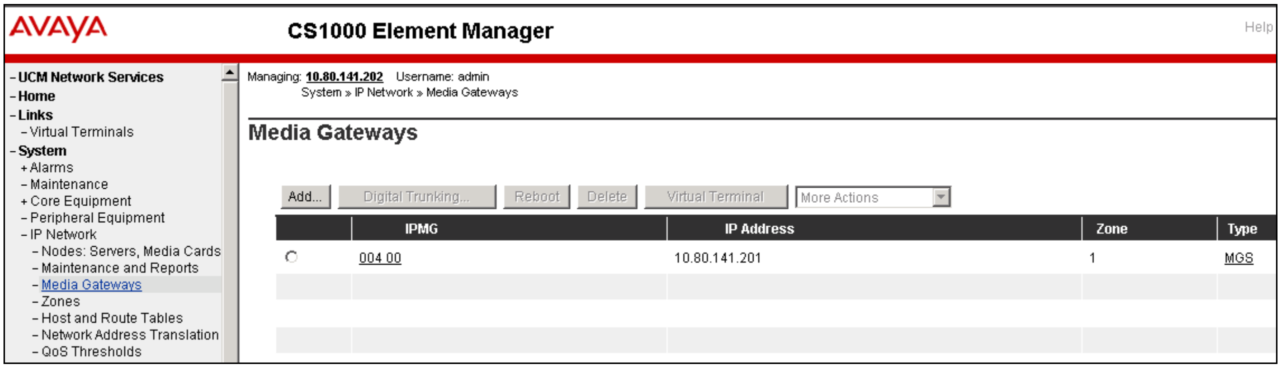
The **Node Details** screen is displayed with additional details as shown below. Under the **Node Details** heading at the top of the screen, make a note of the **Node IPV4 address** under **Telephony LAN (TLAN).** In the sample screen below, the **Node IPV4 address** is **"10.80.140.203".** This IP address will be needed when configuring Session Manager with a SIP Entity for the CS1000E.



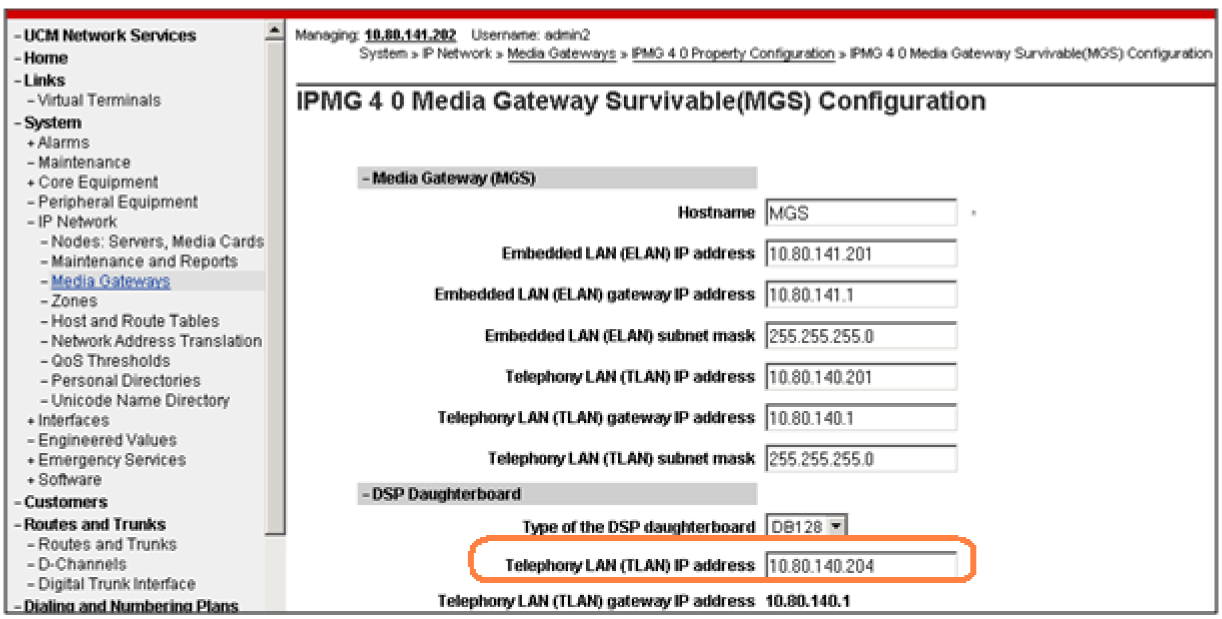
The following screen shows the **Associated Signaling Servers & Cards** heading at the bottom of the screen, simply to document the configuration.



Expand **System → IP Network** on the left panel and select **Media Gateways.** Select the media gateway listed, here **'004 00'.** Click **Next** (not shown).



The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard** 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 IPCC service, the IP Address in the SDP in the INVITE message will be "**10.80.140.204**" in the sample configuration.

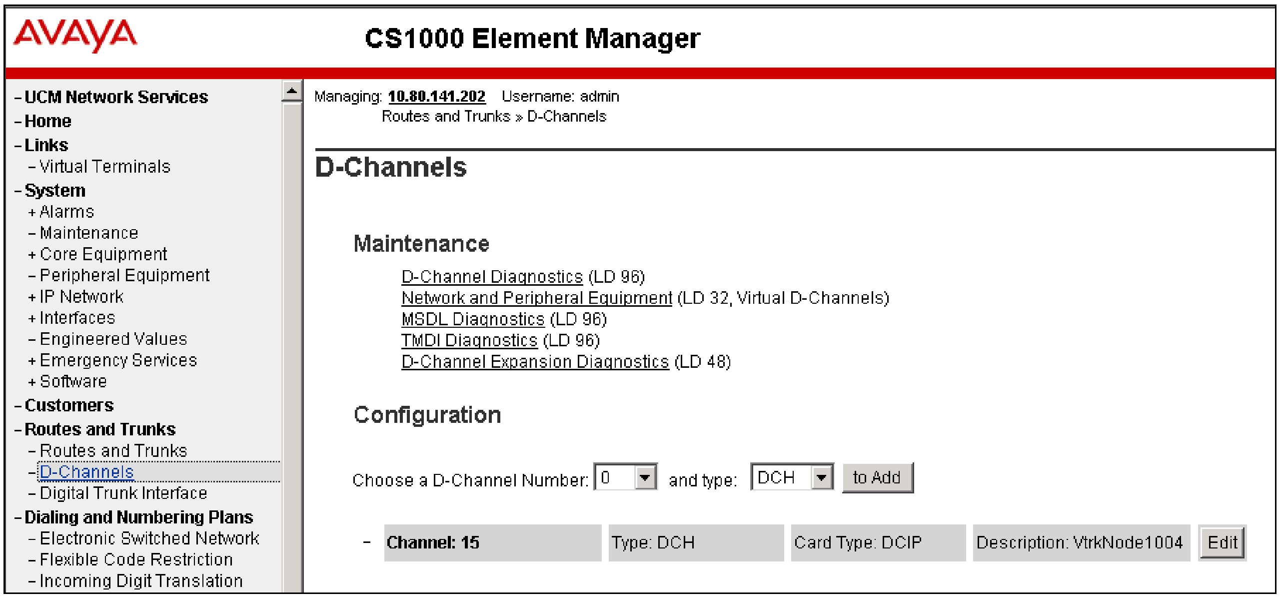


5.2. Virtual D-Channel, Routes and Trunks

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

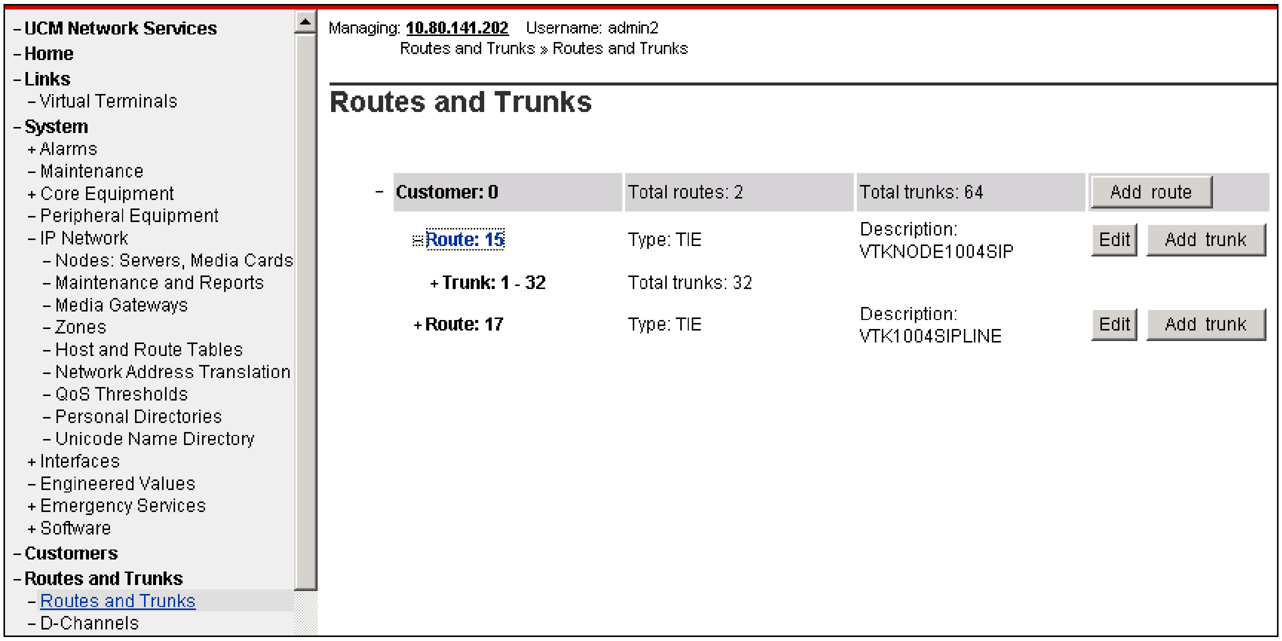
5.2.1 Virtual D-Channel Configuration

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

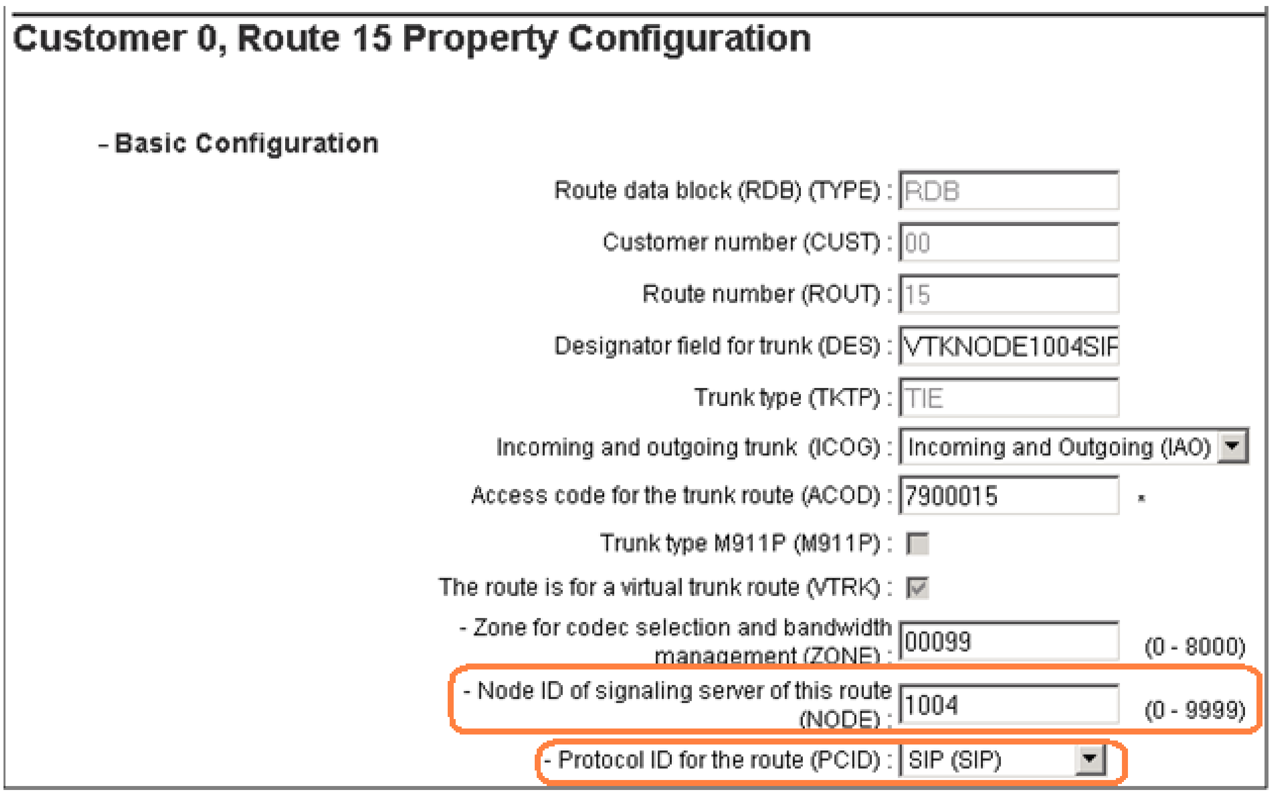


5.2.2 Routes and Trunks Configuration

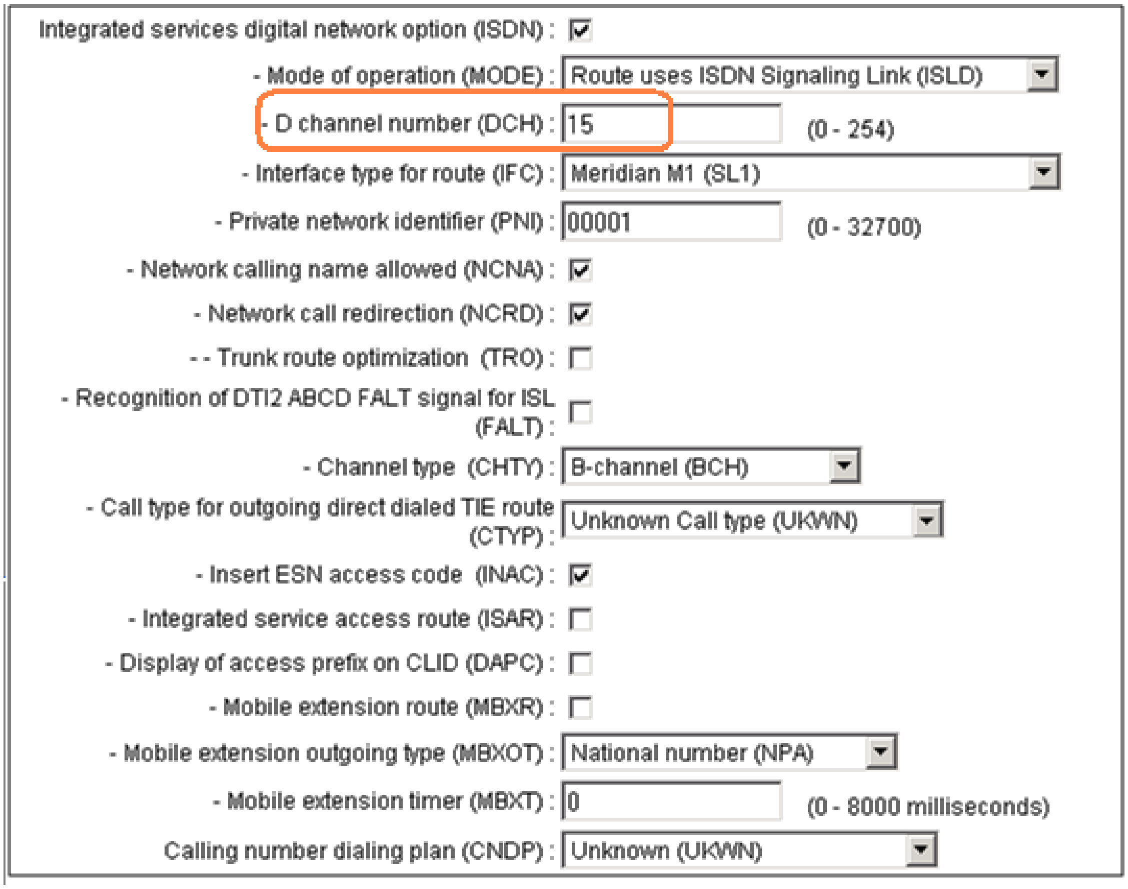
In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured. Expand **Routes and Trunks** on the left navigation panel and expand the customer number. In the example screen that follows, it can be observed that **Route 15** has 32 trunks in the sample configuration.



Select **Edit** to verify the configuration, as shown below. Verify “**SIP (SIP)”** has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.1**. 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. 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.



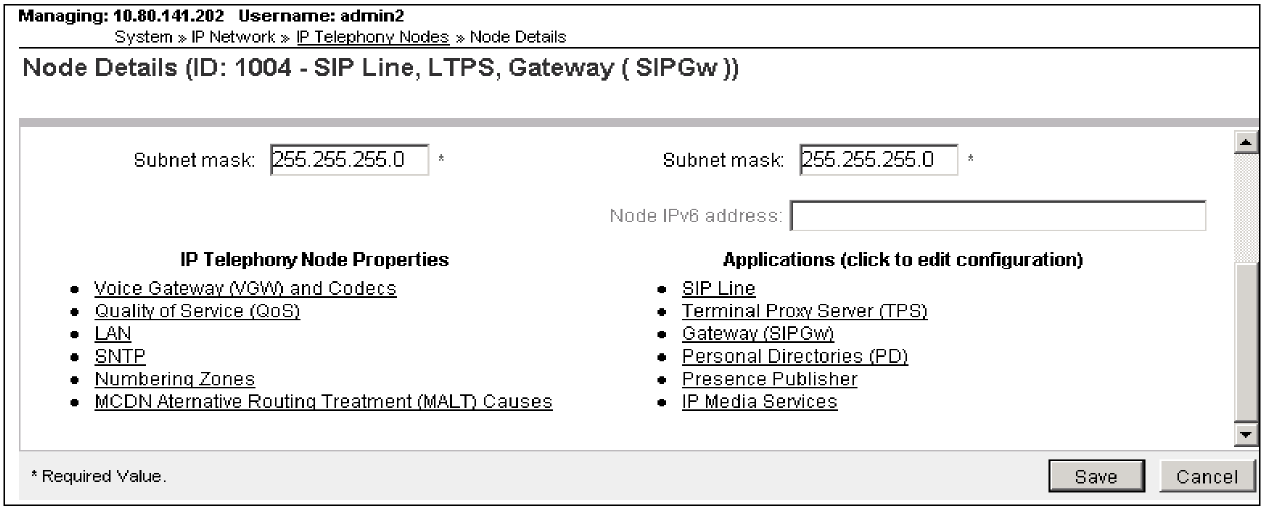
Scrolling down, other parameters may be observed. The **D channel number (DCH)** field must match the D-Channel number shown in **Section 5.2.1**.



5.3. SIP Trunk to Avaya Aura® Session Manager

Expand **System → IP Network → Nodes: Servers, Media Cards**. Click "**1004**" in the **Node ID** column (not shown) to edit configuration settings for the configured node.

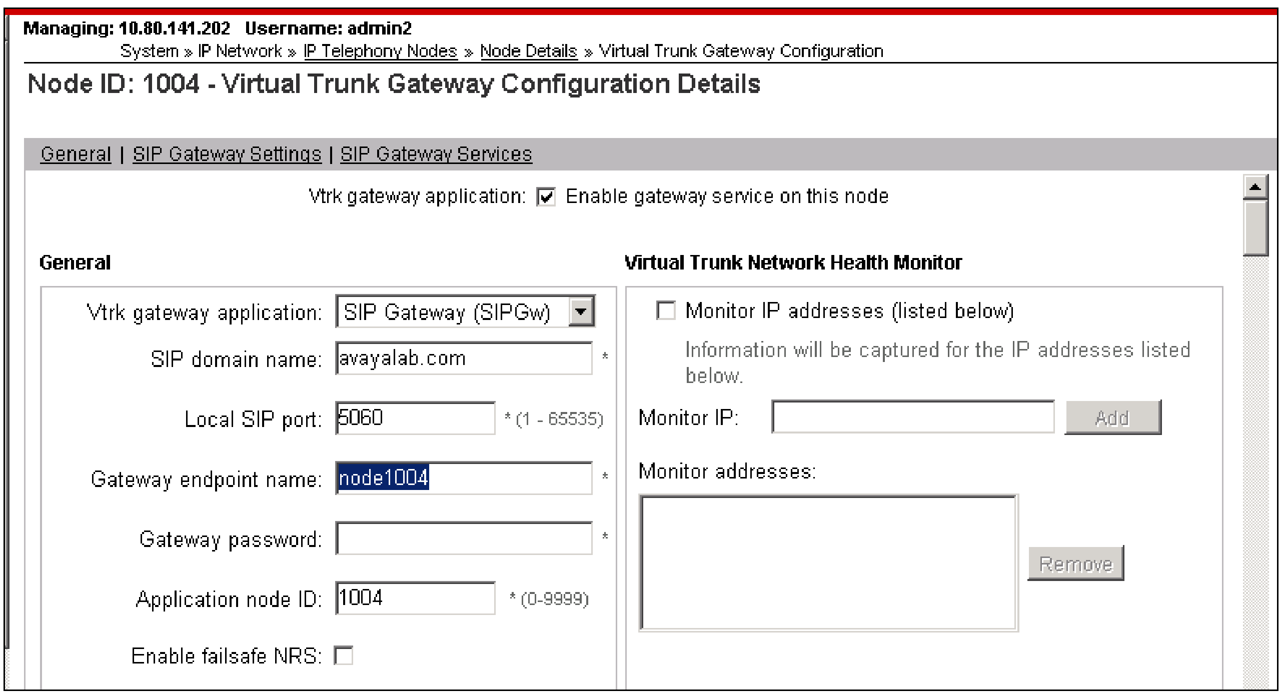
Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Gateway (SIPGw)** link to view or edit the SIP Gateway configuration.



On the **Node ID: 1004 - 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 shared Avaya Solution and Interoperability Test lab environment. Note: The SIP domain name for the enterprise known to Verizon is "*adevc.avaya.globalipcom.com*", and the SIP domain will be adapted by the ASBCE 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 "**1004**" was used matching the node shown in **Section 5.1**.

The values defined for the sample configuration are shown below.

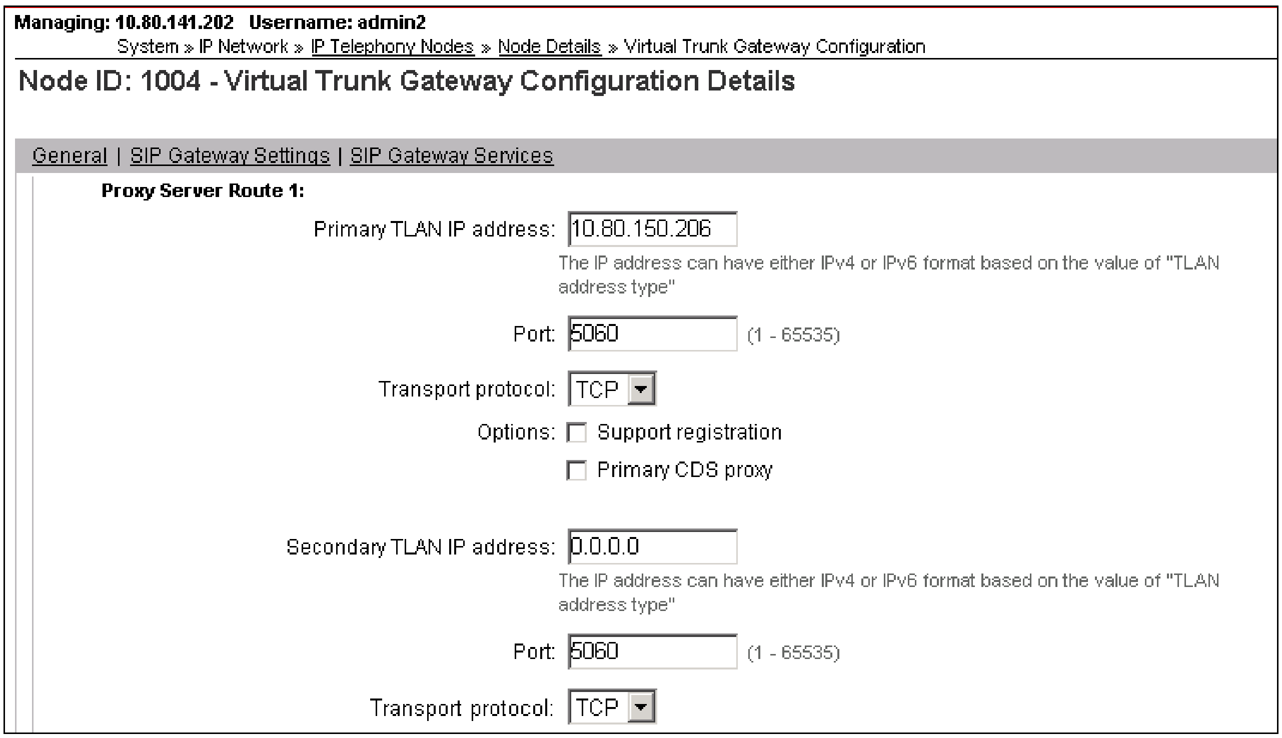


Scroll down to the **SIP Gateway Settings → Proxy or Redirect Server**: section.

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

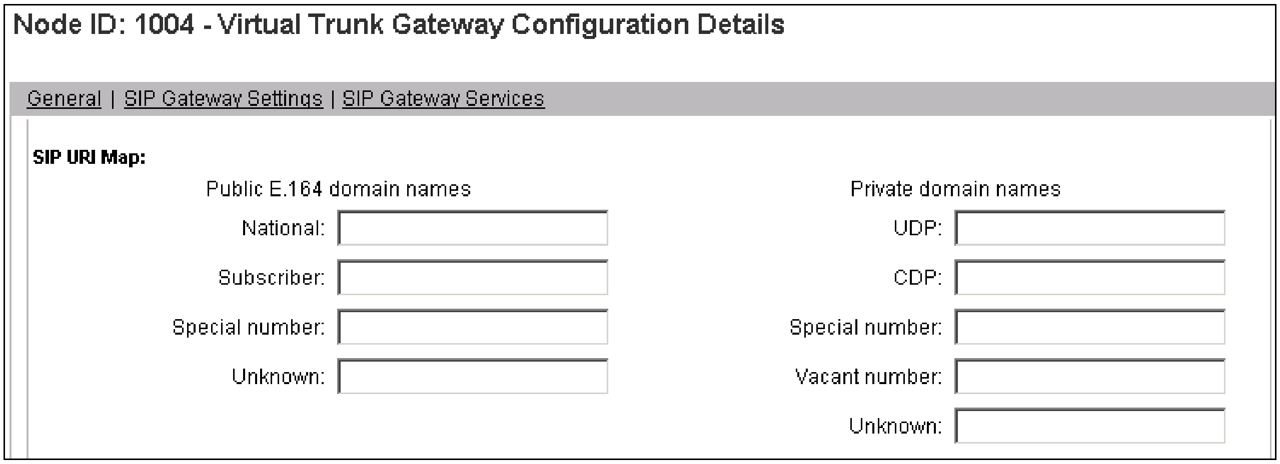
- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface. In the sample configuration, "**10.80.150.206**" was used.
- **Port:** Enter "**5060**".
- **Transport protocol:** Select "**TCP**".

The values defined for the sample configuration are shown below.



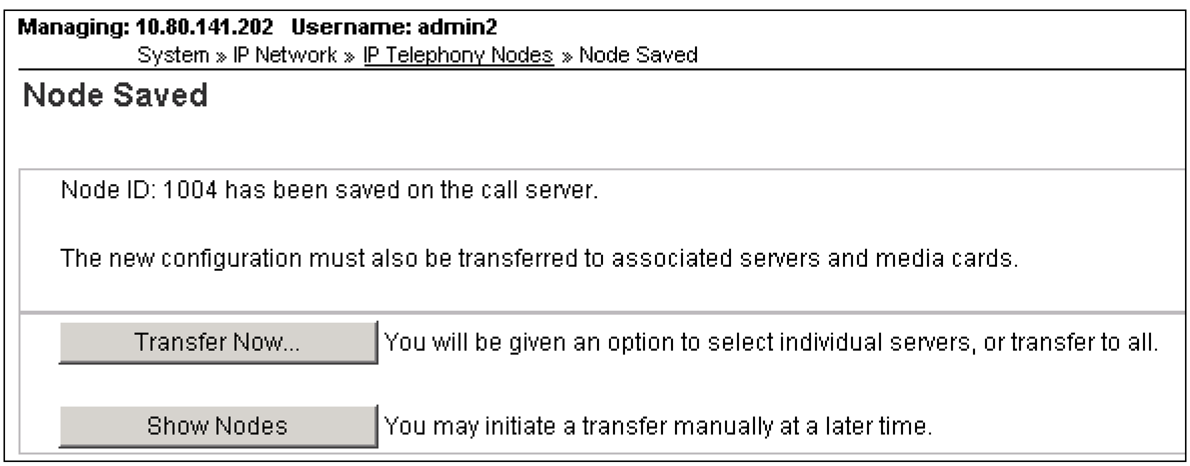
Scroll down and repeat these steps for the **Proxy Server Route 2** (not shown).

Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. In general, the **SIP URI Map** values have been set to blank for calls that may ultimately be routed to the Verizon IPCC service. The CS1000E will put the “string” entered in the **SIP URI Map** in the “phone-context=<string>” parameter in SIP headers such as the P-Asserted-Identity. If the value is configured to blank, the CS1000E will omit the “phone-context=” in the SIP header altogether.

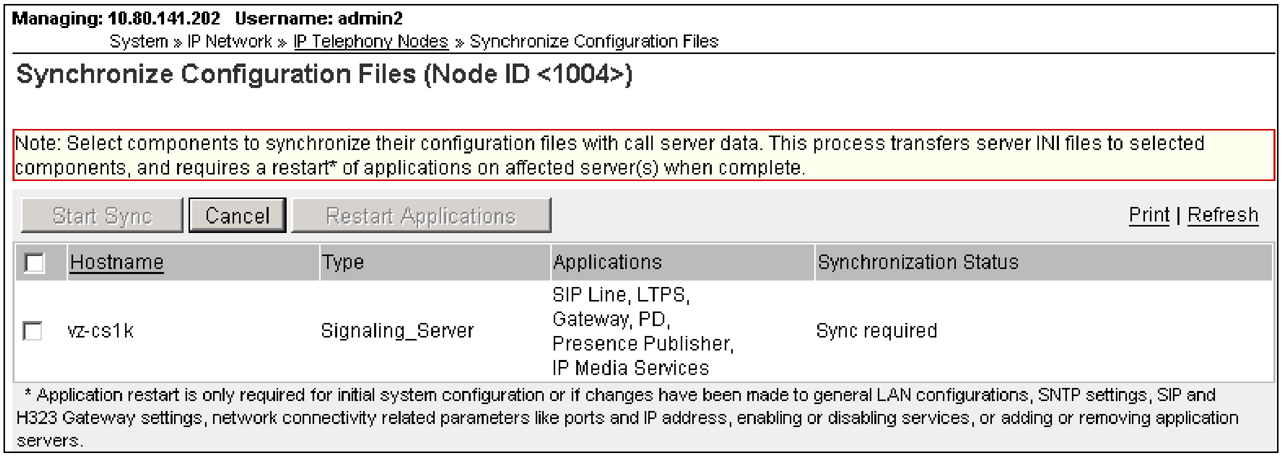


Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen. Click **Save** on the **Node Details** screen (not shown).

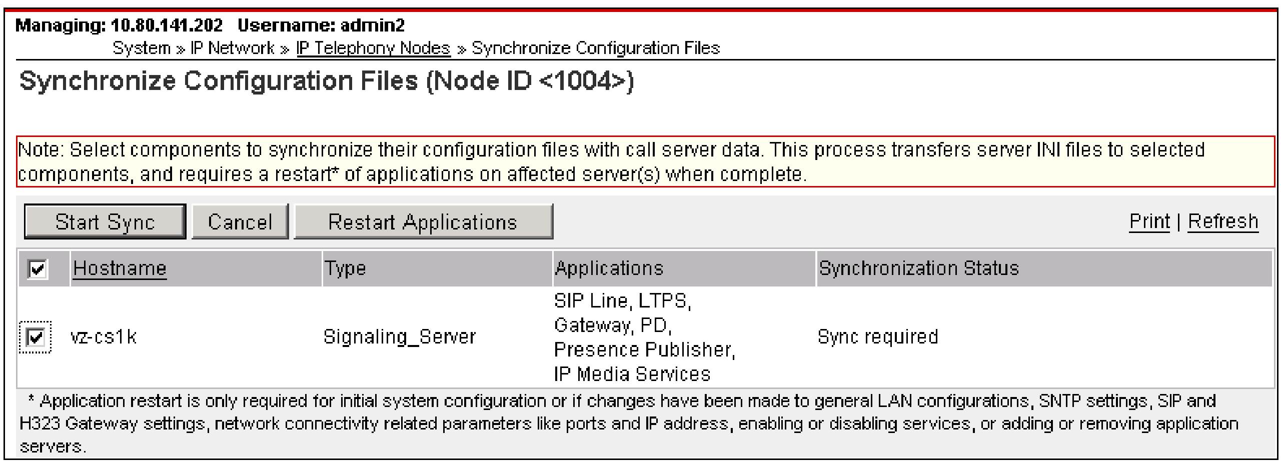
Select **Transfer Now** on the **Node Saved** page as shown below.



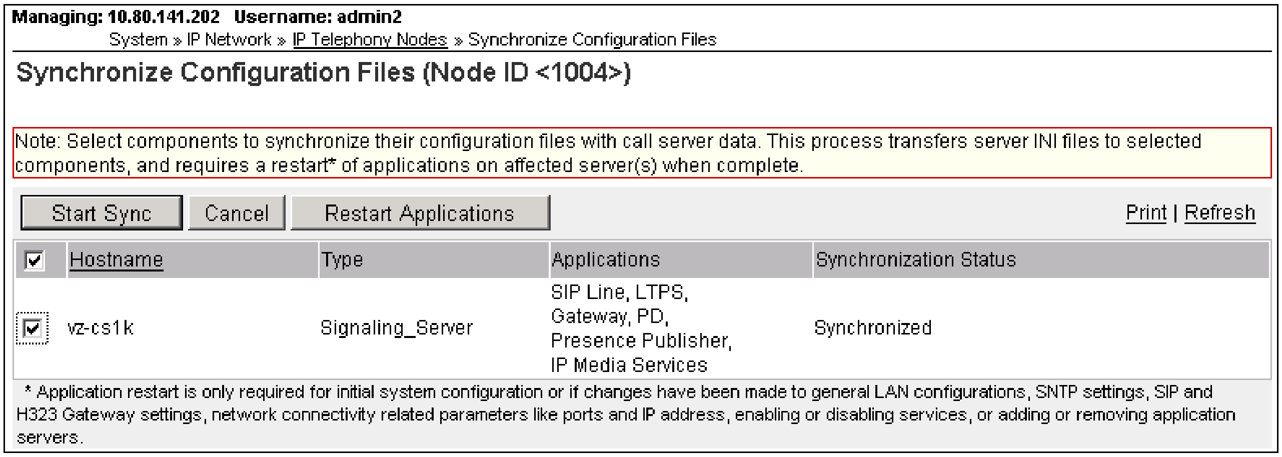
Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.



Select the check box associated with 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 in the previous screen) to **Synchronized** (as shown below). After synchronization completes, select the check box associated with the appropriate Hostname and click **Restart Applications**.

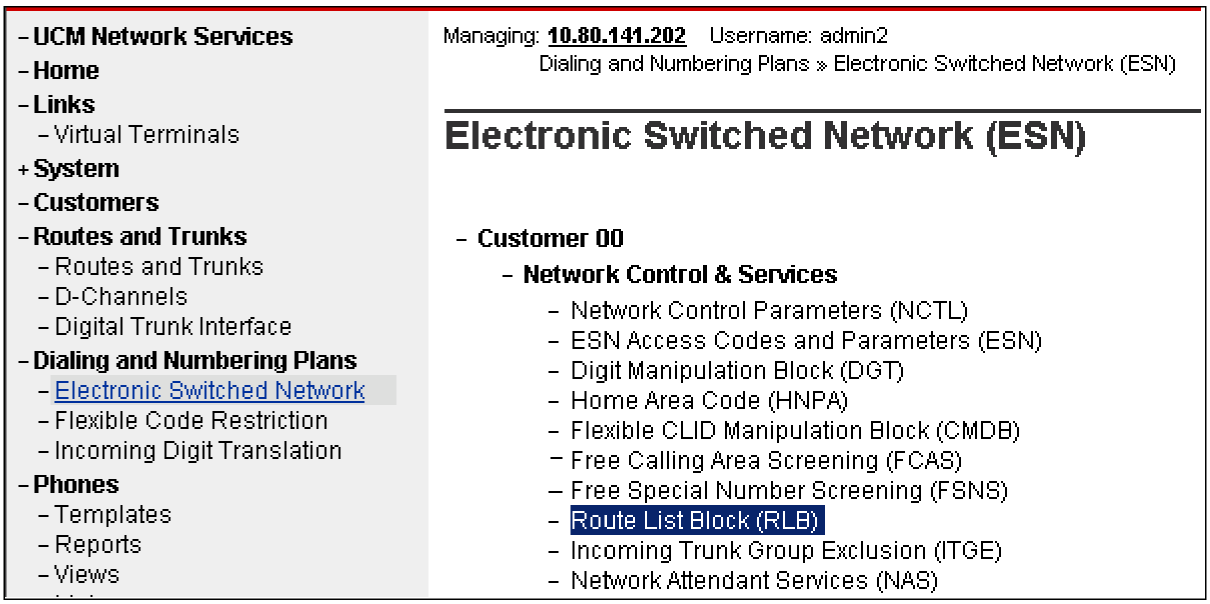


5.4. Routing of Dialed Numbers to Avaya Aura® Session Manager

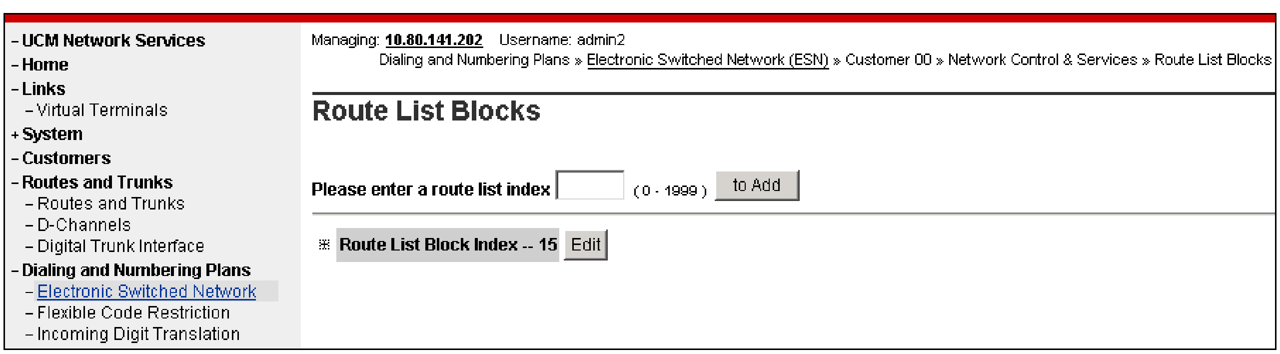
This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Session Manager for calls destined for the Verizon IPCC service. The routing defined in this section is simply an example and not intended to be prescriptive. The example will focus on the configuration enabling a CS1000E telephone user to dial 9-1-303-538-7022 to reach a PSTN telephone using the Verizon IPCC service. Other routing policies may be appropriate for different customer networks.

5.4.1 Route List Block

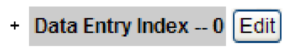
Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network.** Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown below.



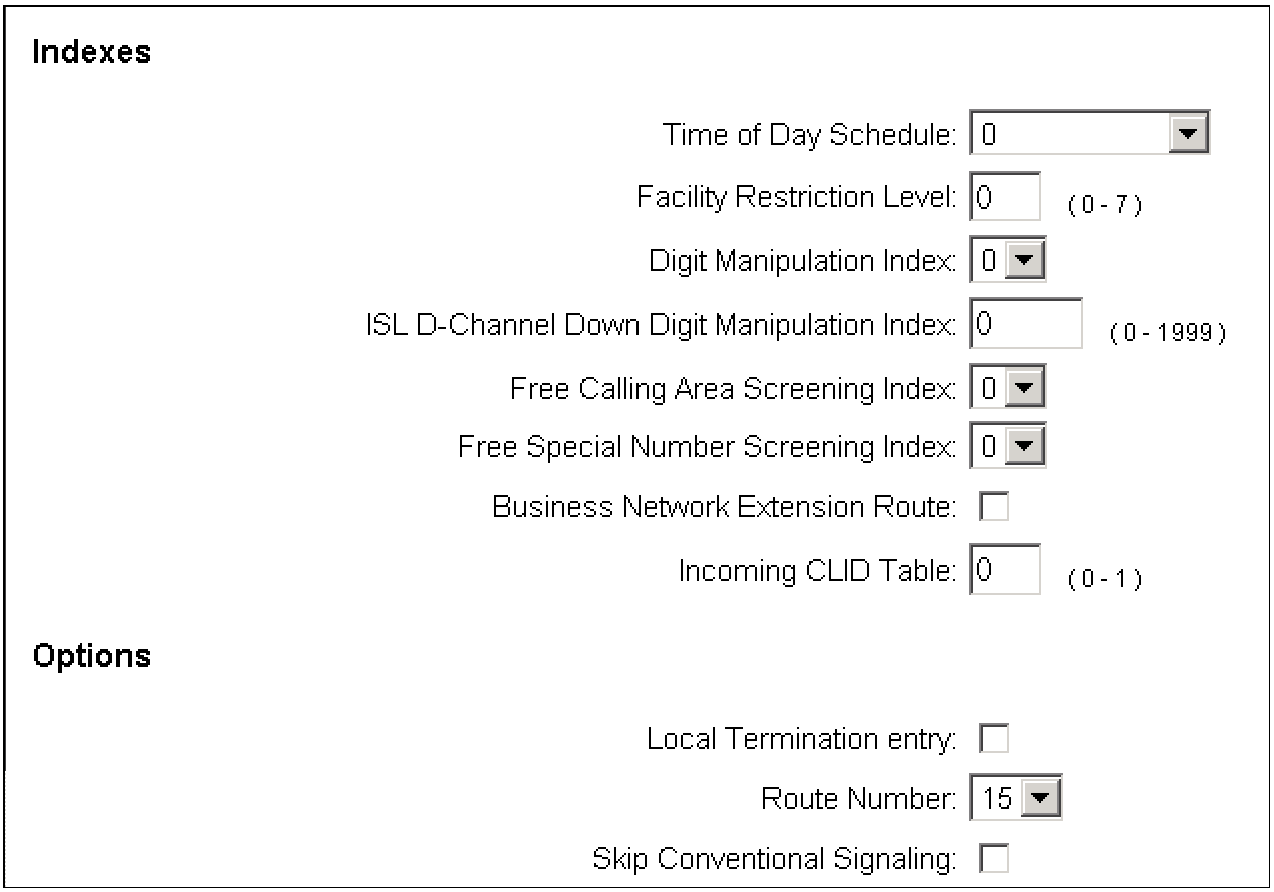
The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click **to Add**, or edit an existing entry by clicking the corresponding **Edit** button. In the sample configuration, route list block index "**15**" is used.



If adding the route list index as new, scroll down to the **Options** area of the screen. If editing an existing route list block index, select the **Edit** button next to the appropriate **Data Entry Index** as shown below, and scroll down to the **Options** area of the screen.



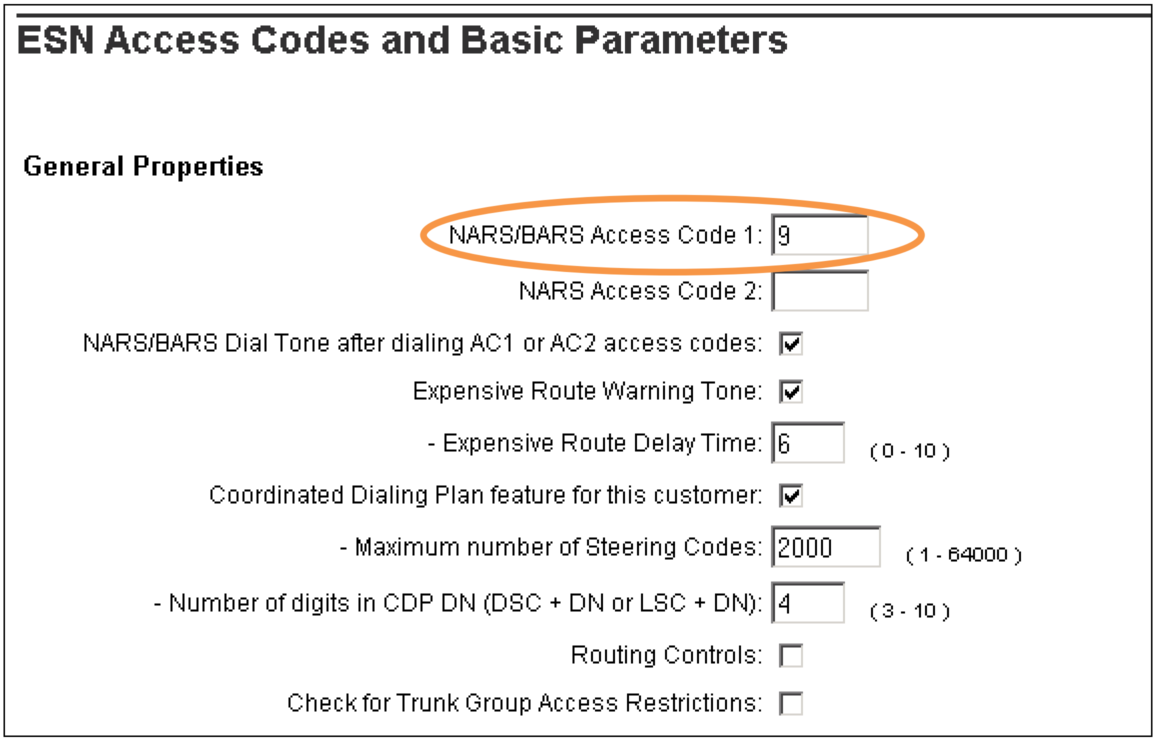
Under the **Options** section, select **“<Route id>”** defined in **Section 5.2.2** in the **Route Number** field. In the sample configuration route number “**15**” was used. Default values may be retained for remaining fields as shown below.



Click **Save** (not shown) to save the Route List Block definition.

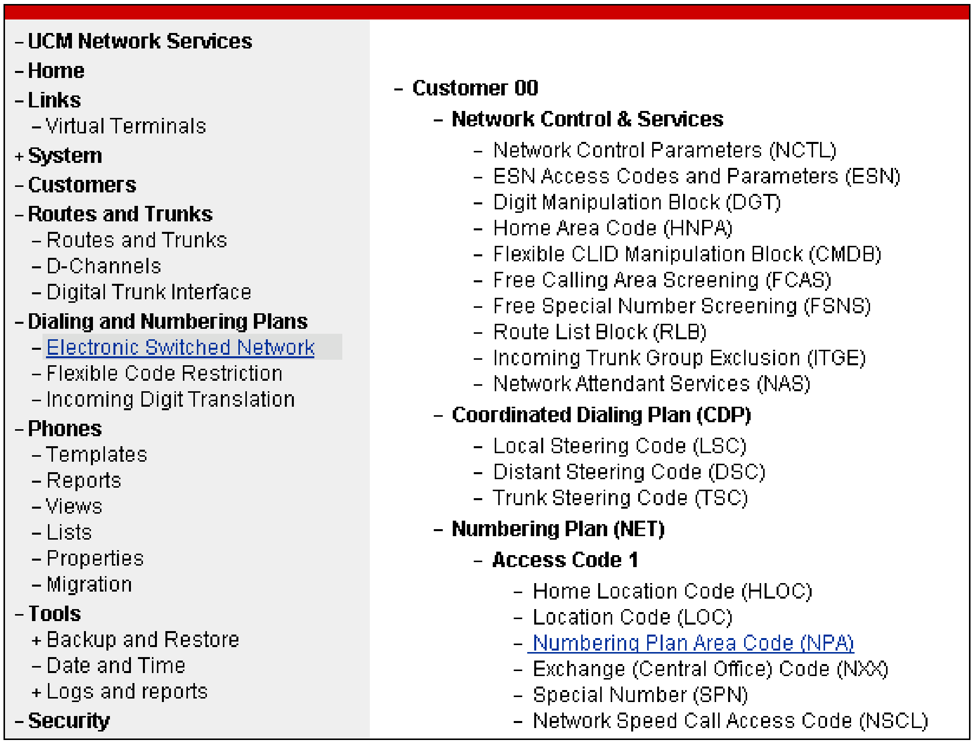
5.4.2 NARS Access Code

Expand **Dialing and Numbering Plans** on the left navigational 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 5.4.1**. 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.

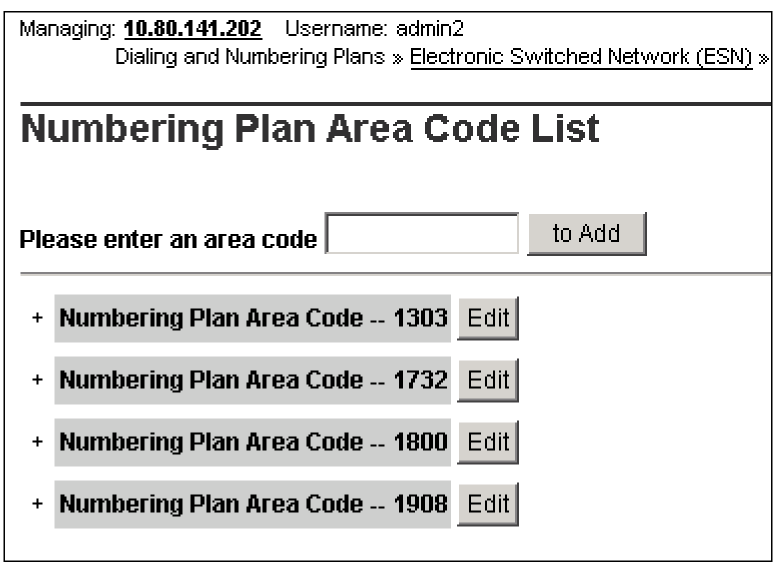


5.4.3 Numbering Plan Area Codes

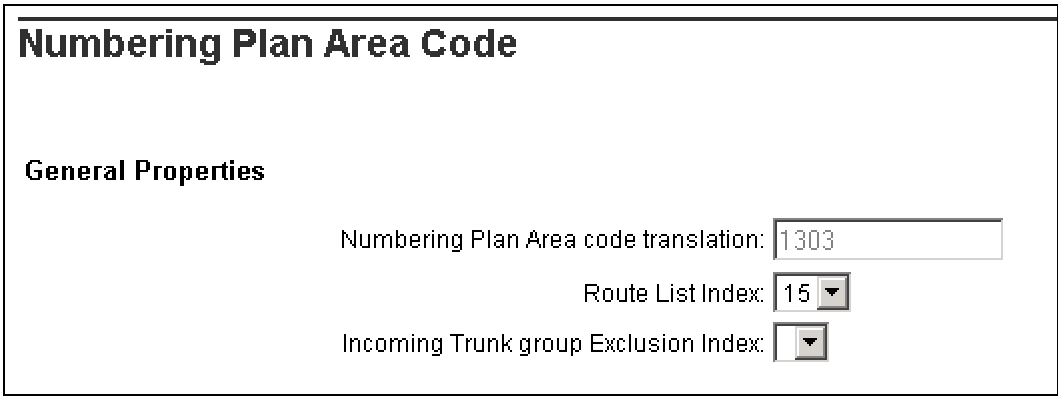
Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network.** Scroll down and select **Numbering Plan Area Code (NPA)** under the appropriate access code heading. In the sample configuration, this is **Access Code 1**, as shown below.



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 "**1800**" and "**1303**" 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 defined in **Section 5.4.1**. 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.

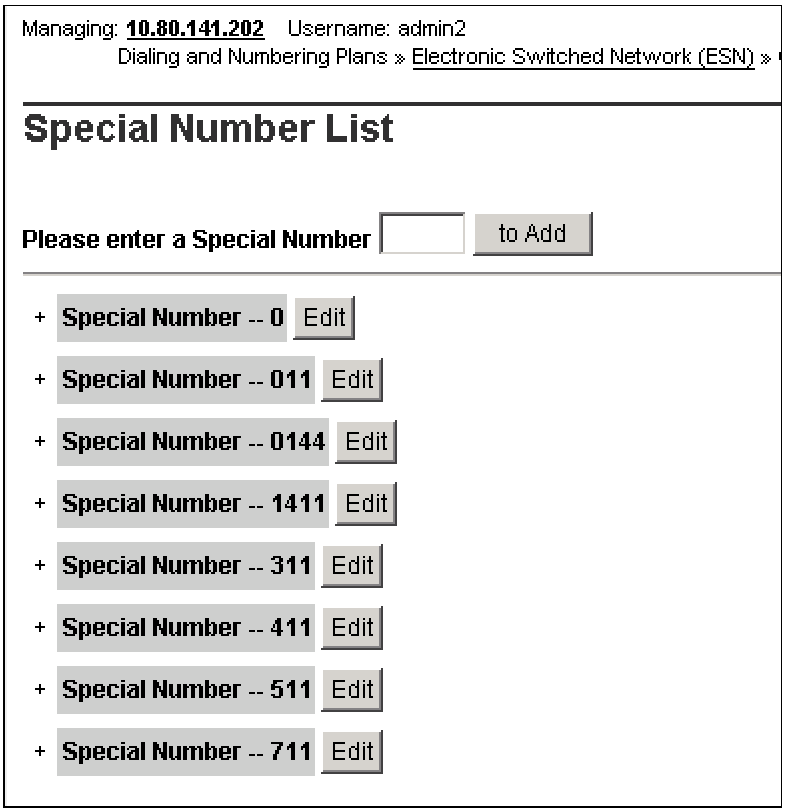


5.4.4 Other Special Numbers to Route to Session Manager

In the testing associated with these Application Notes, non-emergency service numbers such as x11, 1x11, international calls, and operator assisted calls were also routed to Session Manager and ultimately to the Verizon IPCC service. Although not intended to be prescriptive, one approach to such routing is summarized in this section.

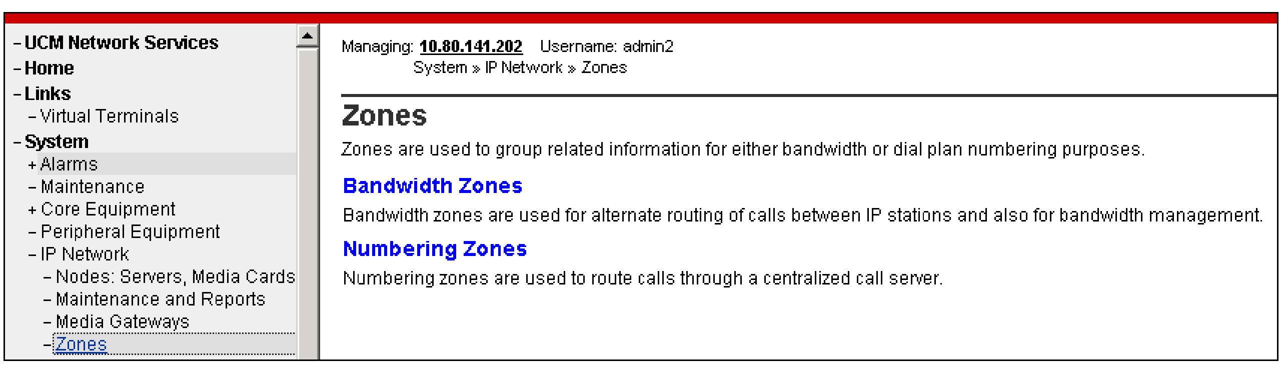
Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network.**   Scroll down and select **Special Number (SPN)** under the appropriate access code heading (as can be observed in the first screen in **Section 5.4.3**).

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**", and non-emergency x11 calls are listed. In each case, **Route list index** "**15**" has been selected in the same manner as shown for the NPAs in the prior section. For special numbers, the **Flexible length** field can also be configured as appropriate for the number. For example, for 511, the **Flexible length** field can be set to "**3**".

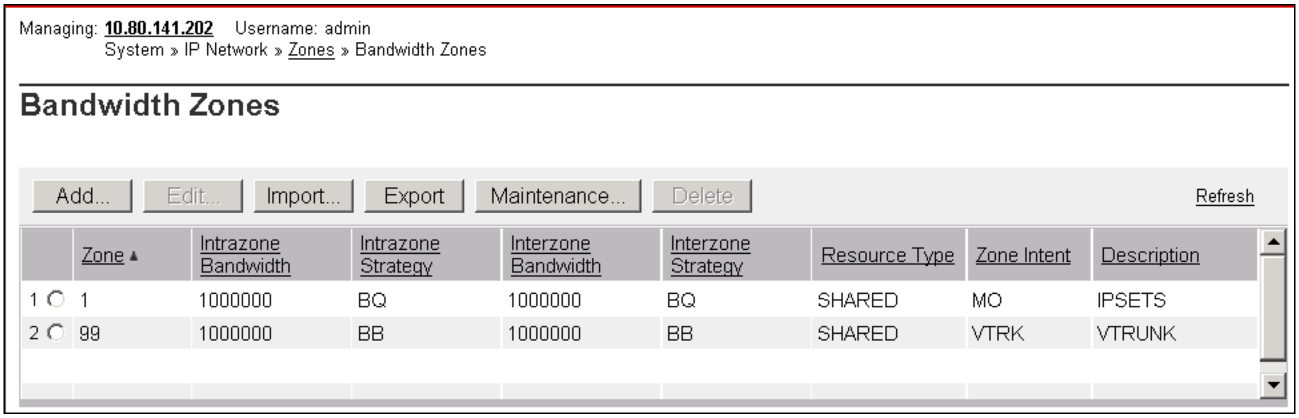


5.5. Zones

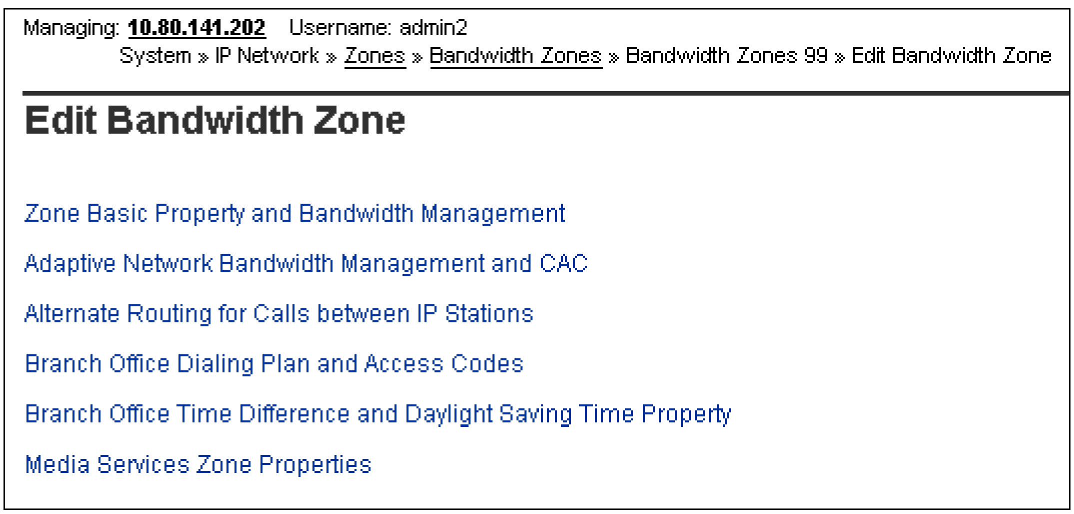
Zone configuration can be used to control codec selection and for bandwidth management. To configure, expand **System → IP Network** and select **Zones** as shown below.



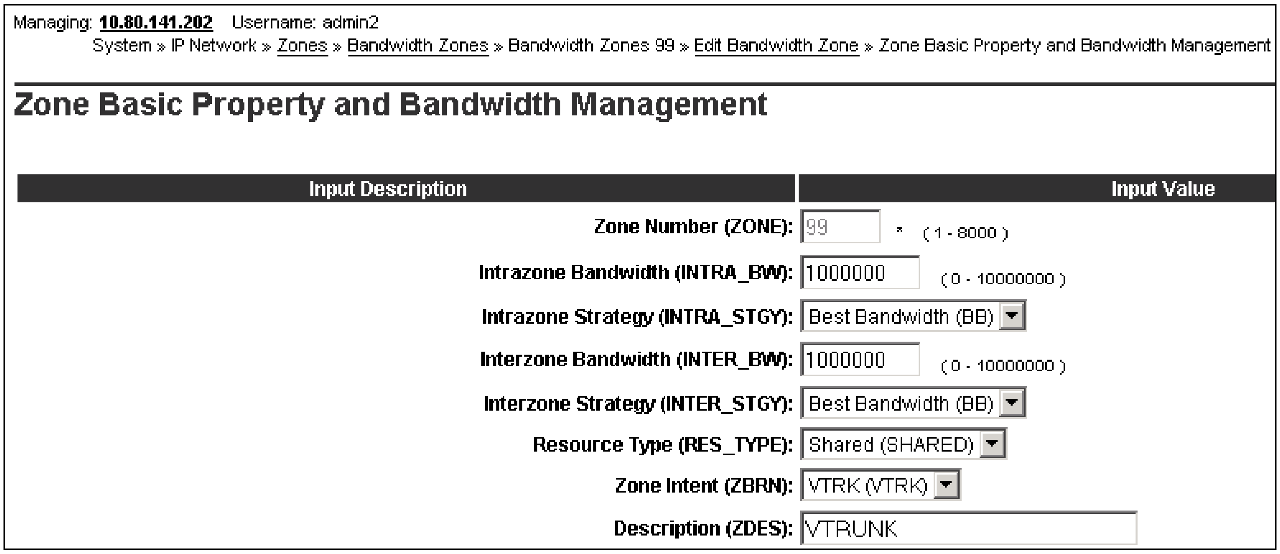
Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured as shown below. In production environments, it is likely that more zones will be required, Select the zone associated with the virtual trunk to Session Manager and click **Edit** as shown below. In the sample configuration,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

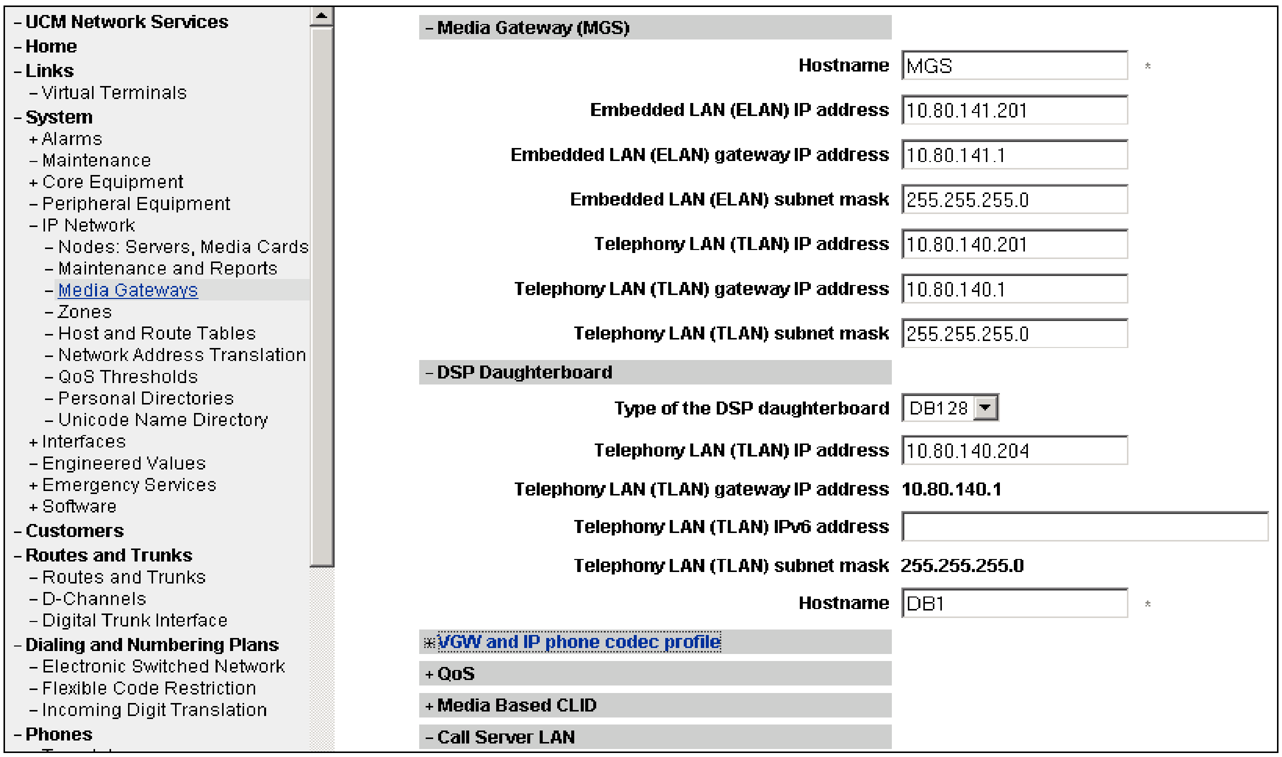


5.6. Codec Parameters, Including Ensuring Annexb=no for G.729

Verizon IPCC Service does not support G.729 Annex B, and Verizon requires that SDP offers and SDP answers in SIP messages include the "**annexb=no**" attribute when G.729 is used. This section includes the configuration that determines whether the "**annexb=no**" attribute is included.

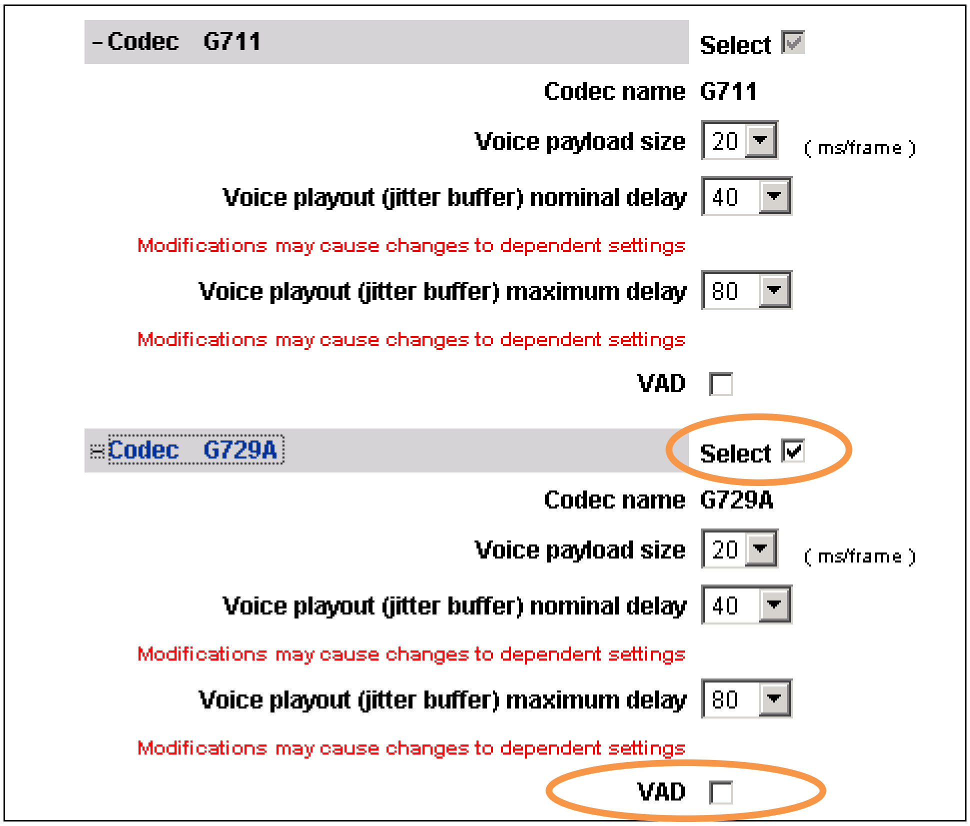
5.6.1 Media Gateway Configuration

To ensure that the "**annexb=no**" attribute is included, expand **System → IP Network** on the left panel and select **Media Gateways**. Select the appropriate media gateway (not shown), and scroll down to the area of the screen containing **VGW and IP phone codec profile** as shown below.



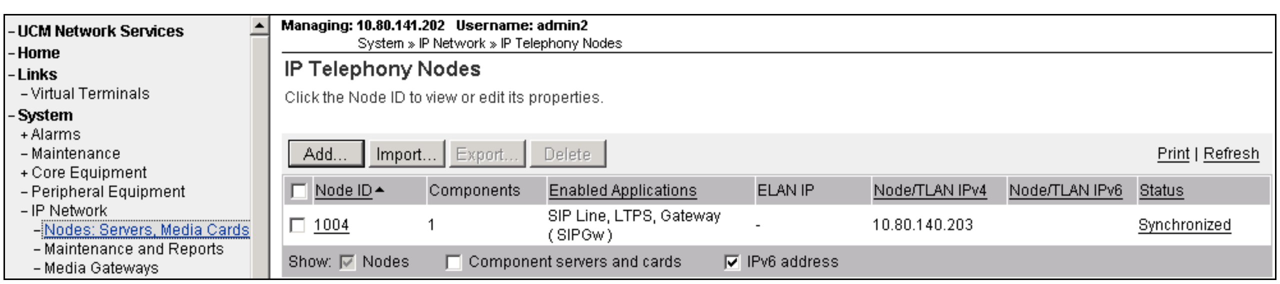
Expand **VGW and IP phone codec profile**. To use G.729A with Verizon IPCC service, ensure that the **Select** box is checked for **Codec G729A**, and the **VAD** (Voice Activity Detection) box is un-checked.

Note that **Codec G.711** is enabled by default. **Voice payload size** of "**20**" can be used with Verizon IPCC service for both G.729A and G.711. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order. The following screen shows the parameters used.

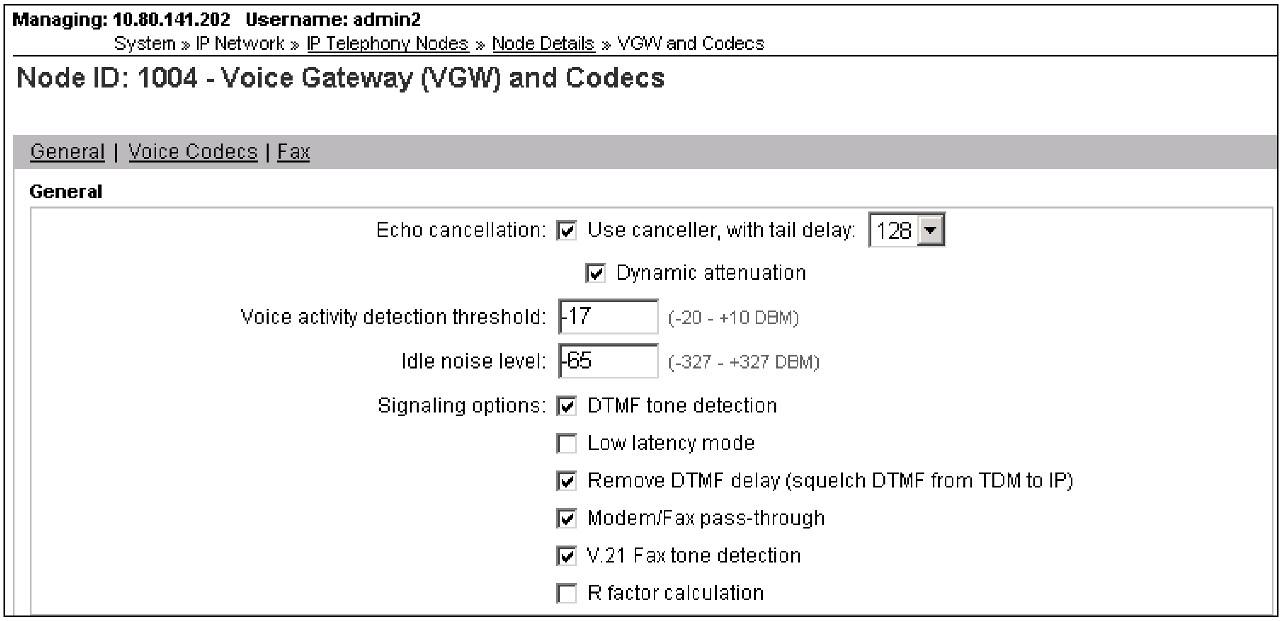


5.6.2 Node Voice Gateway and Codec Configuration

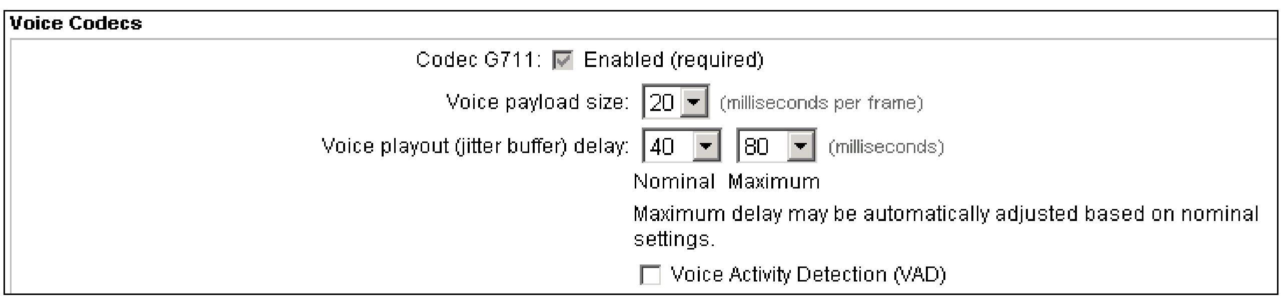
Expand **System → IP Network** and select **Node, Server, Media Cards**. Select the appropriate **Node Id** which is "**1004**" for sample configuration as shown below.



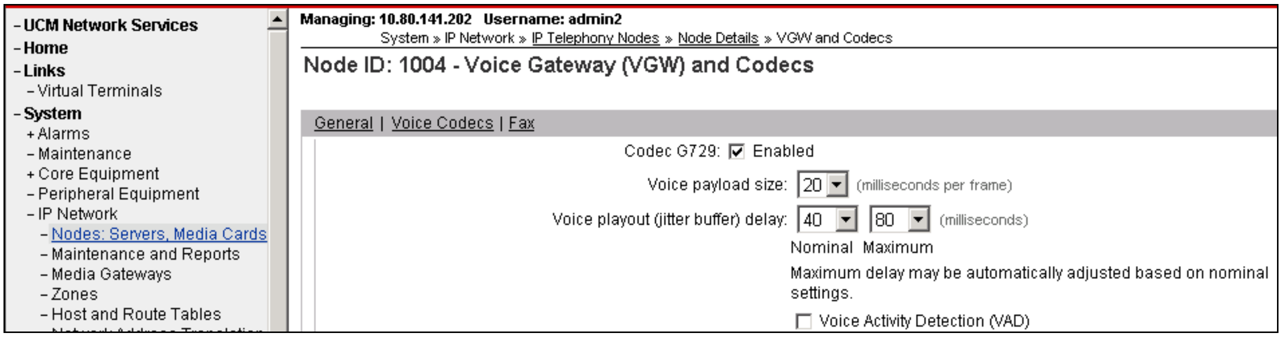
In the resultant screen (not shown) use the scroll bar on the right to select **Voice Gateway (VGW) and Codecs**. The following screen shows the **General** parameters used in the sample configuration.



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



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

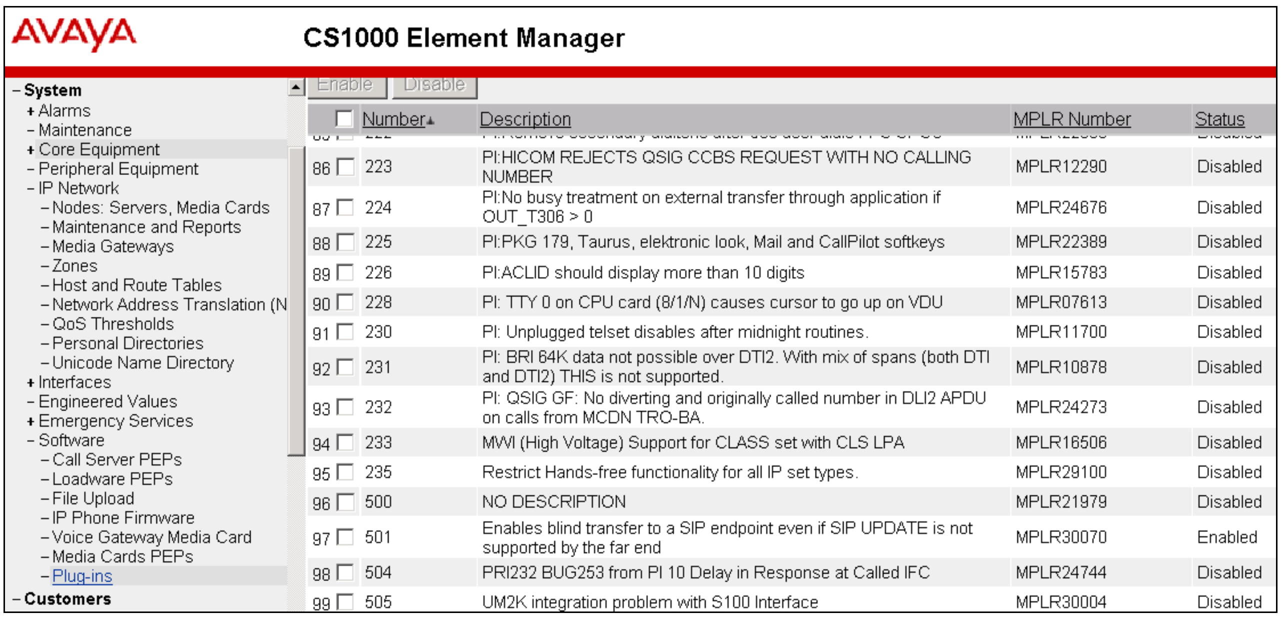


Note: click **Save** (not shown) to save changes and follow the procedure described in **Section 5.3** to transfer and synchronize changes between Node and associated Signaling Server.

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.

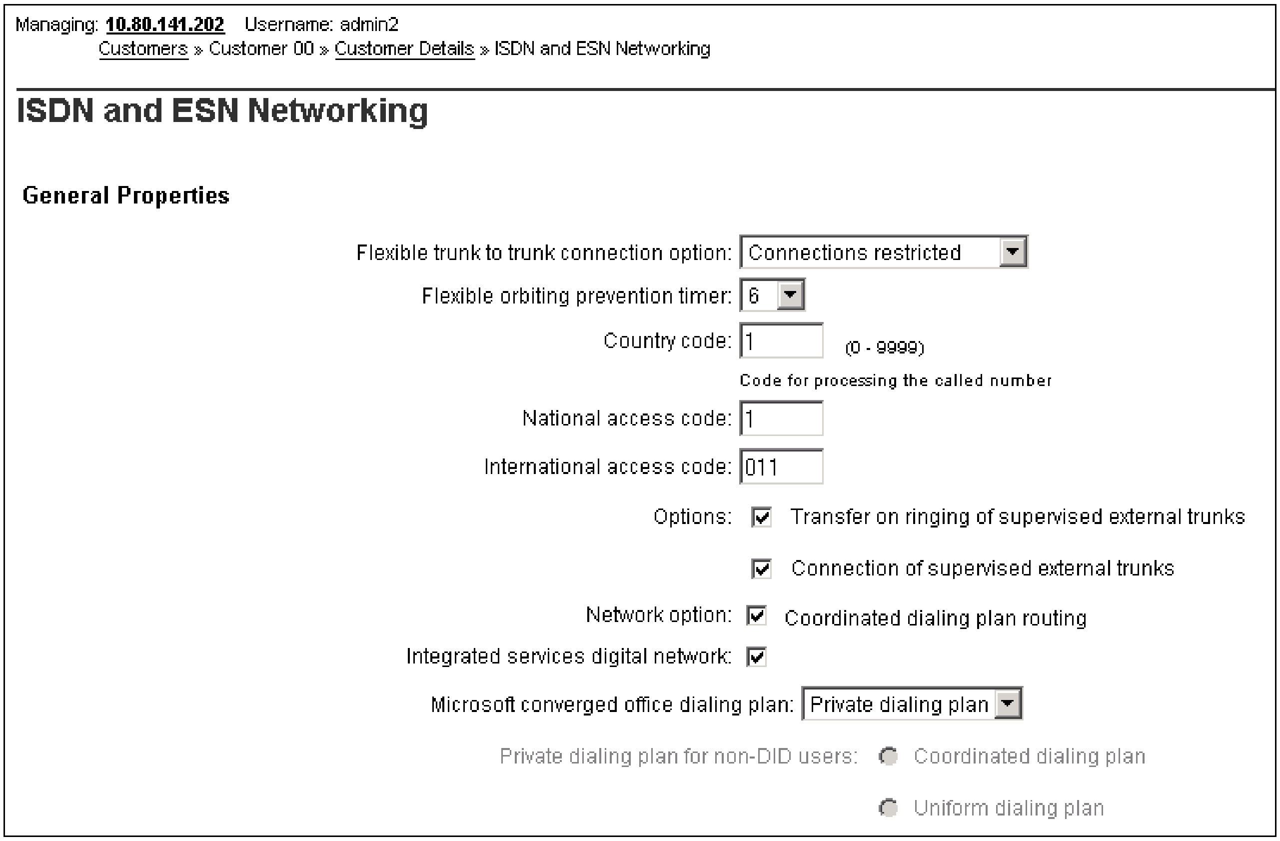
To view or enable a plug-in, from the left navigation menu, expand **System → Software**, and select **Plug-ins**. In the right side screen, a list of available plug-ins will be displayed along with the associated MPLR Number and Status. Use the scroll bar on the right to scroll down so that Plug-in "**501**" is displayed as shown in the screen below. If the **Status** is "**Disabled**", select the check-box next to Number "**501**" and click the **Enable** button at the top, if it is desirable to allow CS1000E users to complete call transfer to PSTN destinations via the Verizon IPCC 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 completed.

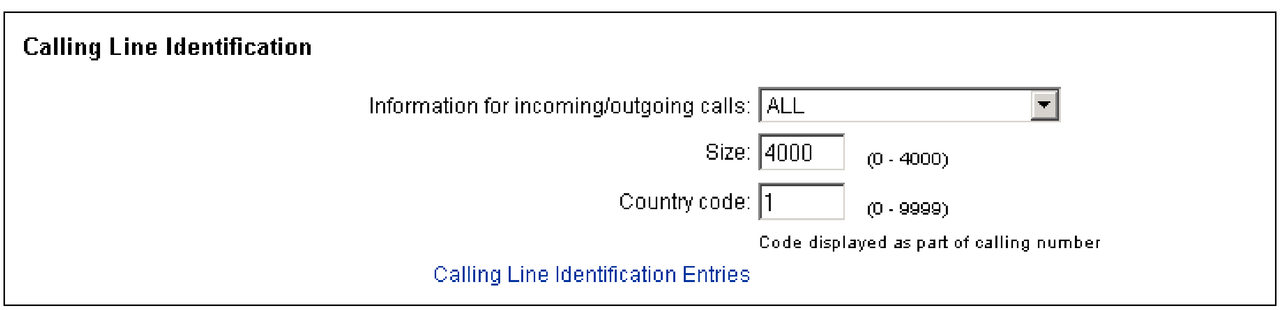


The same procedure may be used to enable Plug-in **201** if desired (not shown). Plug-in 201 will allow a CS1000E user to make a call to the PSTN using the Verizon IPCC service, and then subsequently perform an attended transfer of the call to another PSTN destination via the Verizon IPCC service.

5.8. Customer Information

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

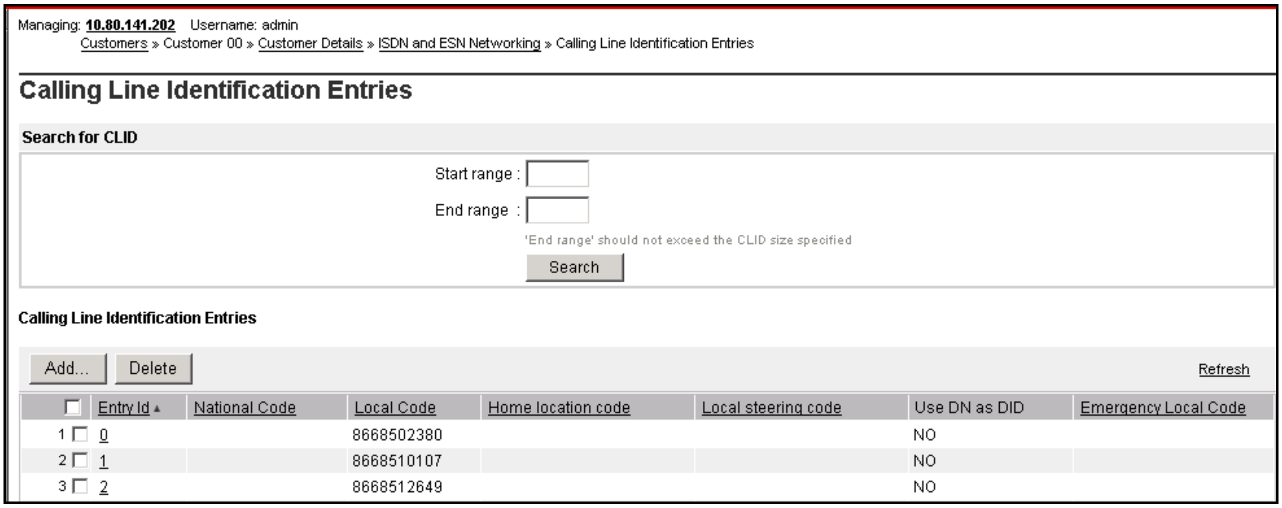




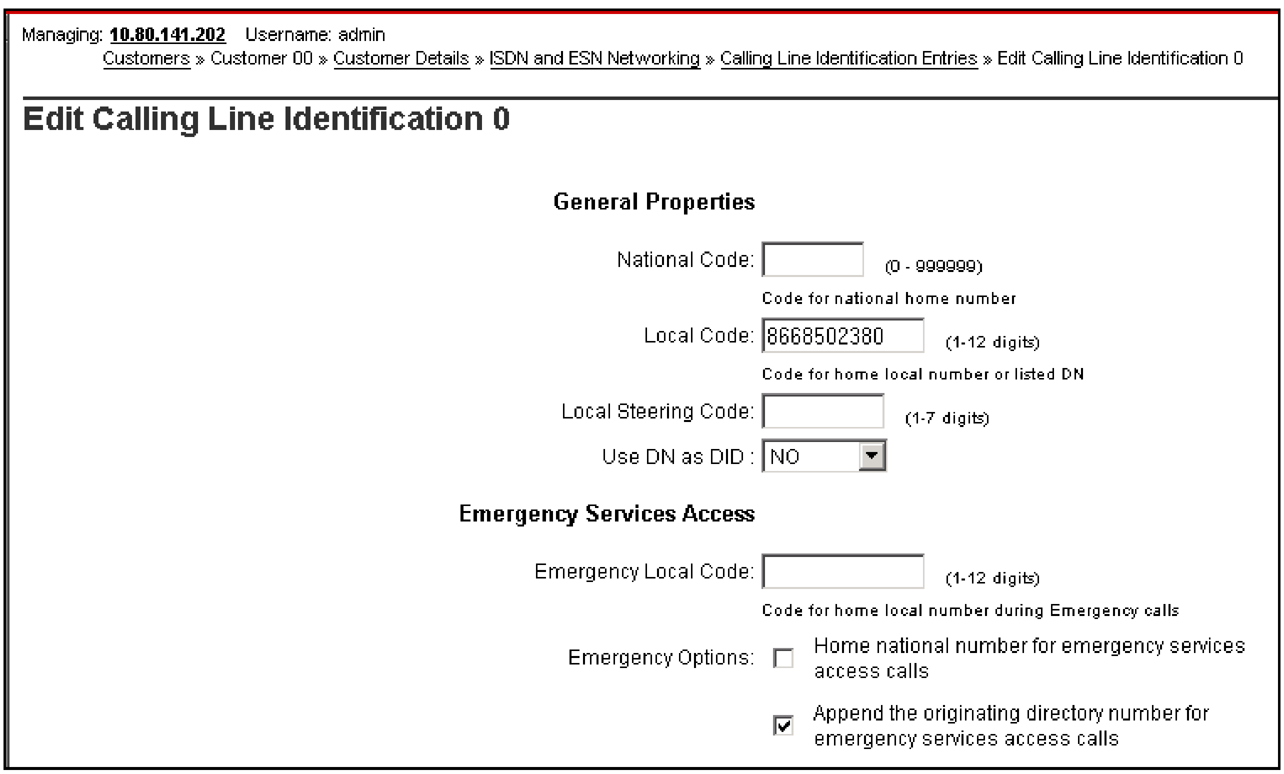
5.8.1 Caller ID Related Configuration

Although not intended to be prescriptive, in the sample configuration the CS1000E would send the user's four-digit directory number in SIP headers such as the From and PAI headers. Session Manager would adapt the user's directory number to an appropriate Verizon IPCC toll-free number before passing the message to the ASBCE towards Verizon.

Scroll down from the screen shown in **Section 5.8**, click the **Calling Line Identification Entries** link (not shown), and search for the **Calling Line Identification Entries** by **Entry ID.** As shown below, the **Use DN as DID parameter** was set to “**NO**” and an entry ID was created for every DID used in the sample configuration. The local DID will be replaced with the **Local Cod**e and the **Entry ID** will be configured on the individual extensions in **Section 5.9.**



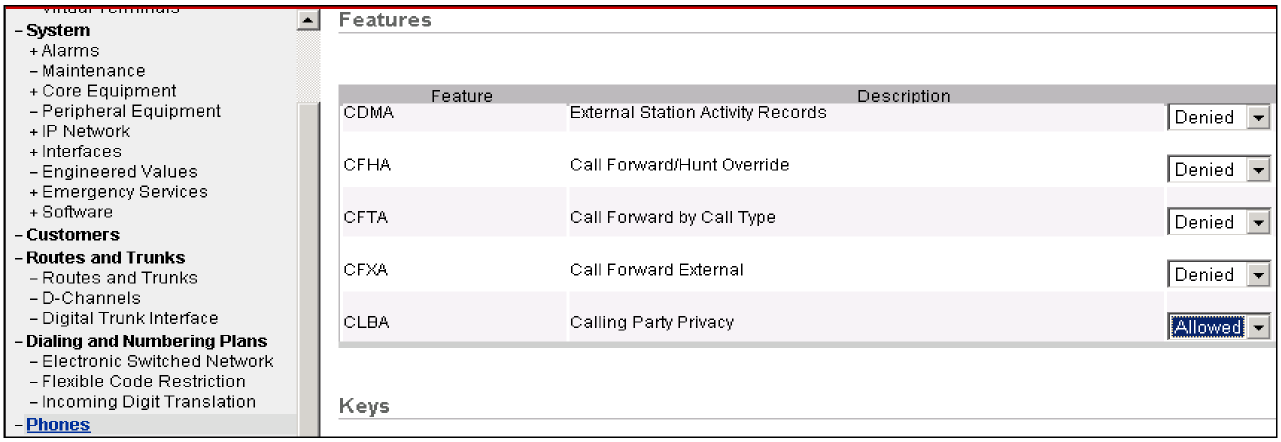
Click on **Entry Id** “**0**” to view or change further details as shown below.



5.8.1.1 Requesting Privacy

One means to have the CS1000E request privacy (i.e., Privacy: id in SIP INVITE) for an outbound call from a specific phone to the Verizon IPCC service is to configure each phone with the appropriate option. Expand **Phones** on the left navigation panel and enter **Search Criteria** to display a list of stations. Select a specific station for editing (not shown).

In the **Features** table, scroll to **CLBA Calling Party Privacy** feature and select "**Allowed**" as shown below.



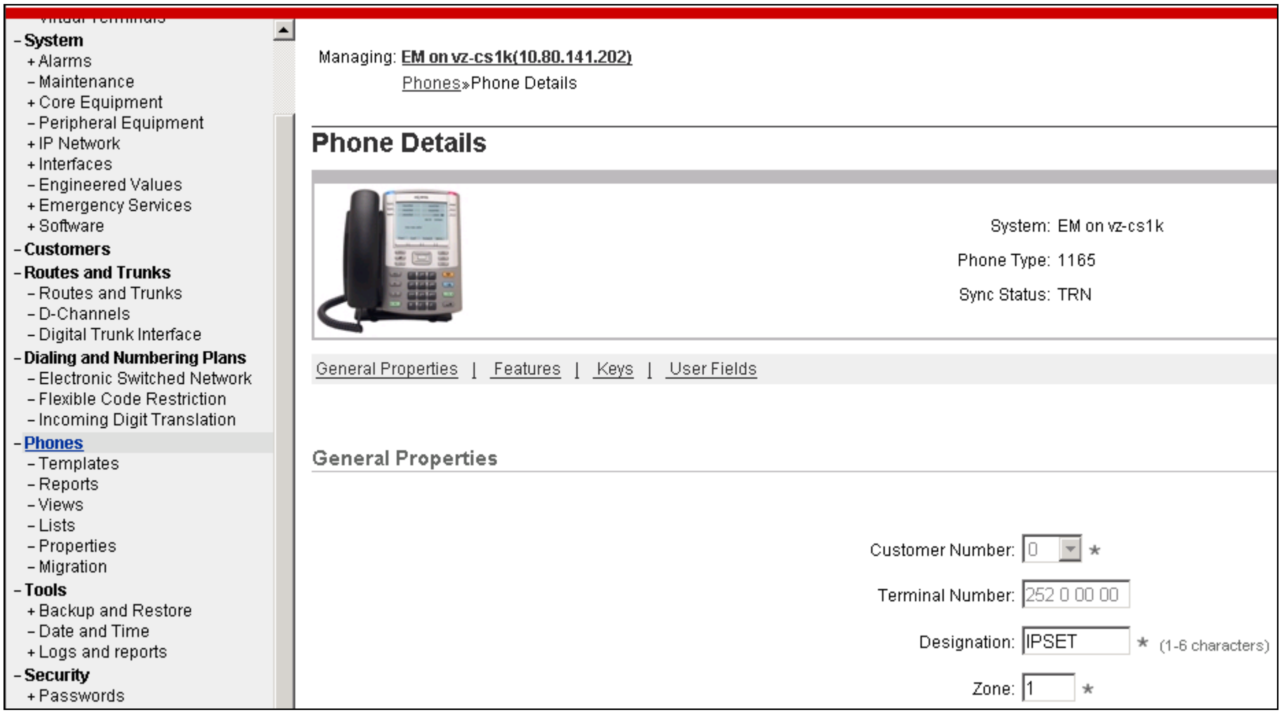
Another means to have the CS1000E request privacy (i.e., Privacy: id in SIP INVITE) for an outbound call from a specific phone to the Verizon IPCC service is to set **DDGA Present/Restrict Calling Number** feature to "**Denied**" via the Phone **Features** table in Element Manager (not shown).

5.9. Example Communication Server 1000E Telephone Users

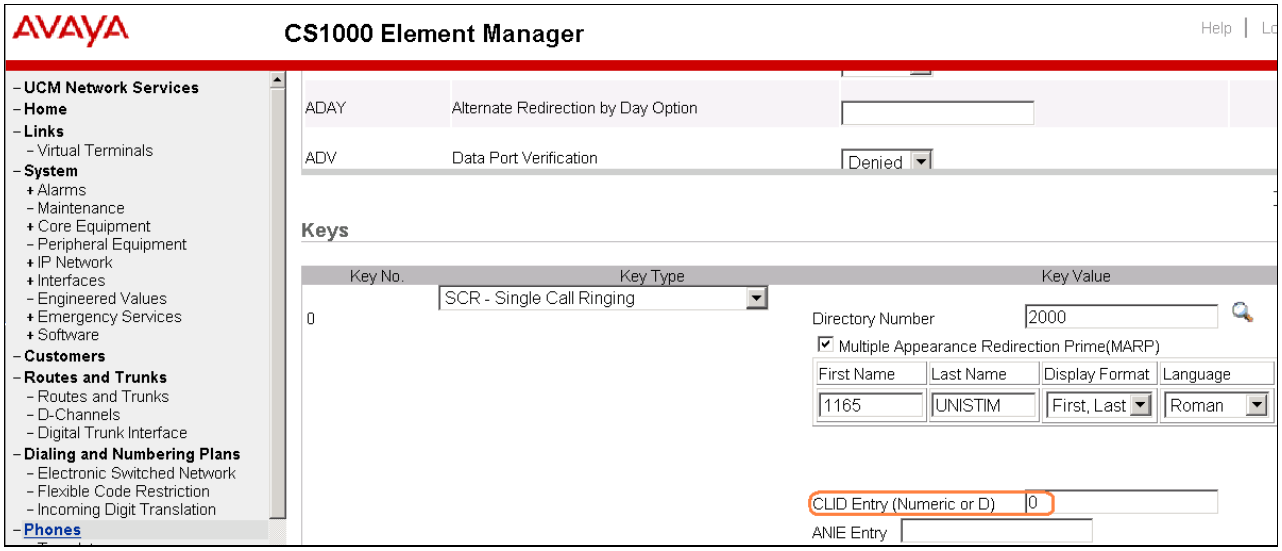
This section is not intended to be prescriptive, but simply illustrates a sampling of the telephone users in the sample configuration.

5.9.1 Example IP UNIStim Phone DN 2000, Codec Considerations

The following screen shows basic information for an IP UNIStim phone in the configuration. The telephone is configured as Directory Number 2000. Note that the telephone is in Zone 1. A call between this telephone and another telephone in Zone 1 will use a "best quality" strategy (see **Section 5.5**) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the Verizon IPCC service, the call would use a "best bandwidth" strategy, and the call would use G.729A.

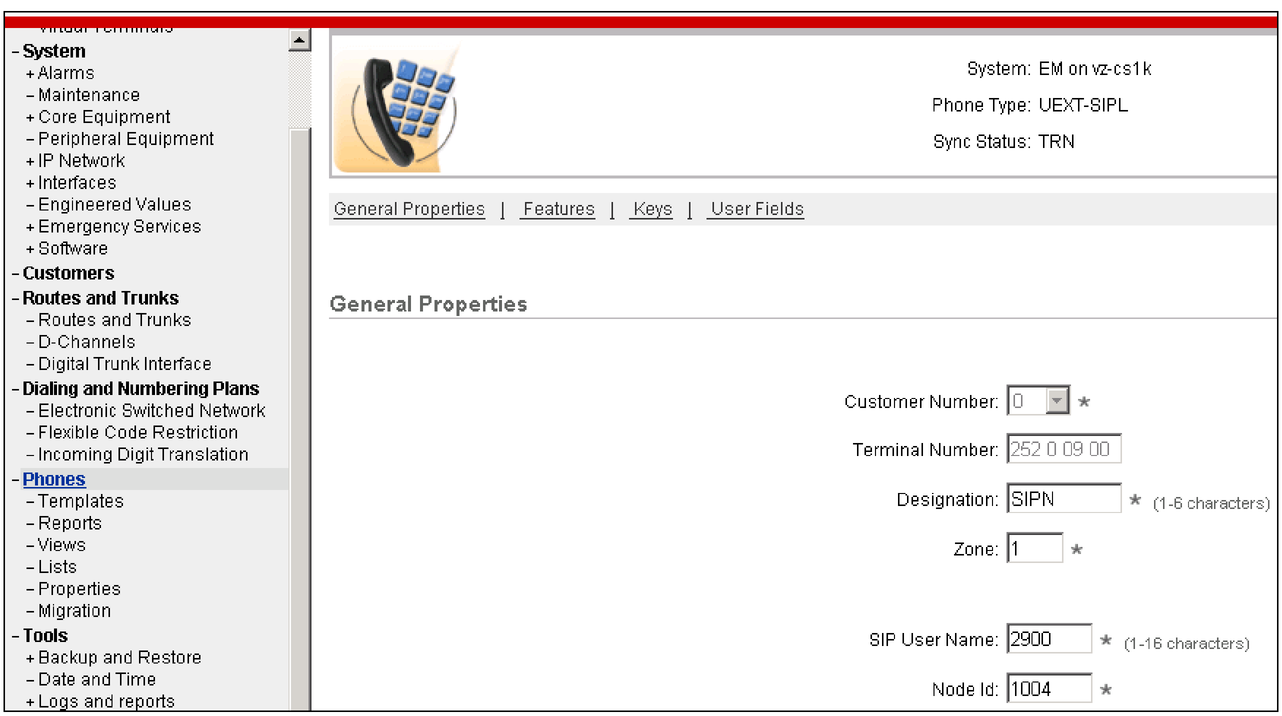


Scrolling down to the **Keys** section. The **First** and **Last Name**, the **Directory Number** as well as the **Calling Lined ID (CLID)** is configured. The **CLID** entry is defined in **Section 5.8.1**.



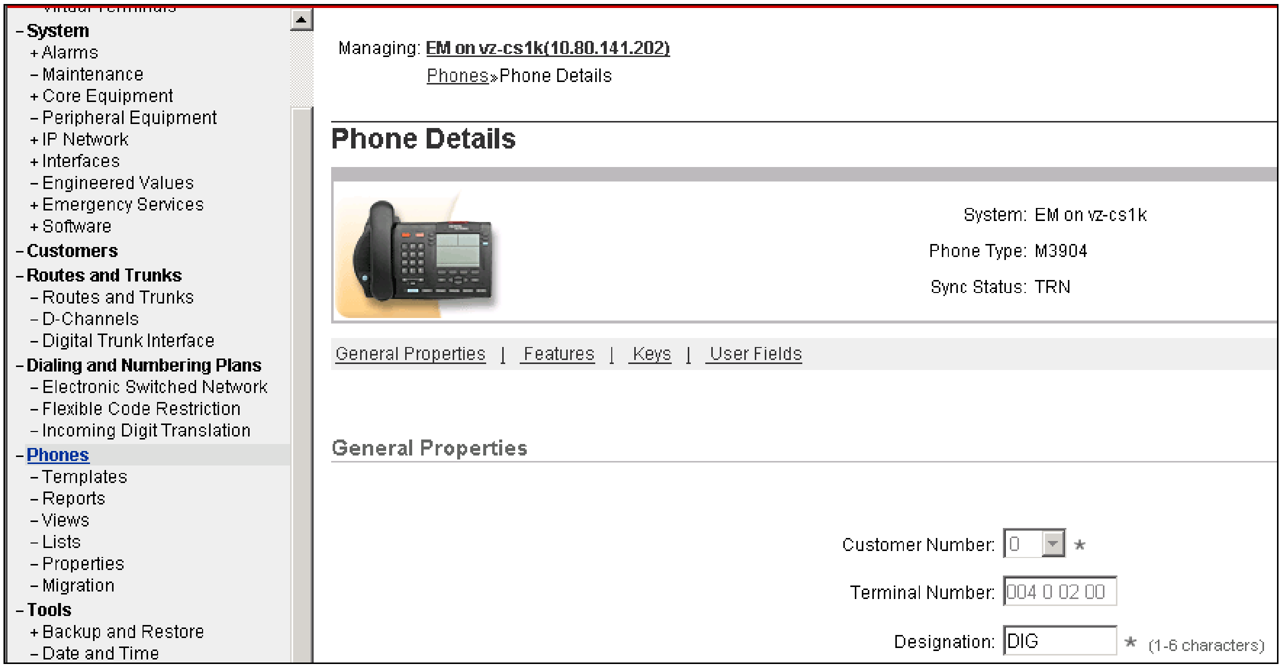
5.9.2 Example SIP Phone DN 2900, Codec Considerations

The following screen shows basic information for a SIP phone in the configuration. The telephone is configured as Directory Number 2900. Note that the telephone is in Zone 1 and is associated with Node 1004 (see **Section 5.1**). A call between this telephone and another telephone in Zone 1 will use a "best quality" strategy (see **Section 5.5**) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the Verizon IPCC service, the call would use a "best bandwidth" strategy, and the call would use G.729A.

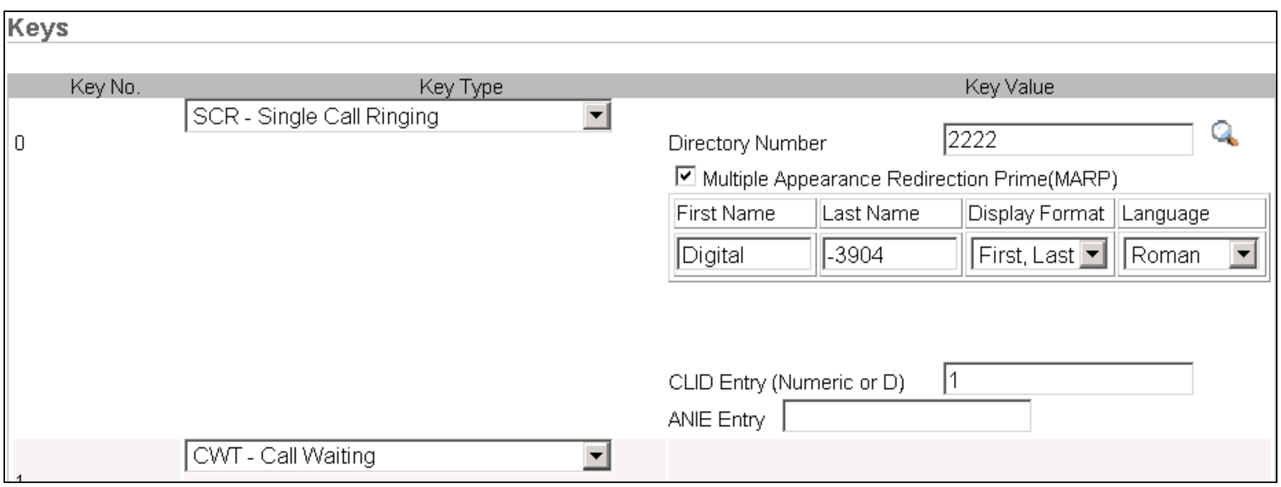


5.9.3 Example Digital Phone DN 2222

The following screen shows basic information for a digital phone in the configuration. The telephone is configured as Directory Number 2222.

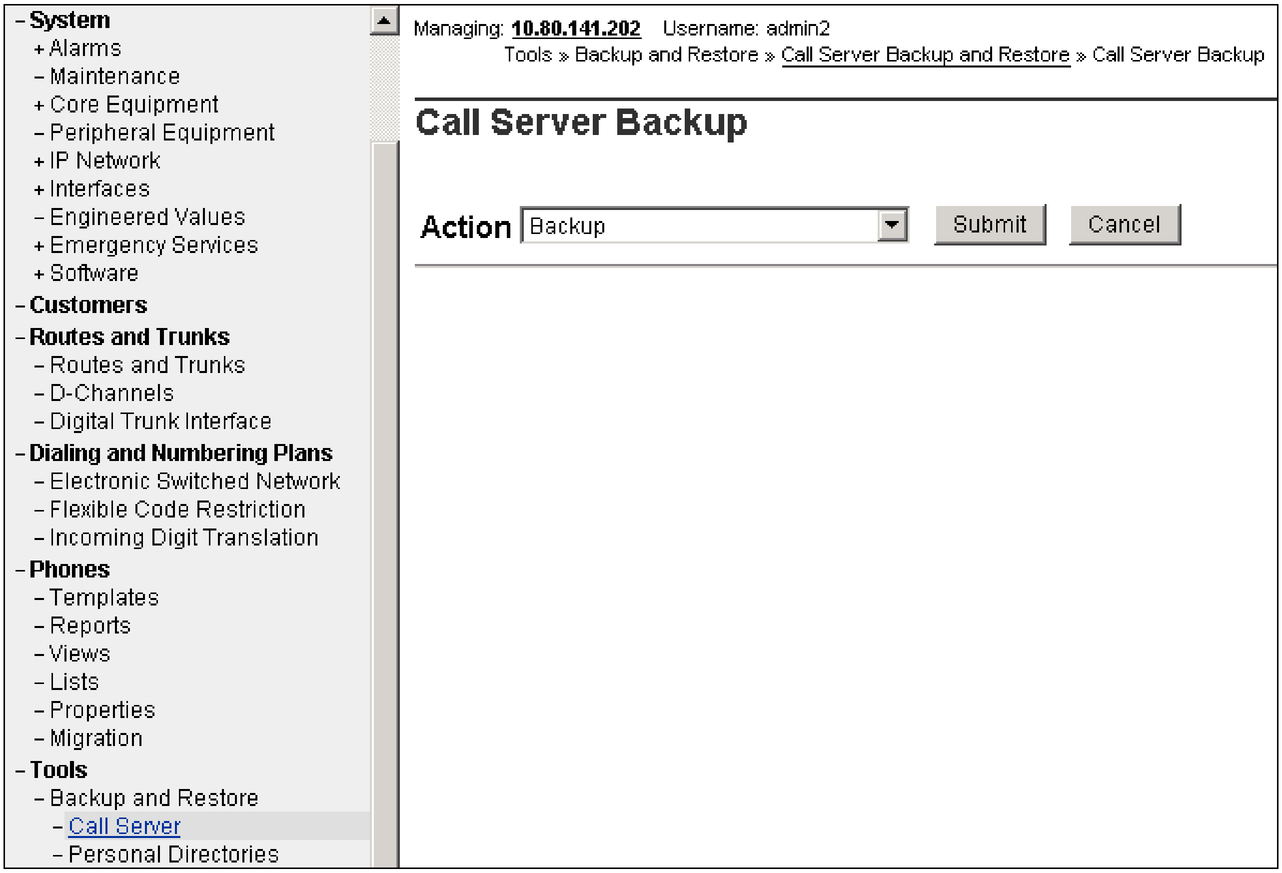


The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone, and uses **CLID Entry** 1 (**Section 5.8.1**). Although not shown in detail below, to use call waiting with tone, assign a key "**CWT – Call Waiting**", set the feature "**SWA – Call waiting from a Station**" to "**Allowed**", and set the feature "**WTA – Warning Tone**" to "**Allowed**".



5.10. Save Configuration

Expand **Tools → Backup and Restore** on the left navigation panel and select **Call Server.** Select **Backup** for **Action** and click **Submit** to save configuration changes as shown below.



The backup process may take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

```
Backing up reten.bkp
Starting database backup
to local Removable Media Device
USB mass storage device found available
.
Backing up reten.bkp to "/var/opt/nortel/cs/fs/usb/backup/single"
Database backup Complete!
TEMU207
Backup process to local Removable Media Device ended successfully.
```

The configuration of Avaya Communication Server 1000E is complete.

6. Configure Avaya Aura® Session Manager

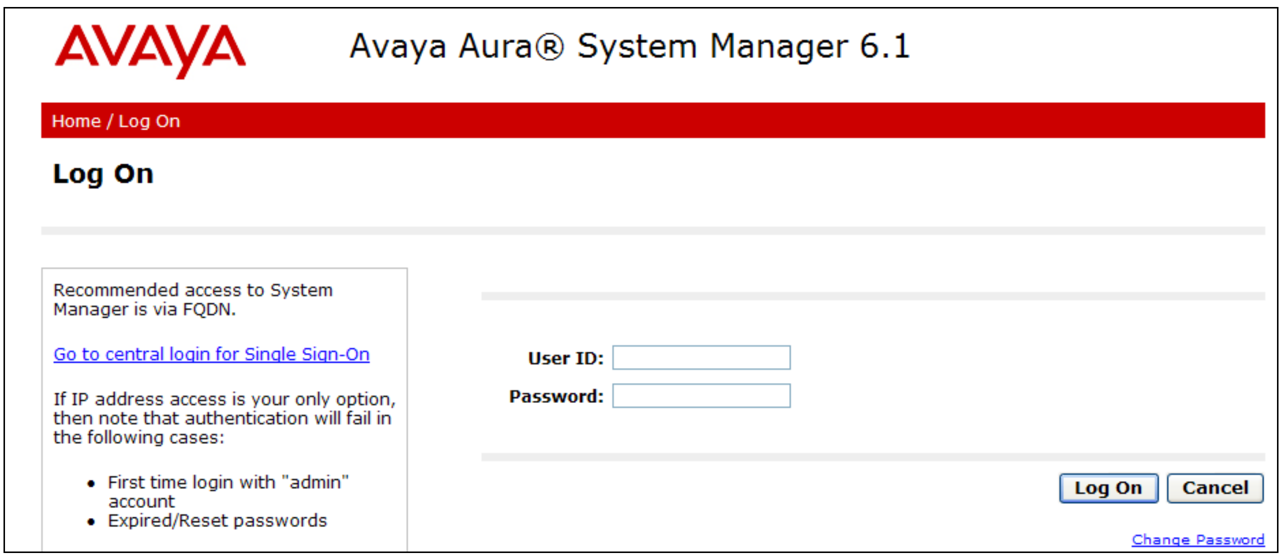
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two. For more information, consult the references in **Section 11**.

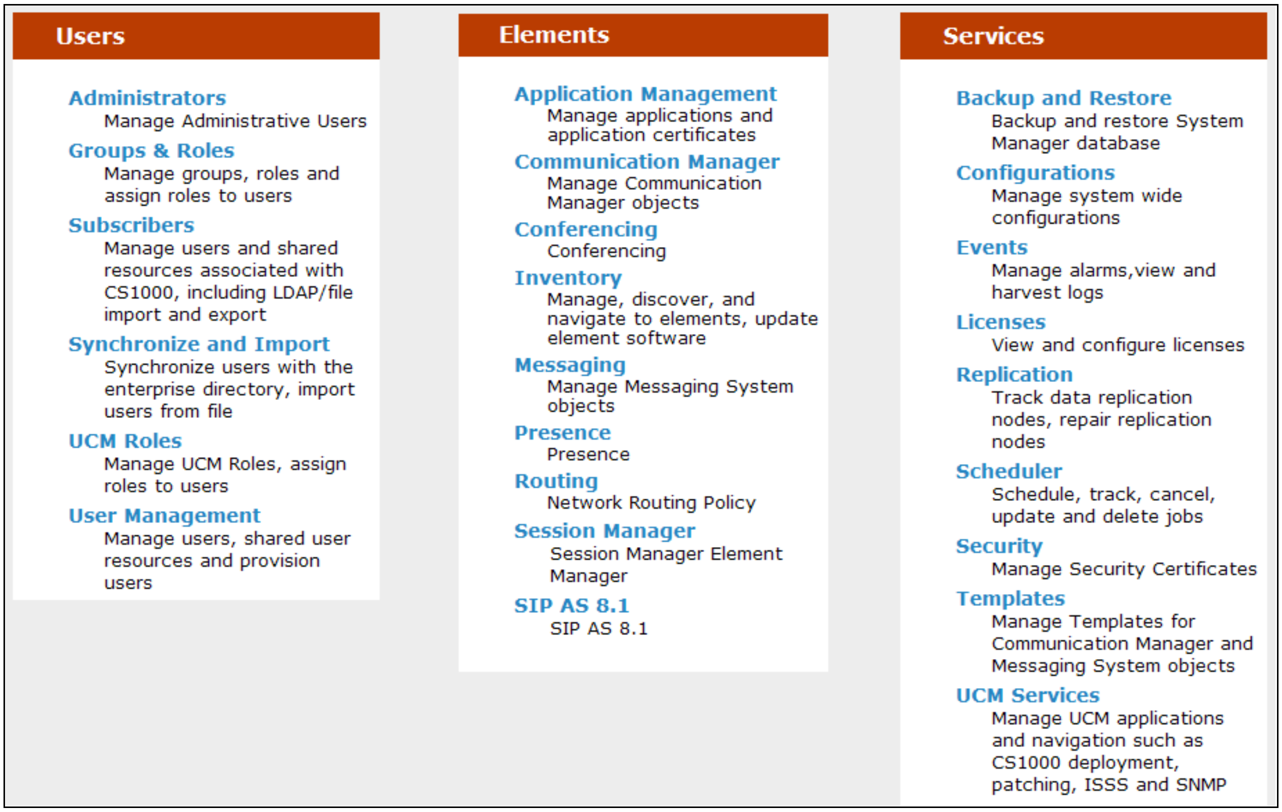
This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Avaya Communication Server 1000E and Session Manager, and the SIP trunk between Session Manager and the ASBCE.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "**http://<ip-address>/SMGR**", where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials.

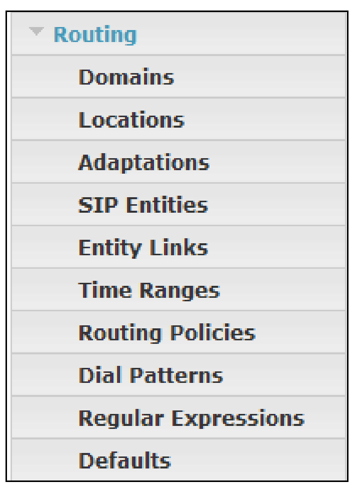
In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button.



Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.



The screen shown below shows the various sub-headings of the left navigation menu that will be referenced in this section.

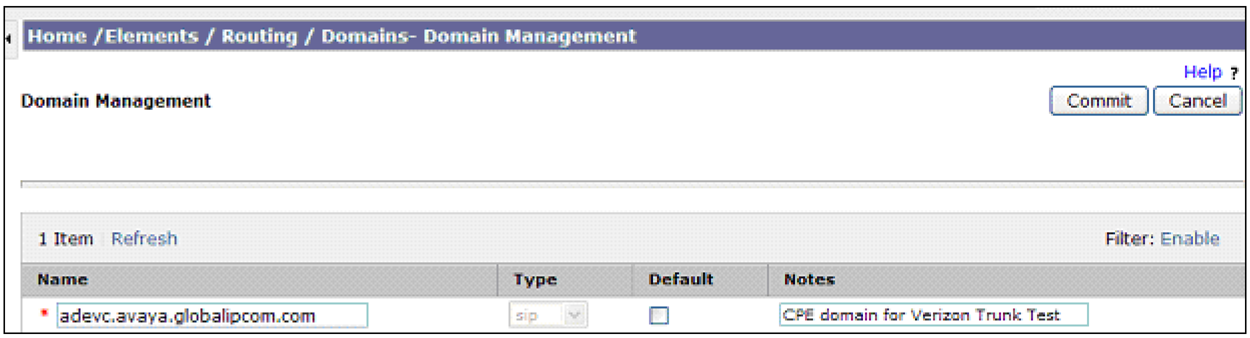


6.1. SIP Domain

Select **Domains** from the left navigation menu. Two domains can be added, one for the enterprise SIP domain, and one for the Verizon network SIP domain. In the shared environment of the Avaya Solution and Interoperability Test lab, a domain "**avayalab.com**" is also defined and used by the shared equipment.

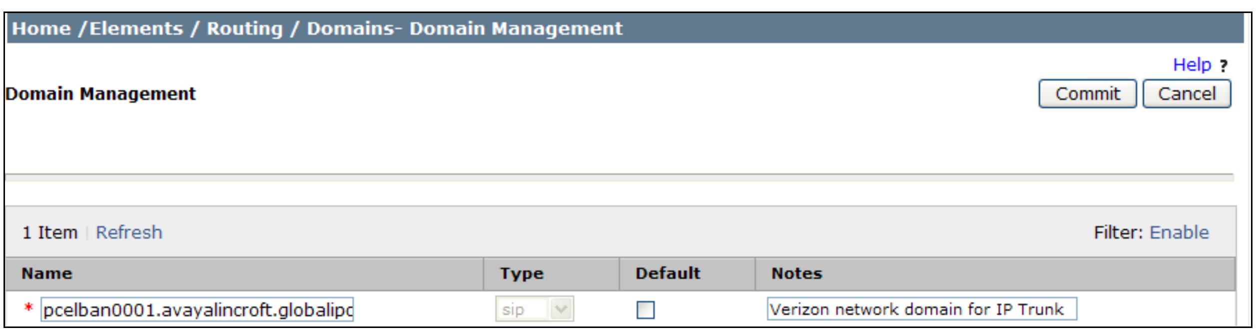
Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, "**adevc.avaya.globalipcom.com**" is shown, the CPE domain known to Verizon.
- **Type:** Verify "**SIP**" is selected.
- **Notes:** Add a brief description. [Optional].



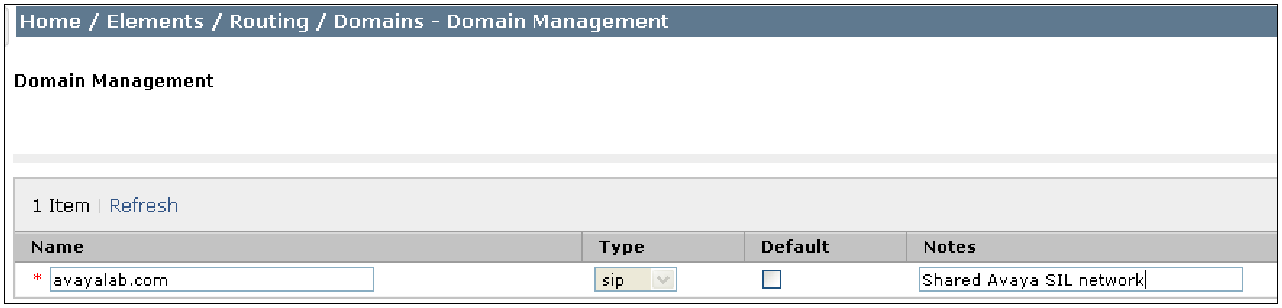
Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name:** Enter the Domain Name used for the Verizon network. In the sample screen below, "**pcelban0001.avayalincroft.globalipcom.com**" is shown.
- **Type:** Verify "**SIP**" is selected.
- **Notes:** Add a brief description. [Optional].



Click **Commit** to save.

The following screen shows the "**avayalab.com**" SIP domain that was already configured in the shared laboratory network.

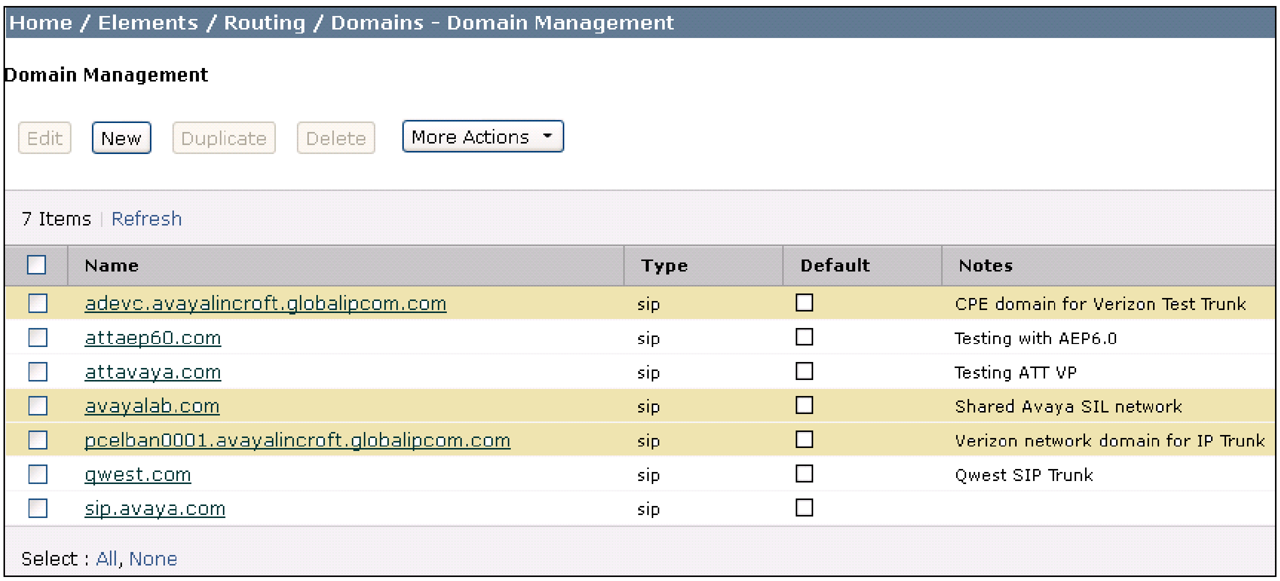

Home / Elements / Routing / Domains - Domain Management

Domain Management

1 Item | Refresh

Name	Type	Default	Notes
* avayalab.com	sip	☐	Shared Avaya SIL network

The screen below shows an example SIP Domain list after SIP Domains are configured. Many SIP Domains can be configured, distinguished, and adapted by the same Session Manager as needed.


Home / Elements / Routing / Domains - Domain Management

Domain Management

Edit | New | Duplicate | Delete | More Actions

7 Items | Refresh

	Name	Type	Default	Notes
☐	adevc.avayalincroft.globalipcom.com	sip	☐	CPE domain for Verizon Test Trunk
☐	attaep60.com	sip	☐	Testing with AEP6.0
☐	attavaya.com	sip	☐	Testing ATT VP
☐	avayalab.com	sip	☐	Shared Avaya SIL network
☐	pcelban0001.avayalincroft.globalipcom.com	sip	☐	Verizon network domain for IP Trunk
☐	qwest.com	sip	☐	Qwest SIP Trunk
☐	sip.avaya.com	sip	☐	

Select : All, None

6.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be used for bandwidth management or location-based routing.

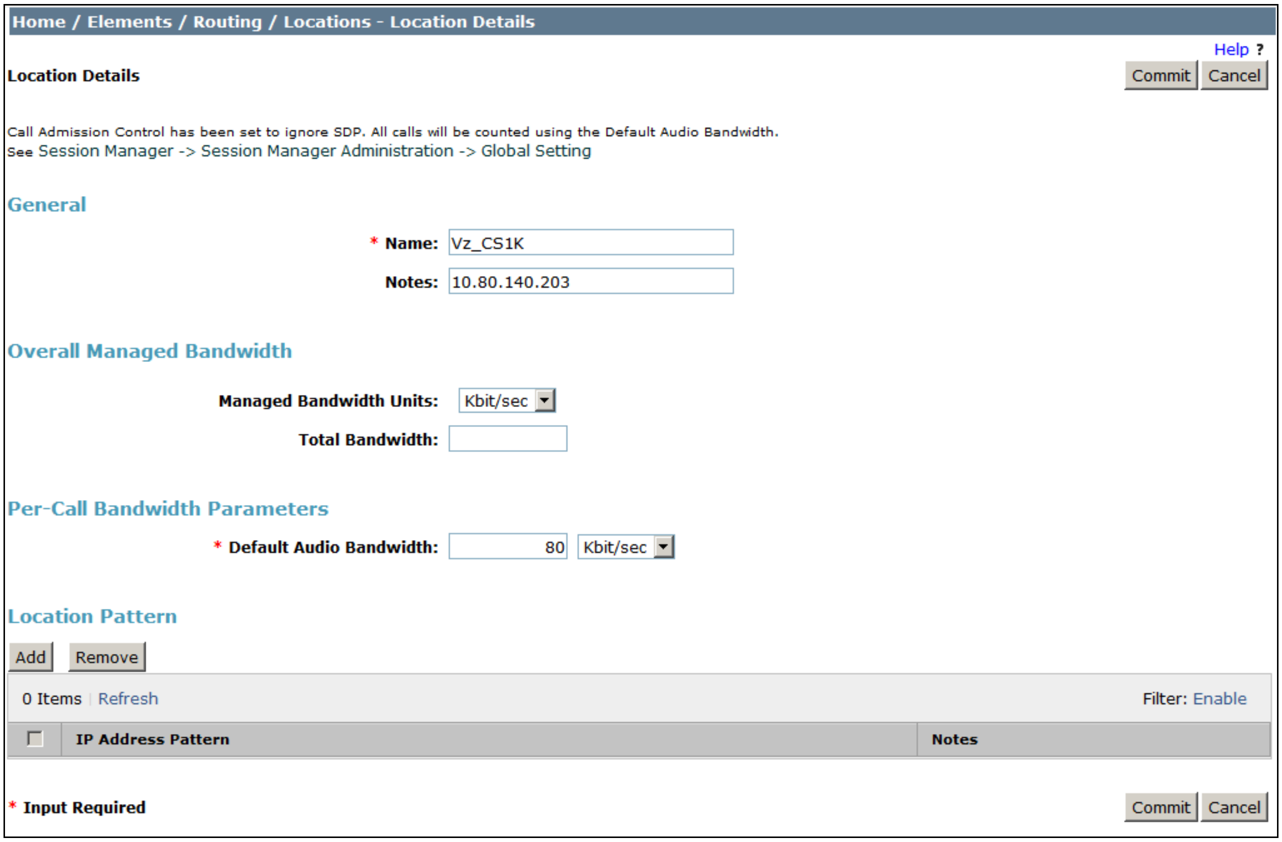
6.2.1 Location for Avaya Communication Server 1000E

Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional].

Click **Commit** to save. **Note:** No IP Address is added in the **Location Pattern** section.

The screen below shows the top portion of the screen for the Location defined for Avaya Communication Server 1000E.



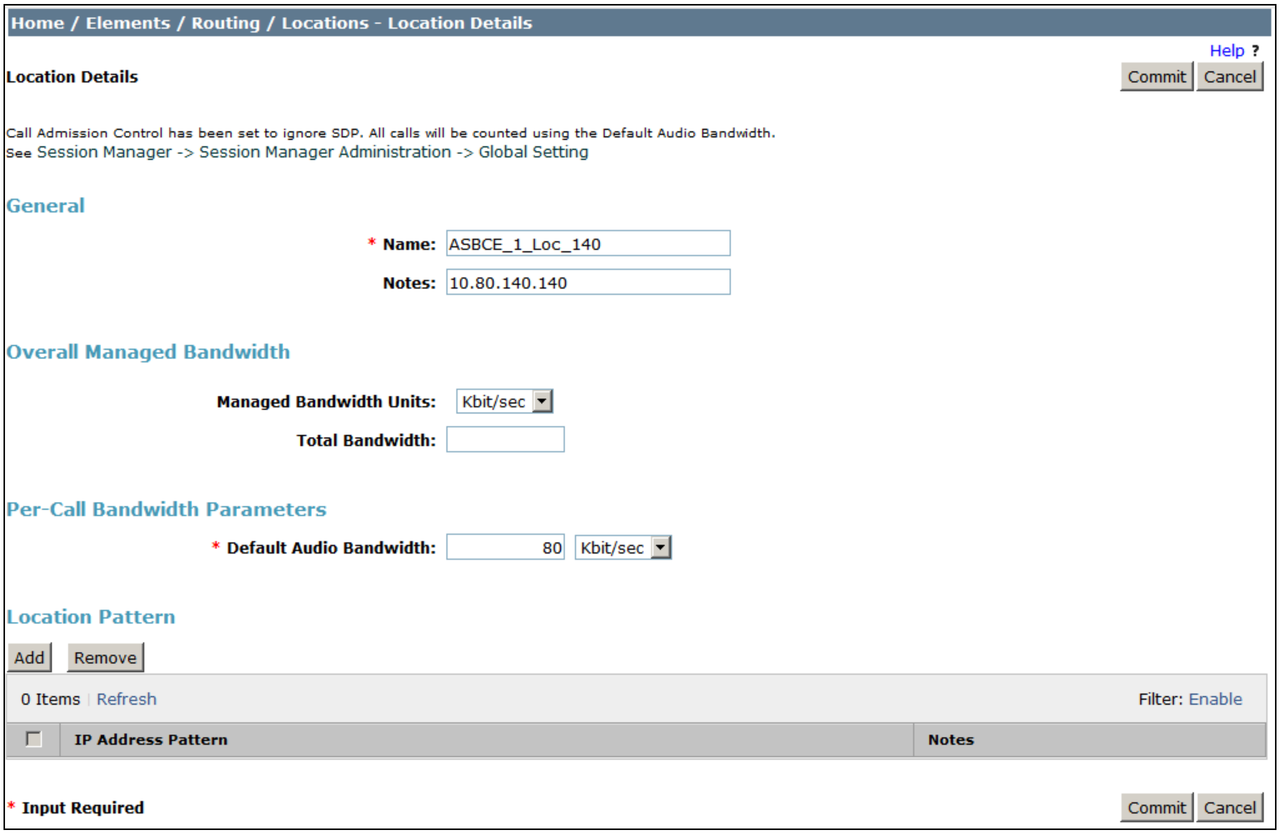
6.2.2 Location for Avaya SBCE For Enterprise

Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional].

Click **Commit** to save.

The screen below shows the Location defined for the ASBCE.



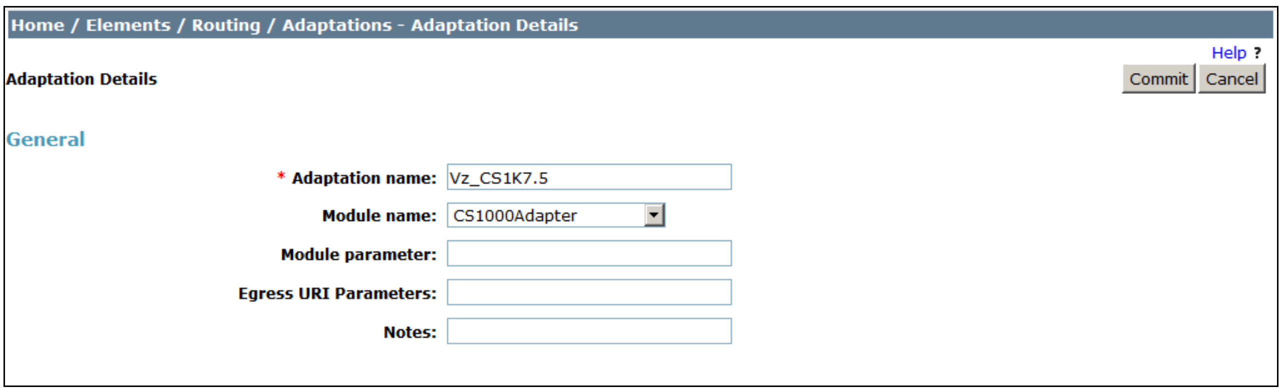
6.3. Configure Adaptations

Session Manager can be configured to use an Adaptation Module designed for Avaya Communication Server 1000E to convert SIP headers in messages sent to Avaya Communication Server 1000E to the format used by other Avaya products and endpoints.

6.3.1 Adaptation for Avaya Communication Server 1000E

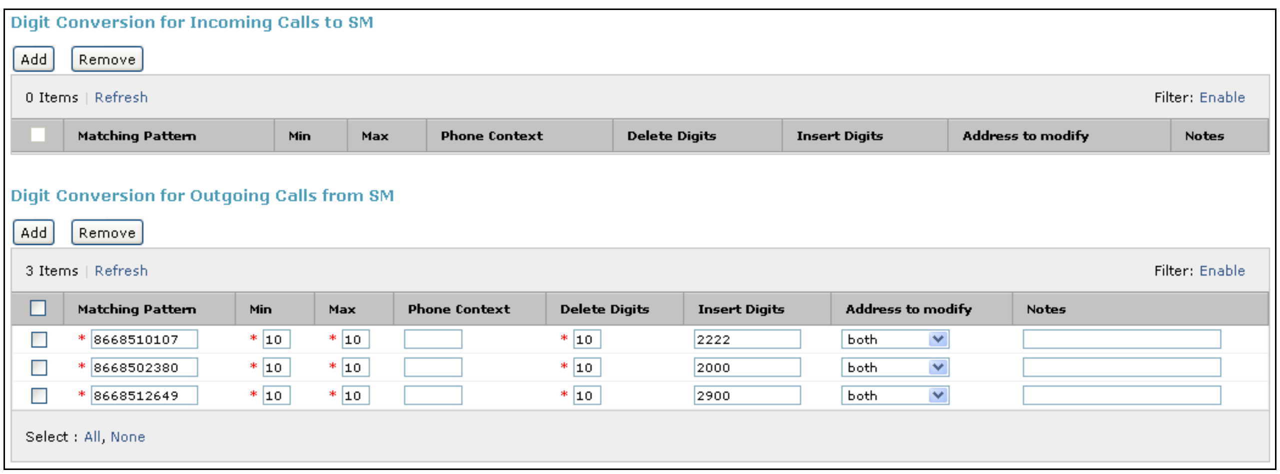
Select **Adaptations** from the left navigational menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., "**Vz_CS1K7.5**").
- **Module Name:** Select "**CS1000Adapter**" from drop-down menu (or add an adapter with name "CS1000Adapter" if not previously defined).



Scrolling down, in the **Digit Conversion for Outgoing Calls from 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 inbound toll-free numbers and corresponding CS1000E directory numbers. **Digit Conversion for Incoming Calls to SM** could be used, however the extensions will be adapted by the CLID entries on the individual extensions (**Section 5.9**).

- **Matching Pattern** Enter Verizon inbound toll-free numbers (or number ranges via wildcard pattern matching). For other entries, enter the dialed prefix for any SIP endpoints registered to Session Manager (if any).
- **Min** Enter minimum number of digits (e.g., 10).
- **Max** Enter maximum number of digits (e.g., 10).
- **Delete Digits** Enter "**10**", the number of digits to be removed from dialed toll-free number before routing by Session Manager. For Verizon DID conversion to the corresponding CS1000E extension, remove all digits in the toll-free number.
- **Insert Digits** Enter the CS1000E extension corresponding to the toll-free number.
- **Address to modify** Select **"both".**



Digit Conversion for Incoming Calls to SM

Add Remove

0 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes

Digit Conversion for Outgoing Calls from SM

Add Remove

3 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
	* 8668510107	* 10	* 10		* 10	2222	both	
	* 8668502380	* 10	* 10		* 10	2000	both	
	* 8668512649	* 10	* 10		* 10	2900	both	

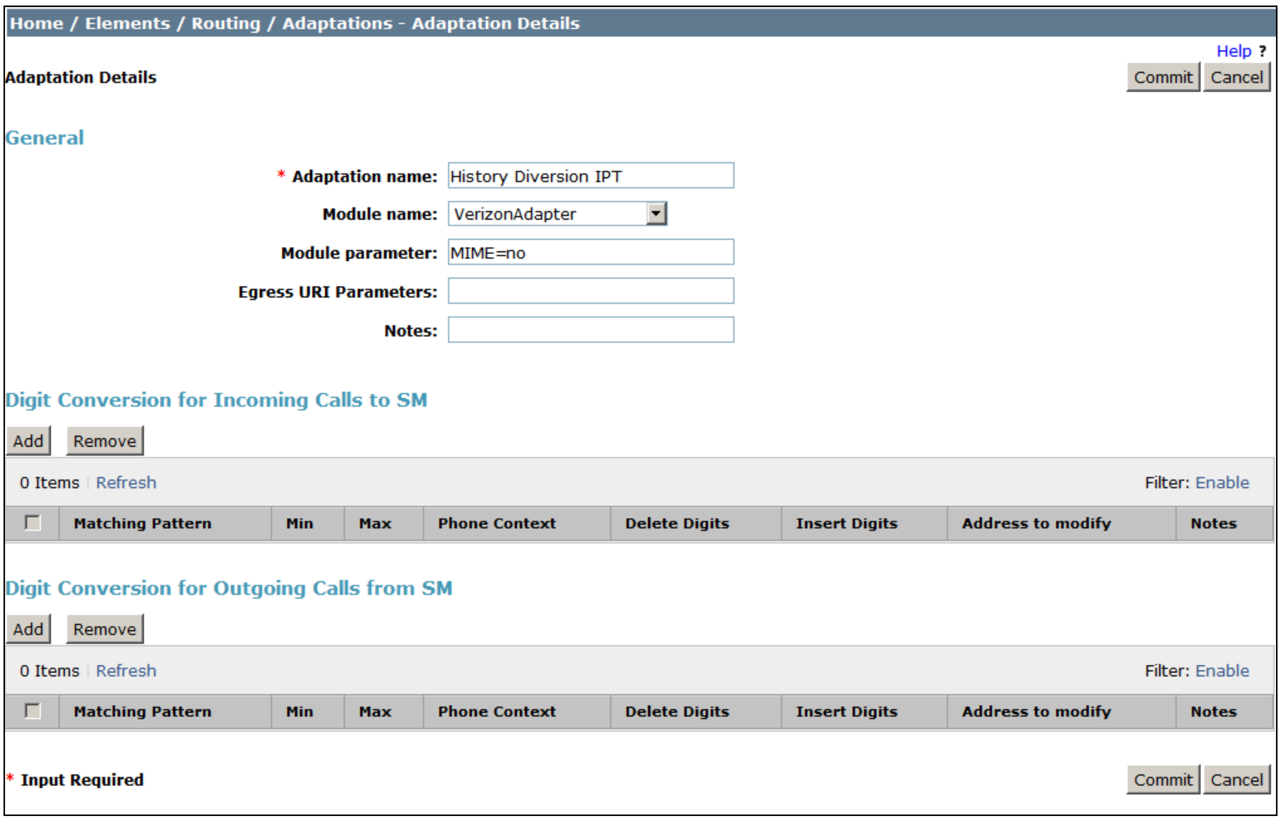
Select : All, None

Click **Commit** (not shown).

6.3.2 Adaptation for Avaya SBC for Enterprise

Select **Adaptations** from the left navigational menu. Click **New (**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.
- **Module Name:** Select "**VerizonAdapter**" from drop-down menu (or add an adapter with name "VerizonAdapter" if not previously defined).
- **Module Parameter:** Enter "**MIME=no**" to strip the CS1000E MIME information from the SDP sent to Verizon.



Click **Commit.**

6.4. SIP Entities

SIP Entities must be added for Avaya Communication Server 1000E and for the ASBCE.

6.4.1 SIP Entity for Avaya Communication Server 1000E

Select **SIP Entities** from the left navigation menu.

Click **New (**not shown**)**. In the **General** section, enter the following values and use default values for remaining fields**.**

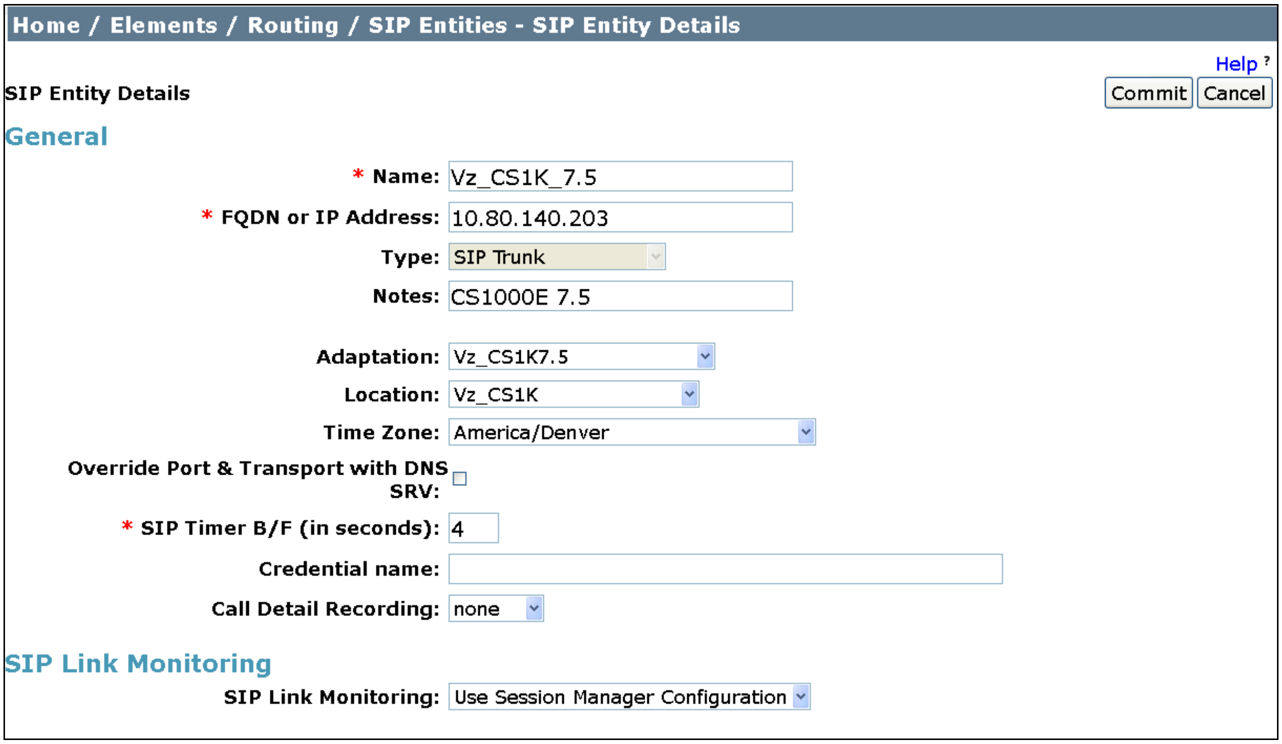
- **Name:** Enter an identifier for the SIP Entity.
- **FQDN or IP Address:** Enter the TLAN IP address of the CS1000E Node.
- **Type:** Select "**SIP Trunk**".
- **Notes:** Enter a brief description. [Optional].
- **Adaptation:** Select the Adaptation Module for CS1000E created in **Section 6.3.1**.
- **Location:** Select the Location for 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 Avaya Communication Server 1000E in the sample configuration.



6.4.2 SIP Entity for Avaya SBC for Enterprise

Select **SIP Entities** from the left navigation menu.

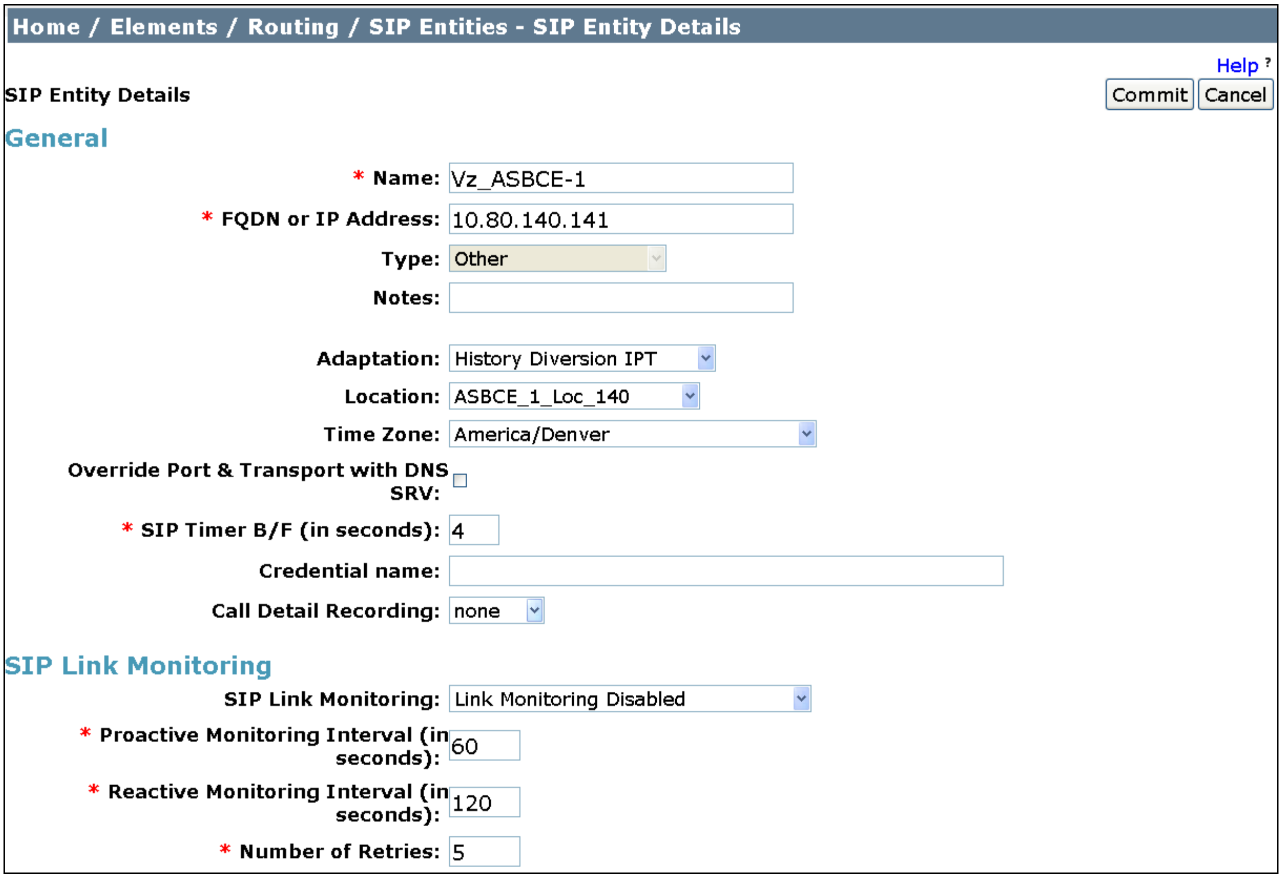
Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for the SIP Entity.
- **FQDN or IP Address:** Enter the private side IP Address of the SBC.
- **Type:** Select "**Other**".
- **Notes:** Enter a brief description. [Optional].
- **Adaptation:** Select the Adaptation Module for the ASBCE created in **Section 6.3.2**.
- **Location:** Select the Location for the ASBCE.

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).

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



6.5. Entity Links

The SIP trunk between Session Manager and Avaya Communication Server 1000E is described by an Entity Link, as is the SIP trunk between Session Manager and the ASBCE.

6.5.1 Entity Link to Avaya Communication Server 1000E

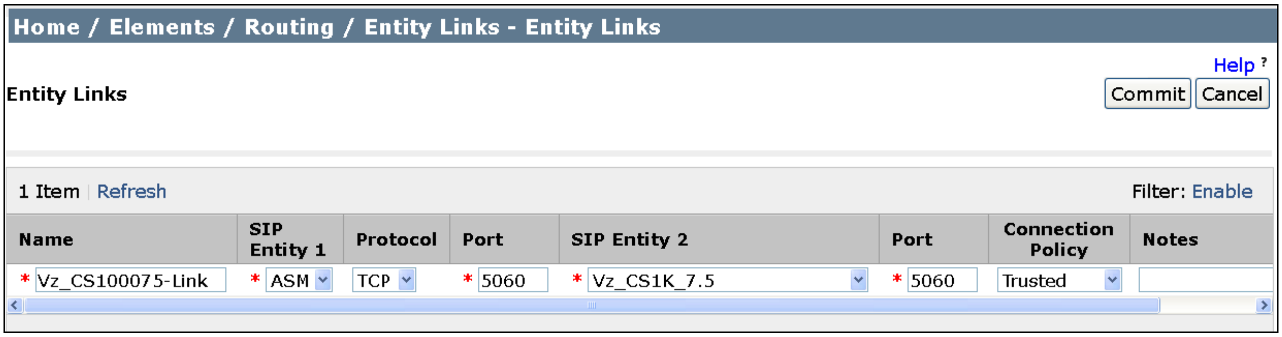
Select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name:** Enter an identifier for the link.
- **SIP Entity 1:** Select SIP Entity defined for Session Manager.
- **Protocol:** Select protocol to use "**TCP**".
- **Port:** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is "**5060**".
- **SIP Entity 2:** Select the SIP Entity defined for CS1000E.
- **Port:** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is "**5060**".
- **Trusted** Check this option box.
- **Notes:** Enter a brief description. [Optional].

Click **Commit** to save the **Entity Link** definition.

The following screen shows the Entity Link defined for the SIP trunk between Session Manager and Avaya Communication Server 1000E.



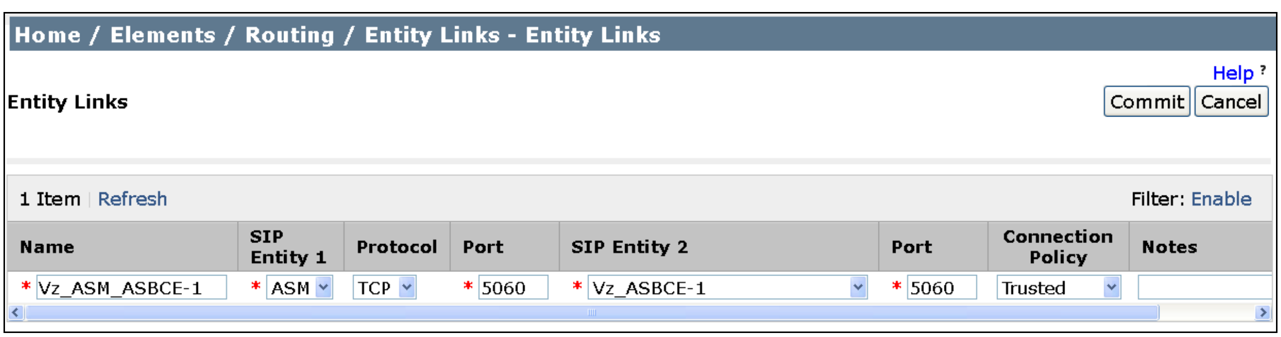
6.5.2 Entity Link to Avaya SBC for Enterprise

Select **Entity Links** from the left navigation menu. Click **New** (not shown). Enter the following values**.**

- **Name:** Enter an identifier for the link.
- **SIP Entity 1:** Select SIP Entity defined for Session Manager.
- **SIP Entity 2:** Select the SIP Entity defined for the ASBCE.
- **Protocol:** After selecting both SIP Entities, select "**TCP"**.
- **Port:** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is "**5060**".
- **Trusted:** Check this option box.
- **Notes:** Enter a brief description. [Optional].

Click **Commit** to save the **Entity Link** definition.

The following screen shows the entity link defined for the SIP trunk between Session Manager and the ASBCE.



6.6. Routing Policies

Routing Policies describe the conditions under which calls will be routed to the Avaya Communication Server 1000E or the ASBCE.

6.6.1 Routing Policy to Avaya Communication Server 1000E

To add a new Routing Policy, select **Routing Policies.** Click **New** (not shown). In the **General** section, enter the following values:

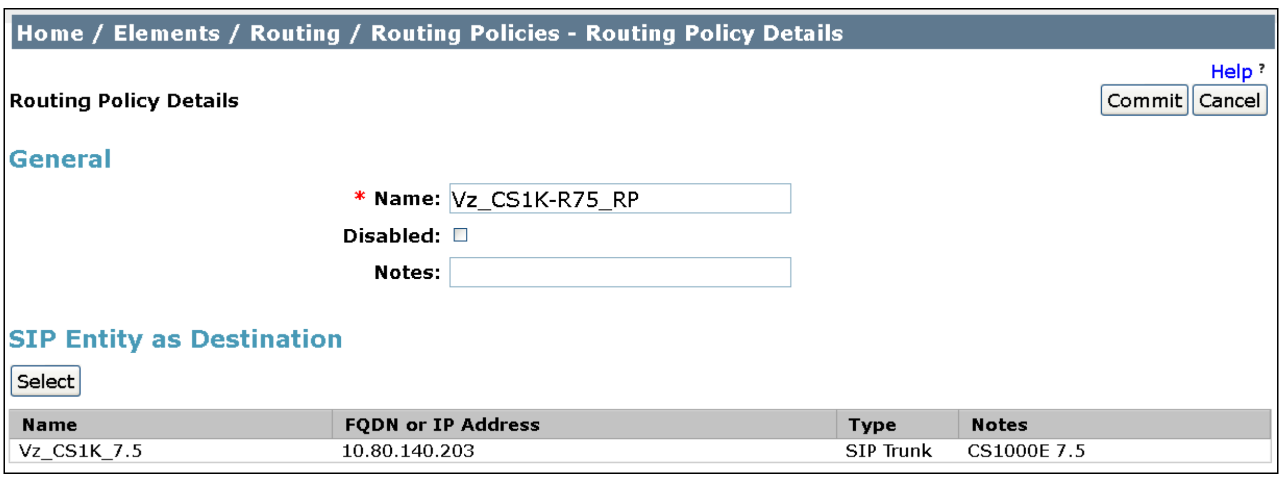
- **Name:** Enter an identifier to define the Routing Policy.
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional].

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with CS1000E and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page (not shown).

Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for Avaya Communication Server 1000E.



6.6.2 Routing Policy to Avaya SBC for Enterprise

To add a new Routing Policy, select **Routing Policies.** Click **New** (not shown). In the **General** section, enter the following values.

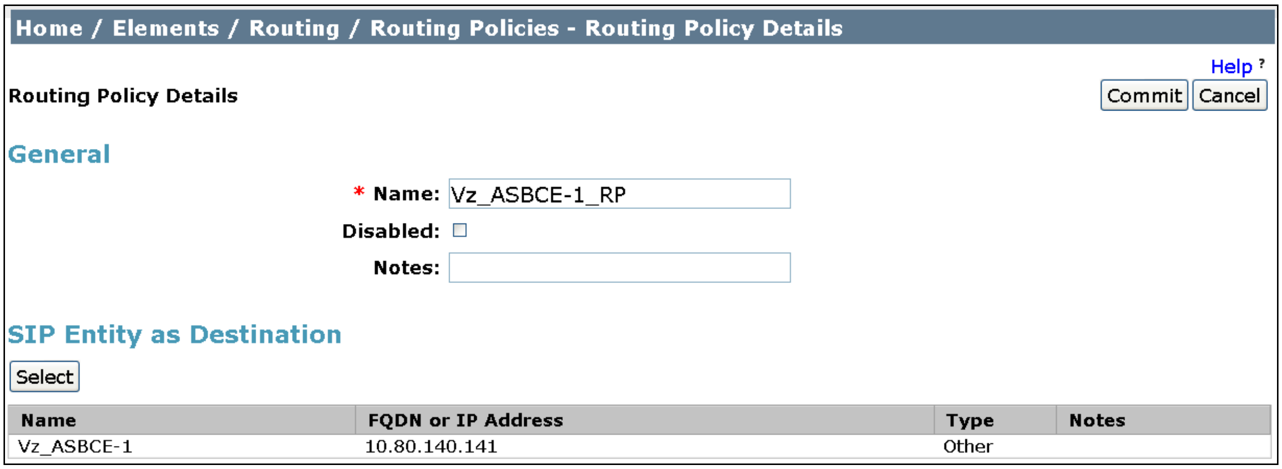
- **Name:** Enter an identifier to define the Routing Policy.
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional].

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with the ASBCE and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page (not shown).

Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for the ASBCE.



6.7. Dial Patterns

Dial Patterns are used to route calls to the appropriate Routing Policies, and ultimately to the appropriate SIP Entities. Dial Patterns will be configured to route outbound calls from CS1000E users to the PSTN via the Verizon IPCC Service. Other dial patterns will be configured to route inbound calls from Verizon IPCC Service to CS1000E users.

6.7.1 Inbound Verizon Calls to CS1000E Users

To define a Dial Pattern, select **Dial Patterns** from the navigation menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to Avaya Communication Server 1000E (e.g., a Verizon inbound toll-free number).
- **Min:** Enter the minimum number of digits.
- **Max:** Enter the maximum number of digits.
- **SIP Domain:** Select a SIP Domain from drop-down menu or select **"All"** if Session Manager should route incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional].

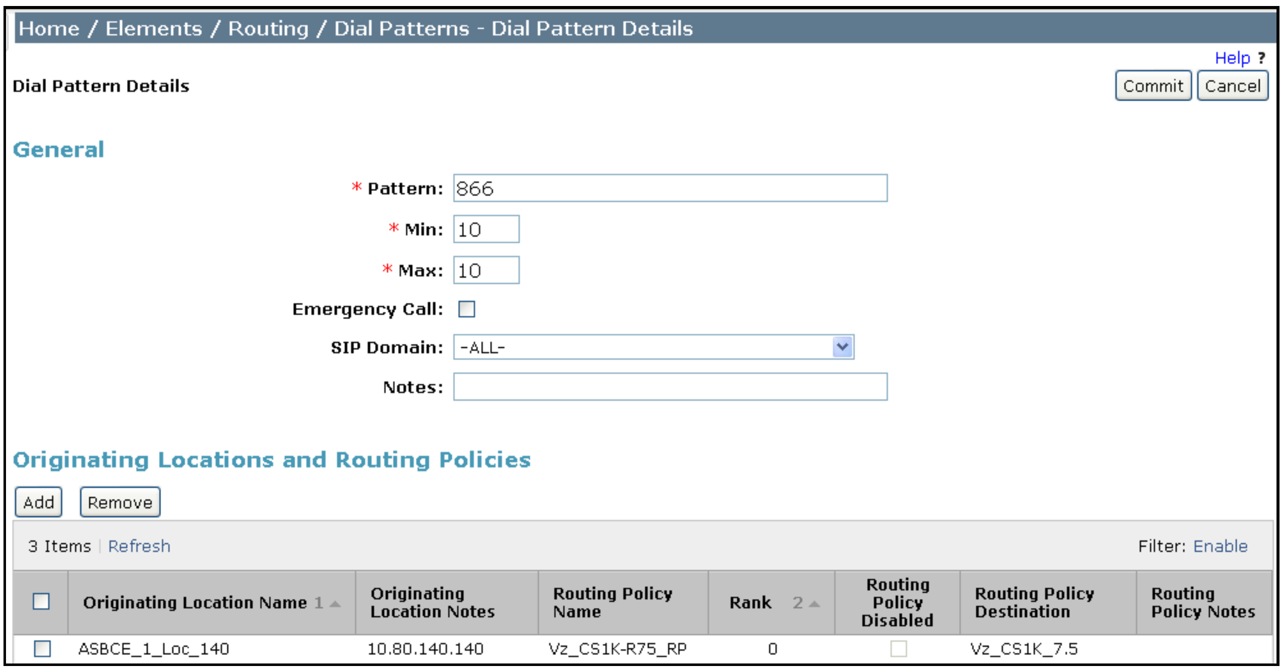
In the **Originating Locations and Routing Policies** section, click **Add.**

The **Originating Locations and Routing Policy List** page opens (not shown).

- In the **Originating Location** list, select "**Apply the Selected Routing Policies to All Originating Locations**" or alternatively, select a specific Location (e.g. "**ASBCE_1_Loc_140**"). In the example below, the ASBCE Location was selected as the originating Location.
- In the **Routing Policies** table, select the Routing Policy defined for Avaya Communication Server 1000E ("**Vz_CS1K_7.5**"**).**
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save.

The following screen shows an example Dial Pattern defined for the sample configuration. Repeat this procedure as needed to allow additional Verizon toll-free numbers to be routed to the CS1000E. Wildcards may be used in the **Pattern** field so that blocks of matching numbers are routed based on a single dial pattern.



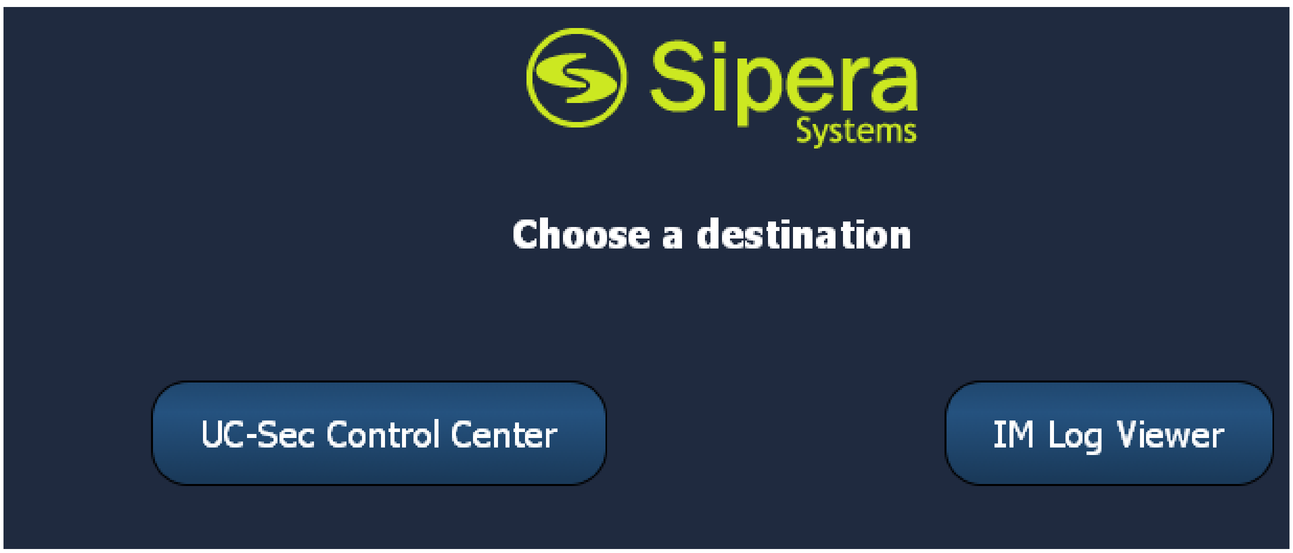
7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya Session Border Controller for Enterprise is used as the edge device between the Avaya CPE and Verizon Business.

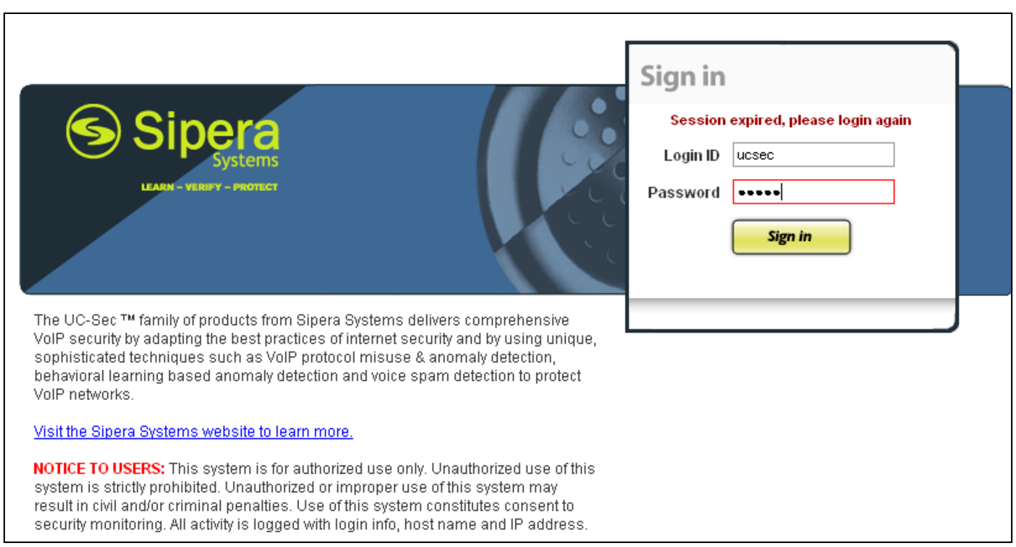
These Application Notes assume that the installation of the ASBCE and the assignment of a management IP Address have already been completed.

7.1. Access the Management Interface

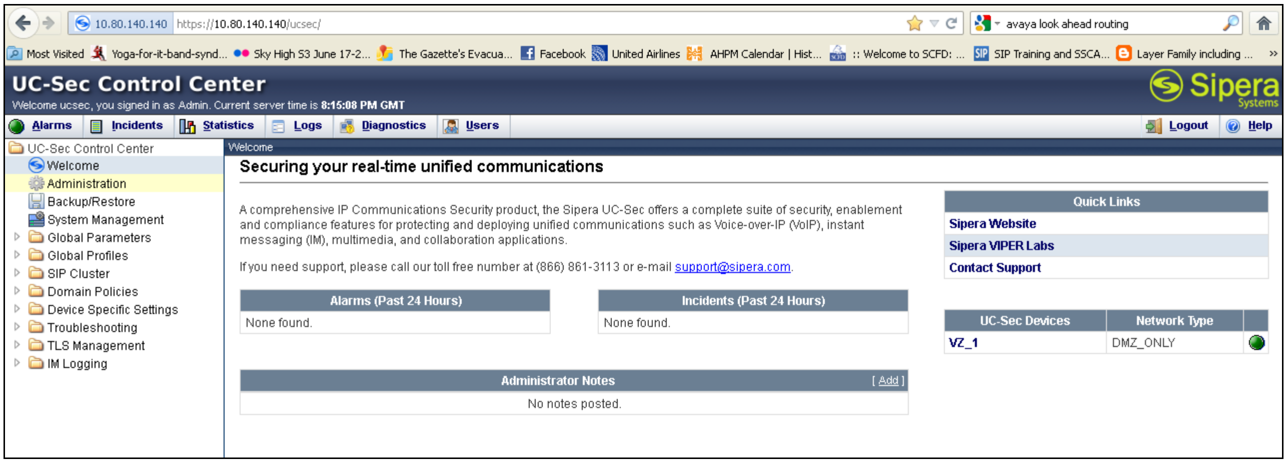
Access the web management interface by entering the URL https://<ip-address> where <ip-address> is the management IP address assigned during installation. Select **UC-Sec Control Center**.



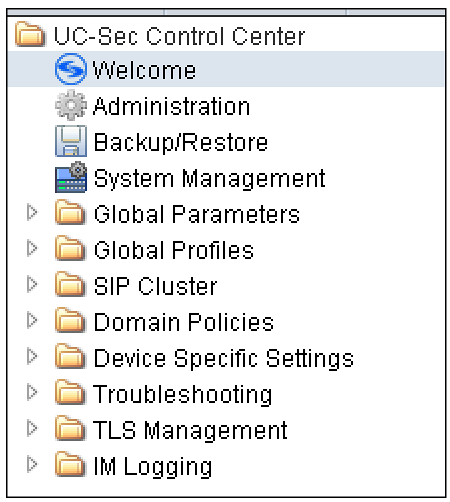
A log-in screen is presented. Enter an appropriate **Login ID** and **Password**.



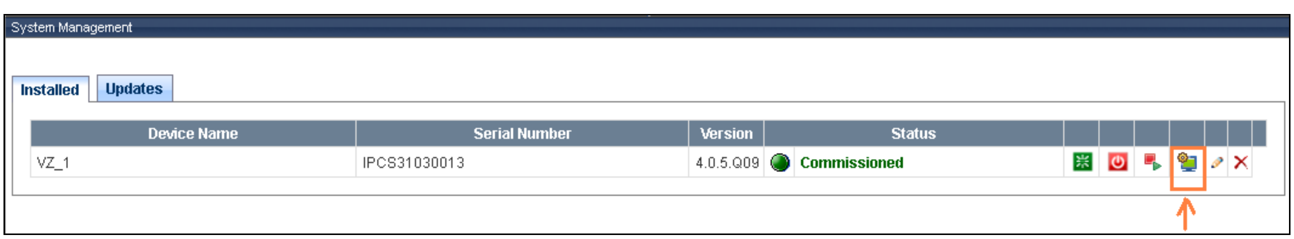
Once logged in, the main page of the UC-Sec Control Center will appear.



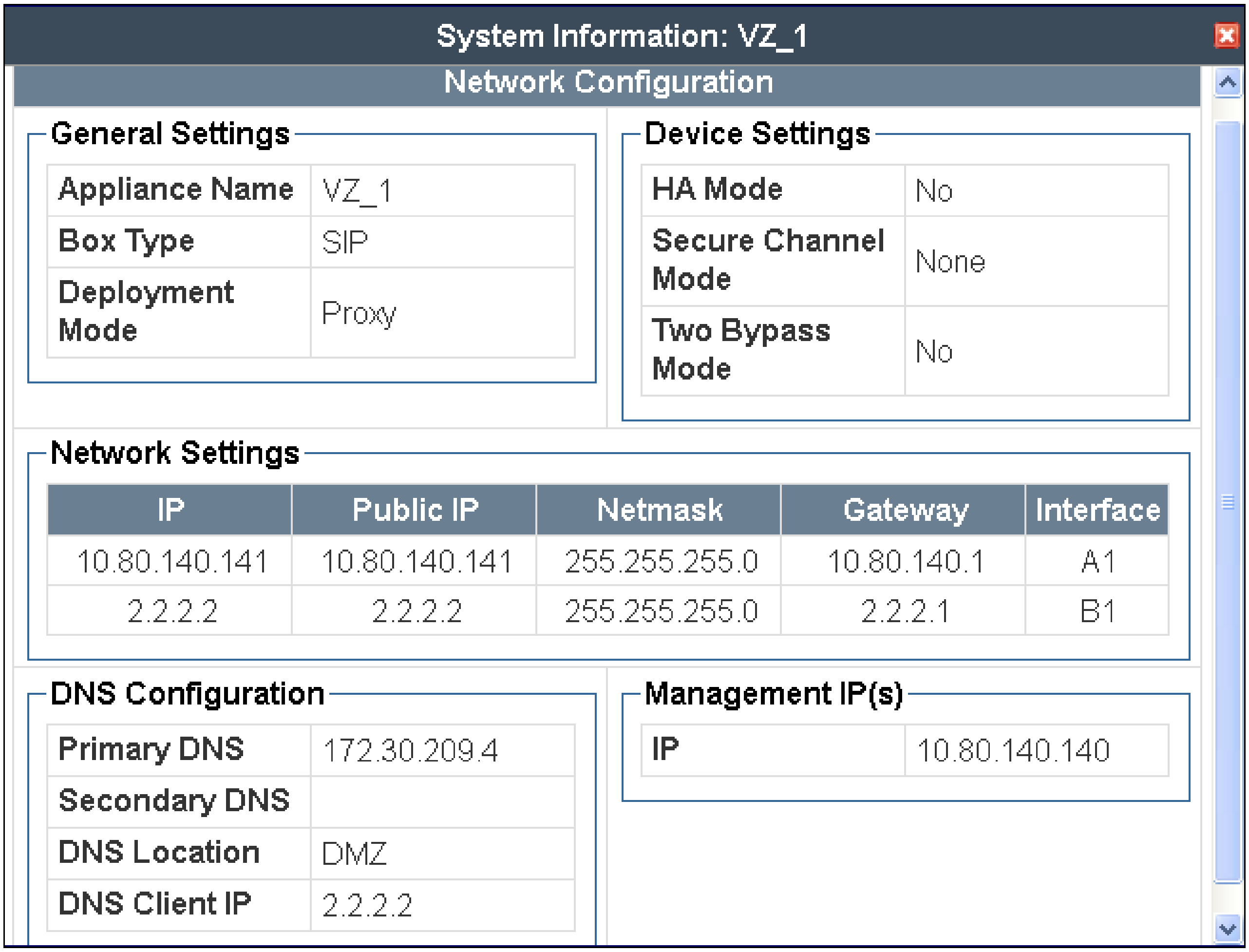
The following image illustrates the menu items available on the left-side of the UC-Sec Control Center screen.



To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named "**VZ_1**" is shown. To view the configuration of this device, click the monitor icon (the third icon from the right).



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”**.



7.2. Device Specific Settings

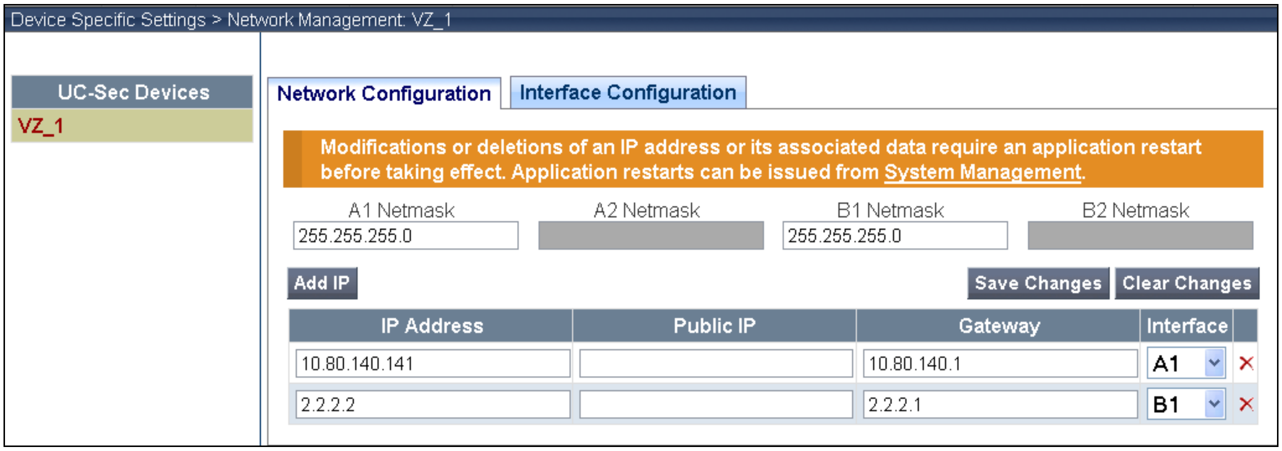
7.2.1 Define Network Information

Network information is required on the ASBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface for the internal side and the **B1** interface for the external side. Each side of the ASBCE can have only one interface assigned. To define the network information, navigate to **Device Specific Settings → Network Management** in the **UC-Sec Control Center** menu on the left hand side and click **Add IP**. A new line appears that can be configured.

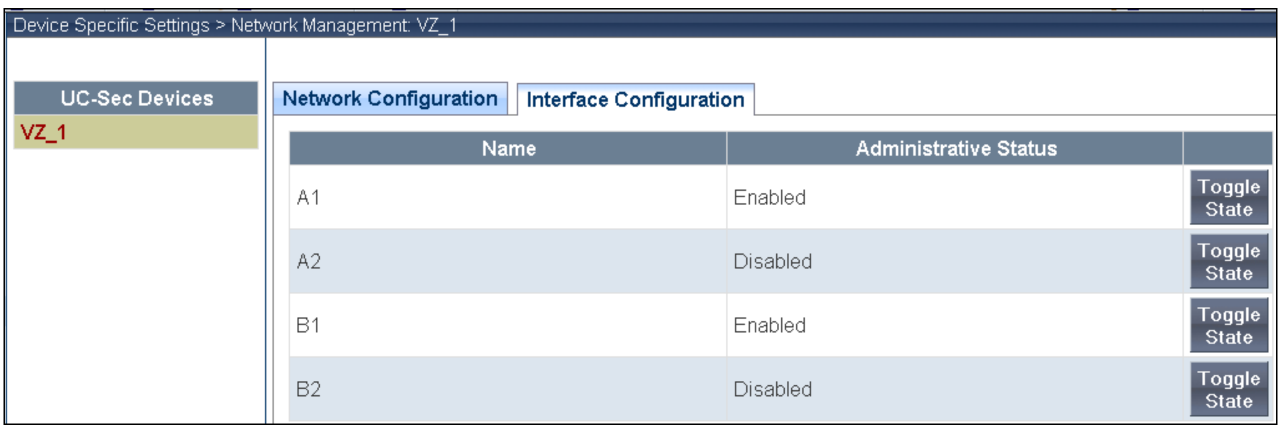
- **IP Address:** Enter the IP Address for the internal interface.
- **Gateway:** Enter the appropriate gateway IP Address.
- **Interface:** Select the desired hardware interface **(A1)**.

Click **Save Changes**. Repeat the process for external interfaces using **B1.**

Note: Multiple IP addresses defined on a single interface must be in the same subnet.



Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.



7.2.2 Signaling Interfaces

To define the signaling interfaces on the ASBCE, navigate to **Device Specific Settings → Signaling Interface** in the **UC-Sec Control Center** menu on the left hand side and Select **Add Signaling Interface**.

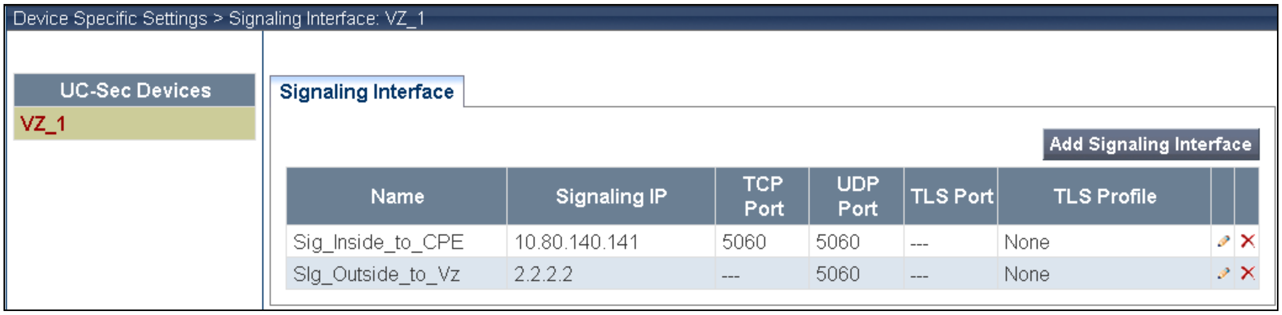
Define a signaling interface for Verizon:

- **Name:** Enter a descriptive name for the external signaling interface for the Verizon network.
- **IP Address:** Choose the external address for signaling.
- **TCP/UDP/TLS Port:** Enter the port for the desired protocol.

Click **Finish** (not shown).

Repeat the process for the internal Avaya network.

The screen below shows the configured internal and external signaling interfaces used in the sample configuration.



7.2.3 **Media Interfaces**

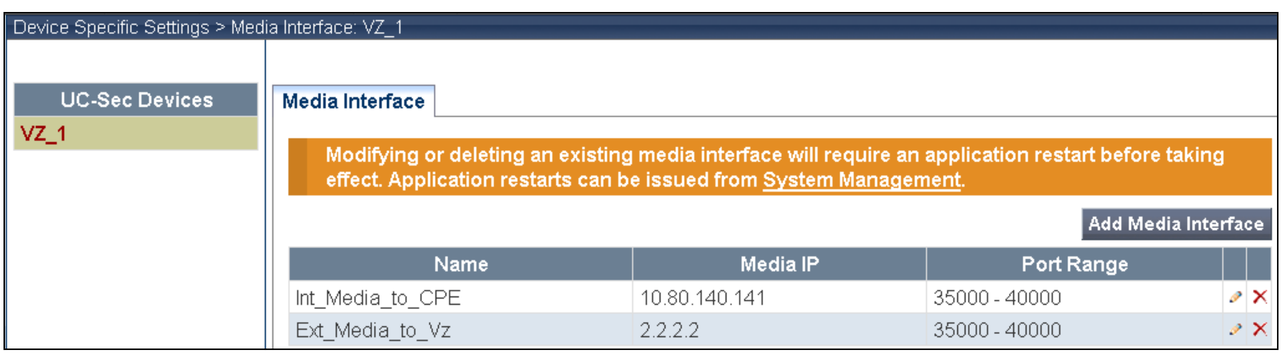
To define the media interfaces on the ASBCE, navigate to **Device Specific Settings → Media Interface** in the **UC-Sec Control Center** menu on the left hand side and select **Add Media Interface**. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signaling or can be different.

Define a media interface for Verizon:

- **Name:** Enter a descriptive name for the external media interface for the Verizon network.
- **IP Address:** Choose the external address for the media.
- **Port Range:** Enter port ranges for the media path.

Repeat the process for the internal Avaya network.

The screen below shows the configured internal and external media interfaces used in the sample configuration.



7.3. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.3.1 Routing Profiles

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.

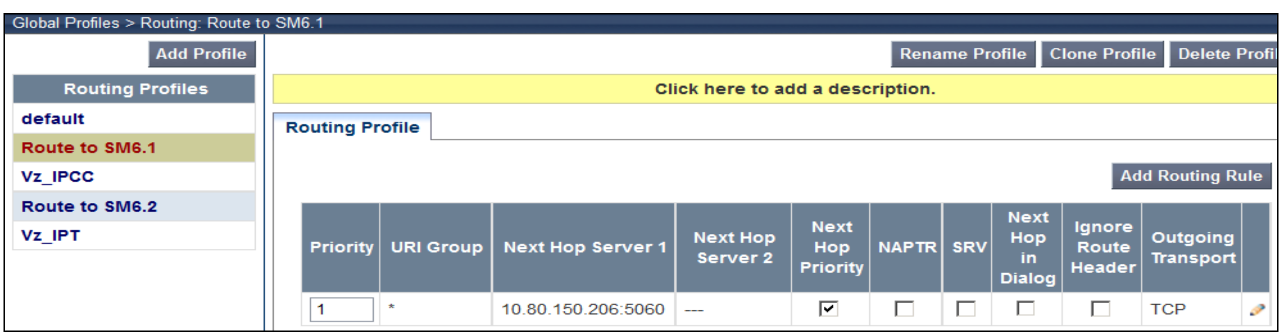
Create a Routing Profile for Session Manager and a separate Routing Profile for Verizon SIP Trunk. To add a Routing Profile, navigate to **UC-Sec Control Center →Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue (not shown).

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

- **URI Group:** Select "*" from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server with a colon and the port.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server**: Checked.
- **Next Hop in Dialog:** (Optional) Checked only if information in the Via Header is to be used instead of received port and IP.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

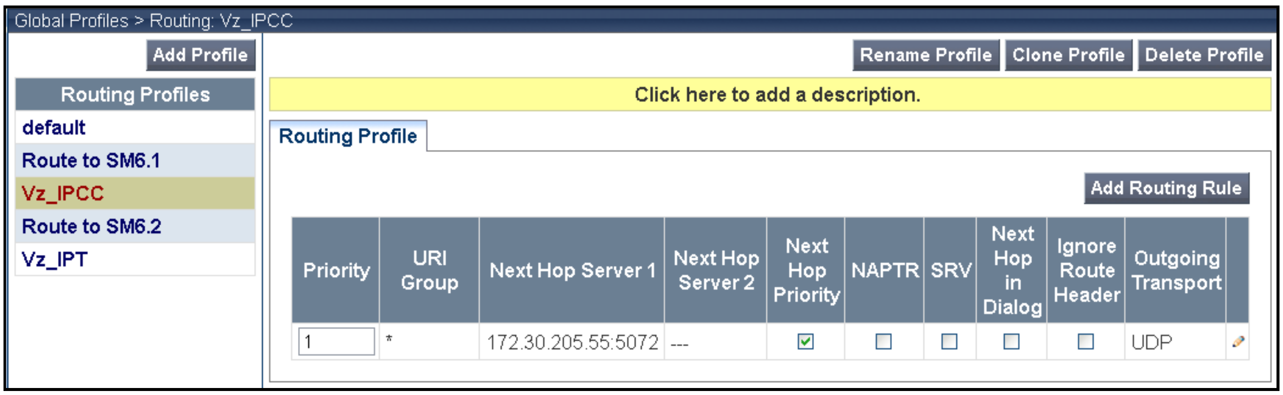
Click **Finish** (not shown).

The following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module followed by a colon and the port being used. The **Outgoing Transport** must match the ASBCE Entity Link created on Session Manager in **Section 6.5**.



The following screen shows the Routing Profile to Verizon. In the **Next Hop Server 1** field enter the IP address that Verizon uses for the Verizon IPCC with a colon and then the port number. Check the **Next Hop Priority.** Enter "**UDP**" for the **Outgoing Transport** field.

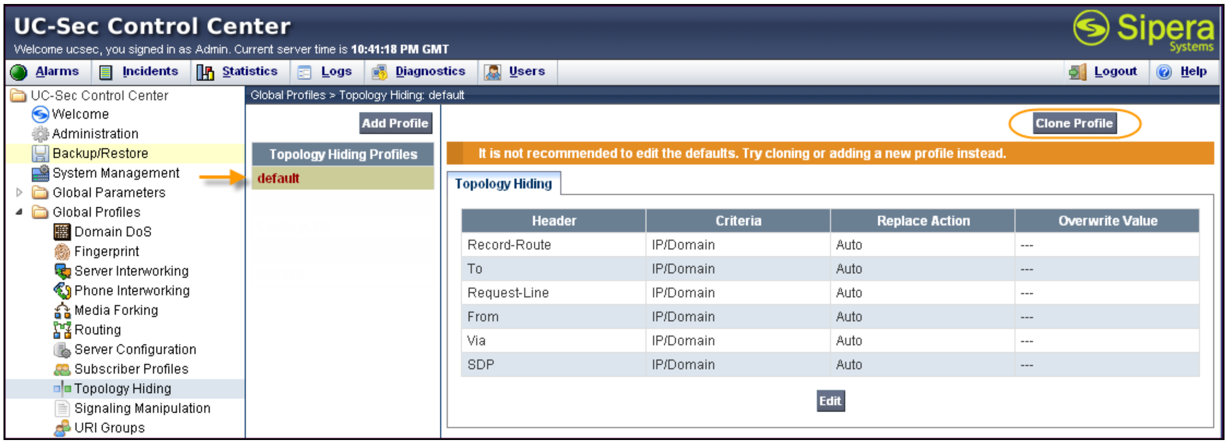
NOTE: If the outside port is something other than 5060 the **Next Hop Server 1** and **Next Hop Server 2** fields **<u>must</u>** contain a colon and the port number after the IP address or domain name. If these are not entered, then the OPTIONS messages from Session Manager will be proxied to the service provider with a port of 5060 and may not get a response. This will cause ASBCE to respond to the Session Manager OPTIONS with a 408 Request Timeout, which will cause the Session Manager to mark the entity link as down.



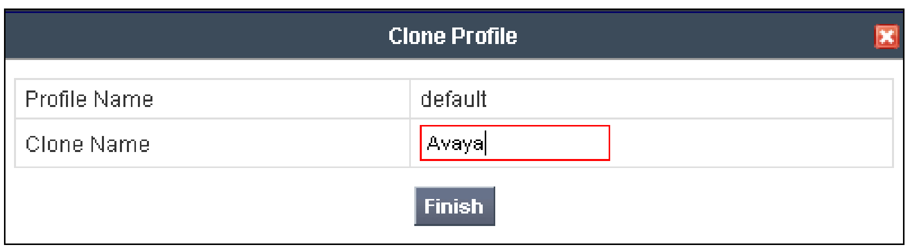
7.3.2 Topology Hiding Profile

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

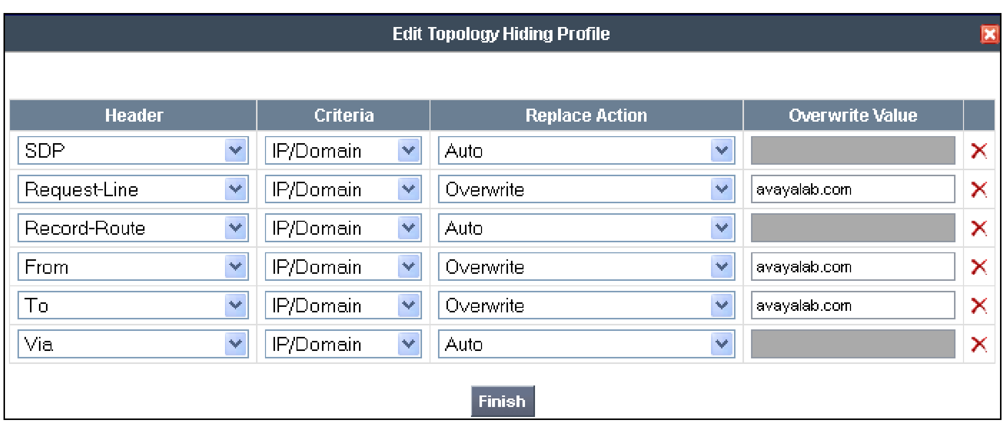
Create a Topology Hiding Profile for the enterprise and a separate Topology Hiding Profile for the Verizon SIP Trunk. In the sample configuration, the **Enterprise** and **SIP Trunk** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center →Global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



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



Edit the **Avaya** profile to overwrite the **To**, **Request-Line** and **From** headers shown below with the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager (**Section 6.1**). Click **Finish** to save the changes.

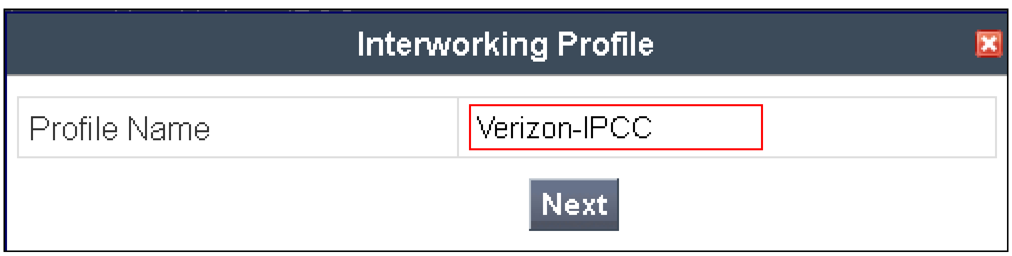


It is not necessary to modify the **Verizon** profile from the default values if IP addresses are used. The following screen shows the Topology Hiding Policy **Verizon** created for Verizon with the domain names overwritten in the appropriate fields:

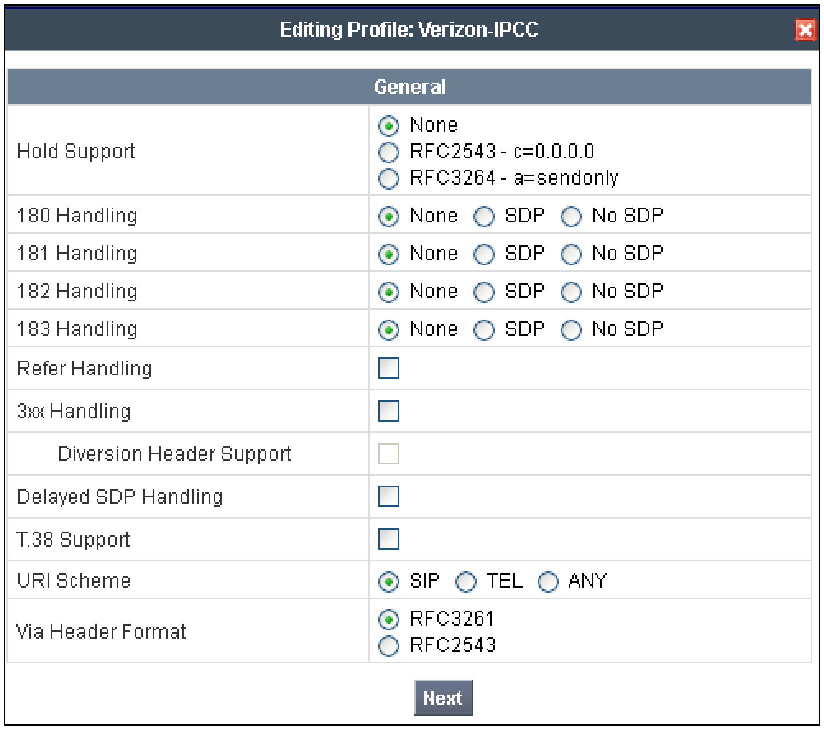
Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	adevc.avaya.globalipcom.com
To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
SDP	IP/Domain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

7.3.3 Server Interworking

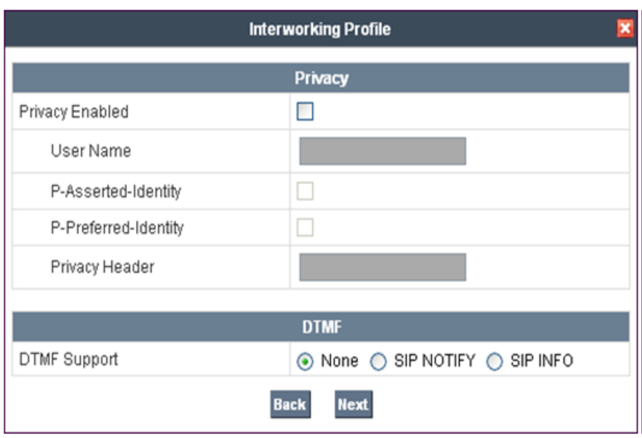
Click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as "**Verizon-IPCC**" shown below. Click **Next**.

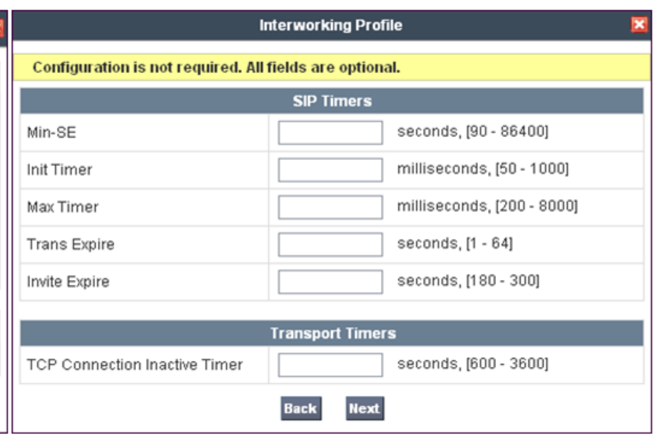


In the new window that appears, default values can be used. Click **Next** to continue**.**



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

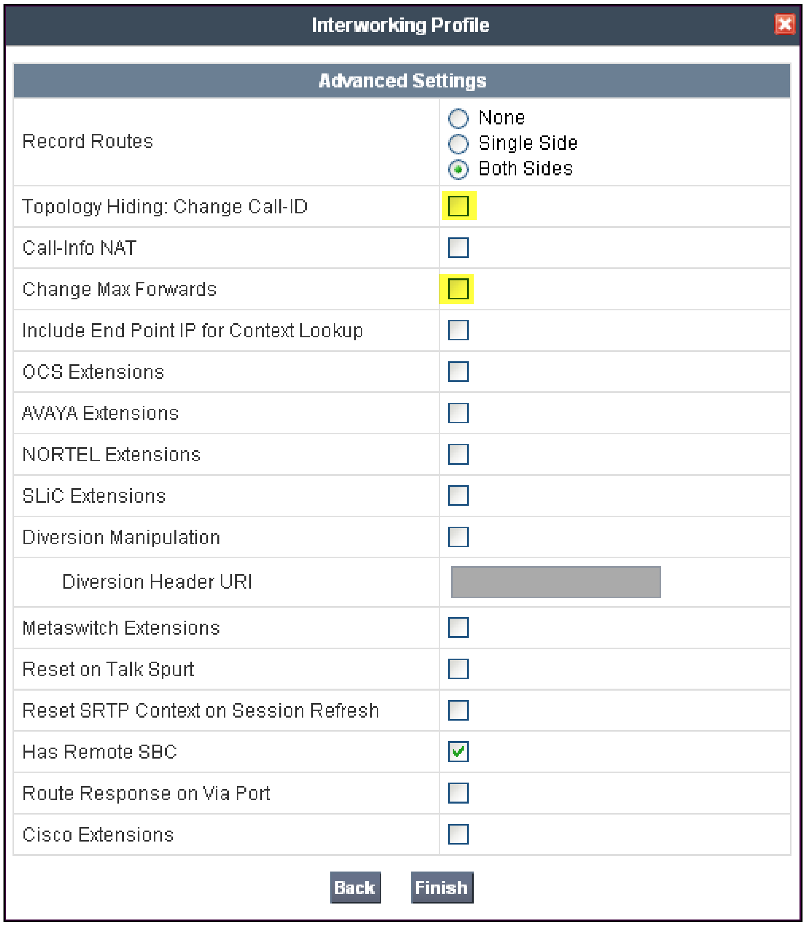




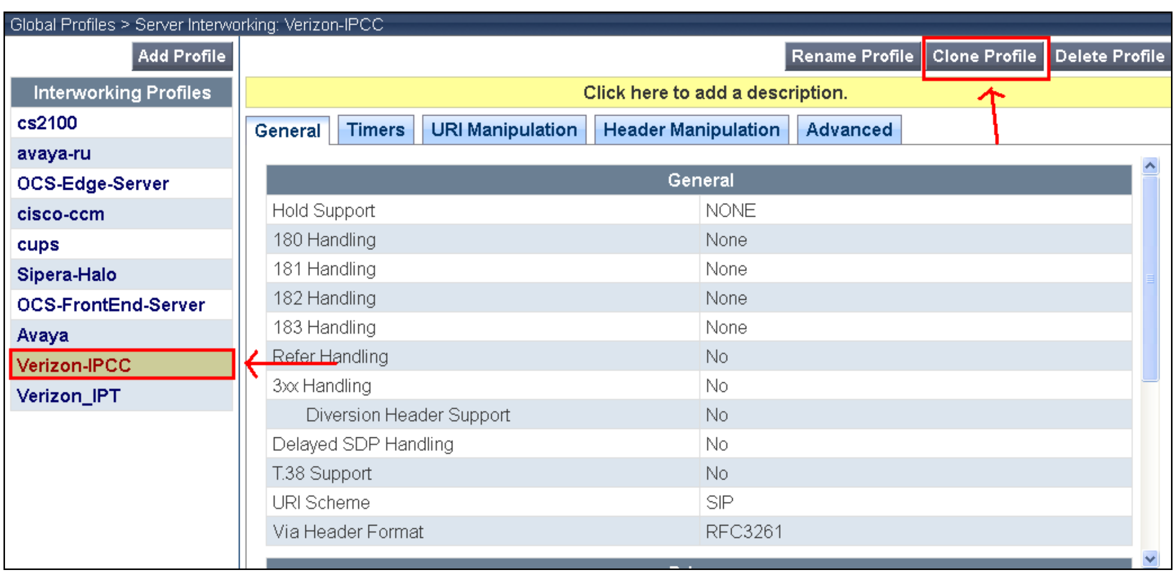
On the **Advanced Settings** window uncheck the following default settings:

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

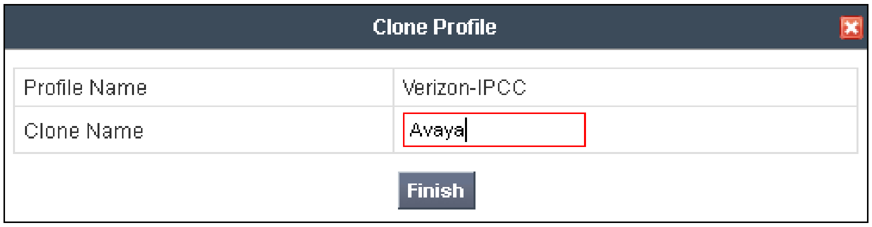
Click **Finish** to save changes.



The Avaya profile will be created by cloning the Verizon profile created in the previous section. To clone a Server Interworking Profile for Avaya, navigate to **UC-Sec Control Center →Global Profiles → Server Interworking** and click on the previously created profile for the enterprise, then click on **Clone Profile** as shown below.



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



7.3.4 **Signaling Manipulation**

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

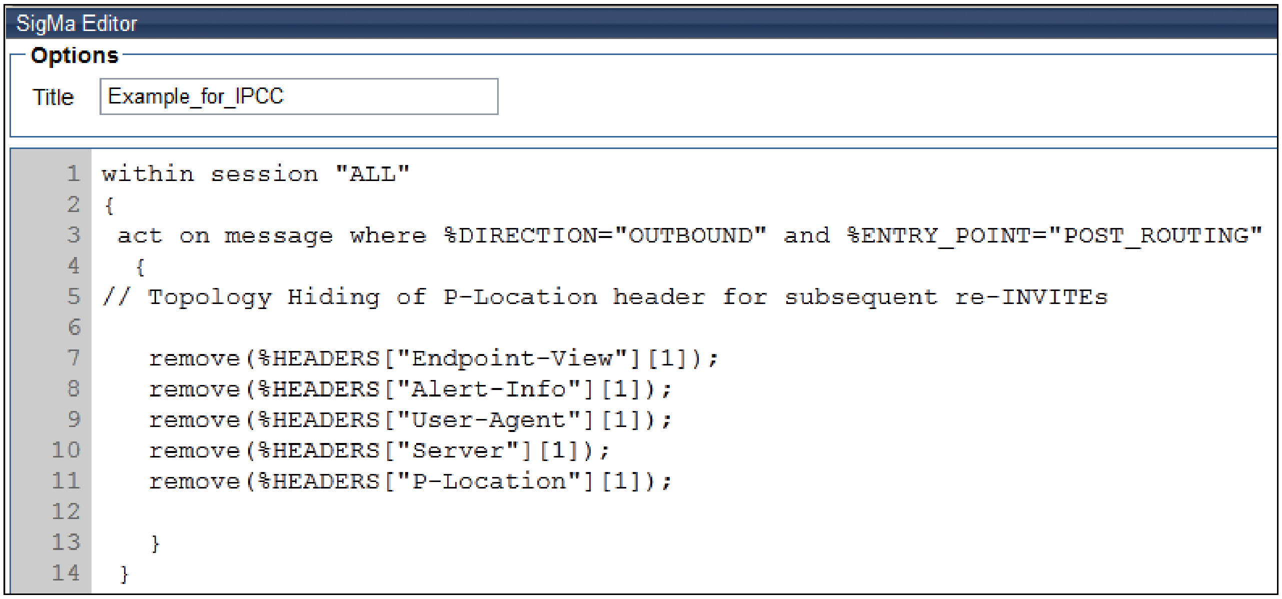
The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the ASBCE. Using this language, a script can be written and tied to a given flow. The ASBCE appliance then interprets this script at the given entry point or "hook point".

These Application Notes will not discuss the full feature of Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding and to remove unwanted headers in the SIP messages to and from Verizon.

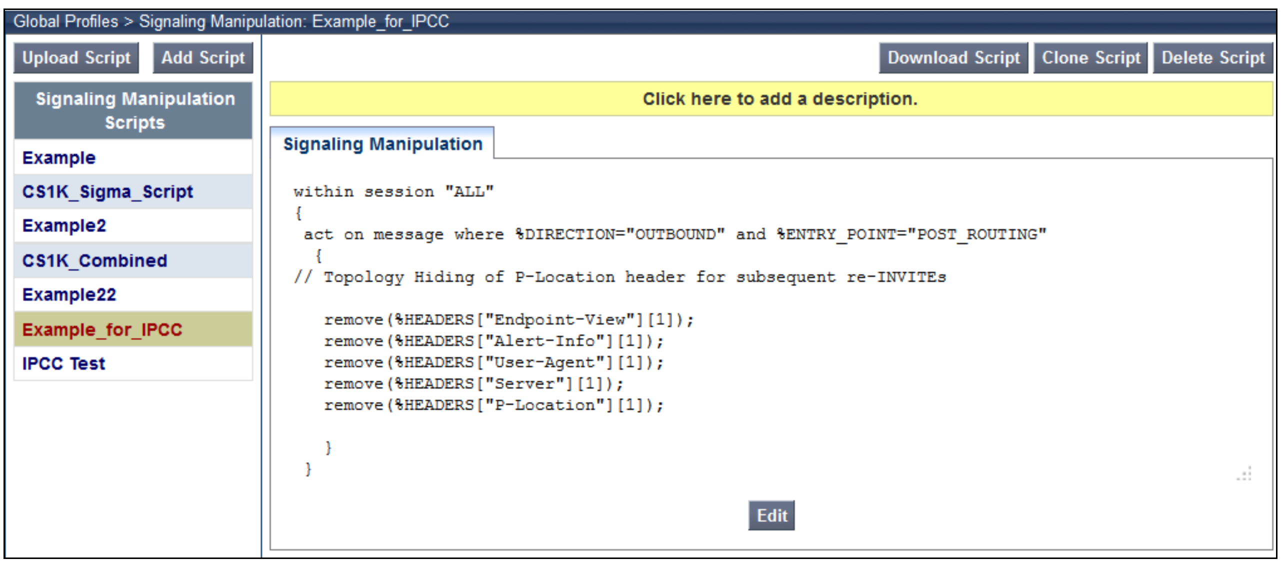
To create a new Signaling Manipulation, navigate to **UC-Sec Control Center →Global Profiles → Signaling Manipulation** and click on **Add Script** (not shown). A new blank SigMa Editor window will pop up. Enter Appropriate script and click **Save**.
The script will act on all outbound traffic to Verizon after the SIP message has been routed through the ASBCE. The script is further broken down as follows:

- **within session "All"** Transformations applied to all SIP sessions. Actions to be taken to any SIP message.
- **act on message %DIRECTION="OUTBOUND"** Applied to a message leaving ASBCE.
- **%ENTRY_POINT="POST_ROUTING"** The "hook point" to apply the script after the SIP message has routed through ASBCE.
- **remove(%HEADERS["P-Location"][1]);** Used to remove an entire header (like P-Location). The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message**.**

With this script Endpoint-View, Alert-Info, User-Agent, Server, and P-Location headers will be removed. These items are being removed for general security purposes and because the SIP Service provider has no need of these items. These are optional inclusions to any SigMa Script.

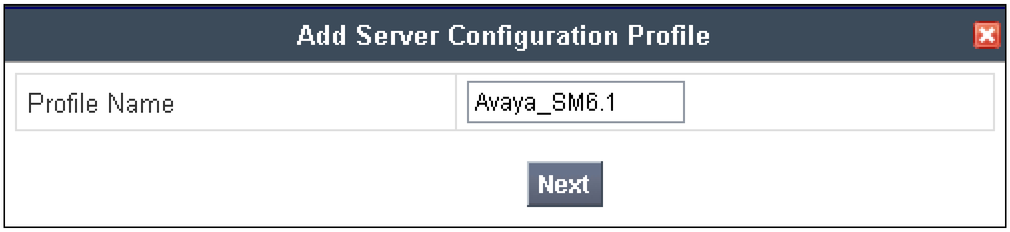


The following screen shows the finished Signaling Manipulation Script **"Example_for_IPCC"**. This script will later be applied to the Verizon Server Configuration in **Section 7.3.6**. The details of these script elements can be found in **Appendix A**.



7.3.5 Server Configuration

Servers are defined for each server connected to the ASBCE. In this case, Verizon is connected as the Trunk Server and Session Manager is connected as the Call Server. To define the Session Manager server, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter a profile name in the pop-up menu.

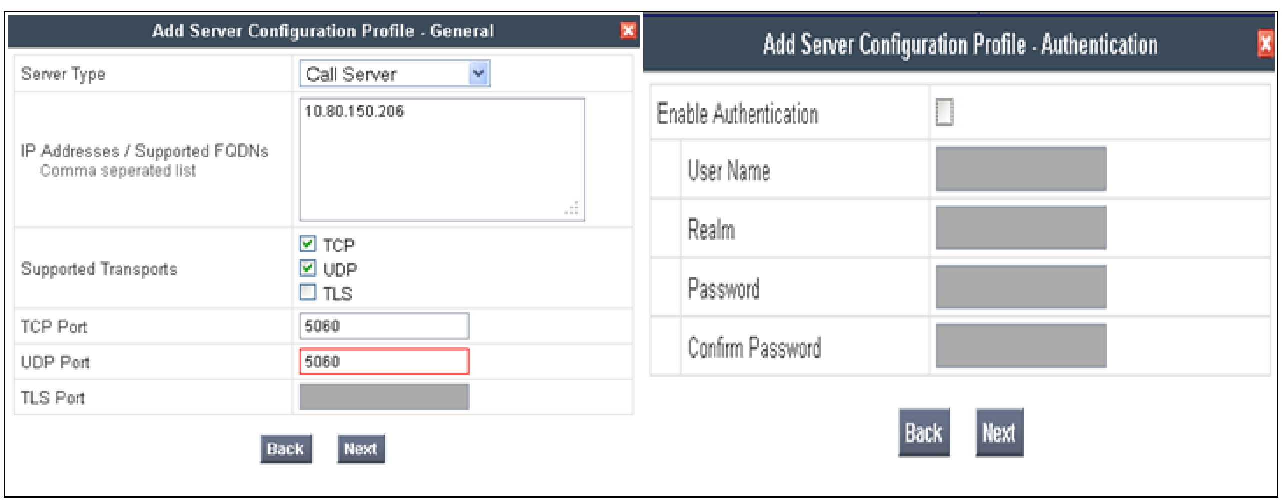


In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select "**Call Server**" from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module.
- **Supported Transports:** Select **TCP** and **UDP**. This is the transport protocol used in the ASBCE Entity Link on Session Manager configured in **Section 6.5**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the ASBCE Entity Link on Session Manager configured in **Section 6.5.**

Click **Next** to continue.

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

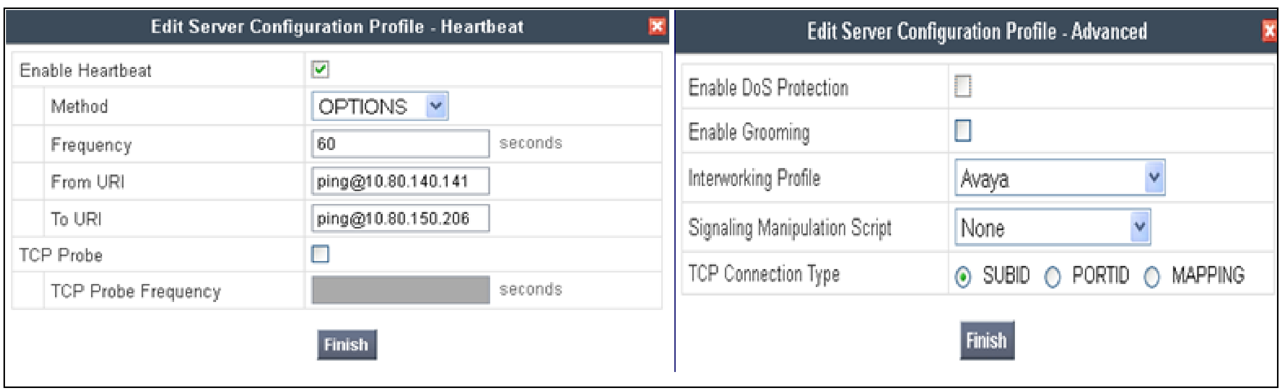


In the new window that appears, OPTIONS were only configured for Session Manager. Enter the following values. Use default values for all remaining fields:

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

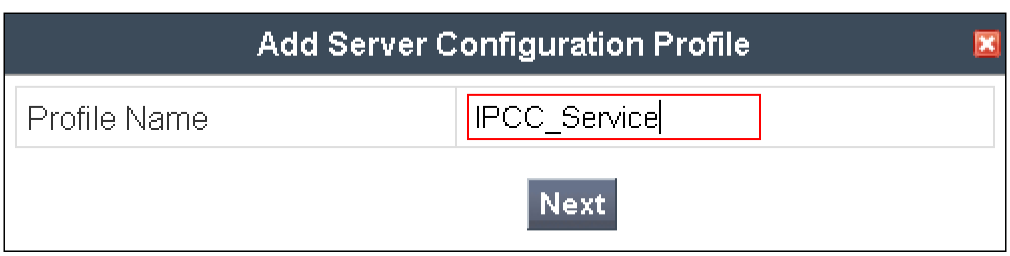
Click **Next** to continue.

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.3.3.** For **Signaling Manipulation Script** select a script if desired. Use default values for all remaining fields. Click **Finish** to save the configuration.

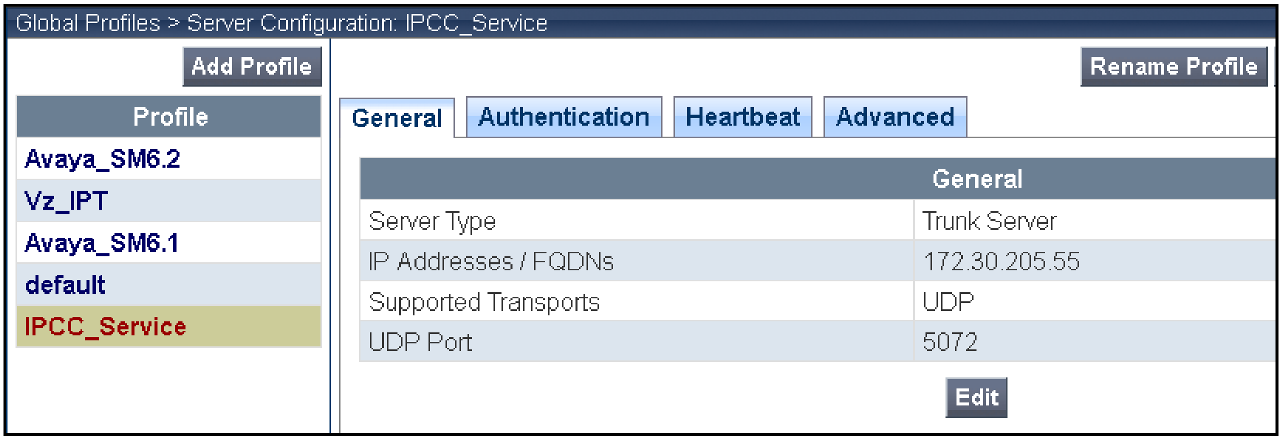


7.3.6 Server Configuration for Verizon IPCC

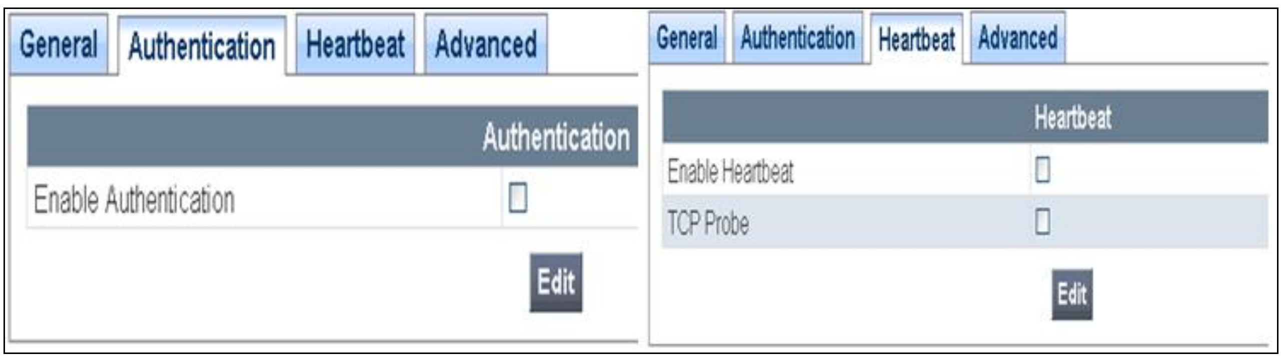
To define the Verizon IPCC, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and repeat the instructions above with appropriate settings.



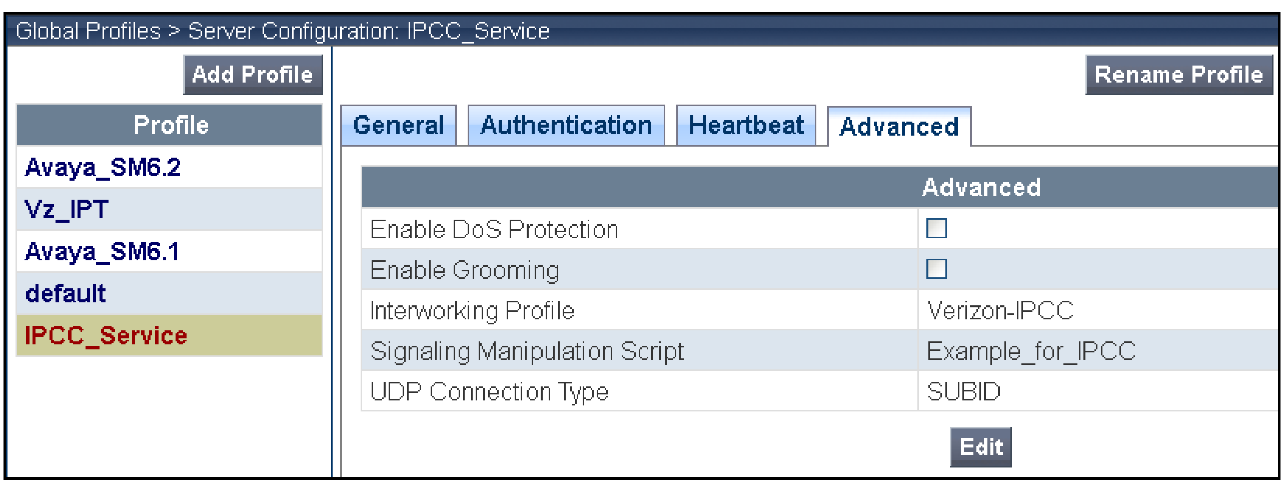
The screen below shows the General parameter settings for the "**IPCC_Service**" server configured as **Trunk Server**, with Verizon IP Address, transport, and port:



The following screens show the settings in the **Authentication** and the **Heartbeat** tabs (note that external OPTIONS to Verizon are not enabled in this configuration):



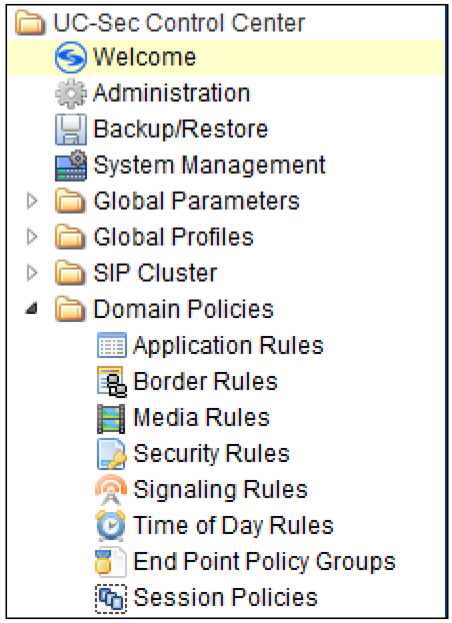
In the **Advanced Tab**, select "**Verizon-IPCC**" for **Internetworking Profile** and "**Example_for_IPCC**" as the **Signaling Manipulation Script** as shown below:



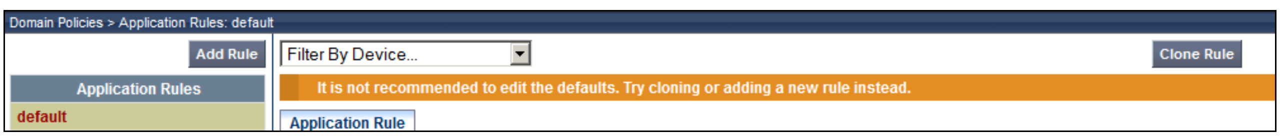
Click **Finish** to save changes (not shown).

7.4. Domain Policies – Application Rule

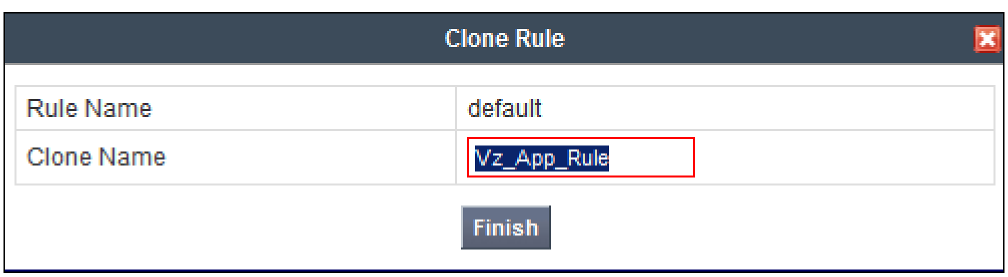
Select **Domain Policies → Application Rules** from the left-side menu as shown below.



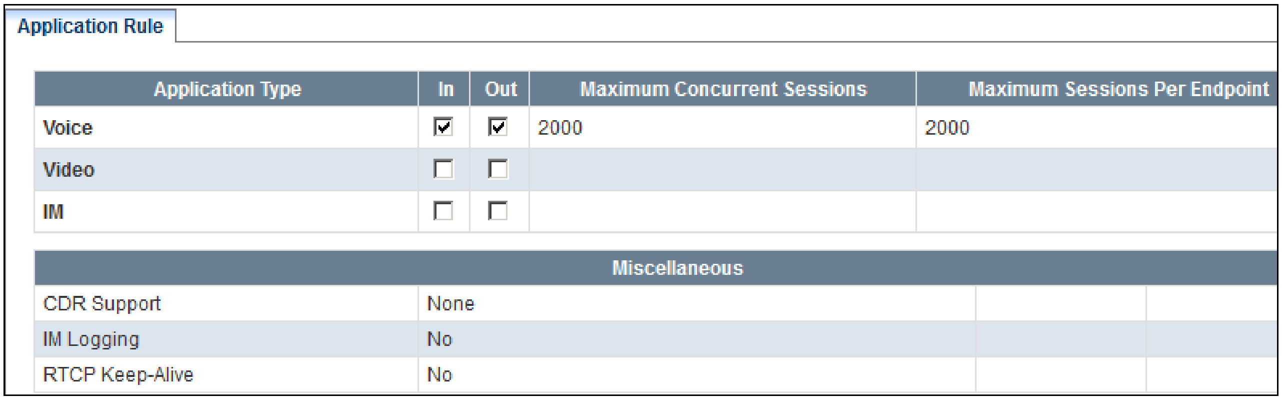
In the sample configuration, a single application rule was created by cloning the default rule called "**default**". Select the default rule and click the **Clone Rule** button.



Enter a name in the **Clone Name** field, such as "**Vz_App_Rule**" as shown below. Click **Finish**.



Select the newly created rule and click the **Edit** button (not shown). In the resulting screen, change the default **Maximum Concurrent Sessions** to 2000, the **Maximum Session per Endpoint** to 2000. Click **Finish**.



Application Rule

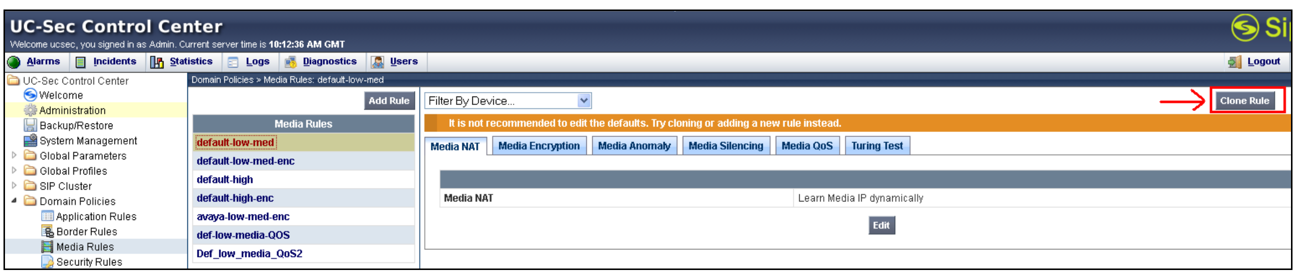
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	2000	2000
Video	☐	☐		
IM	☐	☐		

Miscellaneous	
CDR Support	None
IM Logging	No
RTCP Keep-Alive	No

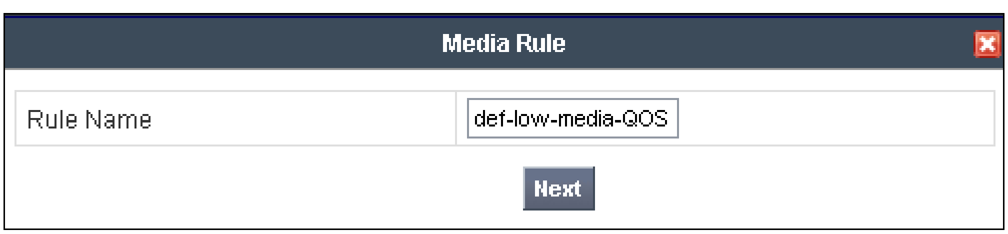
7.5. Domain Policies – Media Rules

Select **Domain Policies → Media Rules** from the left-side menu as shown below.

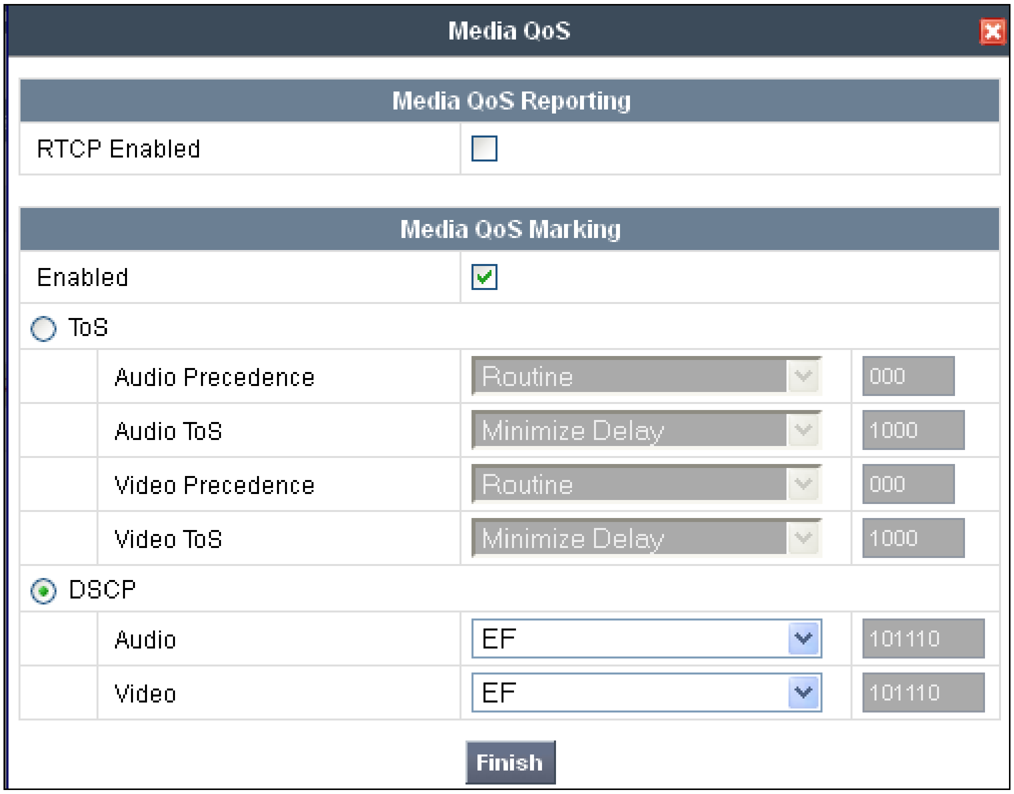
In the sample configuration, a single media rule was created by cloning the default rule called "**default-low-med**". Select the default-low-med rule and click the **Clone Rule** button.



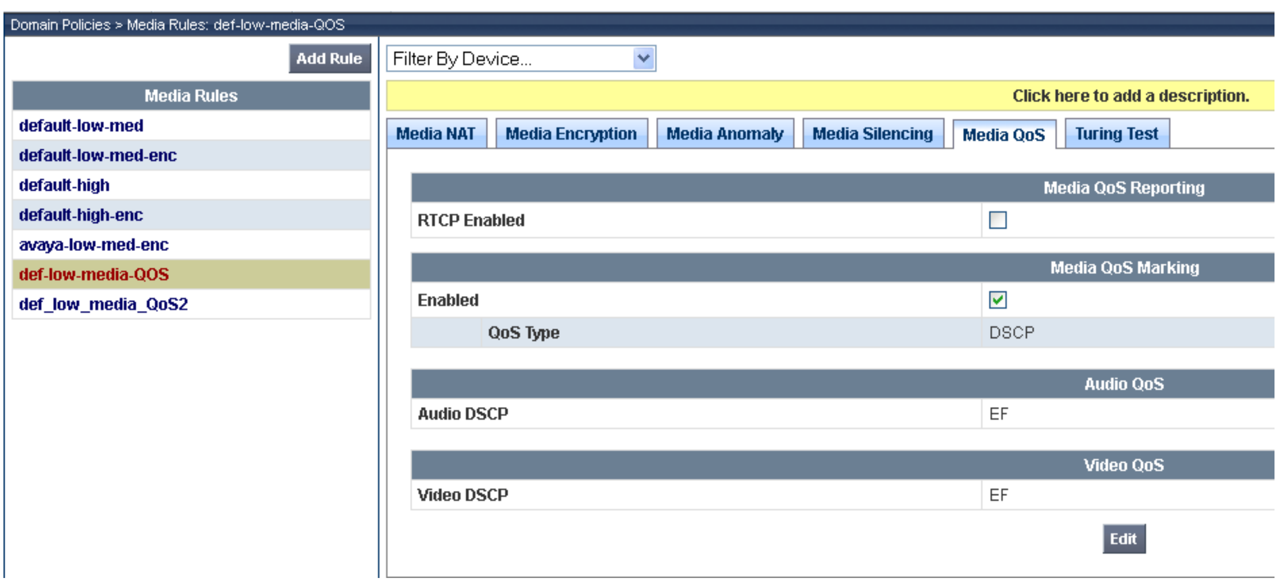
Enter a name in the **Clone Name** field, such as "**def-low-med-QoS**" as shown below. Click **Finish**.



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

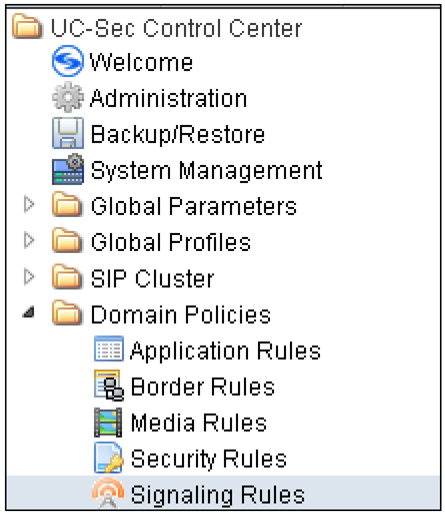


When configuration is complete, the "**def-low-med-QoS**" media rule **Media QoS** tab appears as follows.



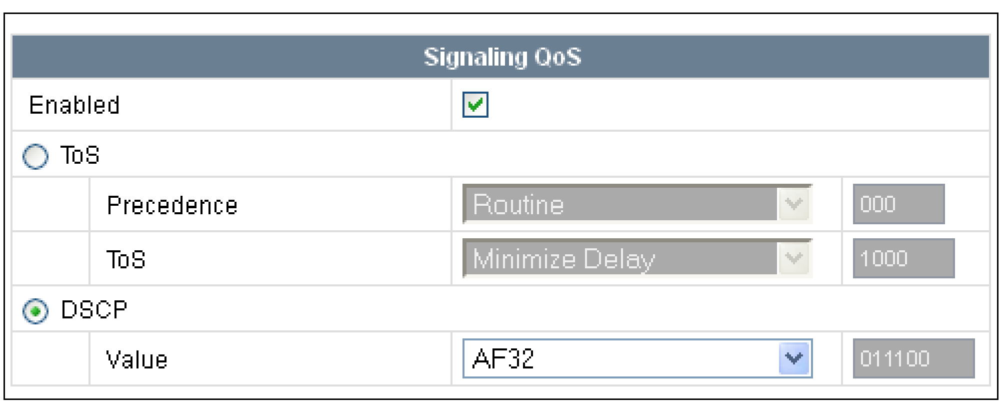
7.6. Domain Policies – Signaling Rules

Select **Domain Policies → Signaling Rules** from the left-side menu as shown below.

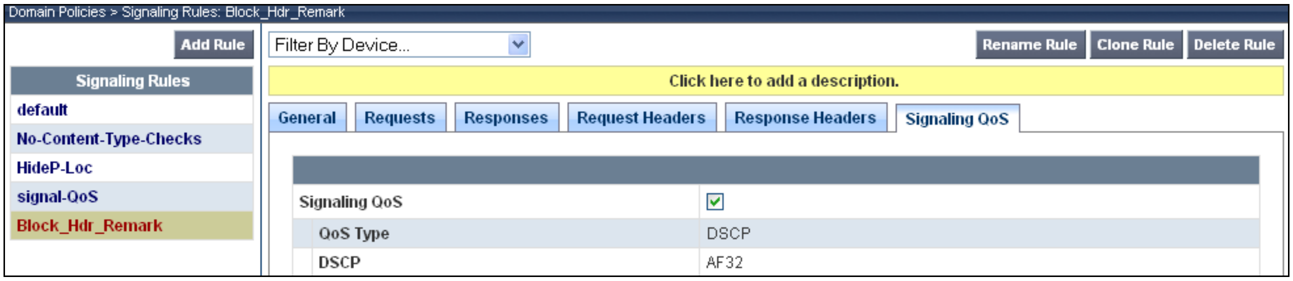


Click the **Add Rule** button (not shown) to add a new signaling rule. In the **Rule Name** field, enter an appropriate name, such as "**Block_Hdr_Remark**". Click **Next**.

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



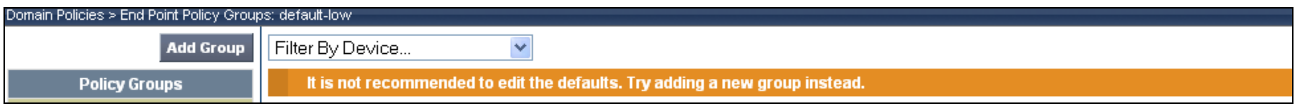
After this configuration, the new "**Block_Hdr_Remark**" rule will appear as follows.



7.7. Domain Policies – End Point Policy Groups

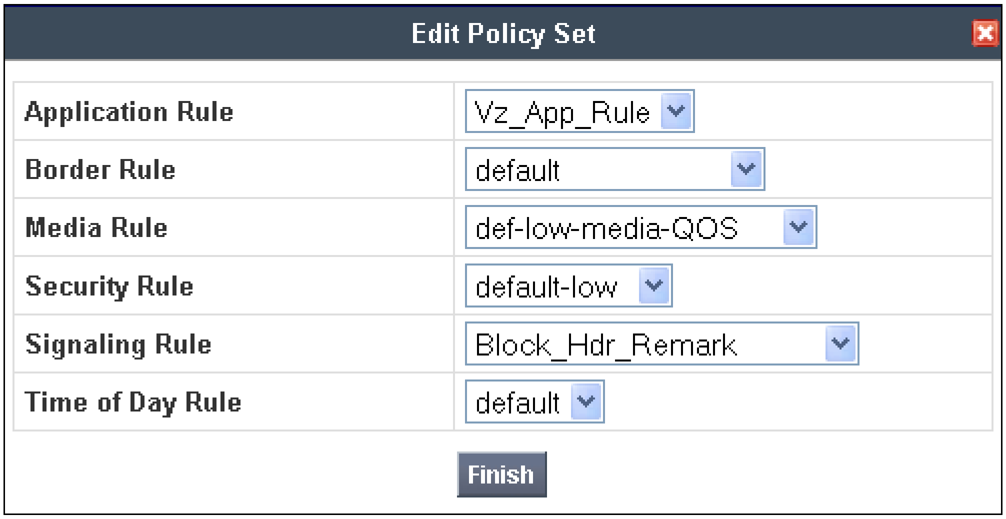
Select **Domain Policies → End Point Policy Groups** from the left-side menu as shown below.

Select the **Add Group** button.

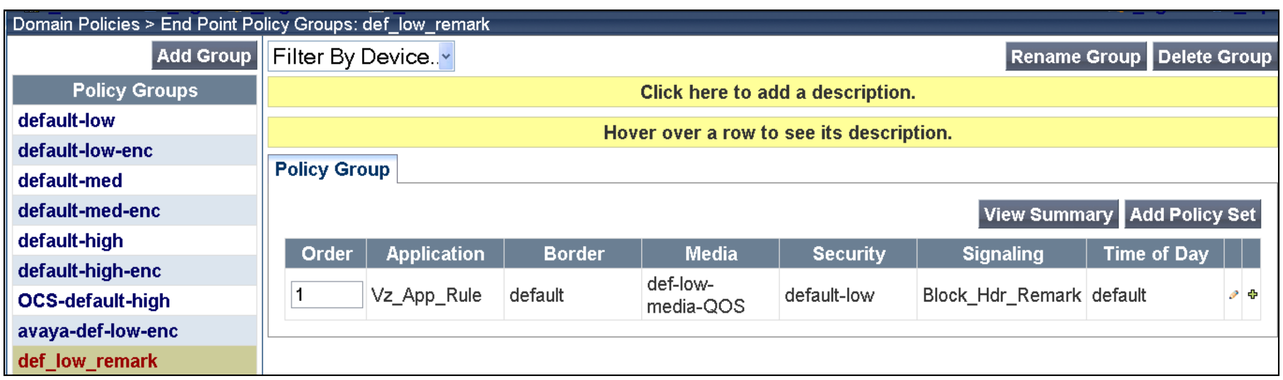


Enter a name in the **Group Name** field, such as "**def_low_remark**" as shown below. Click **Next**.

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

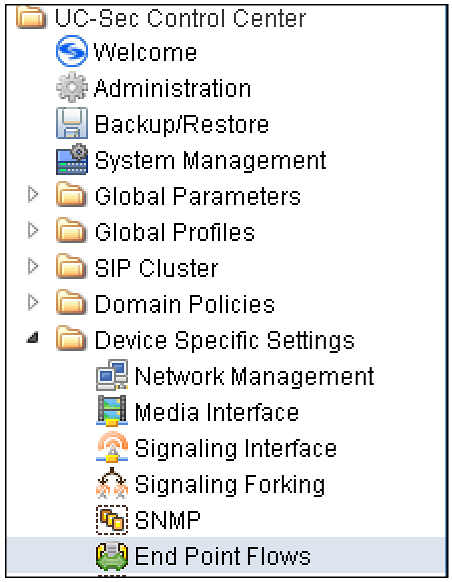


Once configuration is completed, the "**def_low_remark**" policy group will appear as follows.

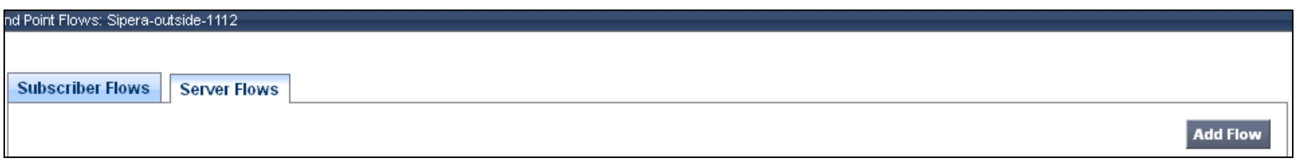


7.8. Device Specific Settings – End Point Flows

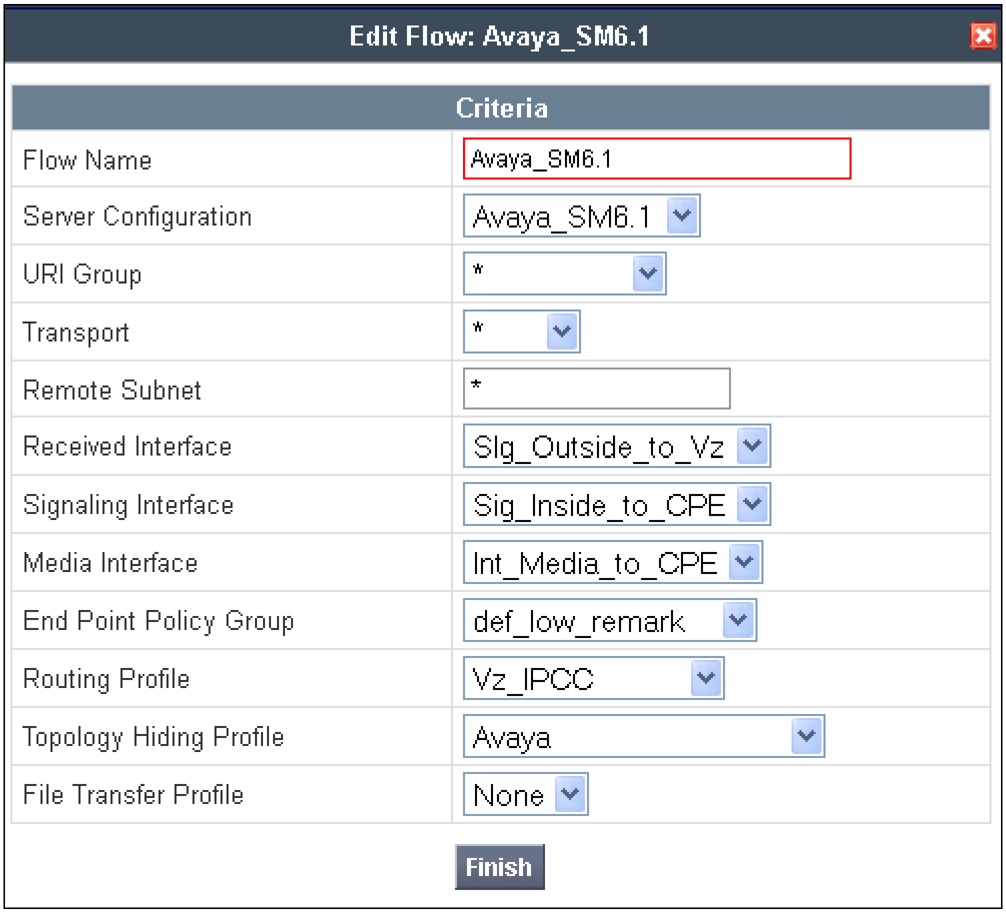
Select **Device Specific Setting → End Point Flows** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named "**Vz_1**" in the sample configuration (not shown). Select the **Server Flows** tab. Select **Add Flow**.

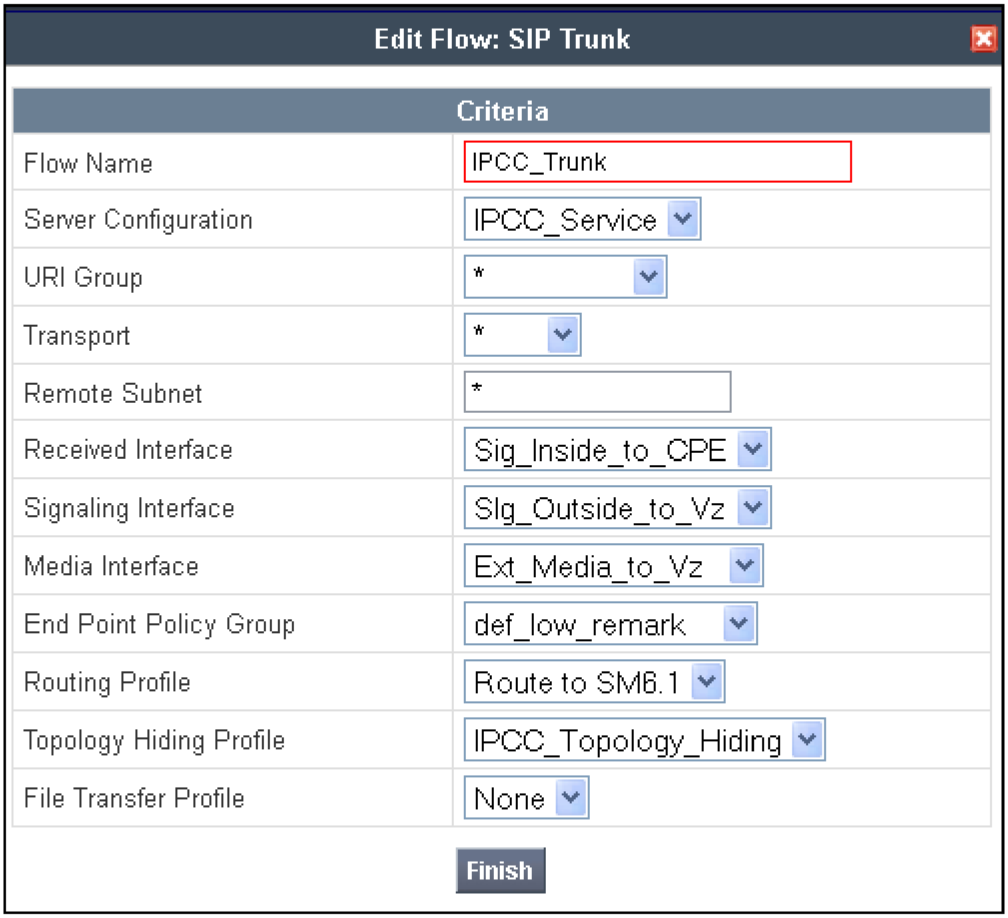


The following screen shows the flow named “**Avaya_SM6.1**” being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections and uses defaults for **URI Group**, **Tranport** and **Remote Subnet**.. Click **Finish**.

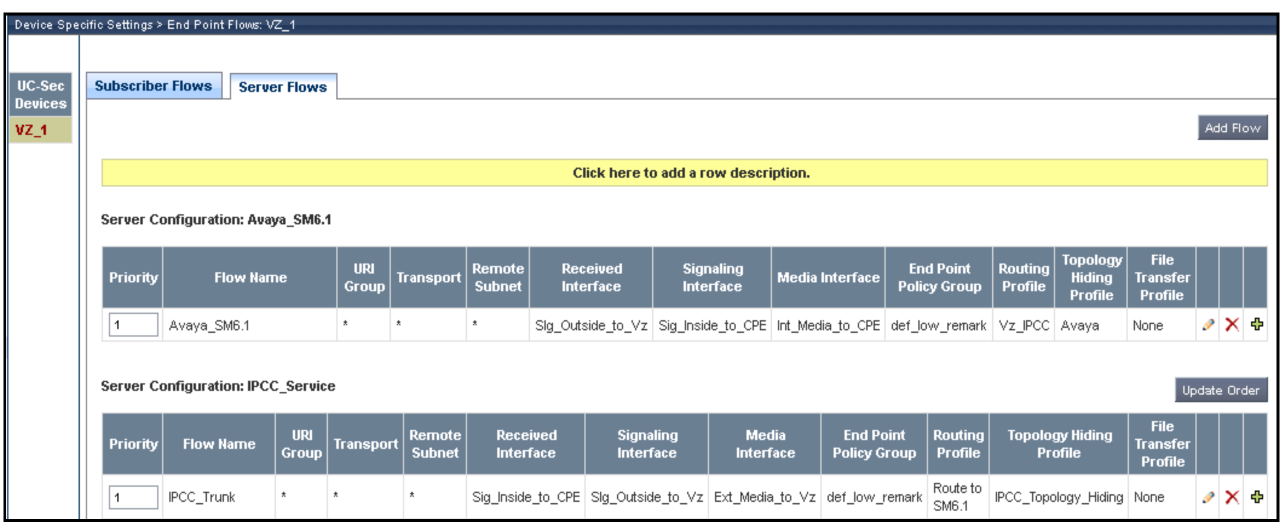


Once again, select the **Server Flows** tab. Select **Add Flow**.

The following screen shows the flow named "**IPCC_Trunk**" being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.



The following screen summarizes the Server Flows configured in the sample configuration.



8. Verizon Business IPCC Service Offer Configuration

Information regarding Verizon Business IPCC service offer can be found at http://www.verizonbusiness.com/us/Products/communications/contact-center/inbound-transport/ 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 IPCC 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 inbound toll-free numbers that could be called from the PSTN. These Verizon-provided toll-free numbers terminated to the Avaya CS1000E location via the Verizon IPCC Service. **Table 1** in **Section 3** shows example Verizon toll-free numbers and the configurable association of the Verizon toll-free numbers with Avaya CS1000E users.

9. Verification Steps

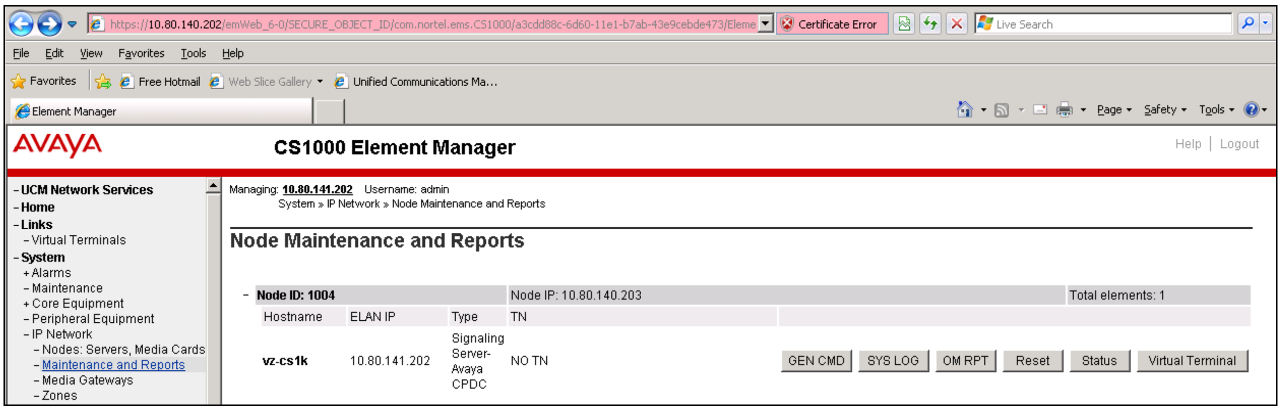
This section provides example verifications of the Avaya configuration with Verizon Business IPCC service.

9.1. Avaya Communication Server 1000E Verifications

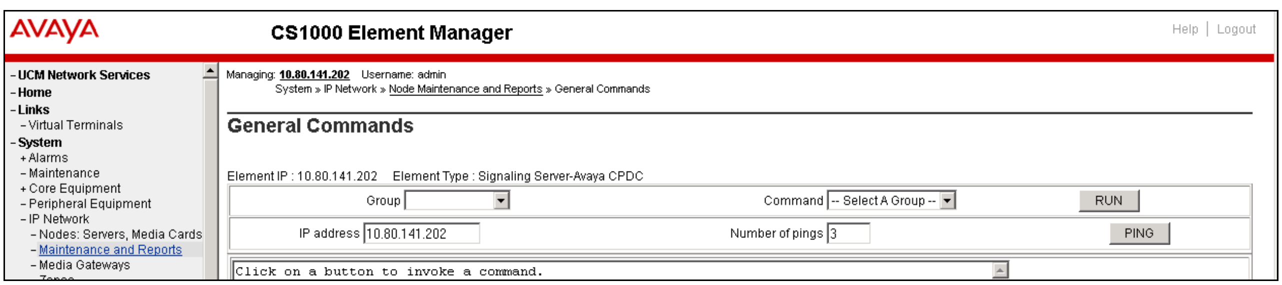
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

9.1.1 IP Network Maintenance and Reports Commands

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

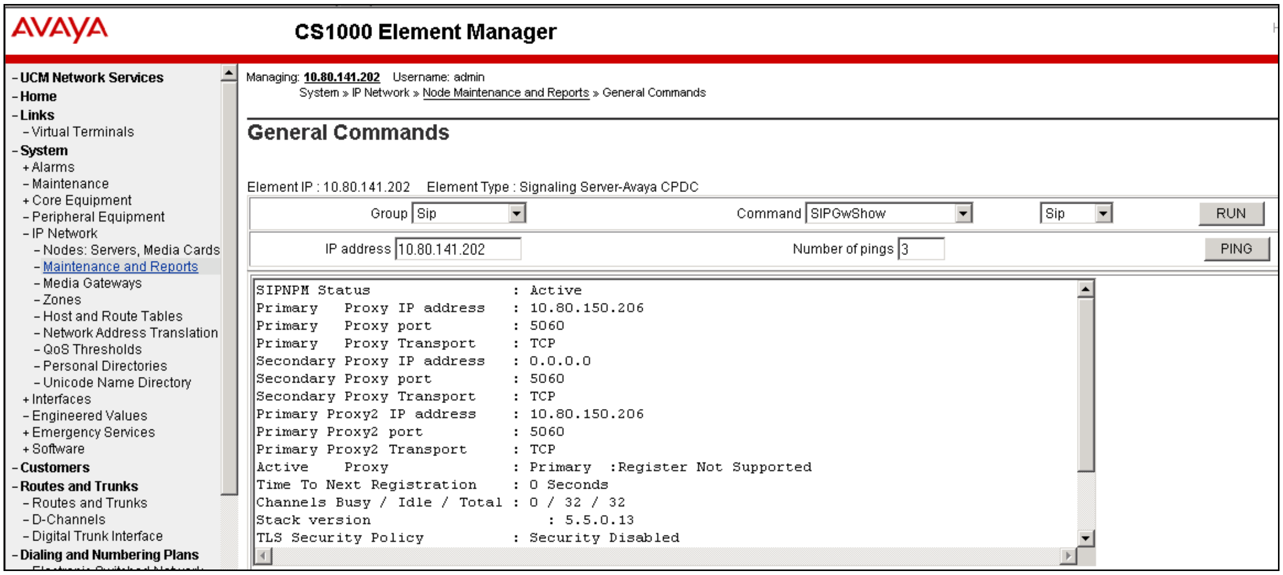


The **General Commands** page is displayed as shown below.

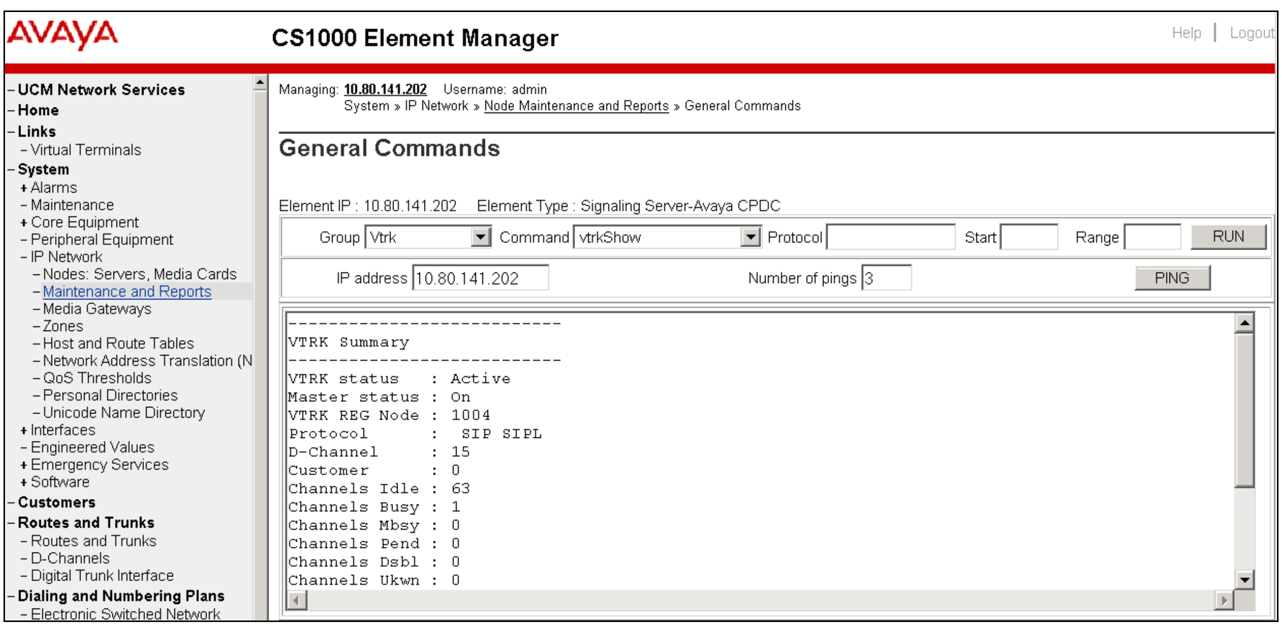


A variety of commands are available by selecting an appropriate **Group** and **Command** from the drop-down menus, and selecting **Run**.

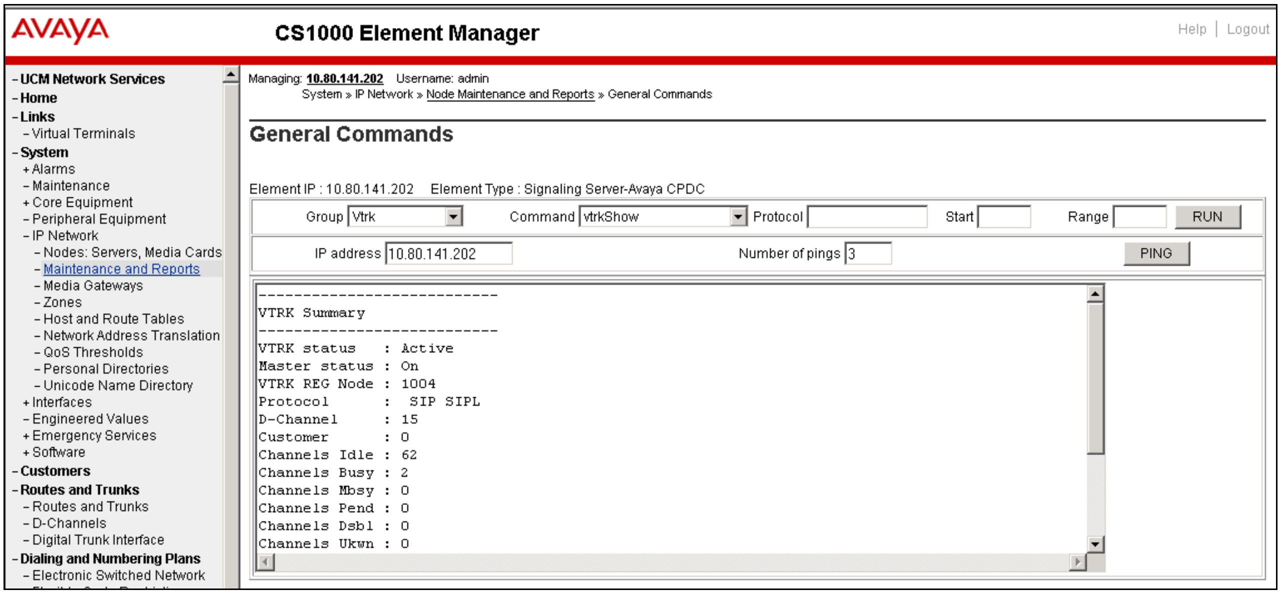
To check the status of the SIP Gateway to Session Manager in the sample configuration, select "**Sip**" from the **Group** menu and "**SIPGwShow**" from the **Command** menu. Click **Run**. The example output below shows that the Session Manager (10.80.150.206, port 5060, TCP) has **SIPNPM Status** "**Active**".



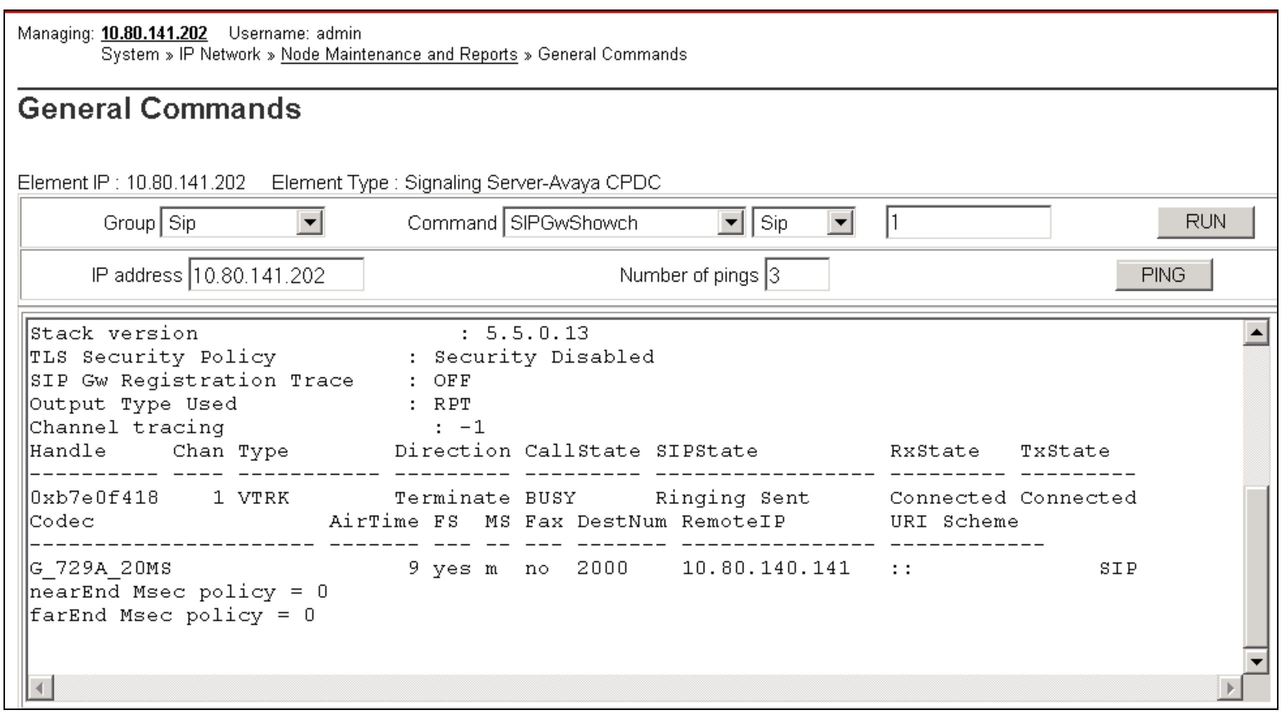
As another example, the following screen shows the results of the "**vtrkShow**" **Command** from the "**Vtrk**" **Group**. The command was run with an active incoming call from the Verizon IPCC to an IP/Unistim telephone. Therefore, one channel is busy, and 63 idle.



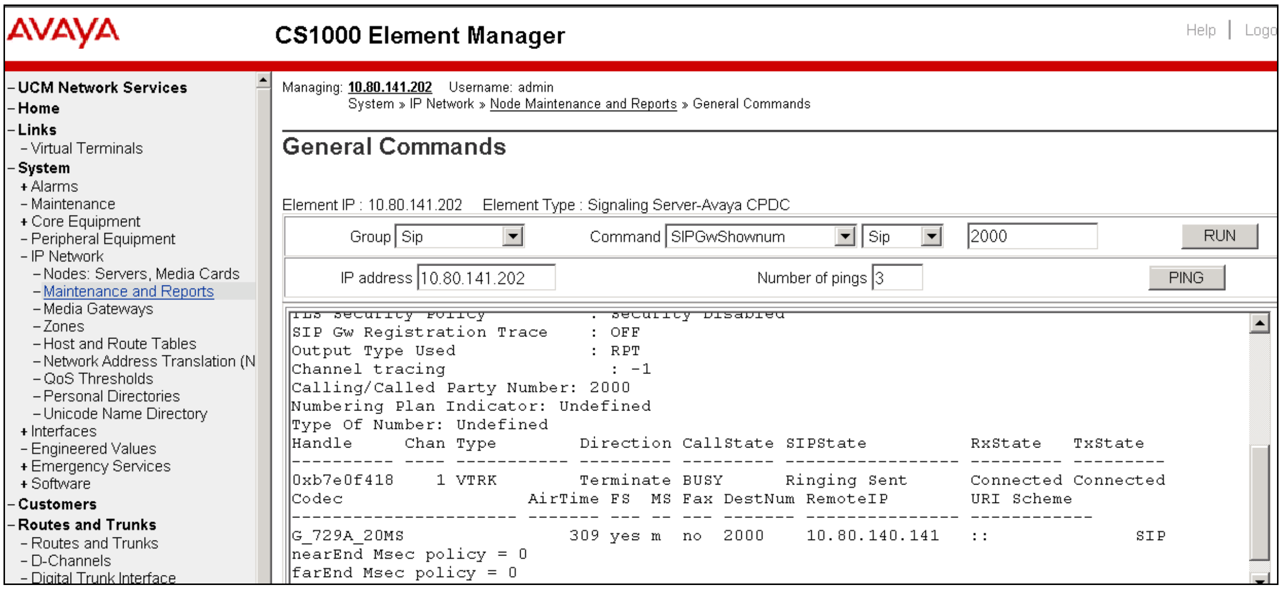
Below is the same call placed to a SIP extension. Notice that that the Channels Busy is now 2 instead of 1.



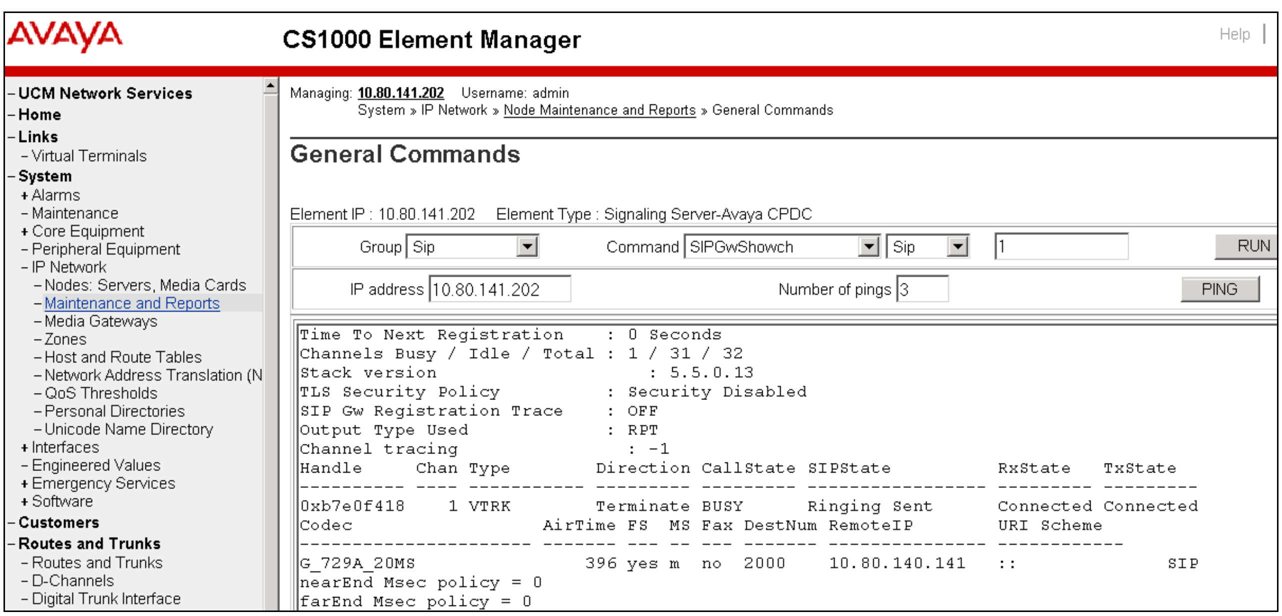
The next screen capture shows the output of the **Command** "**SIPGWShowch**" in **Group** "**Sip**" for channel 1, while an incoming call was active (using channel 1) from the Verizon IPCC Service to an IP-UNIStim phone. In the output below, the scroll bar was used to scroll down to the area showing that the codec in use was "G_729A_20MS". Note that the Remote IP (10.80.140.141) is the IP Address of the inside private interface of ASBCE.



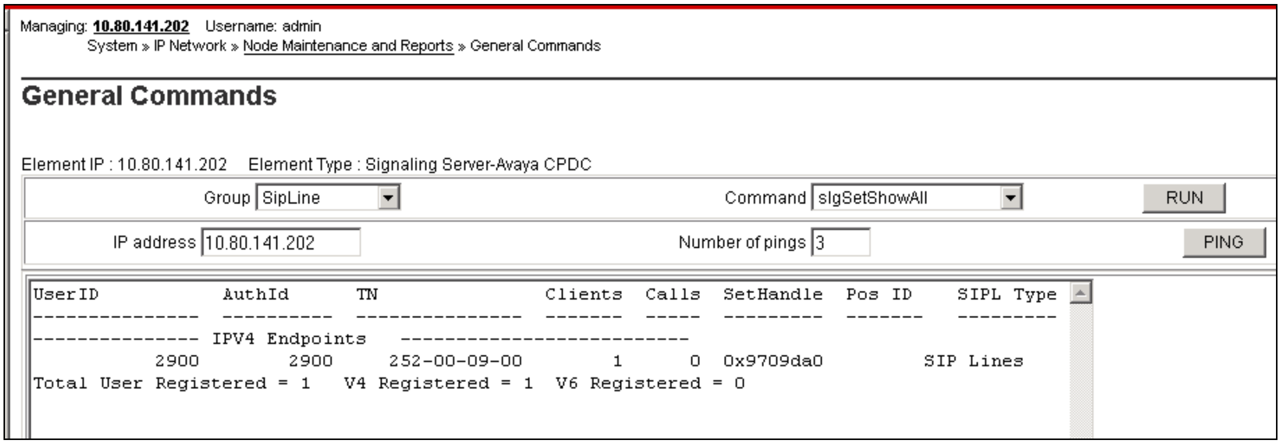
The next screen capture shows an alternate way to view similar information, but in this case, by searching for calls involving a specific directory number. The screen shows the output of the **Command** "**SIPGWShownum**" in **Group** "**Sip**" where DN 2000 was specified. An incoming call was active from the Verizon IPCC Service to the IP-UNIStim phone with DN 2000. In the output below, the scroll bar was used to scroll down to the area showing that the codec in use was "G_729A_20MS". Note that the Remote IP (10.80.140.141) is the IP Address of the inside private interface of the ASBCE.



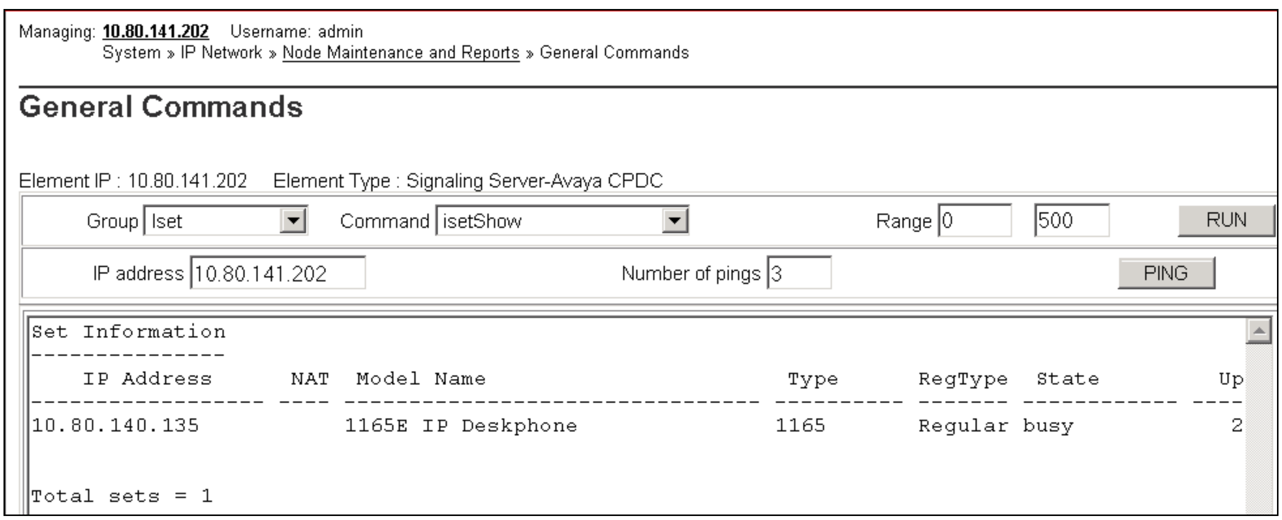
The following screen shows the output of the **Command** "**SIPGWShowch**" in **Group** "**Sip**" for channel 1, when an incoming call was active (using channel 1) to an IP UNIStim telephone via the Verizon IPCC Service. Again, the use of G.729A to the inside IP Address (10.80.140.141) of the SBC can be observed.



The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command** "**slgSetShowAll**" in **Group** "**SipLine**". At the time this screen was captured, the SIP telephone with DN 2900 was involved in an active call with the Verizon IPCC service.

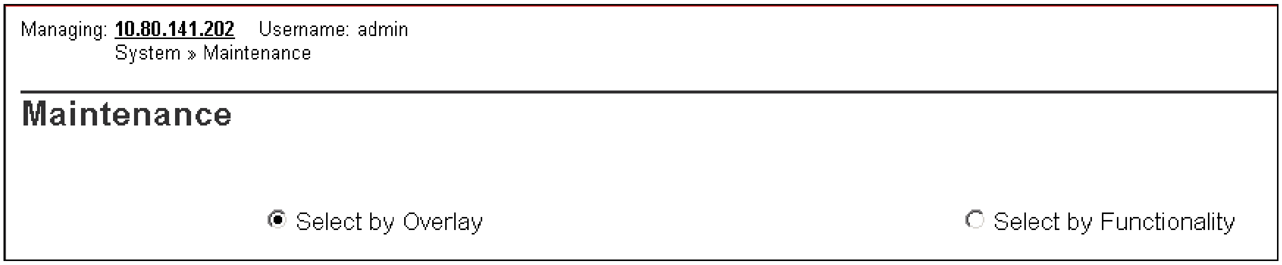


The following screen shows a means to view IP UNIStim telephones. The screen shows the output of the **Command** "**isetShow**" in **Group** "**Iset**". At the time this screen was captured, the "1165E IP Deskphone" UNIStim telephone was involved in an active call with the Verizon IPCC service.

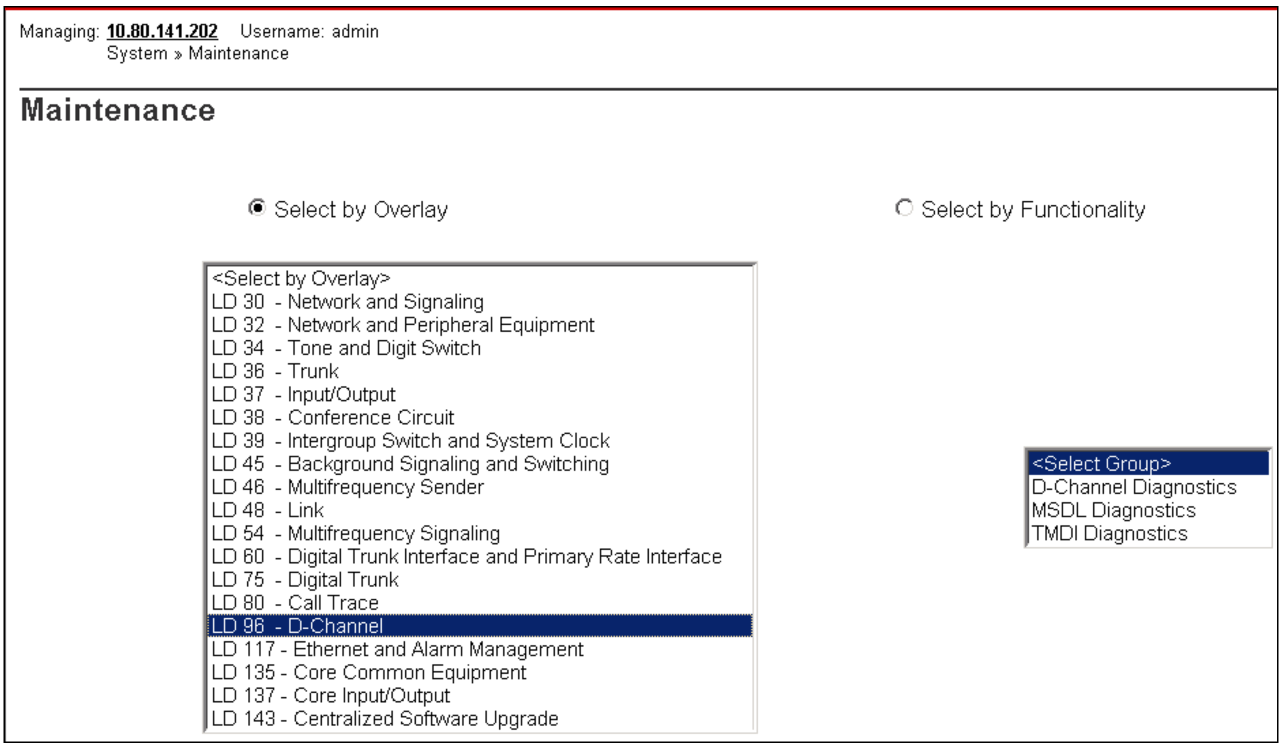


9.1.2 System Maintenance Commands

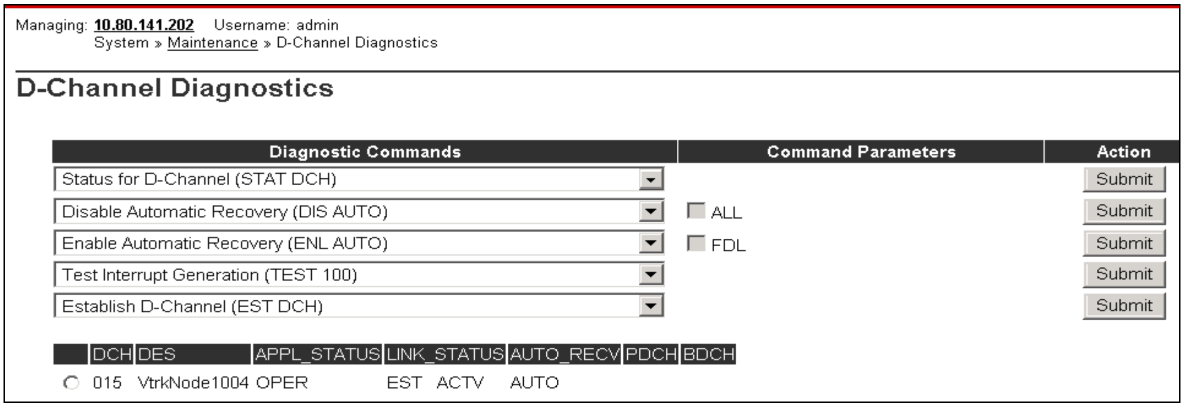
A variety of system maintenance commands are available by navigating to **System → Maintenance** using Element Manager. The user can navigate the maintenance commands using either the "**Select by Overlay**" approach or the "**Select by Functionality**" approach.



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**".



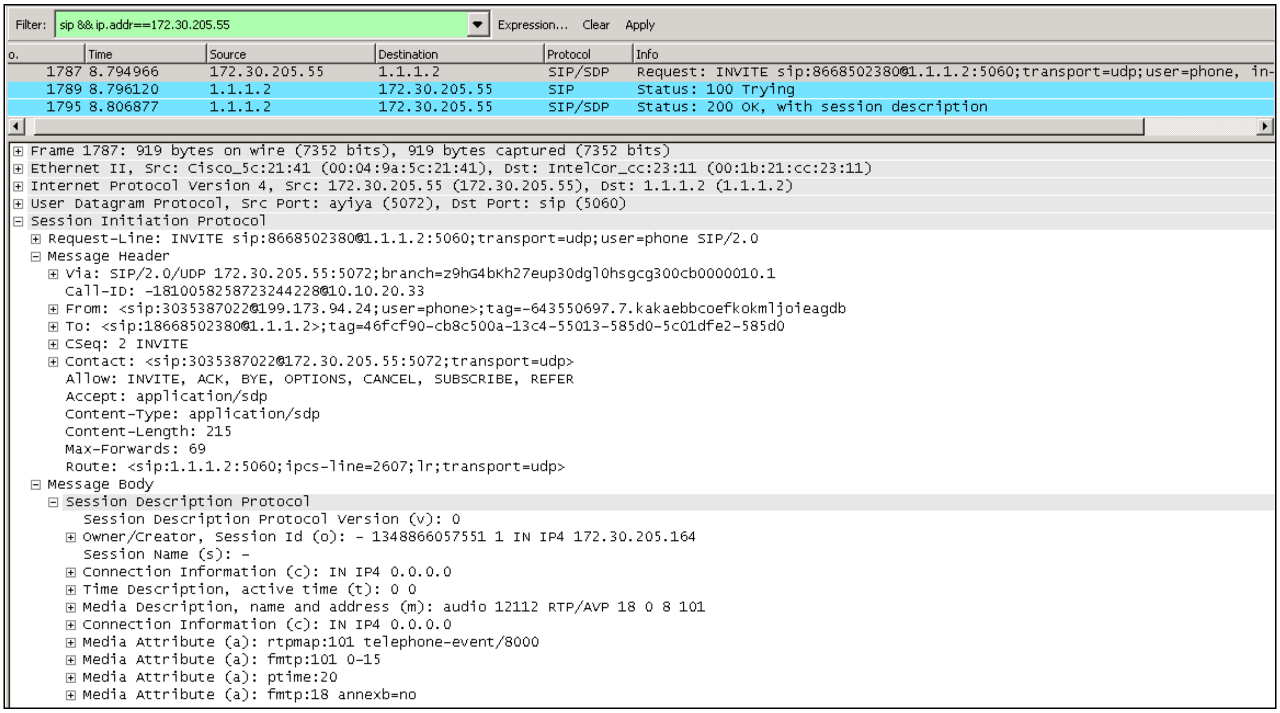
9.2. Wireshark Verifications

This section illustrates Wireshark traces for sample outbound and inbound calls using the sample configuration.

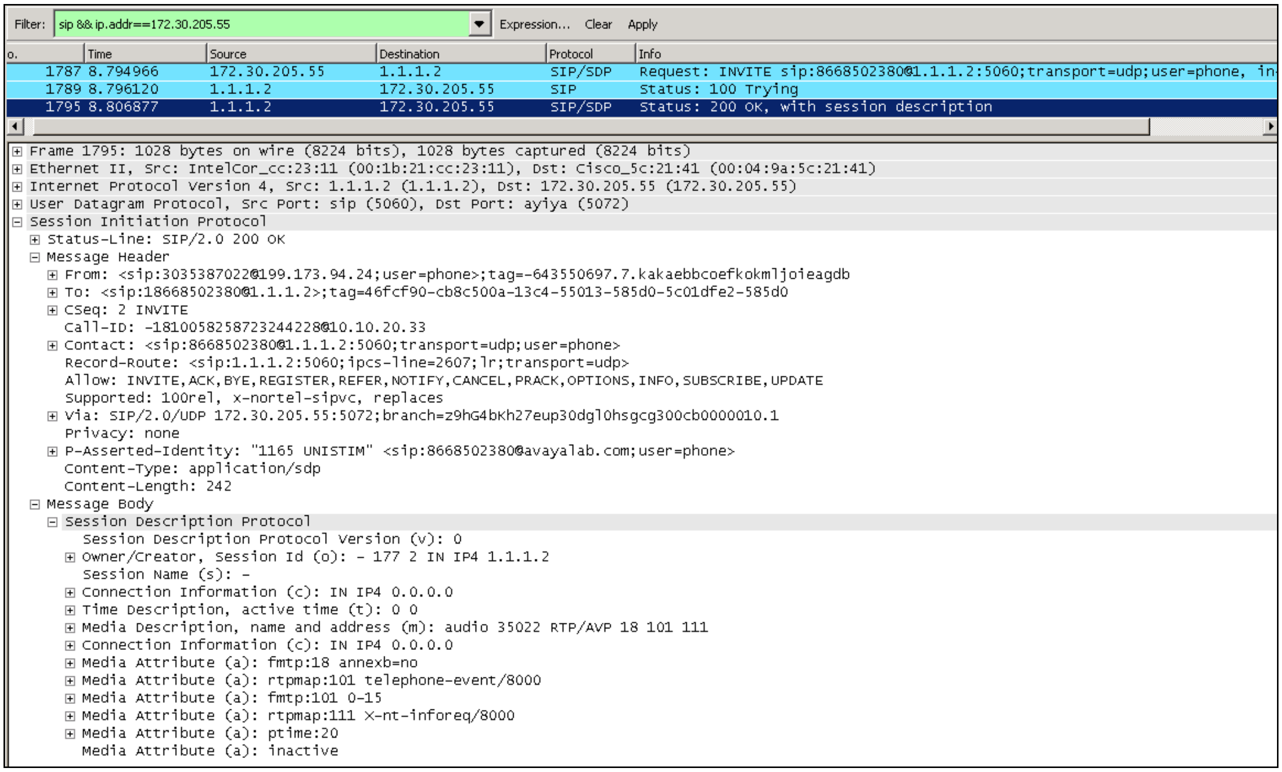
9.2.1 Example Inbound Call

This section illustrates an inbound call from PSTN telephone 303-538-7022 to Verizon IPCC toll free 866-851-2649.

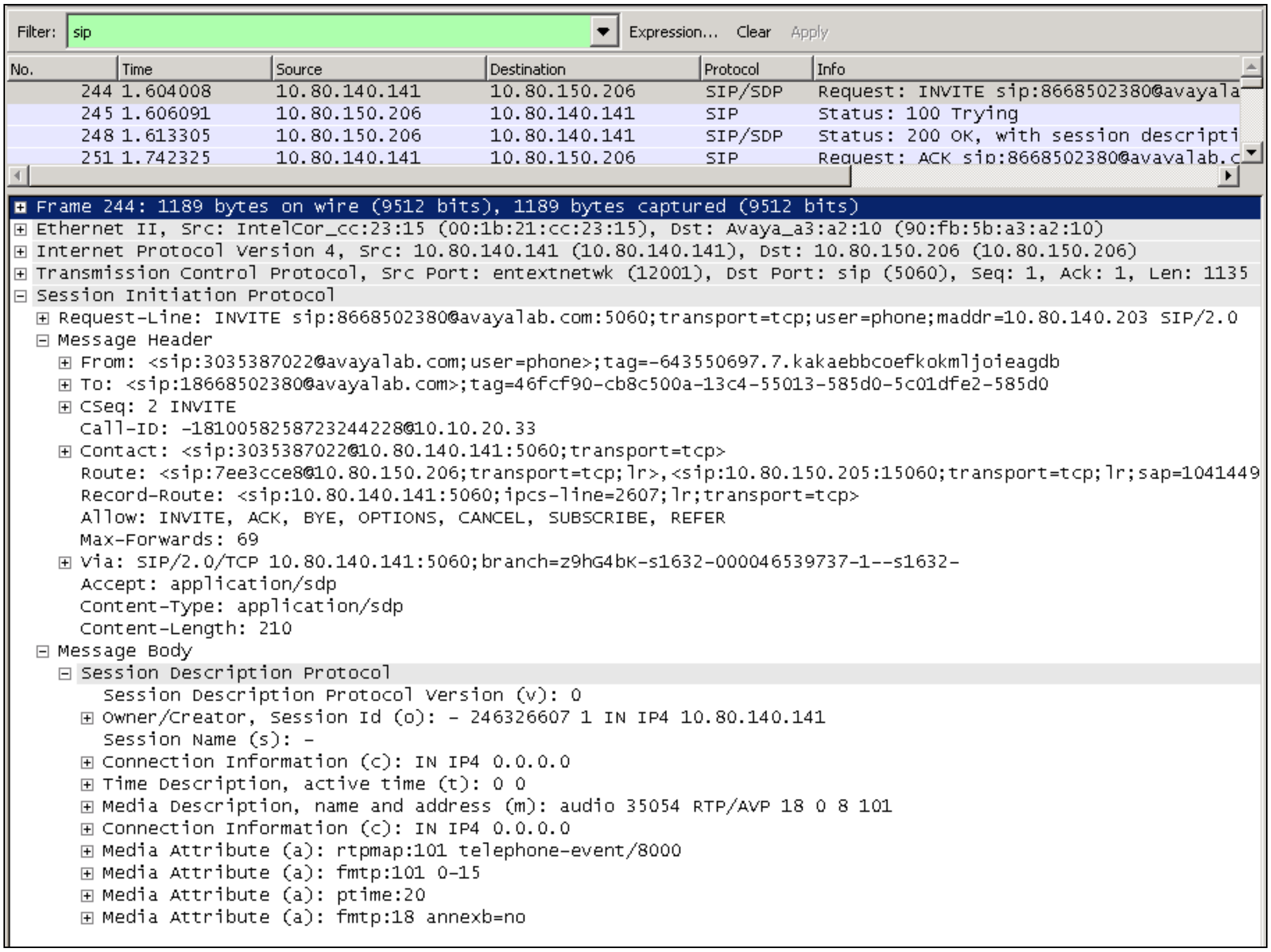
The following screen shows a Wireshark trace filtered on SIP messages to and from the Verizon IP Address and taken from the outside of the ASBCE. The INVITE from Verizon in frame "**1787**" is selected and expanded to illustrate the contents of the message header and message body. Note that Verizon sends the calling party number 3035387022 in the From header, and does not include a PAI header. The Request-URI and To header both contain the dialed Verizon DID 8668502380. In the message body, note that the Verizon SDP offer lists G.729A (18) and G.711MU (0) and G.711A (8). In frame 24, a 180 Ringing (without SDP) response is sent to Verizon.



The following screen shows the 200 OK in frame 1795 expanded to show the contents of the SDP answer containing G.729A returned to Verizon. The use of the value 101 for any transmission of DTMF telephone events via RFC 2833 can also be observed.



The following screen capture shows a Wireshark trace filtered on SIP messages. The INVITE message from the ASBCE is selected and the message header is expanded for visibility. The message headers in the Request-URI, To and From now contain avayalab.com, the internal shared lab domain. Session Manager will adapt 866-850-2380 such that the call rings the IP UNIStim telephone with Directory Number 2000, an IP UNIStim telephone.



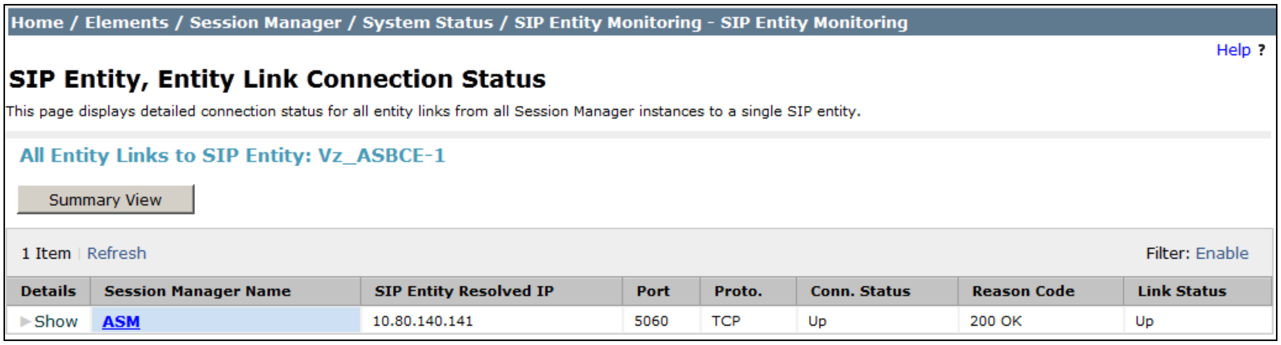
9.3. System Manager and Session Manager Verification

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

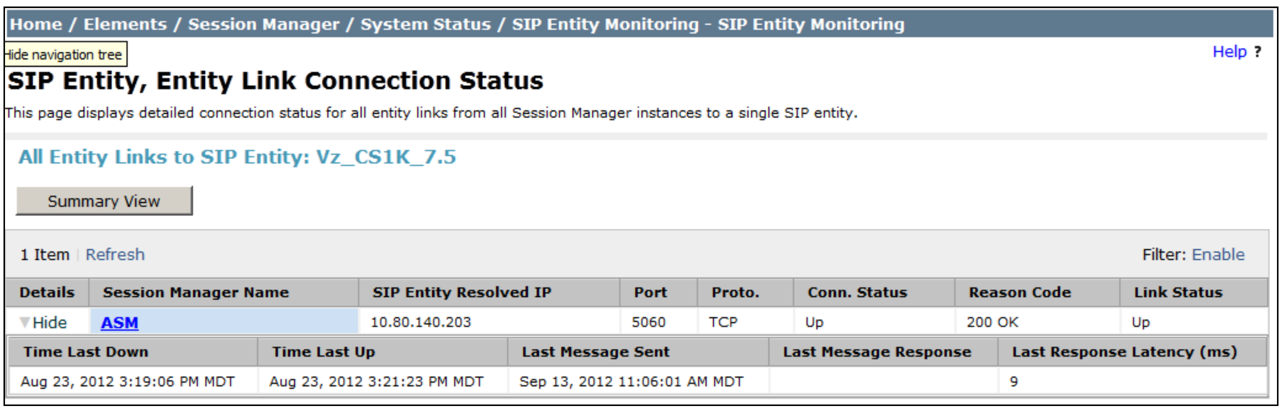
9.3.1 Verify SIP Entity Link Status

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.



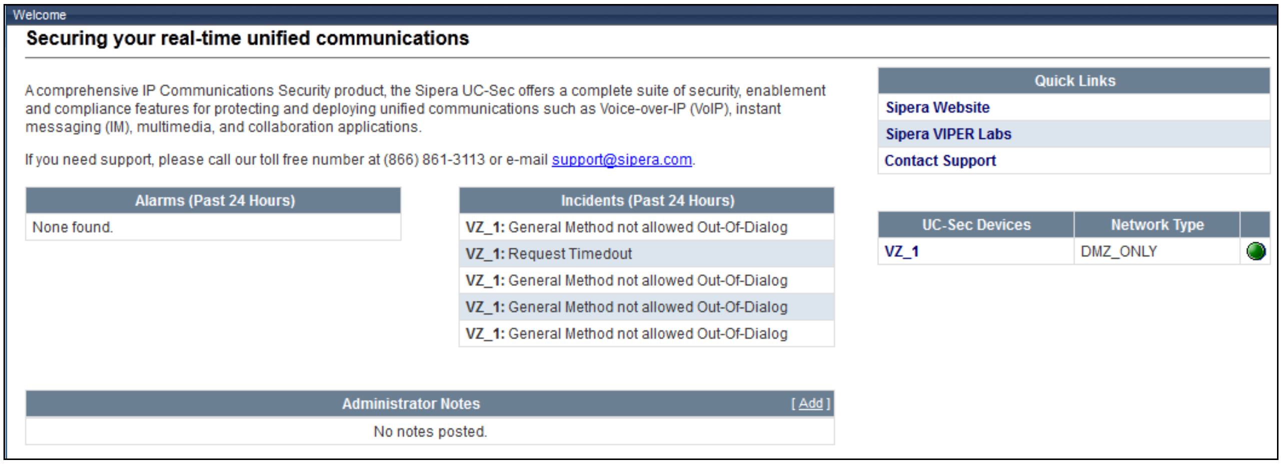
Return to the list of monitored entities, and select another entity of interest, such as "**Vz_CS1K_7.5**". Under normal operating conditions, the **Link Status** should be "**Up**" as shown in the example screen below. In this case, "**Show**" under **Details** was selected to view additional information.



9.4. Avaya Session Border Controller for Enterprise Verification

9.4.1 Welcome Screen

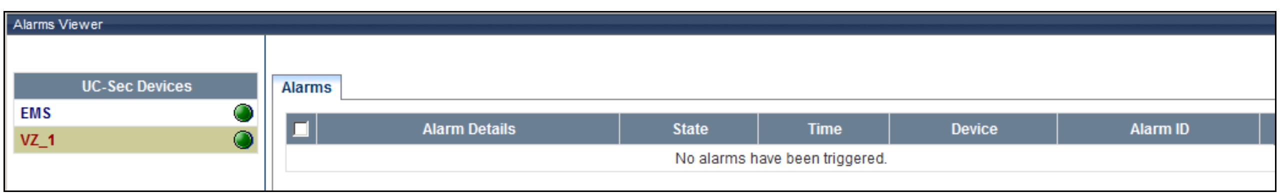
The welcome screen shows alarms, incidents, and the status of all managed ASBCEs at a glance.



9.4.2 Alarms

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

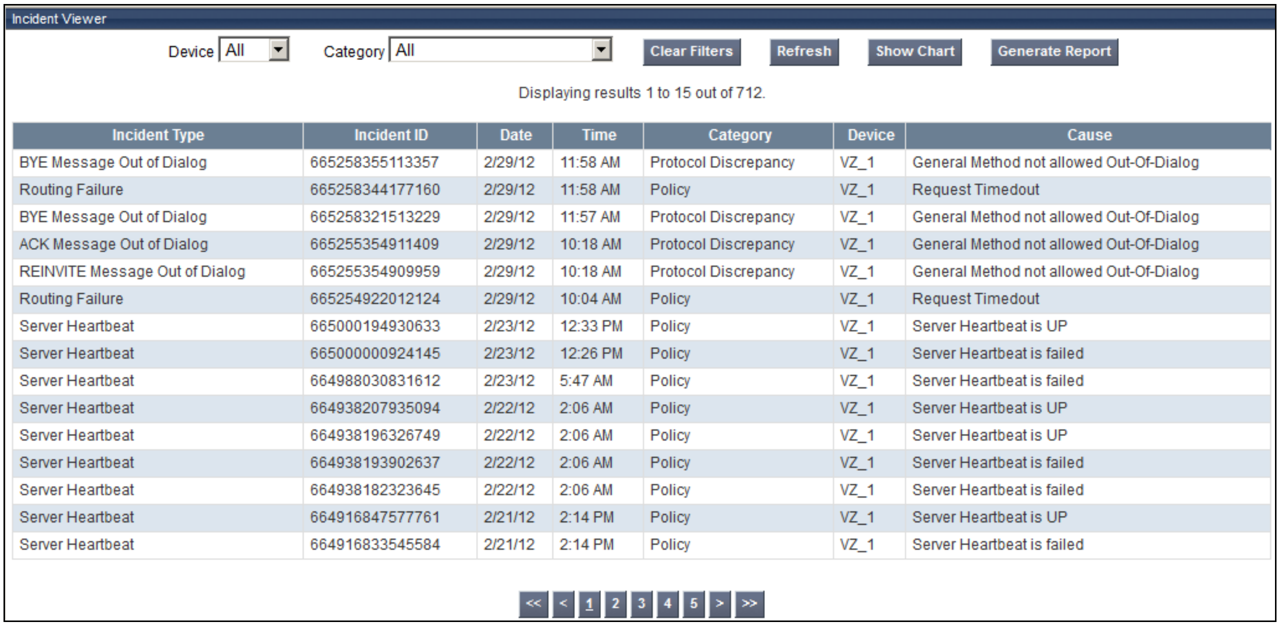
Alarms Viewer:



9.4.3 **Incidents**

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

Incidents Viewer:


Incident Viewer

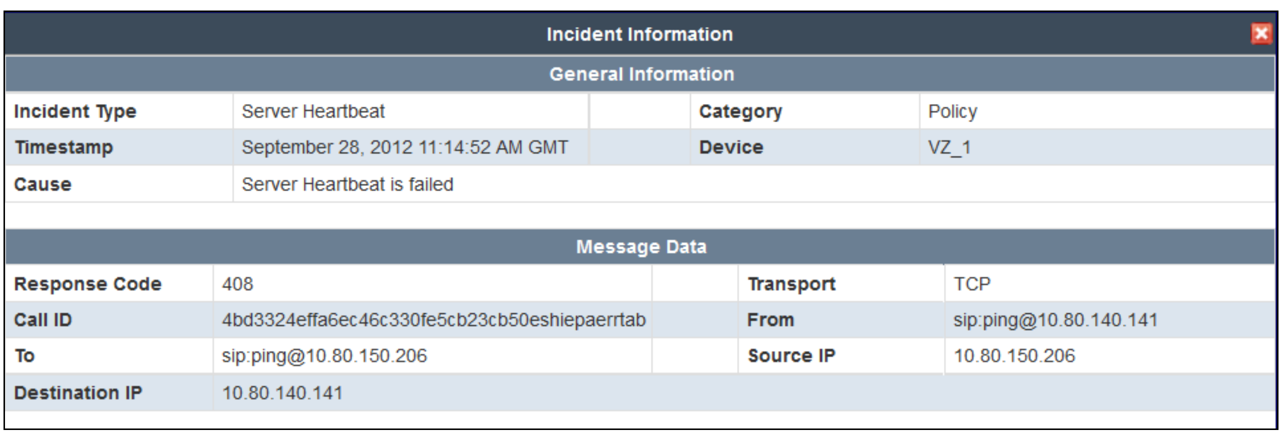
Device All Category All Clear Filters Refresh Show Chart Generate Report

Displaying results 1 to 15 out of 712.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
BYE Message Out of Dialog	665258355113357	2/29/12	11:58 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
Routing Failure	665258344177160	2/29/12	11:58 AM	Policy	VZ_1	Request Timedout
BYE Message Out of Dialog	665258321513229	2/29/12	11:57 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
ACK Message Out of Dialog	665255354911409	2/29/12	10:18 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
REINVITE Message Out of Dialog	665255354909959	2/29/12	10:18 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
Routing Failure	665254922012124	2/29/12	10:04 AM	Policy	VZ_1	Request Timedout
Server Heartbeat	665000194930633	2/23/12	12:33 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	665000000924145	2/23/12	12:26 PM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664988030831612	2/23/12	5:47 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664938207935094	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664938196326749	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664938193902637	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664938182323645	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664916847577761	2/21/12	2:14 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664916833545584	2/21/12	2:14 PM	Policy	VZ_1	Server Heartbeat is failed

<< < 1 2 3 4 5 > >>

Further Information can be obtained by clicking on an incident in the **Incidents** viewer:


Incident Information

General Information

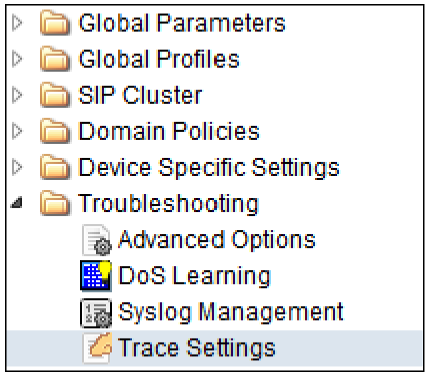
Incident Type	Server Heartbeat	**Category**	Policy
Timestamp	September 28, 2012 11:14:52 AM GMT	**Device**	VZ_1
Cause	Server Heartbeat is failed		

Message Data

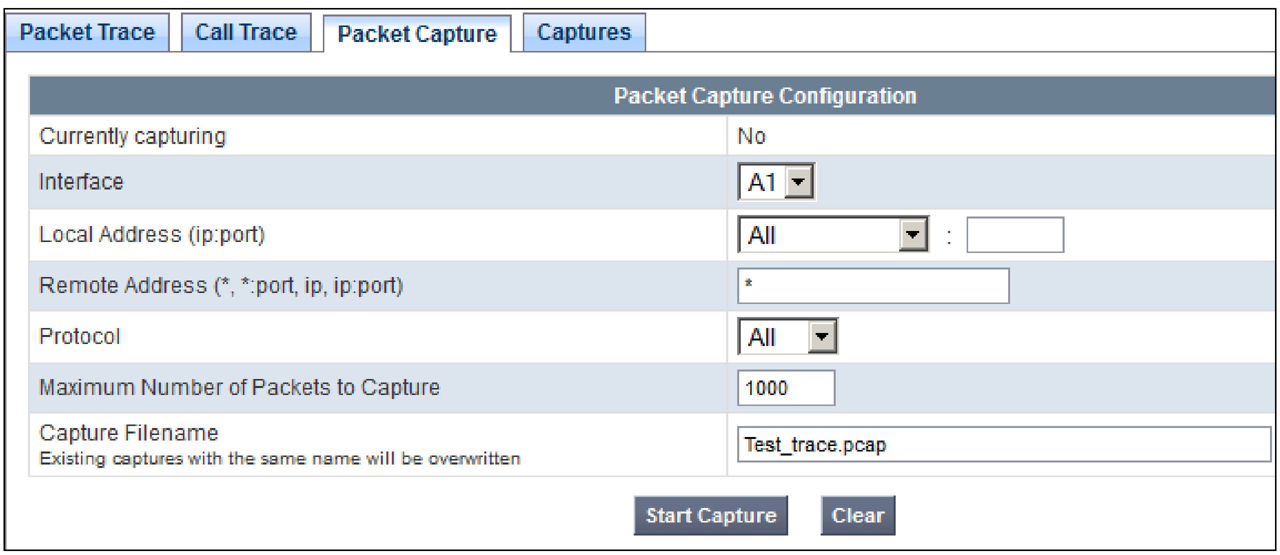
Response Code	408	**Transport**	TCP
Call ID	4bd3324effa6ec46c330fe5cb23cb50eshiepaerrtab	**From**	sip:ping@10.80.140.141
To	sip:ping@10.80.150.206	**Source IP**	10.80.150.206
Destination IP	10.80.140.141		

9.4.4 Tracing

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

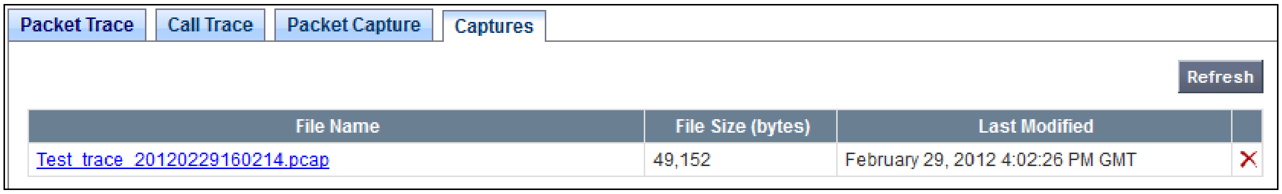


Select the **Packet Capture** tab and set the desired configuration for a call trace, then press **Start Capture**. Only one interface can be selected at once, so only an inside or only an outside trace is possible.



When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, press the **Stop Capture** button at the bottom (not shown).

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



10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise Release 4.0.5 can be configured to interoperate successfully with Verizon Business IPCC service.

Avaya Communication Server 1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon Labs independent certification.

11. Additional References

This section references documentation relevant to these Applications.

11.1. Avaya

Avaya product documentation, including the following, is available at http://support.avaya.com

[1] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Issue 4, Feb 2011 available at http://support.avaya.com/css/P8/documents/100082630

[2] *Installing and Configuring Avaya Aura™ Session Manager,* Doc ID 03-603473 Issue 2.2, April 2011 available at https://downloads.avaya.com/css/P8/documents/100120934

[3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager,* Doc ID 03-603325, Issue 4.2, November 2011 available at https://downloads.avaya.com/css/P8/documents/100120937

[4] *Administering Avaya Aura™ System Manager*, Document Number 03-603324, November 2010 available at https://downloads.avaya.com/css/P8/documents/100120857

Avaya Communication Server 1000E

[1] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, Issue 05.09

[2] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116, Issue 05.17

[3] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.10

[4] Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509, Issue 03.05

[5] Signaling Server and IP Line Applications Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, Issue 03.12

Appendix 1: Sigma Script

```
within session "ALL"
{
 act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
  {
// Topology Hiding of P-Location header for subsequent re-INVITEs

   remove(%HEADERS["Endpoint-View"][1]);
   remove(%HEADERS["Alert-Info"][1]);
   remove(%HEADERS["User-Agent"][1]);
   remove(%HEADERS["Server"][1]);
   remove(%HEADERS["P-Location"][1]);

   }
 }
```

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