Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 6.3 to support Time Warner Cable Business Class SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 9.1 and Avaya Session Border Controller for Enterprise Release 6.3, to interoperate with Time Warner Cable Business Class SIP Trunking Service.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

Time Warner Cable Business Class SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Time Warner Cable's network as an alternative to legacy analog or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

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.

Time Warner Cable is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Time Warner Cable and an Avaya SIP-enabled enterprise solution.

In the sample configuration, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office (hereafter referred to as IP Office) 500v2 Release 9.1, Avaya Session Border Controller for Enterprise (hereafter referred to as Avaya SBCE) Release 6.3, Avaya Communicator for Windows and Avaya Deskphones, including SIP, H.323, digital, and analog. The Avaya SBCE provides security for the Avaya IP Office solution, as well as interoperability features for the SIP trunk.

Time Warner Cable Business Class SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the IP Office solution are able to place and receive PSTN calls via a broadband WAN connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

The terms "service provider" and "Time Warner Cable" will be used interchangeable throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using IP Office to connect to Time Warner Cable's network via the Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the feature and functionality tests listed in **Section 2.1**.

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

2.1 Interoperability Compliance Testing

To verify Time Warner Cable's SIP Trunking interoperability, the following features and functionalities were exercised during the compliance testing:

- SIP Trunk Registration (Dynamic Authentication).
- SIP OPTIONS queries and responses.
- Incoming calls from the PSTN were routed to the DID numbers assigned by Time Warner Cable. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x0 Series IP Deskphones (H.323), Avaya 96x1 Series IP Deskphones (H.323), Avaya 1100 Series IP Deskphones (SIP), Avaya Communicator for Windows, Avaya 1400 Series Digital Deskphones, Avaya 9500 Series Digital Deskphones, and analog Deskphones.
- Outgoing calls to the PSTN were routed via Time Warner Cable's network to the various PSTN destinations.
- Caller ID presentation.

- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codec G.711MU (Time Warner Cable supported audio codec).
- No matching codecs.
- G.711 fax pass-through.
- Proper early media transmissions.
- Voicemail and DTMF tone support (leaving and retrieving voice mail messages from PSTN phones).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

Note: Remote worker was tested as part of this solution; the configuration necessary to support remote workers is beyond the scope of these Application Notes and is not discussed in these Application Notes, see **References [13]**.

Items not supported or not tested included the following:

- Time Warner Cable does not support T.38 fax; therefore T.38 fax was not tested (G.711 fax pass-through was tested successfully).
- The use of the SIP REFER method for network call redirection is not currently supported by Time Warner Cable; therefore SIP REFER was not tested.
- Inbound toll-free calls, 911 emergency and International calls are supported but were not tested.

2.2 Test Results

Interoperability testing with Time Warner Cable was successfully completed with no exception or observations/limitations.

2.3 Support

For support on Time Warner Cable systems visit the corporate Web page at:
http://business.timewarnercable.com/support/overview.html or call 866-892-4249.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 below illustrates the test configuration used. It shows a simulated enterprise site connected to Time Warner Cable's network through the public internet.

For confidentiality and privacy purposes, actual public IP addresses and PSTN routable phone numbers (DIDs) used during the compliance testing have been replaced with fictitious IP addresses and PSTN non-routable phone numbers throughout the Application Notes.

The Avaya components used to create the simulated enterprise customer site includes:

- Avaya IP Office 500v2.
- Avaya Session Border Controller for Enterprise.
- Avaya Voicemail Pro for IP Office.
- Avaya 96x0 Series H.323 IP Deskphones.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 11x0 Series SIP IP Deskphones.
- Avaya Communicator for Windows.
- Avaya 1408 Digital Deskphones.
- Avaya 9508 Digital Deskphones.

Located at the edge of the enterprise is the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **B1** was used to connect to the public network, interface **A1** was used to connect to the enterprise private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

Also located at the enterprise site is Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codec's. The IP Office **LAN1** interface connects to the inside (A1) interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE (B1) connects to Time Warner Cable's network via the public Internet.

The transport protocol between the Avaya SBCE and Time Warner Cable, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is also SIP over UDP.

For inbound calls, the calls flowed from Time Warner Cable to the Avaya SBCE, then to IP Office.

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk; the call was routed to the Avaya SBCE for egress into Time Warner Cable's network.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Time Warner Cable's network (refer to **Section 5.7**). The short code 9 was stripped off by IP Office but the remaining N digits were sent unaltered to the network. Since Time Warner Cable is a U.S. based company, a country member of the North American Numbering Plan (NANP), the users dialed 7 or 10 digits for local calls, and 11 (1 + 10) digits for calls between the NANP.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the enterprise. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and the enterprise must be allowed to pass through these devices

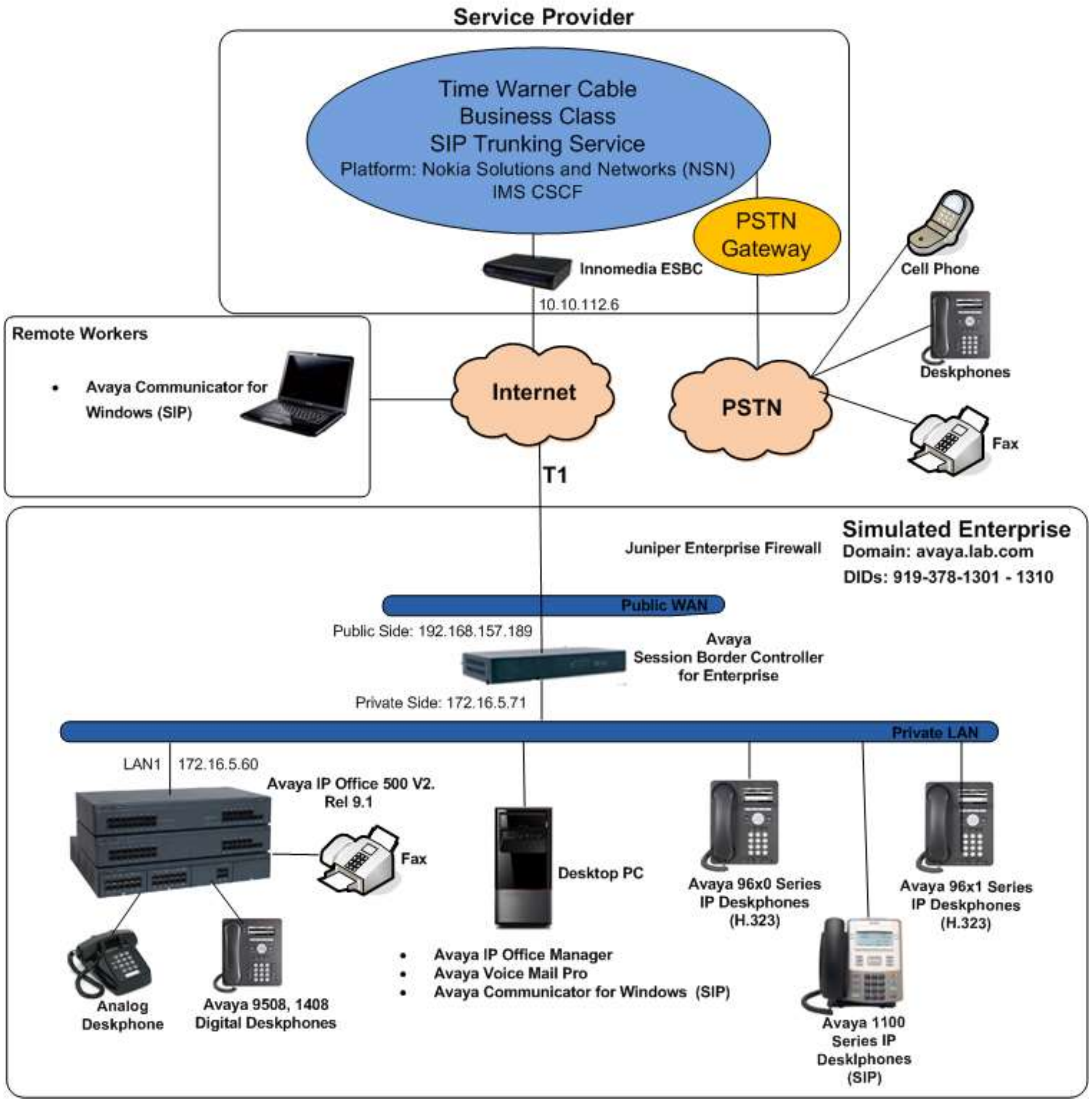


Figure 1: Avaya Interoperability Test Lab Configuration.

4. Equipment and Software Validated

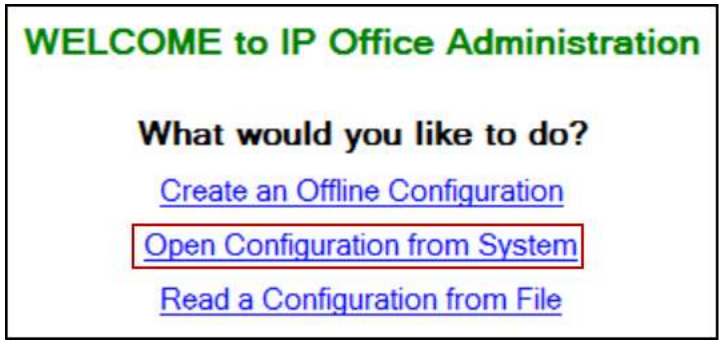
The following equipment and software/firmware were used for the sample configuration.

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	9.1.0.0 Build 437
Avaya IP Office DIG DCPx16 V2	9.1.0.0 Build 437
Avaya IP Office Manager	9.1.0.0 Build 437
Avaya Voicemail Pro Client	9.1.0.0 Build 166
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.3.000-19-4338
Avaya 96x0 IP Deskphones (H.323)	Avaya one-X® Deskphone Edition S3.230A
Avaya 96x1 Series IP Deskphones (H.323)	Avaya one-X® Deskphone H.323 Version 6.4014
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.18.00
Avaya Communicator for Windows	2.0.3.30
Avaya Digital Deskphones 1408	40.0
Avaya Digital Deskphones 9508	0.55
Lucent Analog Phone	--
Time Warner Cable	
Nokia Solutions and Networks (NSN) IMS CSCF	8.2EP2
Innomedia ESBC	2.0.13.0

Note: 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 without T.38 Fax Service.

5. Configure IP Office

This section describes the IP Office configuration required to interwork with Time Warner Cable. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. A screen that includes the following may be displayed.



Select **Open Configuration from System**. If the above screen does not appear, the configuration may be alternatively opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window. Select the proper IP Office from the pop-up window, and log in with the appropriate credentials.

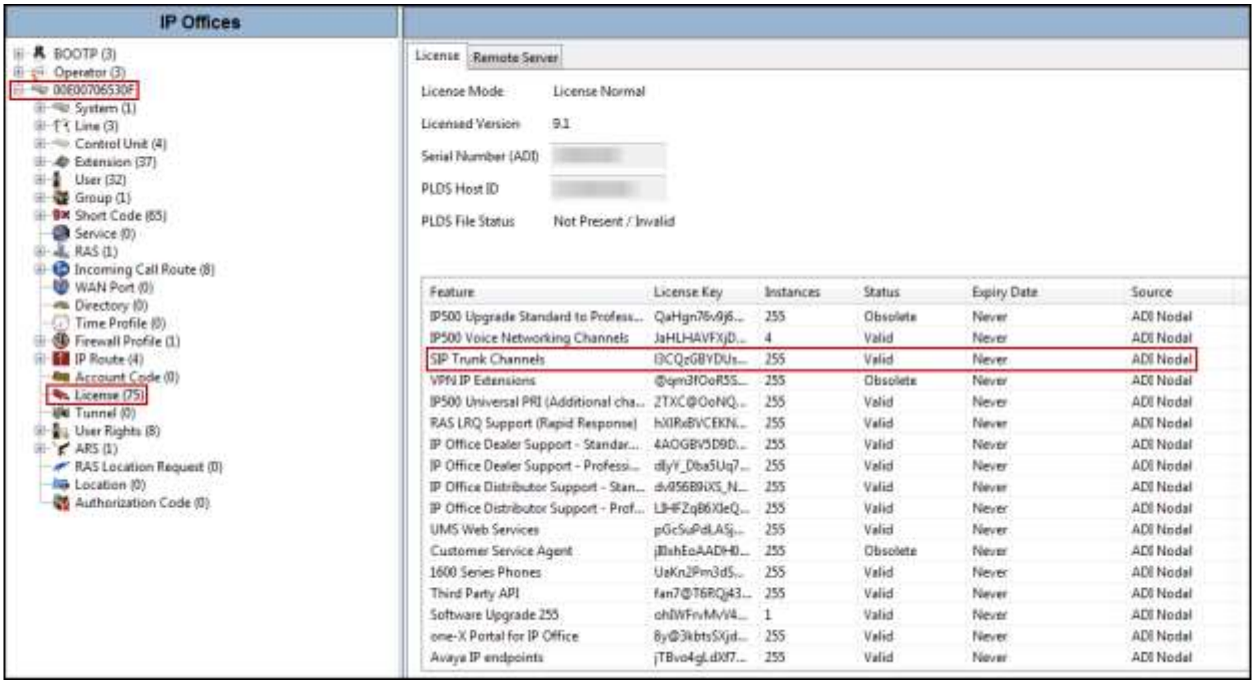
The appearance of the Avaya IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the Group pane has been omitted, its content is shown as submenus in the Navigation pane. These panes (Navigation and Details) will be referenced throughout the IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the service provider is assumed to already be in place.

In the sample configuration, the MAC address **00E00706530F** was used as the system name. All navigation described in the following sections (e.g., **License → SIP Trunk Channels**) appears as submenus underneath the system name **00E00706530F** in the Navigation Pane.

5.1 Licensing

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.

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License** in the Navigation pane and **SIP Trunk Channels** in the Detail pane. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the Details pane. Note that the full **License Key** in the screen below are not shown for security purposes.



5.2 System

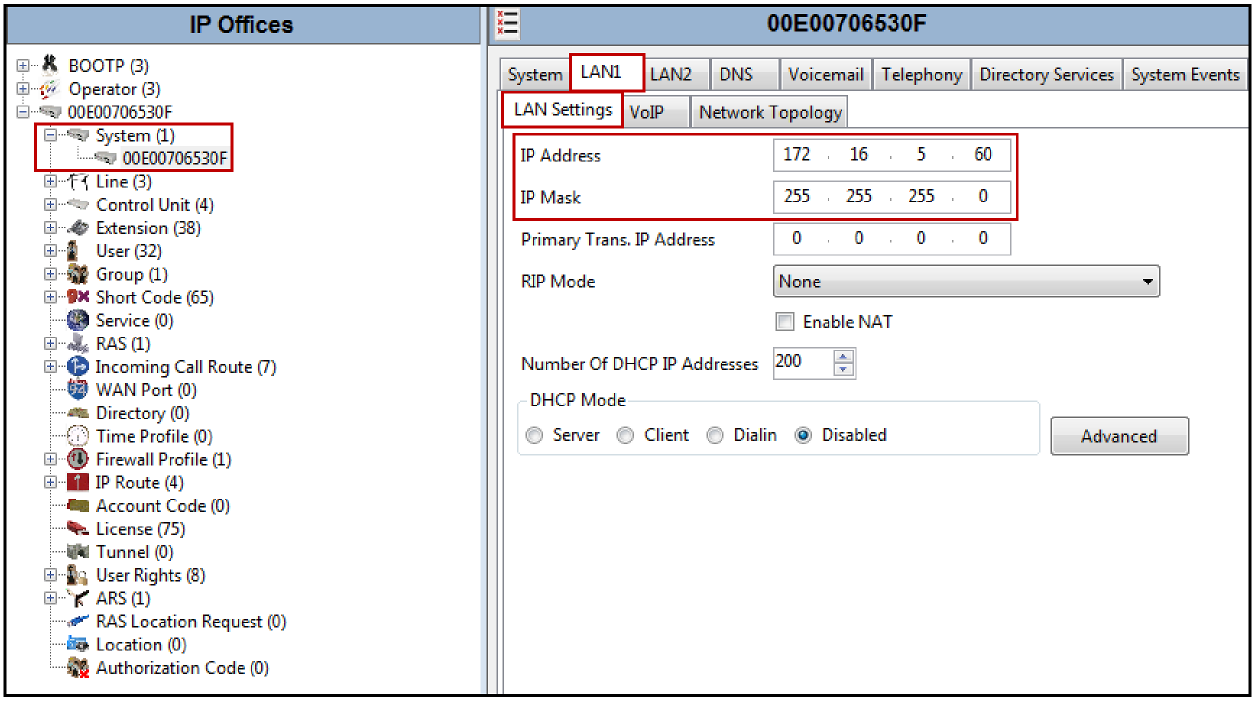
Configure the necessary system settings. In an Avaya IP Office the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.1 System - LAN1 Tab

In the sample configuration, the MAC address **00E00706530F** was used as the system name and the **LAN** port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to Time Warner Cable's network via the public internet. The **LAN1** settings correspond to the **LAN** port in IP Office. To access the **LAN1** settings, navigate to **System (1) → 00E00706530F** in the Navigation Pane then in the Details Pane navigate to the **LAN1→ LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters:

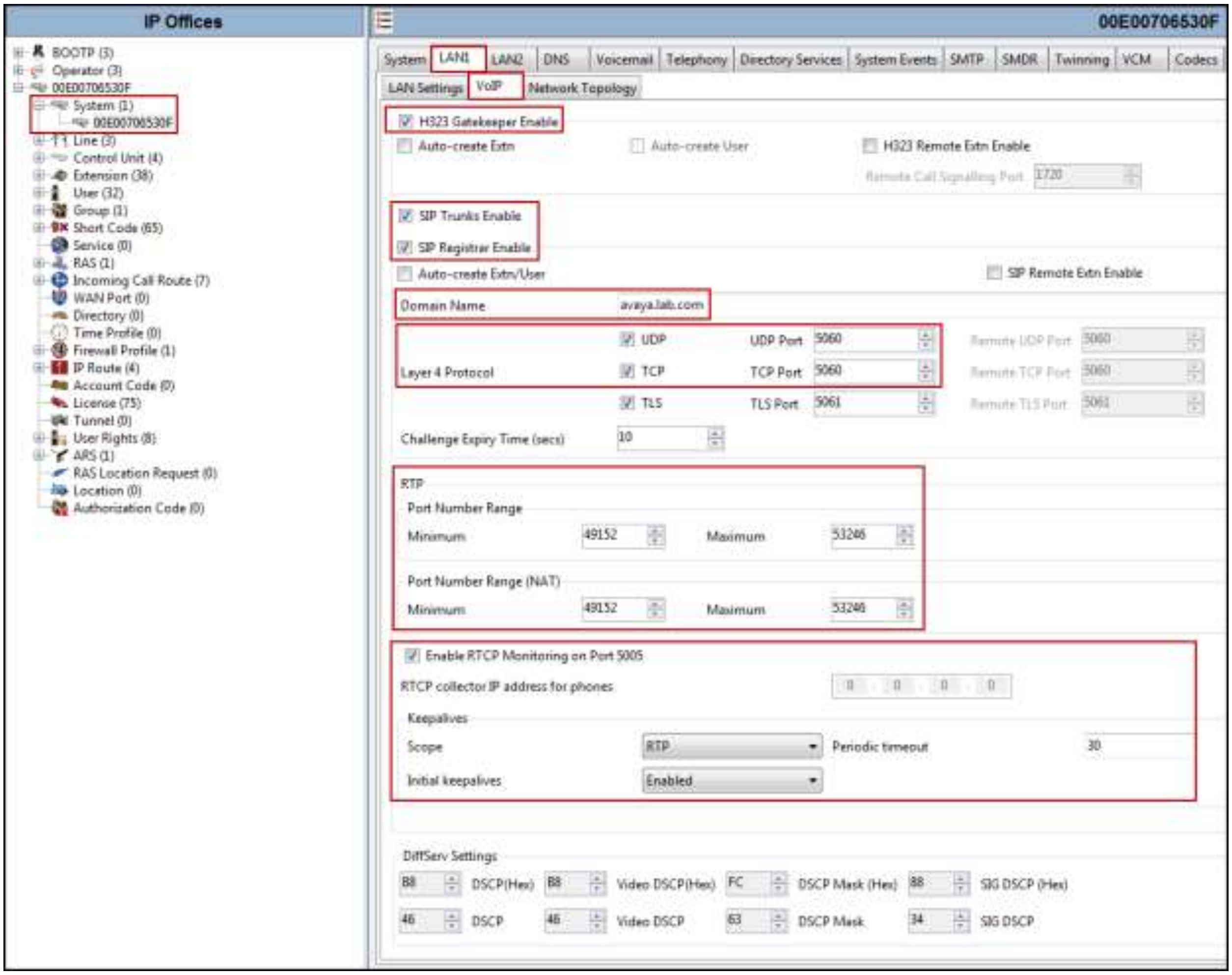
- Set the **IP Address** field to the LAN IP address, e.g., **172.16.5.60**.
- Set the **IP Mask** field to the subnet mask of the public network, e.g., **255.255.255.0**.
- All other parameters should be set according to customer requirements.

- Click **OK** to commit (not shown).



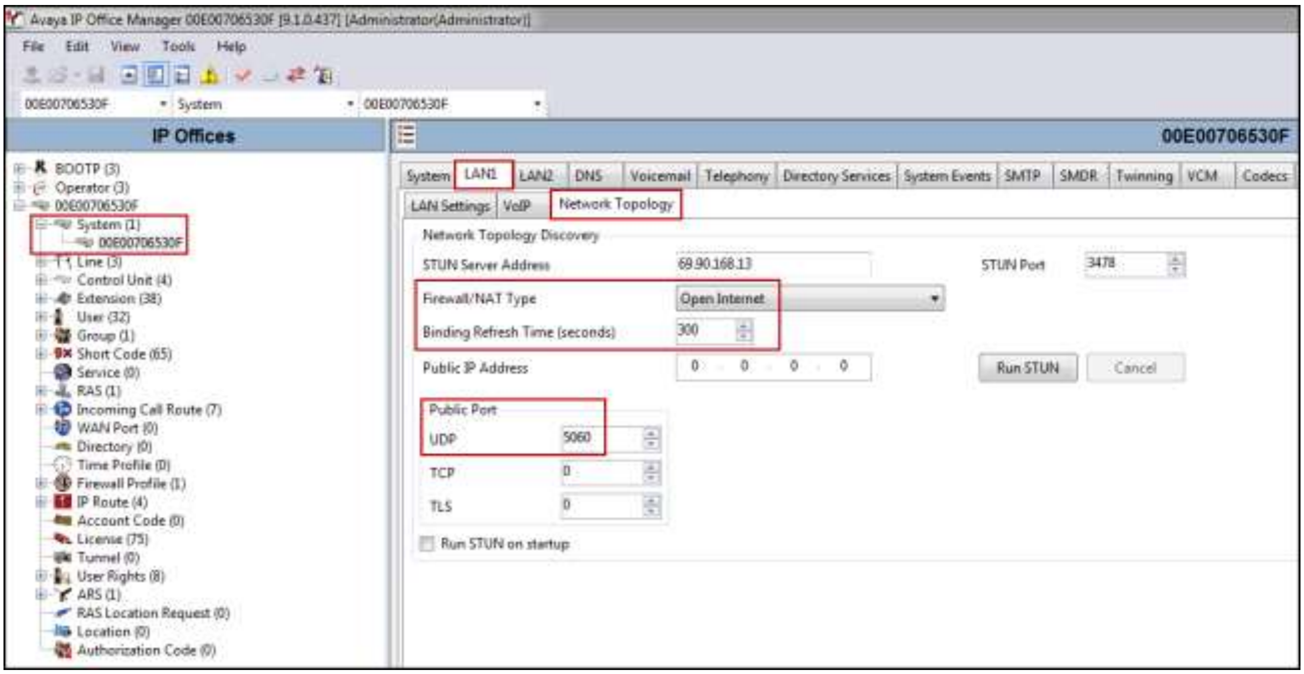
The **VoIP** tab as shown in the screenshot below was configured with following settings:

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Time Warner Cable.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **Domain Name**.
- Verify the **UDP Port** and **TCP Port** numbers under **Layer 4 Protocol** are set to **5060**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP traffic is present.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



In the **Network Topology** tab, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even the default STUN settings are populated but they will not be used.
- Set the **Binding Refresh Time (seconds)** to a desired value, the value of **300** (or every 5 minutes) was used during the compliance testing. This value is used to determine the frequency that IP Office will send OPTIONS heartbeat to the service provider.
- Verify the **Public IP Address** is set to **0.0.0.0**.
- Set the **Public Port** to **5060** for **UDP**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

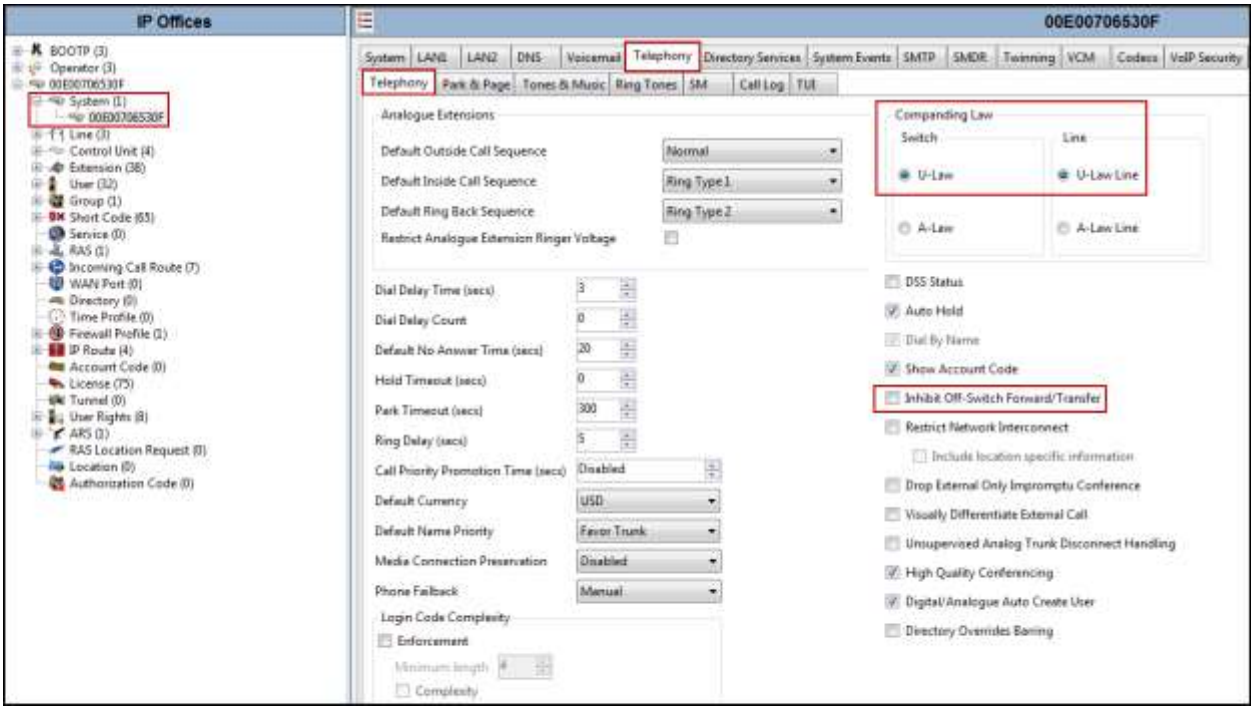


Note: In the compliance test, the **LAN1** interface was used to connect IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.2 System - Telephony Tab

Navigate to the **Telephony → Telephony** Tab in the Details Pane, configure the following parameters:

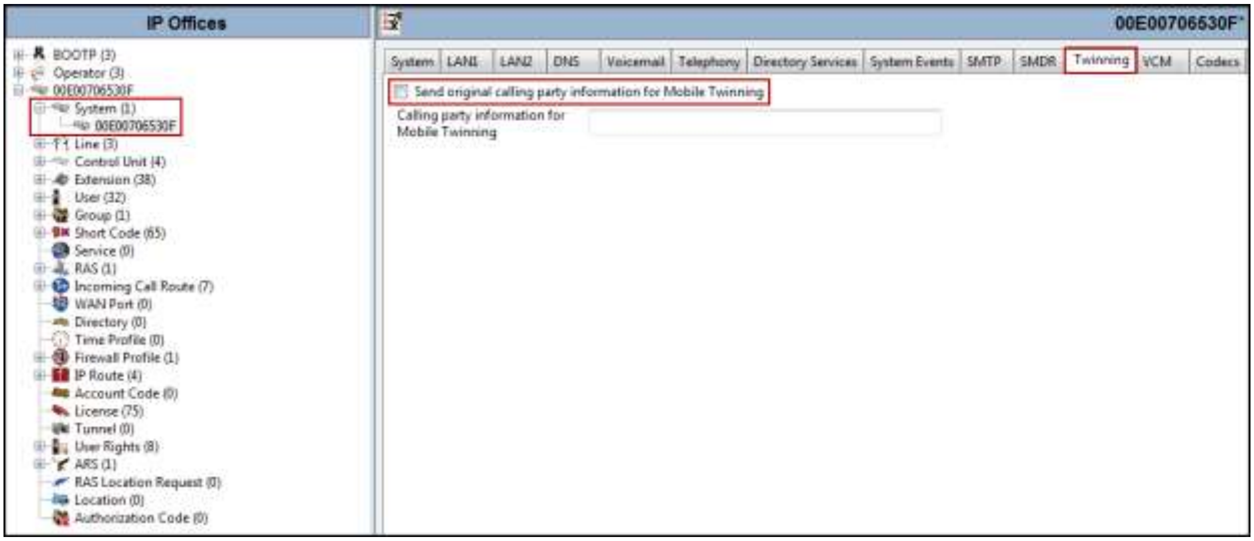
- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).



5.2.3 System - Twinning Tab

Navigate to the **Twinning** tab on the Details Pane, configure the following parameters:

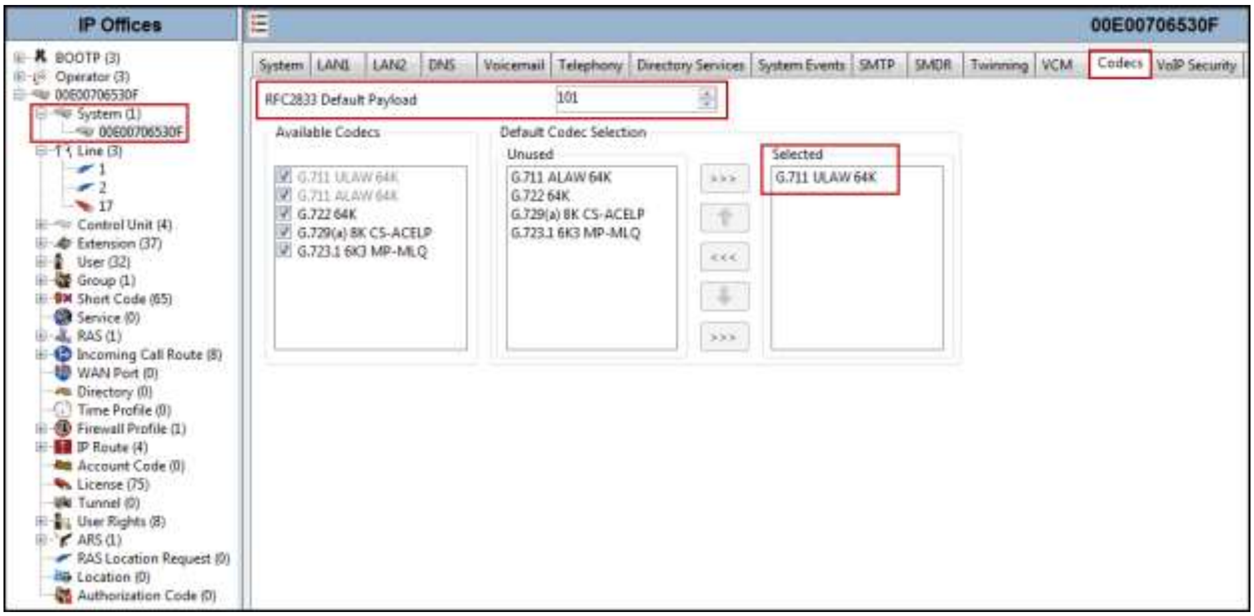
- Uncheck the **Send original calling party information for Mobile Twinning** box. This will allow the Caller ID for Twinning to be controlled by the setting on the SIP Line (**Section 5.4**). This setting also impacts the Caller ID for call forwarding.
- Click **OK** to commit (not shown).



5.2.4 System - Codecs Tab

For **Codec's** settings, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **Codecs** tab and configure the following parameters:

- In the **Codecs** tab of the Details Pane, select or enter **101** for **RFC2833 Default Payload**. This setting was recommended by Time Warner Cable for use with out-band DTMF tone transmissions.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific extension. The example below shows the codecs used for IP phones (SIP and H.323), codec G.711ULAW was used during the compliance testing.



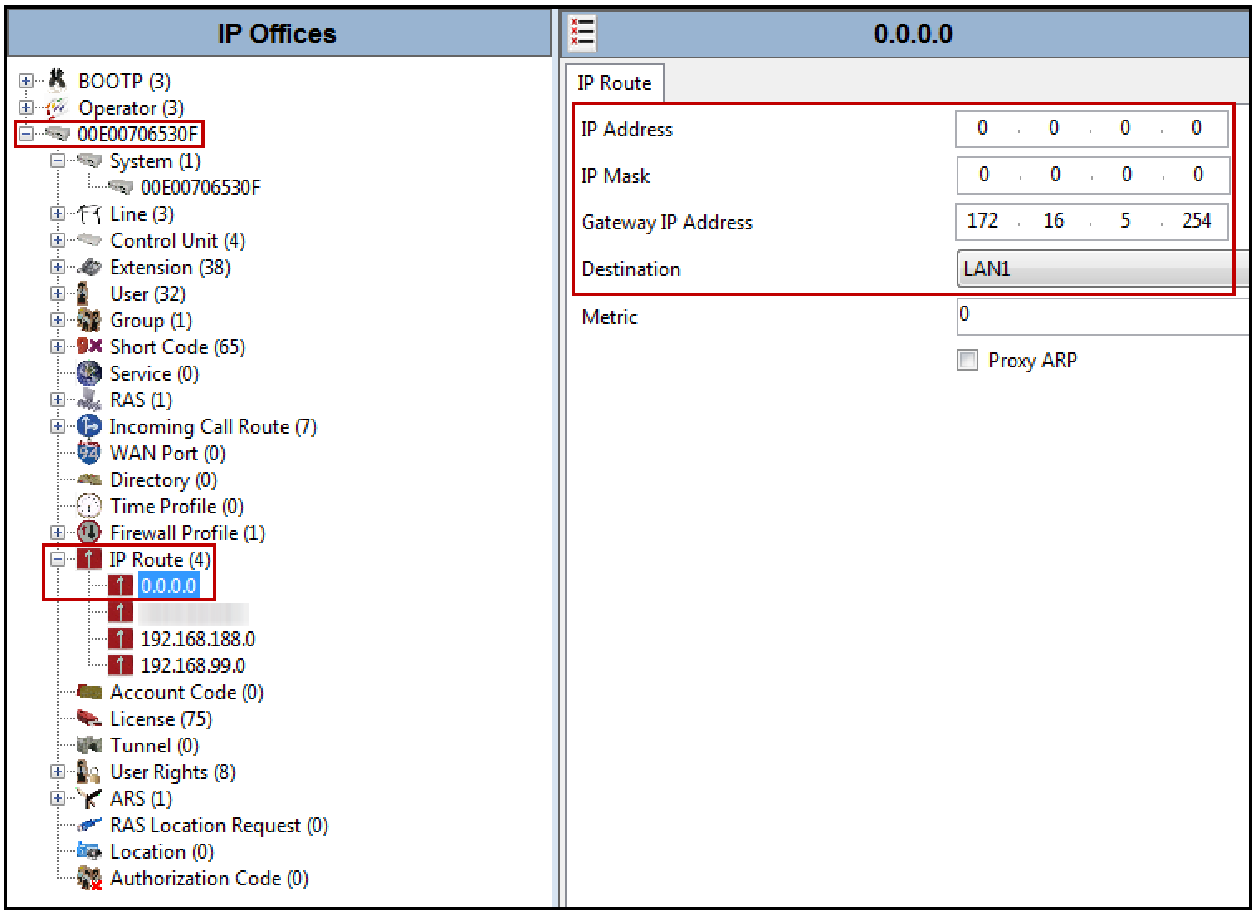
Note: The codec selections defined under this section (System – Codecs Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.7** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.3 IP Route

In the reference configuration, the IP Office LAN1 interface and the private interface of the Avaya SBCE resided on the same IP subnet, so an IP route was not necessary. In an actual customer configuration, these two interfaces may be in different IP subnets, and in that case an IP route would have to be created to specify the IP address of the gateway or router where IP Office needs to send the packets, in order to reach the IP subnet where the Avaya SBCE resides.

To create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides (if located in different IP subnets), on the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** of the IP subnet of the private side of the Avaya SBCE, or enter **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office IP subnet.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).



5.4 SIP Line

A SIP Line is needed to establish the SIP connection between IP Office and Time Warner Cable Business Class SIP Trunking Service. 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 Avaya IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.4.1** and **5.4.2** 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 trunk Registration Credentials.
- 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 **Section 5.4.3**.

Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.3** to **5.4.8**

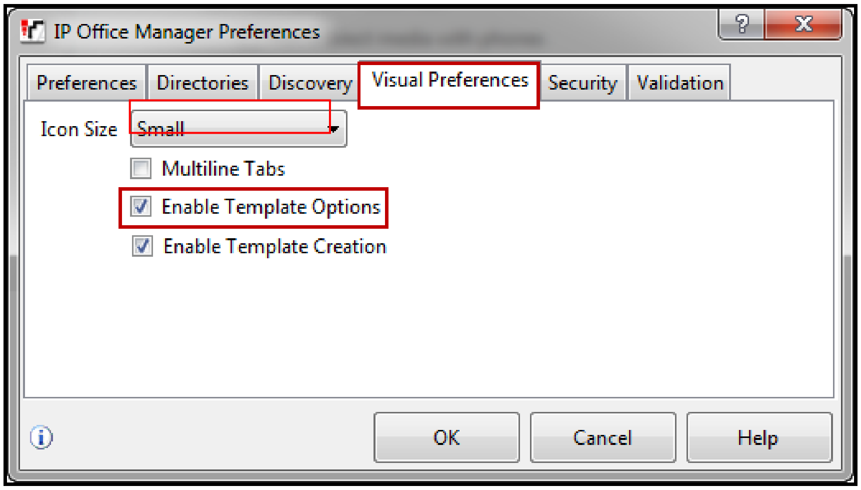
5.4.1 Importing a SIP Line Template

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.

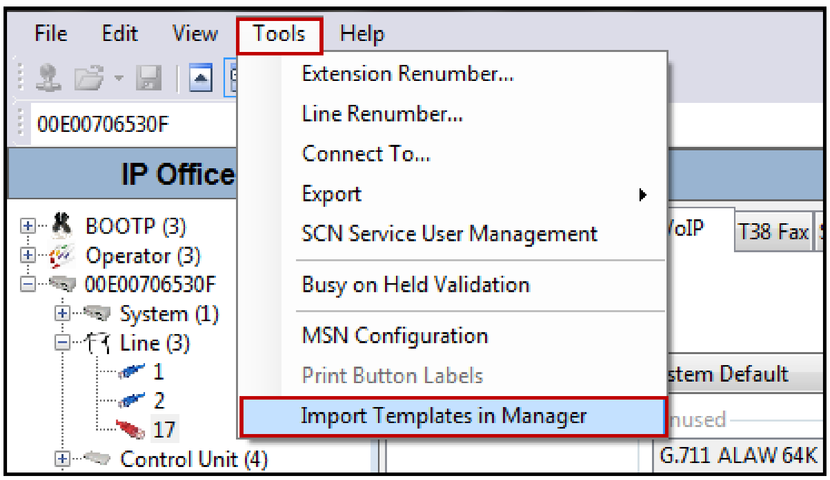
1. Copy a previously created template file to a location (e.g., C:*Temp*) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **AF_<*user supplied text*>_SIPTrunk.xml**, where the **<*user supplied text*>** portion is entered during template file creation.

Note – If necessary, the **<*user supplied text*>** portion of the template file name may be modified, however the **AF_<*user supplied text*>_SIPTrunk.xml** format of the file name must be maintained. For example, an original template file **AF_*TEST* _SIPTrunk.xml** could be changed to **AF_*Test1*_SIPTrunk.xml**. The template file name is selected in **Section 5.4.2**, **step 2**, to create a new SIP Line.

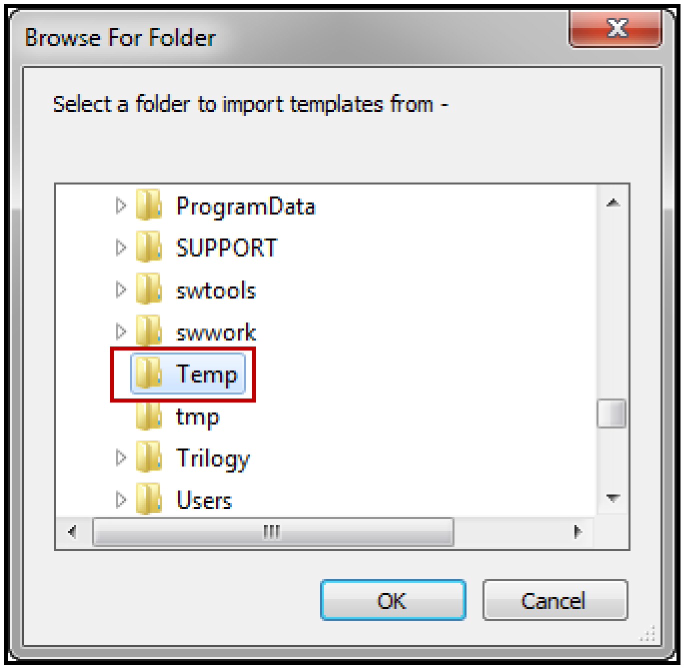
2. Verify that Template Options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the **Visual Preferences** tab. Check the box next to **Enable Template Options**. Click **OK**.



3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**.

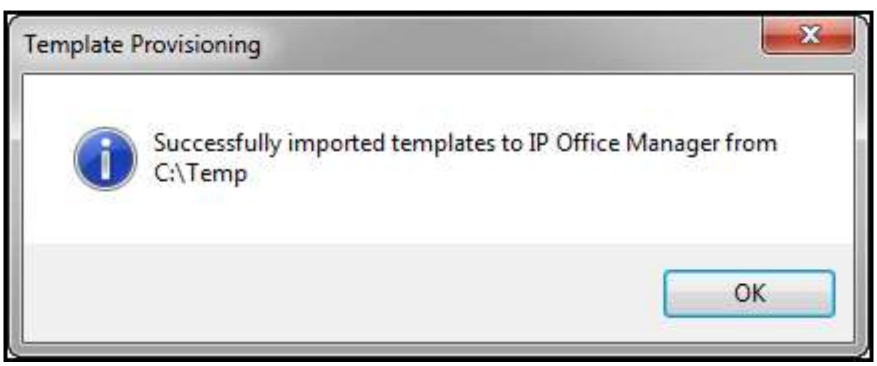


4. A folder browser will open. Select the directory used in **step 1** to store the template(s) (e.g., C:*Temp*).

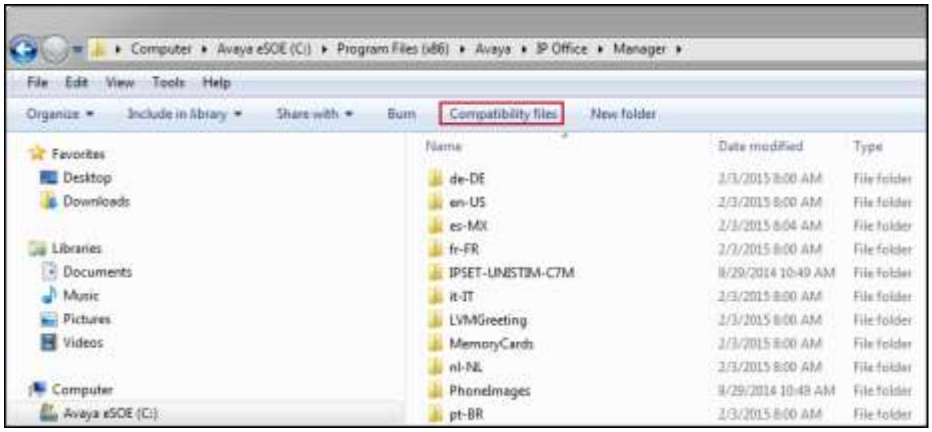


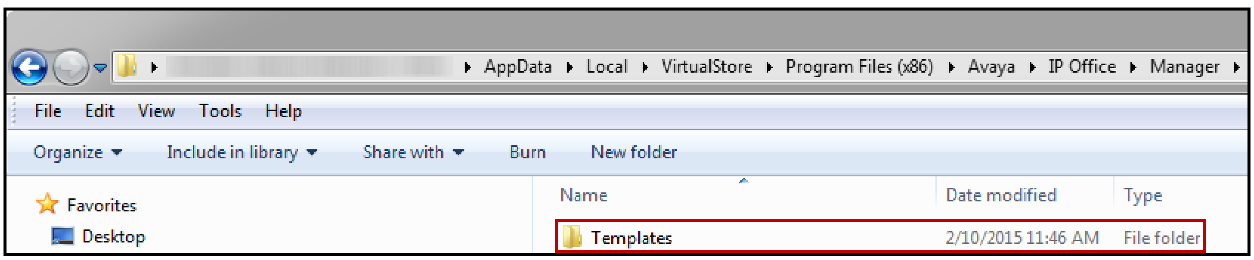
In the reference configuration, template files **AF_TWC with Avaya SBCE_ SIPTrunk.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

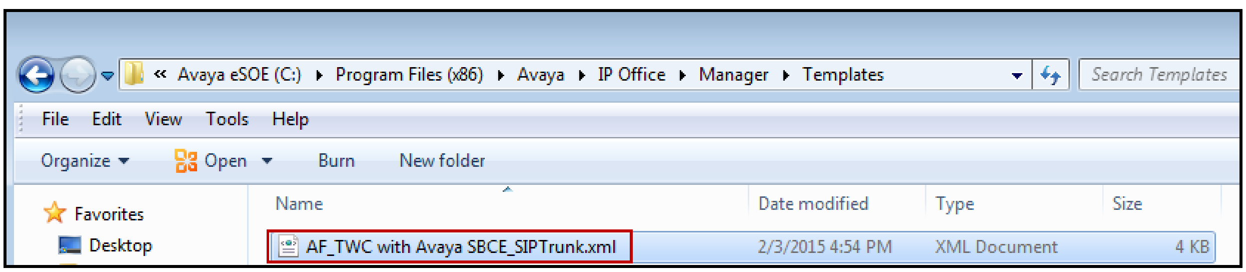
5. After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**.



Note –Windows 7 (and later) locks the Avaya IP Office 9.1 **\Templates** directory, and it cannot be viewed. To enable browsing of the **\Templates** directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or C:*Program Files (x86)*\Avaya\IP Office\Manager\Templates), and then click on the **Compatibility files** option shown below. The **\Templates** directory and its contents can then be viewed.

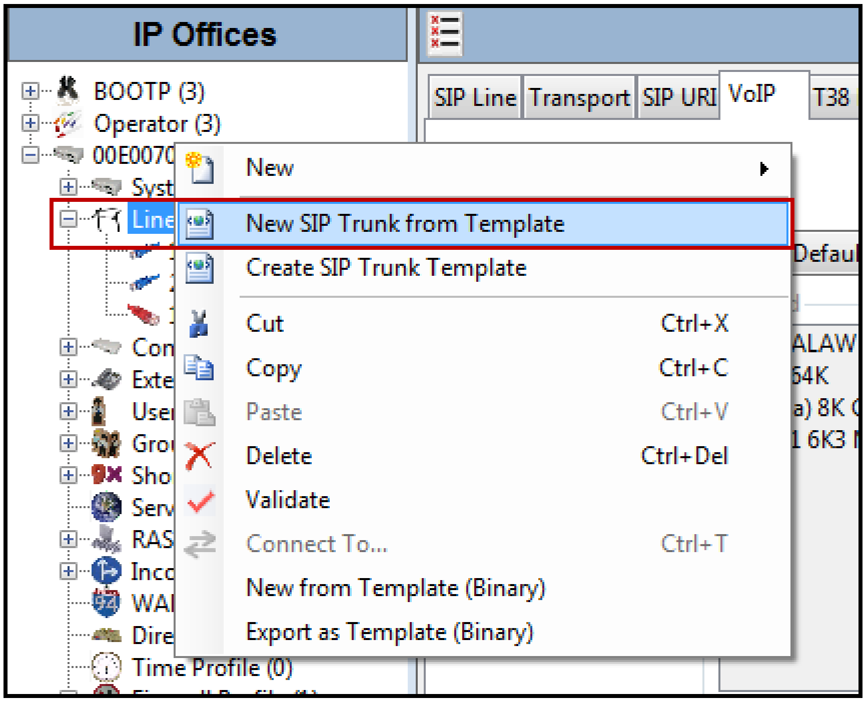






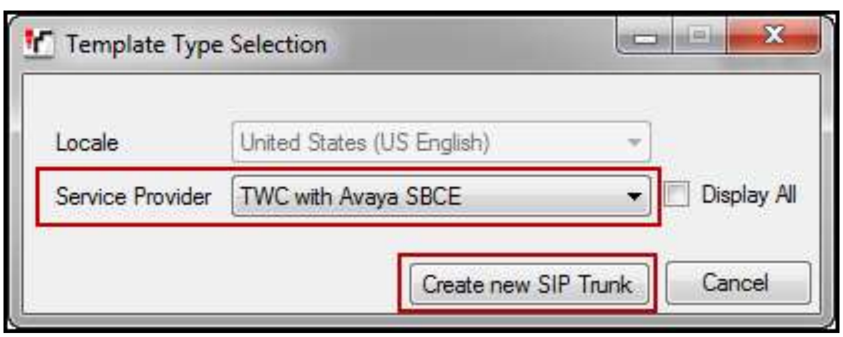
5.4.2 Creating a SIP Trunk from an XML Template

1. To create the SIP Trunk from a template, right-click on **Line** in the Navigation Pane, and select **New SIP Trunk from Template**.

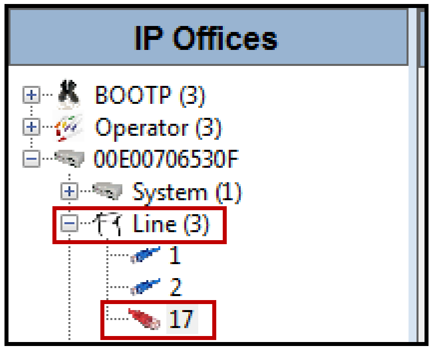


2. In the subsequent **Template Type Selection** pop-up window, from the **Service Provider** pull-down menu, select the XML template name from **Section 5.4.1**. Click **Create new SIP Trunk**.

Note – The drop down menu will display the **<*user supplied text*>** part of the template file name (see **Section 5.4.1**). If you check the **Display All** box, then the full template file name is displayed.



The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line **17**).

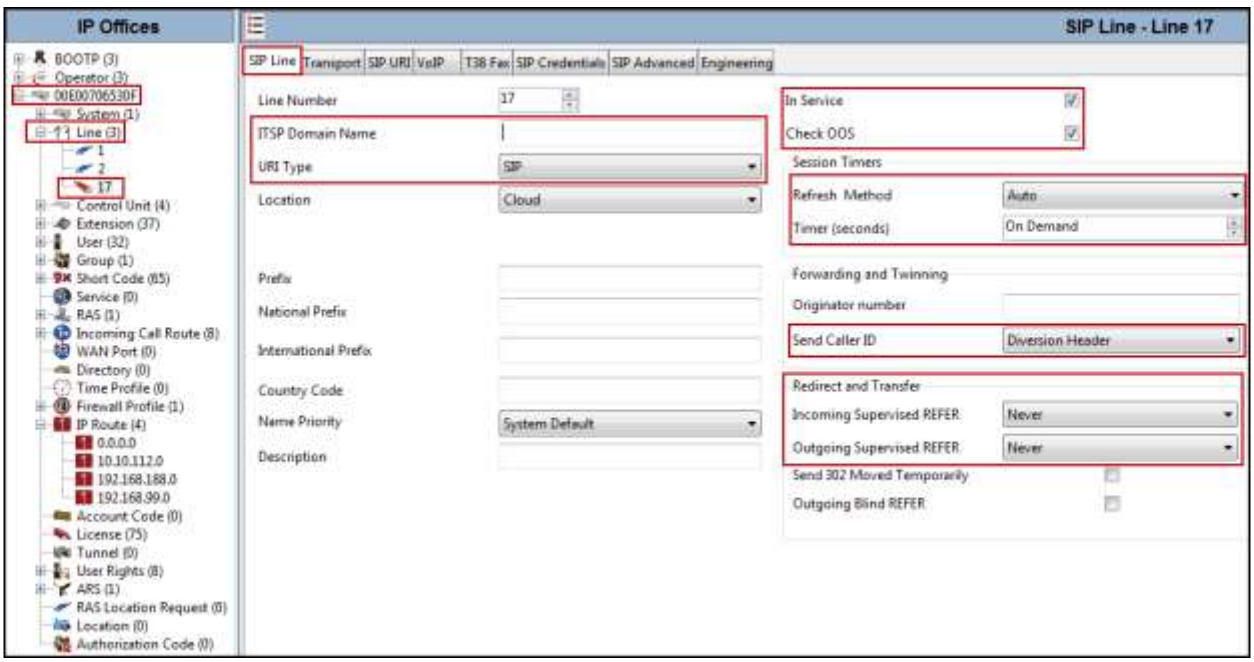


It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.3** to **5.4.8**.

5.4.3 SIP Line - SIP Line Tab

On the **SIP Line** tab in the Details Pane, configure or verify the parameters as shown below.

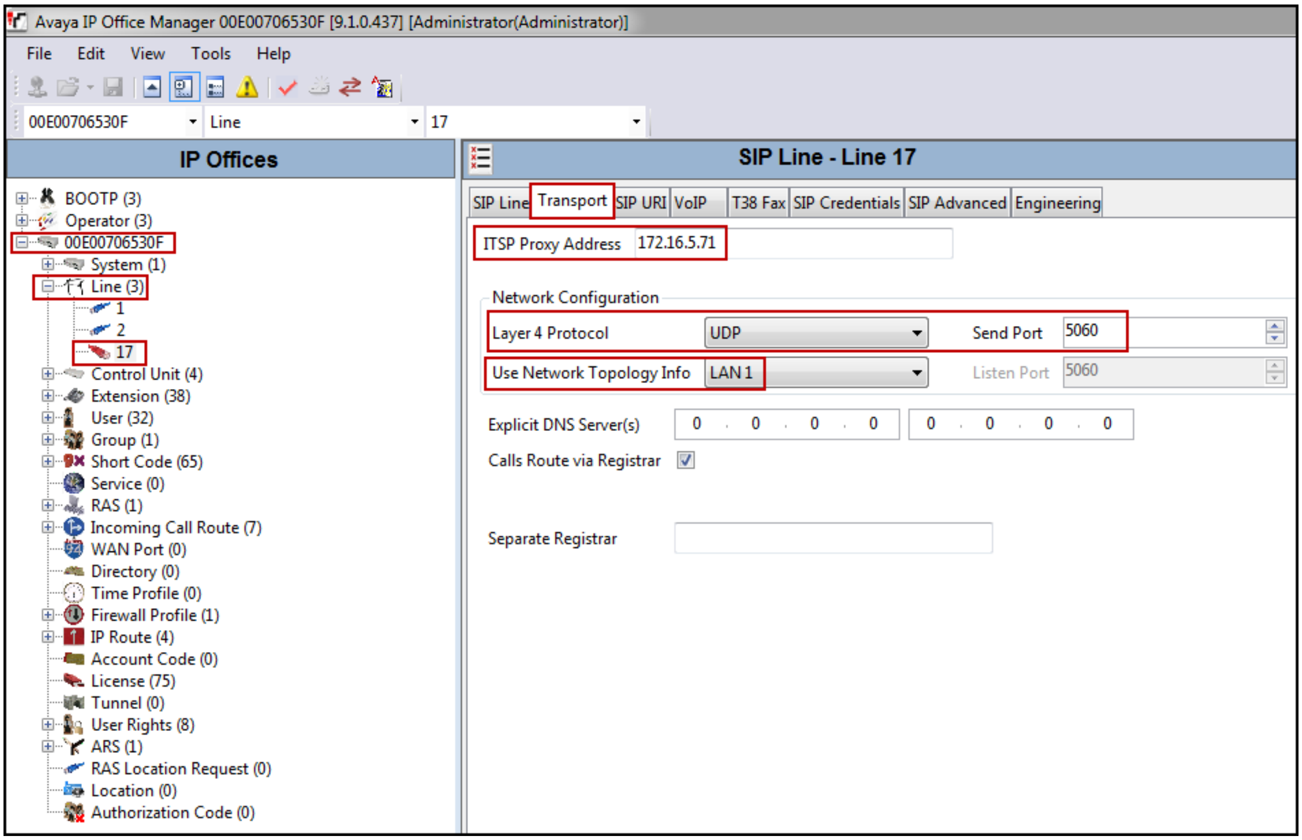
- Leave the **ITSP Domain Name** blank. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- Verify that **URI Type** is set to **SIP**.
- Verify that **In Service** box is checked, which is the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. 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 5.2.1**.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (seconds)** is set to **On Demand**.
- Set **Send Caller ID** to **Diversion Header**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER Support** and **Outgoing Supervised REFER** to **Never** (see **Section 2.1**).
- All other parameters should be set to default or according to customer requirements. Click **OK** to commit (not shown).



5.4.4 SIP Line - Transport Tab

Select the **Transport** tab; configure the parameters as shown below:

- Set the **ITSP Proxy Address** to the inside IP Address of the Avaya SBCE or **172.16.5.71** as shown in **Figure 1**.
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



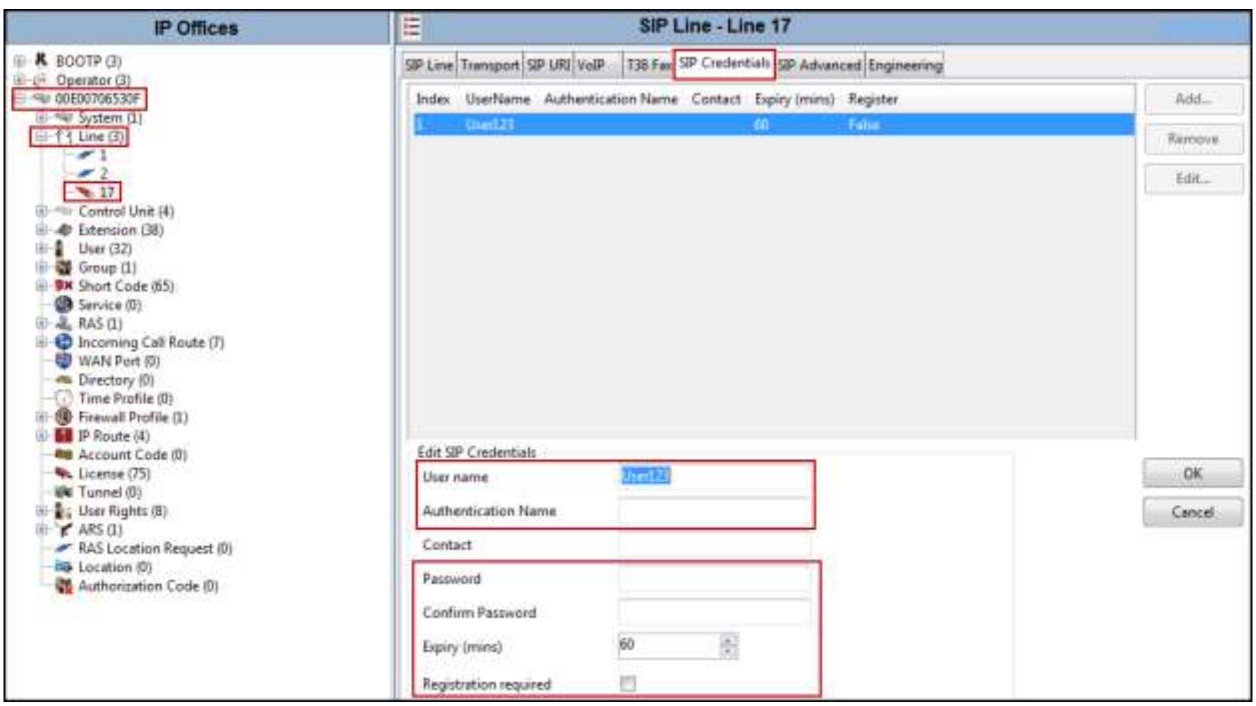
5.4.5 SIP Line – SIP Credentials Tab

SIP Credentials are used to register the SIP Trunk with a service provider that requires SIP Registration. SIP Credentials are also used to provide the required information for Digest Authentication of outbound calls. SIP Credentials are unique per customer and therefore customers must contact the service provider to obtain the proper registration credentials for their deployment.

Note: The SIP Credentials configuration settings shown below are only used to provide the required information for Digest Authentication of outbound calls. In IP Office configurations with the Avaya SBCE, SIP Trunk Registration to the Service Provider's SIP Trunk Service is done by the Avaya SBCE, and **not** by IP Office, Refer to **Section 6.2.3**.

Select the **SIP Credentials** tab, and then click the **Add** button to add the SIP Trunk registration credentials. Set the parameters as shown below:

- For **User name**, add the User name credential provided by Time Warner Cable for SIP Trunk registration. This is the same **User Name** credential, used by the Avaya SBCE, under the Avaya SBCE **Server Configuration**, refer to **Section 6.2.3**.
- Leave **Authentication Name** blank, this field is not used. SIP Trunk Registration to Time Warner Cable SIP Trunk Service will be done by the Avaya SBCE.
- Leave the **Password** blank, this field is not used. SIP Trunk Registration to Time Warner Cable SIP Trunk Service will be done by the Avaya SBCE.
- The **Expiry (mins)** can be left with the default value of **60** mins; this field is not used. SIP Trunk Registration to Time Warner Cable SIP Trunk Service will be done by the Avaya SBCE.
- The **Registration required** should be unchecked; this field is not used. SIP Trunk Registration to Time Warner Cable SIP Trunk Service will be done by the Avaya SBCE.
- Click the **OK** to commit.

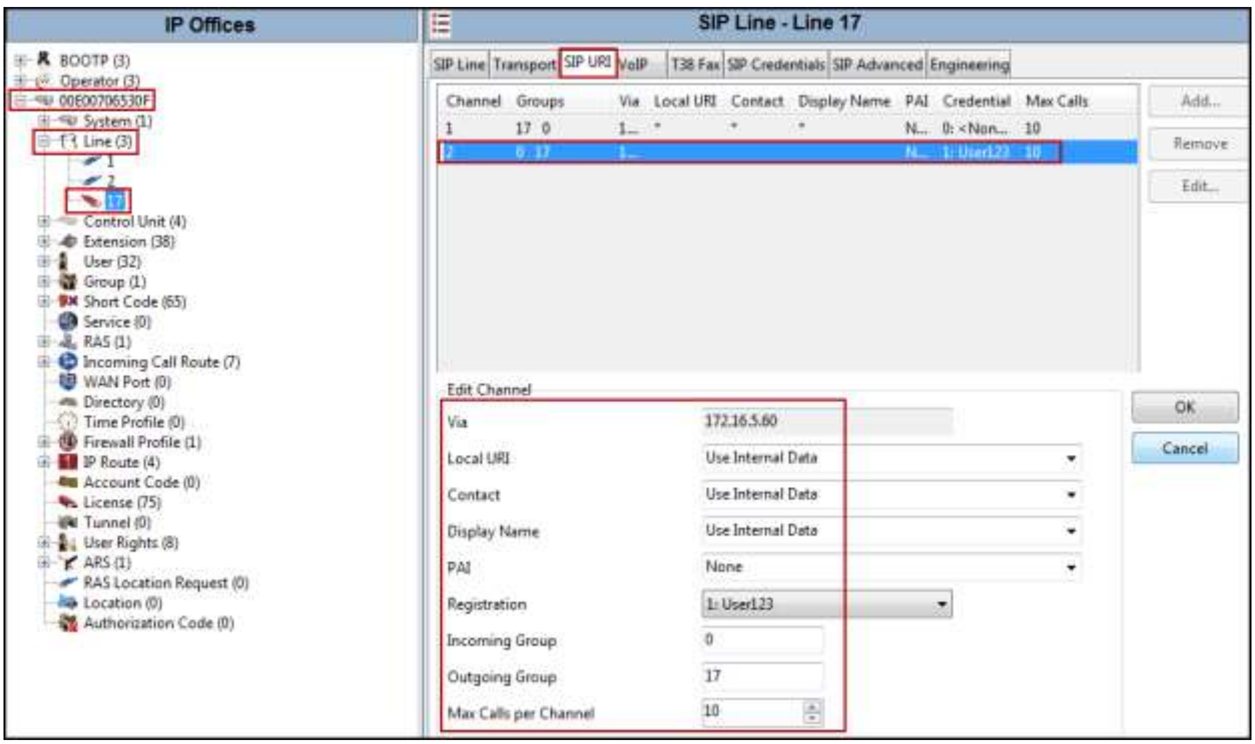


5.4.6 SIP Line - SIP URI Tab

Two SIP URI entries must be created to match each outgoing number that Avaya IP Office will send on this line and incoming numbers that Avaya IP Office will accept on this line.

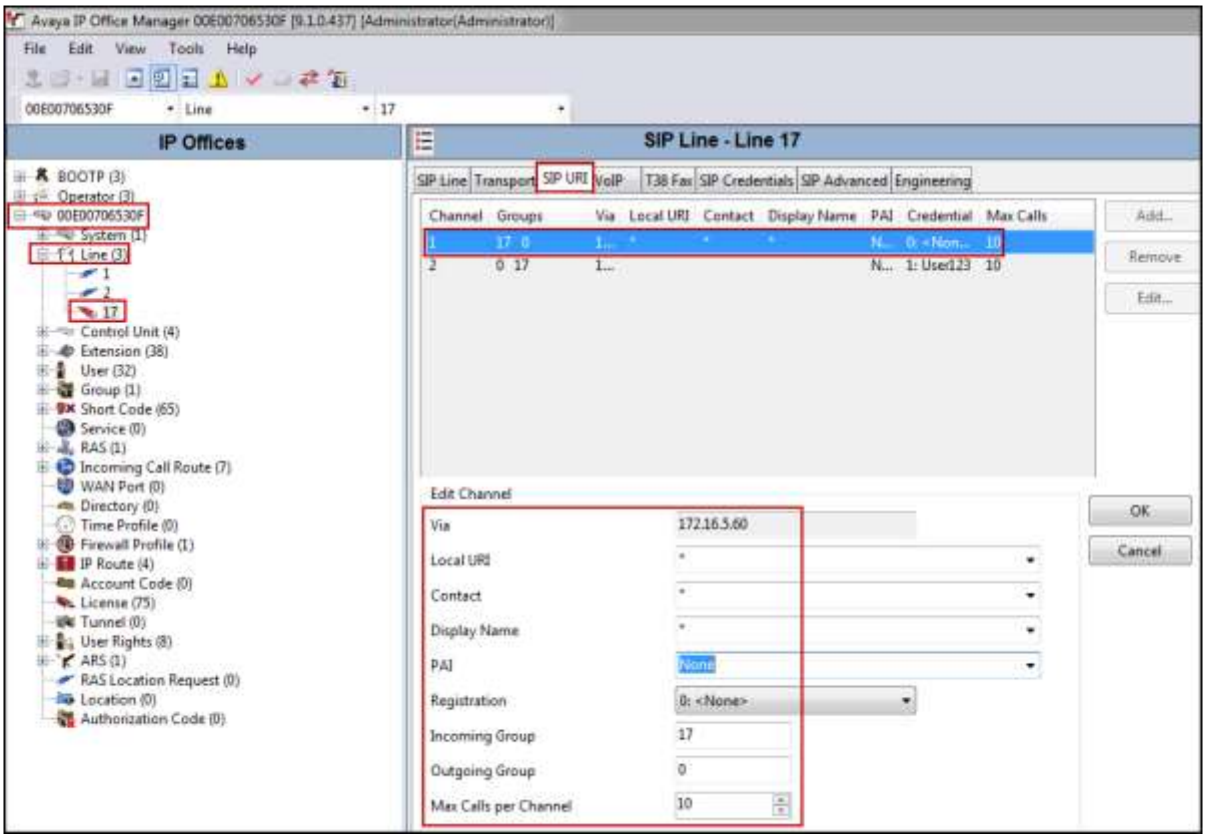
To set the SIP URI for outgoing numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact**, **Display Name** to **Use Internal Data**.
- Set **PAI** to **None**.
- Set **Registration** to **1: User123** (Note that this field will default to the **User Name** used under the **SIP Credentials** tab).
- Set **Incoming Group** to **0**.
- Set **Outgoing Group** to **17** (SIP Line number being used).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit.



To set the SIP URI for incoming numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact**, and **Display Name** to "*****" (asterisk).
- Set **PAI** to **None**.
- Set **Registration** to **0: <None>**.
- Set **Incoming Group** to **17** (SIP Line number being used).
- Set **Outgoing Group** to **0**.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit.

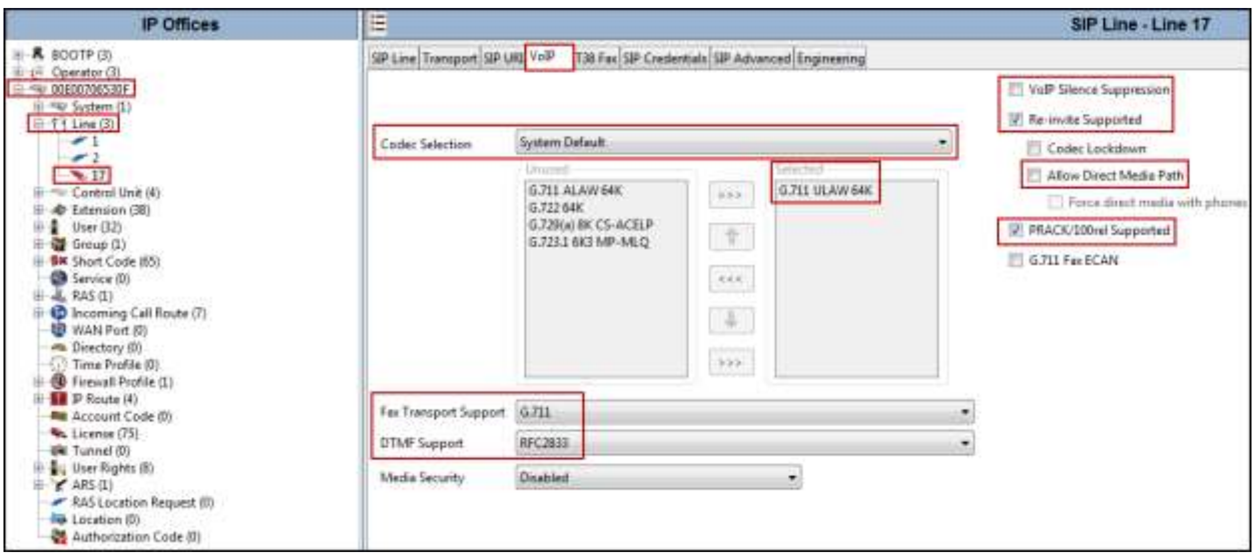


Additional SIP URIs may be required to allow inbound calls to numbers not associated with a user, such as a short code. These URIs are created in the same manner as shown above with the exception that the incoming DID number is entered directly in the **Local URI**, **Contact**, and **Display Name** fields.

5.4.7 SIP Line - VoIP Tab

Select the **VoIP** tab, to set the Voice over Internet Protocol parameters of the SIP Line. Set or verify the parameters as shown below.

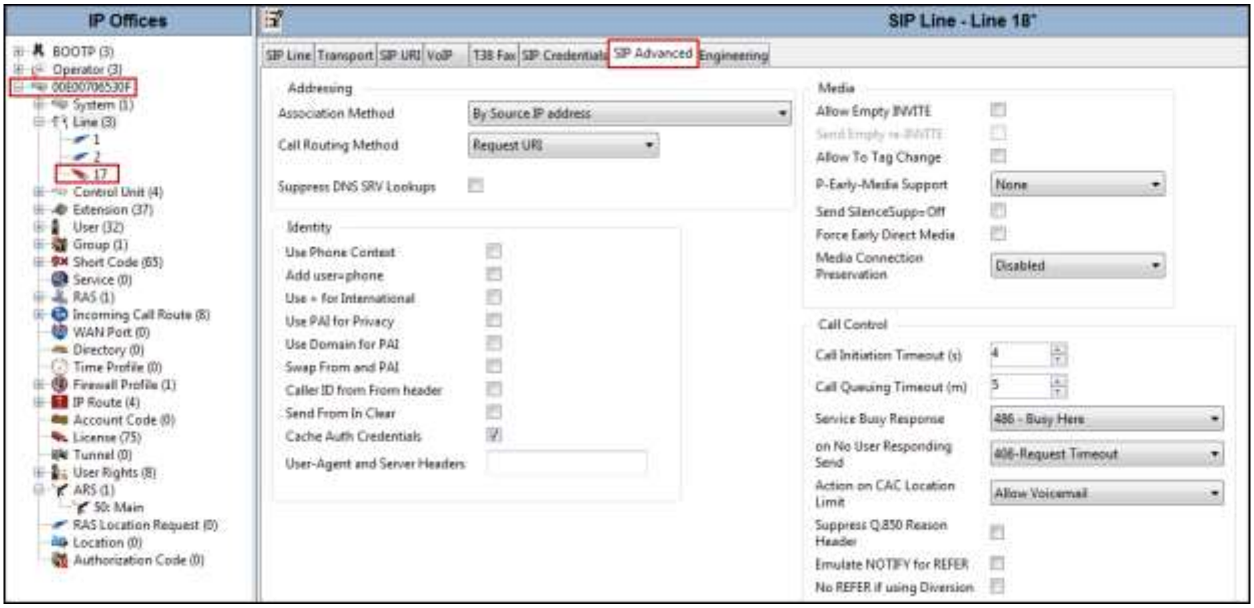
- Set the **Codec Selection** to **System Default**. With this setting the System default codec selection configured under **Section 5.2.4** will be used. The **Codec Selection** can be configured using the **Custom** option instead, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line. Since Time Warner Cable only supports codec G.711ULAW for audio, the System Default was used.
- Select **G.711** for **Fax Transport Support**.
- Set the **DTMF Support** field to **RFC2833**. This directs IP Office to send DTMF tones as out-band RTP events as per RFC2833.
- Uncheck the **VoIP Silence Suppression** option box.
- Check the **Re-invite Supported** option box.
- Verify that **Codec Lockdown** is unchecked.
- Verify that **Allow Direct Media Path** is unchecked.
- Check the **PRACK/100rel Supported** option box. This setting enables support by IP Office for the PRACK (Provisional Reliable Acknowledgement) message on SIP trunks.
- Click the **OK** to commit (not shown).



Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.4** (System –Codec tab) are the codecs selected for the IP phones/extension (H.323 and SIP). Since Time Warner Cable only supports codec G.711ULAW, the Codec Selection was set to use **System Default** defined under **Section 5.2.4**.

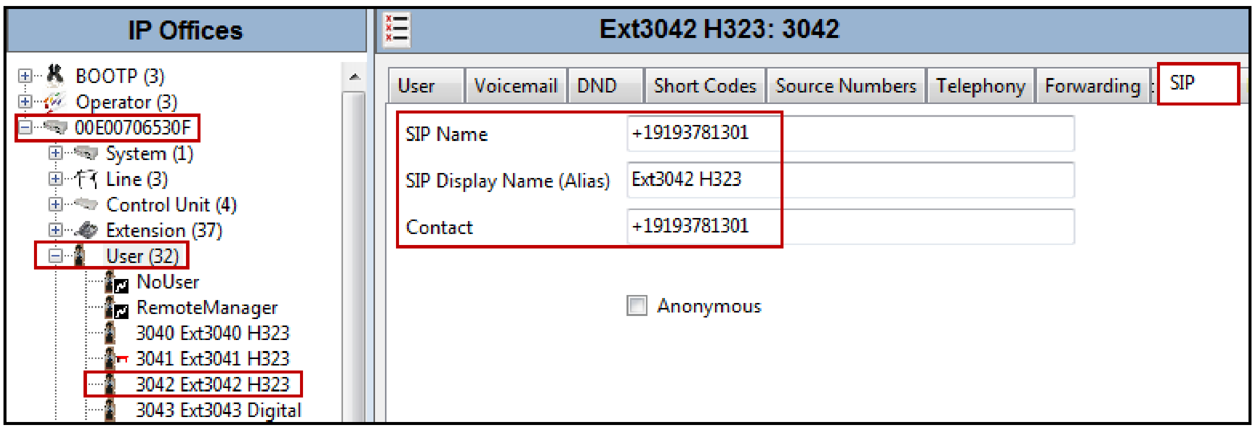
5.4.8 SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab, no changes are required to be made on the **SIP Advanced** tab, default values are used. Verify that all settings are configured with default values as shown below.



5.5 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line defined in **Section 5.4**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Ext3042 H323**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP Line (**Section 5.4.6**). The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Time Warner Cable. Note that a "+" sign was added to the DID number for each user under **SIP Name** and **Contact**, IP Office will insert the "+" sign in front of the 11 digit number included in the **Diversion** header on calls that are re-directed to the PSTN, this is required by Time Warner Cable. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network. This can also be accomplished by activating Withhold Number on H.323 Deskphones (not shown). Click the **OK** to commit (not shown).



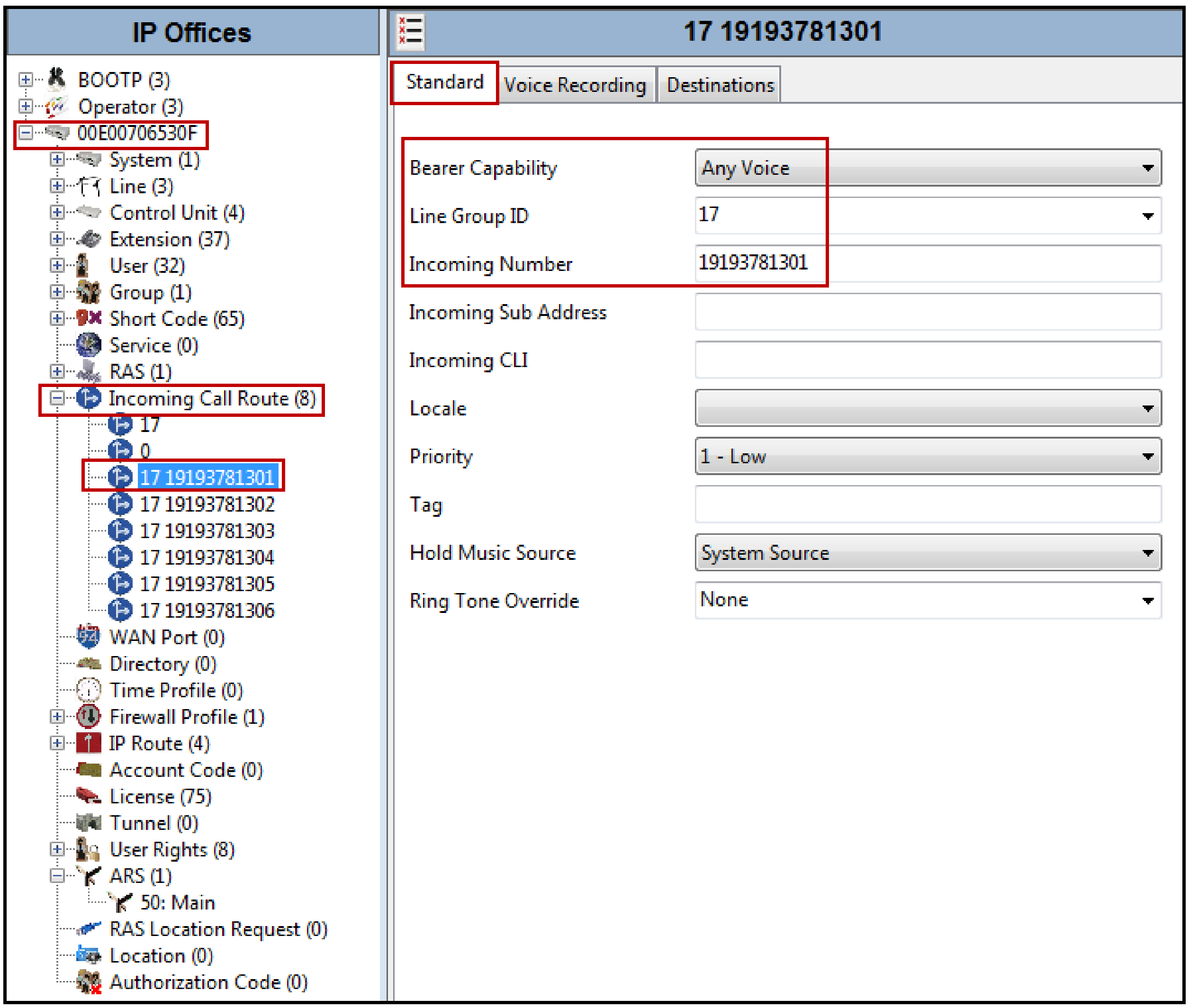
5.6 Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number assigned to IP Office users. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**.

5.6.1 Incoming Call Route – Standard Tab

On the **Standard** tab of the Details Pane, enter the parameters as shown below.

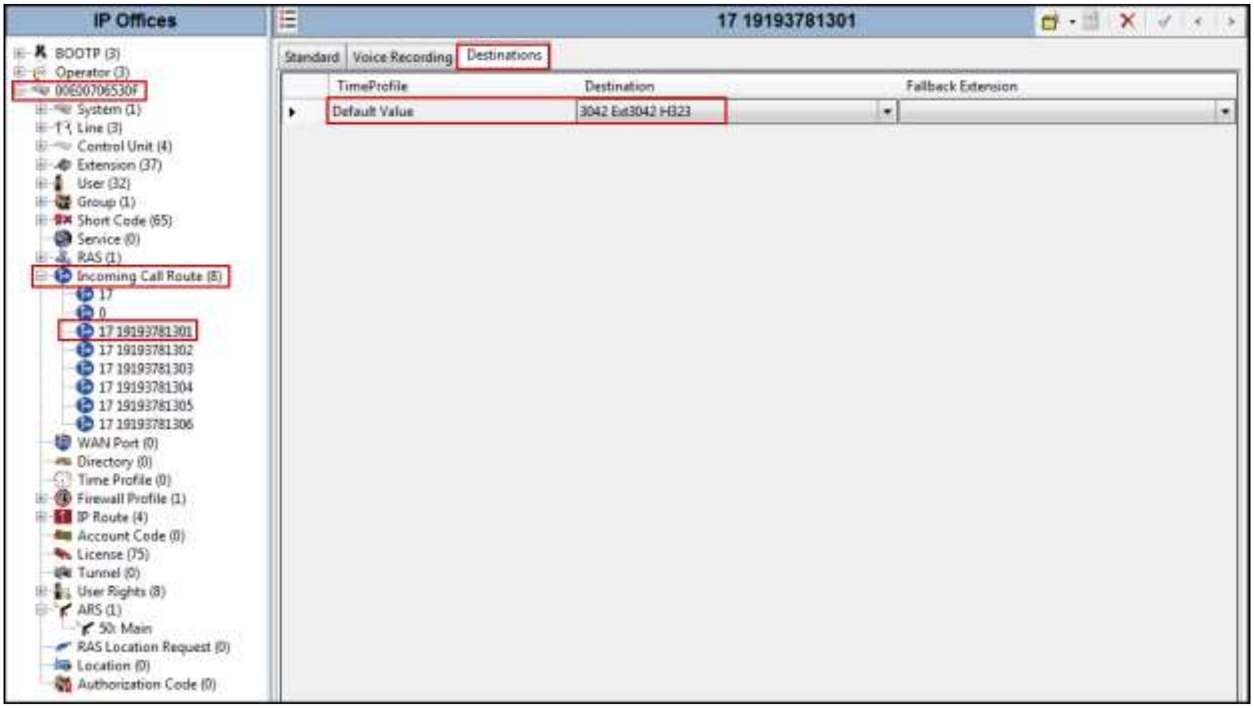
- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4**.
- Set the **Incoming Number** to the incoming DID number on which this route should match.
- Default values can be used for all other fields.



5.6.2 Incoming Call Route – Destinations Tab

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 19193781301 on line 17 are routed to extension 3042.



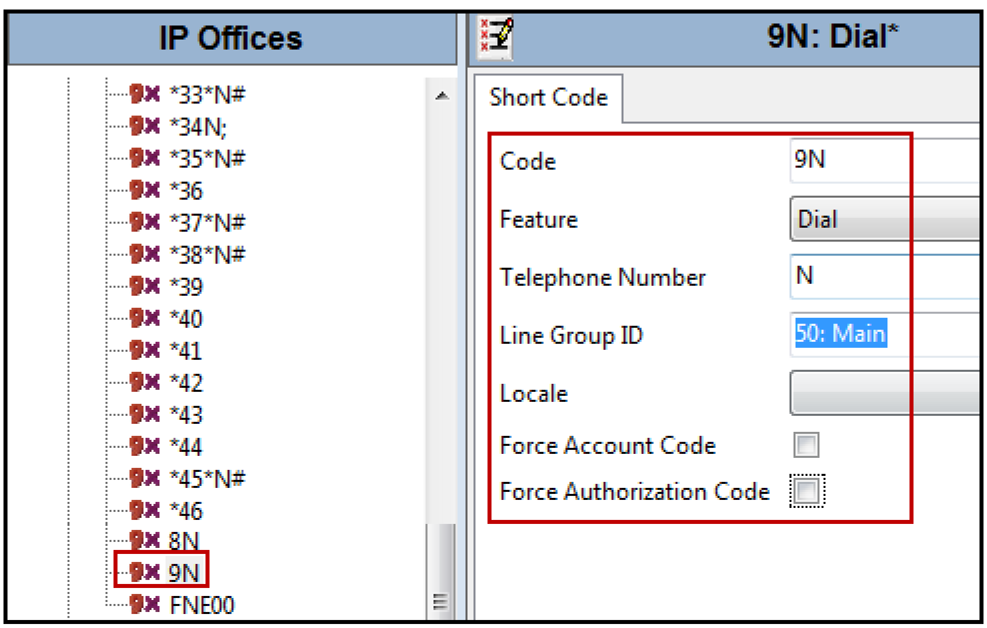
5.7 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance testing.

5.7.1 Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** on the Navigation Pane and select **New**. The screen below shows the short code **9N** created (note that the semi-colon is not used here). In this case, when the IP Office user dials 9 plus any number **N**, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS.

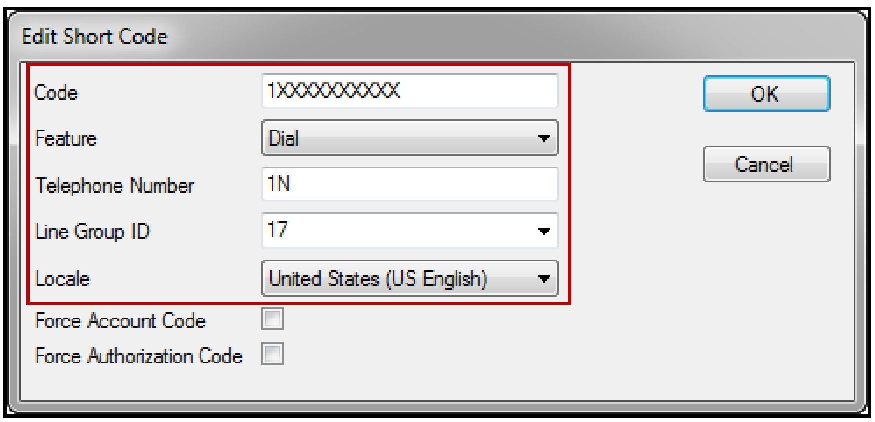
- In the **Code** field, enter the dial string which will trigger this short code. In this case, **9N** was used (note that the semi-colon is not used here).
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group ID** to **50: Main** to be directed to **Line Group 50: Main**, which is configurable via ARS.
- Click the **OK** to commit (not shown).



The following screen shows a sample ARS configuration for the route **Main**. Note the sequence of **X**’s used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

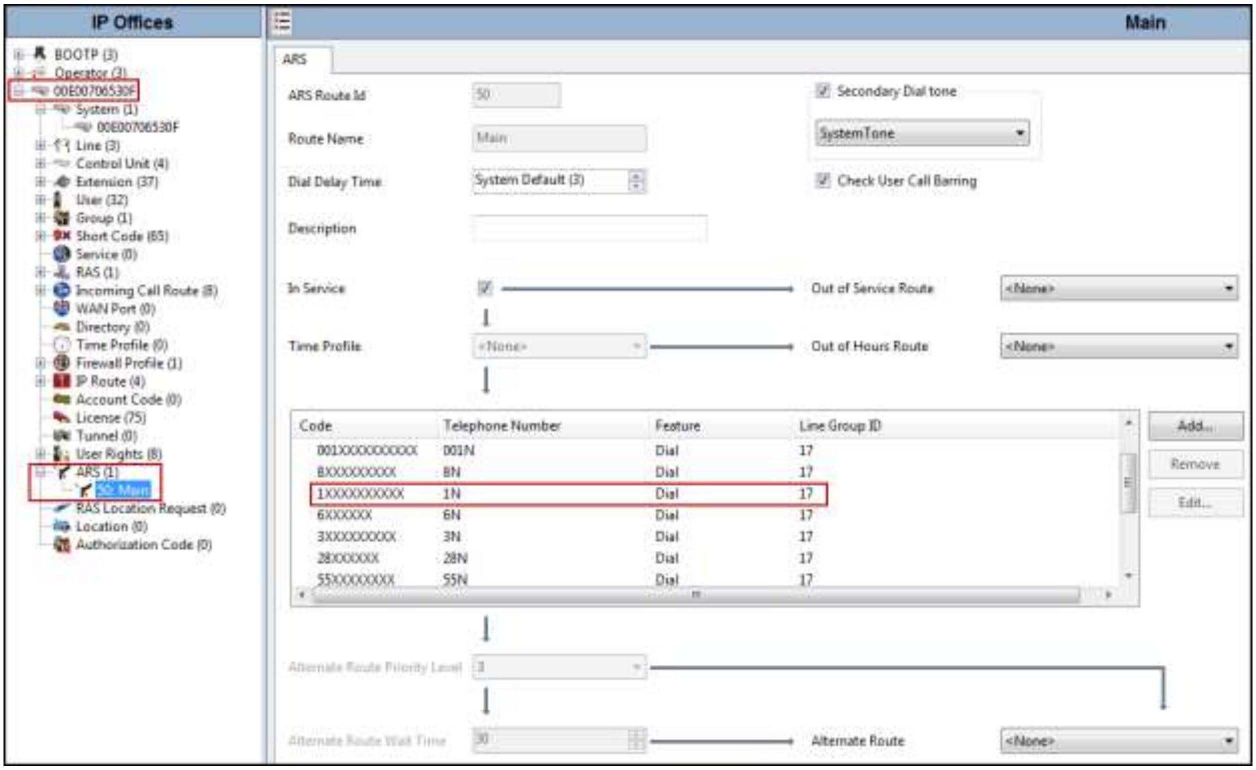
To create a short code to be used for ARS, select **ARS → 50: Main** on the Navigation Pane and click **Add**.

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **1** followed by **10 X**’s to represent the exact number of digits.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **1N**. The value **N** represents the additional number of digits dialed by the user after dialing **1** (The **9** will be stripped off).
- Set the **Line Group ID** to the Line Group number being used for the SIP Line, in this case Line **Group ID 17** was used.
- Set **Locale** to **United States (US English)**.
- Click **OK** to commit.



Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

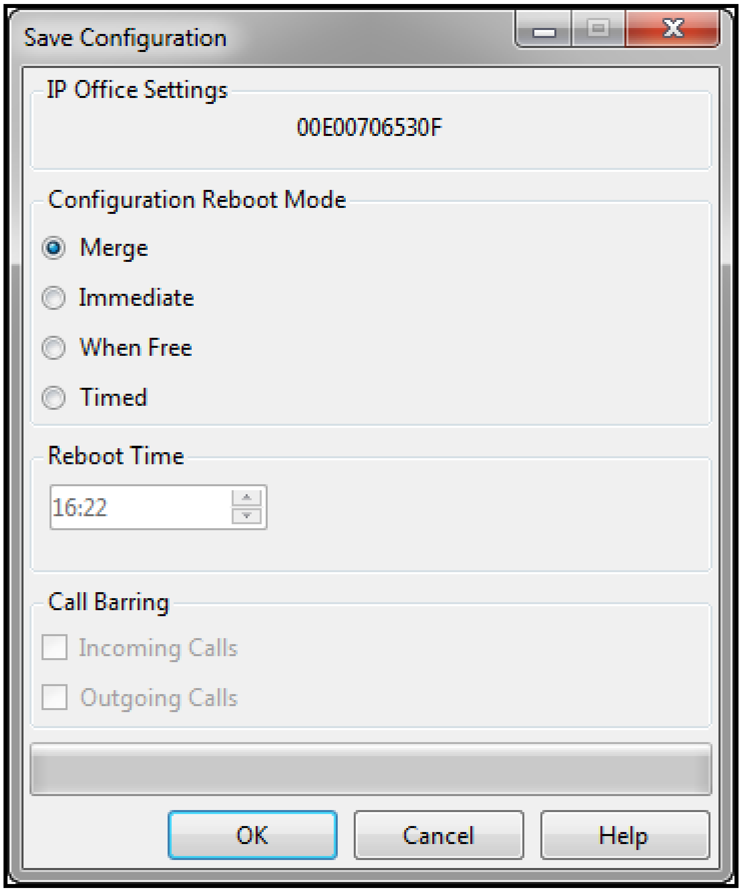
The example highlighted below shows that for calls in the North American numbering plan, the user dialed **9**, followed by **1** and **10** digits (represented by **10 X**'s). The **9** is stripped off, the remaining digits, including the **1**, are included in the SIP INVITE message IP Office sends to Time Warner Cable.



5.8 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 **Immediate** 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.



6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).

This section describes the required configuration of the Avaya SBCE to connect to Time Warner Cable Business Class SIP Trunking Service.

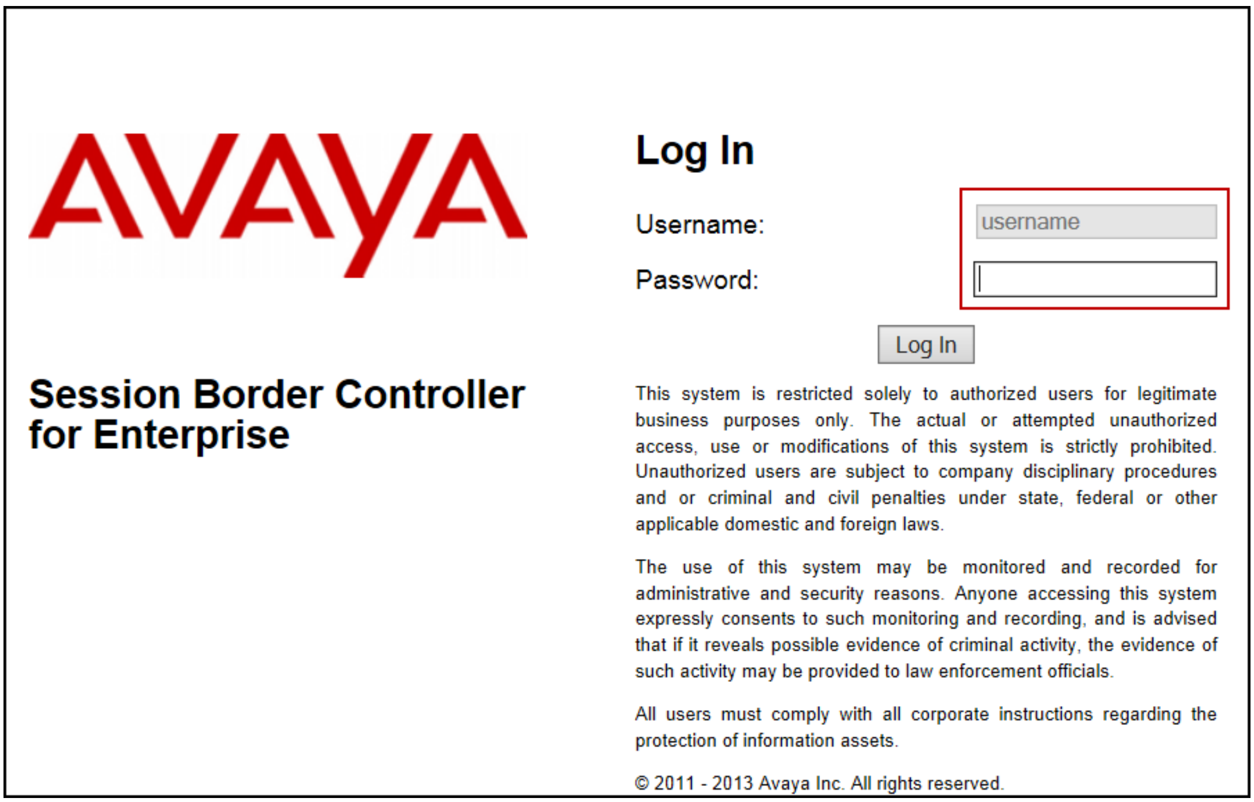
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

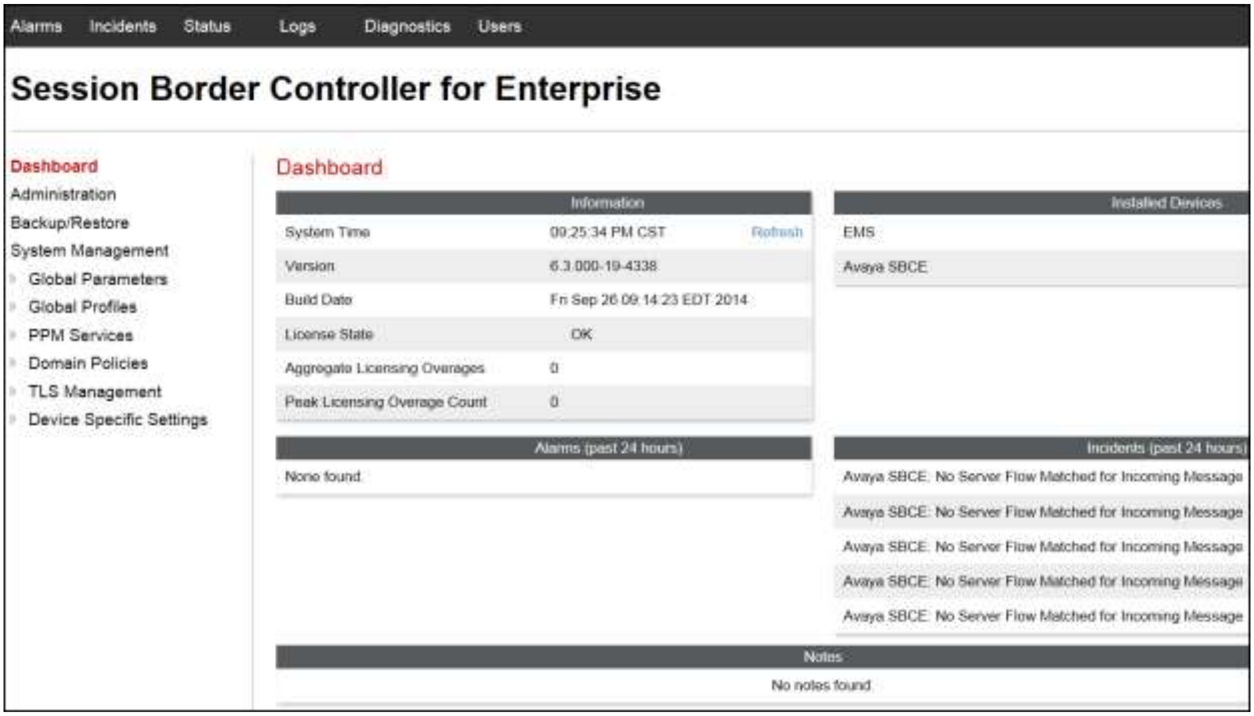
6.1 Log in Avaya SBCE

Use a Web browser to access the Avaya SBCE Web interface. Enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the Avaya SBCE management IP address.

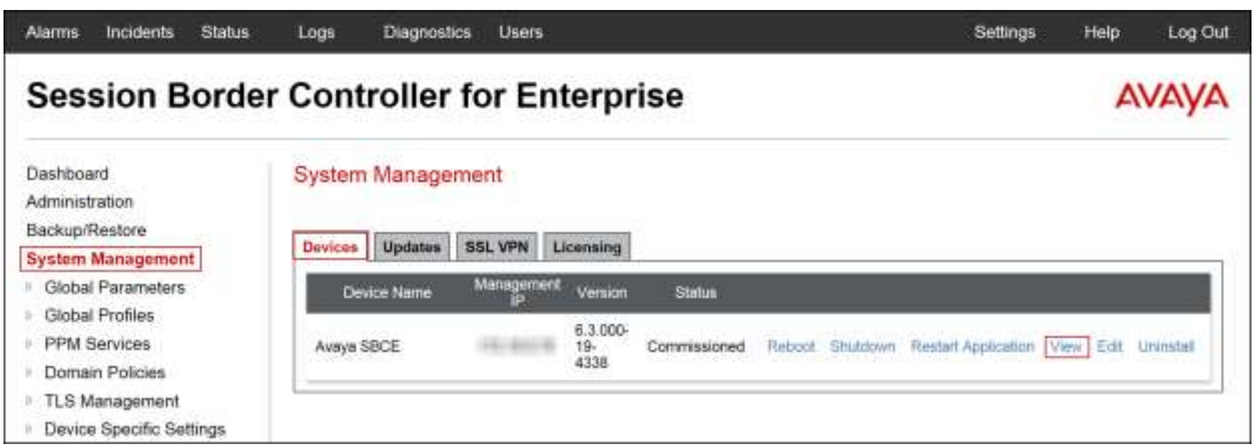
Enter the appropriate credentials and click **Log In**.



The **Dashboard** main page will appear as shown below.

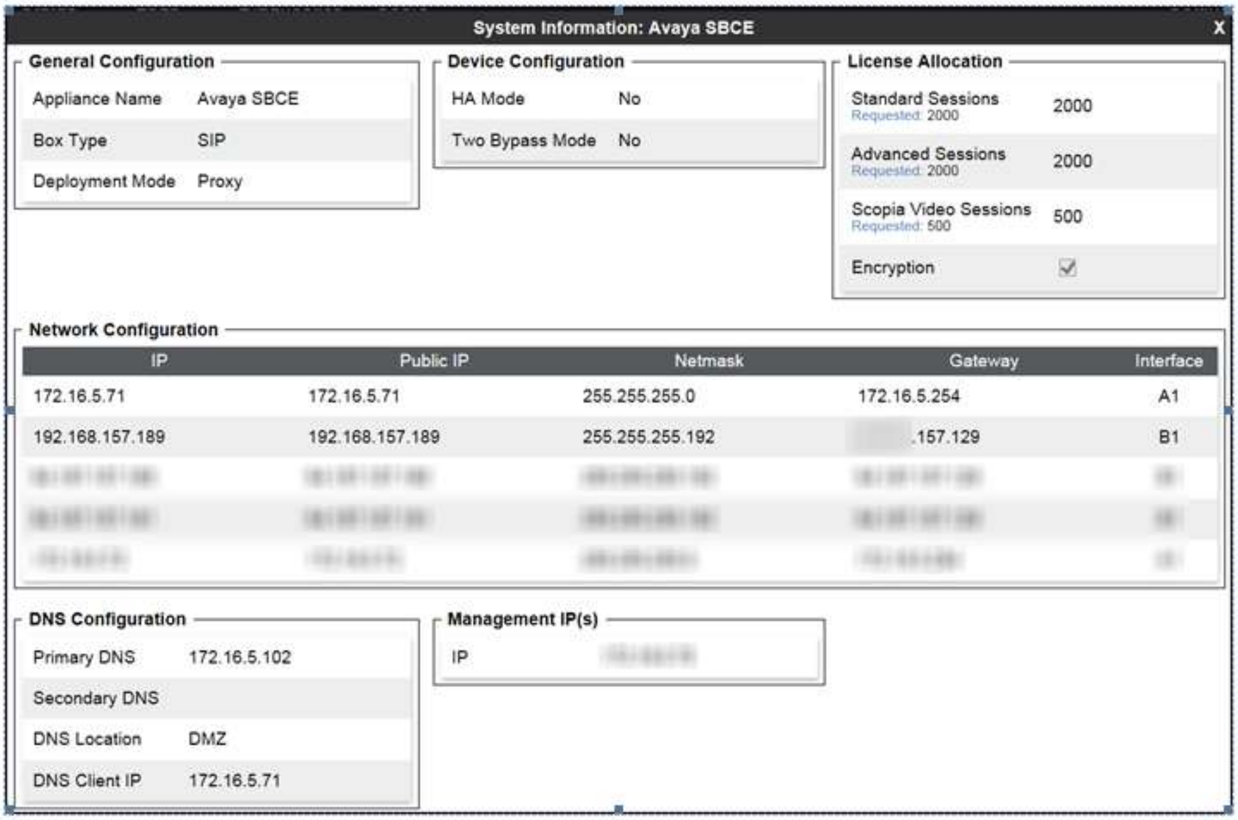


To view the system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya SBCE** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.



To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

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



On the previous screen, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces of the Avaya SBCE, respectively. The **A1** and **B1** interfaces and IP addresses shown are the ones relevant to the configuration of the SIP trunk to Time Warner Cable. Other IP addresses assigned to these interfaces are used to support other functionalities not discussed in this document, these IP addresses have been blurred out. The management IP has also been blurred out for security reasons.

IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled "M1") of the Avaya SBCE <u>must</u> be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to have this resolved.

6.2 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

6.2.1 Server Interworking – Avaya-IPO

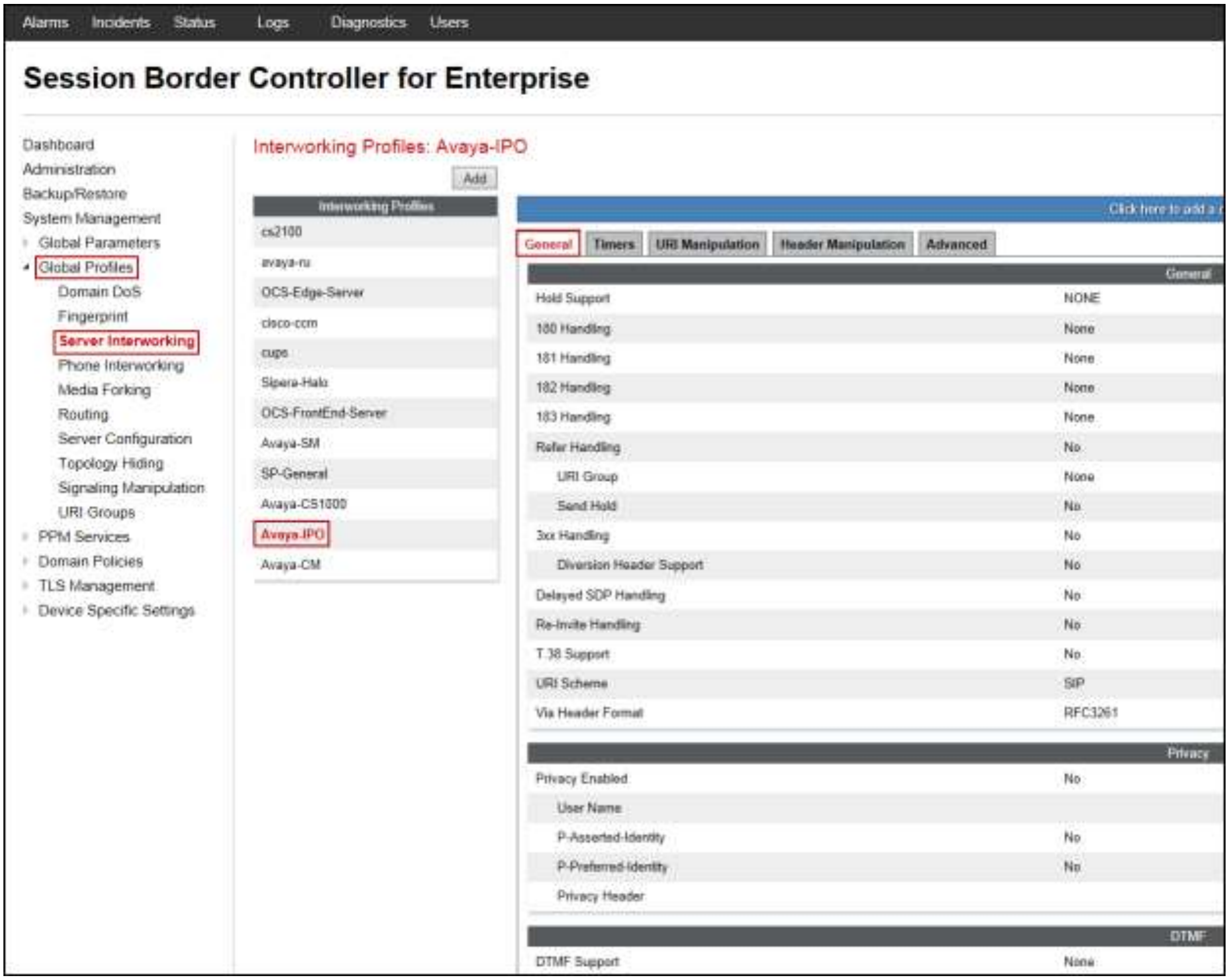
Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or "cloned". Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or "cloned". If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution. For Time Warner Cable, this profile was left with the **avaya-ru** default values.

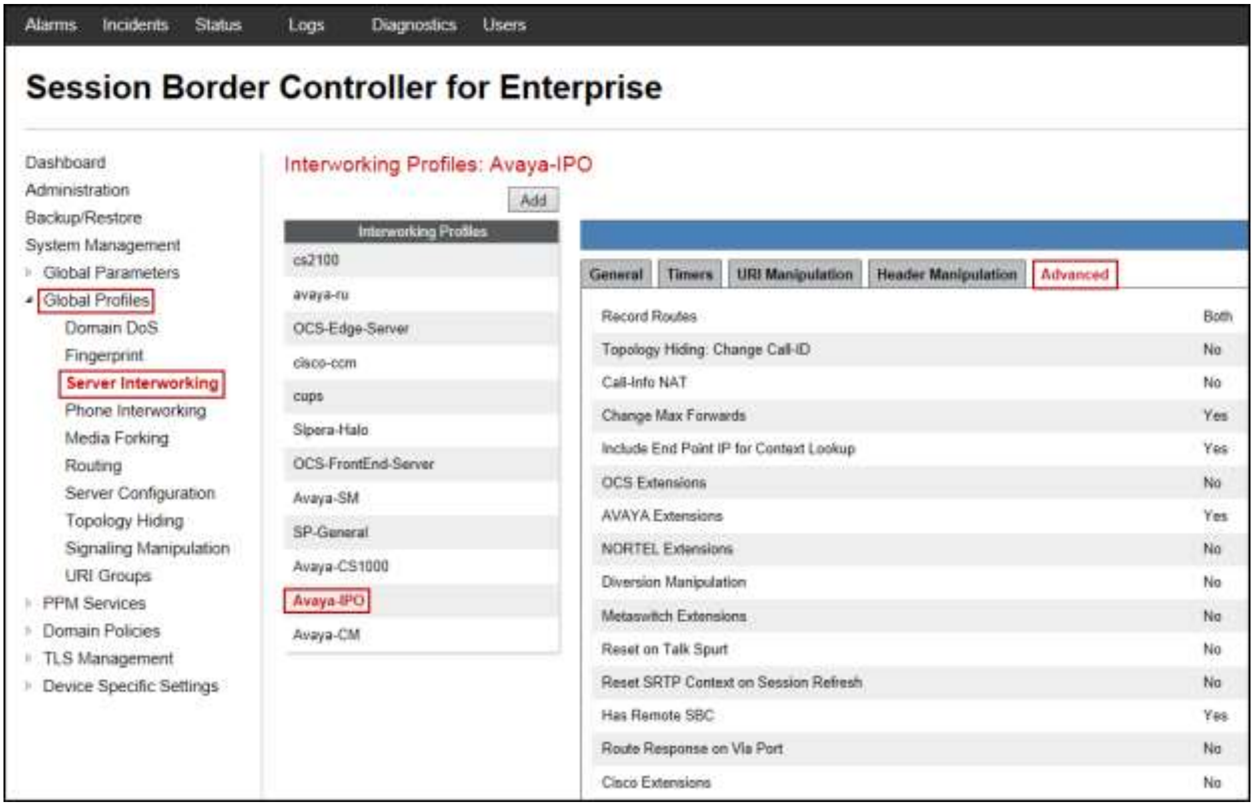
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone** on top right of the screen.

Enter the new profile name in the **Clone Name** field, the name of ***Avaya-IPO*** was chosen in this example. Click **Finish**.

The following screen capture shows the **General** tab of the newly created **Avaya-IPO** Server Interworking Profile.



The following screen capture shows the **Advanced** tab of the newly created **Avaya-IPO** Server Interworking Profile.



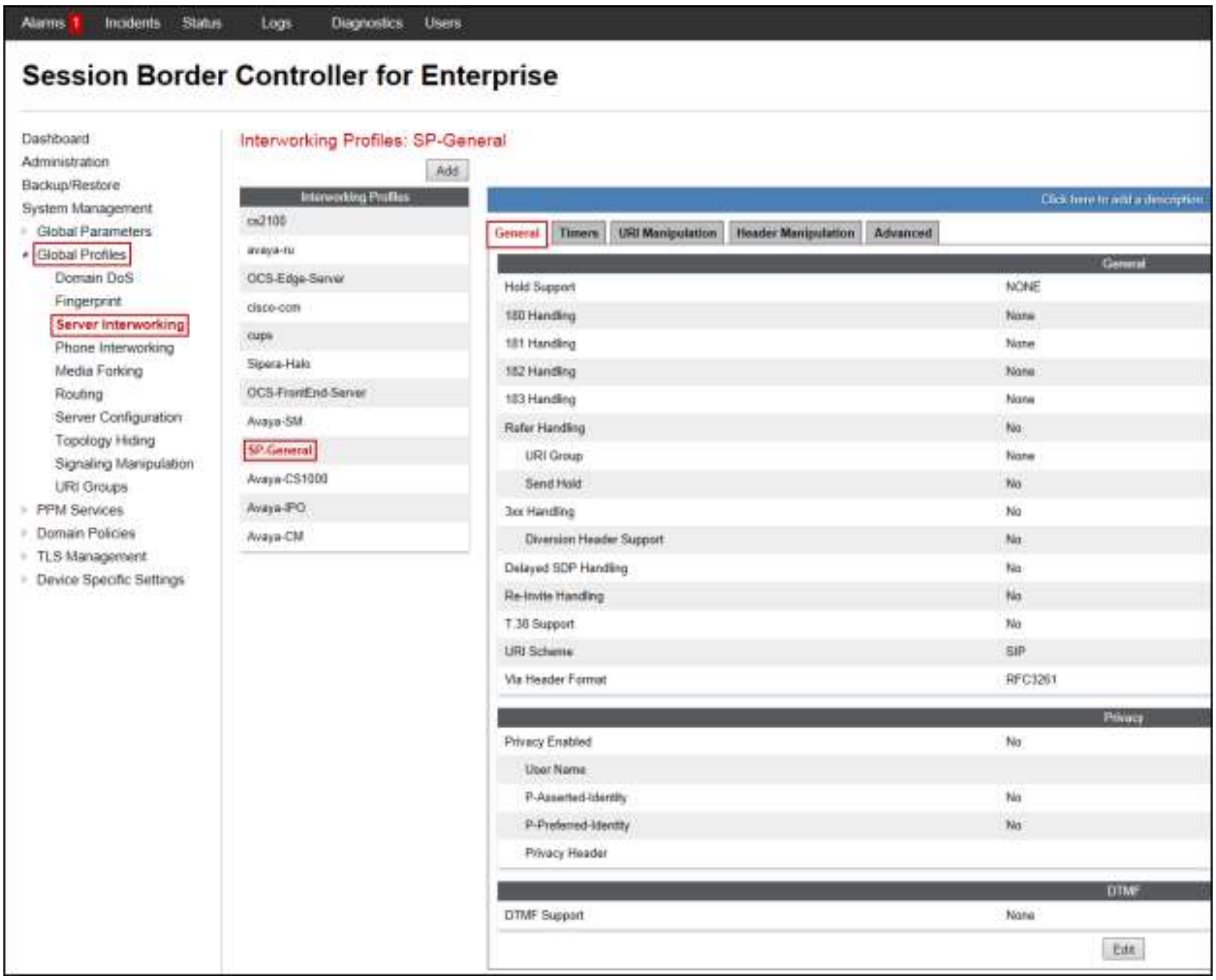
6.2.2 Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the Service Provider.

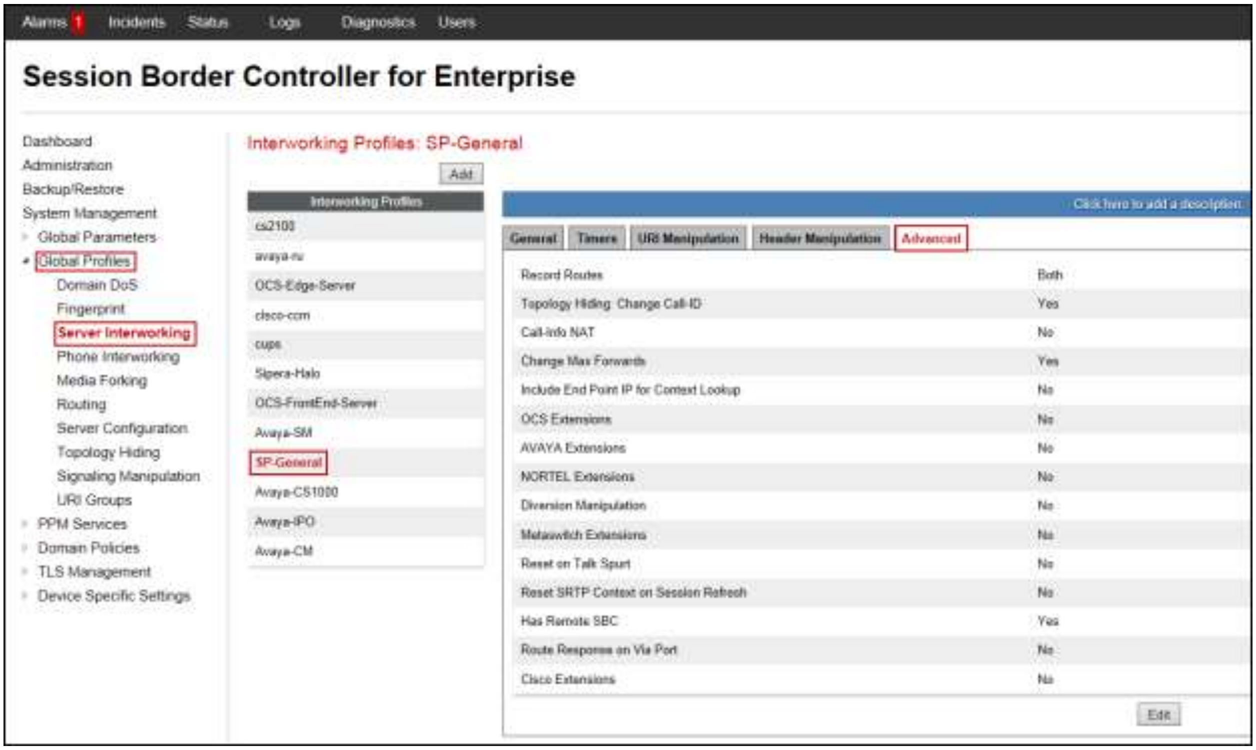
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add** (note that **Add** is being used to create the SP-General profile instead of cloning the avaya-ru profile).

Enter the new profile name, the name of ***SP-General*** was chosen in this example. Accept the default values for all fields by clicking **Next** and then click **Finish**.

The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.



The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.



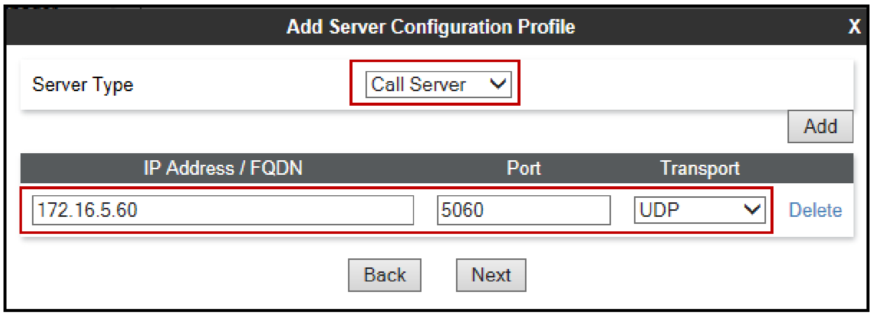
6.2.3 Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (IP Office) and the Trunk Server or SIP Proxy at the service provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add Profile** and enter the profile name: ***IP Office***.

On the **Add Server Configuration Profile - General** window:

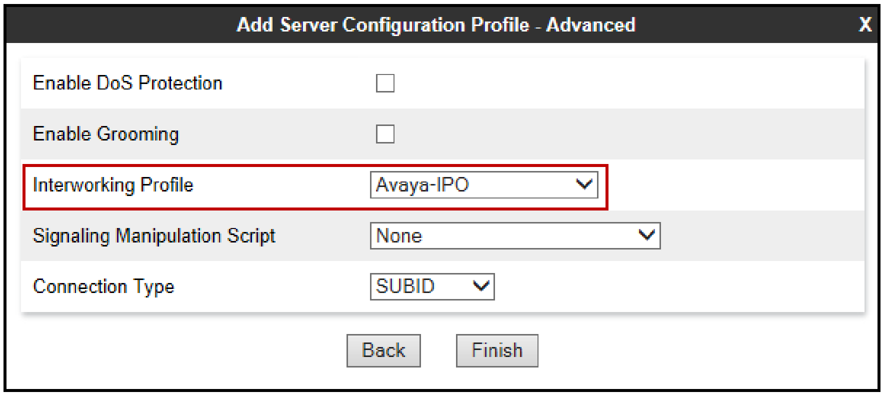
- **Server Type:** Select ***Call Server***.
- **IP Address / FQDN**: ***172.16.5.60*** (IP Address of IP Office).
- **Port:** ***5060*** (This port must match the port number defined in **Section 5.2.1**).
- **Transports**: Select ***UDP***.
- Click **Next**.



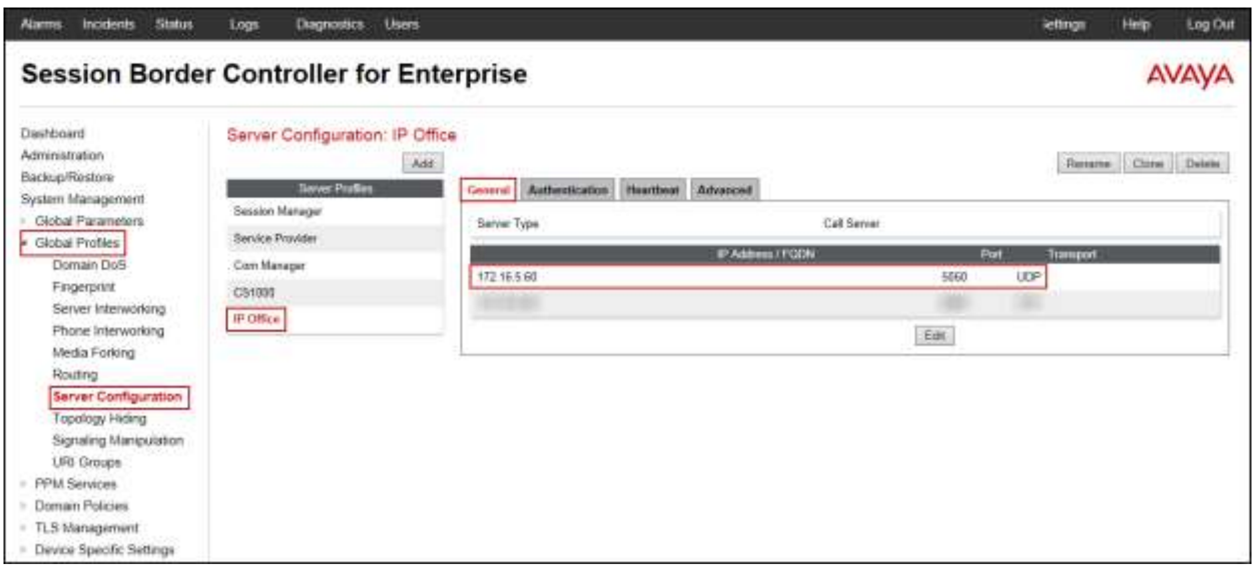
Note: UDP transport protocol was used on the connection between the Avaya SBCE and IP Office. However, TCP can be used instead if necessary.

- Click **Next** on the **Authentication** window.
- Click **Next** on the **Heartbeat** window.

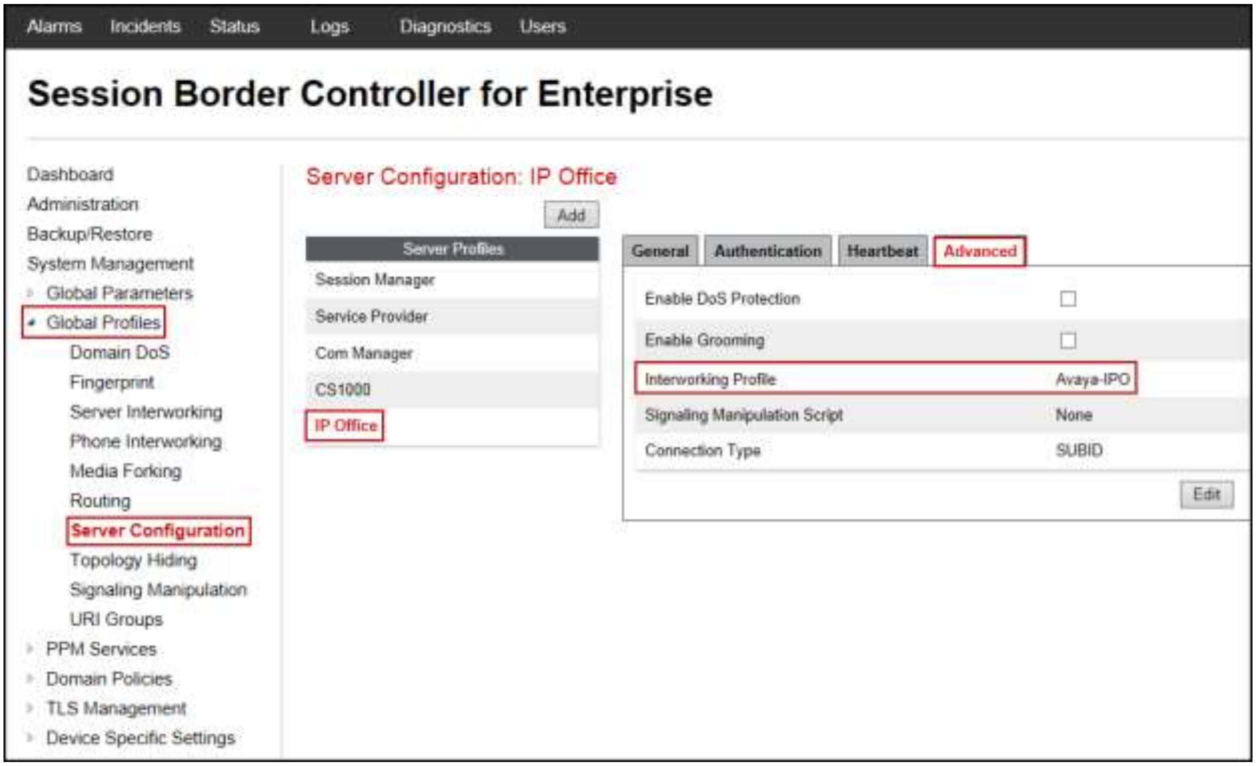
On the **Advanced** tab:
- Select ***Avaya-IPO*** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default ***None***.
- Click **Finish**.



The following screen capture shows the **General** tab of the newly created **IP Office** profile.



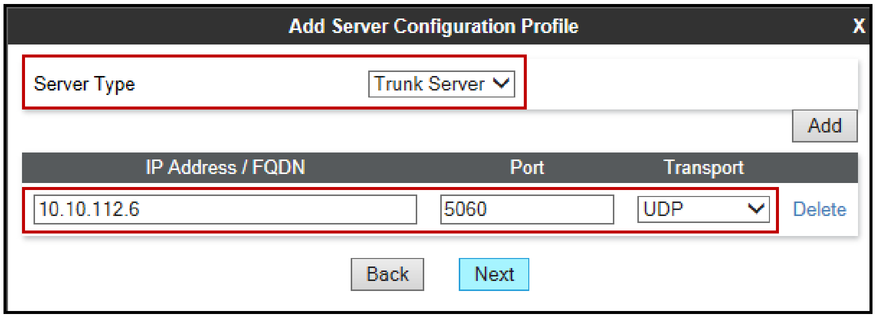
The following screen capture shows the **Advanced** tab of the newly created **IP Office** profile.



To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** section and enter the profile name: ***Service Provider***.

On the **Add Server Configuration Profile - General** window:

- **Server Type:** Select ***Trunk Server***.
- **IP Address / FQDN**: ***10.10.112.6*** (IP Address of the Service Provider SIP Proxy).
- **Port:** ***5060***.
- **Transports**: Select ***UDP***.
- Click **Next**.

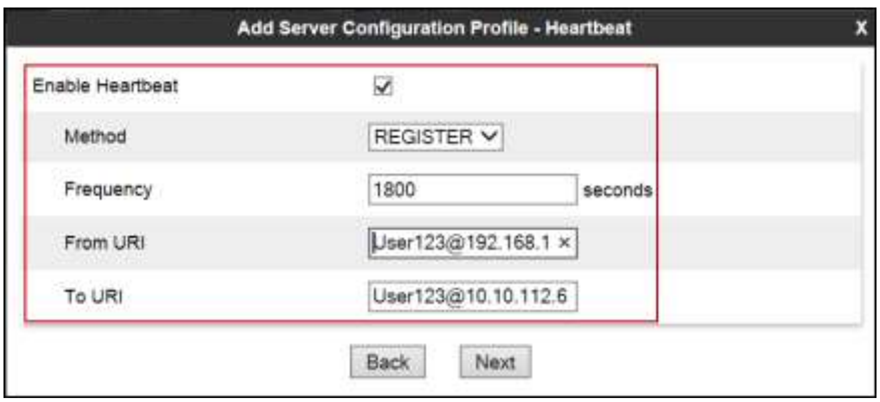


On the **Authentication** tab:

- Check the ***Enable Authentication*** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- **Realm**: ***10.10.112.6*** (IP Address of the Service Provider SIP Proxy).
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

On the **Heartbeat** tab:

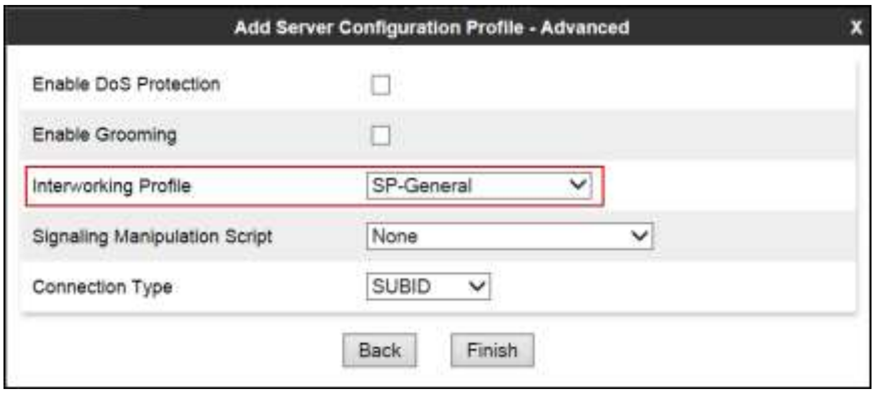
- Check the ***Enable Heartbeat*** box.
- Under **Method**, select ***REGISTER*** from the drop down menu.
- **Frequency:** Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider, ***1800*** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI**: Use the **User Name** entered under the **Authentication** screen (***User123***) and the Public IP address of the Avaya SBCE (***192.168.157.189***), as shown on the screen below.
  - **To URI**: Use the **User Name** entered under the **Authentication** screen (***User123***) and the Service Provider Proxy IP address (***10.10.112.6*****),** as shown on the screen below.
- Click **Next**.



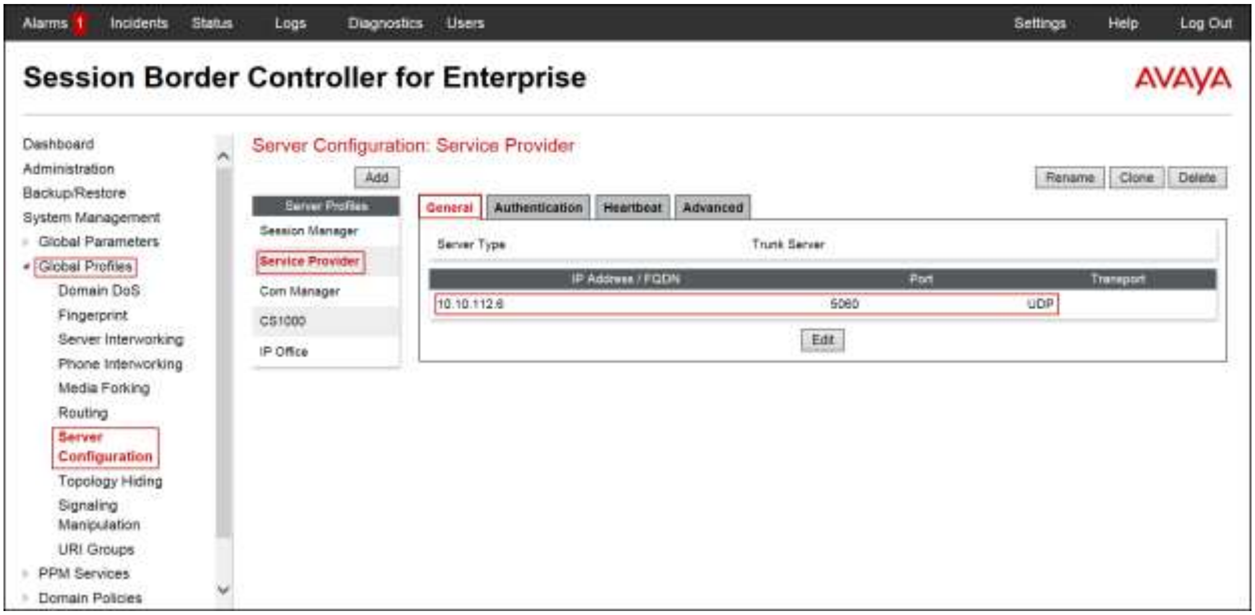
In the **Advanced** window:

- Select ***SP-General*** from the **Interworking Profile** drop down menu.
- Leave other fields with their default values for now, a **Signaling Manipulation** Script will be assigned later.
- Click **Finish**.

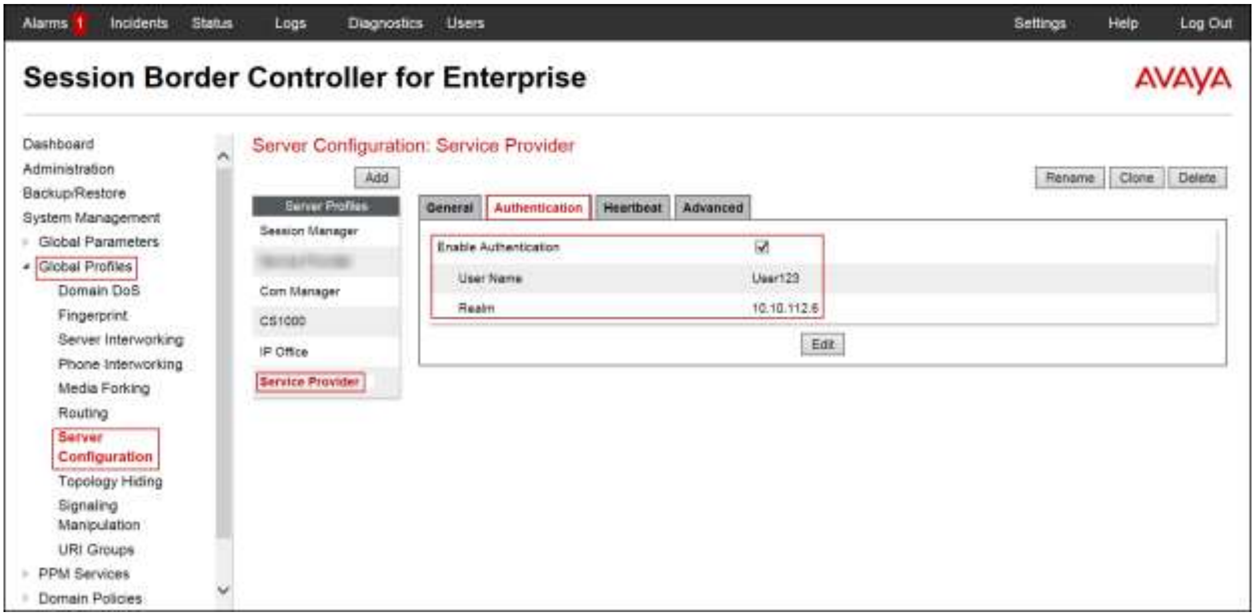
The following screen capture shows the **Advanced** tab of the **Service Provider** Server Configuration Profile.



The following screen capture shows the **General** tab of the newly created **Service Provider** Server Configuration Profile.

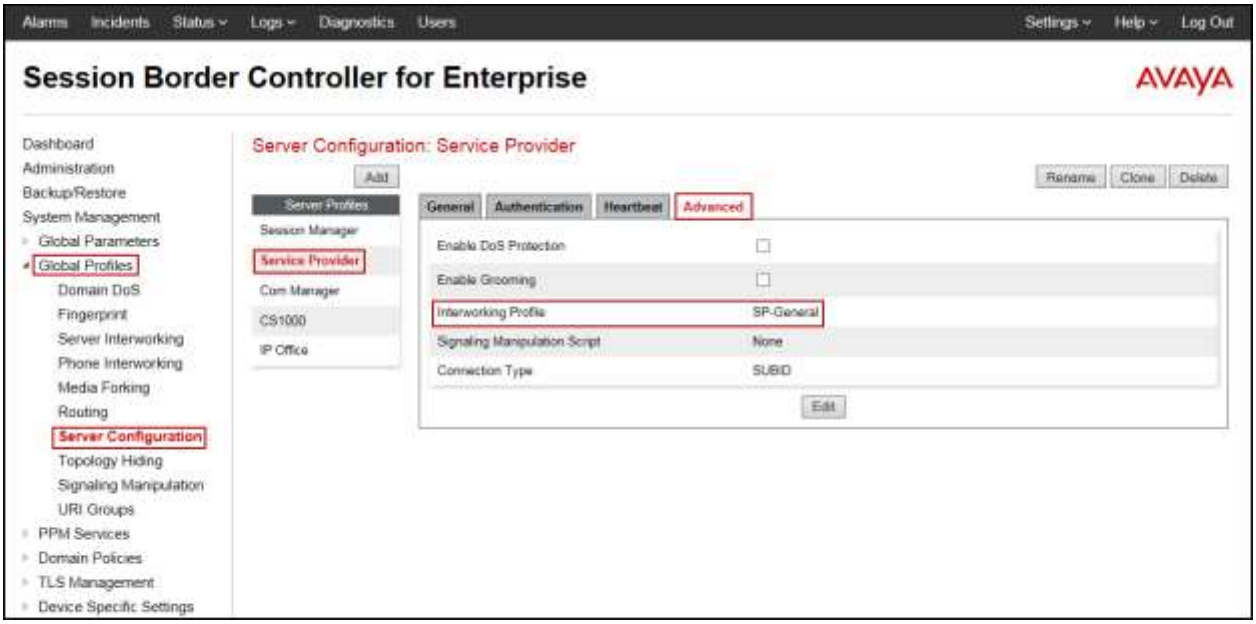


The following screen capture shows the **Authentication** tab of the newly created **Service Provider** Server Configuration Profile.



The following screen capture shows the **Heartbeat** tab of the newly created **Service Provider** Server Configuration Profile.

The following screen capture shows the **Advanced** tab of the newly created **Service Provider** Server Configuration Profile.



6.2.4 Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

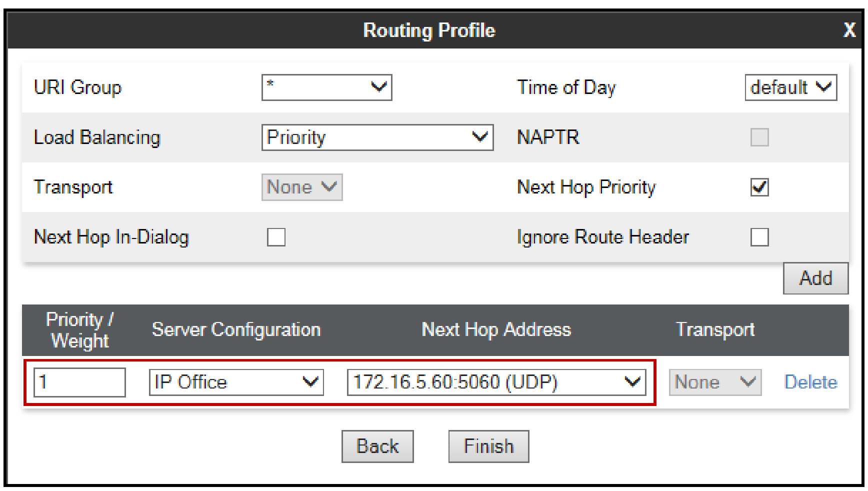
Two Routing profiles were created, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

To create the inbound route, from the **Global Profiles** menu on the left-hand side:

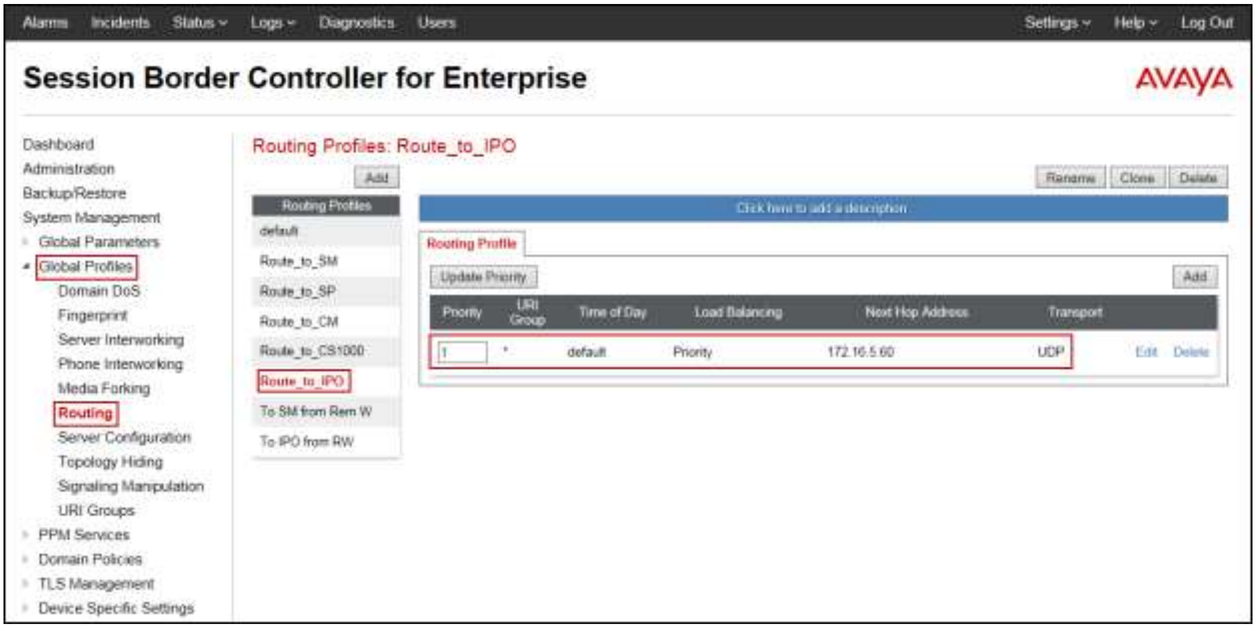
- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: ***Route_to_IPO***.
- Click **Next**.

On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: ***1***
- **Server Configuration**: Select ***IP Office***.
- **Next Hop Address**: Select ***172.16.5.60:5060 (UDP)*** (IP Office IP address, Port and Transport).
- Click **Finish**.



The following screen shows the newly created **Route_to_IPO** Profile.

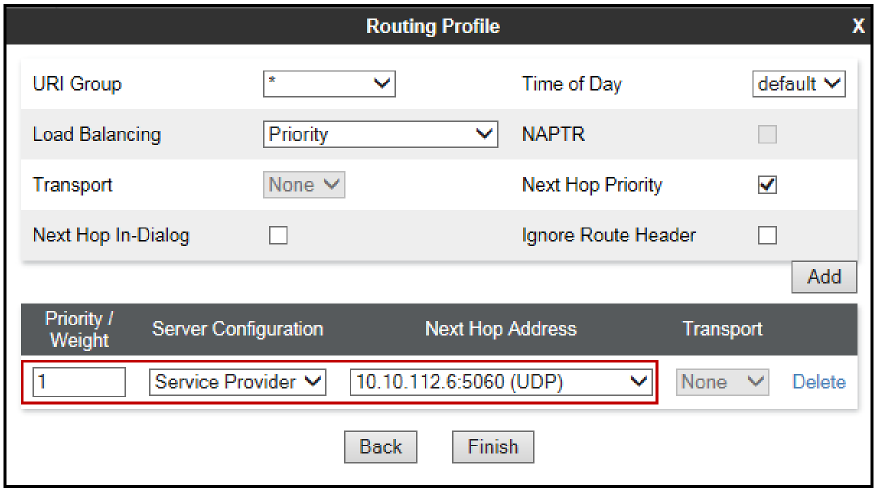


Similarly, for the outbound route:

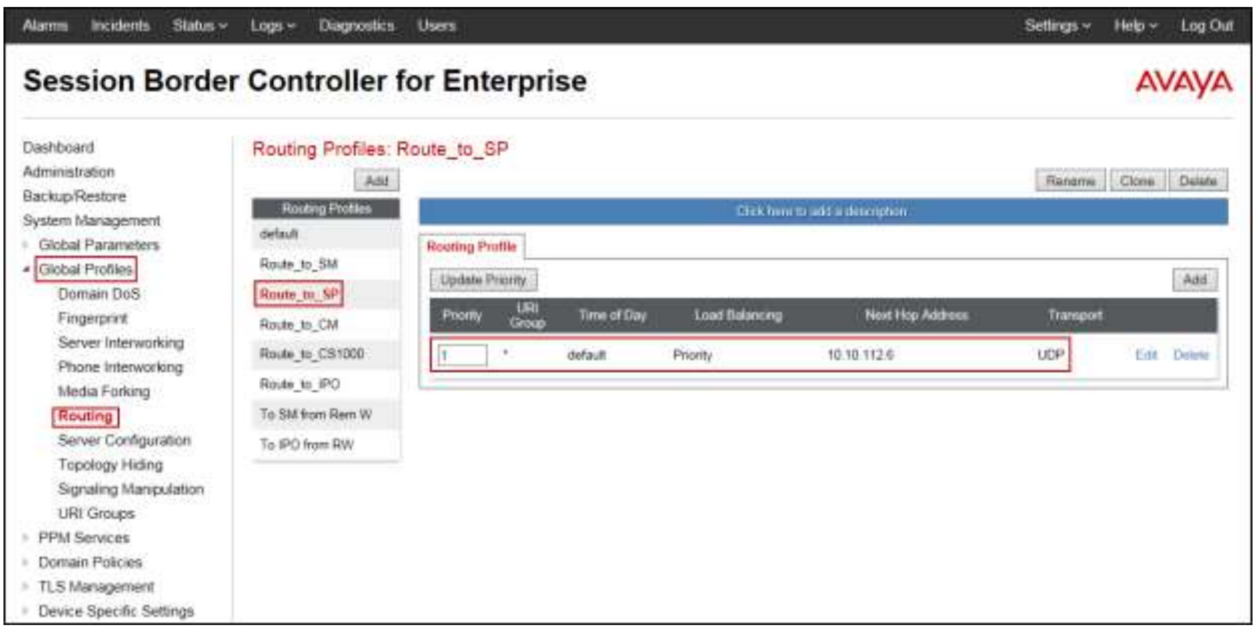
- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: ***Route_to_SP***.
- Click **Next**.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight**: ***1***
- **Server Configuration**: Select ***Service Provider***.
- **Next Hop Address**: Select ***10.10.112.6:5060 (UDP)*** (Service Provider SIP Proxy IP address, Port and Transport).
- Click **Finish**.



The following screen capture shows the newly created **Route_to_SP** Profile.



6.2.5 Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

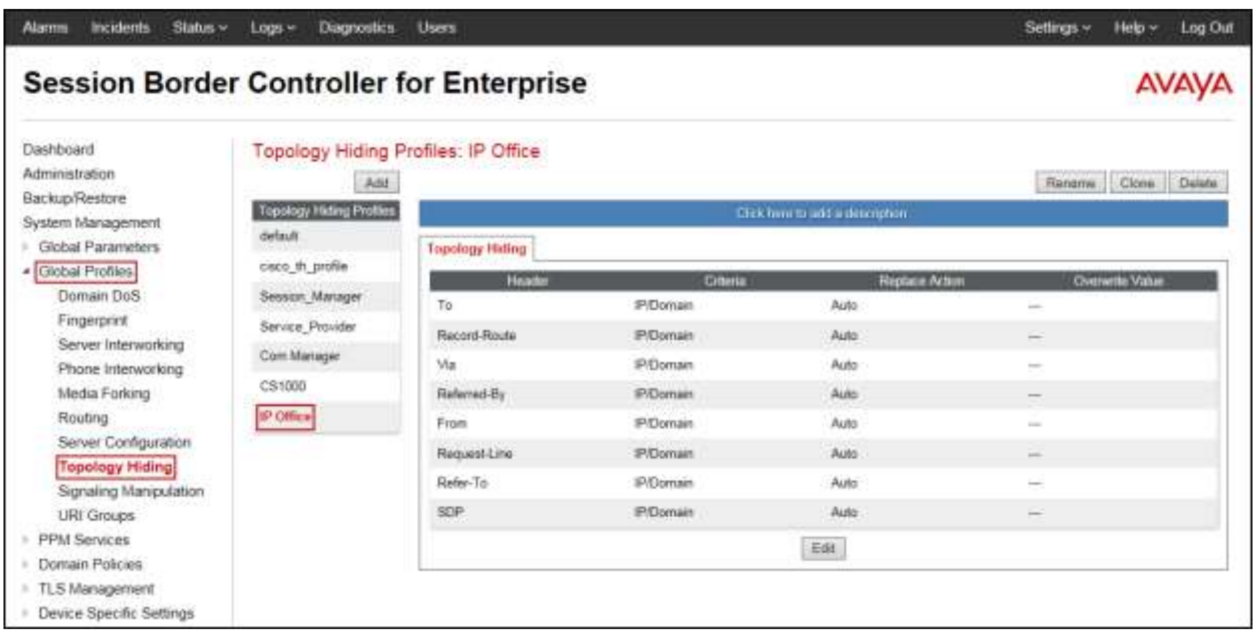
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by IP Office and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name**: ***IP Office***.
- Click **Finish**.

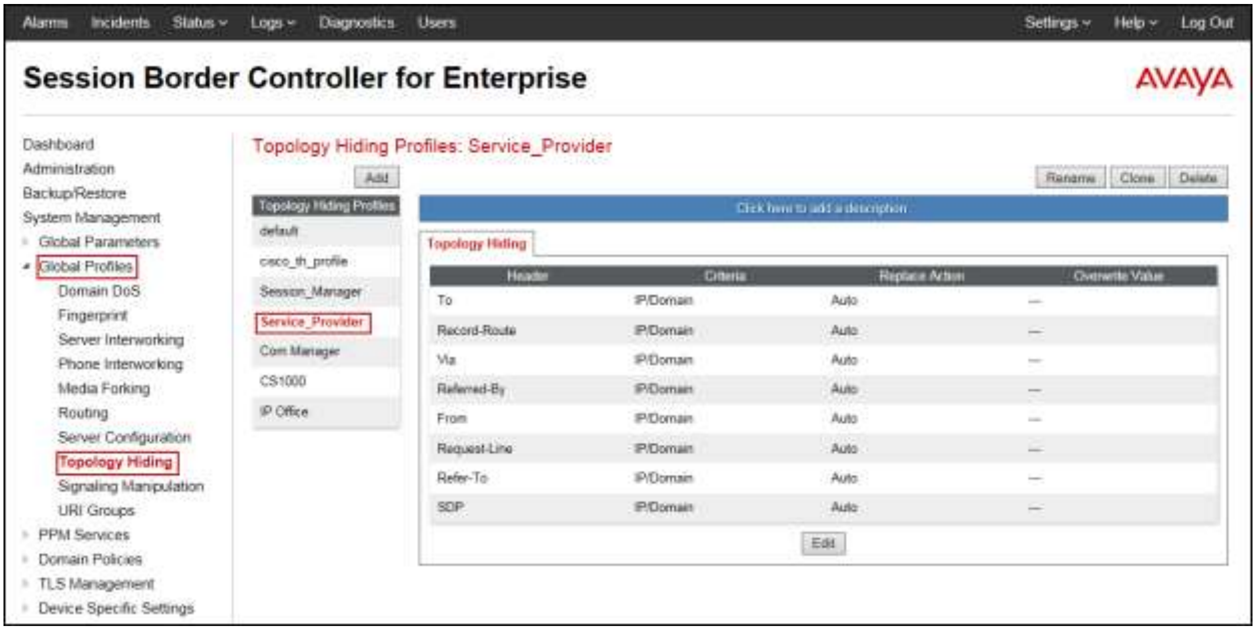
The following screen capture shows the newly added **IP Office** Profile. Note that for IP Office no values were overwritten (default).



To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name**: ***Service_Provider***.
- Click **Finish**.

The following screen capture shows the newly added **Service_Provider** Profile. Note that for the Service Provider no values were overwritten (default).



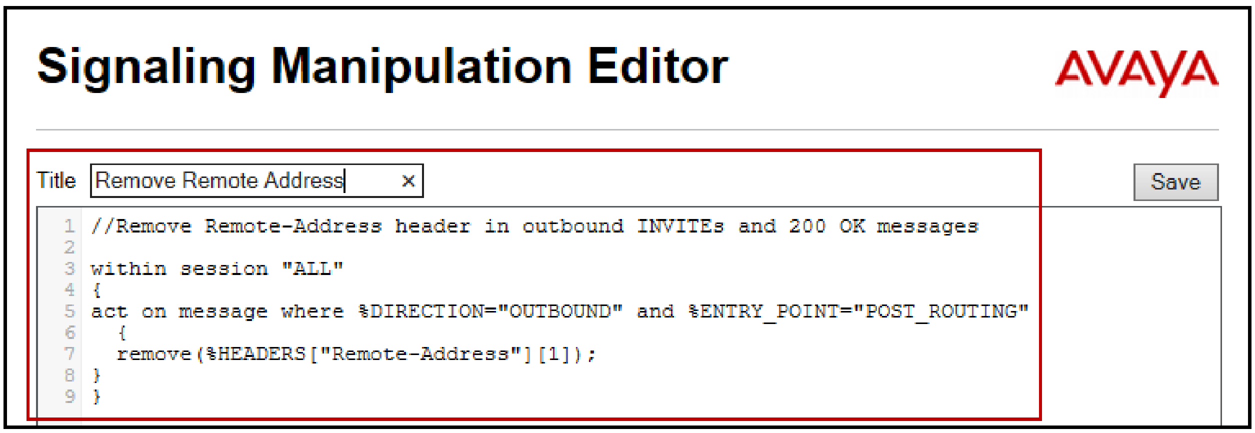
6.2.6 Signaling Manipulation

The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For the test configuration, the Editor was used to create the script needed to handle the header manipulation described below.

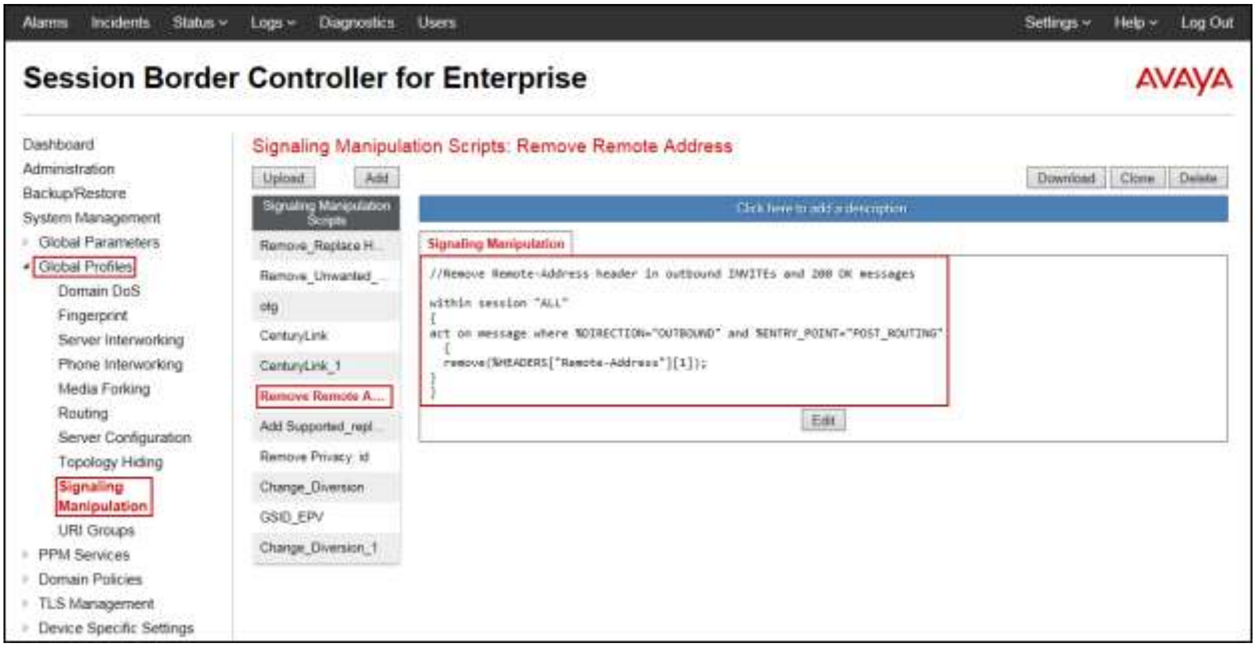
The Signaling Manipulation Script shown below is needed to remove unwanted headers to prevent them from being sent to the Service provider.

From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click on **Add Script** to open the SigMa Editor screen.

- For **Title** enter a name, the name of ***Remove Remote Address*** was chosen in this example.
- Enter the script as shown on the screen below (**Note**: The script can be copied from **Appendix A**).
- Click **Save**.

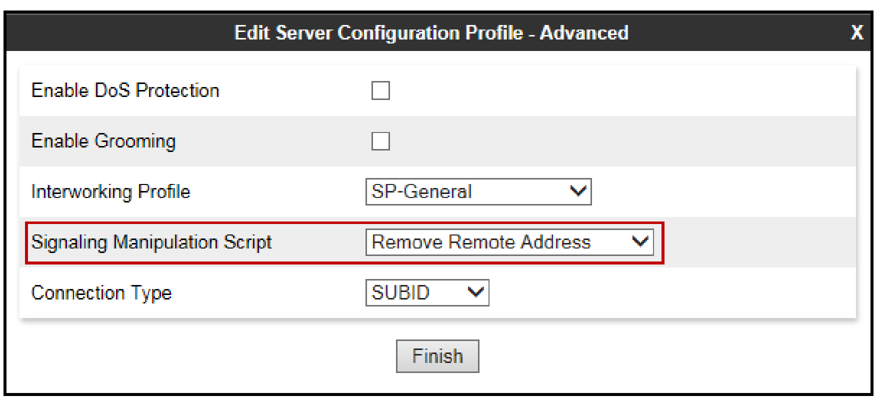


The following screen capture shows the newly added **Remove Remote Address** Signaling Manipulation Script.

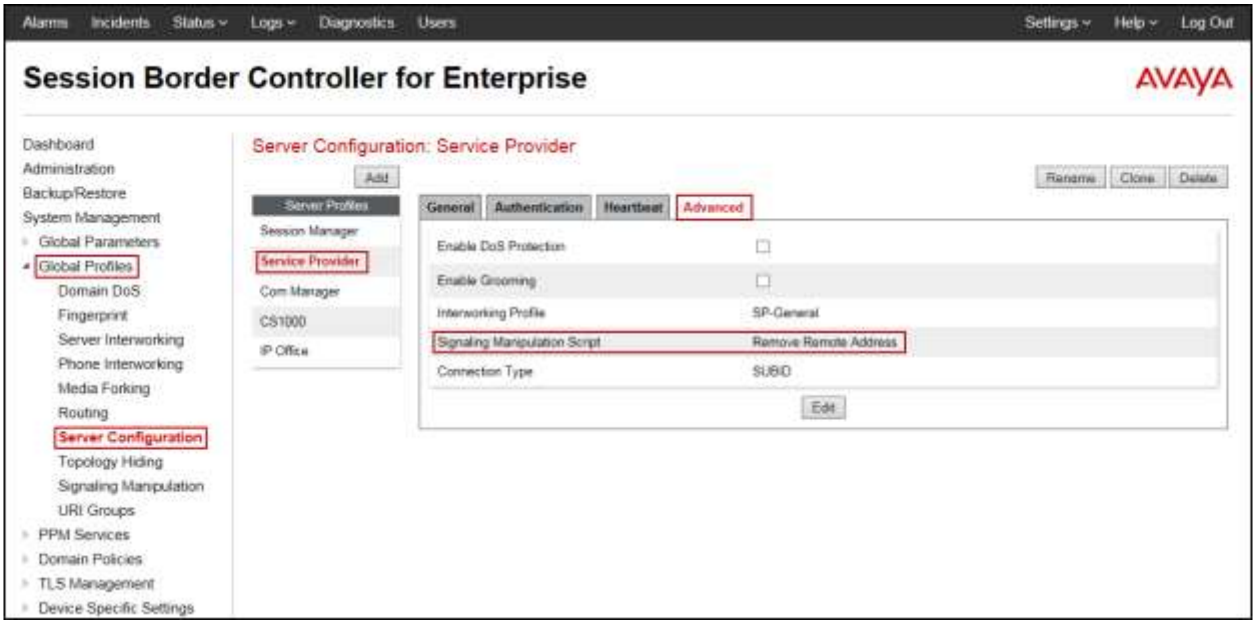


After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 6.2.3**.

Go to **Global Profiles → Server Configuration → Service Provider → Advanced** tab **→ Edit**. Select ***Remove Remote Address*** from the drop down menu on the **Signaling Manipulation Script** field. Click **Finish** to save and exit.



The following screen capture shows the **Advanced** tab of the previously added **Service Provider** Server Configuration Profile with the **Signaling Manipulation Script** assigned.



6.3 Domain Policies

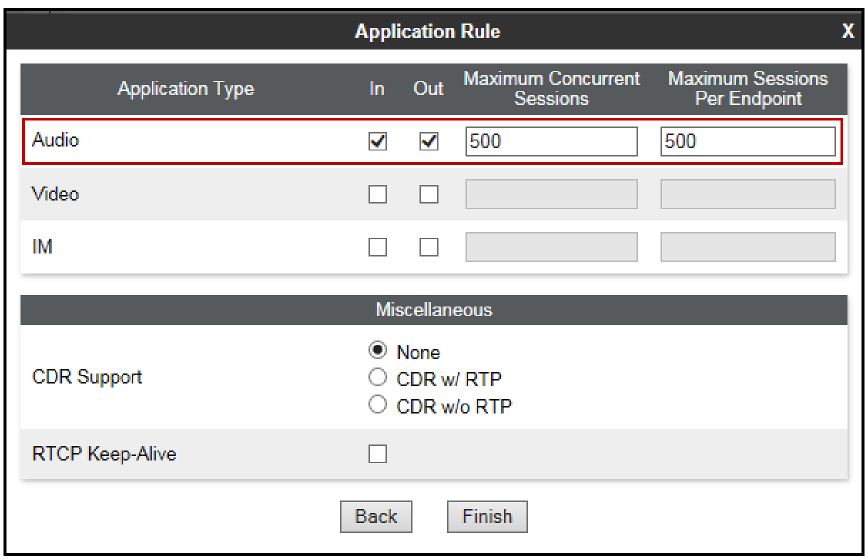
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.3.1 Application Rules

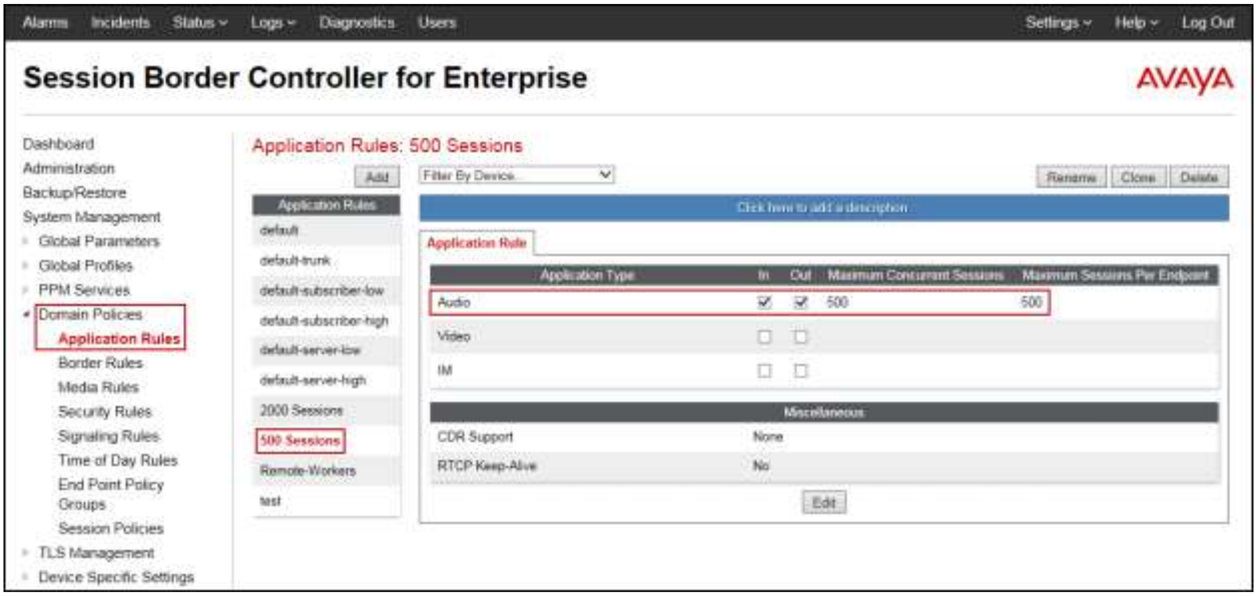
Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent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

From the menu on the left-hand side, select **Domain Policies → Application Rules**.

- Click on the **Add** button to add a new rule.
- **Rule Name:** enter the name of the profile, e.g., ***500 Sessions***.
- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of ***500*** was used in the sample configuration.
- Click **Finish**.



The following screen capture shows the newly created **500 Sessions** Application Rule.

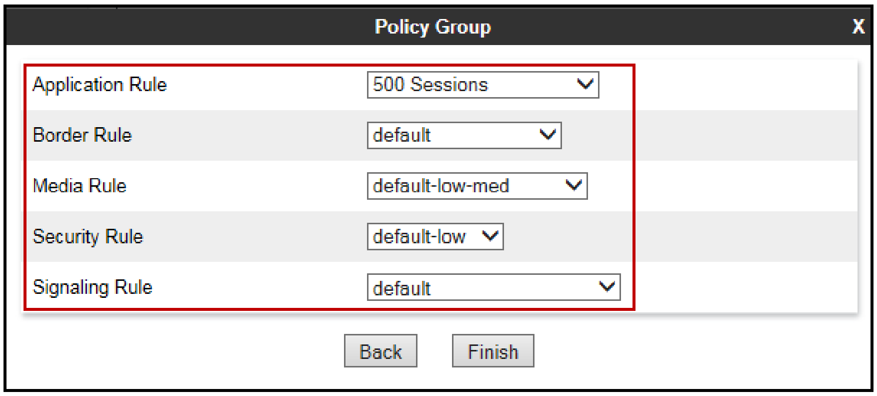


6.3.2 End Point Policy Groups

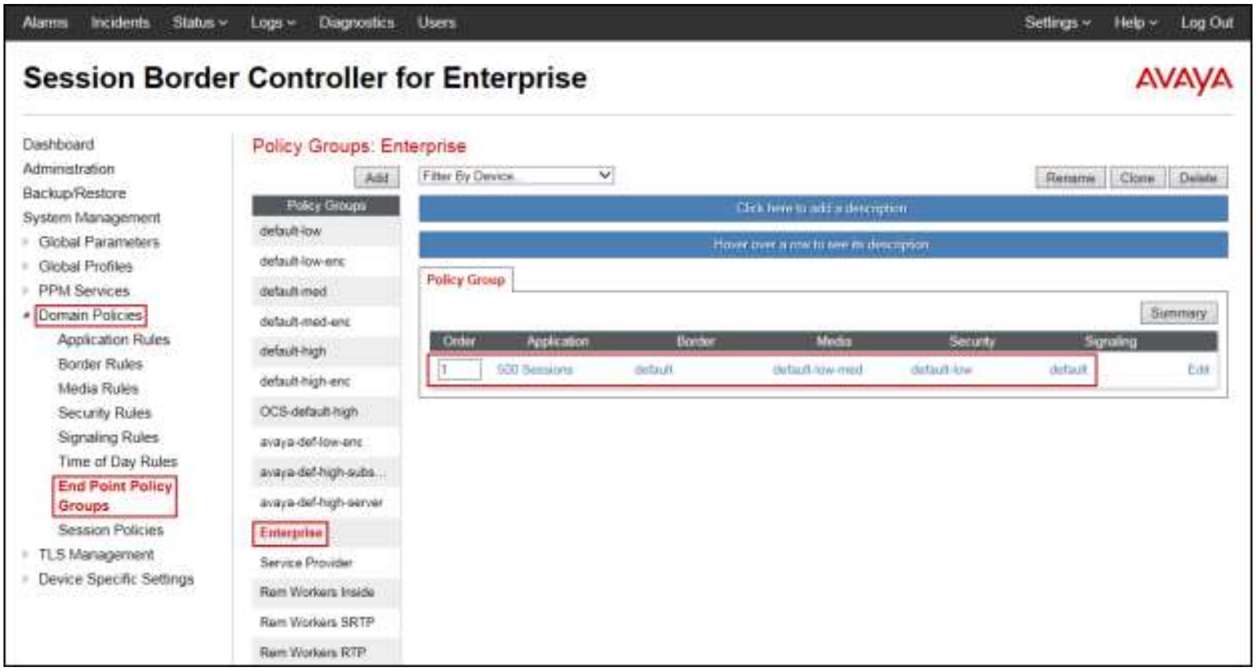
End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add** in the **Policy Groups** section.

- **Group Name:** ***Enterprise***.
- **Application Rule:** ***500 Sessions***.
- **Border Rule:** ***default***.
- **Media Rule:** ***default-low-med***.
- **Security Rule:** ***default-low***.
- **Signaling Rule:** ***default***.
- Click **Finish**.

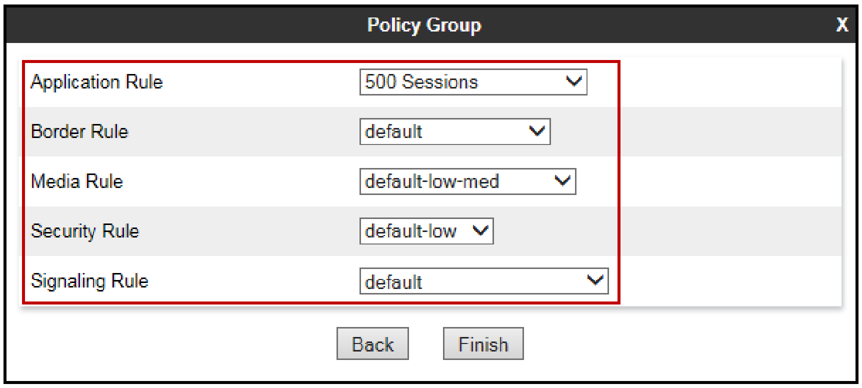


The following screen capture shows the newly created **Enterprise** End Point Policy Group.

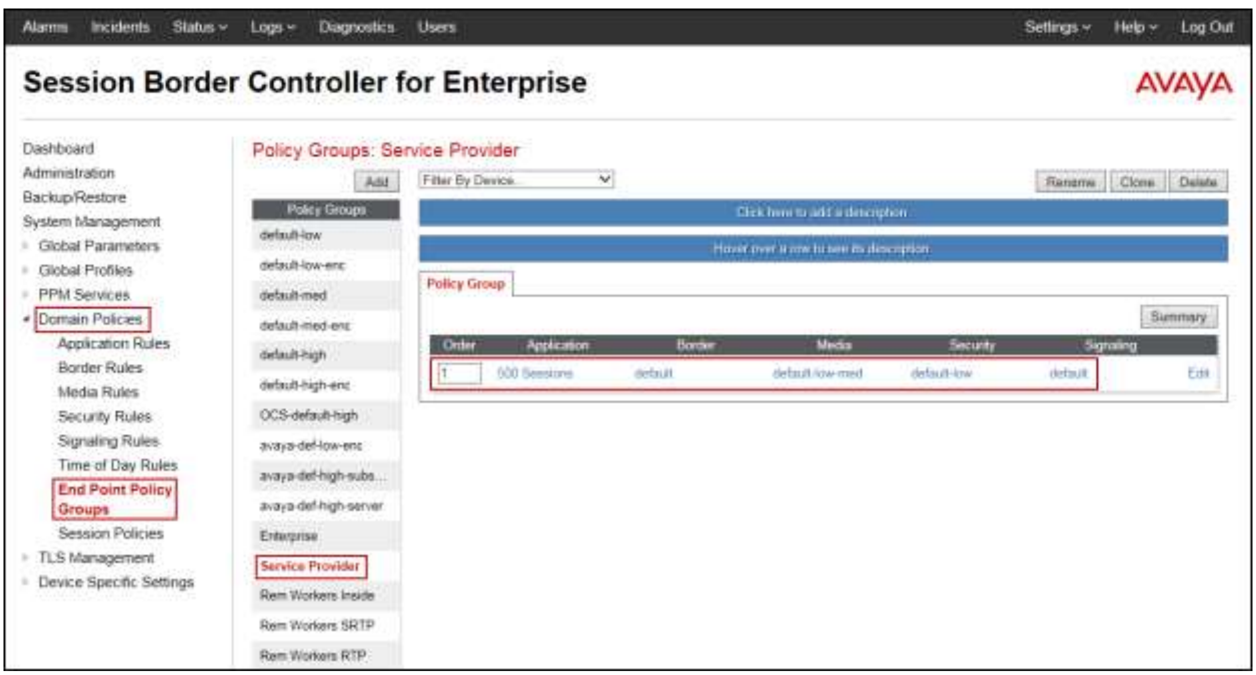


Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add** in the **Policy Groups** section.

- **Group Name:** ***Service Provider***.
- **Application Rule:** ***500 Sessions***.
- **Border Rule:** ***default.***
- **Media Rule:** ***default-low-med***.
- **Security Rule:** ***default-low***.
- **Signaling Rule:** ***default***.
- Click **Finish**.



The following screen capture shows the newly created **Service Provider** End Point Policy Group.



6.4 Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

6.4.1 Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

In the event that changes need to be made to the network configuration information, they can be entered here.

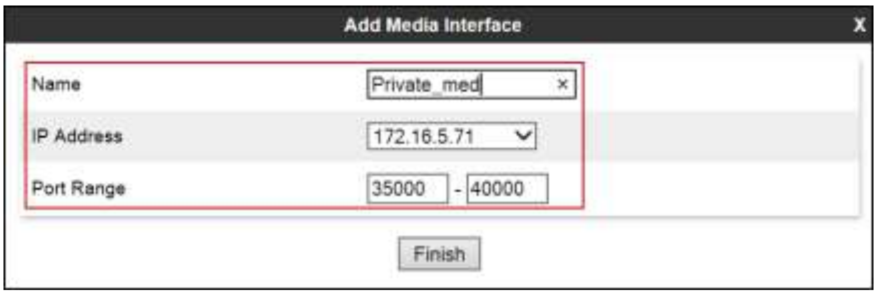
On the Interface Configuration tab, click the **Toggle** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **disabled**, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

6.4.2 Media Interface

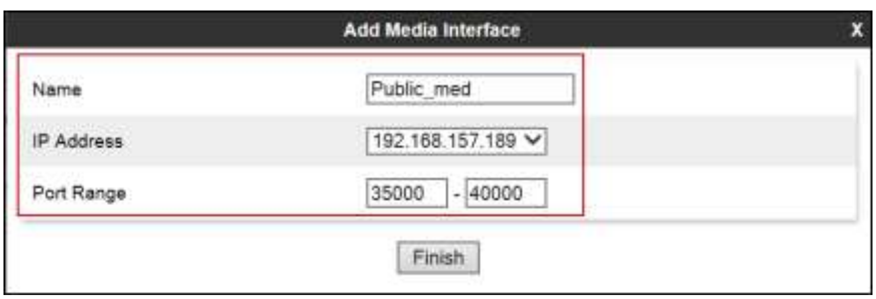
Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**.

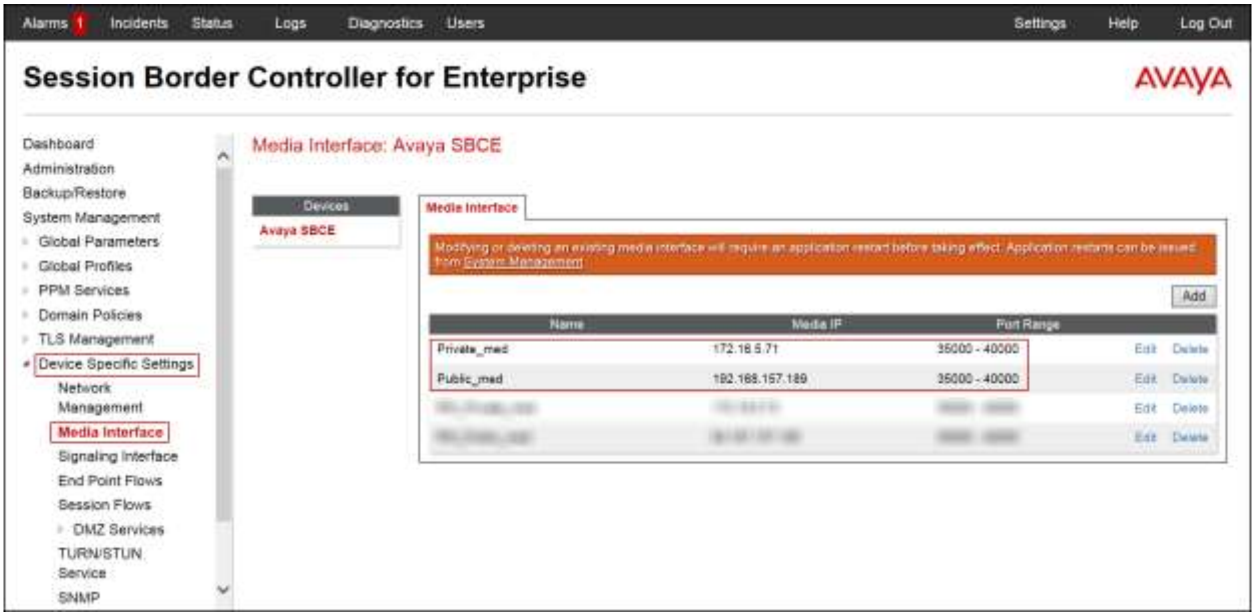
- Select **Add** in the **Media Interface** area.
- **Name:** ***Private_med***.
- Select **IP Address:** ***172.16.5.71*** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **Port Range:** ***35000-40000***.
- Click **Finish**.



- Select **Add** in the **Media Interface** area**.**
- **Name:** ***Public_med***.
- Select **IP Address:** ***192.168.157.189*** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range:** ***35000-40000***.
- Click **Finish**.



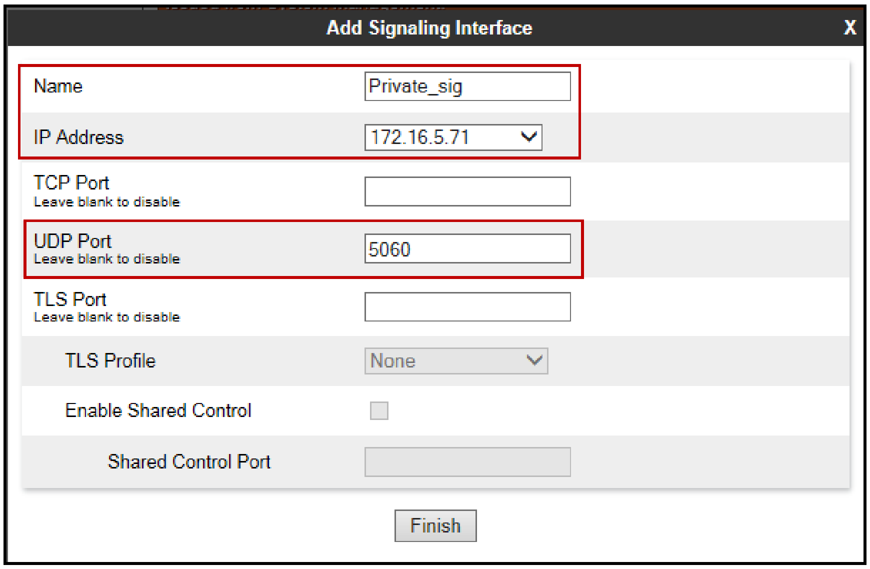
The following screen capture shows the newly created Media Interfaces.



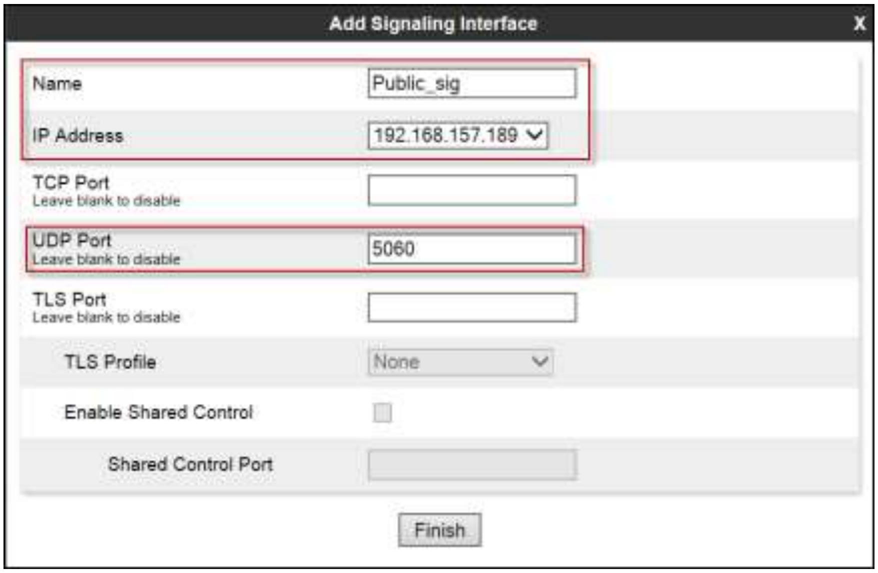
6.4.3 Signaling Interface

To create the Signaling Interface toward IP Office, from the **Device Specific** menu on the left hand side, select **Signaling Interface**.

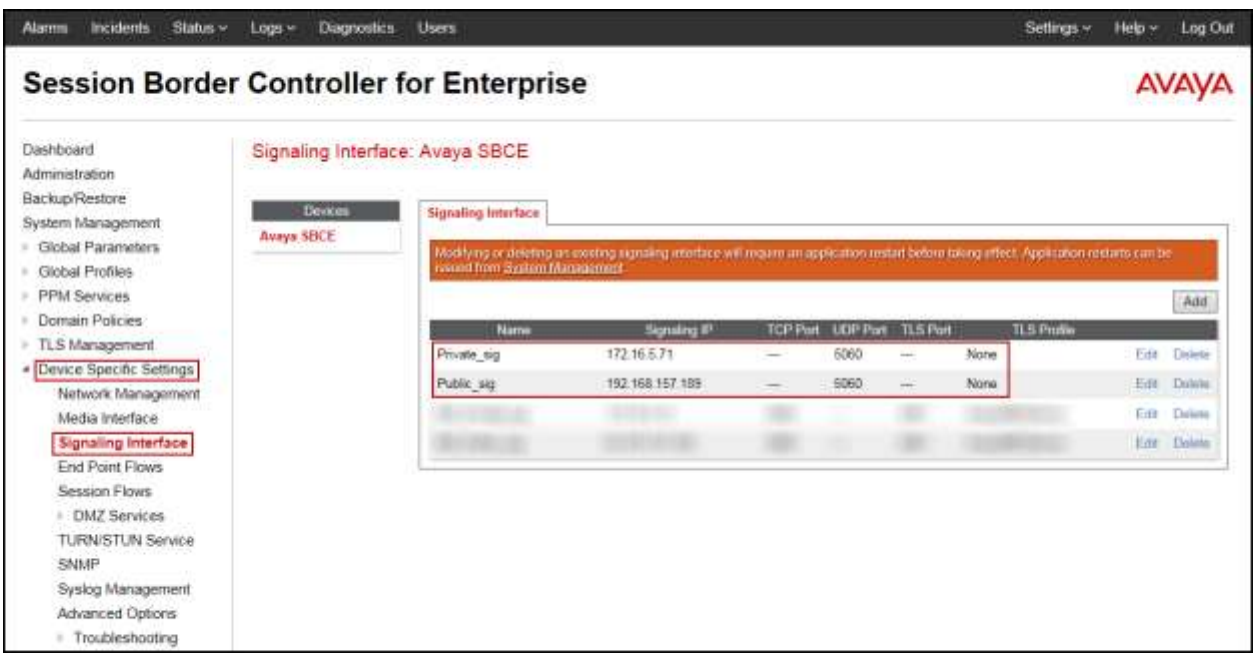
- Select **Add** in the **Signaling Interface** area.
- **Name:** ***Private_sig***.
- Select **IP Address:** ***172.16.5.71*** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port:** ***5060***.
- Click **Finish**.



- Select **Add** in the **Signaling Interface** area.
- **Name:** ***Public_sig***.
- Select **IP Address:** ***192.168.157.189*** (outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port:** ***5060***.
- Click **Finish**.

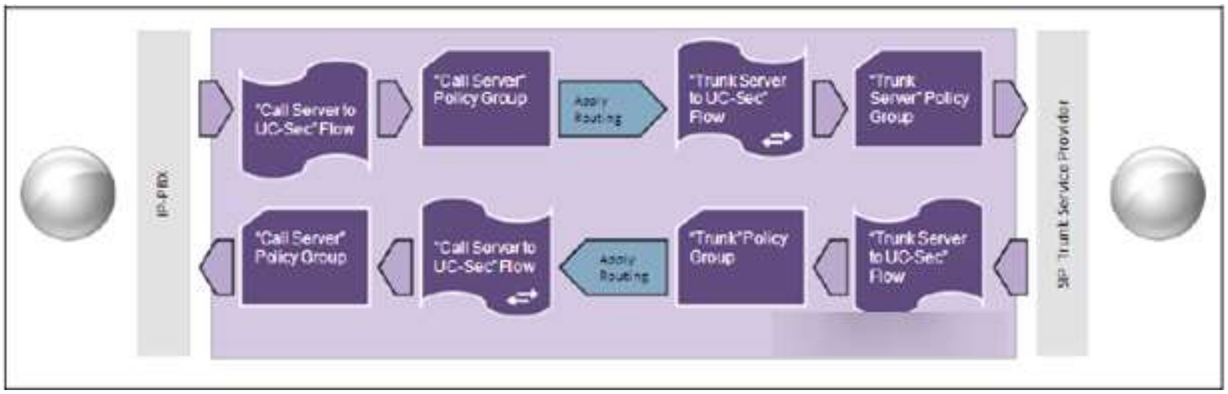


The following screen capture shows the newly created Signaling Interfaces.



6.4.4 End Point Flows

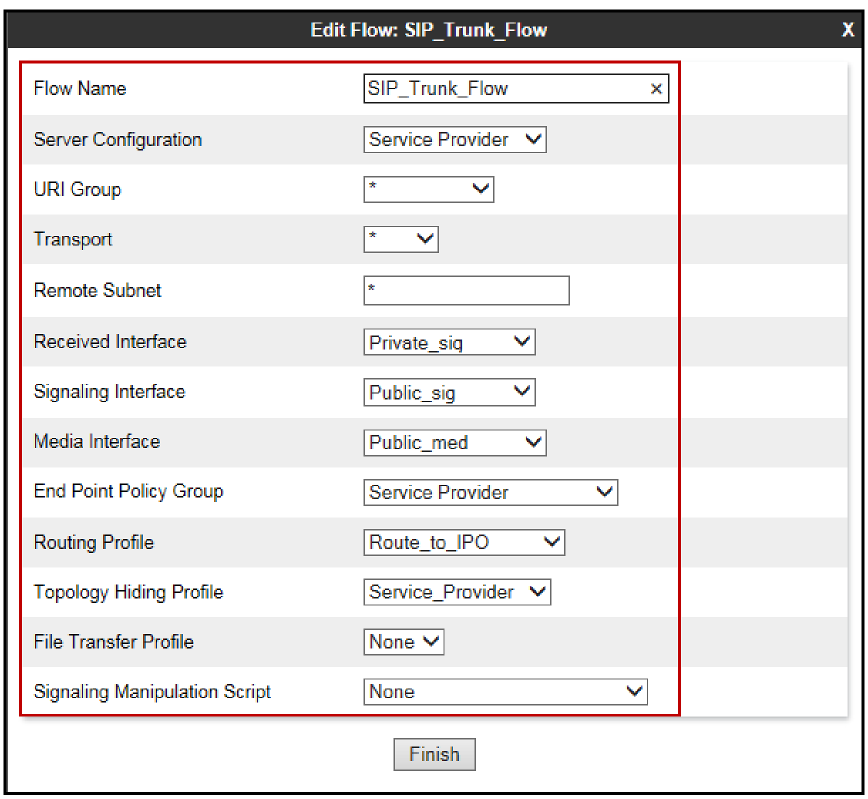
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing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



The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

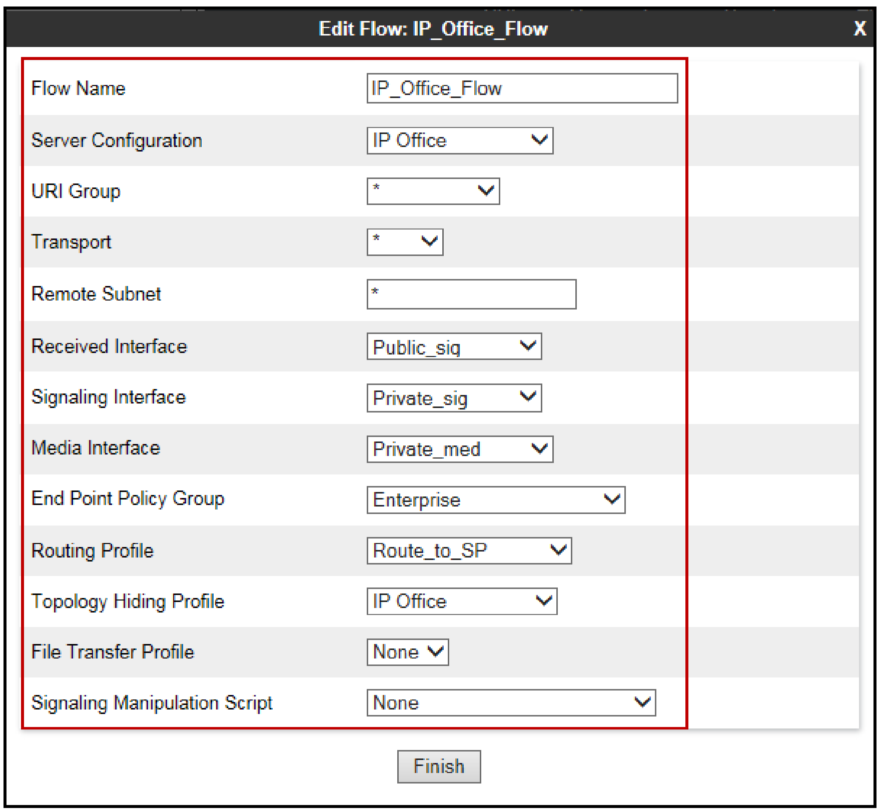
To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, then the **Server Flows** tab. Click **Add**.

- **Name:** ***SIP_Trunk_Flow***.
- **Server Configuration**: ***Service Provider***.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: ***Private_sig***.
- **Signaling Interface: *Public_sig***.
- **Media Interface**: ***Public_med***.
- **End Point Policy Group: *Service Provider***.
- **Routing Profile: *Route_to_IPO*** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: *Service_Provider***.
- **File Transfer Profile: *None***.
- **Signaling Manipulation Script: *None***.
- Click **Finish**.

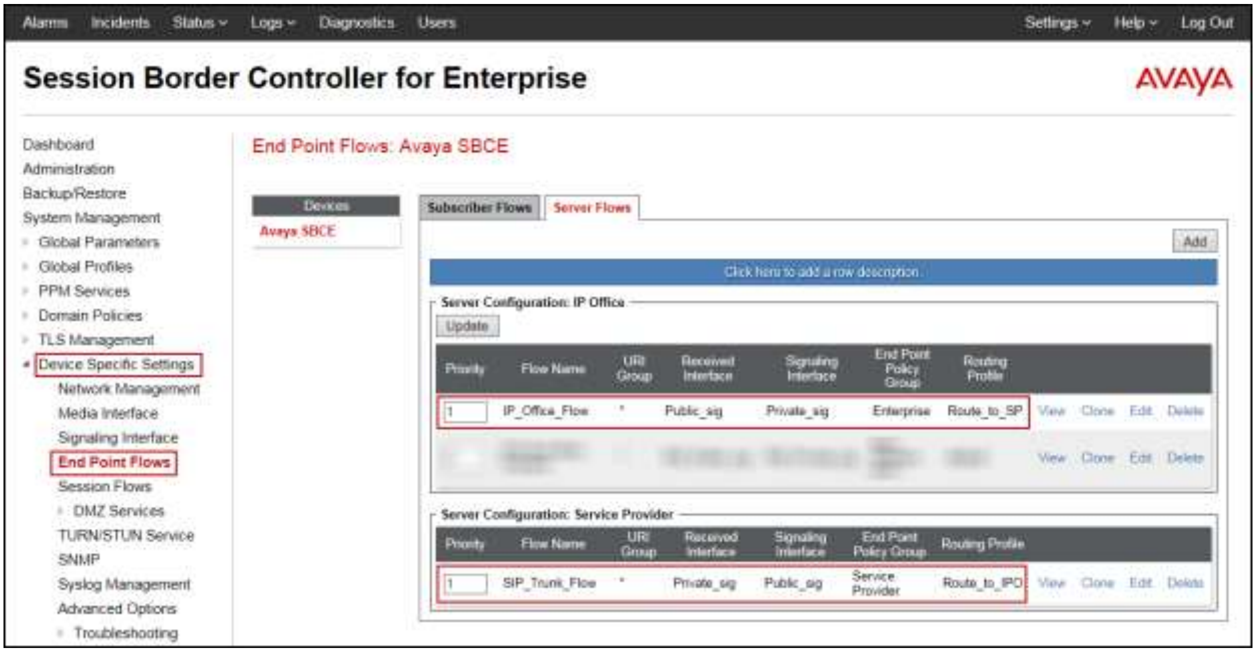


To create the call flow toward IP Office, click **Add**.

- **Name:** ***IP_Office_Flow***.
- **Server Configuration**: ***IP Office***.
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: ***Public_sig***.
- **Signaling Interface: Private_sig**.
- **Media Interface**: ***Private_med***.
- **End Point Policy Group:** ***Enterprise***.
- **Routing Profile:** ***Route_to_SP*** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** ***IP Office***.
- **File Transfer Profile:** ***None***.
- **Signaling Manipulation Script:** ***None***.
- Click **Finish**.



The following screen capture shows the newly created **End Point Flows**.



7. Time Warner Cable SIP Trunking Configuration

To use Time Warner Cable Business Class SIP Trunking Service offering, a customer must request the service from Time Warner Cable using the established sales processes. The process can be started by contacting Time Warner Cable via the corporate web site at: http://business.timewarnercable.com/support/overview.html or call 866-892-4249 and requesting information.

Time Warner Cable is responsible for the configuration of the SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya Session Border Controller for Enterprise at the customer's enterprise site.

Time Warner Cable will provide the customer the necessary information to configure the SIP trunk connection, including:

- IP address of Time Warner Cable's SIP Proxy server.
- SIP Trunk registration credentials.
- Supported codec's and order of preference.
- DID numbers.

8. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting tips that can be used to troubleshoot the solution.

8.1 Verification Steps

The following steps may be used to verify the configuration:

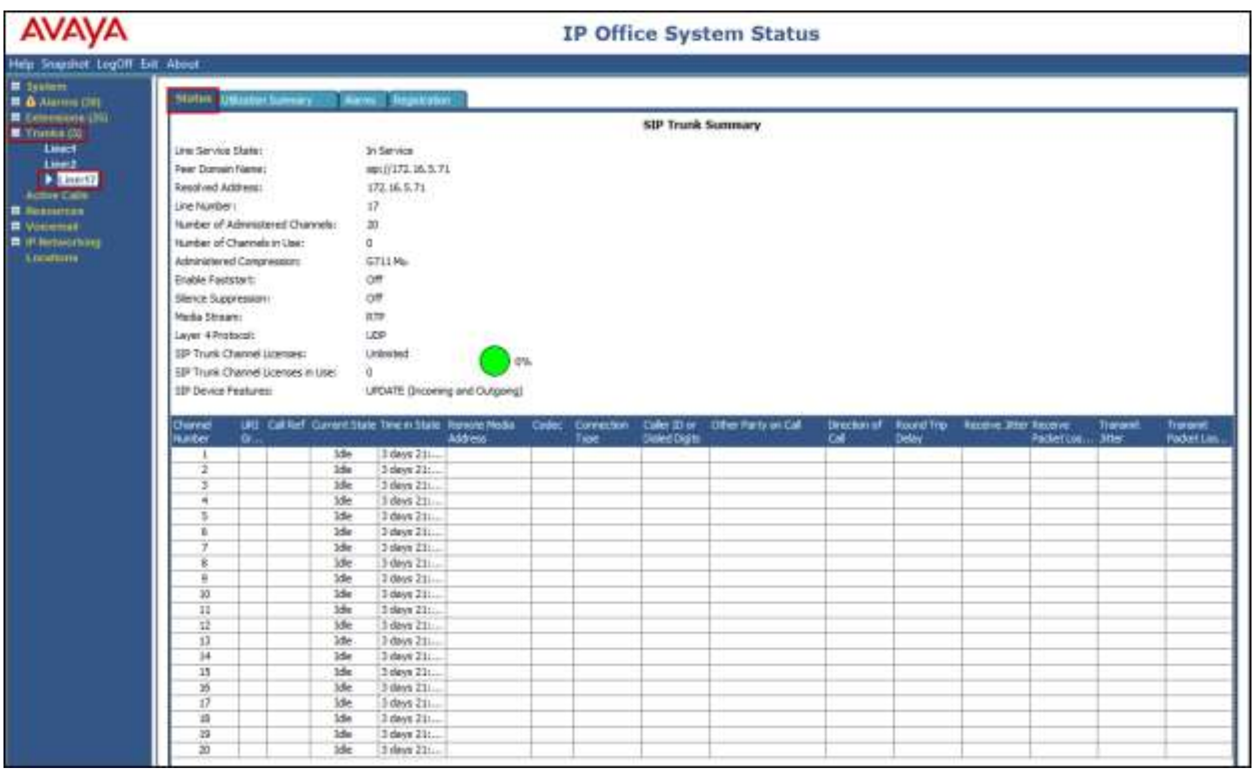
- Verify that endpoints at the enterprise site can place calls to the PSTN.
- Verify that endpoints at the enterprise site can receive calls from the PSTN.
- Verify that users at the PSTN can end active calls to endpoints at the enterprise by hanging up.
- Verify that endpoints at the enterprise can end active calls to PSTN users by hanging up.

8.2 IP Office System Status

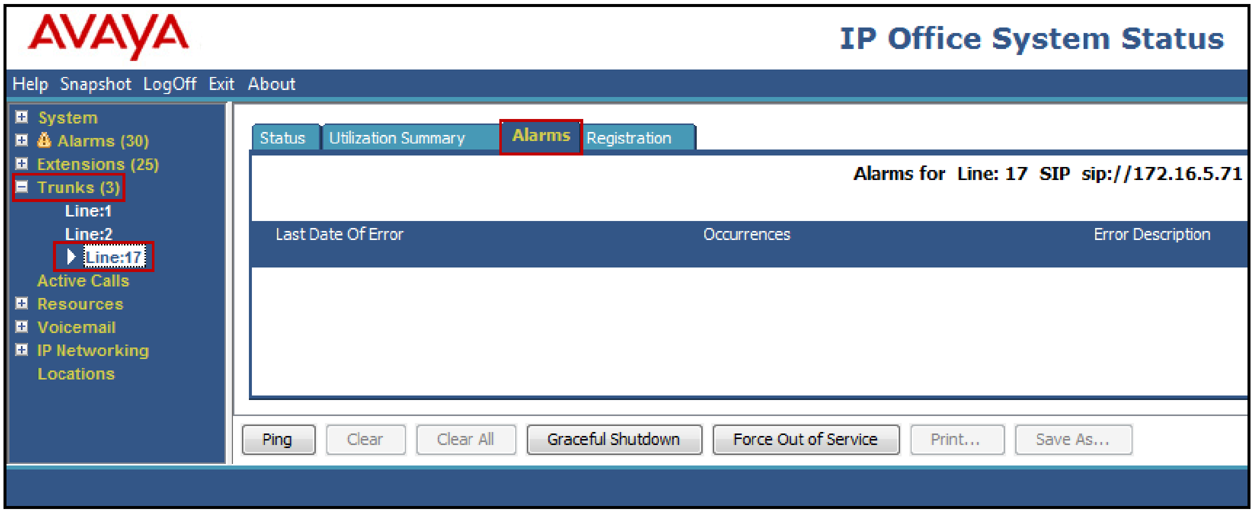
The following steps can also be used to verify the configuration.

Use the Avaya IP Office System Status application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office System Status is installed, log in with the proper credentials.

Select the SIP Line of interest from the left pane. 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).

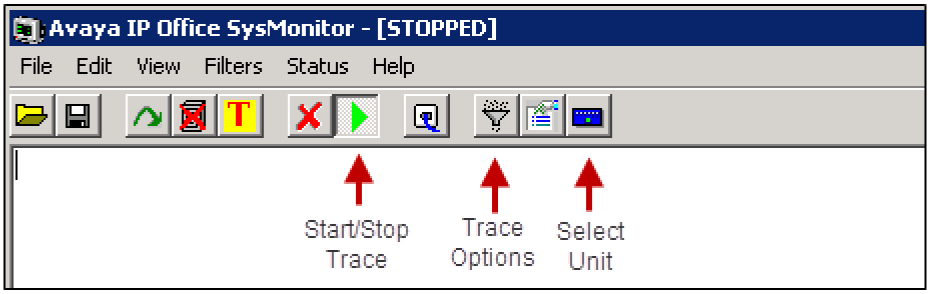


- Select the **Alarms** tab and verify that no alarms are active on the SIP Line.

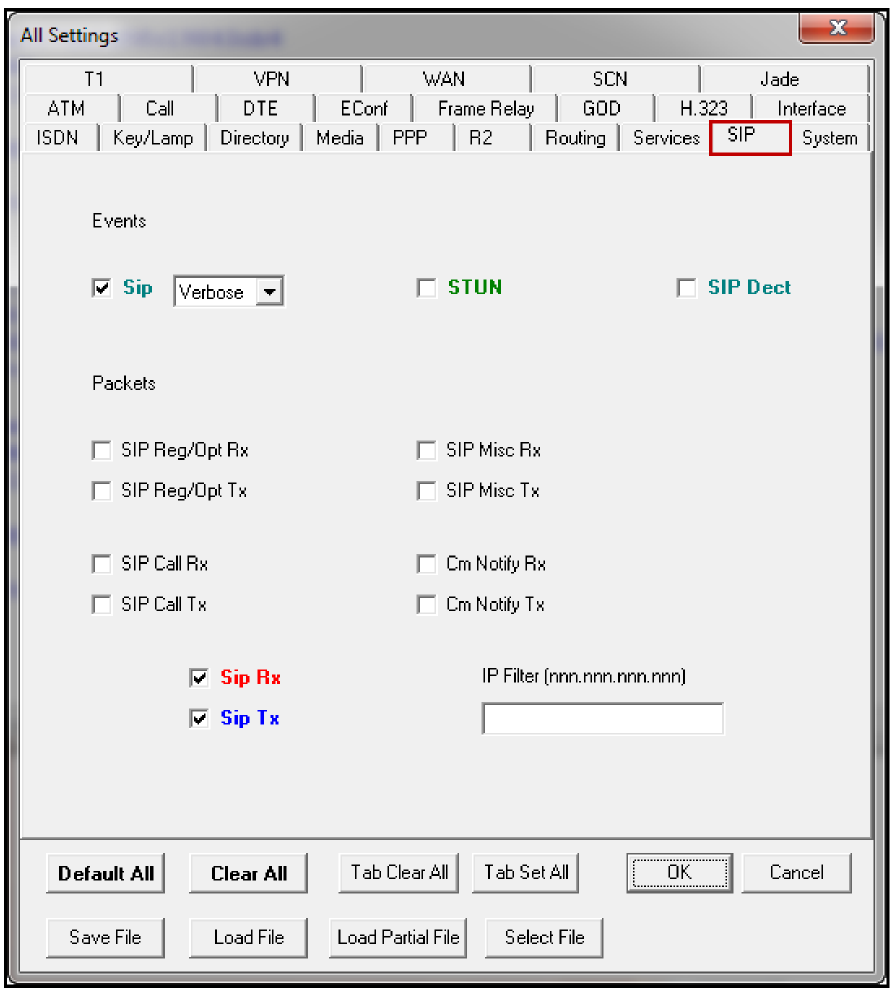


8.3 IP Office Monitor

The 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.



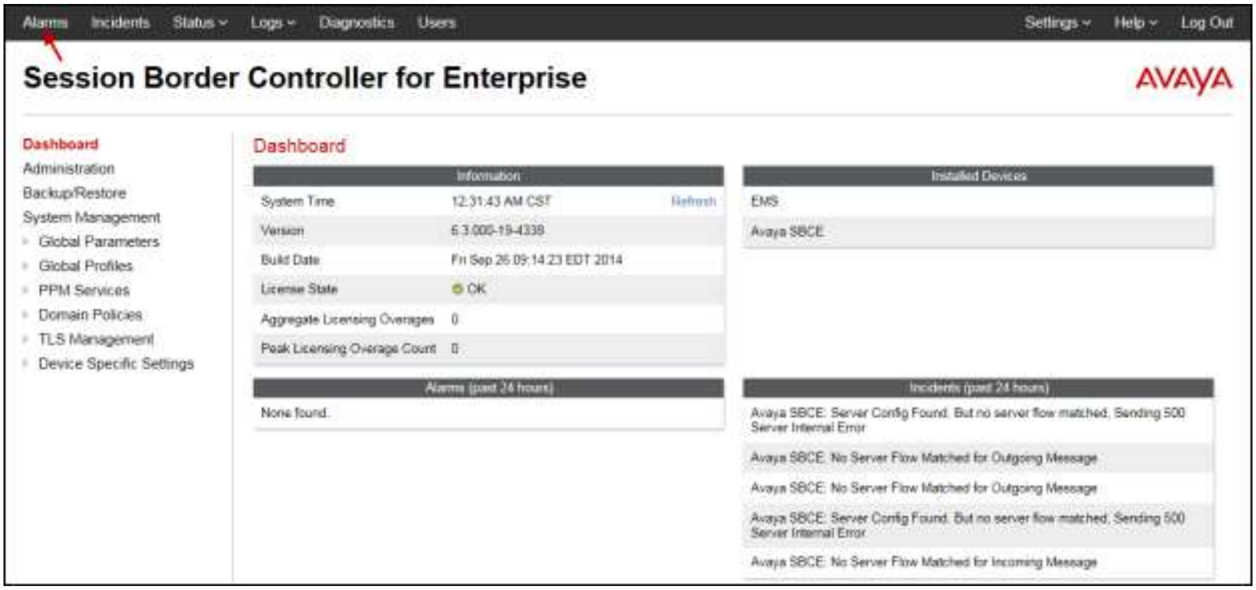
Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type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



8.4 Avaya Session Border Controller for Enterprise

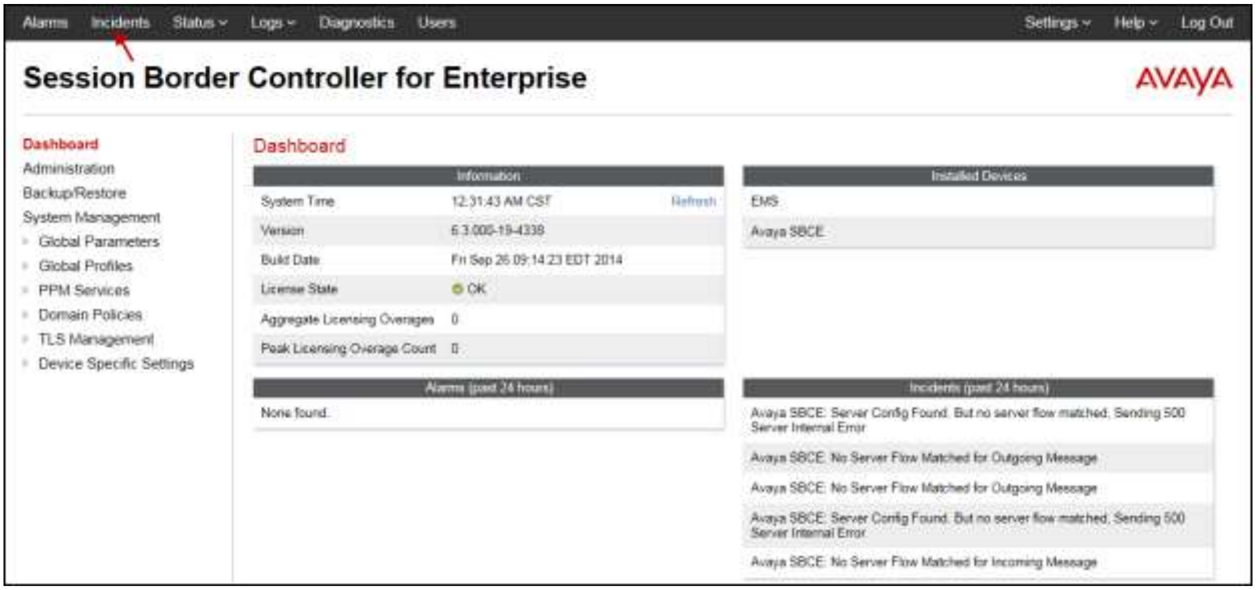
There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

Alarms: Provides information about the health of the Avaya SBCE.



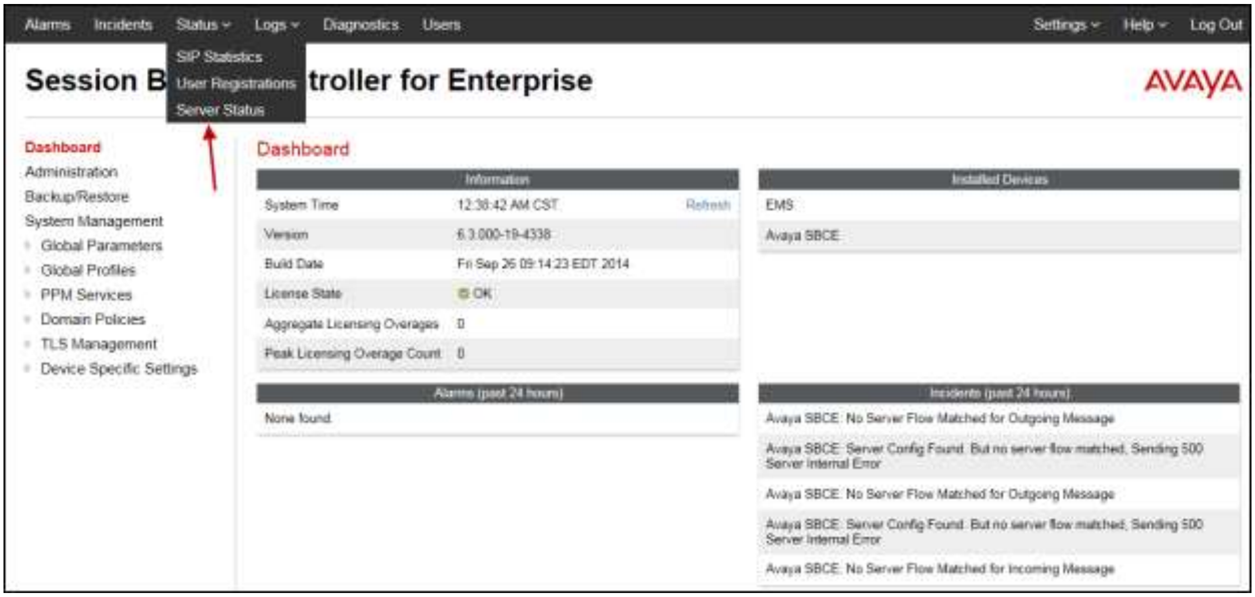
The following screen shows the **Alarm Viewer** page.

Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.

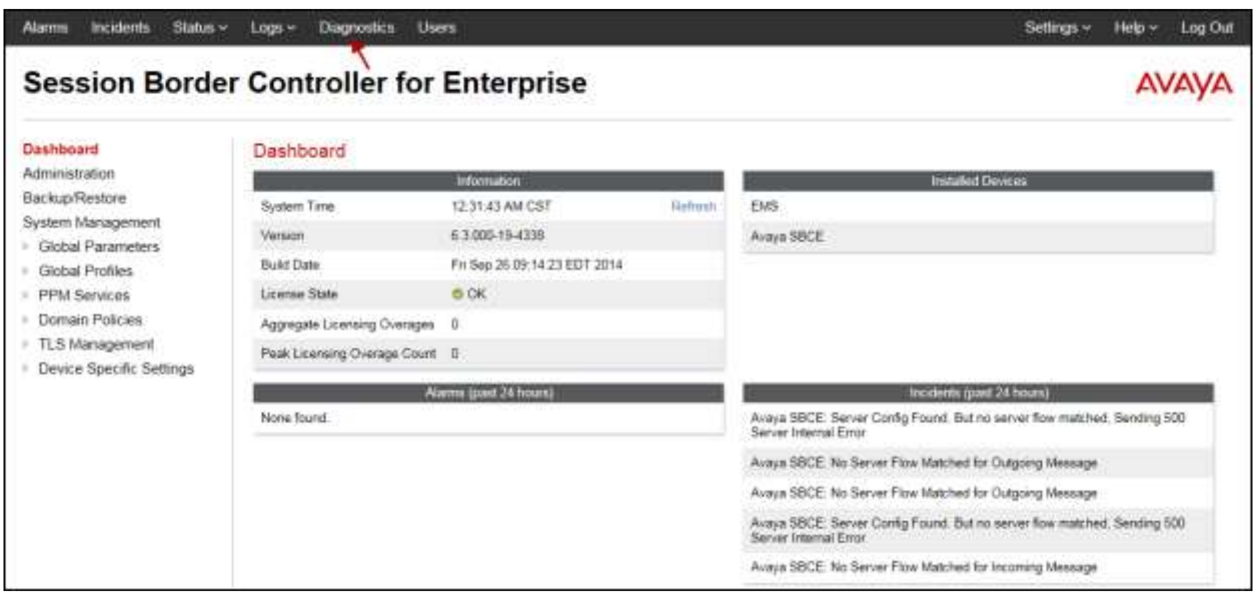


The following screen shows the **Incident Viewer** page.

Status: This screen provides SIP statistics, user registration information for Remote Workers, and server status information.

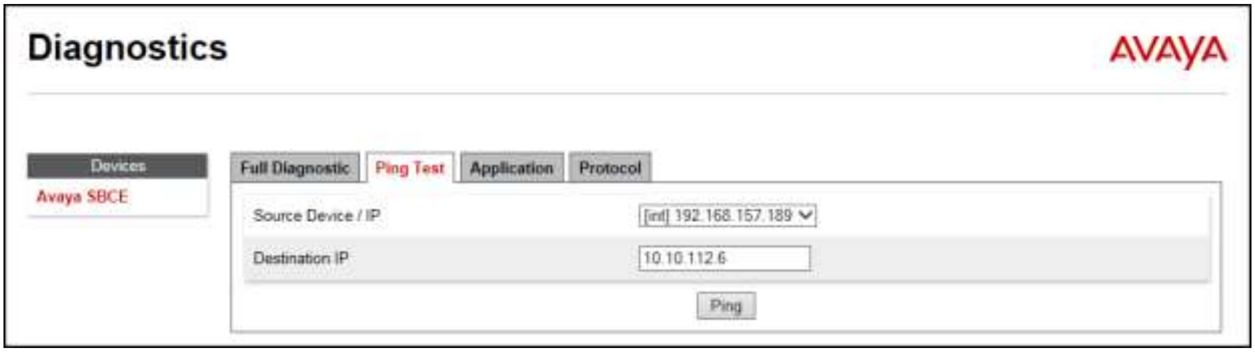


Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

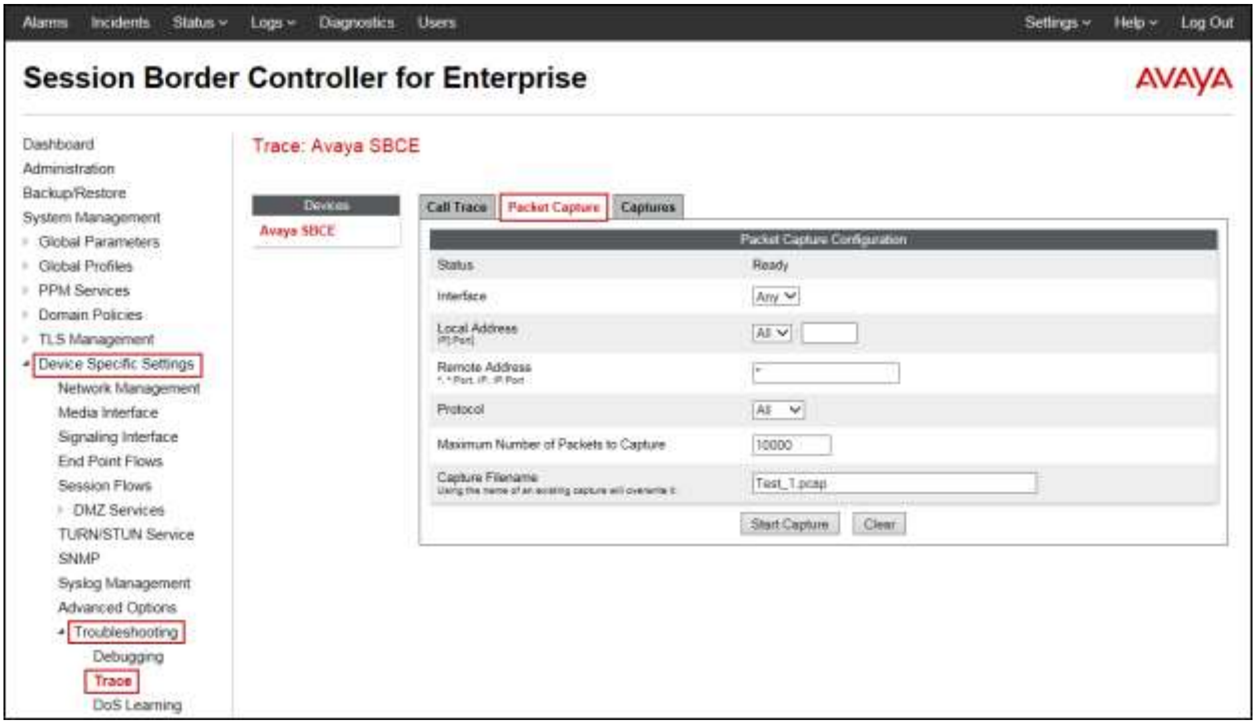


The following screen shows the **Diagnostics** page.

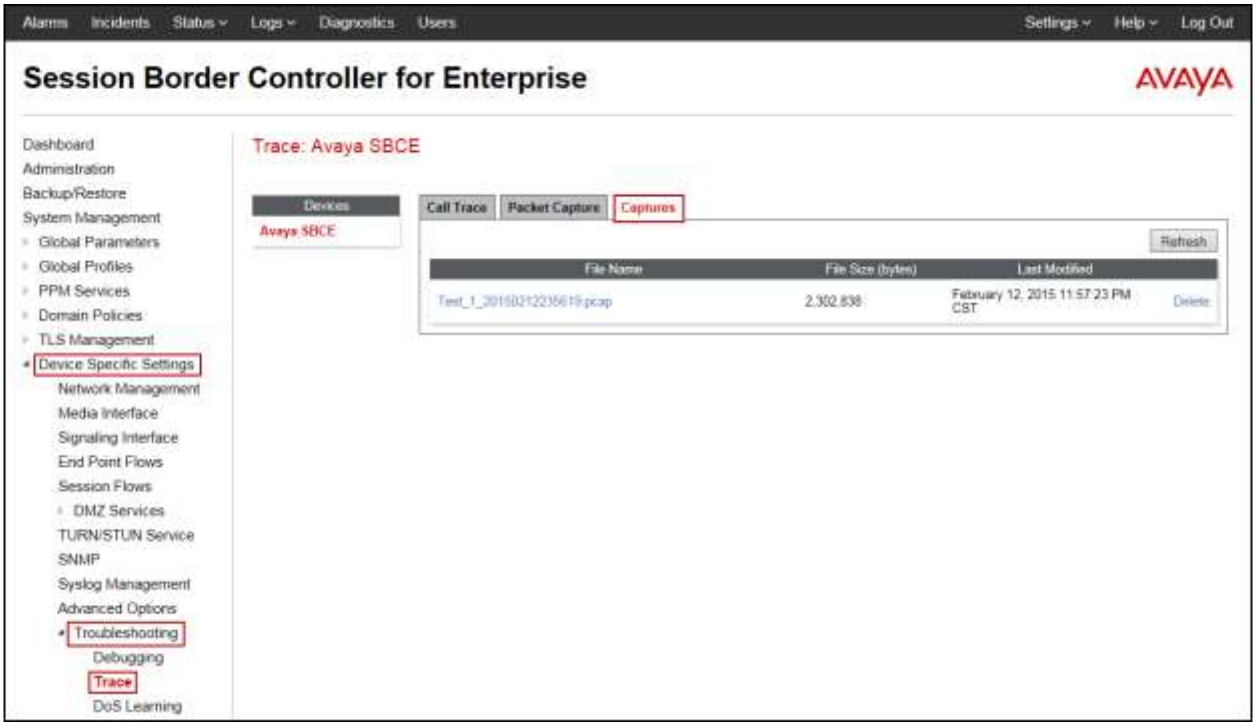
As an example, ping tests can be executed from the Avaya SBCE to verify connectivity to the Service Provider's SIP proxy IP address.



Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Device Specific Settings → Troubleshooting → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.



Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



9. Conclusion

These Application Notes describe the configuration steps necessary for configuring Session Initiation Protocol (SIP) Trunk Service for an enterprise solution consisting of Avaya IP Office Release 9.1 and the Avaya Session Border Controller for Enterprise Rel. 6.3 to interoperate with Time Warner Cable Business Class SIP Trunking Service.

Time Warner Cable Business Class SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

Time Warner Cable Business Class SIP Trunking Service passed compliance testing with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**

10. References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office and the Avaya Session Border Controller for Enterprise, including the following, is available at: http://support.avaya.com/

[1] *Avaya IP Office Platform Solution Description*, *Release 9.1*, Issue 1, December 2014.

[2] *Avaya IP Office Platform Feature Description*, *Release 9.1*, Issue 1, December 2014.

[3] *IP Office Platform 9.1 Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 30g, January 2015.

[4] *Administering Avaya IP Office Platform with Manager*, Release 9.1.0, Issue 10.02, January 2015.

[5] *IP Office Platform 9.1 Using Avaya IP Office Platform System Status*, Document 15-601758, Issue 10b, October 30, 2014.

[6] *IP Office Platform 9.1 Using IP Office System Monitor*, Document 15-601019, Issue 06b, November 13, 2014.

[7] *Using Avaya Communicator for Windows on IP Office*, Release 9.1, December 2014.

[8] *Administering Avaya Communicator on IP Office, Release 9.1*, December 2014.

[9] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.

[10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014.

[11] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*. https://downloads.avaya.com/css/P8/documents/100177106

Additional Avaya IP Office documentation can be found at: http://marketingtools.avaya.com/knowledgebase/

Product documentation for Time Warner Cable Business Class SIP Trunking Service is available from Time Warner Cable.

11. Appendix A: SigMa Script

The following Signaling Manipulation script was used in the configuration of the Avaya SBCE, **Section 6.2.6**:

Title: Remove Remote Address

```
//Remove Remote-Address header in outbound INVITEs and 200 OK messages

within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
  {
  remove(%HEADERS["Remote-Address"][1]);
}
}
```

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