**Avaya Solution & Interoperability Test Lab**

# Application Notes for SIP Trunking Using Verizon Business IP Trunking Service with Avaya IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1 – Issue 1.0

## Abstract


These Application Notes describe a reference configuration using Session Initiation Protocol (SIP) trunking between the Verizon Business IP Trunking service offer and an Avaya IP Office solution. In the reference configuration, the Avaya IP Office solution consists of Avaya IP Office Server Edition Release 11.1, Avaya Session Border Controller for Enterprise Release 8.1 and Avaya SIP, H.323, digital, and analog endpoints.

These Application Notes complement previously published Application Notes by illustrating the configuration screens and Avaya testing of IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1.

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

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Solution & Interoperability Test Lab, utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

# Table of Contents

# 1. Introduction

These Application Notes describe a reference configuration using Session Initiation Protocol (SIP) trunking between the Verizon Business IP Trunking service offer and an Avaya IP Office solution. In the reference configuration, the Avaya IP Office solution consists of an Avaya IP Office Server Edition Primary Server (Primary server), an IP500 V2 Expansion System and an Avaya Session Border Controller for Enterprise

Avaya IP Office is a versatile communications solution that combines the reliability and ease of a traditional telephony system with the applications and advantages of an IP telephony solution. This converged communications solution can help businesses reduce costs, increase productivity, and improve customer service.

The Avaya Session Border Controller for Enterprise (Avaya SBCE) is the point of connection between Avaya IP Office and the Verizon Business IP Trunking service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling and media for interoperability.

These Application Notes complement previously published Application Notes by illustrating the configuration screens and Avaya testing of IP Office Release 11.1 and Avaya Session Border Controller for Enterprise Release 8.1.

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

For more information on the Verizon Business IP Trunking service, including access alternatives, visit https://enterprise.verizon.com/products/business-communications/voip-and-voice-services/voip-ip-trunking/

# 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Verizon Business IP Trunking service, as depicted in **Figure 1**. The Avaya SBCE and IP Office server were configured to use the commercially available SIP Trunking solution provided by the Verizon Business IP Trunking service. This allowed Avaya IP Office users to make calls to the PSTN and receive calls from the PSTN via the Verizon Business IP Trunking service.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

## 2.1. Interoperability Compliance Testing

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

- Incoming calls from the PSTN were routed to the DID numbers assigned by Verizon Business to the Avaya IP Office location. These incoming PSTN calls arrived via the SIP Line and were answered by Avaya SIP telephones, Avaya H.323 telephones, Avaya digital telephones, analog telephones, analog fax machines, Avaya IX™ Workplace for Windows softphones and Avaya Voicemail Pro. The display of caller ID on display-equipped Avaya IP Office telephones was verified.
- Incoming calls answered by members of Hunt Groups were verified.
- Outgoing calls from the Avaya IP Office location to the PSTN were routed via the SIP Line to Verizon Business. These outgoing PSTN calls were originated from Avaya SIP telephones, Avaya H.323 telephones, Avaya digital telephones, analog endpoints and Avaya IX™ Workplace for Windows softphones. The display of caller ID on display-equipped PSTN telephones was verified.
- Inbound / Outbound fax using G.711 and T.38 were verified.
- Proper disconnect when the caller abandoned a call before answer for both inbound and outbound calls.
- Proper disconnect when the IP Office party or the PSTN party terminated an active call.
- Proper SIP signaling and busy tone heard when an IP Office user called a busy PSTN user, or a PSTN user called a busy IP Office user (i.e., if no redirection was configured for user busy conditions).
- Various outbound PSTN call types were tested including long distance, international, toll-free, operator assisted, and directory assistance calls.
- Requests for privacy (i.e., caller anonymity) for IP Office outbound calls to the PSTN were verified. That is, when privacy is requested by IP Office, outbound PSTN calls were successfully completed while withholding the caller ID from the displays of display-equipped PSTN telephones.
- Privacy requests for inbound calls from the PSTN to IP Office users were verified. That is, when privacy is requested by a PSTN caller, the inbound PSTN call was successfully completed to an IP Office user while presenting an “anonymous” display to the IP Office user.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Both Verizon Business and IP Office were able to monitor SIP trunk health using SIP OPTIONS.

- IP Office outbound calls were placed with simple short codes as well as using ARS. Using ARS, the ability of IP Office to route-advance to an alternate route was exercised when the primary SIP line was not responding. The Line Group associated with the Verizon Business SIP Trunk was the primary line group chosen for a call, or an alternate line group was selected upon failure of a primary line.
- Incoming and outgoing calls using the G.729A and G.711MU codecs.
- DTMF transmission (RFC 2833) with successful voice mail navigation using G.729A and G.711MU for incoming and outgoing calls. Successful navigation of a simple auto-attendant application configured on Avaya Voicemail Pro.
- Inbound and outbound long holding time call stability.
- Telephony features such as call waiting, hold, transfer, and conference.
- Attended call transfer using the SIP REFER method.
- Unattended or "blind" call transfer using the SIP REFER method.
- Inbound calls from Verizon IP Trunk service that were call forwarded back to PSTN destinations, presenting true calling party information to the PSTN phone, via Verizon IP Trunk service.
- Mobile twinning to a mobile phone, presenting true calling party information to the mobile phone. Mobility Features such as Outbound and Inbound Mobile Call Control. were also verified successfully.
- DiffServ markings in accordance with Verizon's network requirements for Avaya SBCE SIP signaling and RTP media.
- Avaya Remote Worker functionality, using Avaya IX™ Workplace for Windows softphones, registered to the IP Office via the Avaya SBCE.

## 2.2. Test Results

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

- **SIP endpoint transfers:** When Refer based call transfers are performed, Verizon does not send NOTIFY SIP messages to Avaya IP Office to signal transfer completion. Some Avaya SIP endpoints (e.g., Avaya 1140E, and Avaya Equinox for Windows) require receipt of a NOTIFY when Refer based call transfers are performed. Without the NOTIFY messages, these IP Office users may briefly see "Transfer failed" on the display after the final user operation, even if the transfer has actually succeeded. The IP Office SIP Line option, **Emulate NOTIFY for Refer** can be set, to send the necessary NOTIFY messages to these endpoints (see **Section 5.5.6**), avoiding this issue.
- **Emergency 911/E911 Services Limitations and Restrictions –** Although Verizon provides 911/E911 calling capabilities, 911 capabilities were not tested; therefore, it is the customer's responsibility to ensure proper operation with its equipment/software vendor.

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

## 2.3. Support

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

For technical support on Verizon Business IP Trunking service offer, follow the online support links at https://enterprise.verizon.com/.

# 3. Reference Configuration

**Figure 1** illustrates an example Avaya IP Office solution connected to the Verizon Business IP Trunking service. The Avaya equipment is located on a private IP subnet. An enterprise edge router provides access to the Verizon Business IP Trunking service network via a Verizon Business T1 circuit. This circuit is provisioned for the Verizon Business Private IP (PIP) service.

The reference configuration consisted of the following components:

- Avaya IP Office provides the voice communications services for a particular enterprise site. In the reference configuration, Avaya IP Office runs on the Avaya IP Office Server Edition platform. Note that this solution is extensible to deployments using the standalone IP500 V2 platform as well.
- In the sample configuration, the Primary server runs the Avaya IP Office Server Edition Linux software. Avaya Voicemail Pro, running as a service on the Primary Server, provided the voice messaging capabilities in the reference configuration.
- The Expansion System (V2) is used for the support of digital, analog and additional IP stations. It consists of an Avaya IP Office 500 V2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module).
- Avaya endpoints are represented with Avaya 9608 H.323 Deskphones, Avaya J169 SIP Deskphones, Avaya 1140E SIP Deskphones, Avaya 9508 Digital Deskphones, as well as Avaya IX™ Workplace for Windows (SIP) softphones. Fax endpoints are represented by PCs running Ventafax emulation software connected by modem to the IP Office analog ports.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPTF service and the CPE. In the reference configuration, the Avaya SBCE runs on a VMware platform. This solution is extensible to other Avaya Session Border Controller for Enterprise platforms as well.
- In the reference configuration, Avaya SBCE receives traffic from the Verizon Business IP Trunking service on port 5060 and sends traffic to port 5071, using UDP for network transport, as required by the Verizon Business IP Trunking service.
- Verizon Business IP Trunking service provided Direct Inward Dial (DID) numbers. These DID numbers were mapped to IP Office destinations via Incoming Call Routes in the IP Office configuration.
- Verizon Business used the Fully Qualified Domain Name (FQDN) *pcelban0001.avayalincroft.globalipcom.com*.
- The Avaya CPE environment was assigned FQDN *adevc.avaya.globalipcom.com* by Verizon Business.

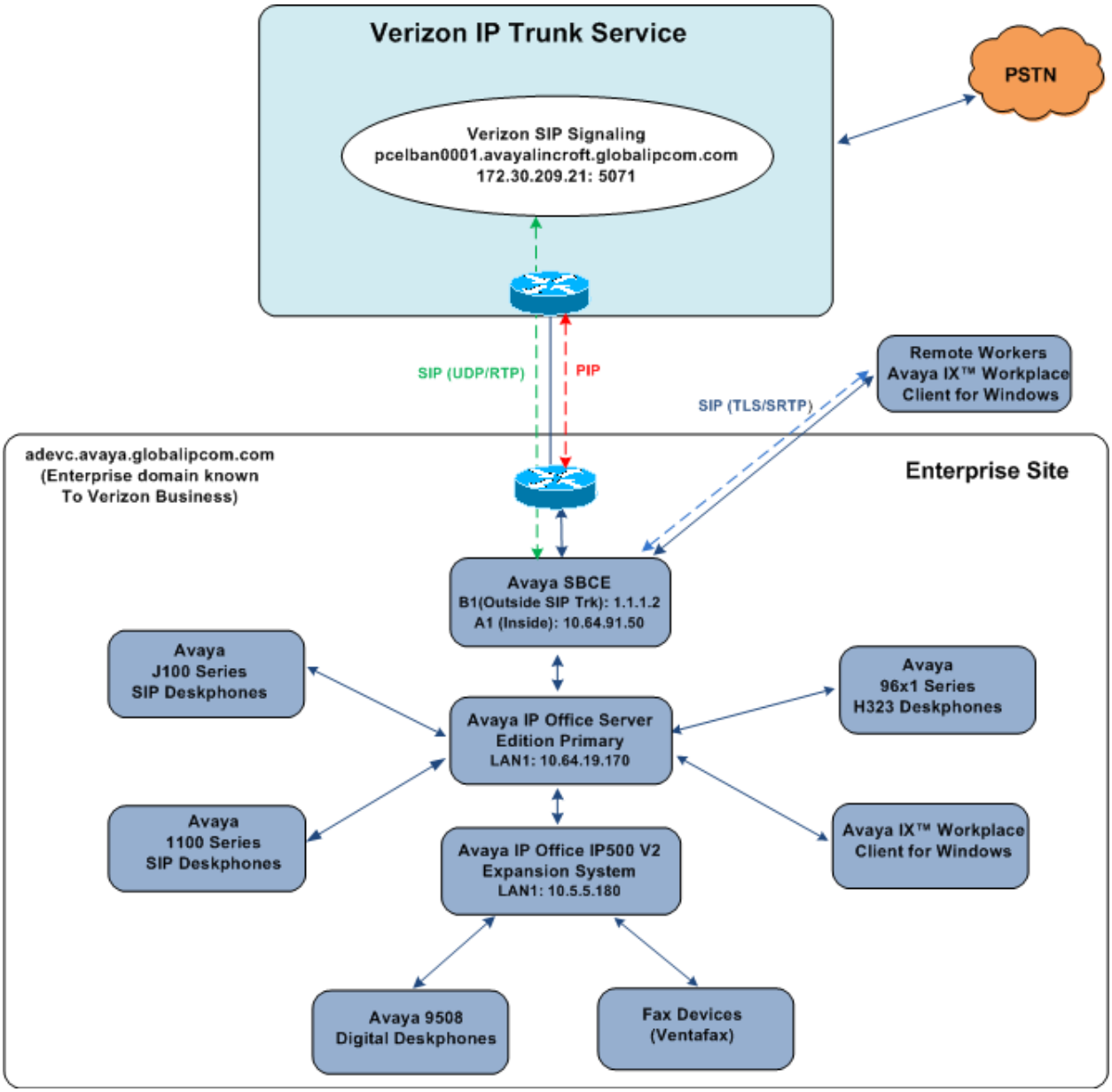



**Figure 1: Avaya Interoperability Test Lab Configuration**

Remote worker endpoints (Avaya IX™ Workplace for Windows) were used in the reference configuration. A remote worker is a SIP endpoint that resides in the untrusted network, registered to IP Office via the Avaya SBCE, using a TLS connection. Remote workers feature the same functionality as any other endpoint within the enterprise. This functionality was successfully tested during the compliance test.

**Note -** The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. For more information on configuring the Avaya SBCE for IP Office remote workers, consult reference **[8]**.

# 4. Equipment and Software Validated

**Table 1** shows the equipment and software used in the reference configuration.

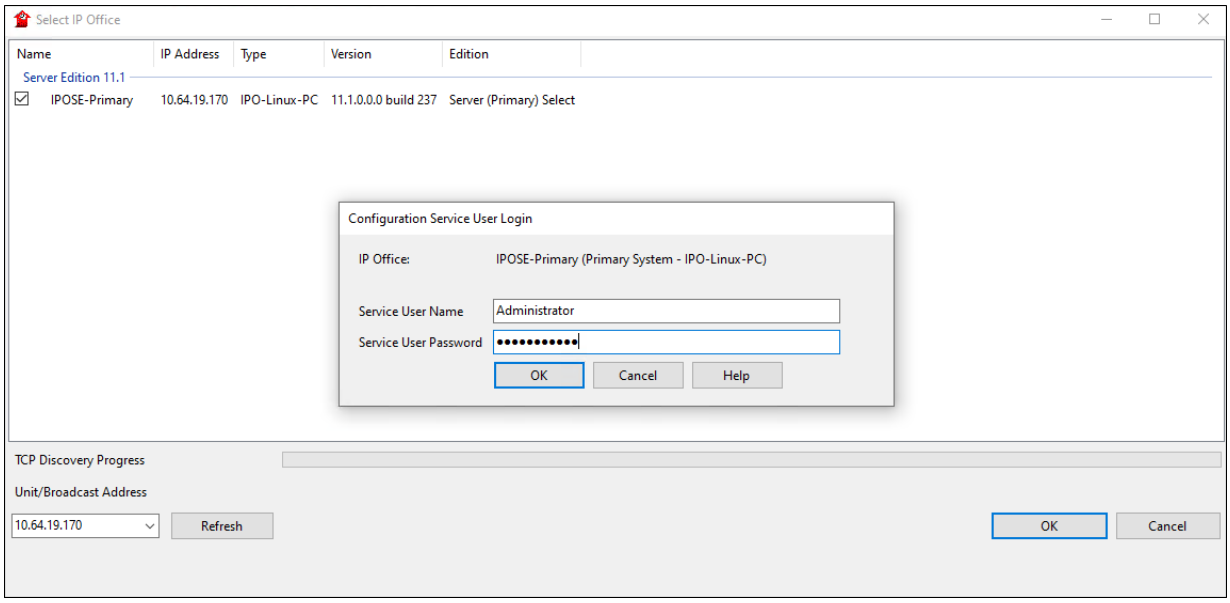
| Avaya IP Telephony Solution Components | |
|---|---|
| **Equipment** | **Software** |
| Avaya IP Office Server Edition<br>- Avaya IP Office Voicemail Pro | Release 11.1.0.0.0 Build 237<br>Release 11.1.0.0.0 Build 234 |
| Avaya IP Office 500 V2 Expansion System | Release 11.1.0.0.0 Build 237 |
| Avaya IP Office Manager | Release 11.1.0.0.0 Build 237 |
| Avaya Session Border Controller for Enterprise | 8.1.0.0.14-18490 |
| Avaya 96x1 Series IP Deskphone (H.323) | Release 6.8304 |
| Avaya 1140E IP Deskphone (SIP) | Release 04.04.23.00 |
| Avaya J169 IP Deskphone (SIP) | Release 4.0.5.0.10 |
| Avaya IX™ Workplace for Windows (SIP) | Release 3.8.5.41.23 |
| Avaya 9508 Digital Deskphone | Release 0.60 |

**Table 1: Equipment and Software Tested**

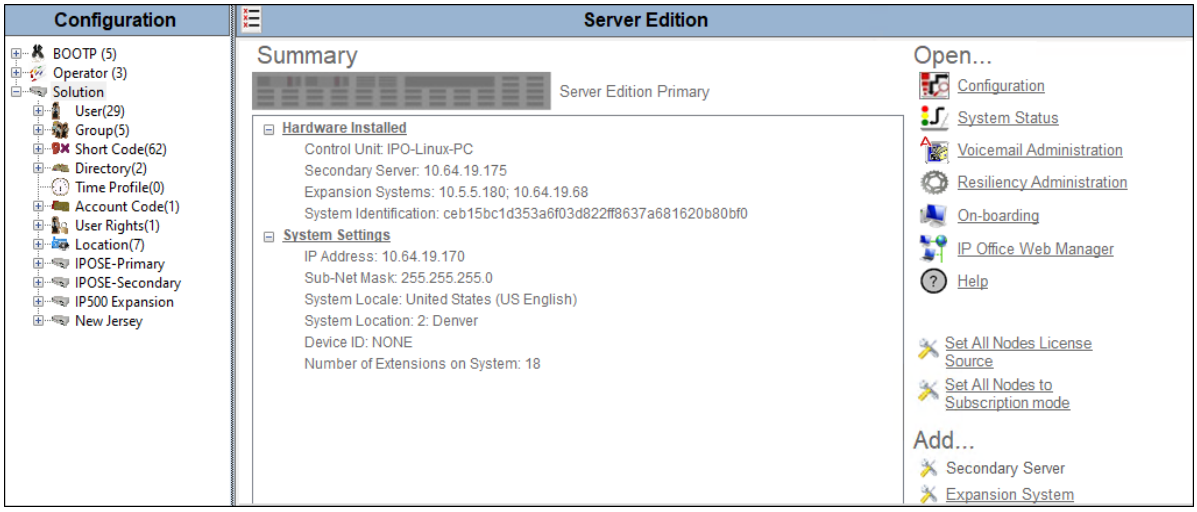
Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2, and also when deployed with all configurations of IP Office Server Edition. Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

# 5. Avaya IP Office Primary Configuration

IP Office is configured via the IP Office Manager program. For more information on IP Office Manager, consult reference **[4]**. From the IP Office Manager PC, select **Start → Programs → IP Office → Manager** to launch the Manager application. Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.




On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the "plus" sign next to the Primary server system name, e.g., **IPOSE-Primary**, on the navigation pane will expand the menu on this server.



In the screens presented in the following sections, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center and the Details pane on the right side. These panes will be referenced throughout the rest of this document.

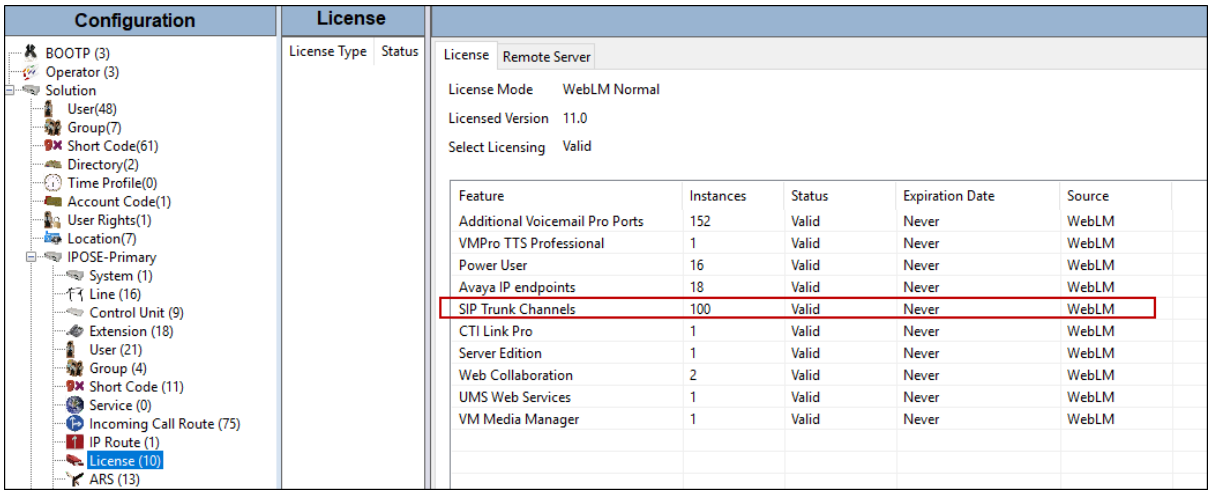
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

## 5.1. Licensing

In the reference configuration, **IPOSE-Primary** was used as the system name of the Primary Server and **IP500 Expansion** was used as the system name of the Expansion System. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane.

The configuration and features described in these Application Notes require the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.

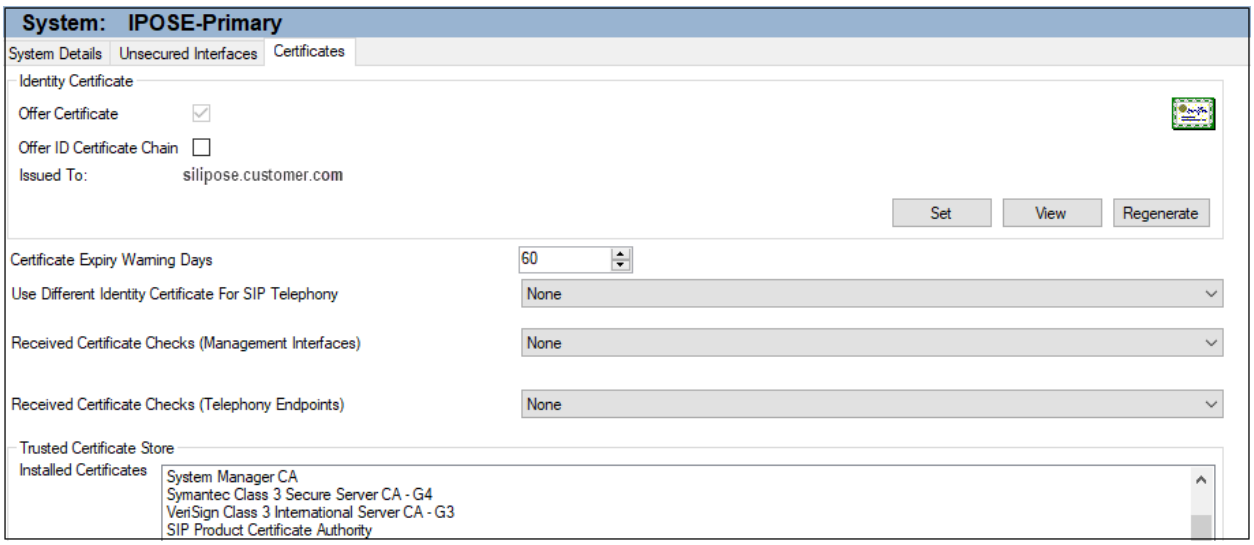


## 5.2. TLS Management

For the compliance test, the signaling on the SIP trunk between IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority **SystemManager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes. However, once the certificates are available they can be viewed on IP Office in the following manner.

To view the certificates currently installed on IP Office, navigate to **File → Advanced → Security Settings**. Log in with the appropriate security credentials (not shown). In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

To verify the identity certificate, locate the **Identity Certificate** section and click **View** to see the details of the certificate.

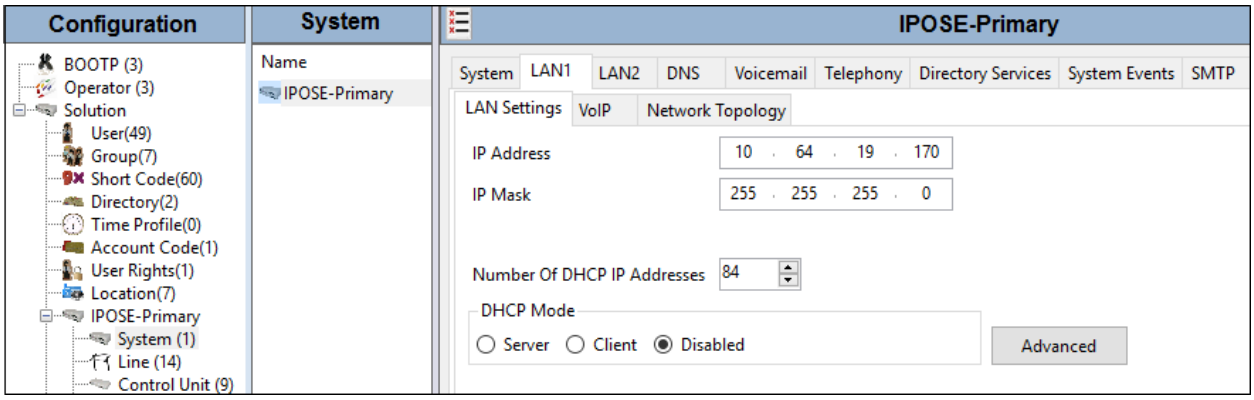


## 5.3. System Settings

This section illustrates the configuration of system settings. Select **System** in the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings. For all the following configuration sections, the **OK** button (not shown) must be selected in order for any changes to be saved.

### 5.3.1. LAN1 Settings

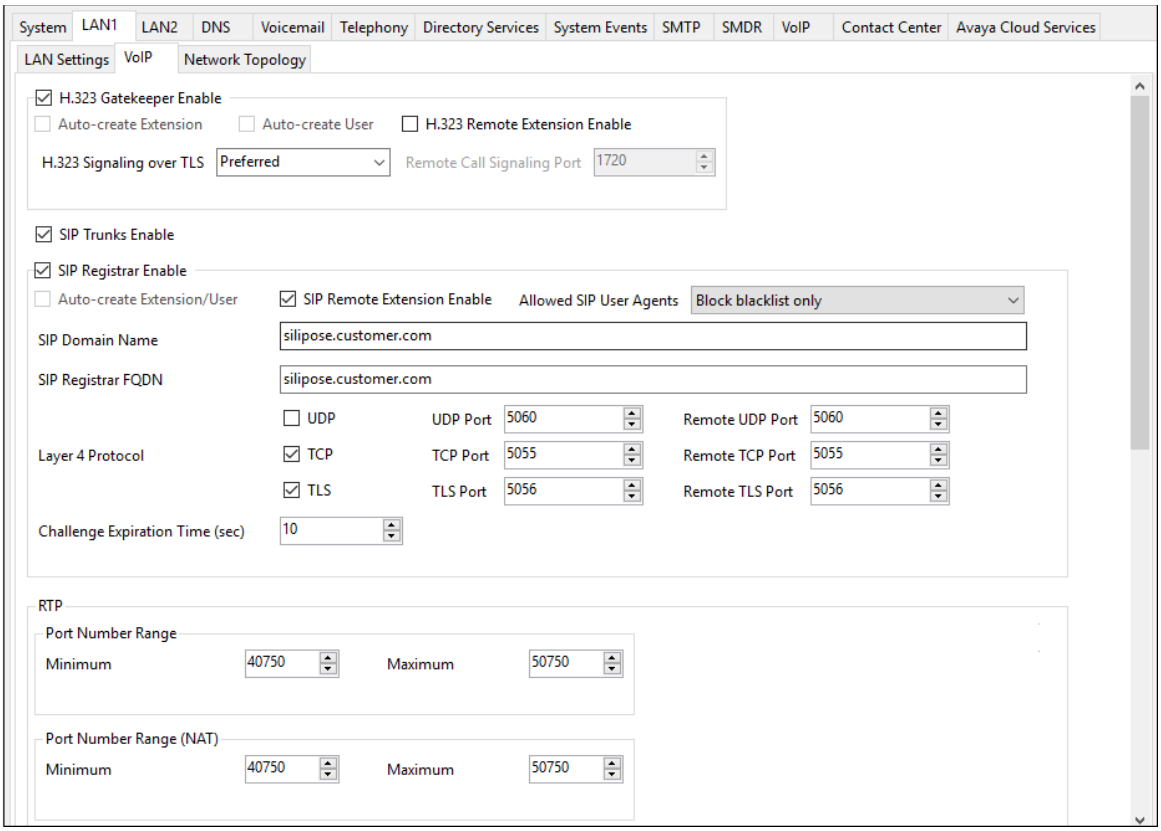
In the reference configuration, LAN1 is used to connect the Primary server to the enterprise network. To view or configure the **IP Address** of LAN1, select the **LAN1** tab followed by the **LAN Settings** tab. As shown in **Figure 1**, the IP Address of the Primary server is **10.64.19.170**. Other parameters on this screen may be set according to customer requirements.



Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** parameter is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 96x1 deskphones used in the reference configuration. The **H.323 Signaling over TLS** should be set based on customer needs. In the reference configuration it was set to **Preferred**. The **SIP Trunks Enable parameter** must be checked to enable the configuration of SIP trunks to Verizon Business. The **SIP Registrar Enable** parameter is checked to allow Avaya J169, Avaya 1140E, and Avaya Equinox usage.

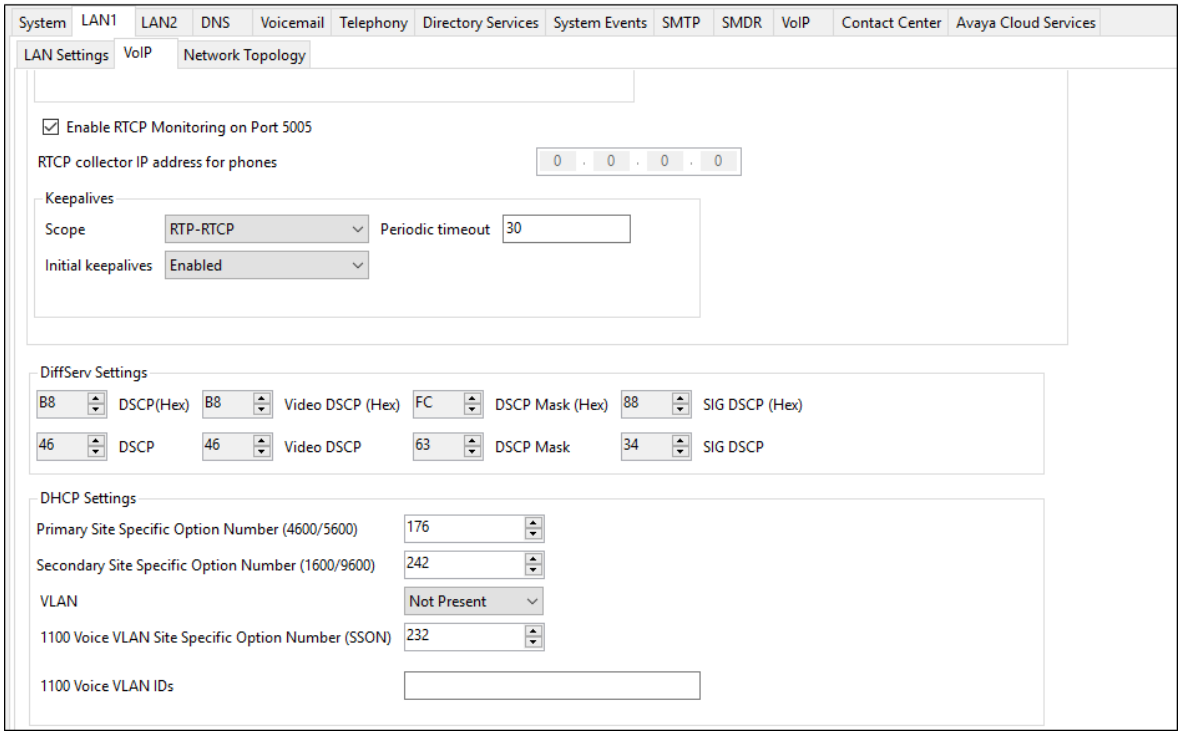
The **SIP Domain Name** and **SIP Registrar FQDN** may be set according to customer requirements. Set the **Layer 4 Protocol** section based on customer needs. In the reference configuration **TCP/5055** and **TLS/5056** were configured.

If desired, the **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media paths from Avaya SBCE to the Primary server. The defaults are used here.

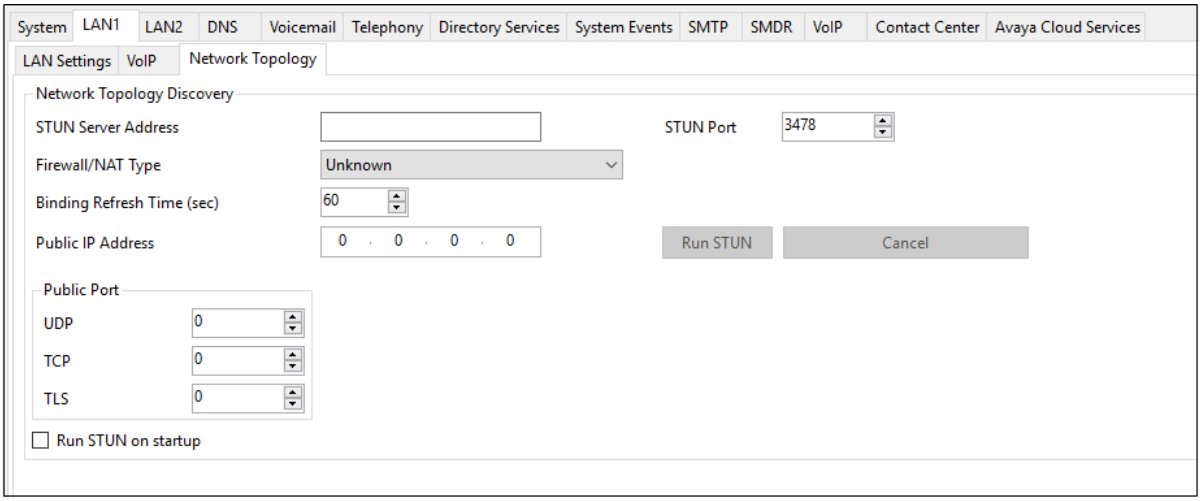


Scrolling down the page, on the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. These settings will cause the Primary server to send RTP and RTCP keepalive packets starting at the time of initial connection and every 30 seconds thereafter if no other RTP or RTCP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting to see media from the other, as well as helping to keep ports open for the duration of the call.

In the **DiffServ Settings** section, the Primary server can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services (QoS) policies for both signaling and media. The **DSCP** field is the value used for media, while the **SIG DSCP** is the value used for signaling. These settings should be set according to the customer's QoS policies in place. The default values used during the compliance test are shown.

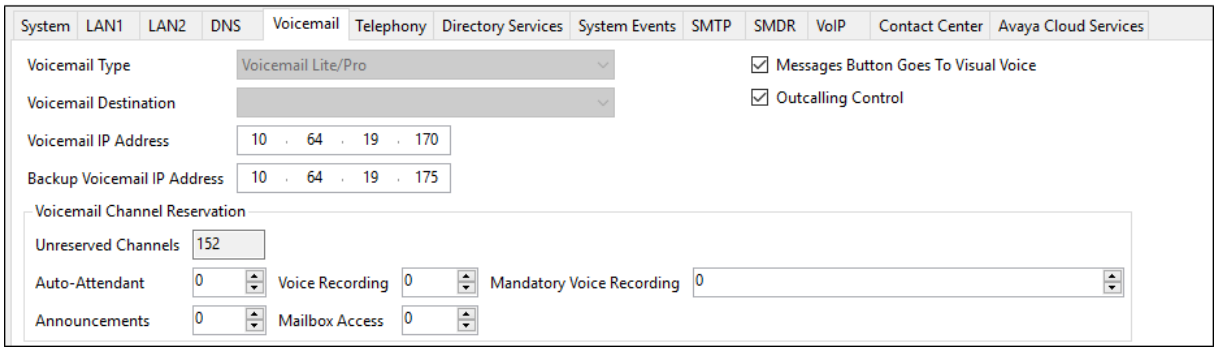


Select the **Network Topology** tab as shown in the following screen. The **Firewall/NAT Type** was set to **Unknown** in the reference configuration. **Binding Refresh Time (sec)** was set to **60** seconds. This is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages, to periodically check the status of the SIP lines configured on this interface. The **Public IP Address** and **Public Port** sections are not used for the Verizon Business SIP trunk service connection.



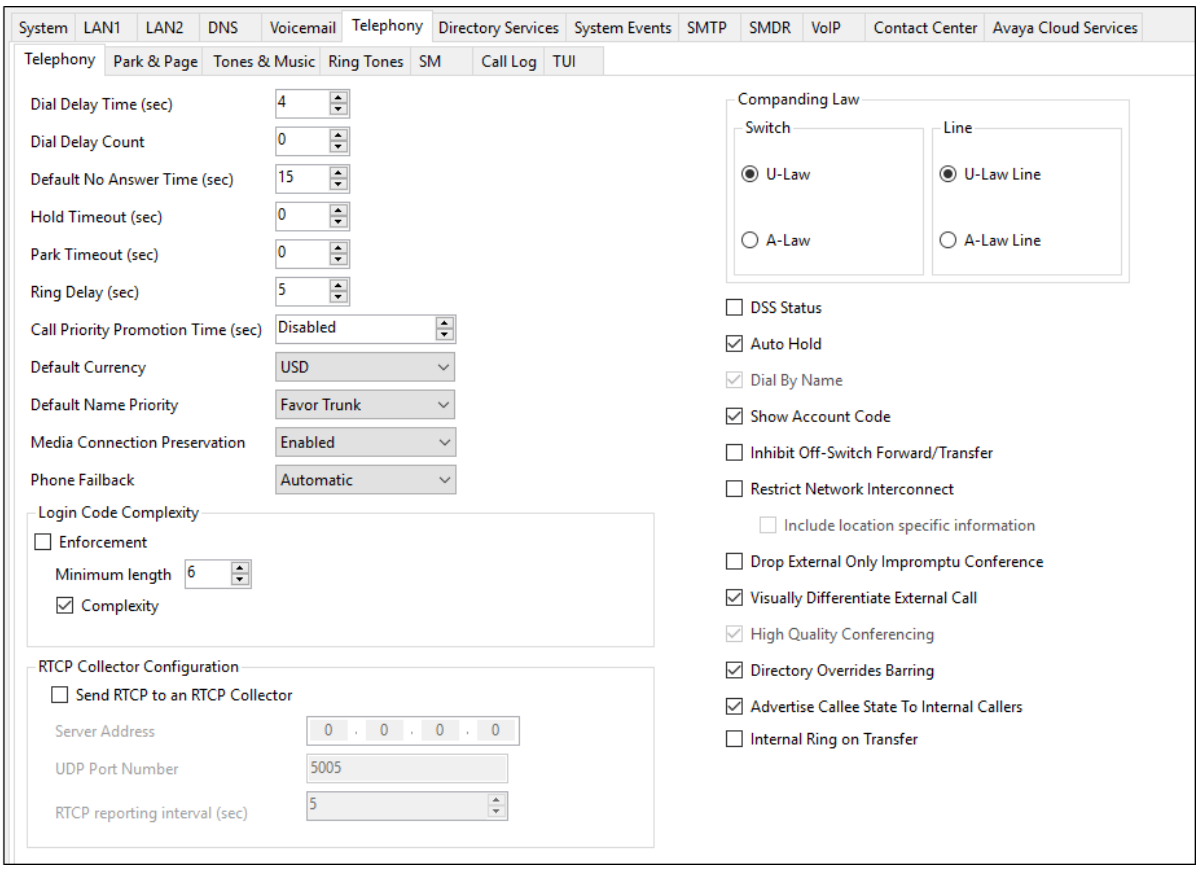

## 5.3.2. Voicemail Settings

To view or change voicemail settings, select the **Voicemail** tab as shown in the following screen. The settings presented here simply illustrate the reference configuration and are not intended to be prescriptive. The **Voicemail Type** in the reference configuration is **Voicemail Lite/Pro**. The **Voicemail IP Address** in the reference configuration is **10.64.19.170**, the IP address of the Primary server running the Voicemail Pro software.



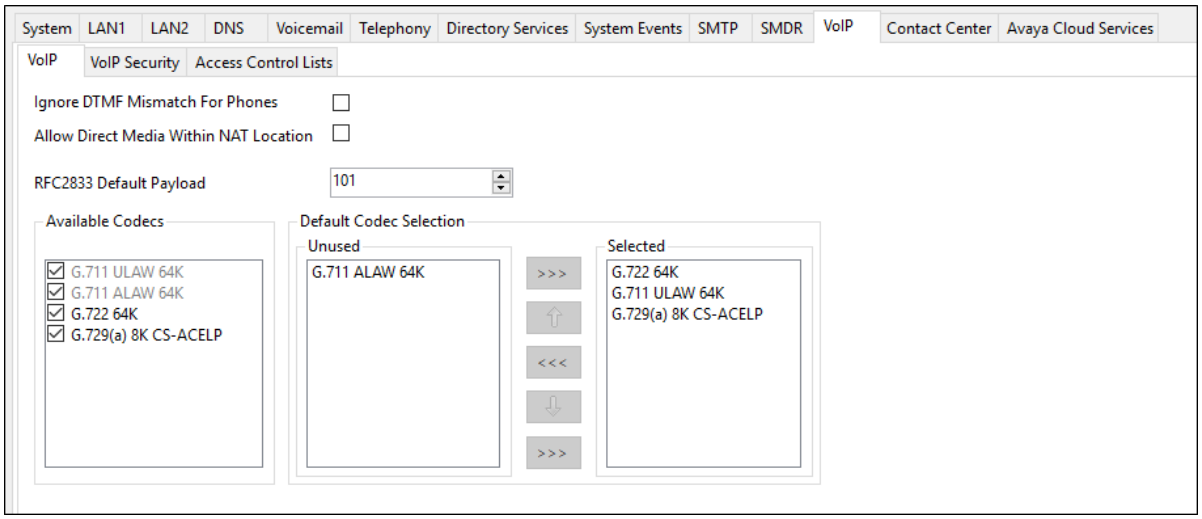
### 5.3.3. System Telephony Settings

To view or change telephony settings, select the **Telephony** tab and **Telephony** sub-tab as shown in the following screen. The settings presented here simply illustrate the reference configuration and are not intended to be prescriptive. In the reference configuration, the **Inhibit Off-Switch Forward/Transfer parameter** is unchecked so that call forwarding and call transfer to PSTN destinations via the Verizon Business IP Trunking service can be tested. That is, a call can arrive to IP Office via the Verizon Business IP Trunking, and be forwarded or transferred back to the PSTN with the outbound leg of the call using the Verizon IP Trunk service. The **Companding Law** parameters are set to **U-Law** as is typical in North American locales. Other parameters on this screen may be set according to customer requirements.

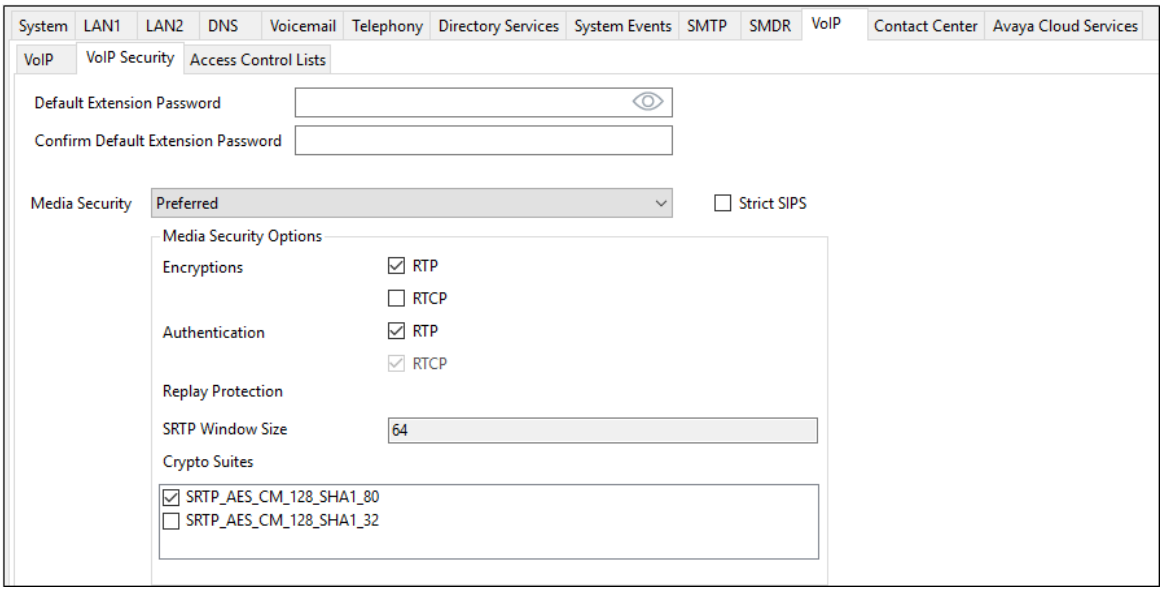


### 5.3.4. System VoIP Settings

To view or change system codec settings, select the **VoIP → VoIP** tab. The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. During the compliance test, this was set to **101**, the value preferred by Verizon Business. For codec selection, on the left, observe the list of **Available Codecs**. In the example screen below, which is not intended to be prescriptive, the parameter next to each codec is checked, making all the codecs available in other screens where codec configuration may be performed (such as the SIP Line in **Section 5.5.5**). The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis, using the up, down, left, and right arrows. By default, all IP (SIP and H.323) lines and extensions will assume the system default codec selection, unless configured otherwise for the specific line or extension.

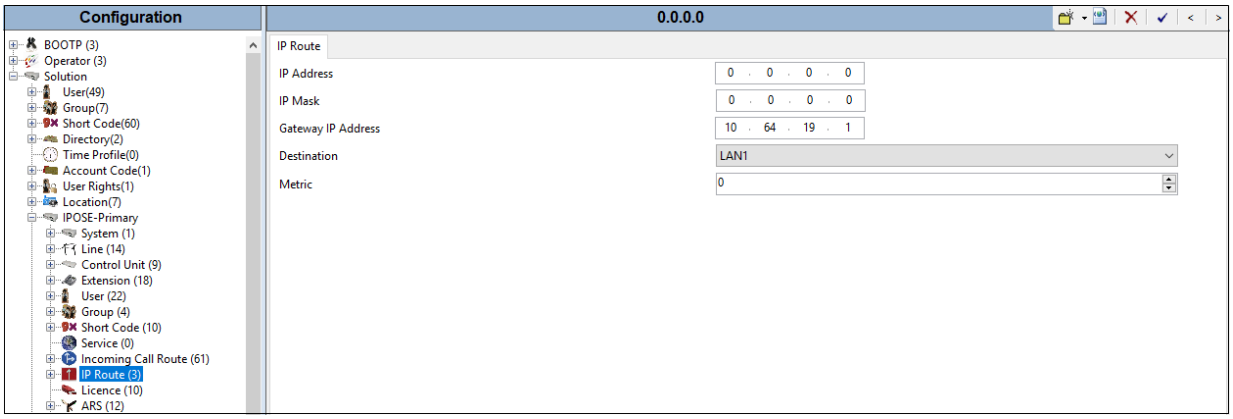


During the compliance test, SRTP was used internal to the enterprise wherever possible. To view or configure the media encryption settings, select the **VoIP → VoIP Security** tab on the Details pane. The **Media Security** drop-down menu is set to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption. Under **Media Security Options**, **RTP** is selected for the **Encryptions** and **Authentication** fields. Under **Crypto Suites**, **SRTP_AES_CM_128_SHA1_80** is selected.



## 5.4. IP Route

In the reference configuration, the Primary server LAN1 port is physically connected to the local area network switch at the IP Office customer site. The default gateway for this network is 10.64.19.1. The Avaya SBCE resides on a different subnet and requires an IP Route to allow SIP traffic between the two devices. To add an IP Route in the Primary server, right-click **IP Route** from the Navigation pane, and select **New** (not shown). To view or edit an existing route, select **IP Route** from the Navigation pane, and select the appropriate route from the Group pane. The following screen shows the Details pane with the relevant route using **LAN1** as **Destination**.



## 5.5. SIP Line

This section shows the configuration screens for the SIP Line in IP Office Release 11.1. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.5.1** to create the SIP Line from the template.

Some items relevant to a specific customer environment are not included in the template or may need to be updated after the SIP Line is created. Examples include the following:

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- Setting of the **Use Network Topology Info** field on the Transport tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2 – 5.5.6**.

In addition, the following SIP Line settings are not supported on Basic Edition:

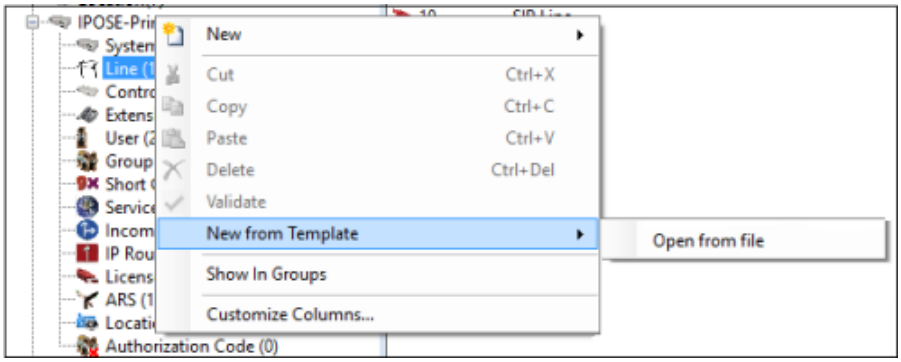
- SIP Line – Originator number for forwarded and twinning calls.
- Transport – Second Explicit DNS Server.
- SIP Credentials – Registration Requirement.
- SIP Advanced Engineering.

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.5.2 – 5.5.6**.

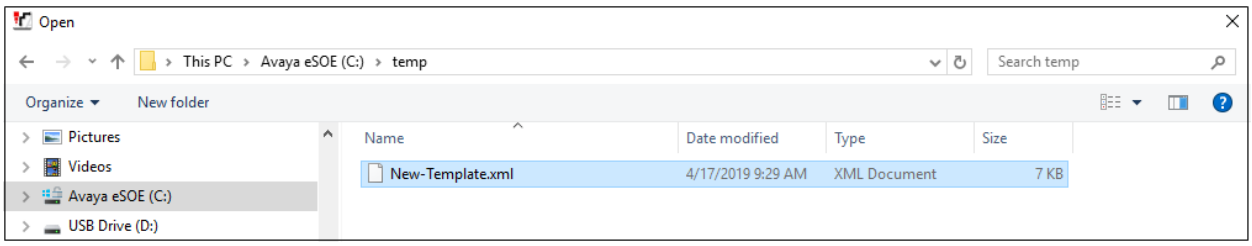
### 5.5.1. Creating a SIP Line Template

> **Note** – DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500v2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

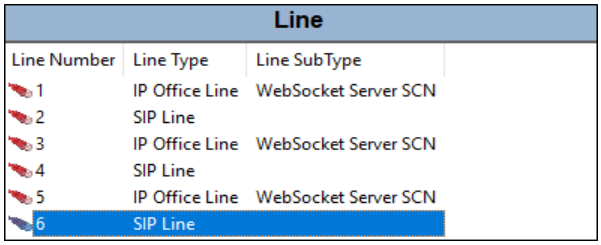
Copy a previously created template file to the computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New →New from Template**. Select **Open from file.**




Navigate to the directory where the template was copied on the local computer (e.g., *\temp*) and select it. Click **Open** (not shown).




The new SIP Line is created, and it will appear on the **Navigation** pane (e.g., SIP Line **6**). The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.5.2** to **5.5.6**.



**Line**

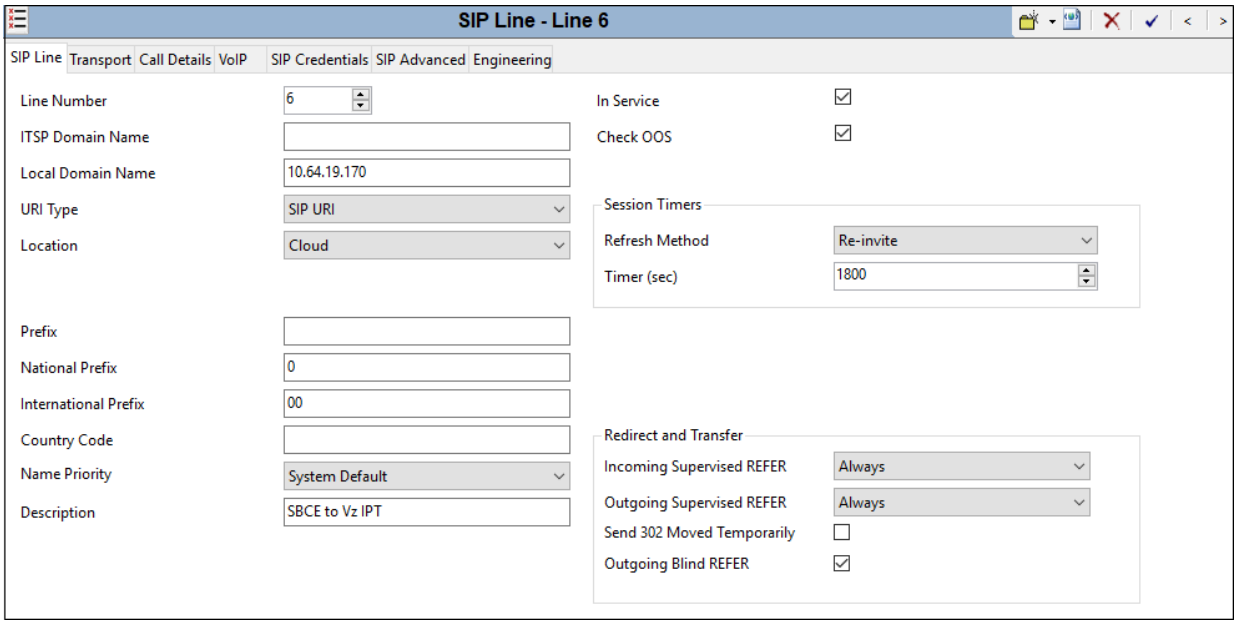
| Line Number | Line Type | Line SubType |
|---|---|---|
| 1 | IP Office Line | WebSocket Server SCN |
| 2 | SIP Line | |
| 3 | IP Office Line | WebSocket Server SCN |
| 4 | SIP Line | |
| 5 | IP Office Line | WebSocket Server SCN |
| 6 | SIP Line | |

### 5.5.2. SIP Line – SIP Line Tab

The **SIP Line** tab in the Details pane is shown below for Line Number **6**, used for Avaya SBCE to the Verizon Business IP Trunking service. The **ITSP Domain Name** is left blank, to have IP Office send the **ITSP Proxy Address** as the domain name (see **Section 5.5.3**). **Local Domain Name** is set to the IP address of the Avaya IP Office LAN1 interface (e.g., **10.64.19.170**). By default, the **In Service** and **Check OOS** boxes are checked. In the reference configuration, IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by IP Office will use the **Binding Refresh Time** for LAN1, as shown in **Section 5.3.1**.

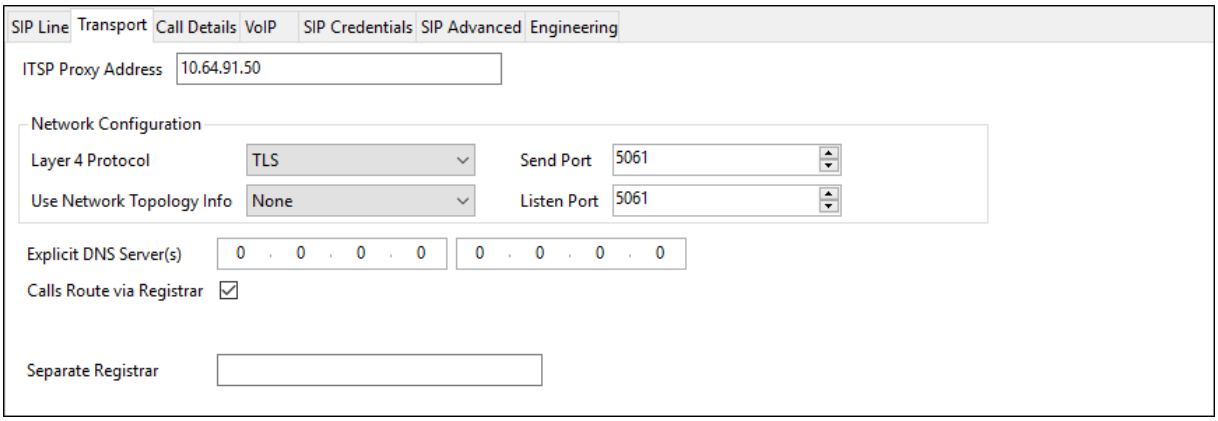
Under **Session Timers**, the **Refresh Method** is set to "**Reinvite**" and the **Timer (seconds)** is set to **1800**. With this configuration, IP Office will send re-INVITEs every 15 minutes (half of the set value) to keep the active session alive.

Under **Redirect and Transfer**, the default setting for the automatic determination of **Incoming Supervised REFER** and **Outgoing Supervised REFER** is **Auto**. Alternatively, the default can be overridden with "**Never**" to explicitly disable use of supervised REFER, or **Always** to explicitly enable use of supervised REFER, as shown below. The **Send 302 Moved Temporarily** setting is unchecked, as Verizon does not support receiving a 302 Moved Temporarily message. Optionally, the **Outgoing Blind REFER** parameter can be checked to enable the use of REFER for blind transfers.



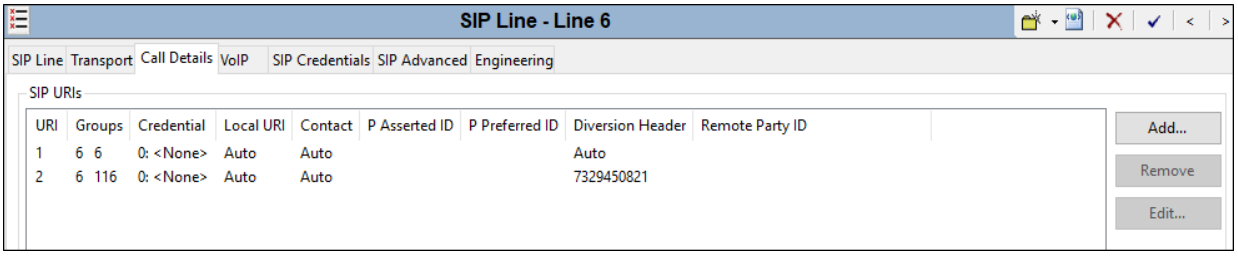
### 5.5.3. SIP Line - Transport Tab

Select the **Transport** tab. The **ITSP Proxy Address** is set to the inside IP address of the primary Avaya SBCE as shown in **Figure 1**. In the **Network Configuration** area, **TLS** is selected as the **Layer 4 Protocol**. The **Send Port** and **Listen Port** can retain the default value 5061. The **Use Network Topology Info** parameter is set to **None**.



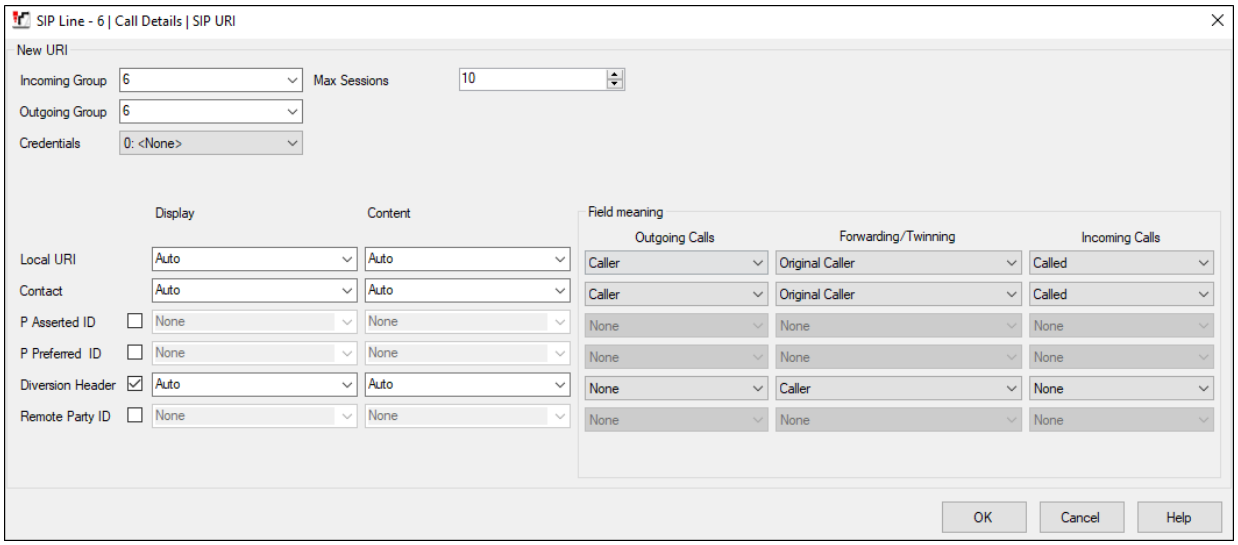

### 5.5.4. SIP Line – Call Details Tab

Select the **Call Details** tab. To add a new SIP URI, click the **Add…** button. A New URI area will be opened. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button.



In the example screen below, a previously configured entry is edited. The **Incoming Group** parameter, set here to **6**, will be referenced when configuring Incoming Call Routes to map inbound SIP trunk calls to IP Office destinations in **Section 5.9**. The **Outgoing Group** parameter, also set to **6**, will be used for routing outbound calls to Verizon via ARS (**Section 5.10**). The **Max Sessions** parameter was set to "**10**". This value sets the maximum number of simultaneous calls that can use the URI before IP Office returns busy to any further calls.

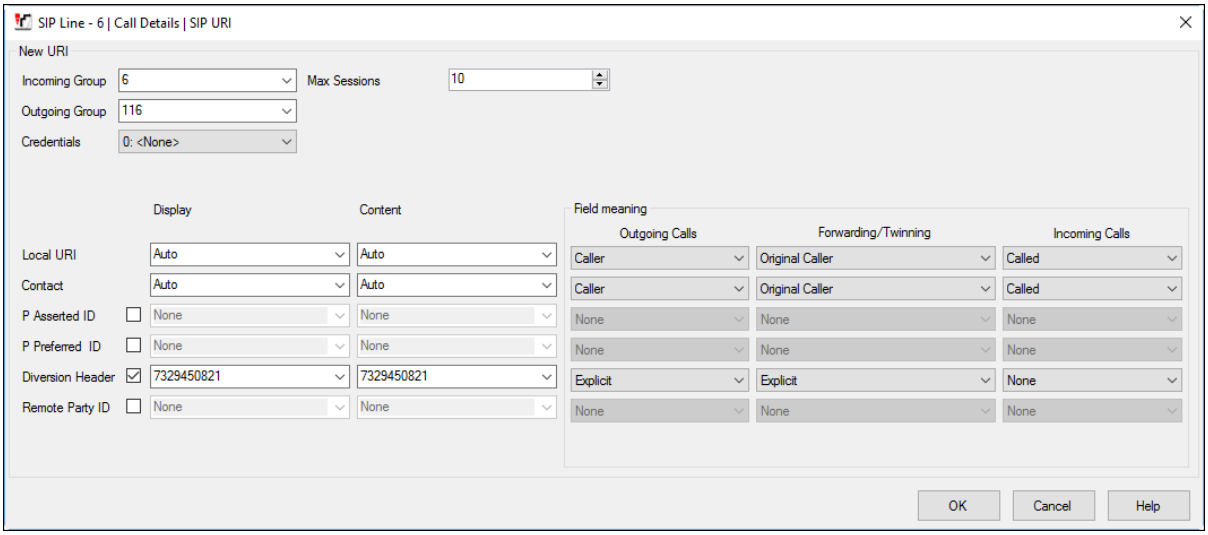
**Auto** is selected for the **Local URI**, **Contact** and **Diversion Header** parameters. With this configuration, information in the Incoming Call Route (**Section 5.9**) is used determine what call is accepted on the SIP Line. The Incoming Call Route for individual users will also be used to populate the SIP From and Contact headers for outbound calls. Set the **Field meaning** section to the values shown in the screenshot below.




In the reference configuration, the single SIP URI shown above was sufficient to allow incoming calls for Verizon DID numbers destined for specific IP Office users, hunt groups or short codes.

The following screen shows an example configuration for the Verizon's Unscreened ANI feature. This optional configuration allows customers to send an "unscreened" ANI to Verizon's network which is then displayed to the called party as Caller ID. An "unscreened" ANI can be any telephone number that the customer passes through Verizon's network for Caller ID display purposes only. If this feature is enabled on the Verizon IP Trunk services, Verizon will designate one of the assigned telephone numbers as a "Screened Telephone Number" for each unique location. Verizon will use this Screened Telephone Number to determine call origination for billing, call routing, and E911.

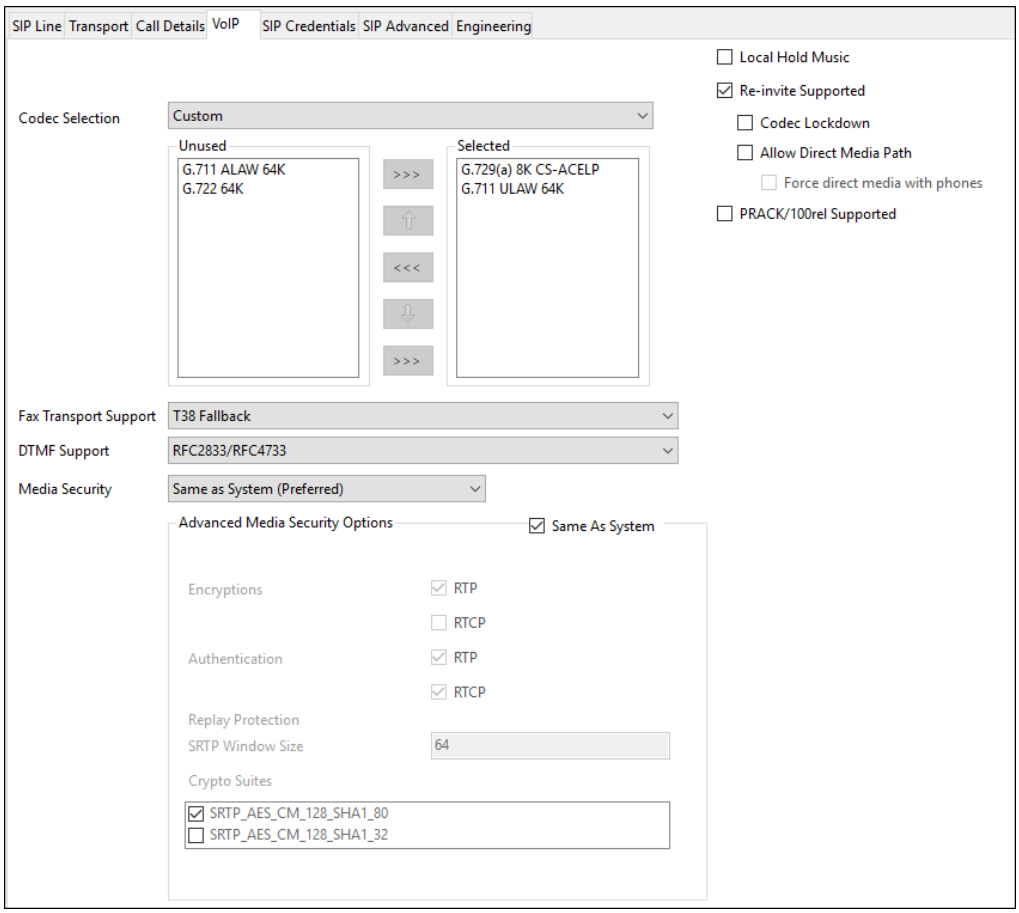
The Screened Telephone Number (STN) provided by Verizon for this test is 732-945-0821. Typically, customers would have one or more STN; one for every location. A central Primary server could be used to pass multiple STNs to Verizon based on the **Outgoing Group** selected. The STN would then be entered in the **Diversion Header** field as shown below.



### 5.5.5. SIP Line - VoIP Tab

Select the **VoIP** tab. The **Codec Selection** drop-down parameter **System Default** (default) will match the codecs set in the system wide Default Selection list (**System → VoIP**). In the reference configuration, **Custom** is selected and the codecs **G729(a) 8K CS-ACELP** and **G.711 ULAW 64K** preferred by Verizon are specified. This will cause IP Office to include these codecs in the Session Description Protocol (SDP) offer, in that order. The **Fax Transport Support** drop-down is set to **T38 Fallback**. This enables T.38 to be used for fax if supported, and will fall back to G.711 if not. The **DTMF Support** parameter can remain set to the default value **RFC2833/RFC4733**. The **Media Security** drop-down menu is set to **Same as System (Preferred)** to have IP Office use the system setting for media security set in **Section 5.3.4** to encrypted RTP toward Avaya SBCE. The **Re-invite Supported** parameter is checked to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.

For PSTN originations, Verizon preferred the G.729a codec in the SDP, while also allowing the G.711MU codec. During testing, the IP Office configuration was varied such that G.711MU was the preferred or only codec listed, and G.711MU calls were also successfully verified.

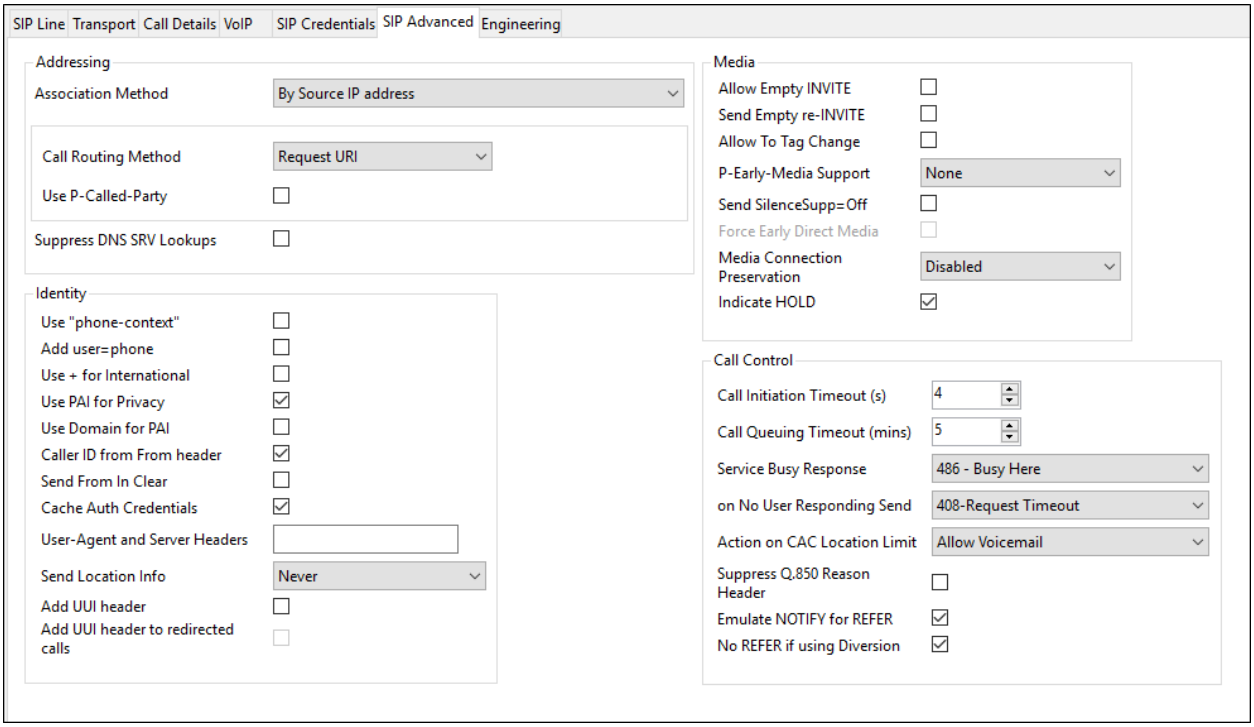


### 5.5.6. SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab. In the **Identity** area, the **Use PAI for Privacy** parameter is checked to include the caller's DID number in the P-Asserted-Identity (PAI) SIP header for a privacy requested call. This PAI SIP header is required by Verizon Business to admit an otherwise anonymous caller to the network. The **Caller ID from From header** parameter is checked to have IP Office use the Caller ID information in the From SIP header rather than the PAI or Contact SIP header for inbound calls. This will allow the Caller Name presented in the From SIP header by Verizon Business to also be included in the Caller ID.

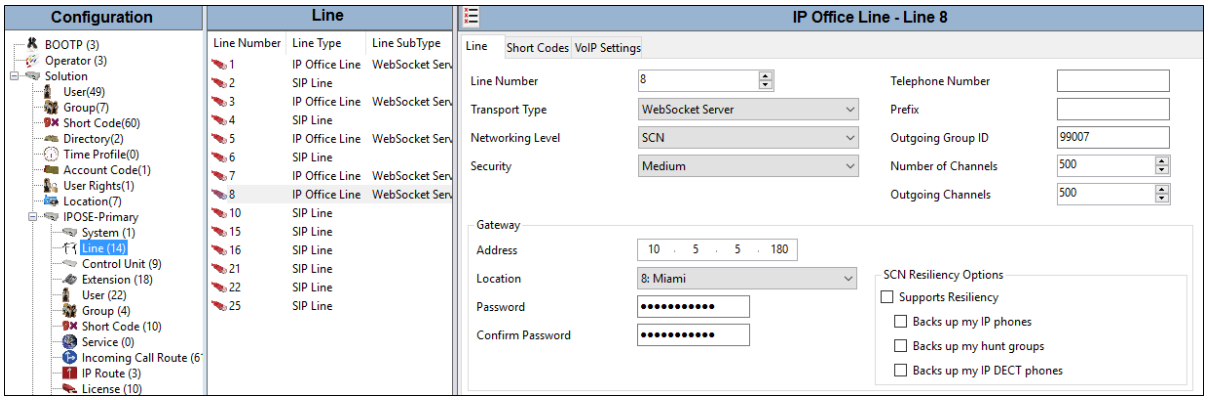
In the Media area, the **Indicate HOLD** parameter is checked to have IP Office send an INVITE with media attribute "sendonly", indicating the call was placed on hold. This is the preferred behavior for Verizon Business to indicate placing a call on hold.

In the **Call Control** area, the **Emulate NOTIFY for Refer** parameter is checked. This is required for some SIP endpoints that perform Refer based transfers across the SIP line. See **Section 2.2** for more details. The **No Refer if using Diversion** parameter is checked to prevent IP Office from using the SIP REFER method on call forwarded scenarios that use a Diversion SIP header. Verizon does not support this type of refer and would respond with a "403 Forbidden" SIP message if a REFER is sent in this scenario.

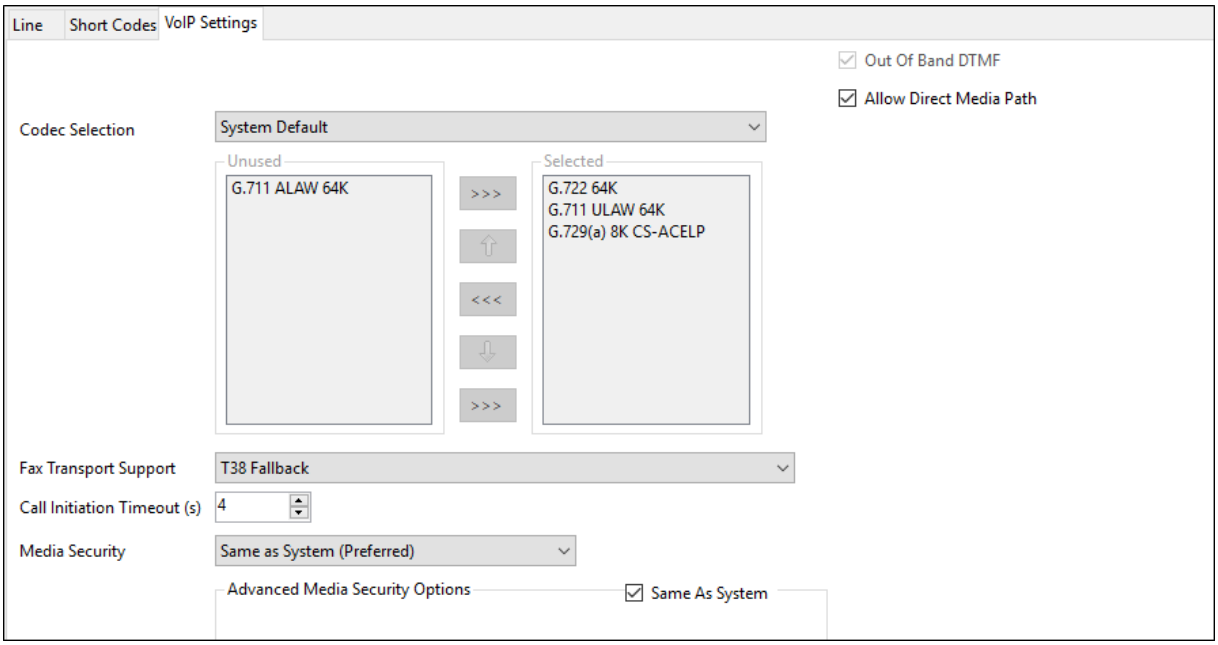


## 5.6. IP Office Line

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the IP500 V2 Expansion System.



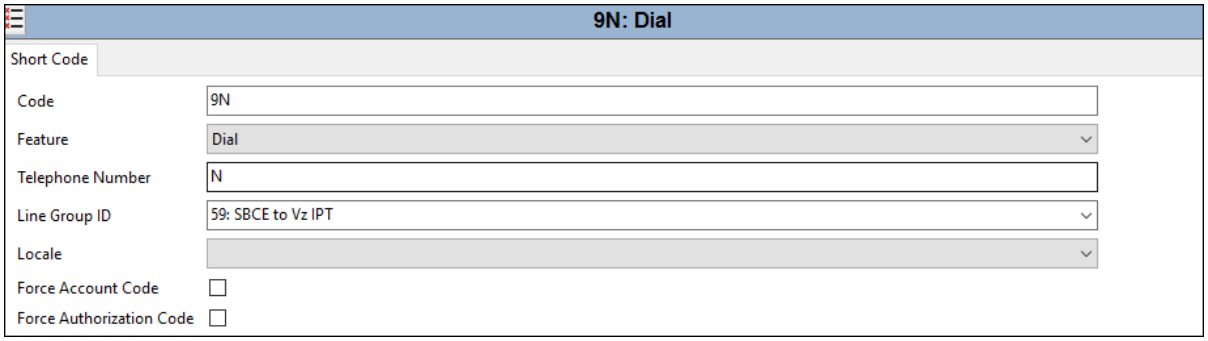

The screen below shows the IP Office Line, **VoIP Settings** tab. In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. **Fax Transport Support** is set to **T.38 Fallback**. The **Media Security** is set to **Same as System (Preferred)** to have IP Office use the system setting for media security set in **Section 5.3.4** to encrypted RTP. Default values were used for all other parameters.



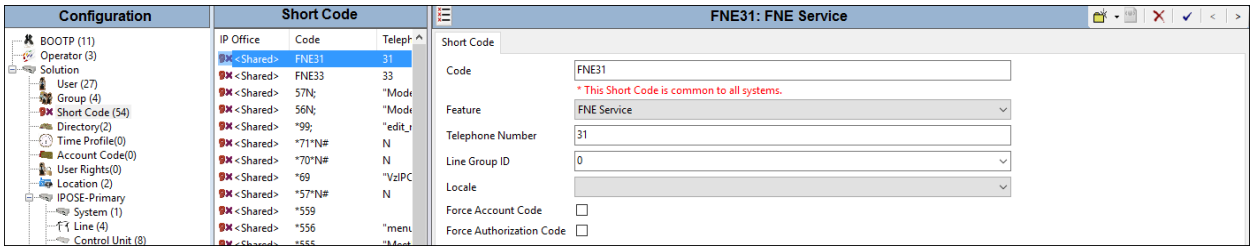
## 5.7. Short Codes

In this section, various examples of IP Office short codes will be illustrated. To add a short code, right click on **Short Code** in the Navigation pane, and select **New**. To edit an existing short code, click **Short Code** in the Navigation pane, and the short code to be configured in the Group pane.

In the screen shown below, the short code **9N** is illustrated. The **Code** parameter is set to **9N**. The **Feature** parameter is set to **Dial**. The **Telephone Number** parameter is set to **N**. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message. The **Line Group ID** parameter is set to **59: SBCE to Vz IPT**, configurable via ARS. See **Section 5.10** for example ARS route configuration.




The following screen illustrates a solution level short code, common to all servers, that acts like a feature access code rather than a means to access a SIP Line. In this case, the **Code FNE31** is defined for **Feature FNE Service** to **Telephone Number 31** (Mobile Call Control). This short code will be used as means to allow a Verizon DID to be programmed to route directly to this feature, via inclusion of this short code as the destination of an Incoming Call Route. See **Section 5.9**. This feature is used to provide dial tone to twinned mobile devices (e.g., cell phone) directly from IP Office; once dial tone is received the user can perform dialing actions including making calls and activating Short Codes.

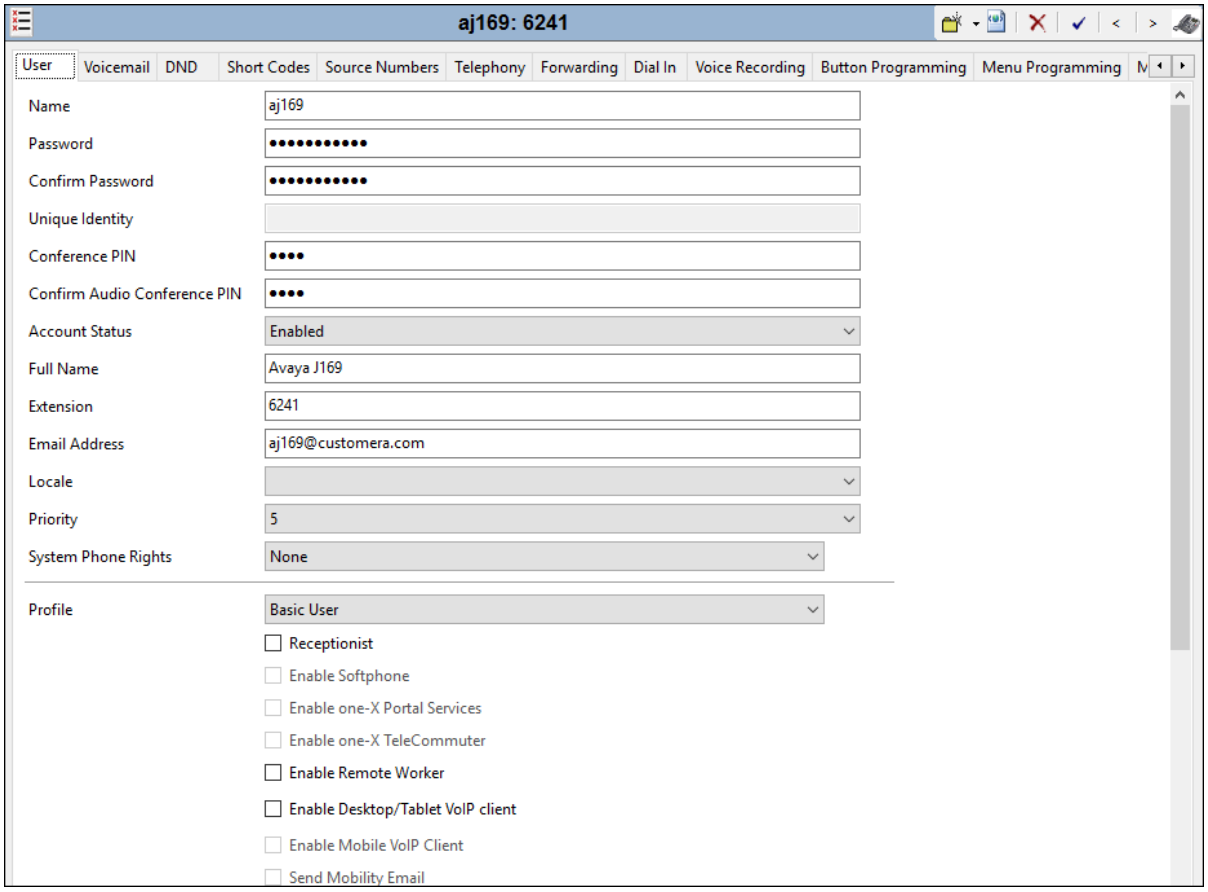



## 5.8. Users, Extensions, and Hunt Groups

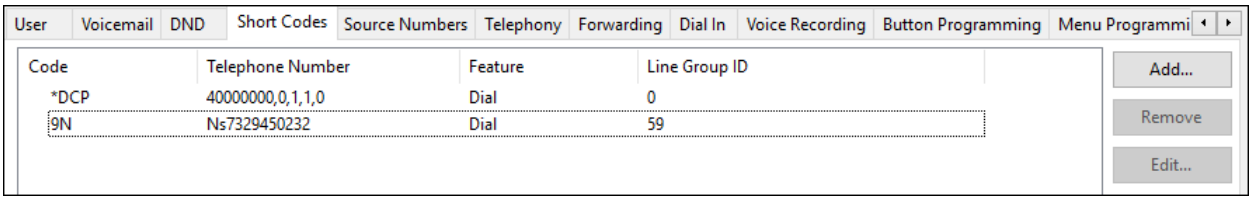
In this section, examples of an IP Office User, Extension, and Hunt Group will be illustrated. In the interests of brevity, not all users and extensions shown in **Figure 1** will be presented, since the configuration can be easily extrapolated to other users. To add a User, right click on **User** in the Navigation pane, and select **New**. To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane.

### 5.8.1. SIP User

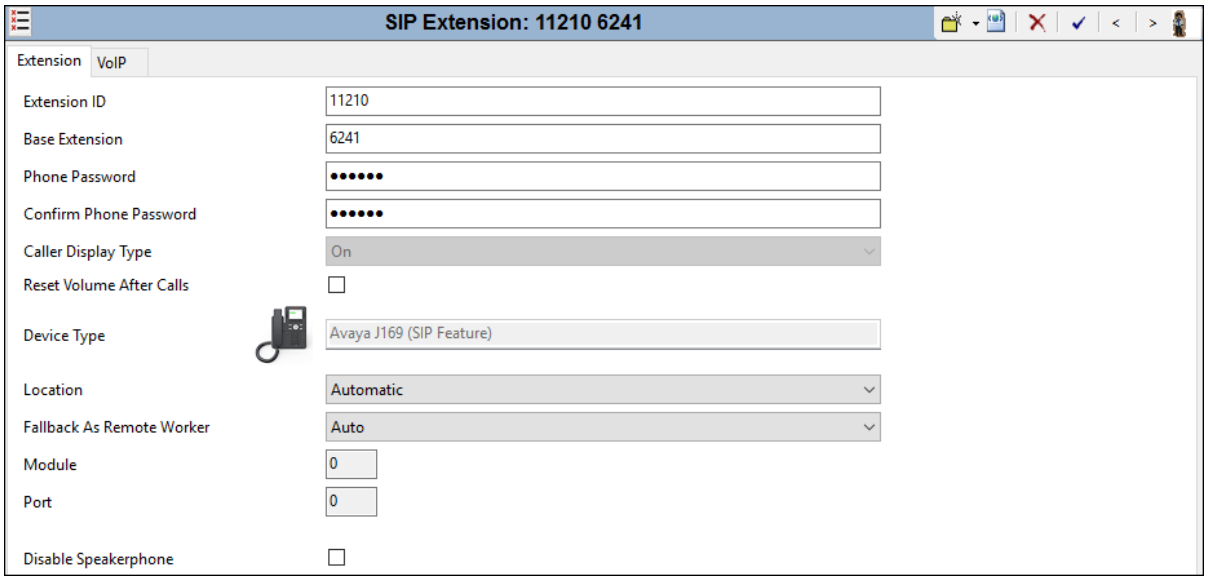
The following screen shows the **User** tab for user 6241. As shown in **Figure 1**, this user corresponds to the Avaya J169 SIP endpoint.



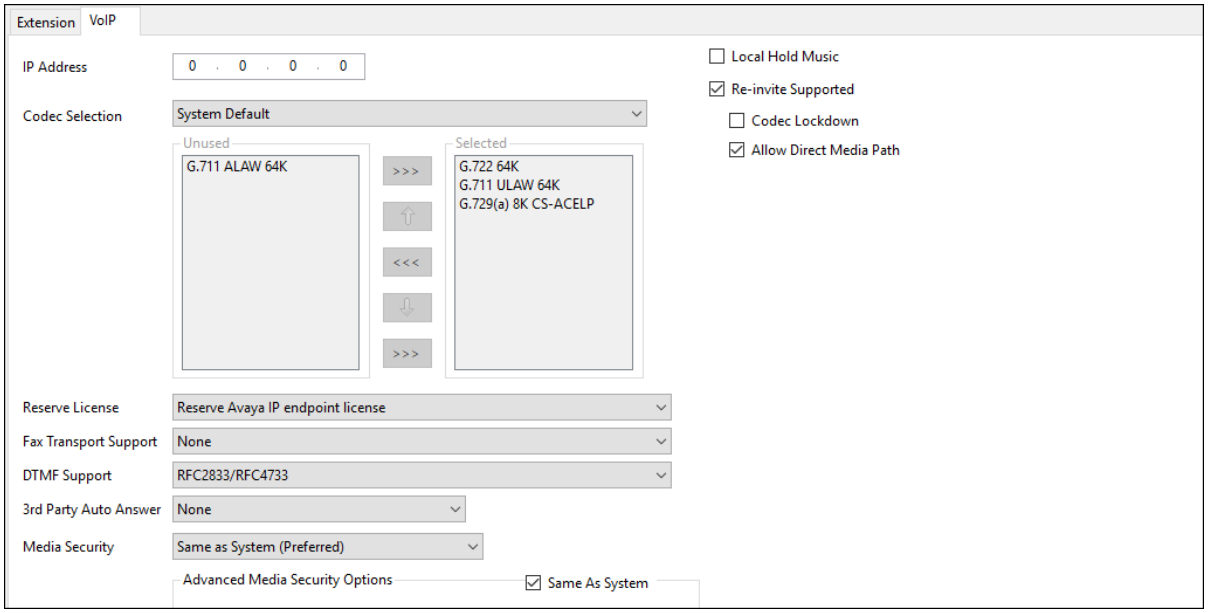

Optionally, if the user does not have a 10-digit telephone number assigned to it in the incoming call route (**Section 5.9**), a User Short Code can be created to set the outbound caller ID. The following screen shows the **Short Codes** tab for user 6322. This user is not associated with an incoming call route. The **Telephone Number** is set to **Ns7329450232**. The number after "s" is used to construct the From and Contact headers in the outgoing SIP INVITE message.



The following screen shows the Extension information for this user. To view, select **Extension** from the Navigation pane, and the appropriate extension from the Group pane.



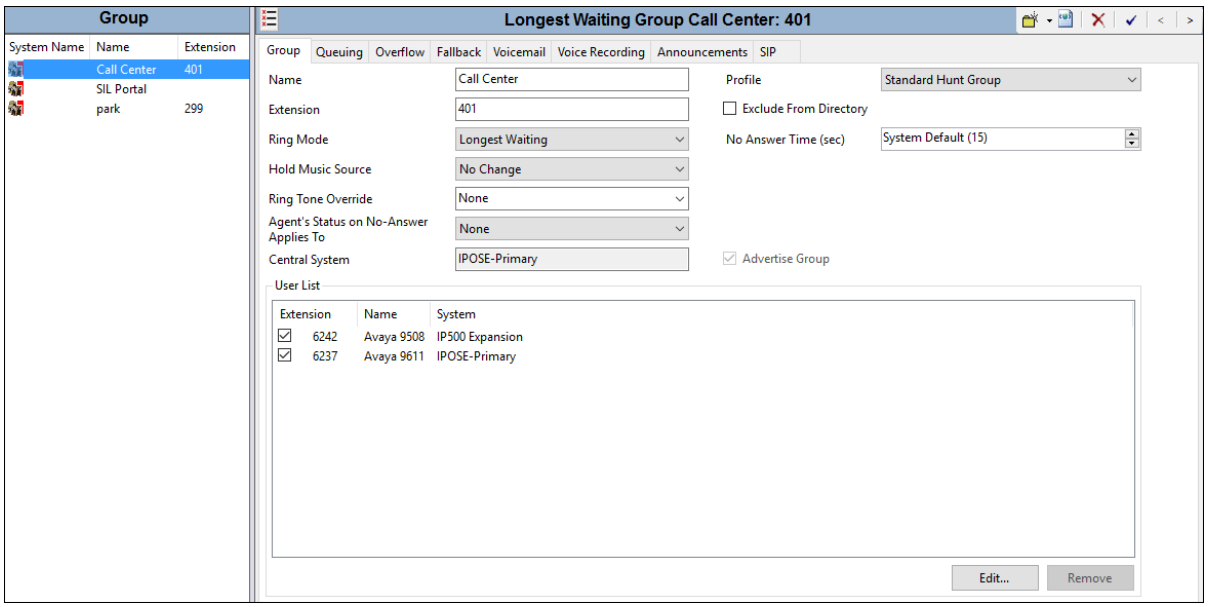

The following screen shows the **VoIP** tab for the extension. The **IP Address** field may be left blank. Check the **Reserve Avaya IP endpoint license** box. The **Codec Selection** parameter may retain the default setting "**System Default**" to follow the system configuration shown in **Section 5.3.4**. The Media Security parameter may also retain the default setting **Same as System (Preferred)** to follow the system configuring shown in **Section 5.3.4**.



### 5.8.2. Hunt Groups

During the verification of these Application Notes, users could also receive incoming calls as members of a hunt group. To configure a new hunt group, right-click **Group** from the Navigation pane, and select **New**. To view or edit an existing hunt group, select **Group** from the Navigation pane, and the appropriate hunt group from the Group pane.

The following screen shows the **Group** tab for hunt group 401. The telephone extensions in the **User List** are rung based the extension that has been unused for the longest period, due to the **Ring Mode** setting **Longest Waiting** (i.e., "longest waiting", most idle user receives next call). Click the **Edit** button to change the **User List**.

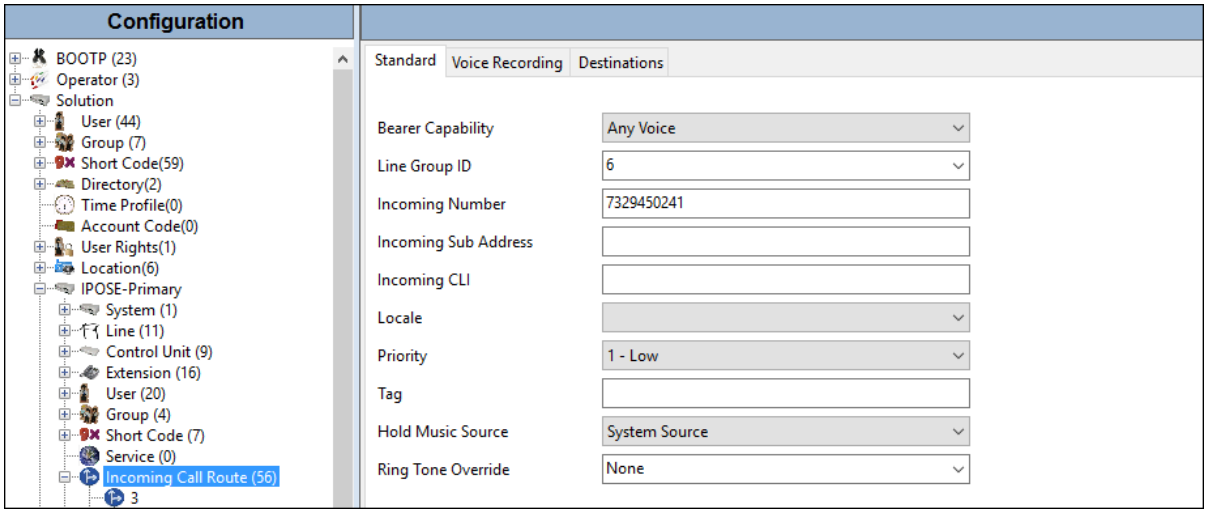


## 5.9. Incoming Call Routes

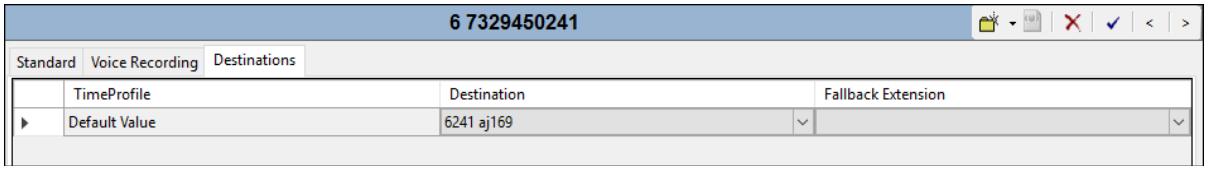
In this section, IP Office Incoming Call Routes are illustrated. To add an incoming call route, right click on **Incoming Call Route** in the Navigation pane and select **New**. To edit an existing incoming call route, select **Incoming Call Route** in the Navigation pane, and the appropriate incoming call route to be configured in the Group pane.

In the screen shown below, a simple incoming call route is illustrated. The **Line Group Id** is **6**, matching the **Incoming Group** field configured in the **SIP URI** tab for the SIP Line to Verizon Business in **Section 5.5.4**. The **Incoming Number** field is set to the incoming number on which this route should match. Matching is right to left.

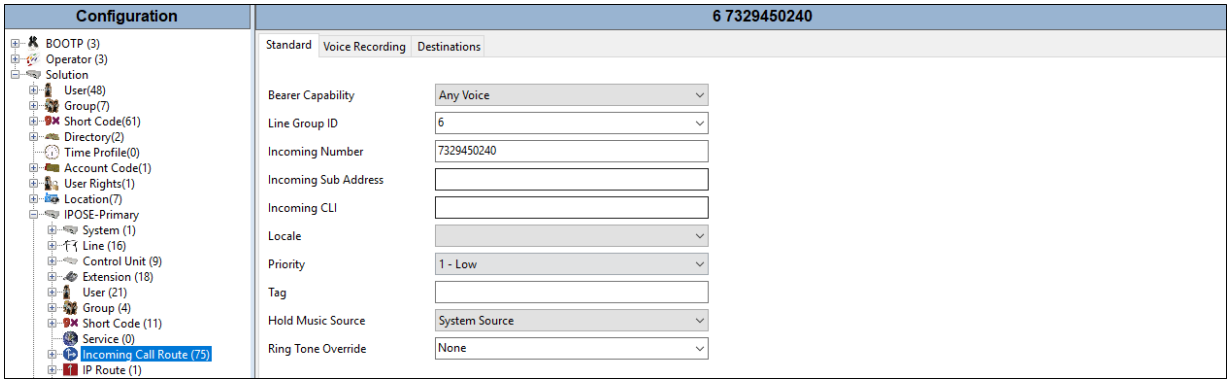
**Note**: When the destination is a user's extension, the **Incoming Number** can be used to construct the From and Contact headers in place of the extension number in the outgoing SIP INVITE message for the user, for caller ID purposes.




On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, incoming calls to 7329459241 on line 6 are routed to extension 6241.



In the following example, the incoming call route for **Incoming Number 7329450240** is illustrated. The **Line Group Id** is **6**, matching the Incoming Group field configured in the **SIP URI** tab for the SIP Line to Verizon Business in **Section 5.5.4**.




On the **Destinations** tab, the **Destination** field is set to **FNE31**, manually entered. The name "FNE31" is the short code for accessing the "Mobile Call Control" application configured in **Section 5.7**. An incoming call to 732-945-0240 will be delivered directly to internal dial tone from the IP Office, allowing the caller to perform dialing actions including making calls and activating Short Codes. The incoming caller ID must match the Twinned Mobile Number entered in the Mobility tab of one of the IP Office users; otherwise the IP Office responds with a "486 Busy Here" and the caller will hear a busy tone.

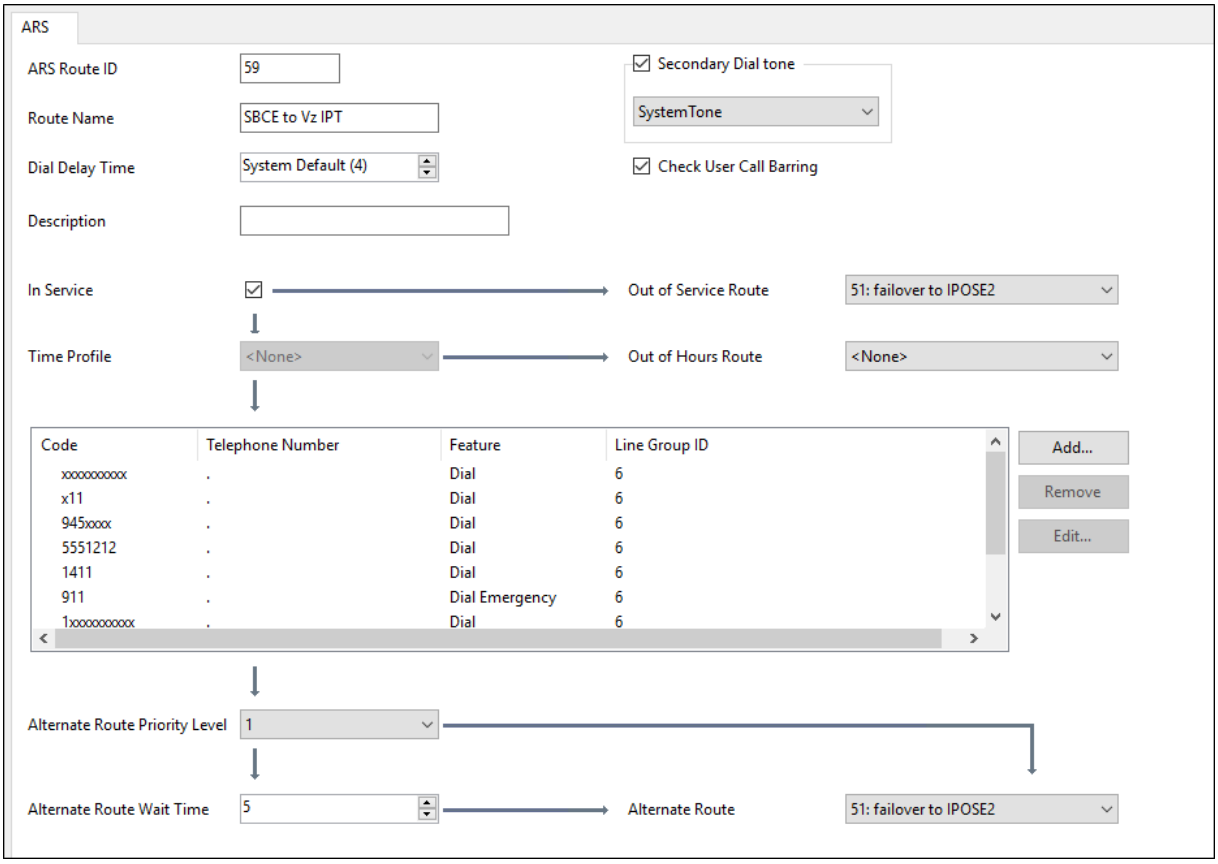

Repeat this process to route the rest of the Verizon DID numbers to additional users, as well as other Avaya IP Office destinations (Hunt Group, Voicemail, Short Codes, etc.).

## 5.10. ARS Routing

While detailed coverage of ARS is beyond the scope of these Application Notes, this section includes some basic screen illustrations of the ARS settings used during the compliance test.

As described in **Section 5.7**, Short Code **9N** was defined for ARS access. Therefore, outbound calls via ARS are dialed as 9 plus the number. ARS will strip off the 9, and it will process the call based on the remaining digits.

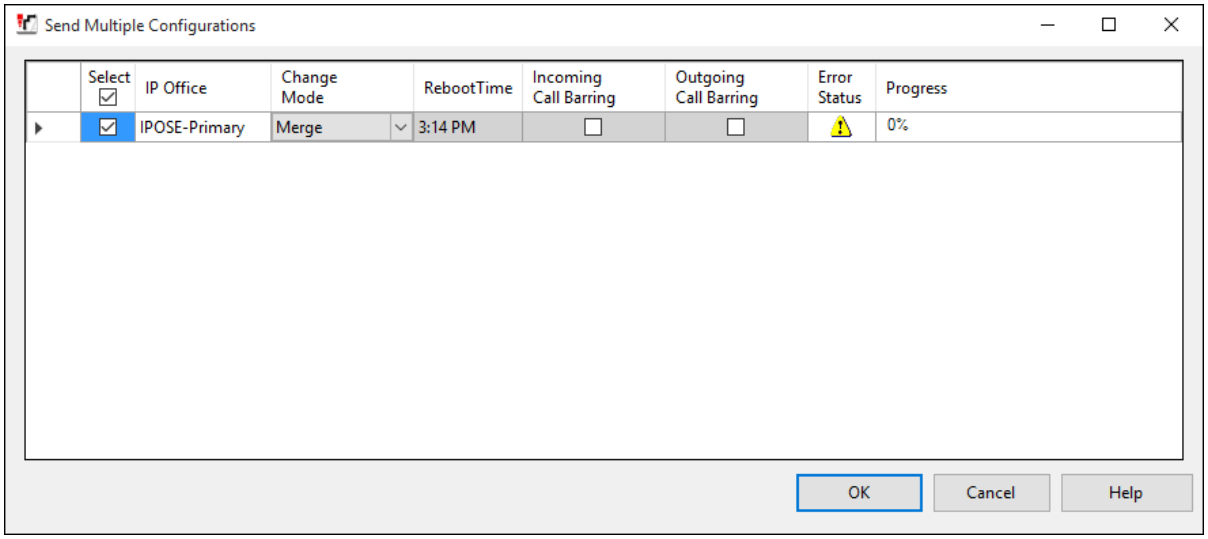
To add a new ARS route, right-click **ARS** in the **Navigation** pane, and select **New** (not shown). The following screen shows the **ARS Route ID 59**, created in the sample configuration. The sequence of **X**s used in the **Code** column of the entries are used to specify the exact number of digits to be expected following the access code. The first entry below shows that for calls to area codes in the North American Numbering Plan, the user dials 9, followed by 10 digits. The list of codes defined below is simply an example and not intended to be prescriptive. Other dialing codes may be appropriate for different customer networks. The **Line Group ID** is set to **6** matching the number of the **Outgoing Group** configured on the **SIP URI** tab of SIP Line 6 to Verizon Business (**Section 5.5.4**).



## 5.11. Save Configuration

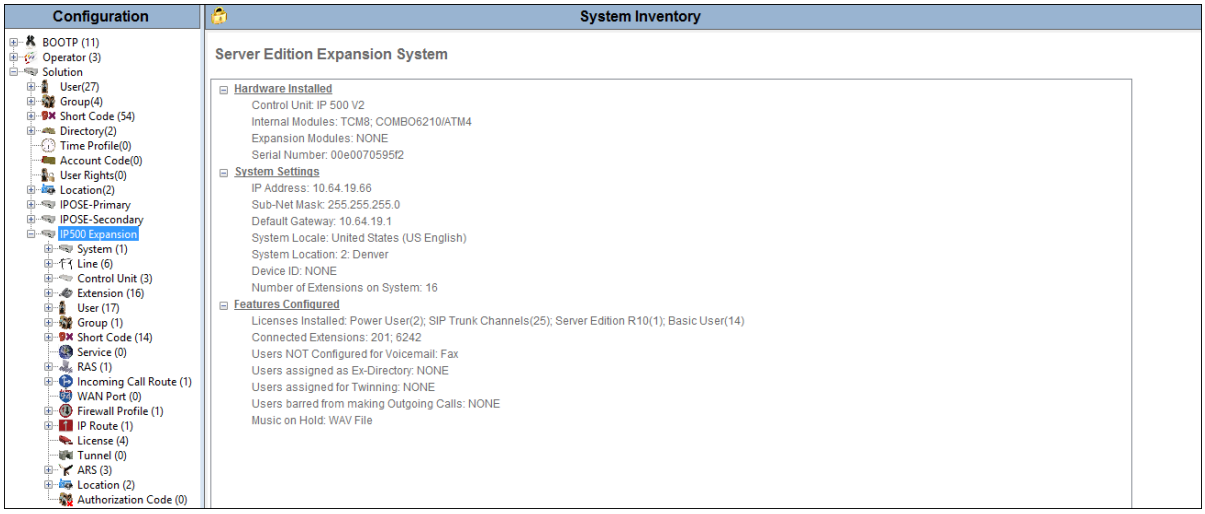
Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections.

The following will appear, with either **Merge** or **Reboot** selected for the **Change Mode**, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** if desired.



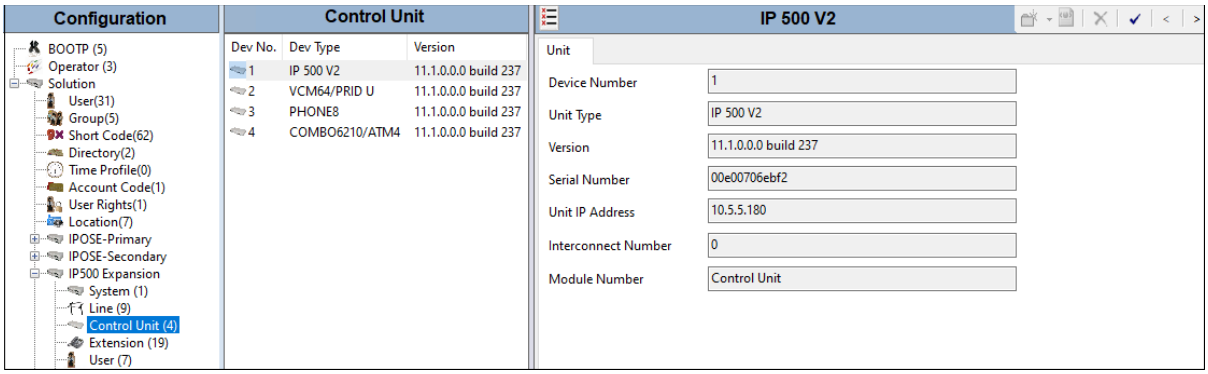
# 6. Avaya IP Office Expansion Configuration

Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the "plus" sign next to **IP500 Expansion** on the left navigation pane will expand the menu on this server.



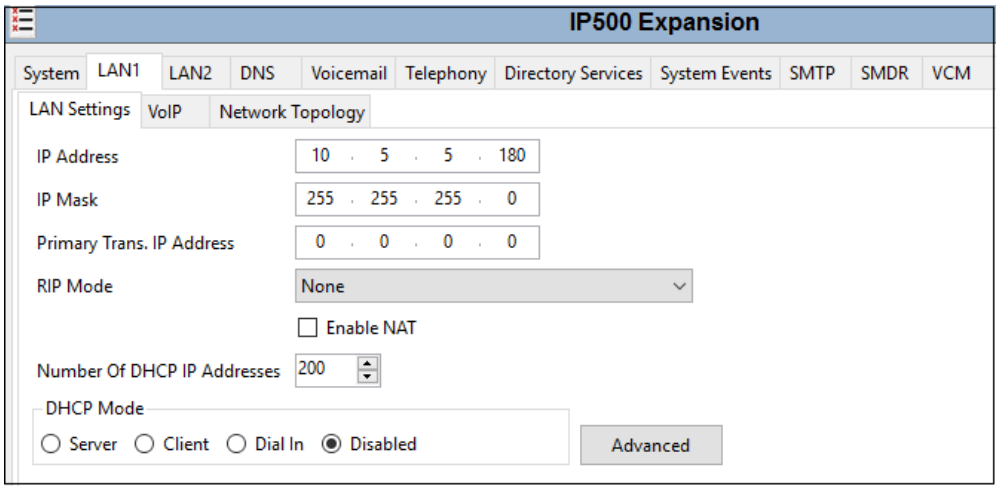

## 6.1. Expansion System - Physical Hardware

In the sample configuration, the IP500 V2 Expansion System contained a PHONE8 analog card and a COMBO6210 card, for the support of analog and digital stations. Also included is a VCM64 (Voice Compression Module). Both the VCM64 and the COMBO6210 cards provide voice compression channels to the control unit. Voice compression channels are needed to support VoIP calls, including IP extensions and or IP trunks.



## 6.2. Expansion System - LAN Settings

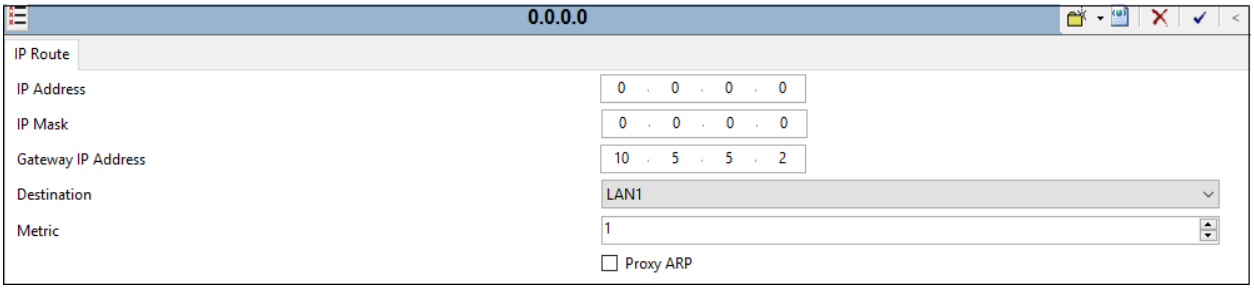
In the sample configuration, LAN1 is used to connect the Expansion System to the enterprise network. To view or configure the LAN1 IP address, select **System** on the Navigation pane. Select the **LAN1 → LAN Settings** tab on the Details pane. As shown in **Figure 1**, the IP Address of the Expansion System is **10.5.5.180**. Other parameters on this screen may be set according to customer requirements




Defaults were used on the **VoIP** and **Network Topology** tabs (not shown).

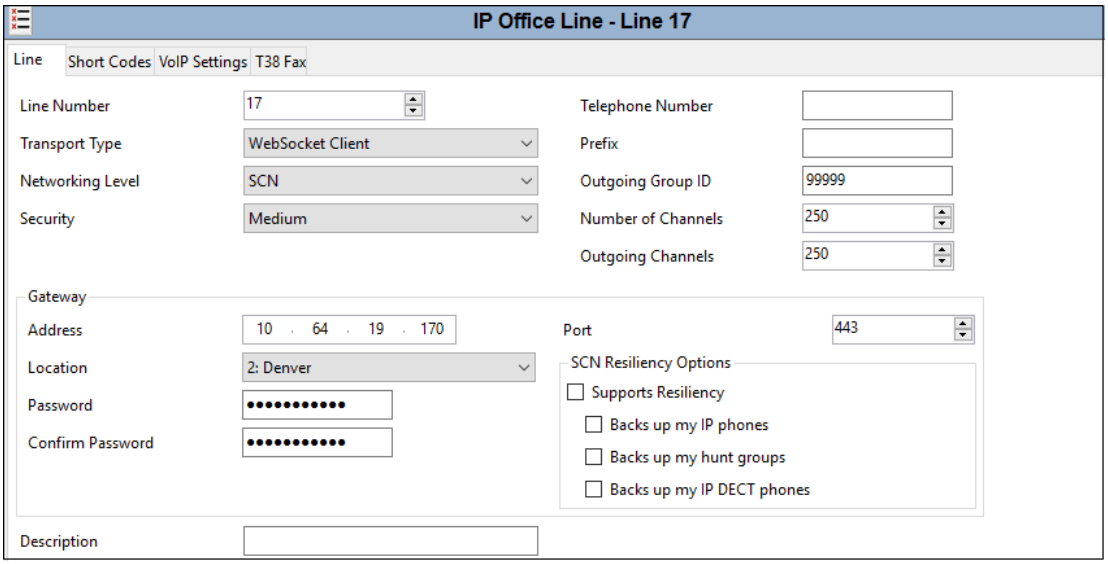
## 6.3. Expansion System - IP Route

To create an IP route for the Expansion System, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown). The configuration is similar to the one on the Primary server (**Section 5.4**), with the difference that in the reference configuration, the default gateway for the Expansion System is **10.5.5.2**

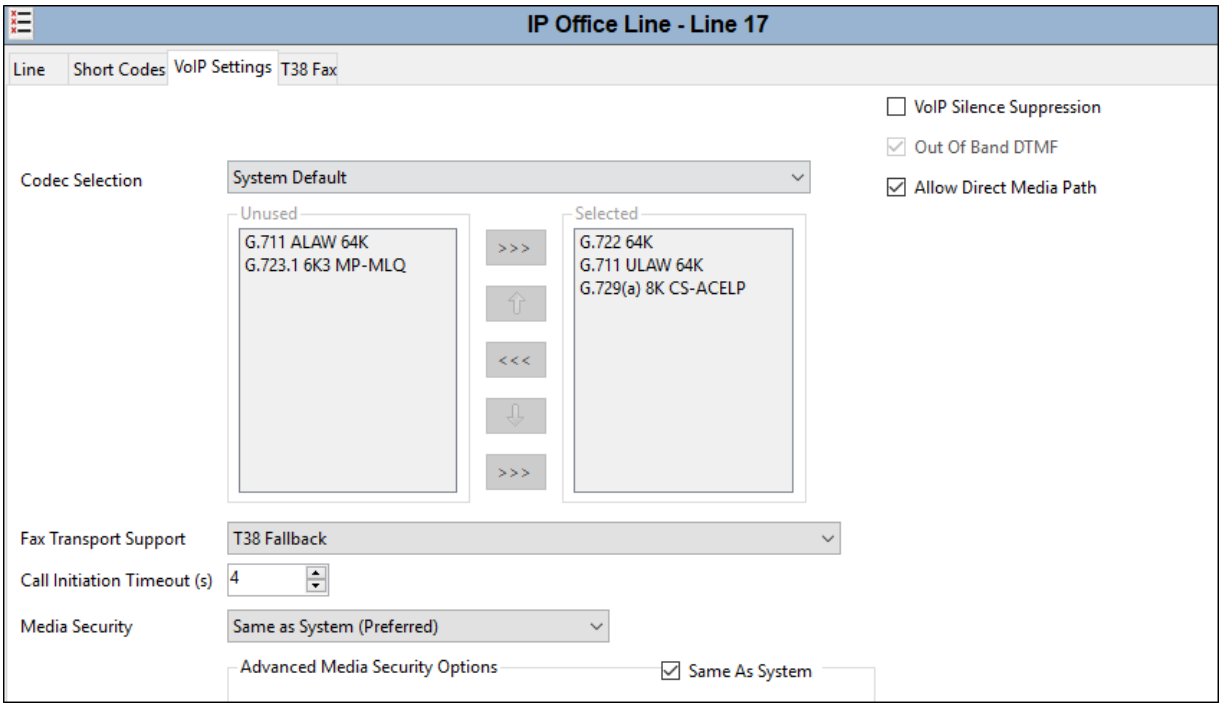


## 6.4. Expansion System - IP Office Line

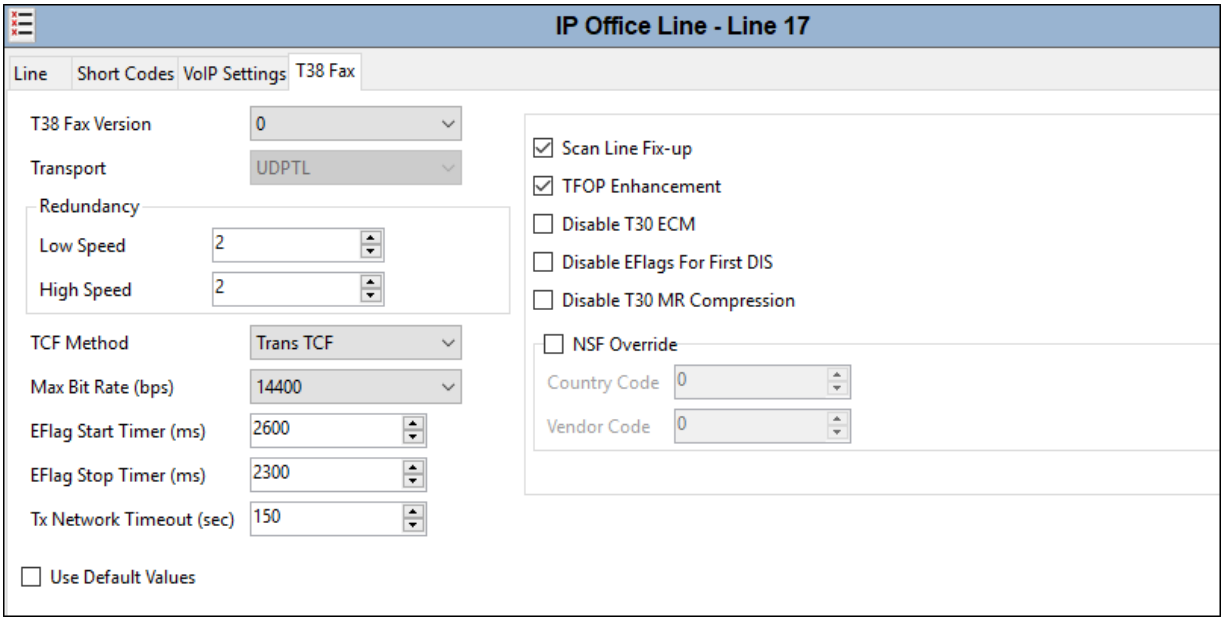
The IP Office Lines are automatically created on each server when the Expansion System is added to the solution. Below is the IP Office Line (**Line Number 17**) to the Primary server.




In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate T.38 fax, select the **VoIP Settings** tab and set **Fax Transport Support** to **T38 Fallback.** The **Media Security** drop-down menu is set to "**Same as System (Preferred)**" to have IP Office use the system setting for media security set in **Section 5.3.4** to encrypted RTP.

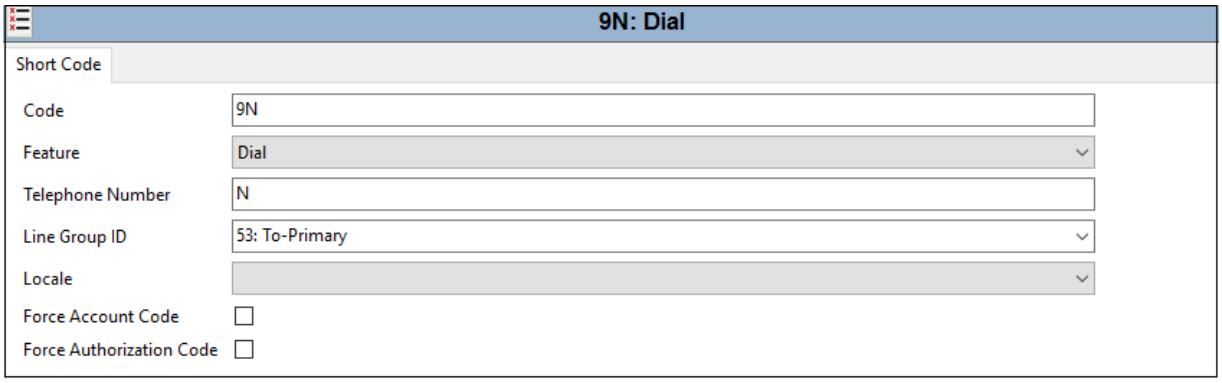


Select the **T38 Fax** tab. The **Use Default Values** box is unchecked, and the **T38 Fax Version** is set to **0**. In the **Redundancy** area, the **Low Speed** and **High Speed** parameters are set to **2**. All other values are left at default.



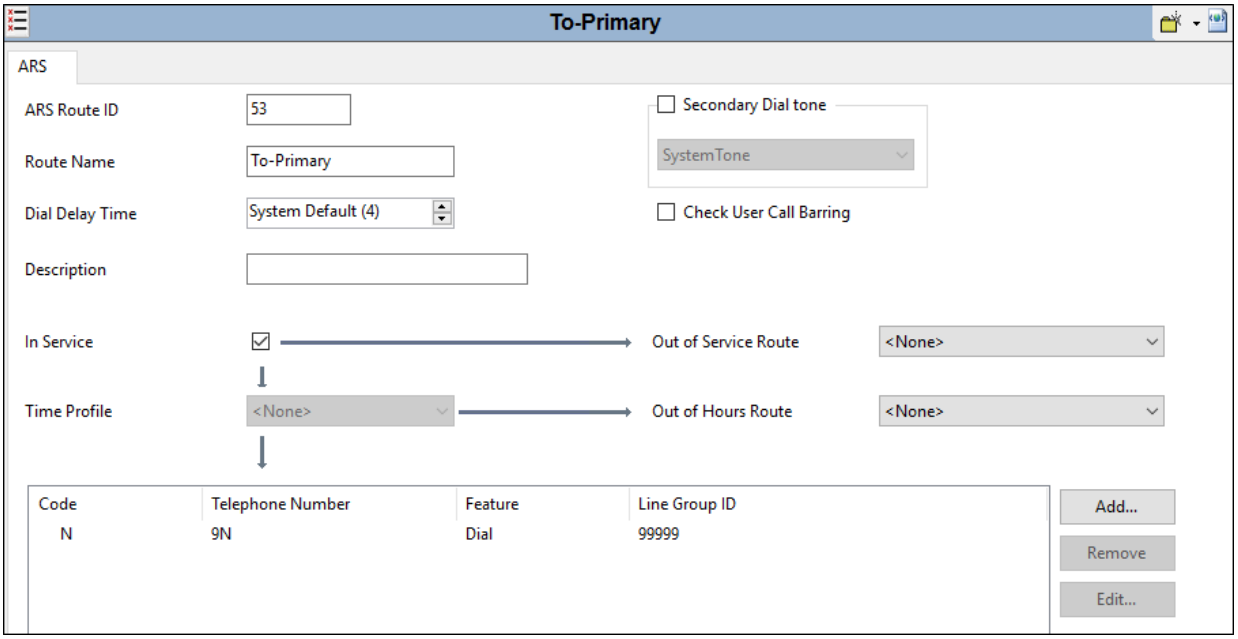

## 6.5. Expansion System - Short Codes

Similar to the configuration of the Primary server in **Section 5.7**, a Short Code is created to access ARS. In the reference configuration, the **Line Group ID** is set to an ARS route illustrated in the next section.



## 6.6. Expansion System - Automatic Route Selection – ARS

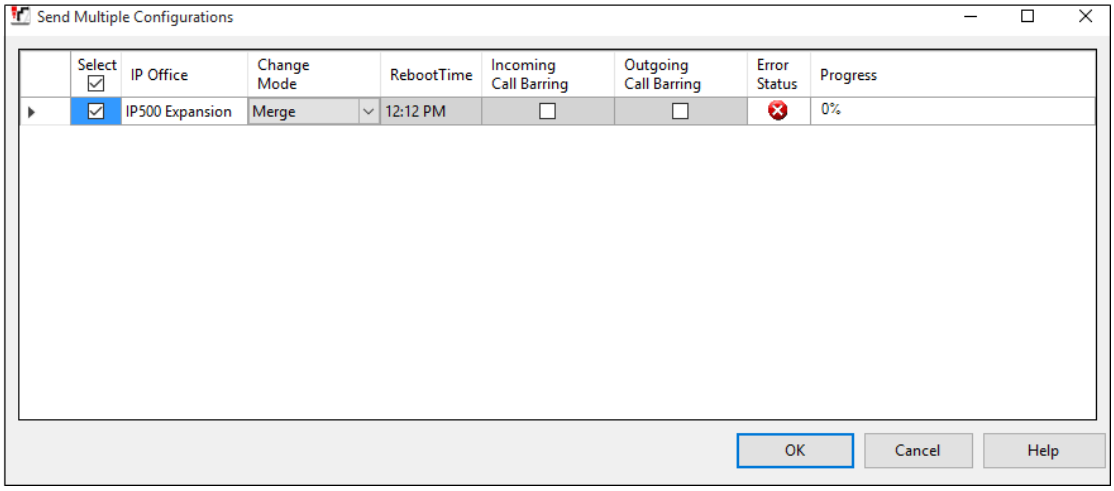
The following screen shows an example ARS configuration for the route named **To-Primary** on the Expansion System. The **Telephone Number** is set to **9N**. The **Line Group ID** is set to **99999** matching the number of the **Outgoing Group ID** configured on the IP Office Line 17 to the Primary server (**Section 6.4**).




## 6.7. Save IP Office Expansion System Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections

The following will appear, with either **Merge** or **Reboot** selected, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to proceed.



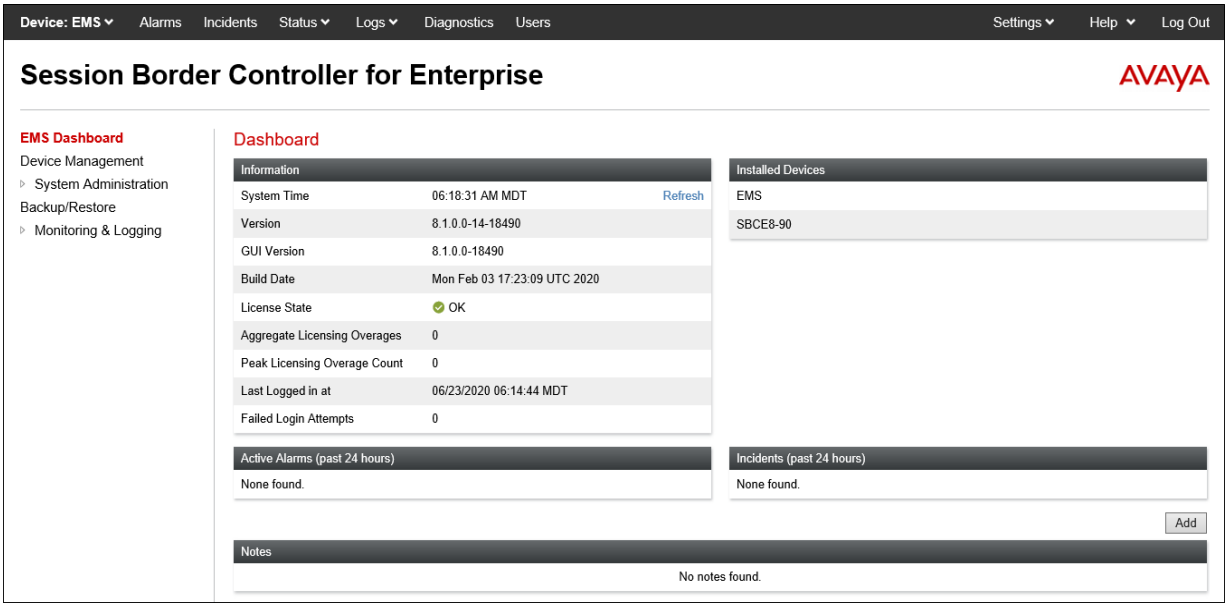
# 7. Configure Avaya Session Border Controller for Enterprise

In the reference configuration, Avaya SBCE is used as an edge device between the CPE and Verizon Business.

This section covers the configuration of the Avaya SBCE. It is assumed that the initial provisioning of the Avaya SBCE, including the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

Use a web browser to access the Element Management Server (EMS) web interface and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE. Log in using the appropriate credentials.

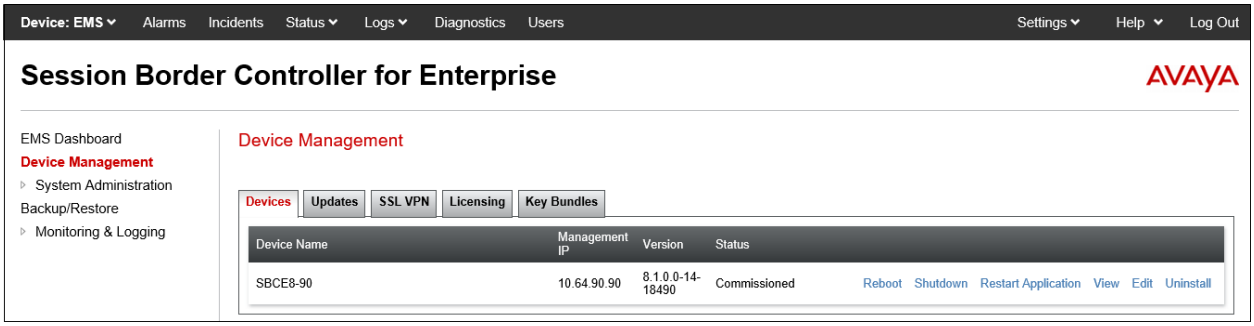
The EMS Dashboard page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is **"OK"**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.



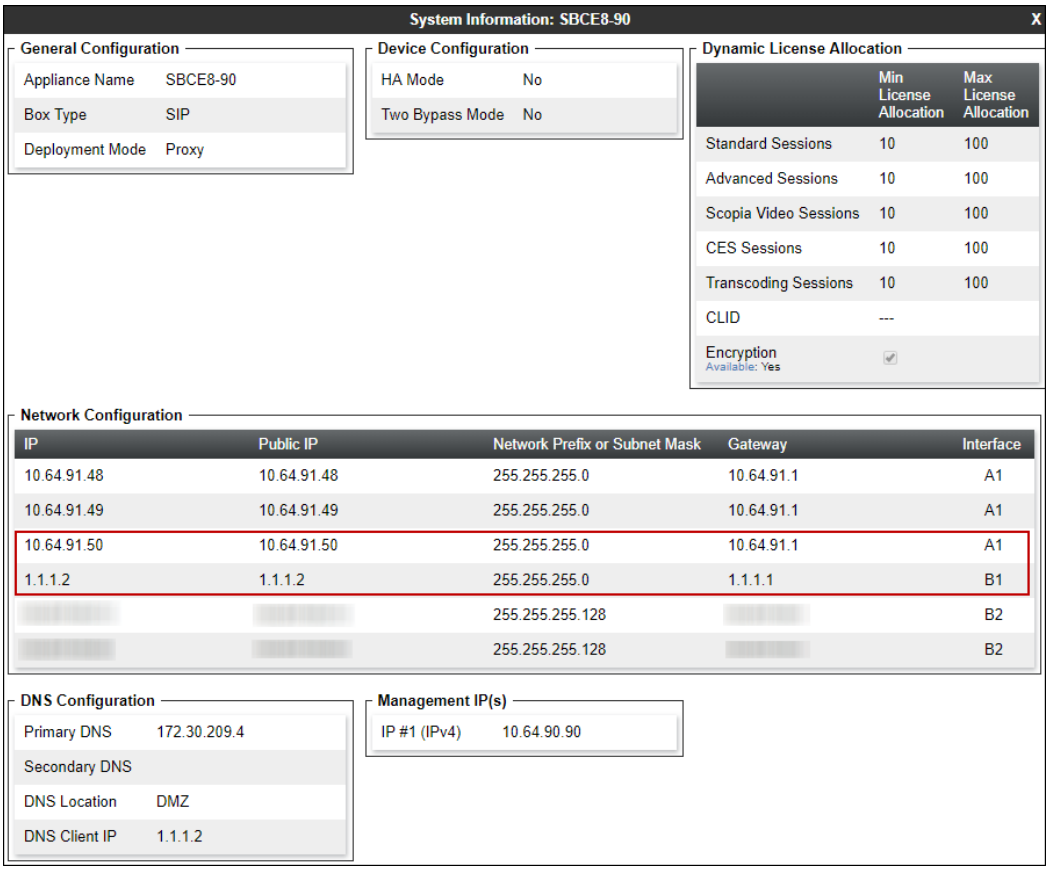

## 7.1. Device Management – Status

Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **SBCE8-90** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya representative. To view the configuration of this device, click **View** on the screen below.

> **Note** – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.



The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation, corresponding to **Figure 1**. In the shared test environment, the highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Verizon. Other IP addresses assigned to interfaces **A1** and **B2** on the screen below are used to support remote workers and are not the focus of these Application Notes. Note that the **Management IP** must be on a separate subnet from the IP interfaces designated for SIP traffic.



System Information: SBCE8-90

General Configuration

| | |
|---|---|
| Appliance Name | SBCE8-90 |
| Box Type | SIP |
| Deployment Mode | Proxy |

Device Configuration

| | |
|---|---|
| HA Mode | No |
| Two Bypass Mode | No |

Dynamic License Allocation

| | Min License Allocation | Max License Allocation |
|---|---|---|
| Standard Sessions | 10 | 100 |
| Advanced Sessions | 10 | 100 |
| Scopia Video Sessions | 10 | 100 |
| CES Sessions | 10 | 100 |
| Transcoding Sessions | 10 | 100 |
| CLID | --- | |
| Encryption Available: Yes | ✓ | |

Network Configuration

| IP | Public IP | Network Prefix or Subnet Mask | Gateway | Interface |
|---|---|---|---|---|
| 10.64.91.48 | 10.64.91.48 | 255.255.255.0 | 10.64.91.1 | A1 |
| 10.64.91.49 | 10.64.91.49 | 255.255.255.0 | 10.64.91.1 | A1 |
| 10.64.91.50 | 10.64.91.50 | 255.255.255.0 | 10.64.91.1 | A1 |
| 1.1.1.2 | 1.1.1.2 | 255.255.255.0 | 1.1.1.1 | B1 |
| [illegible] | [illegible] | 255.255.255.128 | [illegible] | B2 |
| [illegible] | [illegible] | 255.255.255.128 | [illegible] | B2 |

DNS Configuration

| | |
|---|---|
| Primary DNS | 172.30.209.4 |
| Secondary DNS | |
| DNS Location | DMZ |
| DNS Client IP | 1.1.1.2 |

Management IP(s)

| | |
|---|---|
| IP #1 (IPv4) | 10.64.90.90 |

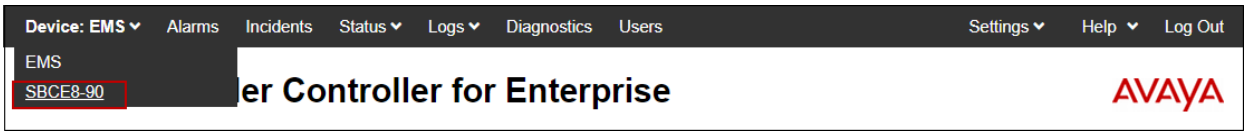
## 7.2. TLS Management

**Note** – Testing was done using identity certificates signed by a local certificate authority. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between IP Office and Avaya SBCE. The following procedures show how to view the certificates and configure the profiles to support the TLS connection.

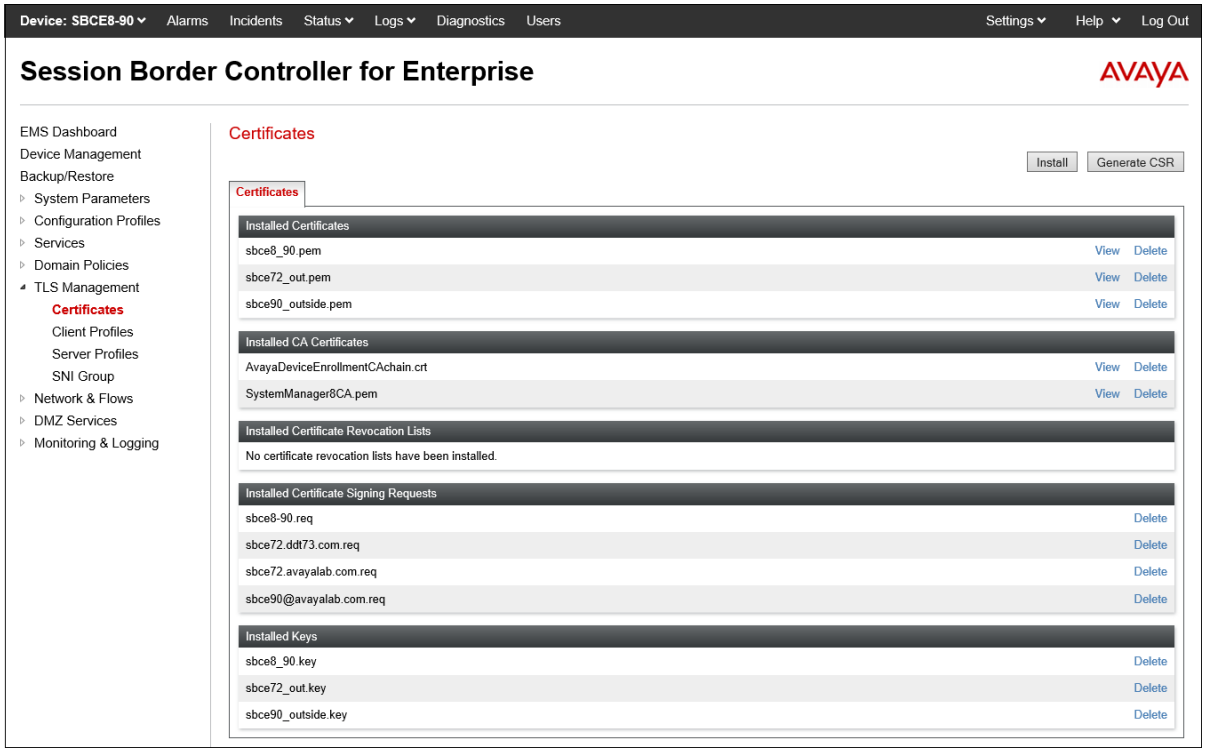
### 7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.



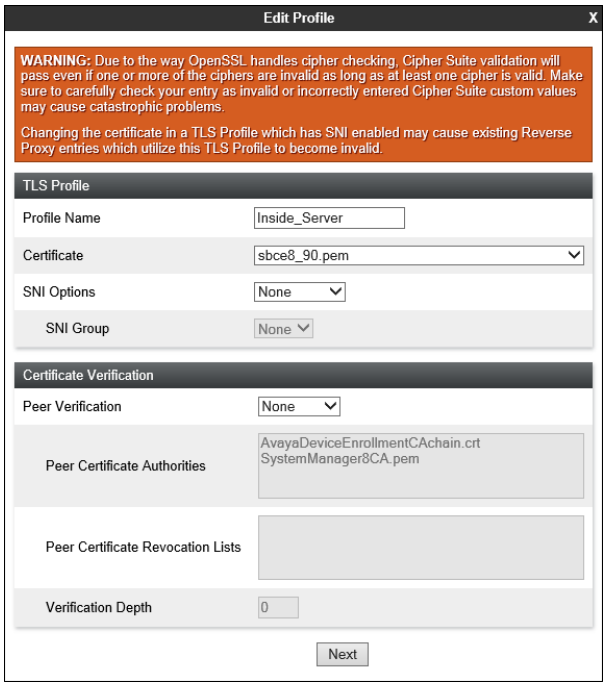

**Note** – The provisioning described in the following sections use the menu options listed in the left-hand column shown below.

Select **TLS Management → Certificates** from the left-hand menu. Verify the root CA certificate is present in the **Installed CA Certificates** area. The signed identity certificate is present in the **Installed Certificates** area. The private key associated with the identity certificate is present in the **Installed Keys** area.

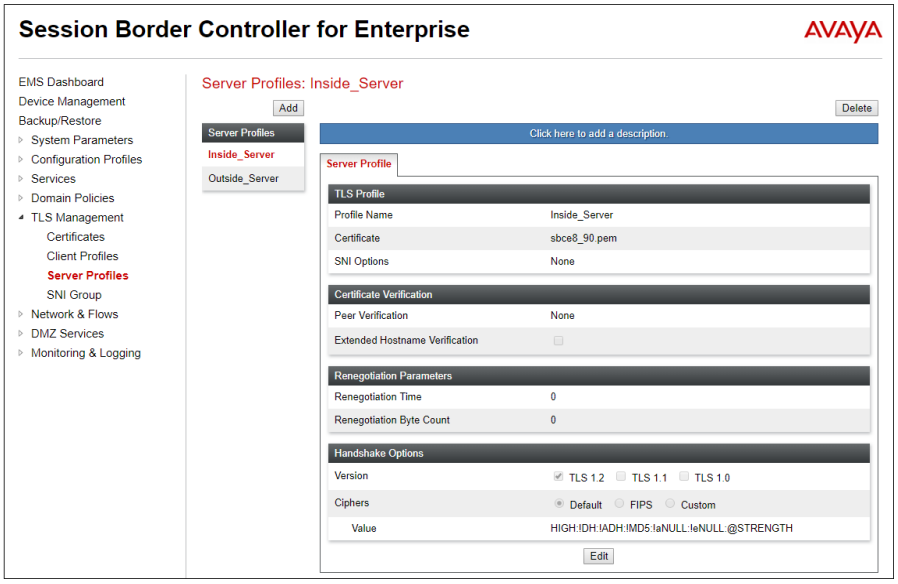


### 7.2.2. Server Profiles

Navigate to **TLS Management → Server Profiles** and click the **Add** button to add a new profile or select an existing profile. Enter a descriptive **Profile Name** such as **Inside_Server** show below. Select the Avaya SBCE identity certificate for the inside interface from the **Certificate** drop-down menu. In the reference configuration this is **sbce8_90.pem**. Select **None** from the **Peer Verification** drop-down menu. Click **Next** and accept default values for the next screen, then click **Finish** (not shown).

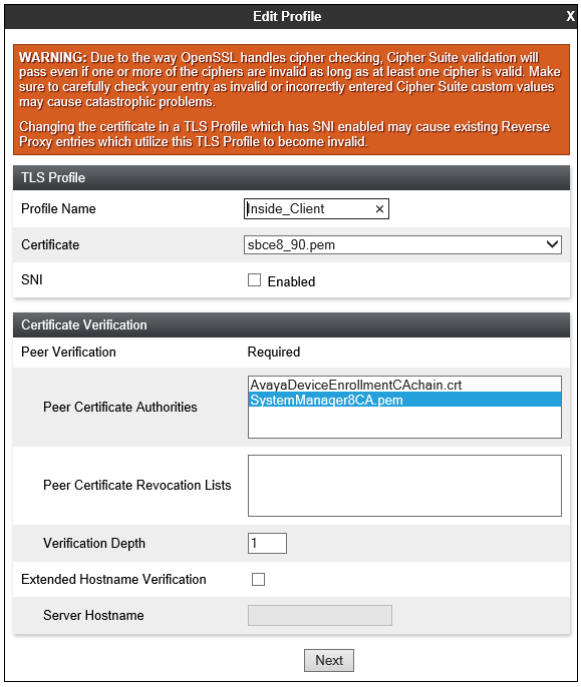



The following screen shows the completed TLS **Server Profile** form:

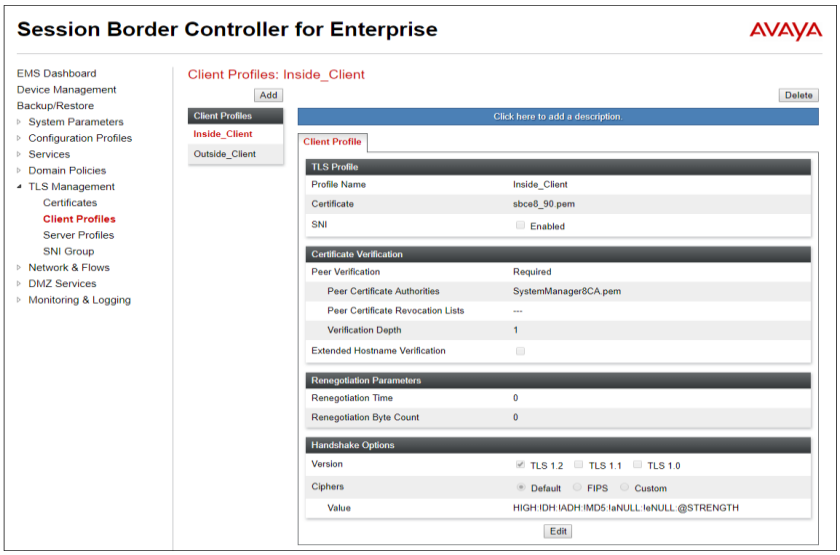


### 7.2.3. Client Profiles

Navigate to **TLS Management → Client Profiles** and click the **Add** button to add a new profile or select an existing profile. Enter a descriptive **Profile Name**, such as **Inside_Client** show below. Select the identity certificate from the **Certificate** drop-down menu. In the reference configuration this is **sbce8_90.pem**. The **Peer Certificate Authorities** field is set to the root certificate used to verify the IP Office certificate, e.g., **SystemManager8CA.pem**. The **Verification Depth** field is set to **1**. Click **Next** and accept default values for the next screen and click **Finish** (not shown).

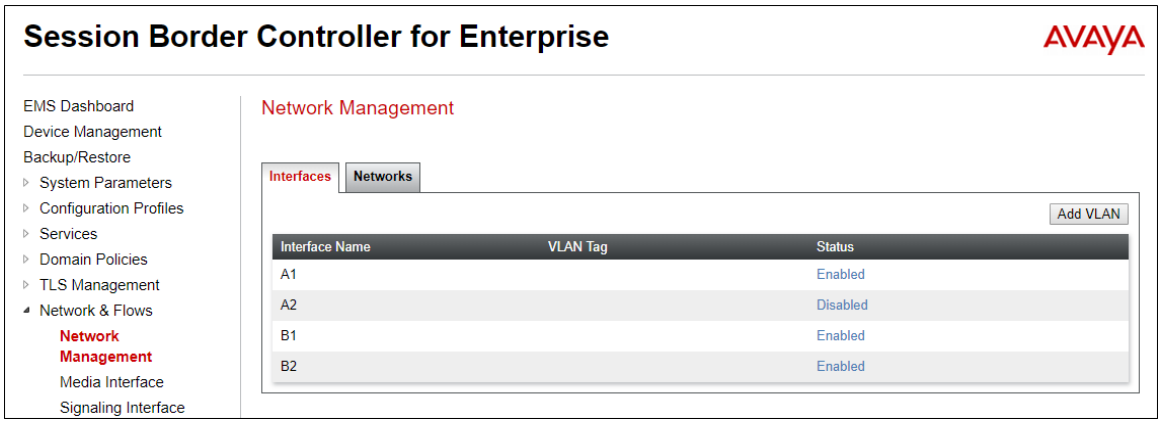



The following screen shows the completed TLS **Client Profile** form:



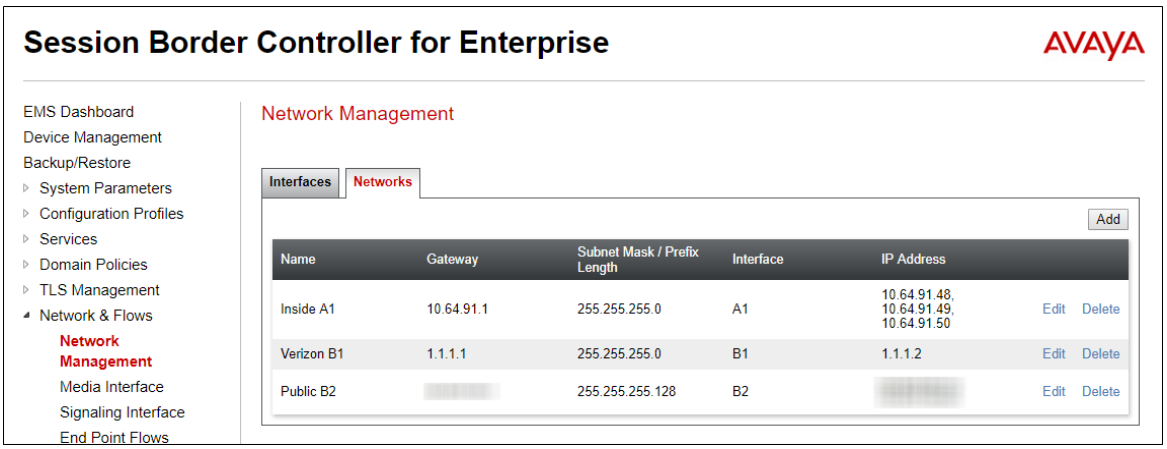
## 7.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Networks & Flows → Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 and B1 are used.




Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however, some of these values may not be changed if associated provisioning is in use.

- **A1**: **10.64.91.50** – "Inside" IP address, toward IP Office.
- **B1: 1.1.1.2** – "Outside" IP address toward the Verizon SIP trunk. This address is known to Verizon and is associated with the FQDN *adevc.avaya.globalipcom.com*.

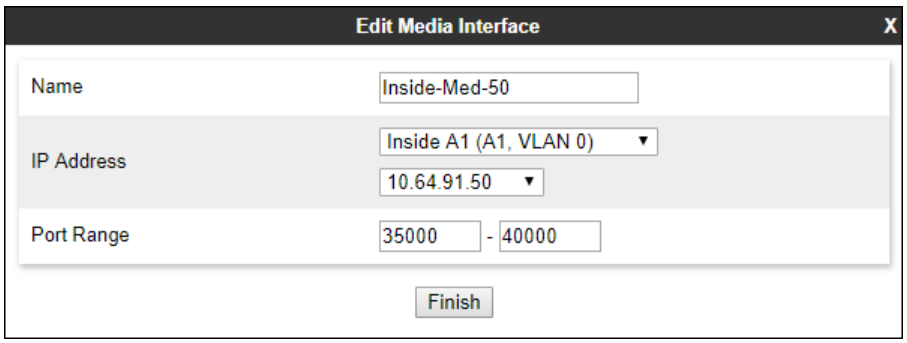


## 7.4. Media Interfaces

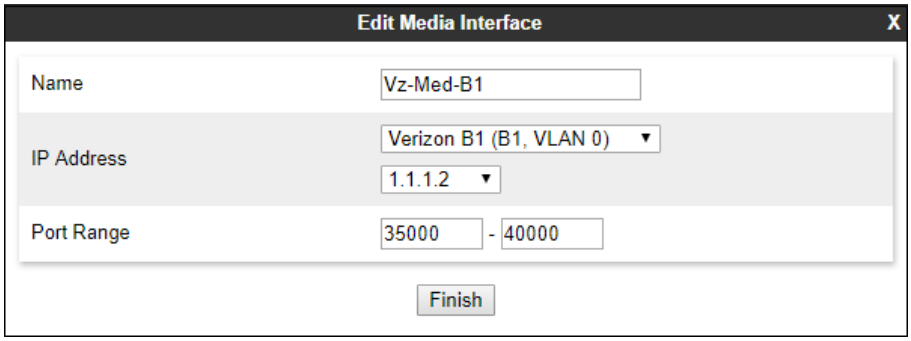
Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server. Create a SIP Media Interface for both the inside and outside IP interfaces.

To create a new Media Interface, navigate to Select **Network & Flows → Media Interface** from the menu on the left-hand side and select **Add** (not shown).

The screen below shows the **Inside-Med-50** Media Interface created toward the IP Office. On the **IP Address** drop-down menus, **Inside-A1 (A1,VLAN0)** and **10.64.91.50** are selected. Default **Port Range** values are used.




The screen below shows the **Vz-Med-B1** Media Interface created toward Verizon. On the **IP Address** drop-down menus, **Verizon-B1 (B1,VLAN0)** and **1.1.1.2** are selected. Default **Port Range** values are used.

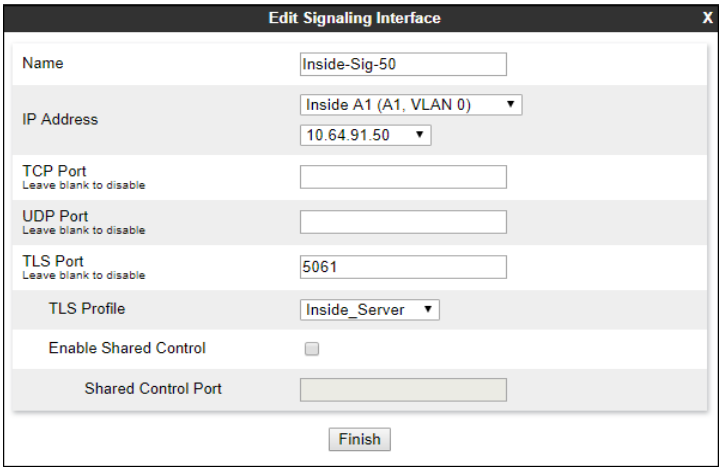


## 7.5. Signaling Interfaces

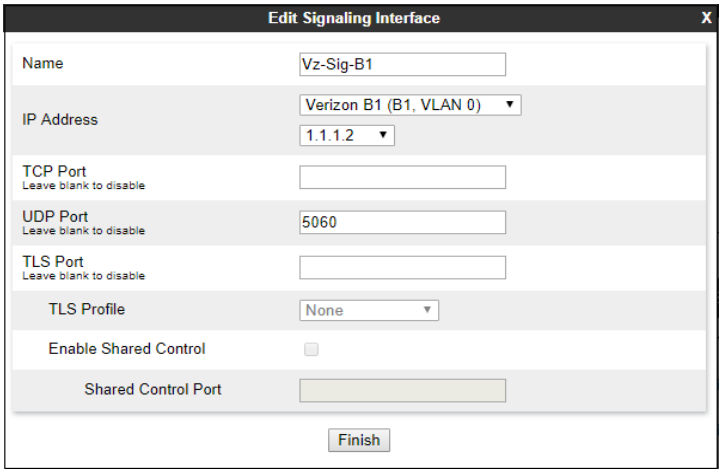
The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to Select **Network & Flows → Media Interface** from the menu on the left-hand side and select **Add** (not shown).

The screen below shows the **Inside-Sig-50** Signaling Interface created toward the IP Office. On the **IP Address** drop-down menus, **Inside-A1 (A1,VLAN0)** and **10.64.91.50** are selected. **TLS Port 5061** is used. The TLS server profile created in **Section 7.2.2** (e.g., **Inside_Server**) is selected on the TLS Profile drop-down menu.




The screen below shows the **Vz-Sig-B1** Signaling Interface created toward Verizon. On the **IP Address** drop-down menus, **Verizon-B1 (B1,VLAN0)** and **1.1.1.2** are selected. **UDP Port 5060** is used.



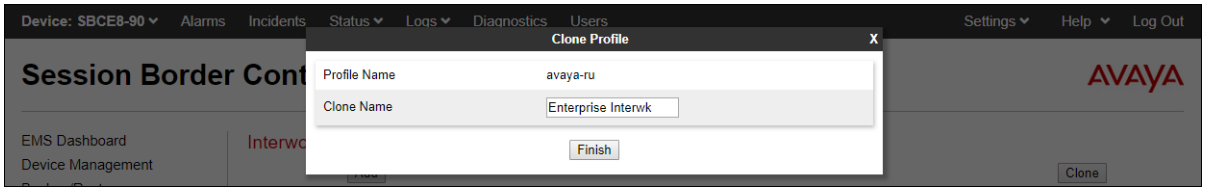
## 7.6. Server Interworking Profile

The Server Internetworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

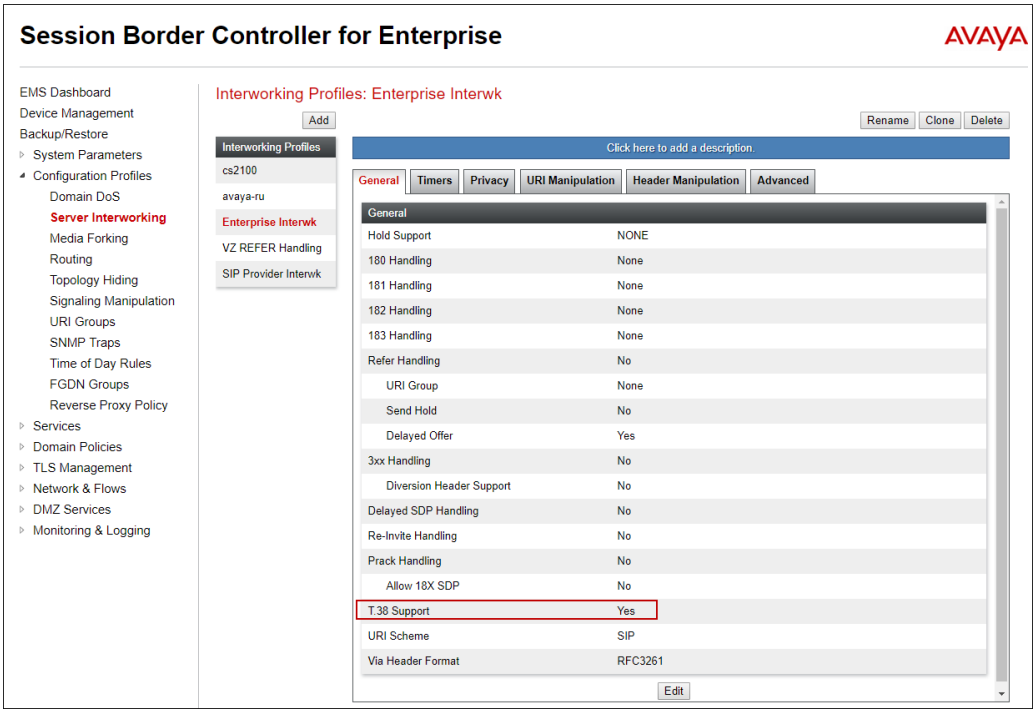
In the reference configuration, separate Server Interworking Profiles were created for IP Office and Verizon Business IP Trunking service.

### 7.6.1. Server Interworking Profile – IP Office

In the reference configuration, the IP Office Server Interworking profile was cloned from the default **avaya-ru** profile. To clone a Server Interworking Profile for IP Office, navigate to **Configuration Profiles → Server Interworking**, select the **avayu-ru** profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.

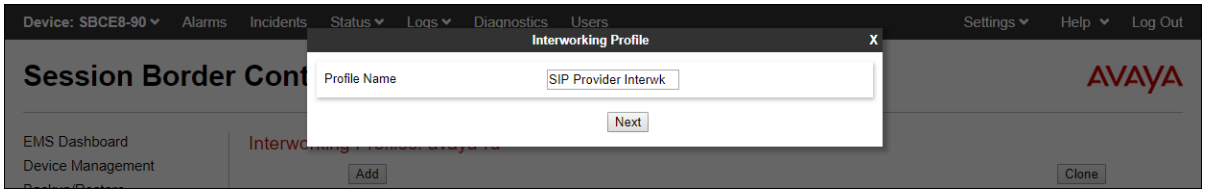



The following screen shows the **Enterprise Interwk** profile used in the reference configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish** (not shown). Default values can be used for all other fields.

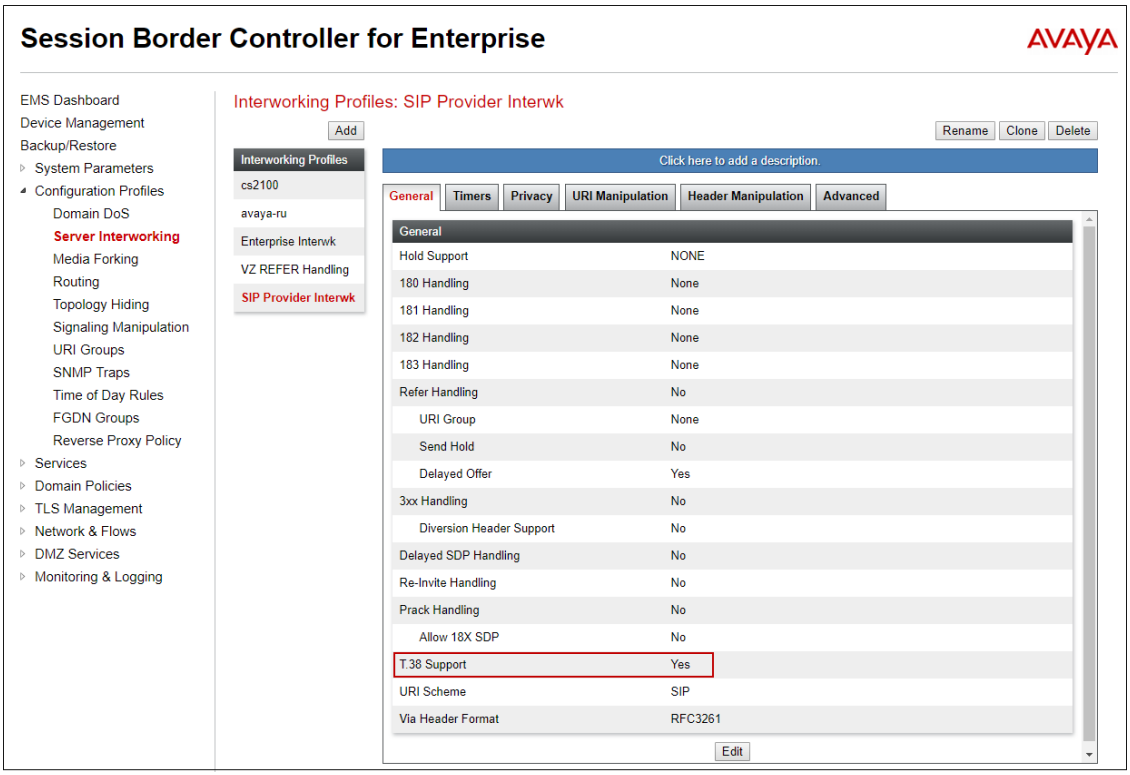


## 7.6.2. Server Interworking Profile – Verizon

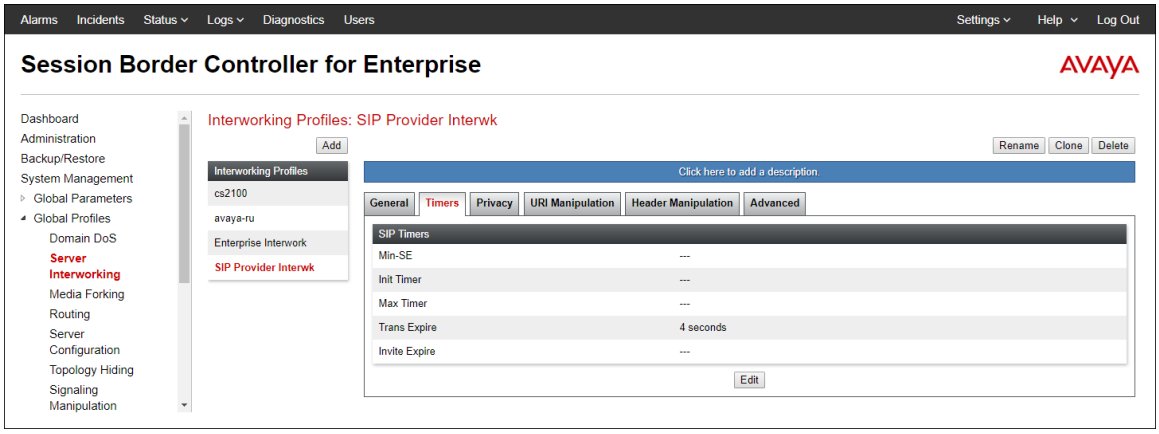
To create a new Server Interworking Profile for Verizon, navigate to **Configuration Profiles → Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**.



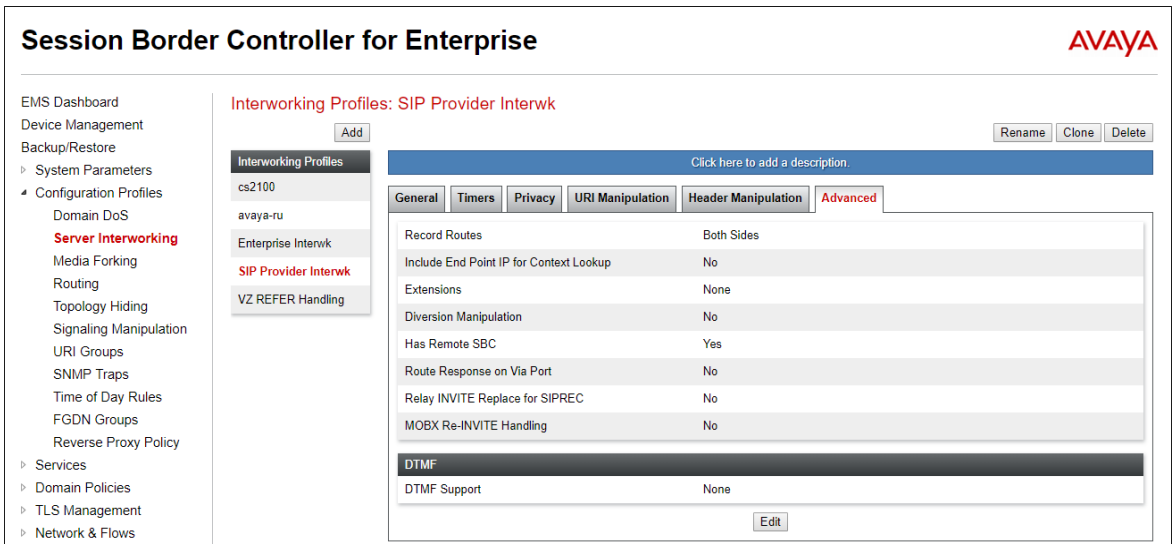

The following screens show the **SIP Provider Interwk** profile used in the reference configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to **Yes**.



The **Timers** tab shows the values used for compliance testing for the **Trans Expire** field. The **Trans Expire** timer sets the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if one exists.




Default parameters were used for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown). On the **Advanced** tab, **Record Routes** is set to **Both Sides**. Default values can be used for all other fields.

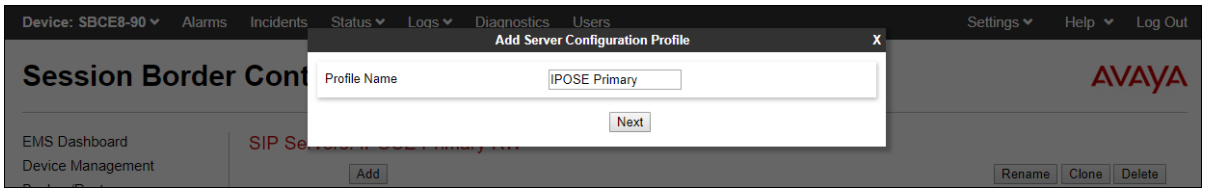


## 7.7. SIP Server Profiles

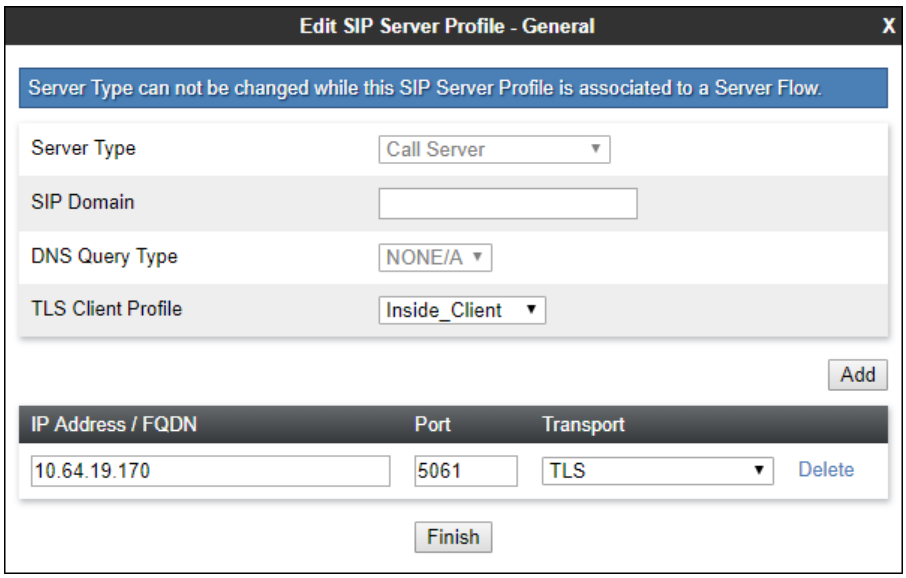
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

### 7.7.1. SIP Server Profile – IP Office

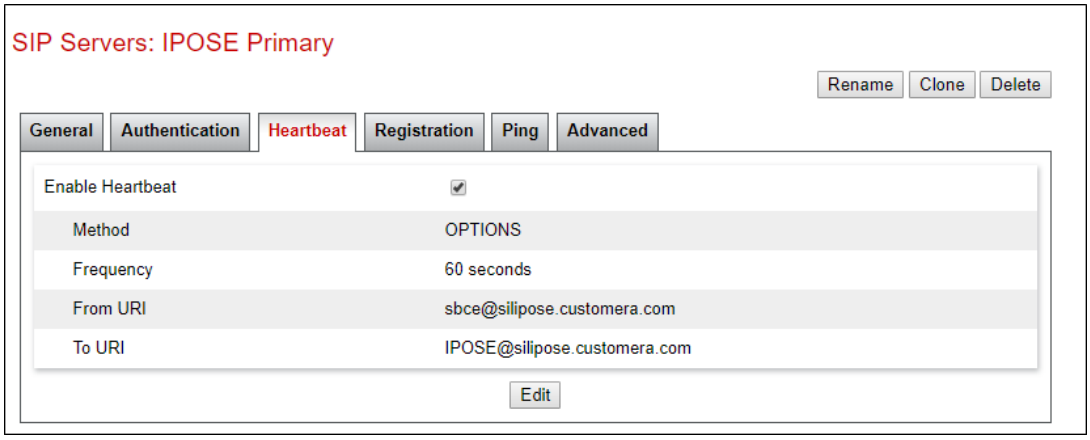
To add a SIP Server Profile for IP Office, navigate to **Services → SIP Servers** on the left-hand menu and click **Add**. Enter a descriptive name for the new profile and click **Next**.



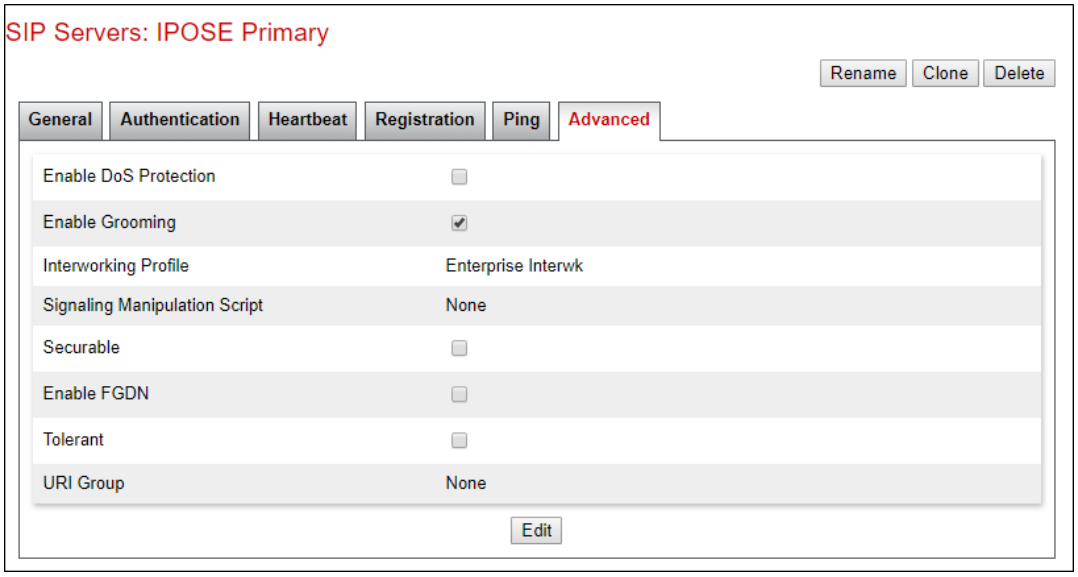

The following screen illustrate the SIP Server Profile named **IPOSE Primary**. In the **General** parameters, the **Server Type** is set to **Call Server**. In the **IP Address / FQDN** field, the IP Address of IP Office LAN 1 interface in the sample configuration is entered. This IP address is **10.64.19.170**. Under **Port**, **5061** is entered, and the **Transport** parameter is set to **TLS**. The TLS profile **Inside_Client** created in **Section 7.2.3** is selected for **TLS Client Profile**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source "heartbeats" in the form of PINGs or SIP OPTIONS towards IP Office. Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE.

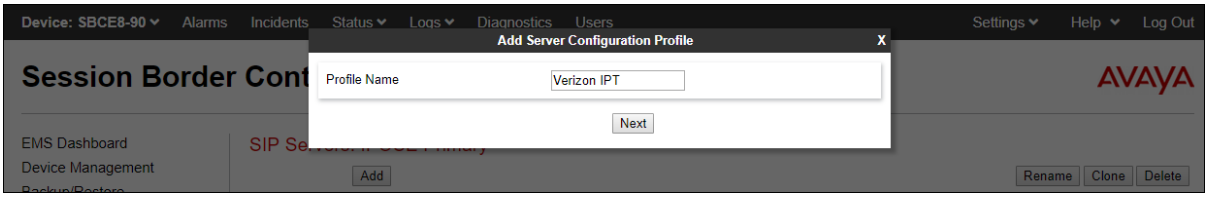



On the **Advanced** tab, select the **Enable Grooming** checkbox. The **Interworking Profile** is set to the **Enterprise Interwk** profile created in **Section 7.6.1** for IP Office.

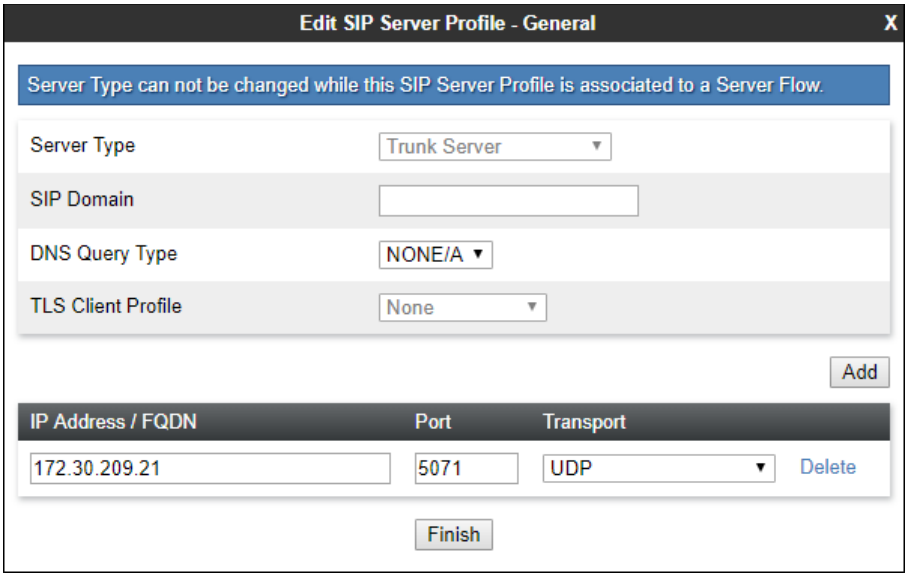


### 7.7.2. SIP Server Profile - Verizon

To add a SIP Server Profile for Verizon, navigate to **Services → SIP Servers** and click **Add**. Enter a descriptive name for the new profile and click **Next**.

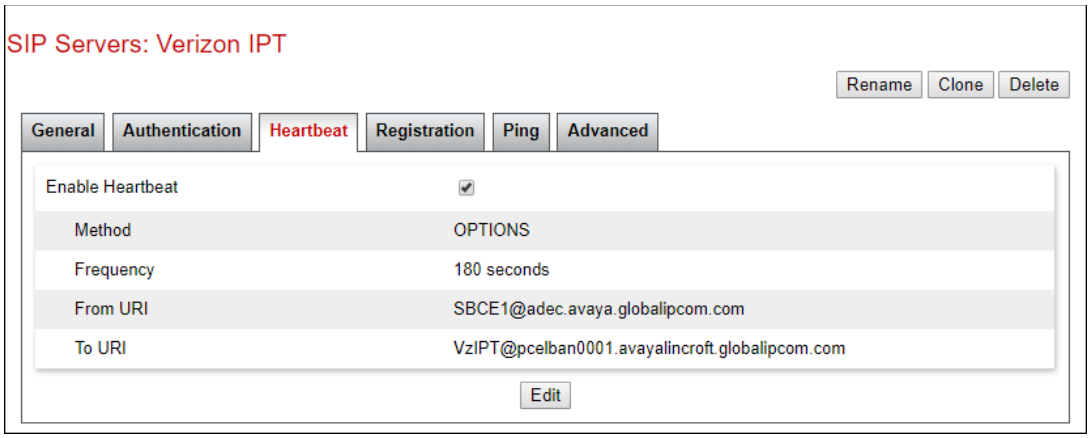



The following screens illustrate the SIP Server Profile named **Verizon IPT**. In the **General** parameters, the **Server Type** is set to **Trunk Server**. The **DNS Query Type** is set to **NONE/A**. In the **IP Address / FQDN** field, the Verizon-provided IP address is entered. This is **172.30.209.21**. Under **Port**, **5071** is entered, and the **Transport** parameter is set to **UDP**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

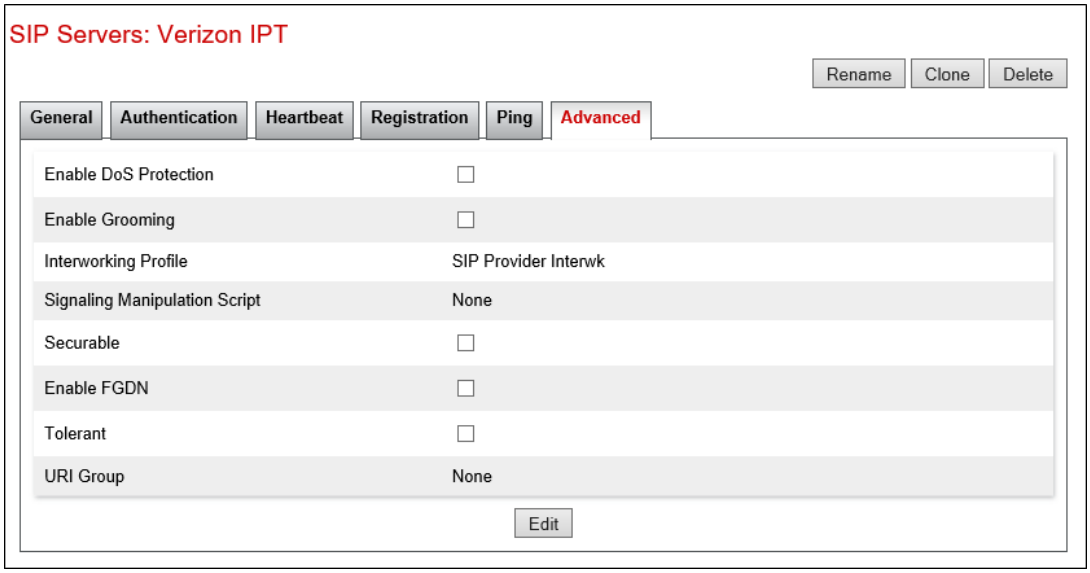



Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source "heartbeats" in the form of SIP OPTIONS towards Verizon. This configuration is optional. Independent of whether the Avaya SBCE is configured to source SIP OPTIONS towards Verizon, Verizon will receive OPTIONS from the IP Office site as a result of the **Check OOS** parameter being enabled on IP Office (see **Section 5.5.2**). When IP Office sends SIP OPTIONS to the inside private IP Address of the Avaya SBCE, the Avaya SBCE will forward the SIP OPTIONS to Verizon. When Verizon responds, the Avaya SBCE will pass the response to IP Office.

Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE.




On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and is left unchecked. The **Interworking Profile** is set to **SIP Provider Interwk** created in **Section 7.6.2** for Verizon.

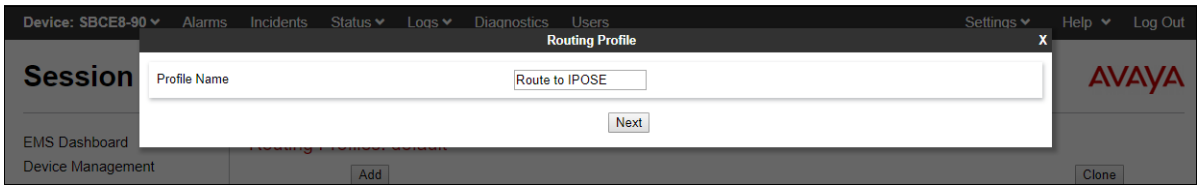


## 7.8. Routing Profiles

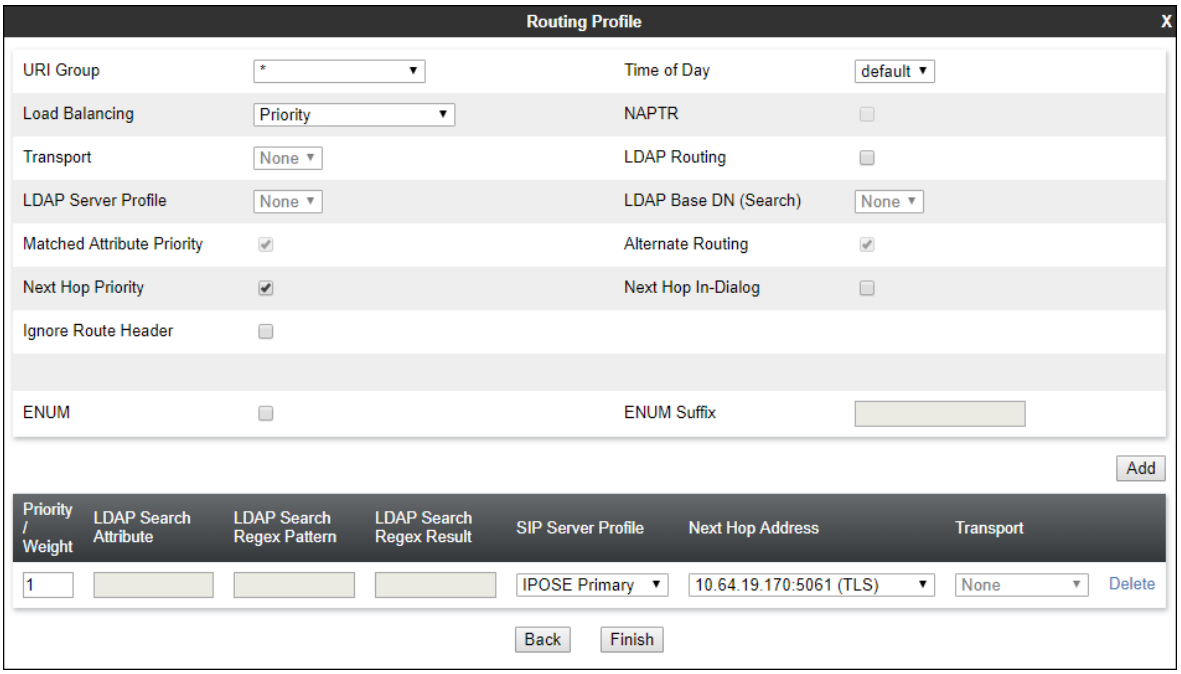
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

### 7.8.1. Routing Profile – IP Office

To add a routing profile for the IP Office, navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.

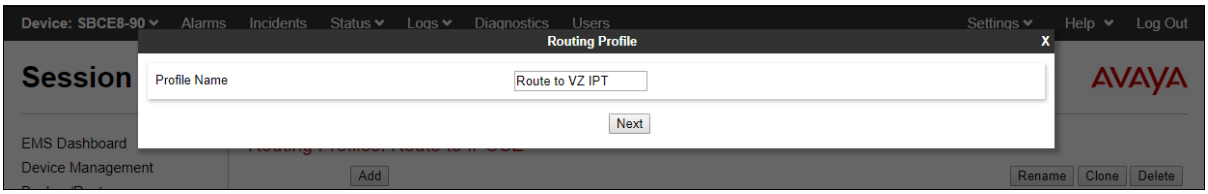



The following screen shows the Routing Profile R**oute to IPOSE** created in the reference configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the IP Office **SIP Server Profile**, created in **Section 7.7.1**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.

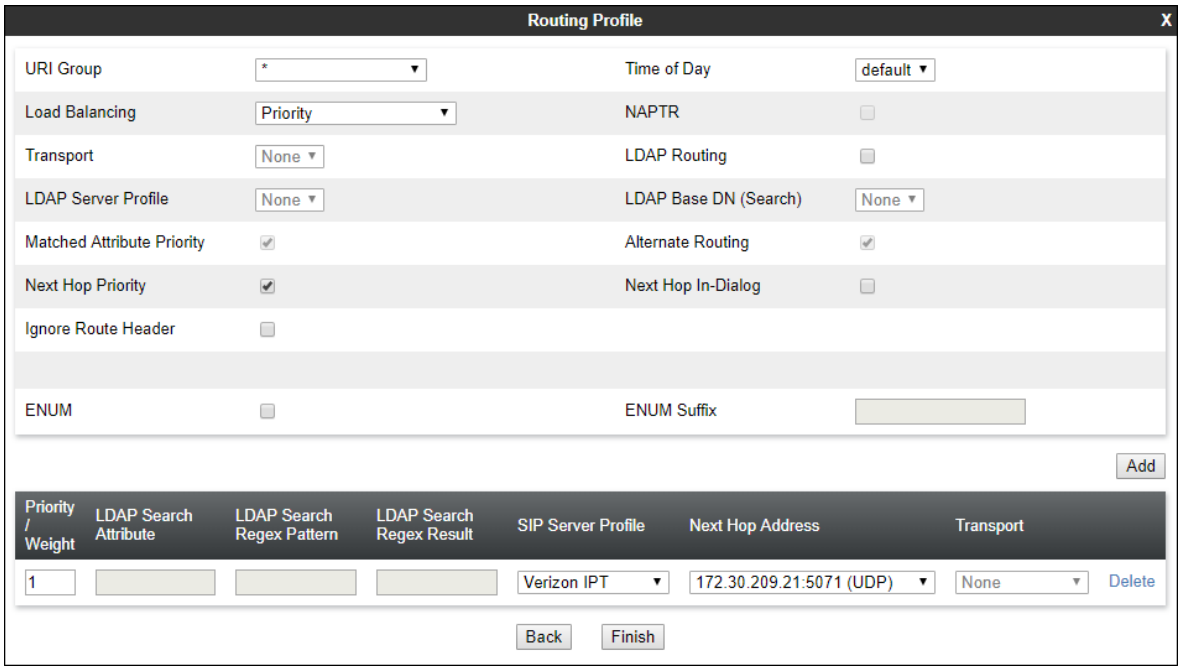


## 7.8.2. Routing Profile – Verizon

Similarly add a Routing Profile to Verizon Business IP Trunking.




The following screen shows the Routing Profile R**oute to Vz IPT** created in the reference configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to **1**, and the Verizon **SIP Server Profile**, created in **Section 7.7.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the SIP Server Profile, and **Transport** becomes greyed out. Click **Finish**.



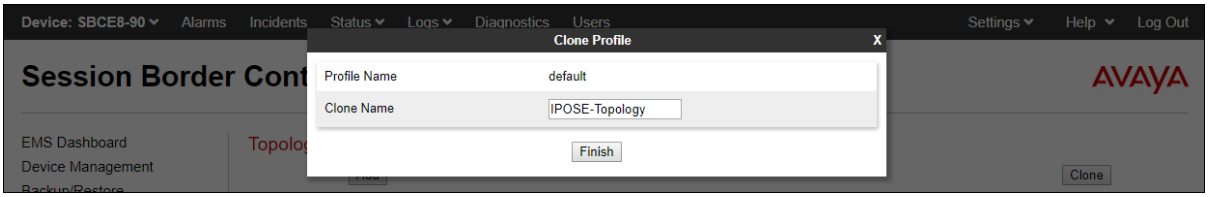
## 7.9. Topology Hiding Profile

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.

Topology Hiding can also be used as an interoperability tool to adapt the host portion of the SIP headers, to the IP addresses or domains expected on the service provider and the enterprise networks.

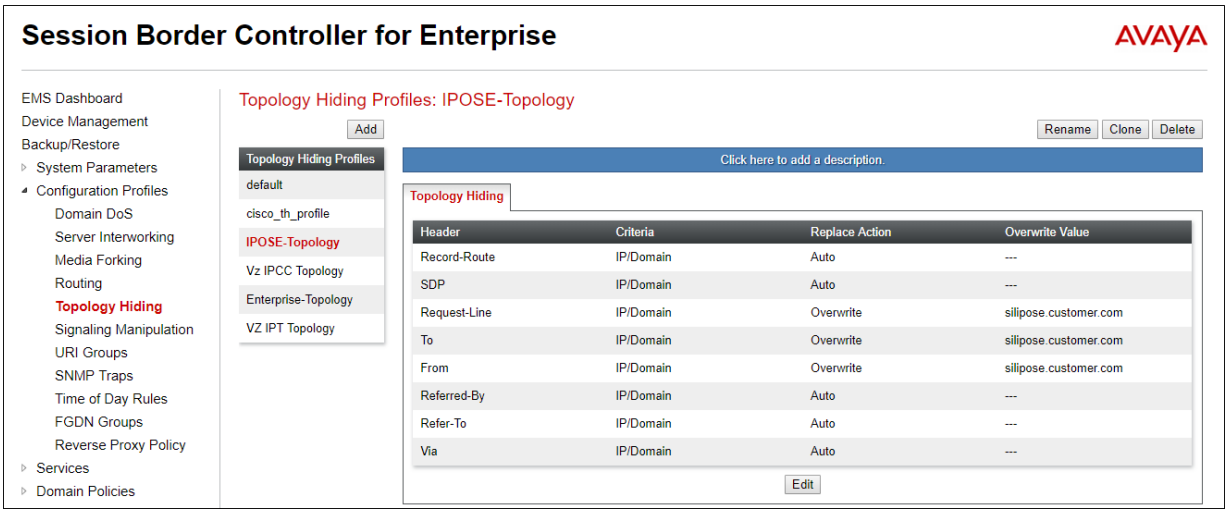
### 7.9.1. Topology Hiding – IP Office

In the sample configuration, the IP Office Topology Hiding profile was cloned from the **default** profile and then modified. Select **Configuration Profiles → Topology Hiding** from the left-hand menu. Select the pre-defined **default** profile and click the **Clone** button. Enter profile name (e.g., **IPOSE-Topology**) and click **Finish** to continue.



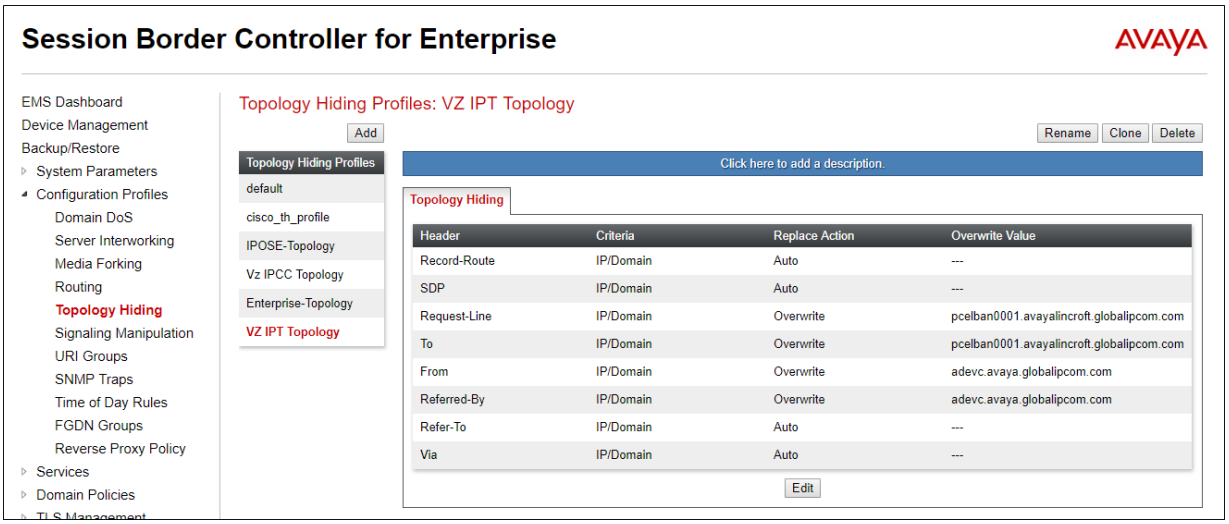

On the newly created profile, in the **Replace Action** column, an action of **Auto** will replace the header field with the IP address of the Avaya SBCE interface, while **Overwrite** will use the value in the **Overwrite Value**.

The screen below shows the **IPOSE-Topology** used in the reference configuration. For the **Request-Line**, **To** and **From** headers, **Overwrite** is selected under the **Replace Action** column. The domain of the enterprise (e.g., **silipose.customer.com**) is entered on the **Overwrite Value** field.



### 7.9.2. Topology Hiding – Verizon

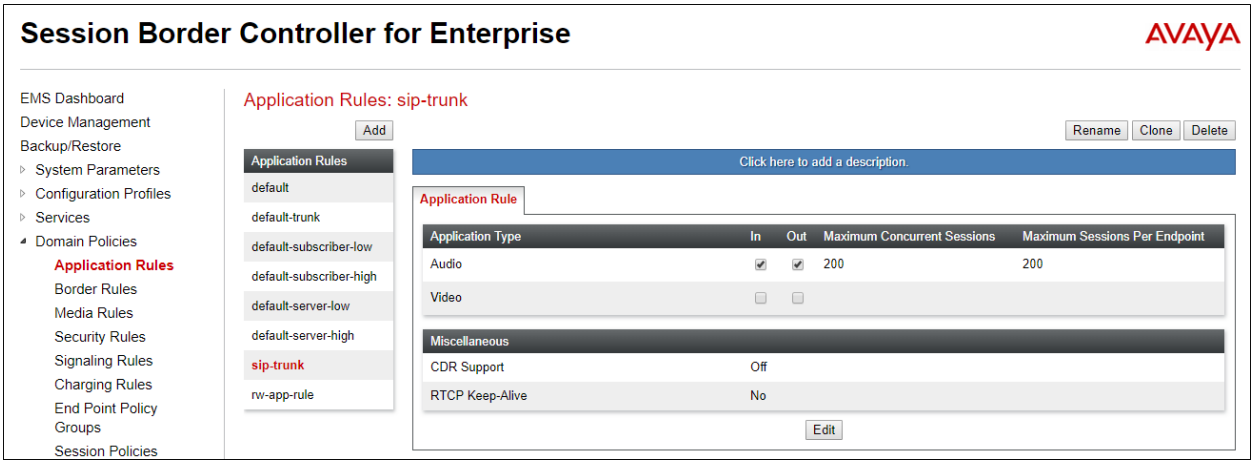
Similarly create a Topology Hiding profile for the Avaya SBCE connection to Verizon. Enter a Profile Name (e.g., **VZ IPT Topology**). Overwrite the headers with the FQDNs known by Verizon, as shown on the screen below.




## 7.10. Application Rules

Application Rules define which types of SIP-based Unified Communications applications the Avaya SBCE security device will protect. In addition, the maximum number of concurrent voice and video sessions the network will process are set, in order to prevent resource exhaustion.

Select **Domain Policies → Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the reference configuration, the **sip-trunk** profile was created for IP Office and Verizon Business. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** application to a value slightly larger than the licensed sessions. For example, if licensed for 150 sessions set the values to **200**. The **Maximum Session Per Endpoint** should match the **Maximum Concurrent Sessions**.

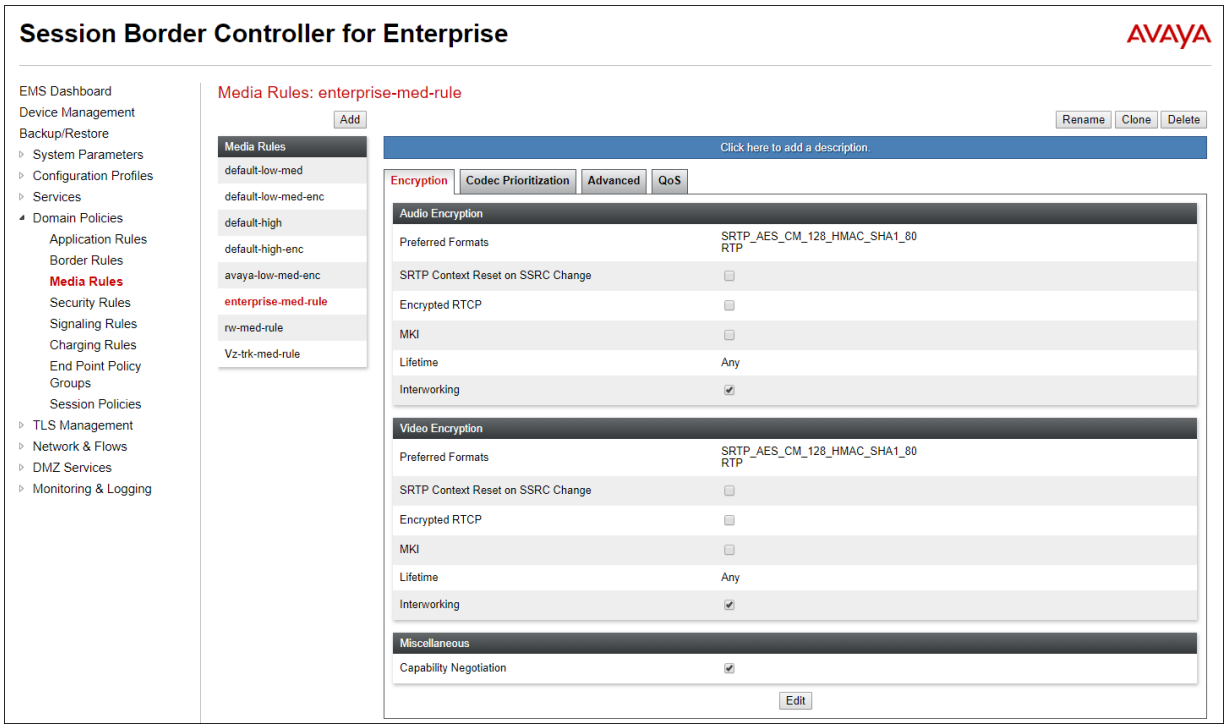


## 7.11. Media Rules

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

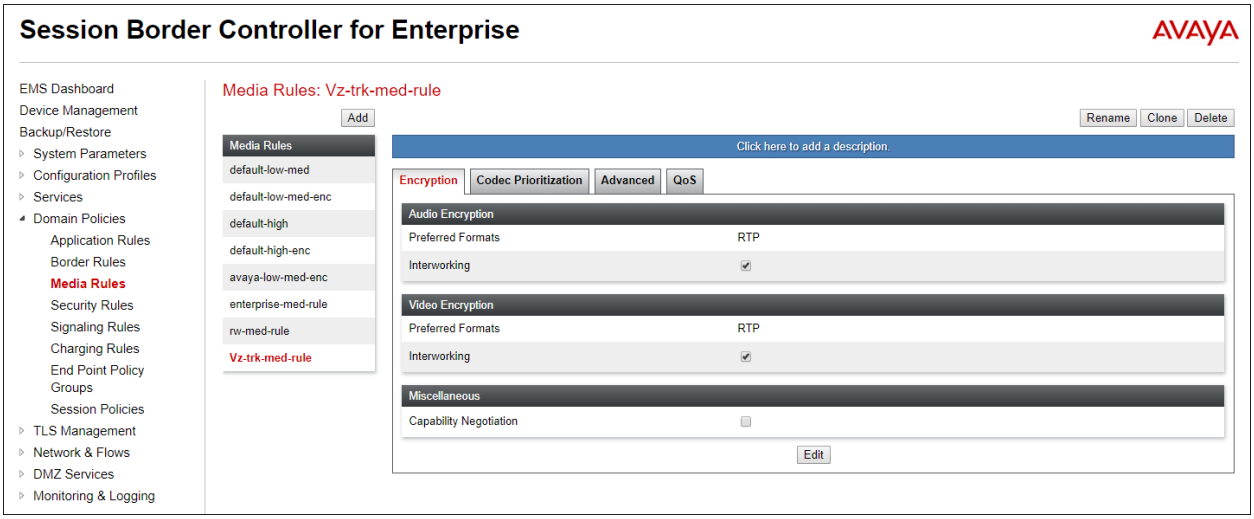
To create a Media Rule for the IP Office, select **Domain Policies → Media Rules** from the left-side menu. In the sample configuration, the default **avaya-low-med-enc** rule was cloned for IP Office, and then modified as shown on the screen below. With the **avaya-low-med-enc** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

The Media Rule **enterprise-med-rule** created for the IP Office is shown below. The **Preferred Formats** are changed to include **SRTP_AES_CM_128_HMAC_SHA1_80** as the first choice and **RTP** as second. In the **Miscellaneous** section, **Capability Negotiation** is checked. All other fields retained their default cloned value.

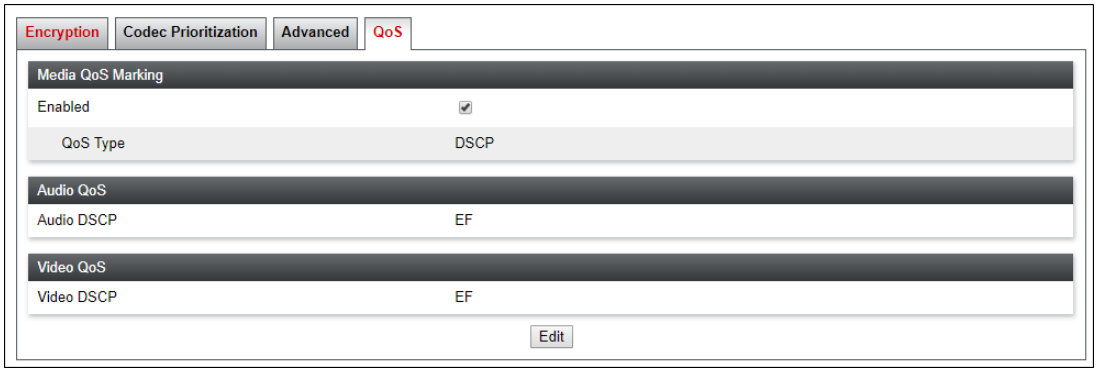


Similarly, a Media Rule is created for Verizon. In this case, the **default-low-med** profile was cloned. With the **default-low-med** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

The Media Rule named **Vz-trk-med-rule**, used for Verizon in the sample configuration is shown below.



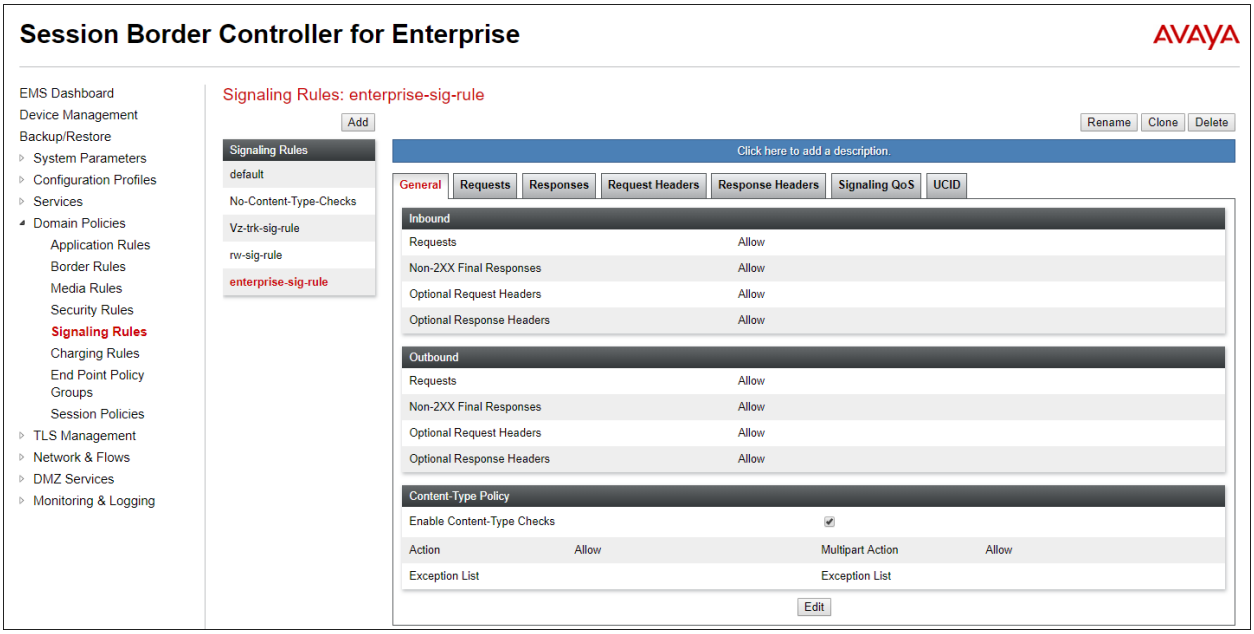

Note the DSCP values **EF** for expedited forwarding (default value) used for Media **QoS,** as specified by Verizon.



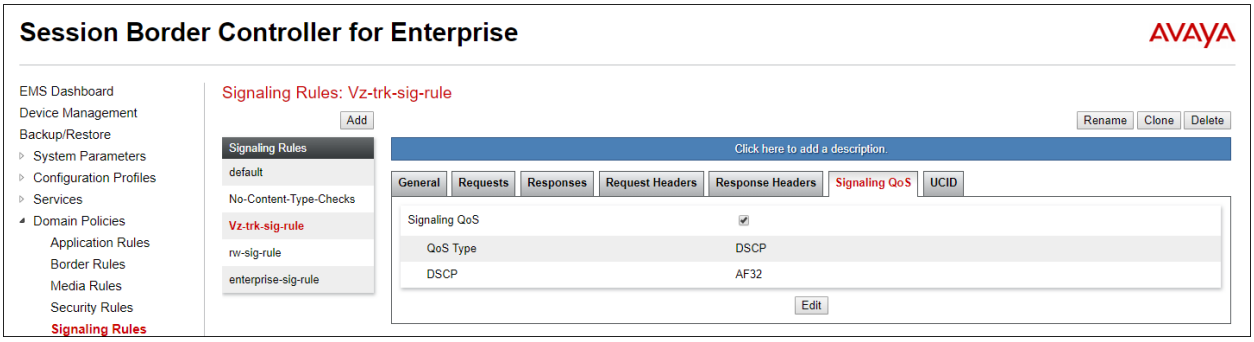
## 7.12. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. Signaling Rules are also used to define QoS parameters for the SIP signaling packets.

Clone and modify the **default** signaling rule as needed, to add the proper quality of service to the SIP signaling. To clone a signaling rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown). In the reference configuration, signaling rule **enterprise-sig-rule** is unchanged from the default rule.



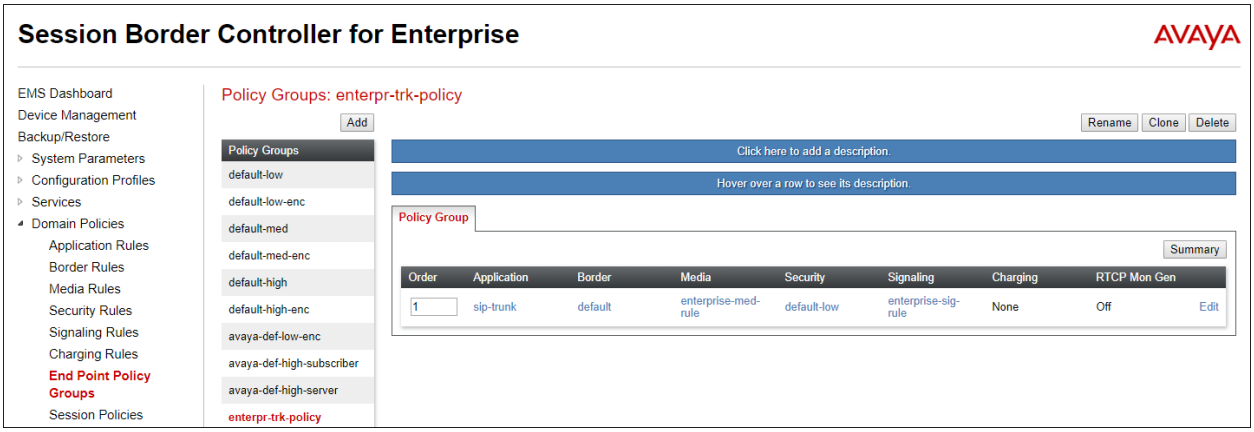

Signaling rule **Vz-trk-sig-rule** was also cloned from the default rule and used for Verizon. The settings for **Signaling QoS** are changed from the default values to **DSCP** value **AF32** for assured forwarding, as specified by Verizon, shown below.



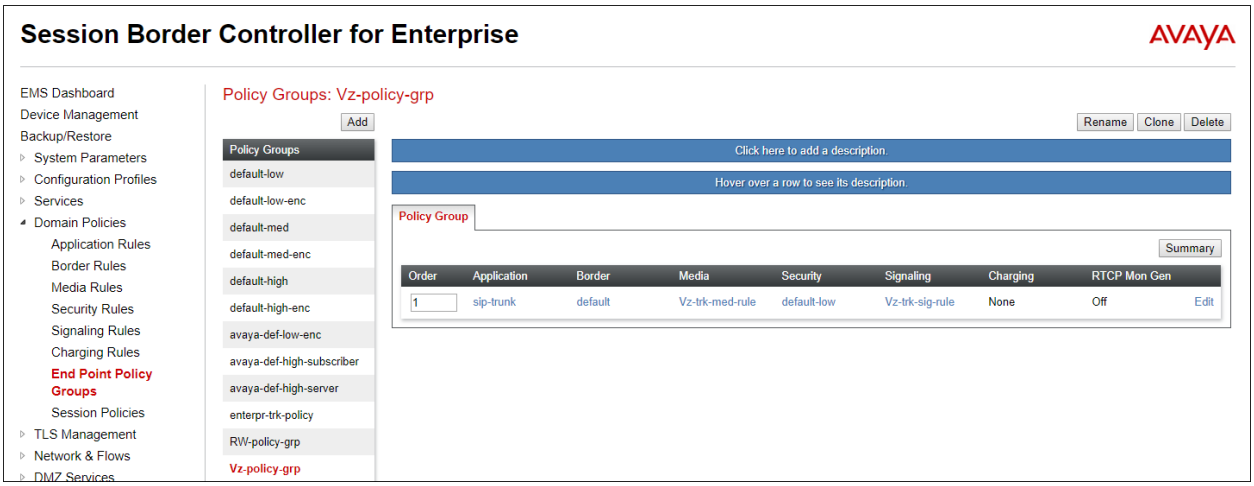
## 7.13. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.144**.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** as shown below. The following screen shows the **enterpr-trk-policy** created for IP Office. The details of the non-default rules chosen are shown in previous sections.




The following screen shows the **Vz-policy-grp** created for Verizon Business IP Trunking service. The details of the non-default rules chosen are shown in previous sections.

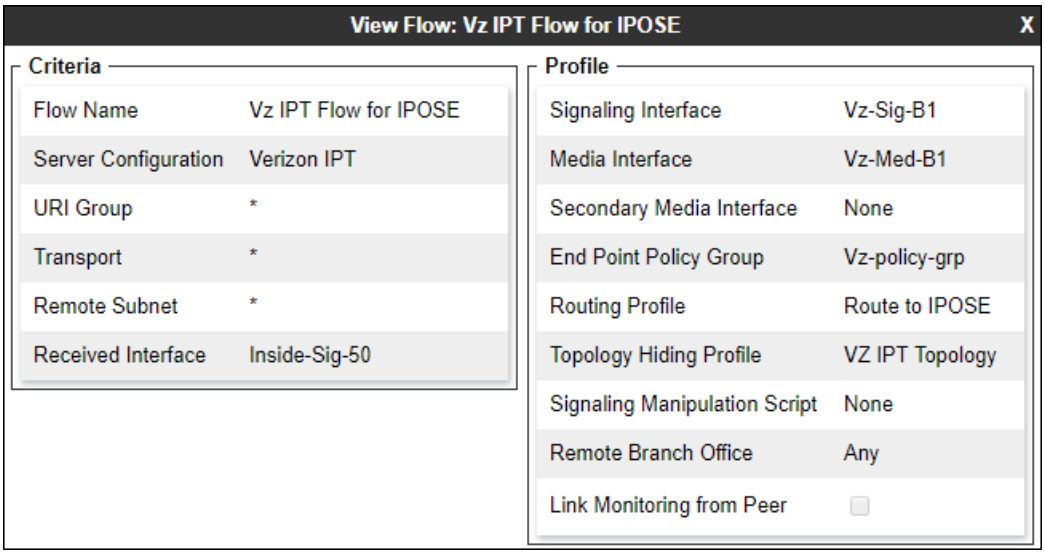


## 7.14. End Point Flows - Server Flows

Server Flows combine the interfaces, polices, and profiles defined in the previous sections into inbound and outbound flows. When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow.

Create a Server Flow for IP Office and Verizon Business IP Trunking service. To create a Server Flow, navigate to **Network and Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown).

The following screen shows the flow named **Vz IPT Flow for IPOSE** viewed from the reference configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.



**View Flow: Vz IPT Flow for IPOSE** X

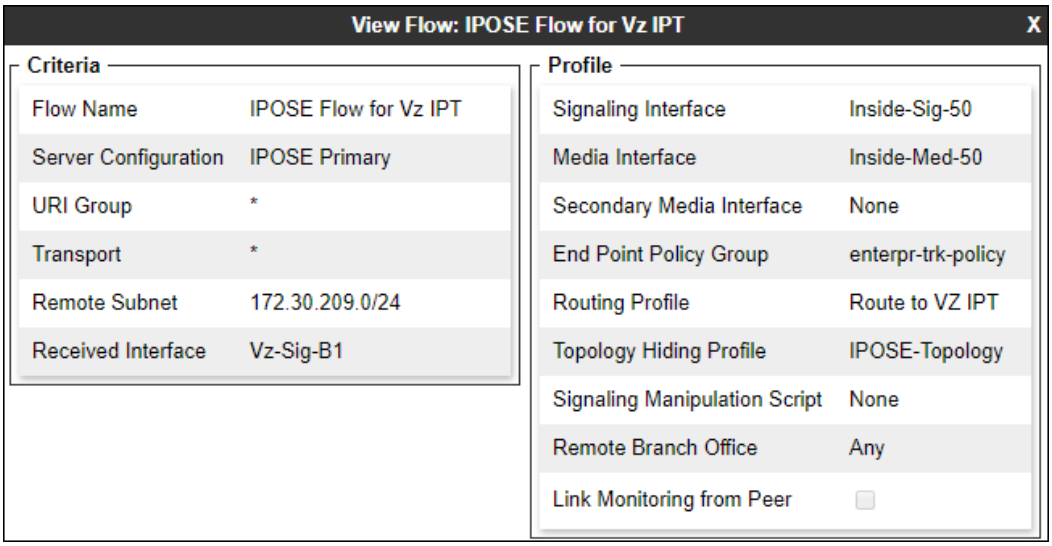
**Criteria**

| | |
|---|---|
| Flow Name | Vz IPT Flow for IPOSE |
| Server Configuration | Verizon IPT |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | Inside-Sig-50 |

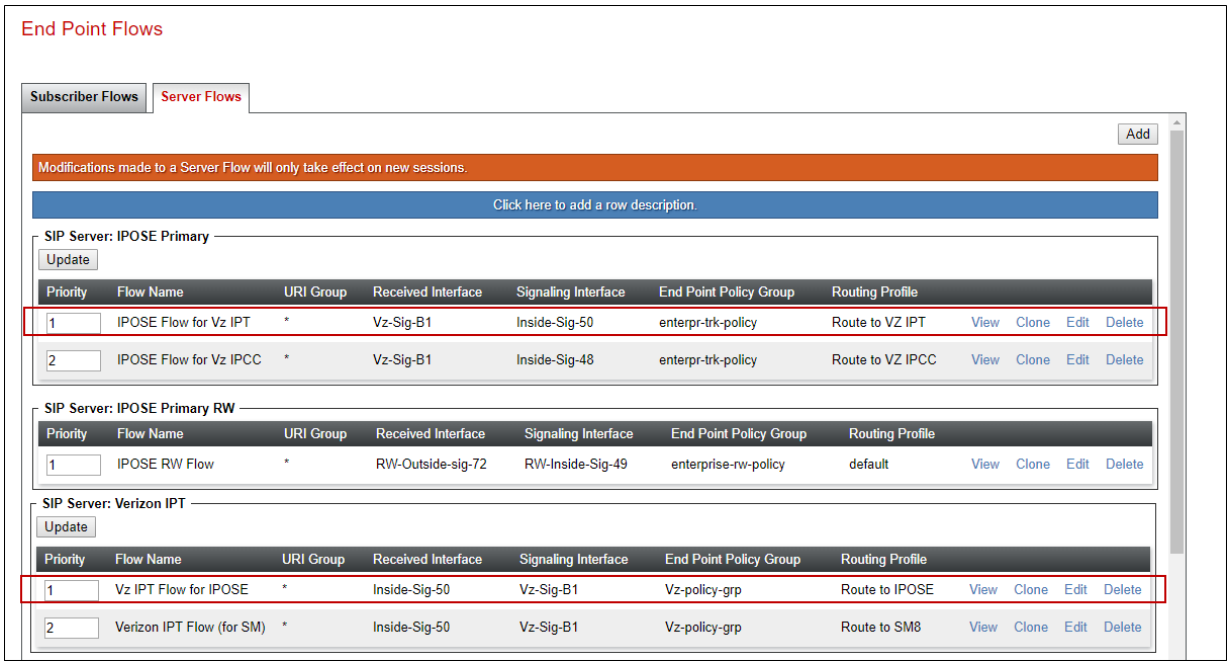
**Profile**

| | |
|---|---|
| Signaling Interface | Vz-Sig-B1 |
| Media Interface | Vz-Med-B1 |
| Secondary Media Interface | None |
| End Point Policy Group | Vz-policy-grp |
| Routing Profile | Route to IPOSE |
| Topology Hiding Profile | VZ IPT Topology |
| Signaling Manipulation Script | None |
| Remote Branch Office | Any |
| Link Monitoring from Peer | |

Once again, select the **Server Flows** tab and click **Add**. The following screen shows the flow named **IPOSE Flow for Vz IPT** viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections. In addition, the **Remote Subnet** can be optionally configured with the Verizon-provided IP address/mask of the subnet for the IP Trunk service, i.e., **172.30.209.0/24**.




The screen below shows the completed **Server Flows** tab as configured in the shared test environment. The highlighted flows are the ones relevant to the configuration of the IP Office SIP trunk to Verizon Business IP Trunking.



# 8. Verizon Business IP Trunking Services Configuration

Information regarding the Verizon Business IP Trunking Services suite offer can be found at https://enterprise.verizon.com/products/business-communications/voip-and-voice-services/voip-ip-trunking/ or by contacting a Verizon Business sales representative.

The reference configuration described in these Application Notes is located in the Avaya Solutions and Interoperability Test Lab. Access to the Verizon Business IP Trunking Services suite was via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

For service provisioning, Verizon will require the customer IP address used to reach the Avaya SBCE. The following service access information (FQDN, ports, DID numbers) was provided by Verizon for the sample configuration.

| CPE (Avaya) | Verizon Network |
|---|---|
| ***adevc.avaya.globalipcom.com***<br>***UDP port 5060*** | ***pcelban0001.avayalincroft.globalipcom.com***<br>***UDP Port 5071*** |

| IP DID Numbers |
|---|
| 732-945-0231 |
| 732-945-0232 |
| 732-945-0233 |
| 732-945-0234 |
| 732-945-0235 |
| 732-945-0236 |
| 732-945-0237 |
| 732-945-0238 |
| 732-945-0239 |

# 9. Verification Steps

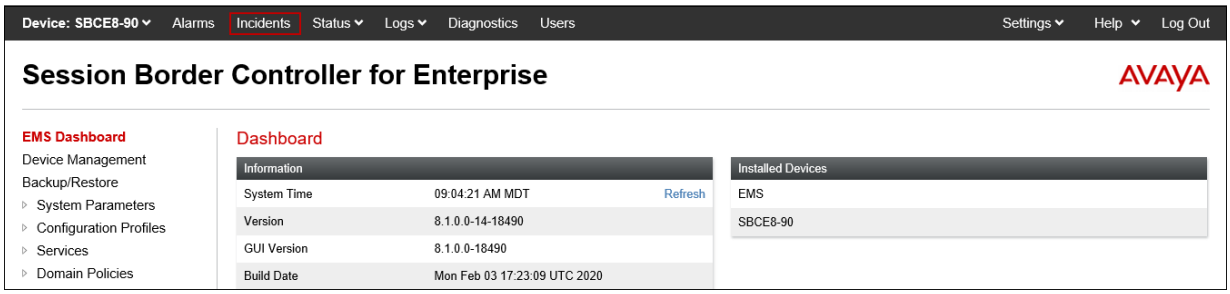
This section provides example verifications of the Avaya configuration with Verizon Business Private IP (PIP) Trunk service.

## 9.1. Avaya SBCE

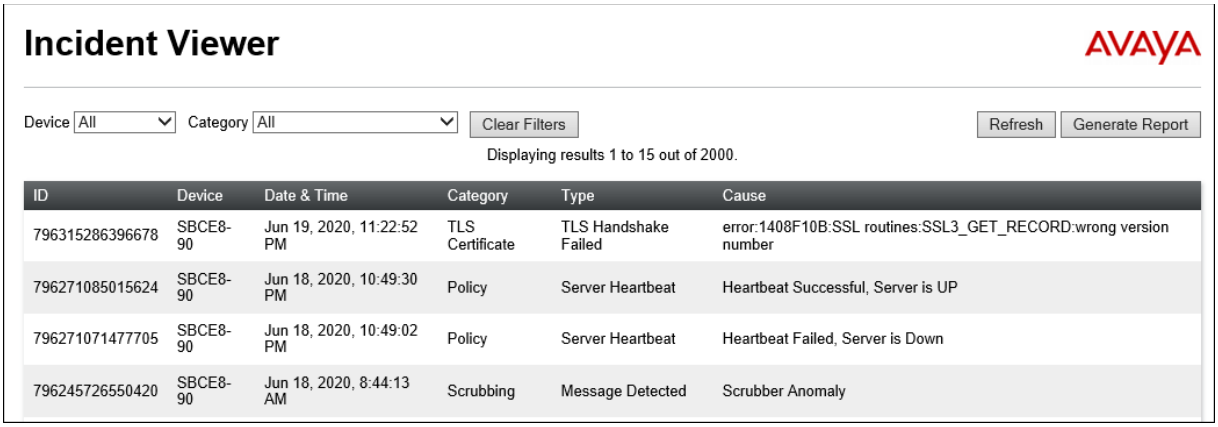
This section provides verification steps that may be performed with the Avaya SBCE.

### 9.1.1. Incidents

The Incident Viewer can be accessed from the Avaya SBCE top navigation menu as highlighted in the screen shot below.



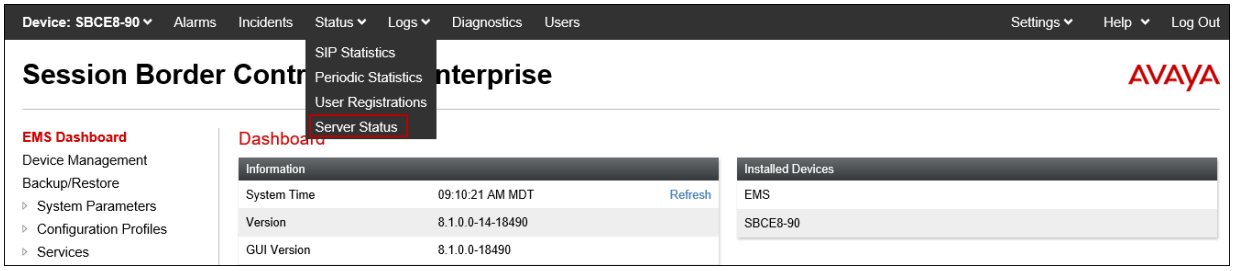

Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing and other failures.



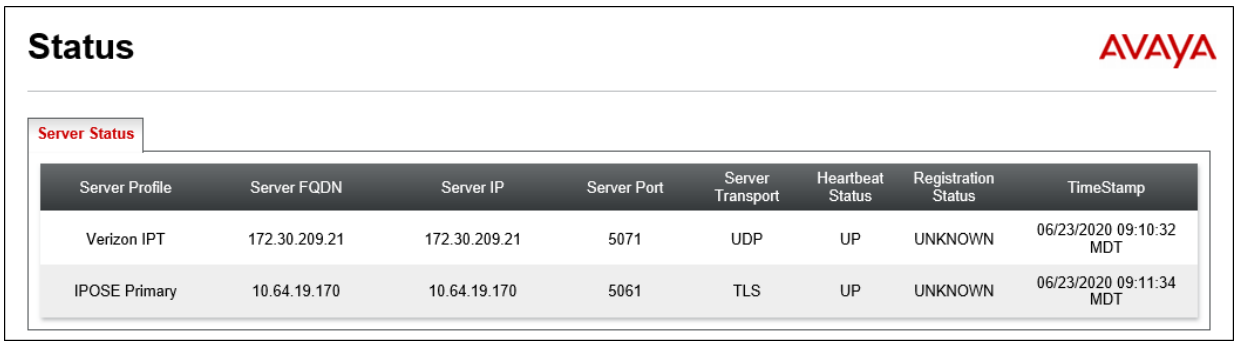

| ID | Device | Date & Time | Category | Type | Cause |
|---|---|---|---|---|---|
| 796315286396678 | SBCE8-90 | Jun 19, 2020, 11:22:52 PM | TLS Certificate | TLS Handshake Failed | error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number |
| 796271085015624 | SBCE8-90 | Jun 18, 2020, 10:49:30 PM | Policy | Server Heartbeat | Heartbeat Successful, Server is UP |
| 796271071477705 | SBCE8-90 | Jun 18, 2020, 10:49:02 PM | Policy | Server Heartbeat | Heartbeat Failed, Server is Down |
| 796245726550420 | SBCE8-90 | Jun 18, 2020, 8:44:13 AM | Scrubbing | Message Detected | Scrubber Anomaly |

### 9.1.2. Server Status

The **Server Status** can be access from the Avaya SBCE top navigation menu by selecting the **Status** menu, and then **Server Status**.



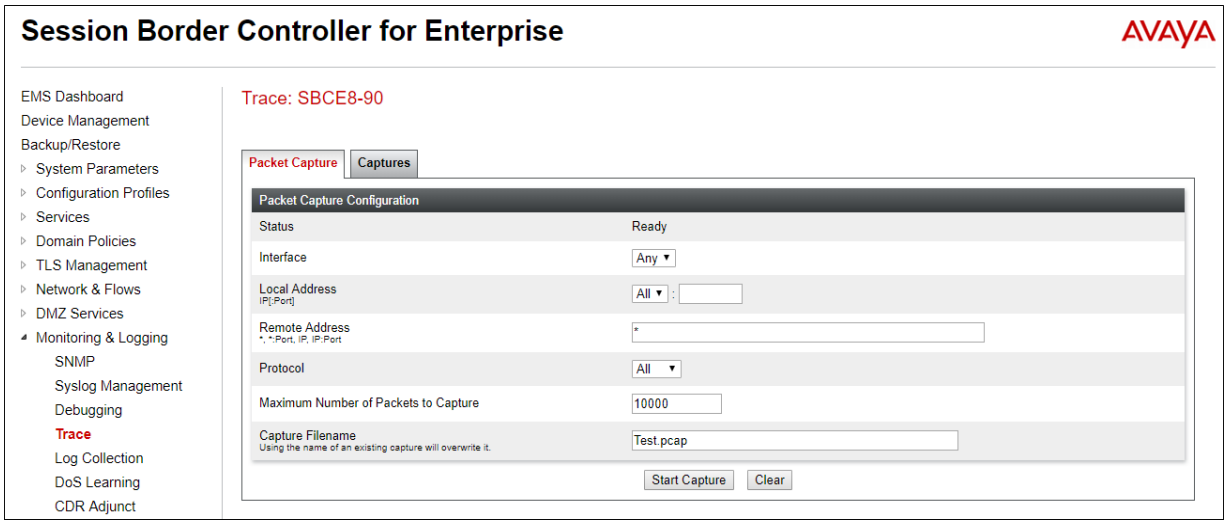

The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 7.77**.



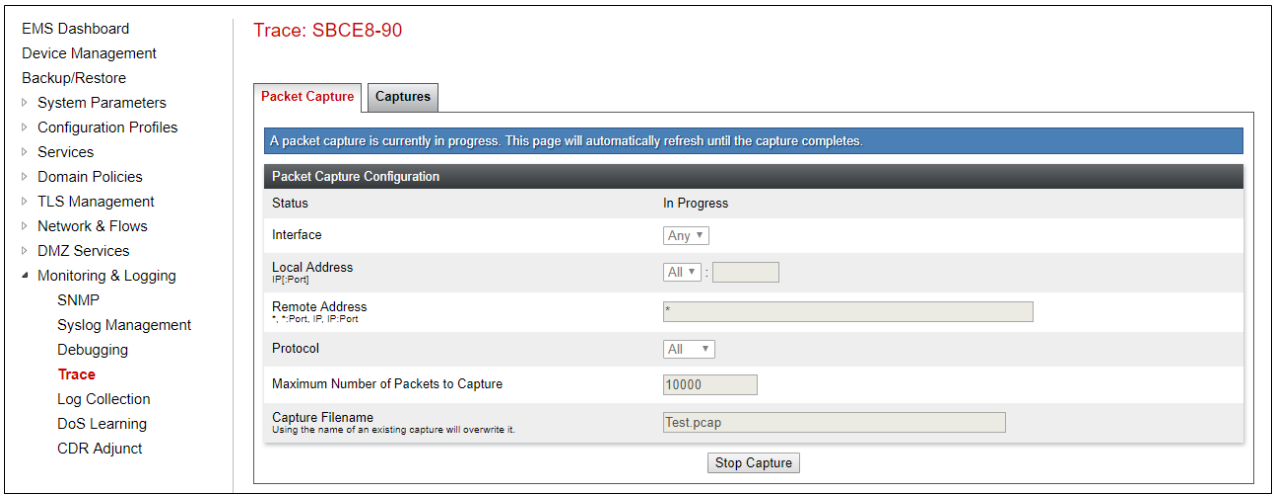

| Server Profile | Server FQDN | Server IP | Server Port | Server Transport | Heartbeat Status | Registration Status | TimeStamp |
|---|---|---|---|---|---|---|---|
| Verizon IPT | 172.30.209.21 | 172.30.209.21 | 5071 | UDP | UP | UNKNOWN | 06/23/2020 09:10:32 MDT |
| IPOSE Primary | 10.64.19.170 | 10.64.19.170 | 5061 | TLS | UP | UNKNOWN | 06/23/2020 09:11:34 MDT |

### 9.1.3. Tracing

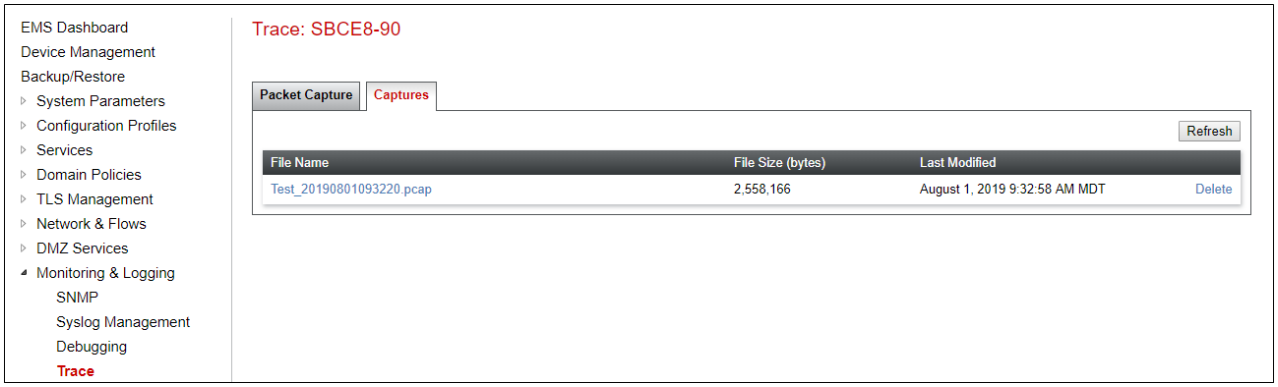
To take a call trace, navigate to **Monitoring & Logging → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.



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




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

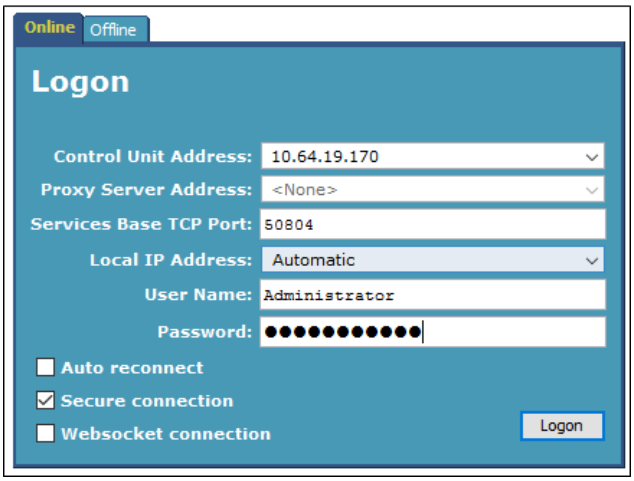


## 9.2. Avaya IP Office

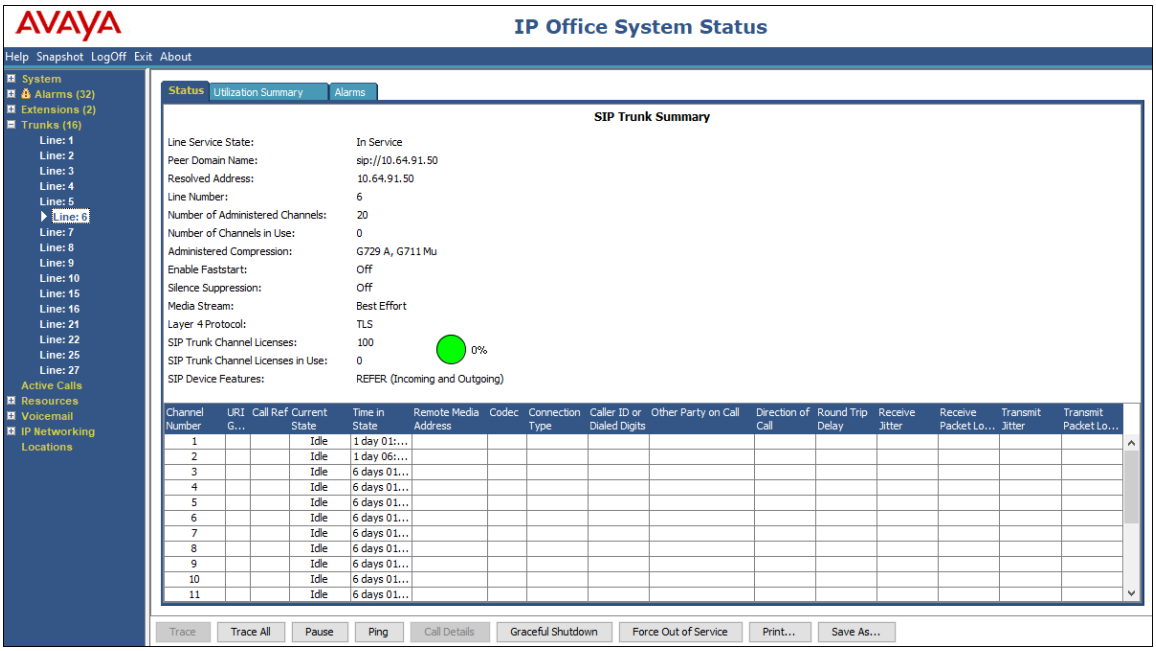
This section provides verification steps that may be performed with the IP Office.

### 9.2.1. System Status Application

The Avaya IP Office System Status application can be used to verify the service state of the SIP line. From the IP Office Manager application, select **File → Advanced → System Status**. Under **Control Unit IP Address** select the IP address of the IP Office system under verification. Log in using the appropriate credentials.

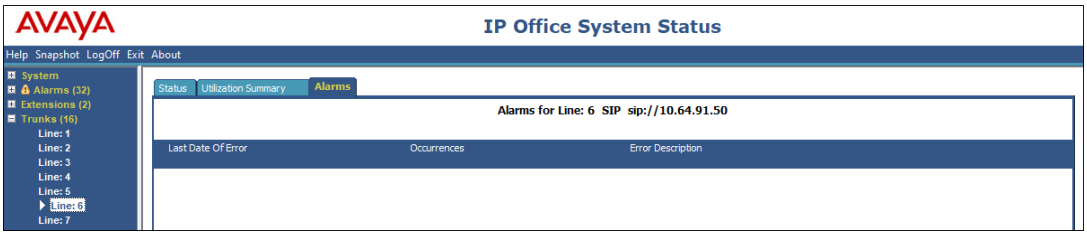



Select the SIP line from the left pane (**Line 6** in the reference configuration). On the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).



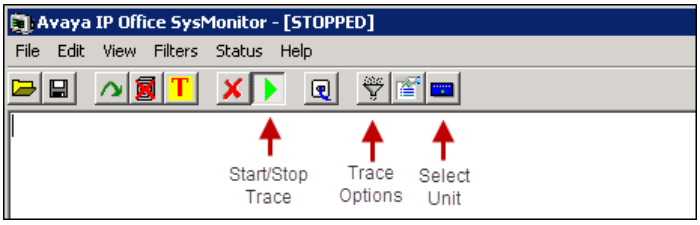
In the lower part of the screen, the **Trace All** button may be pressed to display real time tracing information as calls are made using this SIP Line. The **Ping** button can be used to ping the other end of the SIP trunk (e.g., Avaya SBCE).

Select the **Alarms** tab and verify that no alarms are active on the SIP line.

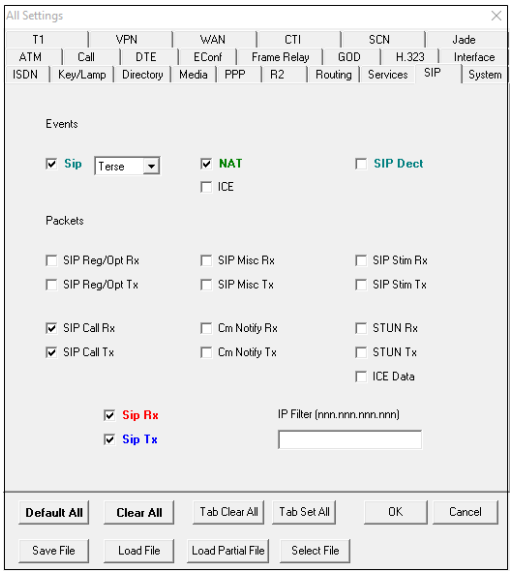



## 9.2.2. System Monitor

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.




Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting to the desired color.



The following example shows a portion of the System Monitor window for an outbound call from extension 6322, whose DID is 732-945-0232, calling out to the PSTN via the Verizon Business IP Trunking service. The telephone user dialed 9-1-786-331-0799.

```
Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.64.19.170 (IPOSE-Primary (Server Edition(P)) (Select)); Log Settings - C:\Users\...\sysmonitorsettings.ini
File  Edit  View  Filters  Status  Help

14:19:45 1215553230mS SIP Tx: TLS 10.64.19.170:9150 -> 10.64.91.50:5061
                    INVITE sip:17863310799@10.64.91.50 SIP/2.0
                    Via: SIP/2.0/TLS 10.64.19.170:5061;rport;branch=z9hG4bK20b907216c366360699f22941cd83b4a
                    From: "ATT-Avaya 9608" <sip:7329450232@10.64.19.170>;tag=d327ced18d701de9
                    To: <sip:17863310799@10.64.91.50>
                    Call-ID: ecbd4e567c03a20d5fc40d6b0b06669c
                    CSeq: 994081180 INVITE
                    Contact: "ATT-Avaya 9608" <sip:7329450232@10.64.19.170:5061;transport=tls>
                    Max-Forwards: 70
                    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY
                    Supported: timer
                    Min-SE: 1800
                    Session-Expires: 1800;refresher=uac
                    User-Agent: IP Office 11.0.4.1.0 build 11
                    Content-Type: application/sdp
                    Content-Length: 417

                    v=0
                    o=UserA 542848335 963841840 IN IP4 10.64.19.170
                    s=Session SDP
                    c=IN IP4 10.64.19.170
                    t=0 0
                    m=audio 42068 RTP/AVP 18 0 101
                    a=rtpmap:18 G729/8000
                    a=fmtp:18 annexb=no
                    a=rtpmap:0 PCMU/8000
                    a=rtpmap:101 telephone-event/8000
                    a=fmtp:101 0-15
                    a=tcap:1 RTP/SAVP RTP/AVP
                    a=acap:1 crypto:1 AES_CM_128_HMAC_SHA1_80 inline:P44sGb6OhV7rCeBW4qF7Z6BOE2fCAegaI9TuddJ4 UNENCRYPTED_SRTCP
                    a=pcfg:1 t=1 a=1
                    a=pcfg:2 t=2
14:19:45 1215553230mS CMCallEvt:    0000000000000000 0.2491.0 -1 TargetingEP: StateChange: END=X CMCSOffering->CMCSDelete
14:19:45 1215553230mS CMCallEvt:    0000000000000000 0.2491.0 -1 BaseEP: DELETE CMEndpoint f594f078 TOTAL NOW=3 CALL_LIST=1
14:19:45 1215553231mS CD: CALL: 365.2490.0 BState=Idle Cut=3 Music=0.0 Aend="ATT-Avaya9608(6322)" (0.0) Bend="" [Line 6] (0.0) CalledNum=917863310799 () CallingNum=6322
14:19:45 1215553235mS SIP Rx: TLS 10.64.91.50:5061 -> 10.64.19.170:9150
                    SIP/2.0 100 Trying
                    From: "ATT-Avaya 9608" <sip:7329450232@10.64.19.170>;tag=d327ced18d701de9
                    To: <sip:17863310799@10.64.91.50>
                    CSeq: 994081180 INVITE
                    Call-ID: ecbd4e567c03a20d5fc40d6b0b06669c
                    Via: SIP/2.0/TLS 10.64.19.170:5061;rport=9150;branch=z9hG4bK20b907216c366360699f22941cd83b4a
                    Content-Length: 0

14:19:45 1215553235mS CMLineRx: v=0
           CMProceeding
           Line: type=SIPLine 6 Call: lid=6 id=2493 in=0
```

# 10. Conclusion

IP Office is a highly modular IP telephone system designed to meet the needs of home offices, standalone businesses, and networked branch and head offices for small and medium enterprises.

These Application Notes demonstrated how IP Office Release 11.1 with Avaya Session Border Controller for Enterprise Release 8.1 can be configured to interoperate successfully with a Verizon Business IP Trunking service connection to create an end-to-end SIP Telephony business solution. By following the example configurations provided in this document, customers using Avaya IP Office and Avaya SBCE can connect to the PSTN via a Verizon Business IP Trunking service connection, thus eliminating the costs of analog or digital trunk connections previously required to access the PSTN. Utilizing this solution, IP Office customers can leverage the operational efficiencies and cost savings associated with SIP trunking while gaining the advanced technical features provided through the marriage of best of breed technologies from Avaya and Verizon.

# 11. Additional References

This section references documentation relevant to these Application Notes. In general, Avaya product documentation is available at http://support.avaya.com.


[1] *IP Office, Deploying IP Office Server Edition*, Release 11.1, Issue 14, April 2020.
[2] *IP Office™ Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, June 2020.
[3] *IP Office™ Platform 11.1, Deploying an IP500 V2 IP Office Essential Edition*, June 2020.
[4] *Administering Avaya IP Office™ Platform with Manager*, Release 11.1, Issue 2, May 2020.
[5] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.1, Issue 2, May 2020.
[6] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac and Windows*, Release 3.8, Issue 1, March 2020.
[7] *Using Avaya IX™ Workplace Client for Android, iOS, Mac and Windows*, Release 3.8, Issue 1, March 2020.
[8] *IP Office Platform 11.1, IP Office SIP Phones with ASBCE, Issue 04c*, April 2020.
[9] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 8.1, April 2020.
[10] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 2, April 2020.
[11] *RFC 3261 SIP: Session Initiation Protocol*. https://www.ietf.org/rfc/rfc3261.txt


Additional IP Office documentation can be found at:
https://ipofficekb.avaya.com/

The following documents may be obtained by contacting a Verizon Business Account Representative.

- *Retail VoIP Interoperability Test Plan*
- *Network Interface Specification Retail VoIP Trunk Interface (for non-registering devices)*

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.