Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunk Service with Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring MTS Allstream Session Initiation Protocol (SIP) Trunking Service with Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise Release 6.2.

MTS Allstream SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and MTS Allstream network as an alternative to legacy analog or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

MTS Allstream 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.

©2014 Avaya Inc. All Rights Reserved.

Table of Contents

©2014 Avaya Inc. All Rights Reserved.

©2014 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service in between the service provider MTS Allstream and Avaya IP Office solution.

In the sample configuration, the Avaya IP Office solution consists of Avaya IP Office (IP Office) 500v2 Release 9.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2, Avaya IP Office Video Softphone, Avaya Flare® Experience for Windows and Avaya Deskphones, including SIP, H.323, digital, and analog. The Remote Worker capability was also tested. The Avaya SBCE provides security for the Avaya IP Office solution, as well as interoperability features for the SIP trunk.

MTS Allstream SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the Avaya IP Office solution are able to place and receive PSTN calls via a broadband WAN connection using 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

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using IP Office to connect to MTS Allstream 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.

Testing was performed with IP Office 500v2 R9.0, but it also applies to IP Office Server Edition R9.0. Note that IP Office Server Edition requires an Expansion IP Office 500v2 R9.0 to support analog, digital endpoints or trunks.

2.1 Interoperability Compliance Testing

To verify MTS Allstream SIP Trunking interoperability, the following features and functionalities were exercised during the compliance testing:

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, digital and analog at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP Trunk from the service provider networks.
- Outgoing PSTN calls from Avaya endpoints including SIP, H.323, digital and analog telephone at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider networks.
- Remote Worker capability using Avaya Flare® Experience for Windows.
- Incoming and outgoing PSTN calls to/from Avaya IP Office Video Softphone.

©2014 Avaya Inc. All Rights Reserved.

- Incoming and outgoing PSTN calls to/from Avaya Flare® Experience for Windows.
- Dialing plans including long distance, international, outbound toll-free, etc.
- Caller ID presentation and Caller ID restriction.
- Codec G.729A and G.711MU.
- T.38 fax.
- Proper early media transmissions.
- DTMF tone transmissions per RFC 2833.
- Voicemail navigation for incoming and outgoing calls.
- Telephony features such as hold and resume, call transfer, call forward and conferencing.
- Off-net call forwards and transfers.
- Mobility Twinning of incoming calls to mobile phones.
- Response to incomplete call attempts and trunk errors.

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 will not be discussed in these Application Notes.

Inbound toll-free calls and 911 emergency calls are supported but were not tested as part of the compliance test.

The following items are not supported:

- **SIP REFER**.

2.2 Test Results

Interoperability testing with MTS Allstream was successfully completed with the exception of observations/limitations described below:

- **T.38 Fallback** – With **Fax Transport Support** set as **T38 Fallback** in IP Office (SIP Line→VoIP), incoming fax calls (PSTN→IP Office), will fail to connect with G.711 transport when T.38 is disabled at the Service Provider. Outbound fax calls will successfully default to G.711 transport. The problem is only seen with incoming (PSTN→IP Office) fax calls. **T.38** transport was successfully tested in both directions (PSTN→IP Office and IP Office→PSTN). For this solution Avaya recommends only using **T.38** as the fax transport (with **Transport Support** set as **T38** in IP Office (SIP Line→VoIP)). This issue is under investigation by Avaya.
- **Direct Media** – With Direct Media enabled in IP office, when calling IVR systems (or any recorded messaging system), from IP Office, a noticeable clipping of the recorded announcement/message is heard when IP Office sends the re-Invite to establish the direct media connection to the IP Phone. Testing was done with Direct Media disabled in IP Office. This issue is under investigation by Avaya.
- **Codec Lockdown on Outbound Calls –** On outbound calls, MTS Allstream responds to the INVITE request sent by IP Office, with multiple codecs instead of selecting one from the INVITE SDP list. IP Office uses the first compatible codec in the list. This behavior has no user impact, calls were successful.
- **INVITE message with m:audio and m:image in the SDP –** Voice/audio calls made from the PSTN to IP Office, mapped to a particular DID, contained multiple "m:" lines in the SDP of the INVITE message sent by MTS Allstream, with "m:" lines in the following order:

©2014 Avaya Inc. All Rights Reserved.

m:audio first (top) followed by m:image second (bottom). When the call was answered at the IP Office station, IP Office sends the 200 OK with "m:" lines in the reverse order or m:image first (top) followed by m:audio second (bottom), this behavior resulted in one-way audio. This behavior only occurs when "Fax Transport Support" is set to "None" under SIP Line/VoIP. With "Fax Transport Support" set only as "T.38" (Avaya recommended value for this solution) this behavior doesn't occur, with it set as "T.38" IP Office will only include m:audio in the 200 OK message (m:image in not included) resulting in good audio in both directions. Since Avaya recommends only using **T.38** as the fax transport for this solution this behavior will not be seen.

- **Disable the use of PAI** – IP Office SIP Line; disable the use of P-Asserted-Identity (PAI) header. Disabling the use of the PAI header in IP Office provided the expected calling party number, such as for calls forwarded to the PSTN and for call twinning scenarios.

2.3 Support

For technical support on the MTS Allstream SIP Trunking service, visit the MTS Allstream customer support web page at https://www.mts.ca/mts/contact+us

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. It shows a simulated enterprise site connected to the MTS Allstream 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 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 9600 Series H.323 IP Telephones.
- Avaya 11x0 Series SIP IP Telephones.
- Avaya IP Office Video Softphone.
- Avaya Flare® Experience for Windows.
- Avaya 1408 Digital Telephones.
- Avaya 9508 Digital Telephones.

©2014 Avaya Inc. All Rights Reserved.

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. IP Office **LAN1** 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 MTS Allstream networks via the public internet.

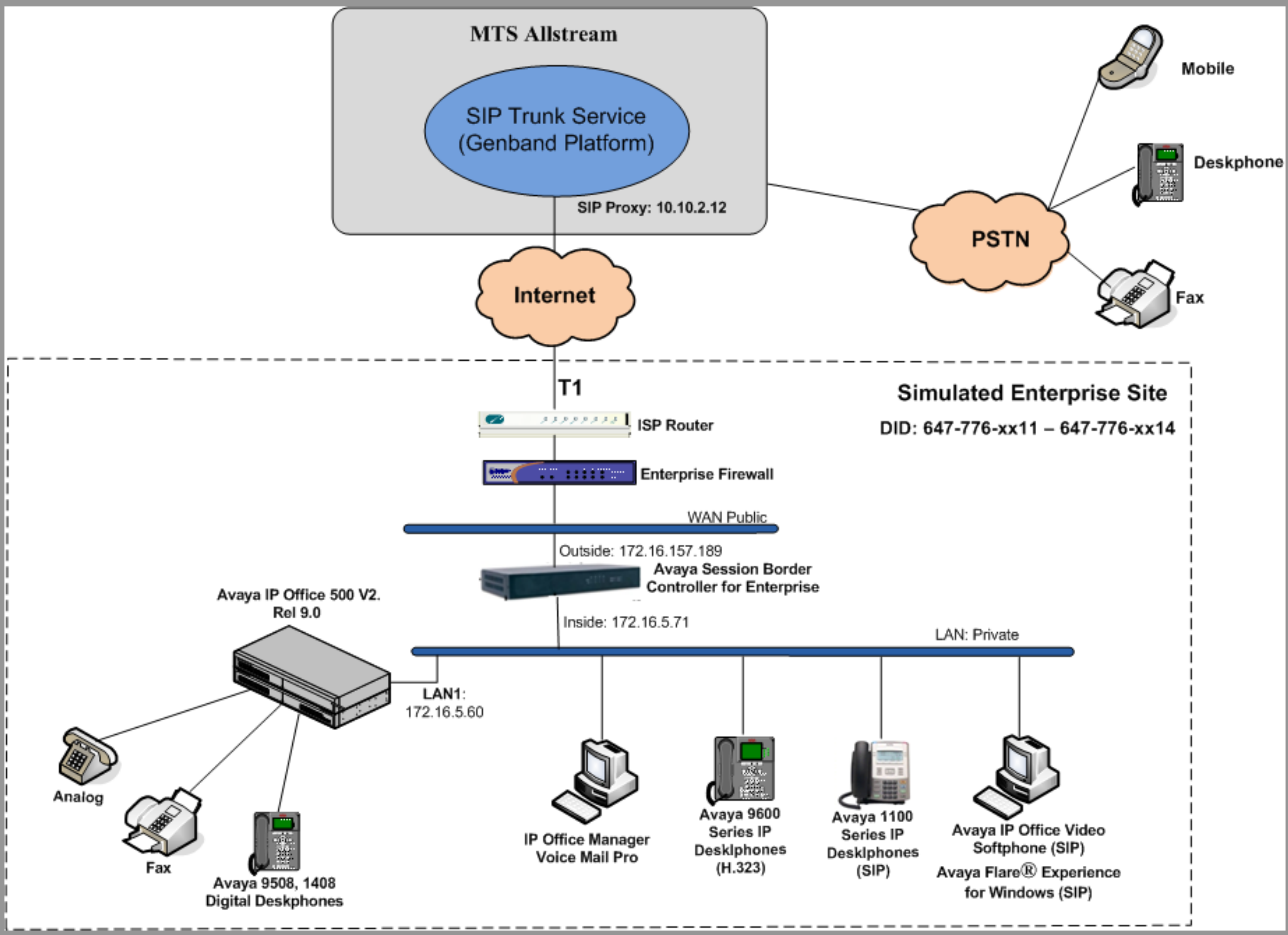


Figure 1: Avaya Interoperability Test Lab Configuration.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to MTS Allstream (refer to **Section 5.11**). The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network. Since MTS Allstream is a Canadian company, and Canada is a country member of the North American Numbering Plan (NANP), the users dialed 10 digits for local calls, including the area code, and 11 (1 + 10) digits for other calls between the NANP.

©2014 Avaya Inc. All Rights Reserved.

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.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment/Software	**Release/Version**
Avaya IP Office 500v2	9.0 Build 829
Avaya IP Office DIG DCPx16 V2	9.0 Build 829
Avaya IP Office Manager	9.0 Build 829
Avaya Voicemail Pro for IP Office	9.0 Build 311
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2 (6.2.0.Q48)
Avaya 9620 IP Telephone (H.323)	Avaya one-X® Deskphone Edition S3.2
Avaya 1140 IP Telephone (SIP)	SIP1140 Ver. 04.03.18.00
Avaya IP Office Video Softphone	3.2.3.49 68975
Avaya Flare® Experience for Windows	1.1.4.23
Avaya Digital Telephones 1408	32
Avaya Digital Telephones 9508	0.45

MTS Allstream SIP Trunk Service	
Equipment/Software	**Release/Version**
Genband S3 Session Border Controller	7.1.13.1
Nortel CS2K	CVM15

©2014 Avaya Inc. All Rights Reserved.

5. Configure IP Office

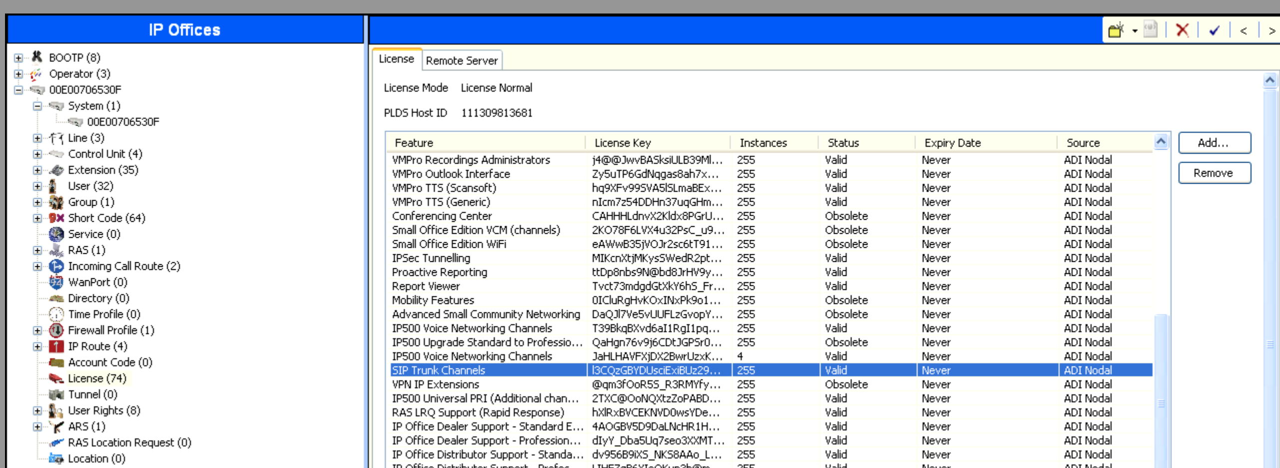
This section describes the IP Office configuration required to interwork with MTS Allstream. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. Navigate to **File → Open Configuration**, select the proper IP Office from the pop-up window, and log in with the appropriate credentials. A management window will appear as shown in the next sections. The appearance of IP Office Manager can be customized using the **View** menu (not shown). In the screenshots presented in this section, the **View** menu was configured to show the **Navigation Pane** on the left side and the **Details Pane** on the right side. These panes will be referenced throughout these Application Notes.

These Application Notes assume the basic installation and configuration have already been completed and are not discussed here. For further information on IP Office, please consult References in **Section 10**.

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 Group pane. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the Details pane. Note that the actual License Keys in the screen below were edited for security purposes.



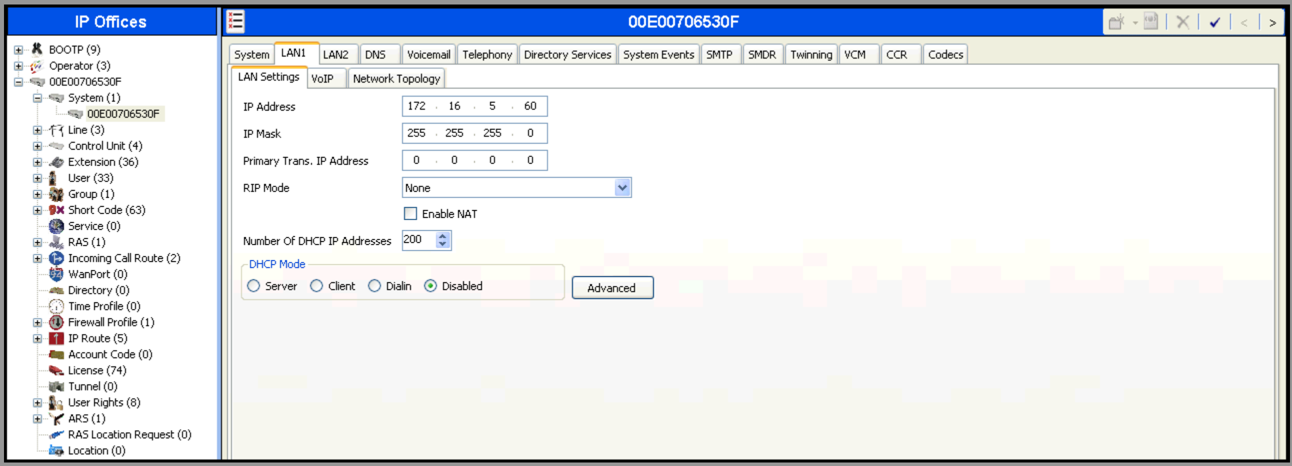
5.2 LAN1 Settings

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 MTS Allstream networks 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

©2014 Avaya Inc. All Rights Reserved.

navigate to the **LAN1→ LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters.

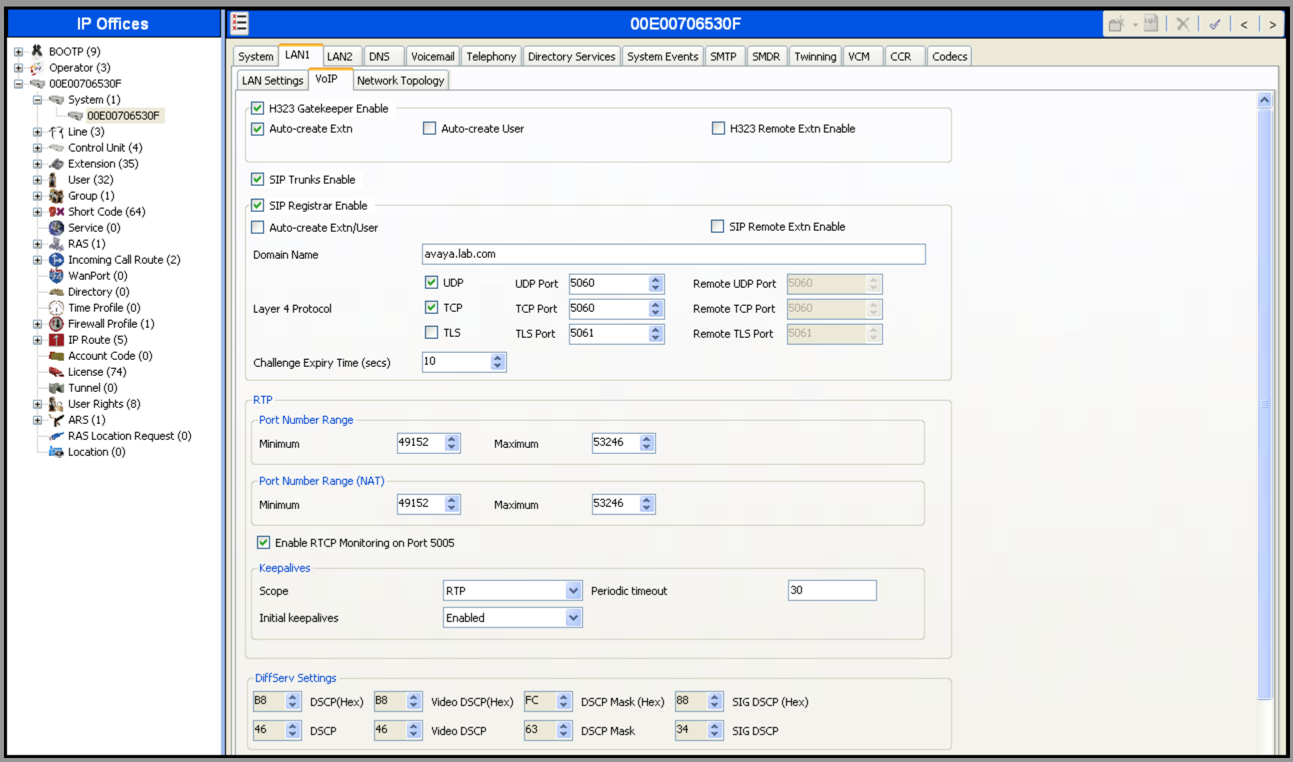
- Set the **IP Address** field to the LAN IP address, e.g. **172.16.5.60**.
- Set the **IP Mask** field to the subnet mask of the public network, e.g. **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown).



©2014 Avaya Inc. All Rights Reserved.

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

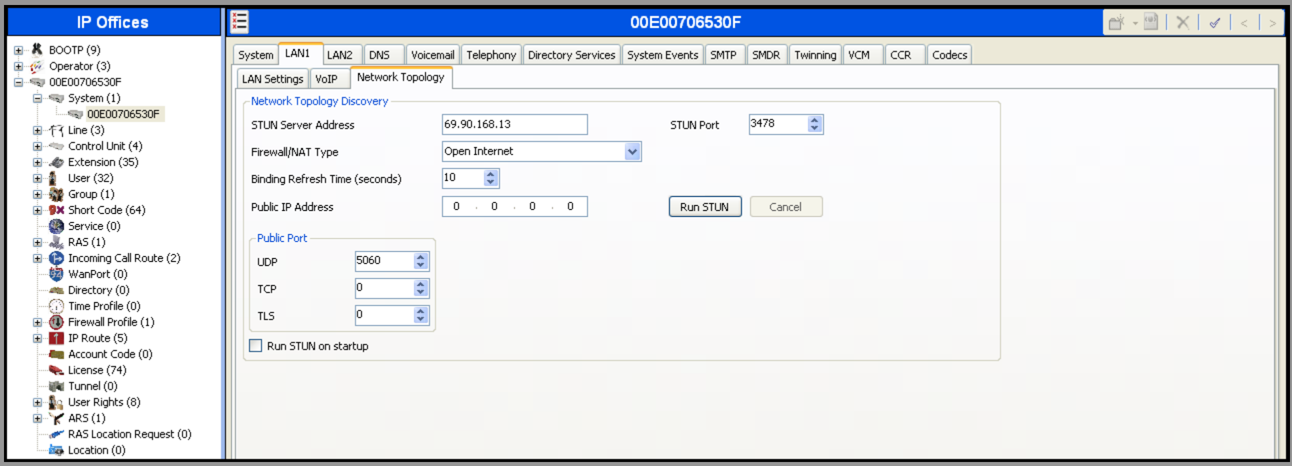
- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to MTS Allstream.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register 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).



©2014 Avaya Inc. All Rights Reserved.

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).



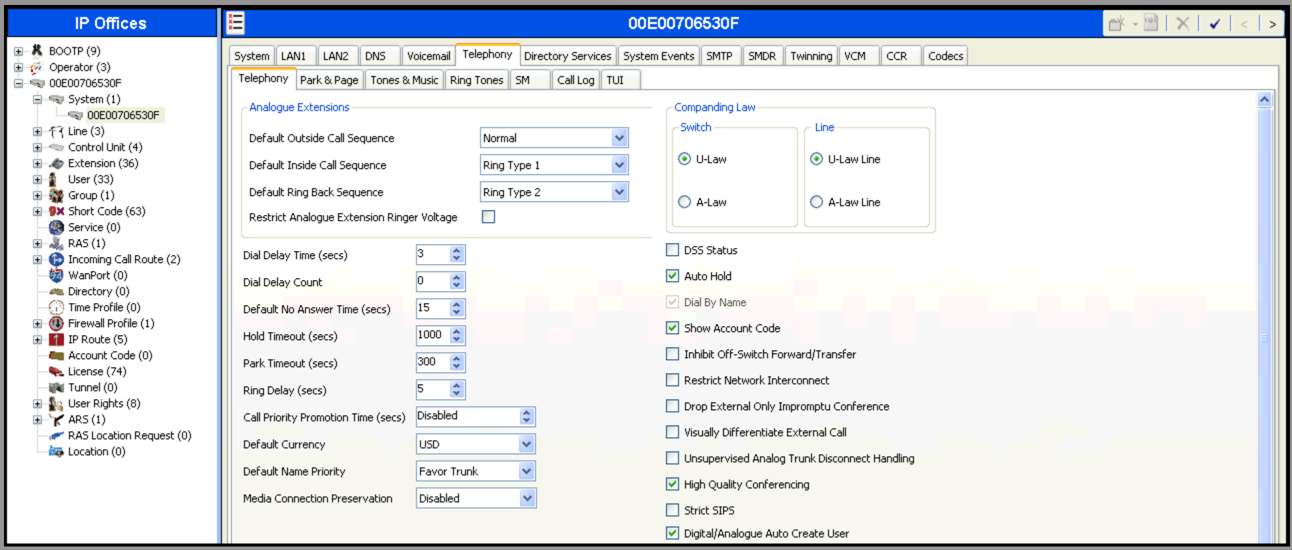
In the compliance test, the **LAN1** interface was used to connect Avaya IP Office to the enterprise private network (LAN), **LAN2** was not used.

©2014 Avaya Inc. All Rights Reserved.

5.3 System Telephony Settings

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).

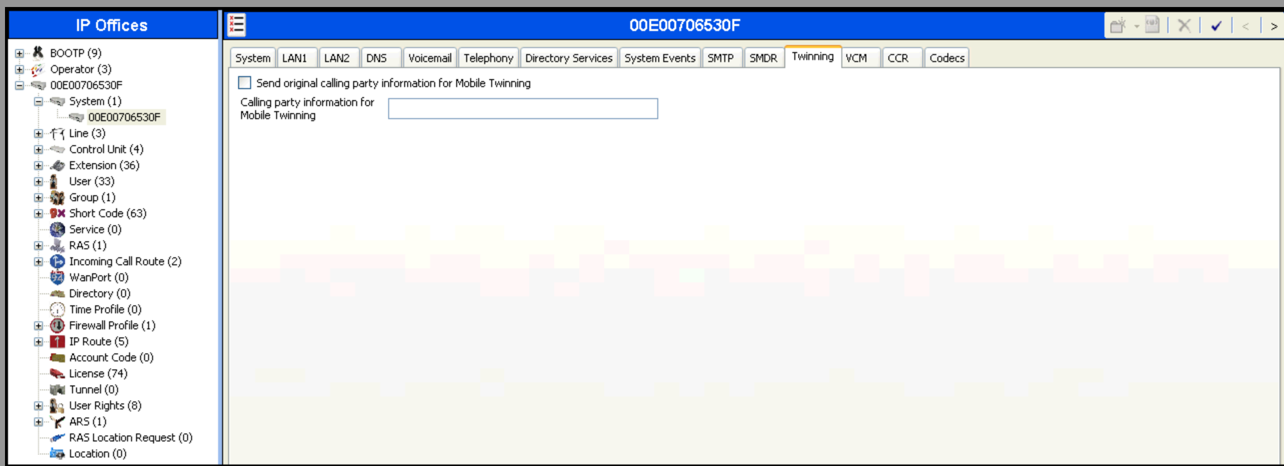


©2014 Avaya Inc. All Rights Reserved.

5.4 Twinning Calling Party Settings

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 5.7**). This setting also impacts the Caller ID for call forwarding.
- Click OK to commit (not shown).

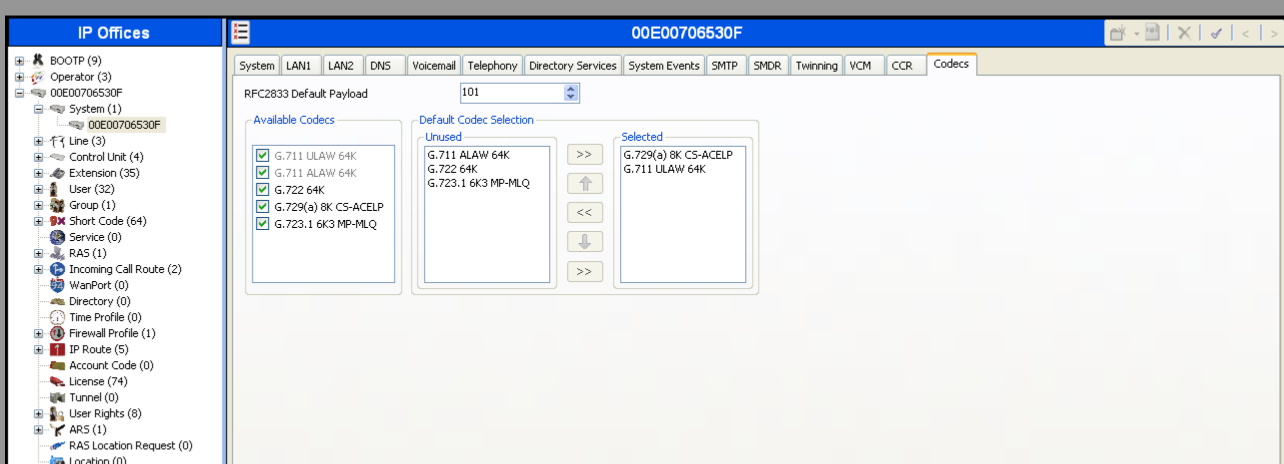


5.5 Codec's settings

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

- The **RFC2833 Default Payload** field is new in IP Office release 9.0. It allows the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used
- Select the **Codecs**.
- Click OK to commit (not shown).

The **Codec's** settings are shown in the screenshot below with G.729(a) and G.711ULAW selected in prioritized order.

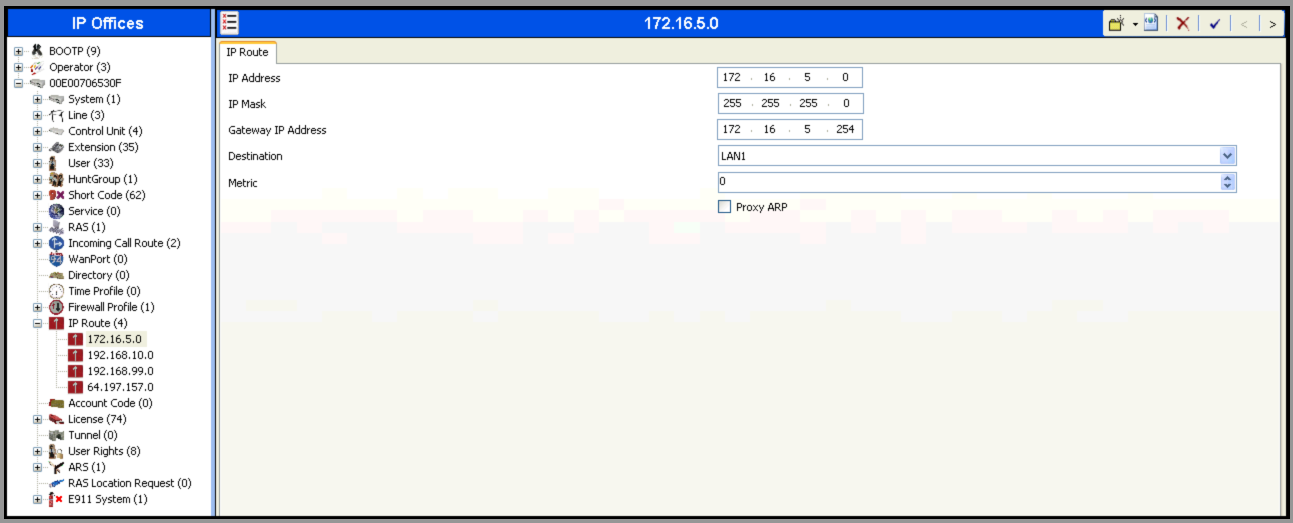


©2014 Avaya Inc. All Rights Reserved.

5.6 IP Route

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 subnet where the SIP proxy is located on the MTS Allstream network. On the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask.**
- Set **Gateway IP Address** to the IP Address of the router used to reach the external network.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click OK to commit (not shown).



©2014 Avaya Inc. All Rights Reserved.

5.7 Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the MTS Allstream SIP Trunk 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 IP Office Manager to create a SIP Line. Follow the steps in **Section 5.7.1** 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 5.7.2 – 5.7.5**.

Also, 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 Required

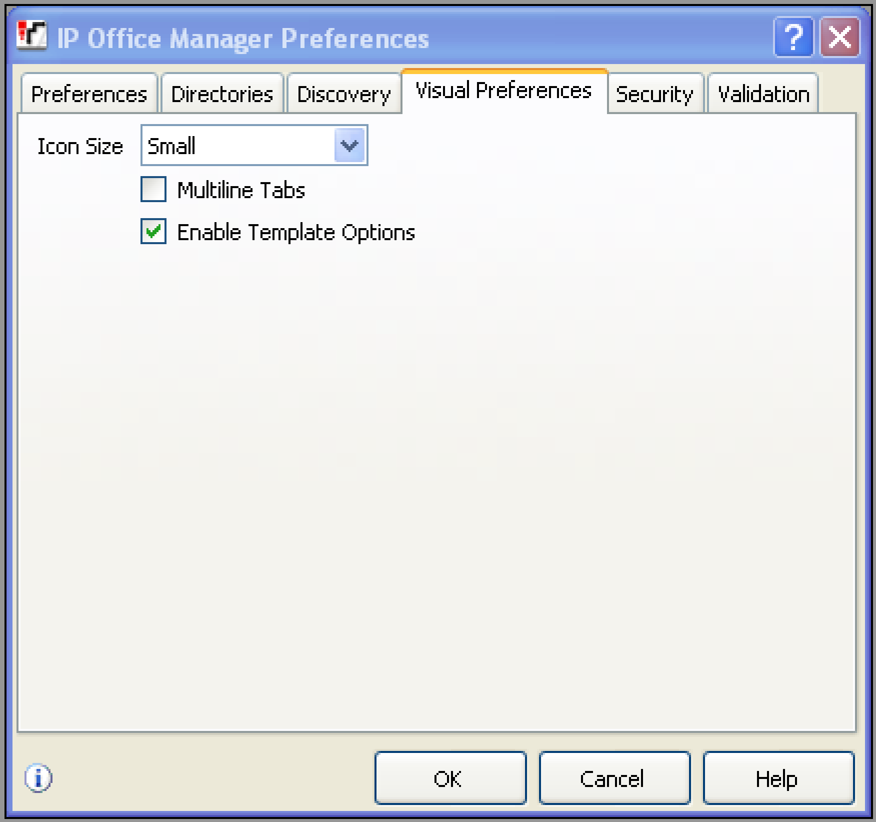
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.7.2 – 5.7.5**.

5.7.1 Create a New SIP Trunk from Template

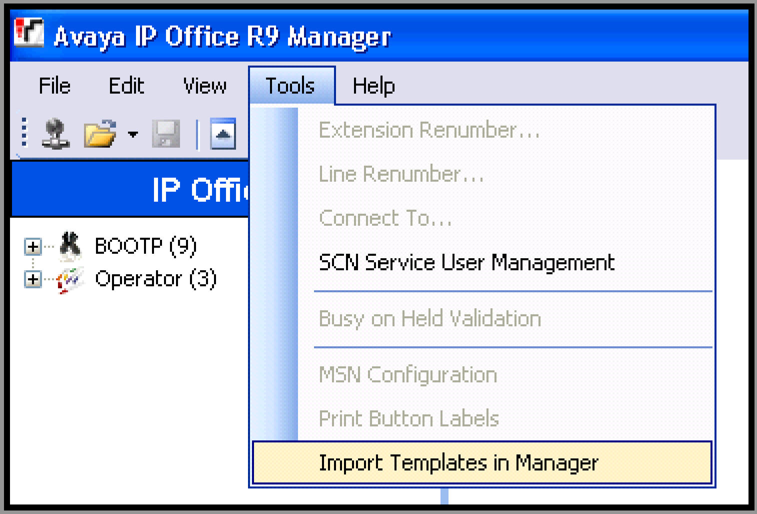
1. Copy the template file to the computer where IP Office Manager is installed. If needed rename the template file to **CA_MTS Allstream_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.

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. Verify that the box is checked next to **Enable Template Options**. Click **OK**.

©2014 Avaya Inc. All Rights Reserved.



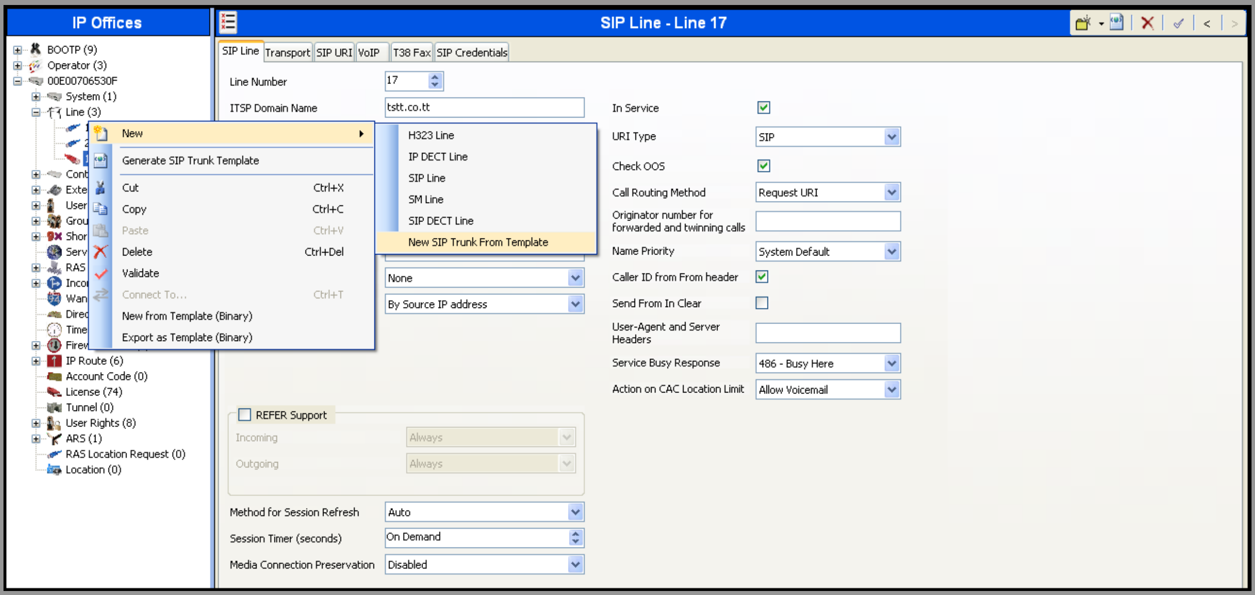
3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.



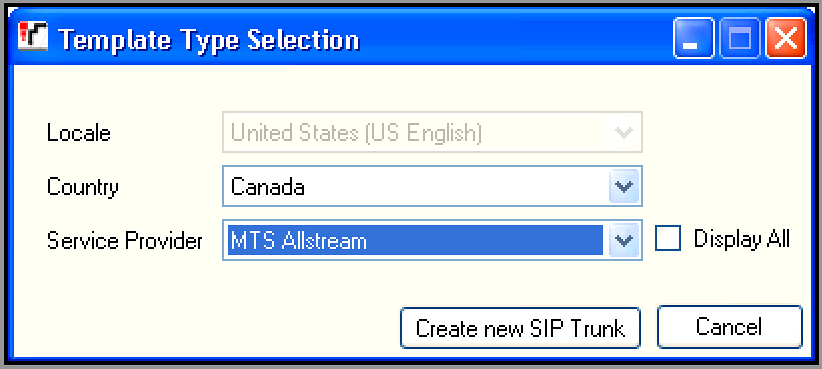
©2014 Avaya Inc. All Rights Reserved.

4. In the pop-up window (not shown) that appears select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

5. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New SIP Trunk From Template**.



6. In the subsequent Template Type Selection pop-up window, select **Canada** from the **Country** pull-down menu and select **MTS Allstream** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**CA_MTS Allstream_SIPTrunk.xml)** created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



©2014 Avaya Inc. All Rights Reserved.

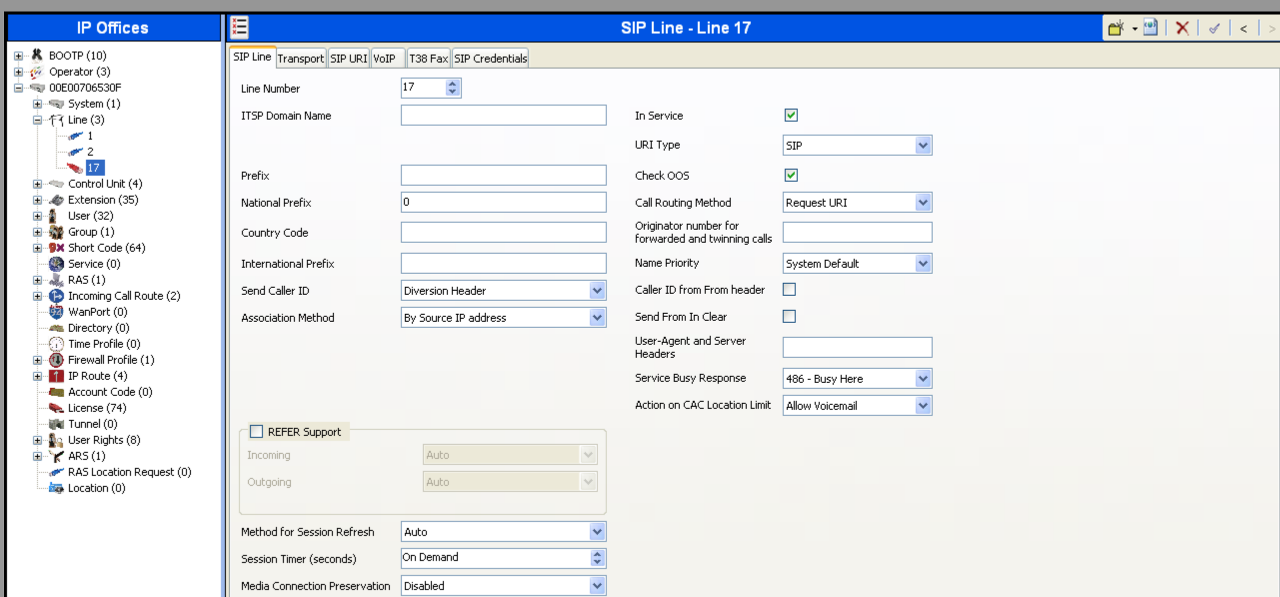
Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.7.2 – 5.7.5.**

Alternatively, a SIP Line can be created manually with the parameters shown below. To create a SIP line manually, begin by navigating to **Line** in the Navigation Pane. Right-click and select **New→ SIP Line**.

5.7.2 SIP Line Tab

On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

- Leave the **ITSP Domain Name** blank.
- Verify that **In Service** box is checked.
- Verify that **Check OOS** box is checked. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Call Routing Method** is set to **Request URI**.
- Set **Send Caller ID** to **Diversion Header**.
- Uncheck the **REFER support** box. IP Office will not send REFER messages for calls that are transferred back to the PSTN. MTS Allstream doesn't support SIP REFER messages.
- Set **Method for Session Refresh** to **Auto**.
- Set **Session Timer (Seconds**) to **On Demand.**
- Set **Media Connection Preservation** to **Disabled.**
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

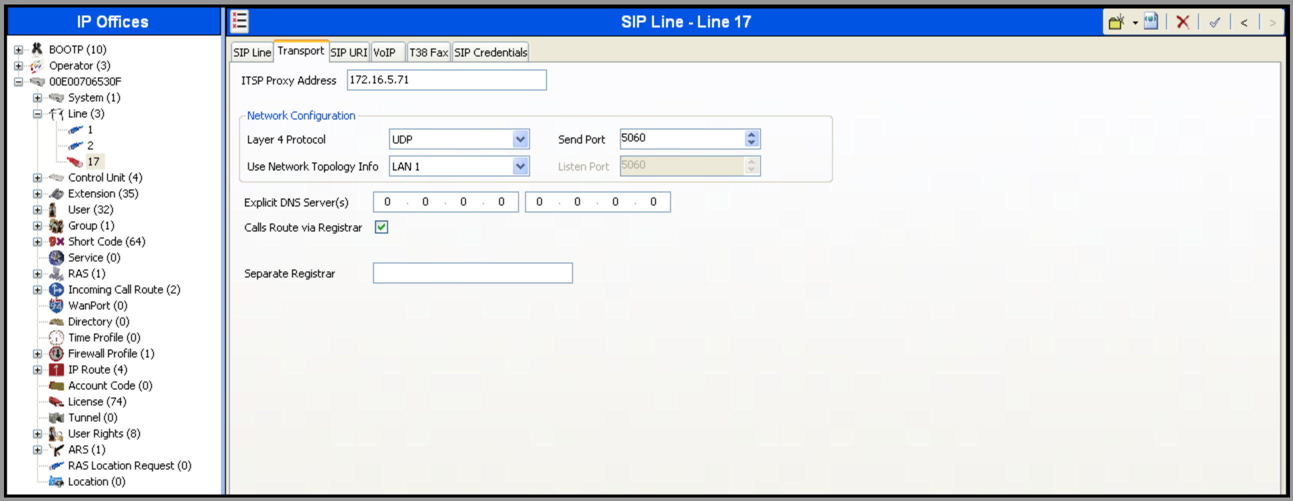


©2014 Avaya Inc. All Rights Reserved.

5.7.3 Transport Tab

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

- Set the **ITSP Proxy Address,** this address was set 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).

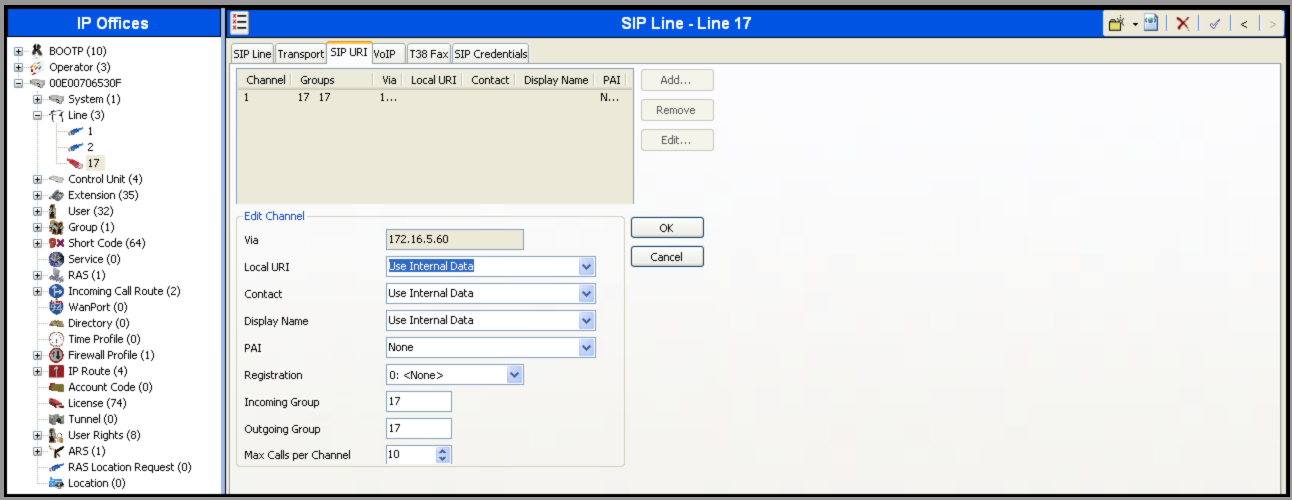


©2014 Avaya Inc. All Rights Reserved.

5.7.4 SIP URI Tab

A SIP URI entry needs to be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, and 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. In the example screen below, a previously configured entry was edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**,
- Set **PAI** to **None**. IP Office will not include the PAI header in SIP messaging. Removing the use of the PAI header provided the expected calling party number across the PSTN carriers encountered in the compliance test, especially for the call forwarding and twinning scenarios.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click OK to commit (not shown).

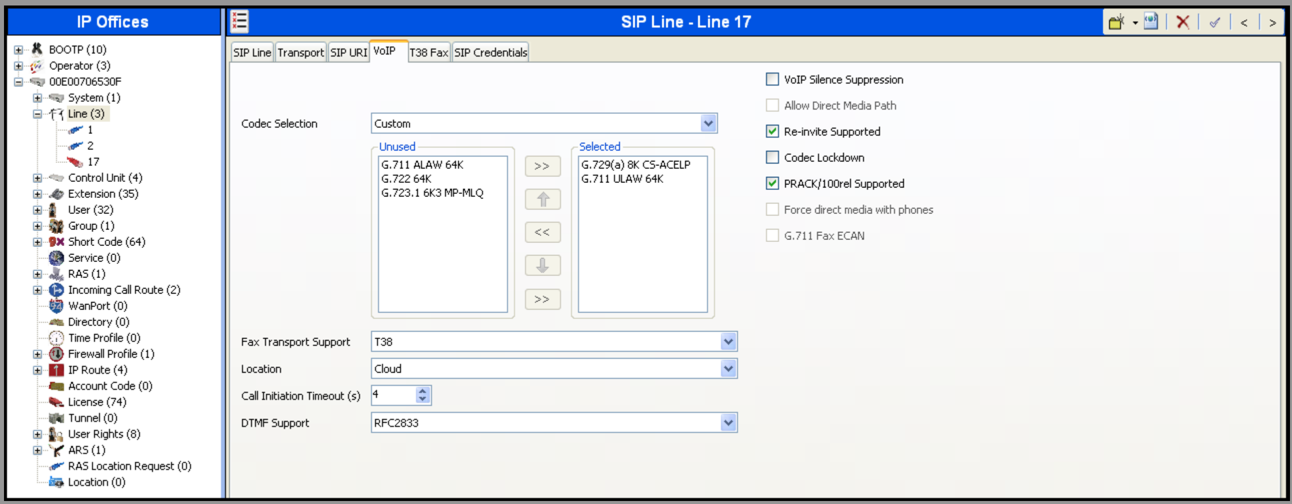


©2014 Avaya Inc. All Rights Reserved.

5.7.5 VoIP Tab

Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

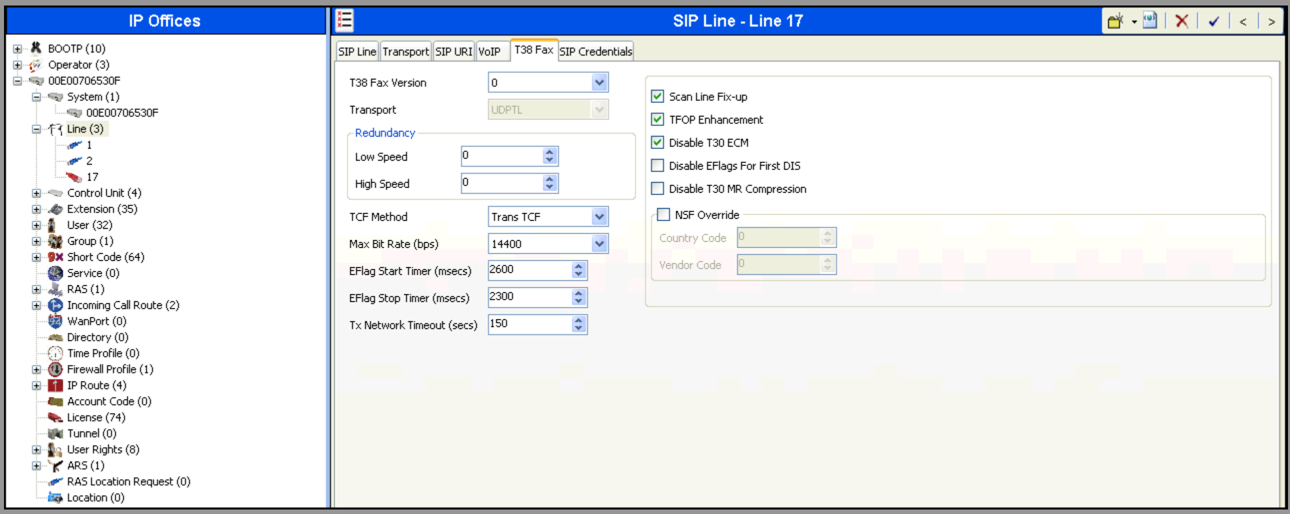
- In the sample configuration, the **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codec's to be specified. The buttons allow setting the specific order of preference for the codec's to be used on the line, as shown. MTS Allstream supports codec's G.729A and G.711ULAW (or G.711MU).
- Set **Fax Transport Support** to **T.38** (refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833.** This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Verify that **Allow Direct Media Path** is unchecked. Testing was done with Direct Media disabled (Refer to **Section 2.2**).
- Check the **Re-invite Supported** box 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.
- Check the **PRACK/100rel Supported** box, to advertise the support for reliable provisional responses and Early Media to MTS Allstream.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



©2014 Avaya Inc. All Rights Reserved.

Select the **T38 Fax** tab to set the Fax over Internet Protocol parameters of the SIP line. Set the parameters as shown below.

- Uncheck **Use Default Values** at the bottom of the screen.
- Set **T38 Fax Version** to **0**. MTS Allstream SIP Trunking supports T.38 fax version 0.
- Set **Max Bit Rate (bps**) to 14400, the highest fax bit rate that Avaya IP Office supports for T.38 faxing.
- Check the **Disable T30 ECM** option.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

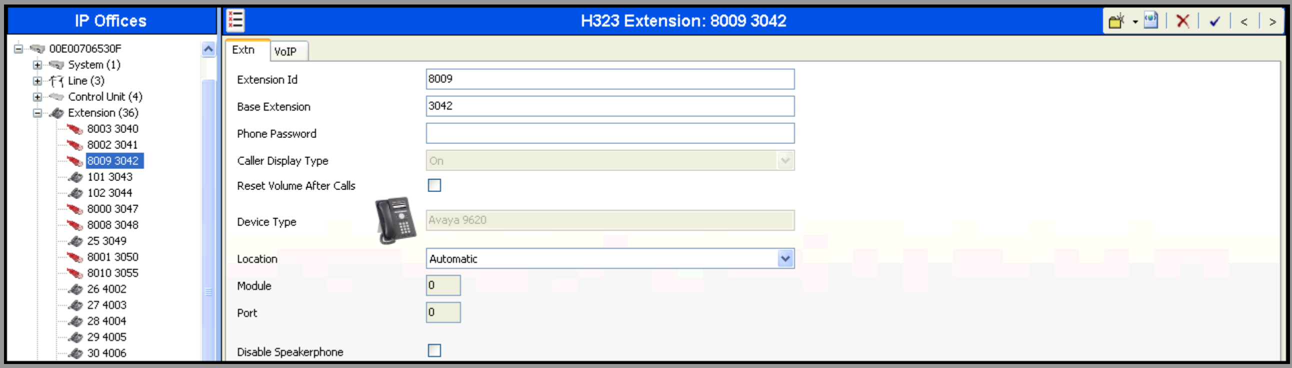


©2014 Avaya Inc. All Rights Reserved.

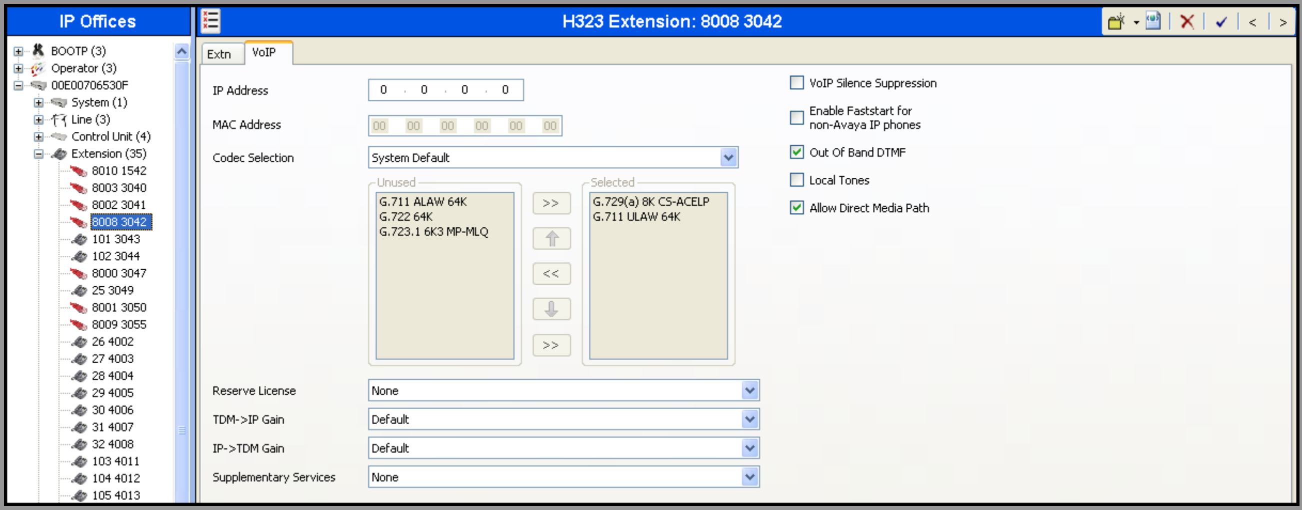
5.8 Extension

In this section, an example of an Avaya IP Office Extension will be illustrated. In the interests of brevity, not all users and extensions will be presented, since the configuration can be easily extrapolated to other users and extensions. To add an Extension, right click on **Extension** then select **New → Select H323 or SIP.**

Select the **Extn** tab. Following is an example of extension 3042; this extension corresponds to an H.323 extension.



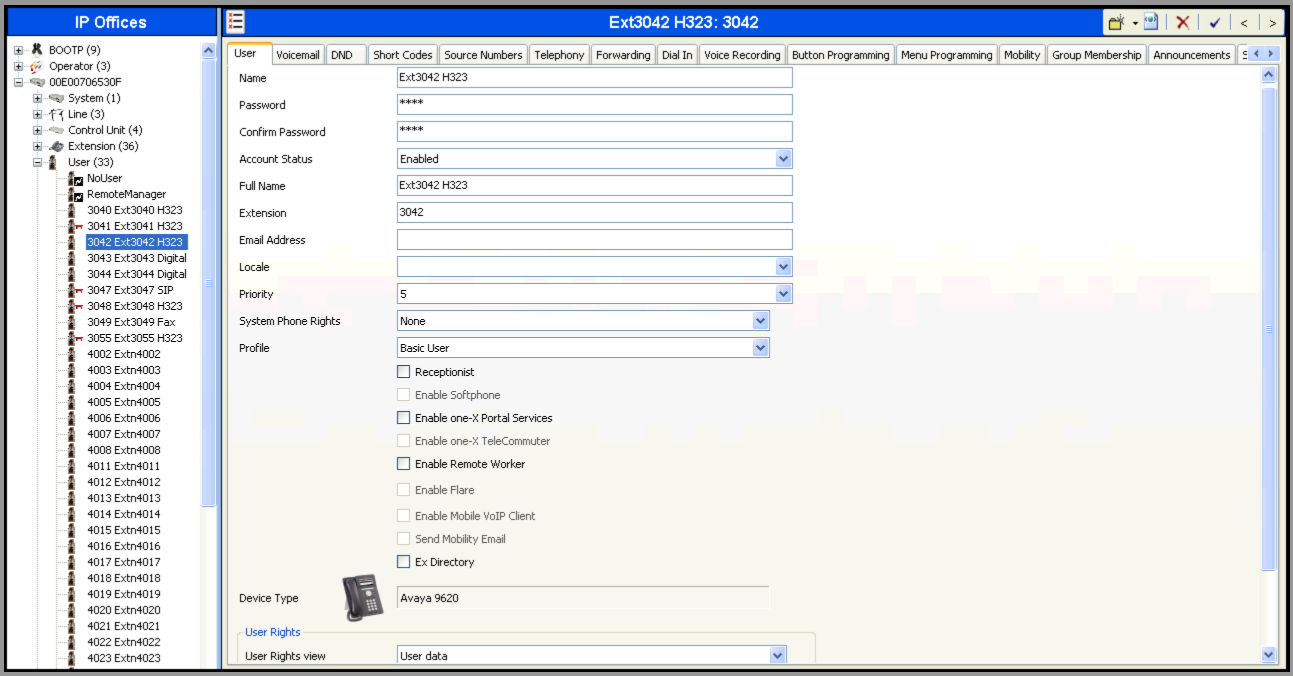
Select the **VOIP** tab. Use default values on VoIP tab. Following is an example for Extension 3042; this extension corresponds to an H.323 extension.



©2014 Avaya Inc. All Rights Reserved.

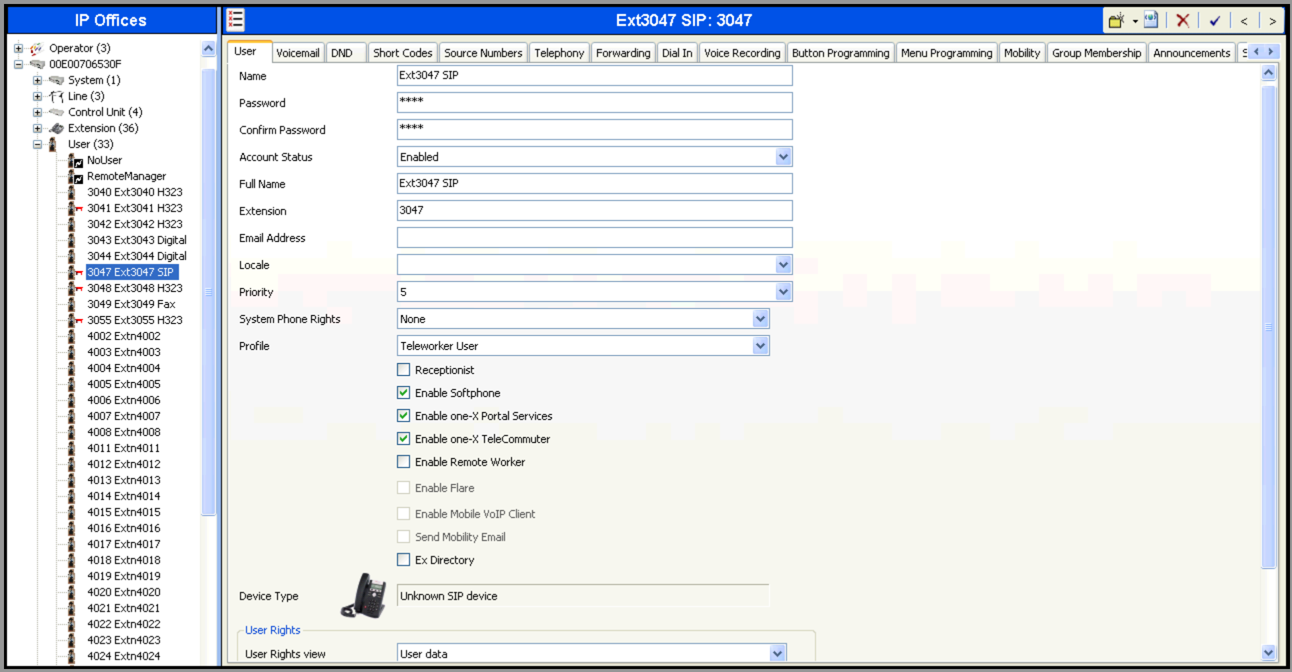
5.9 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.7**. To configure these settings, first navigate to **User** in the left Navigation Pane, and then select the name of the user to be modified in the center Group Pane. In the example below, the name of the user is **Ext3042 H323**.

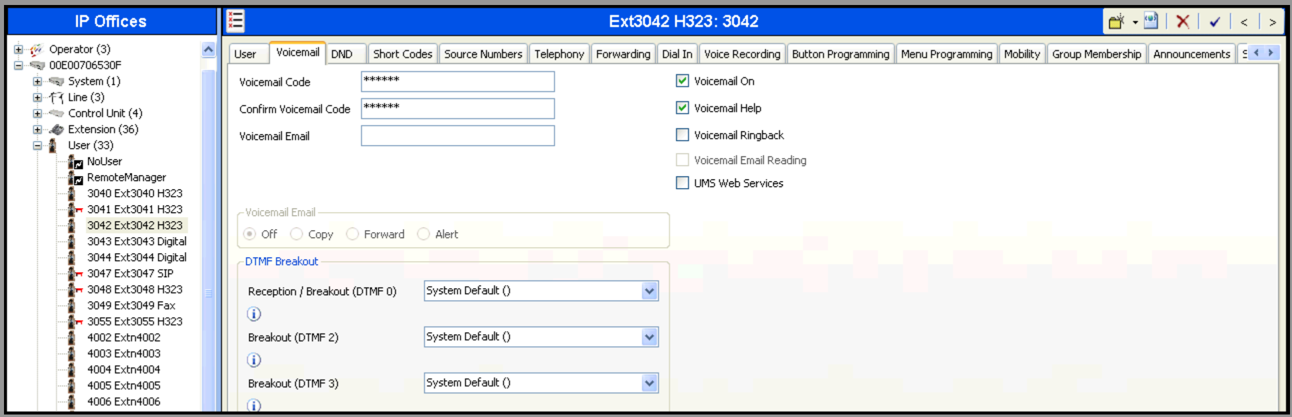


©2014 Avaya Inc. All Rights Reserved.

In the example below, the name of the user is “Ext3047 SIP”. This is an Avaya IP Office Softphone user, set the Profile to **Teleworker User** and check **Enable Softphone**.

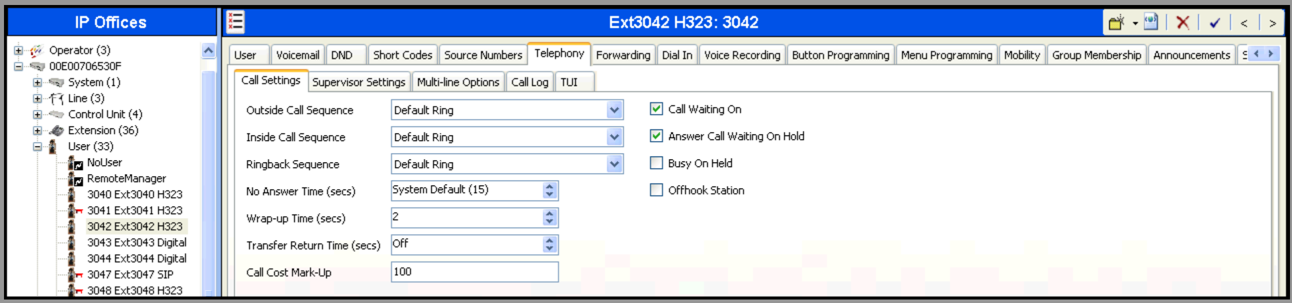


Select the **Voice Mail** tab. The following screen shows the **Voicemail** tab for the user with extension 3042. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application Notes, incoming calls from MTS Allstream to this user were redirected to Voicemail Pro after no answer. Voicemail messages were recorded and retrieved successfully. Voice mail navigation and retrieval were performed locally and from PSTN telephones to test DTMF using RFC 2833.

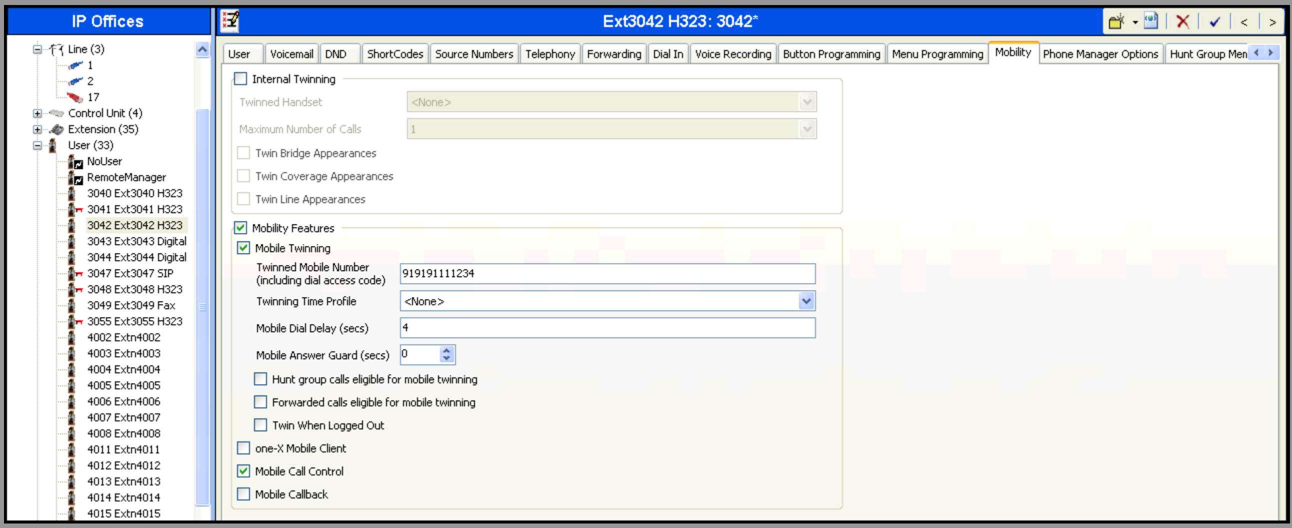


©2014 Avaya Inc. All Rights Reserved.

Select the **Telephony** tab, then **Call Settings** tab as shown below. Check the **Call Waiting On** box to allow an Avaya IP Office phone logged in as this extension to have multiple call appearances and for call transfers.

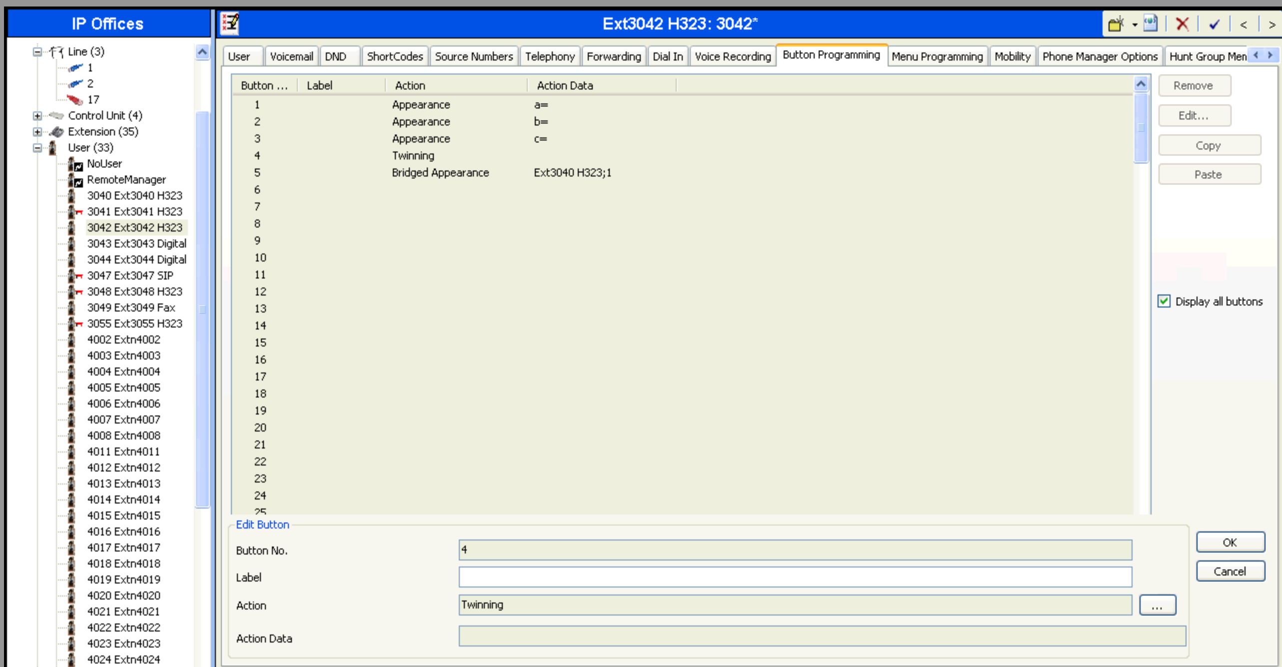


Select the **Mobility** tab. In the sample configuration user 3042 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for User 3042. The **Mobility Features** and **Mobile Twinning** boxes are checked**.** The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned telephone, in this case **919191111234**. Other options can be set according to customer requirements.



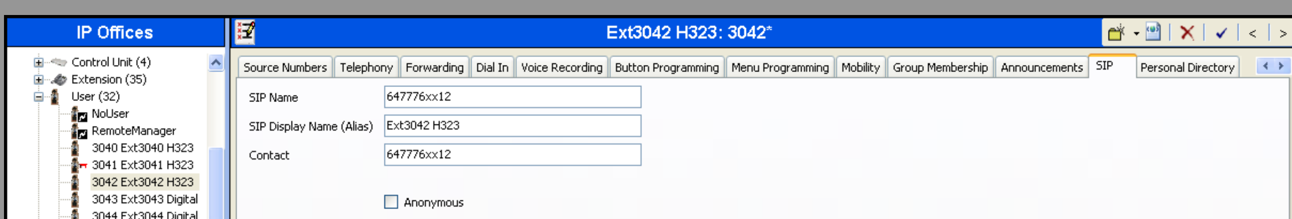
©2014 Avaya Inc. All Rights Reserved.

To program a key on the telephone to turn Mobil Twinning on and off, select the **Button Programming** tab on the user, then select the button to program to turn Mobil Twinning on and off, click on **Edit → Emulation → Twinning**. In the sample below, button **4** was programmed to turn Mobil Twinning on and off on user 3042.



Select the **SIP** tab, the values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls. In addition, these settings are used to match against the SIP URI of incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.7**). The example below shows the settings for user "Ext3042 H323". The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by MTS Allstream. In the example, DID number **647776xx12** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

If all calls involving this user should be considered private, then the **Anonymous** box may be checked to withhold the Caller ID information from the network.



©2014 Avaya Inc. All Rights Reserved.

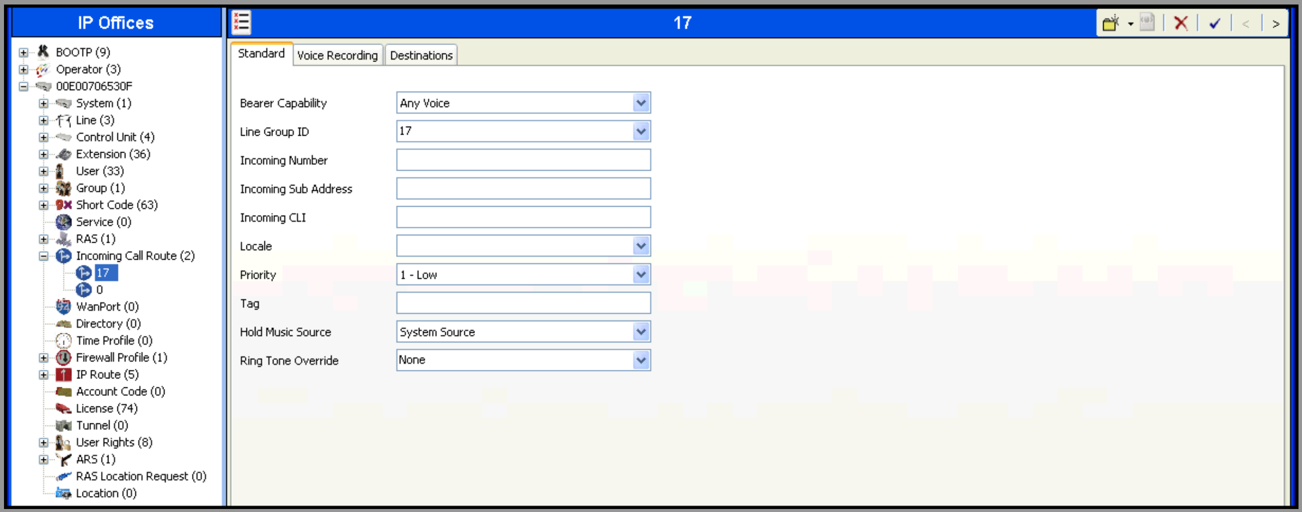
5.10 Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc, within the IP Office system. Incoming call routes should be defined for each DID number assigned by the service provider.

In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** and **SIP URI (Section 5.7)** and the users **SIP Name** and **Contact**, already populated with the assigned MTS Allstream DID numbers **(Section 5.9)**

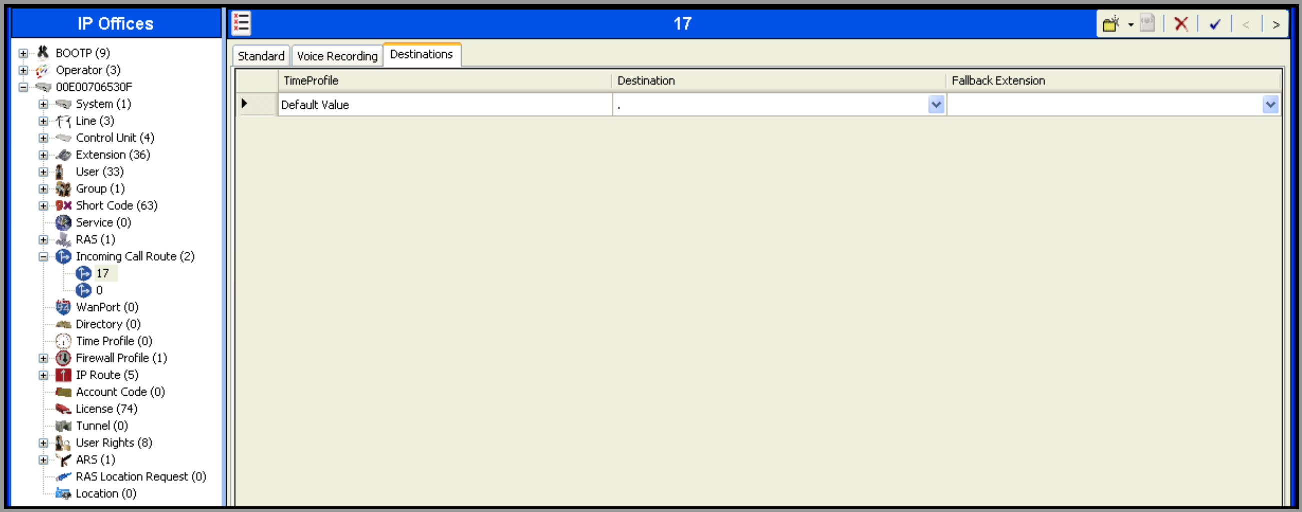
From the left Navigation Pane, right-click on **Incoming Call Route** and select **New.**
On the Details Pane (not shown), under the **Standard** tab, set the parameters as show bellow:

- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.7**.
- Default values may be used for all other parameters.



©2014 Avaya Inc. All Rights Reserved.

- Under the **Destinations** tab, enter "**.**" for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User,** which matches the number present on the user part of the incoming Request URI.
- Click OK to commit (not shown).



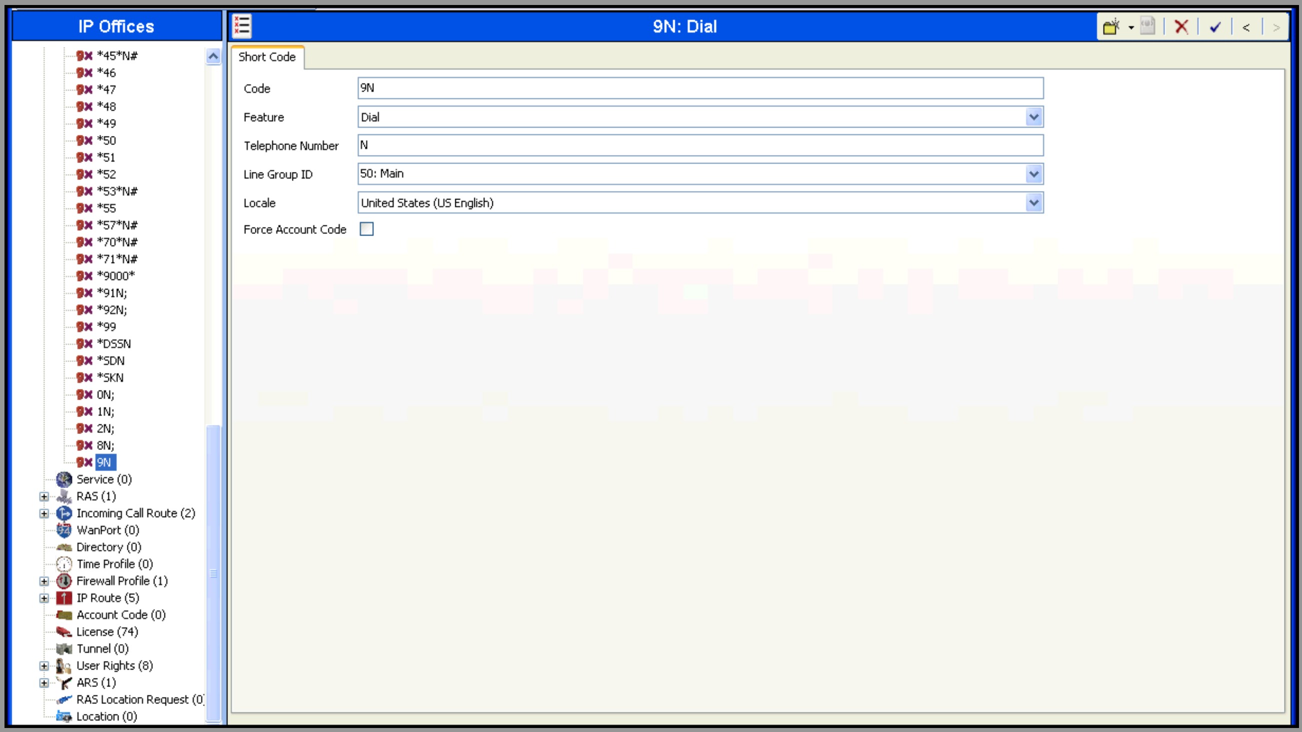
©2014 Avaya Inc. All Rights Reserved.

5.11 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.

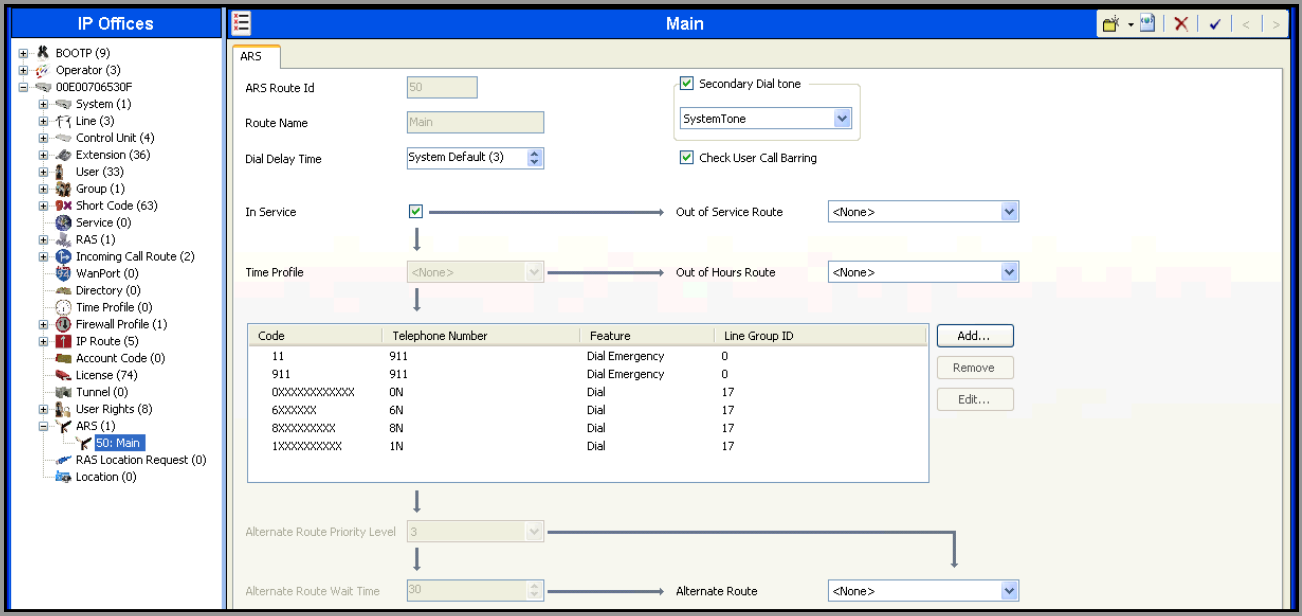
5.11.1 Short Codes and Automatic Route Selection

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 Avaya 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.



©2014 Avaya Inc. All Rights Reserved.

The following screen shows the example 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 digit on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office. The example below shows that for calls to area codes in the North American Numbering Plan, the user dialed 9, followed by 11 digits, starting with a 1.

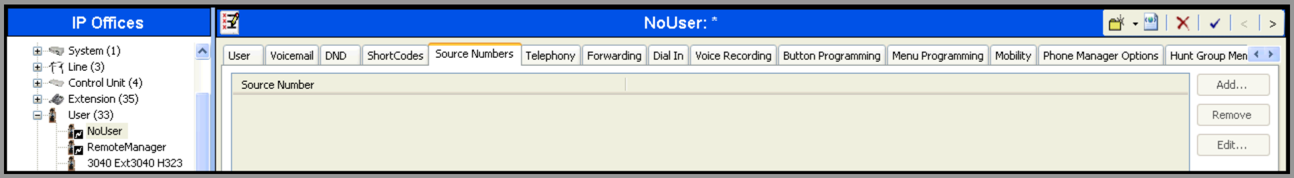


©2014 Avaya Inc. All Rights Reserved.

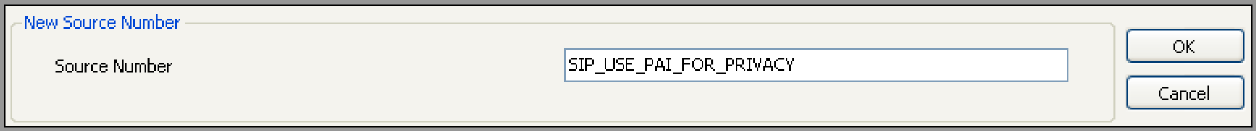
5.12 Privacy/Anonymous Calls

For outbound calls with privacy (anonymous) enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with “restricted” and “anonymous” respectively. Avaya IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity (PAI) header to pass the actual calling party information for authentication and billing. By default, Avaya IP Office will use PPI for privacy. For the compliance test, PAI was used for the purposes of privacy.

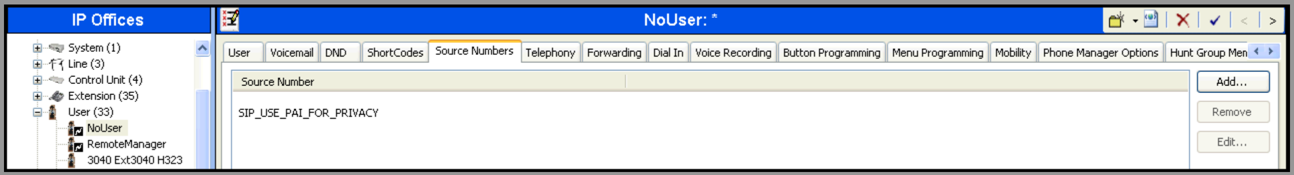
To configure Avaya IP Office to use PAI for privacy calls, navigate to **User → NoUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP_USE_PAI_FOR_PRIVACY**. Click **OK**.



The **SIP_USE_PAI_FOR_PRIVACY** parameter will appear in the list of Source Numbers as shown below.



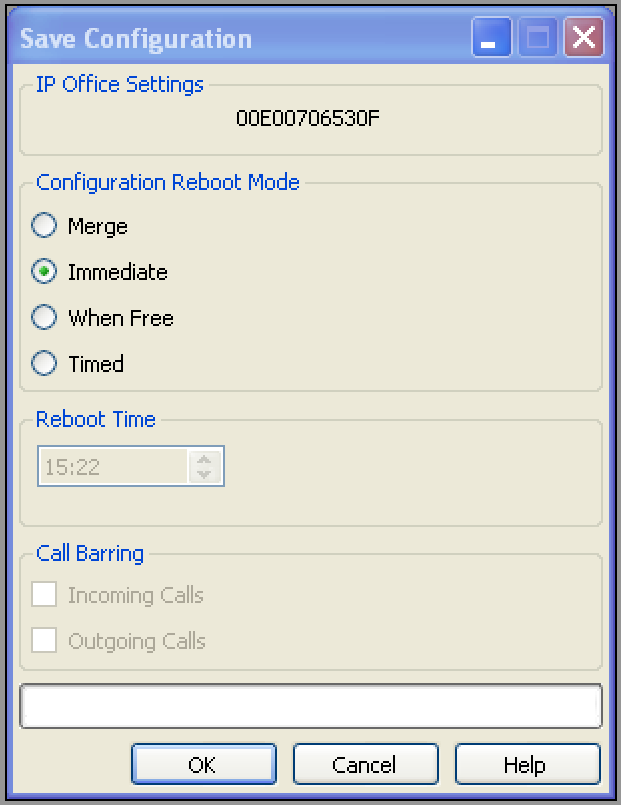
©2014 Avaya Inc. All Rights Reserved.

5.13 Save Configuration

When desired, send the configuration changes made in Avaya IP Office Manager to the Avaya IP Office server in order for the changes to take effect.

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

Once the configuration is validated, a screen similar to the following will appear, with either the **Merge** or the **Immediate** radio button chosen based on the nature of the configuration changes made since the last save. Note that clicking OK may cause a service disruption due to system reboot. Click OK if desired.



©2014 Avaya Inc. All Rights Reserved.

6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For additional information on these configuration tasks, see **References Error! Reference source not found.**, **Error! Reference source not found.** and Error! Reference source not found. in **Section 10**.

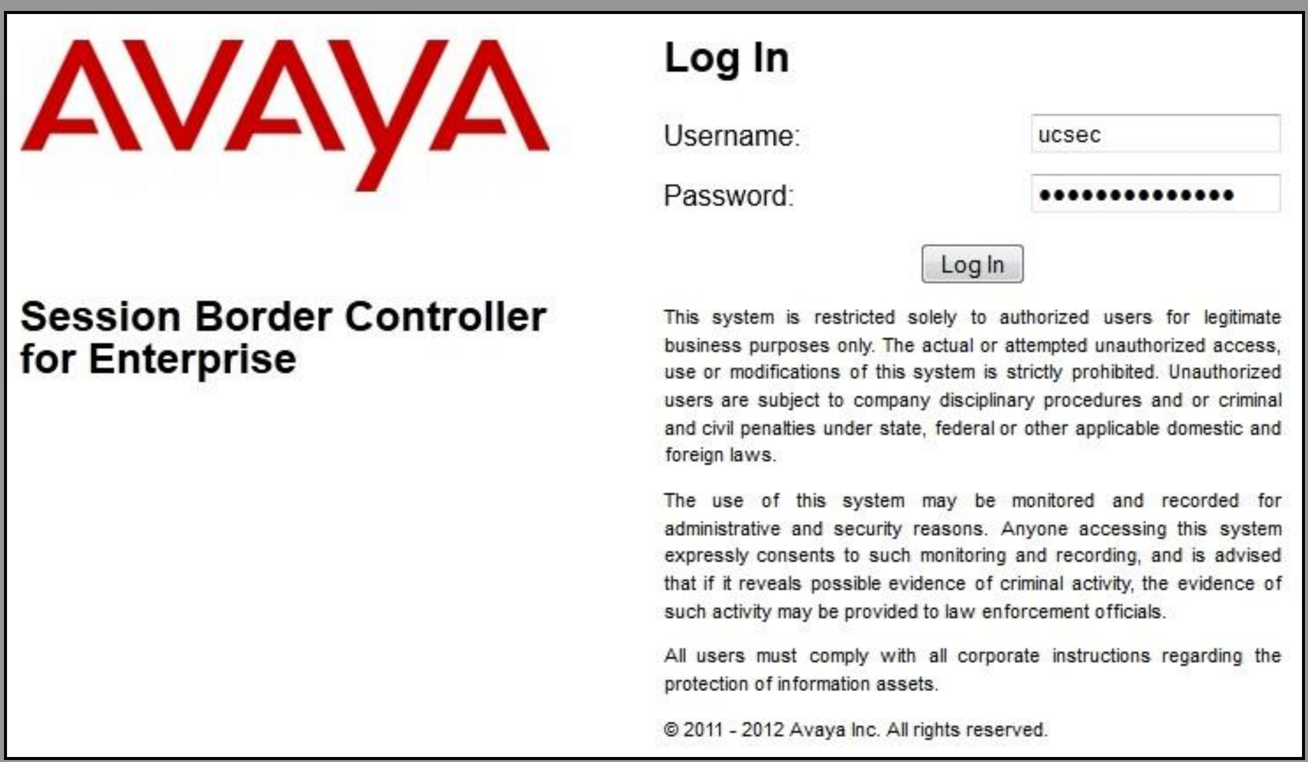
The configuration of the Avaya SBCE covers two major components, the Trunk Server for the service provider and Call Server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration was defined using the Avaya SBCE web user interface as described in the following sections.

Note: During the next pages and for brevity in these Application Notes not every provisioning step will have a screenshot associated with it.

6.1 Log into the Avaya Session Border Controller for Enterprise

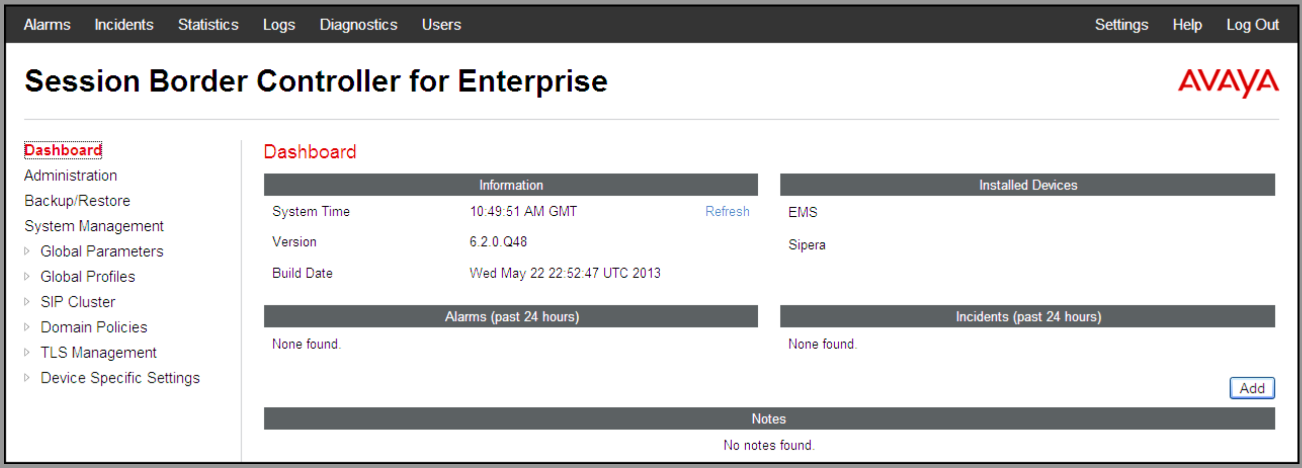
Use a Web browser to access the Avaya SBCE Web interface, enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the management IP address.

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

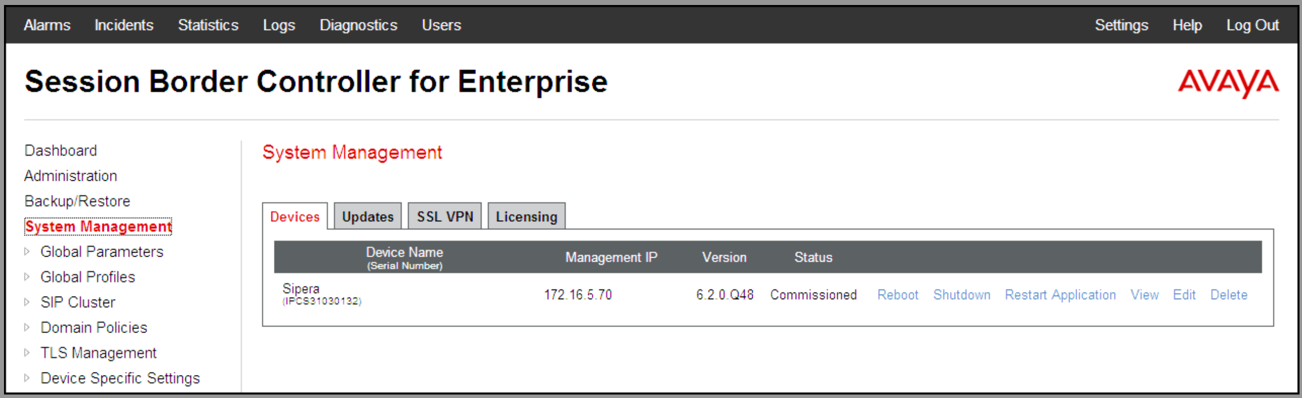


©2014 Avaya Inc. All Rights Reserved.

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



To view the system information that has been 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 **Sipera** was already added. To view the configuration of this device, click the **View** as shown in the screenshot below.

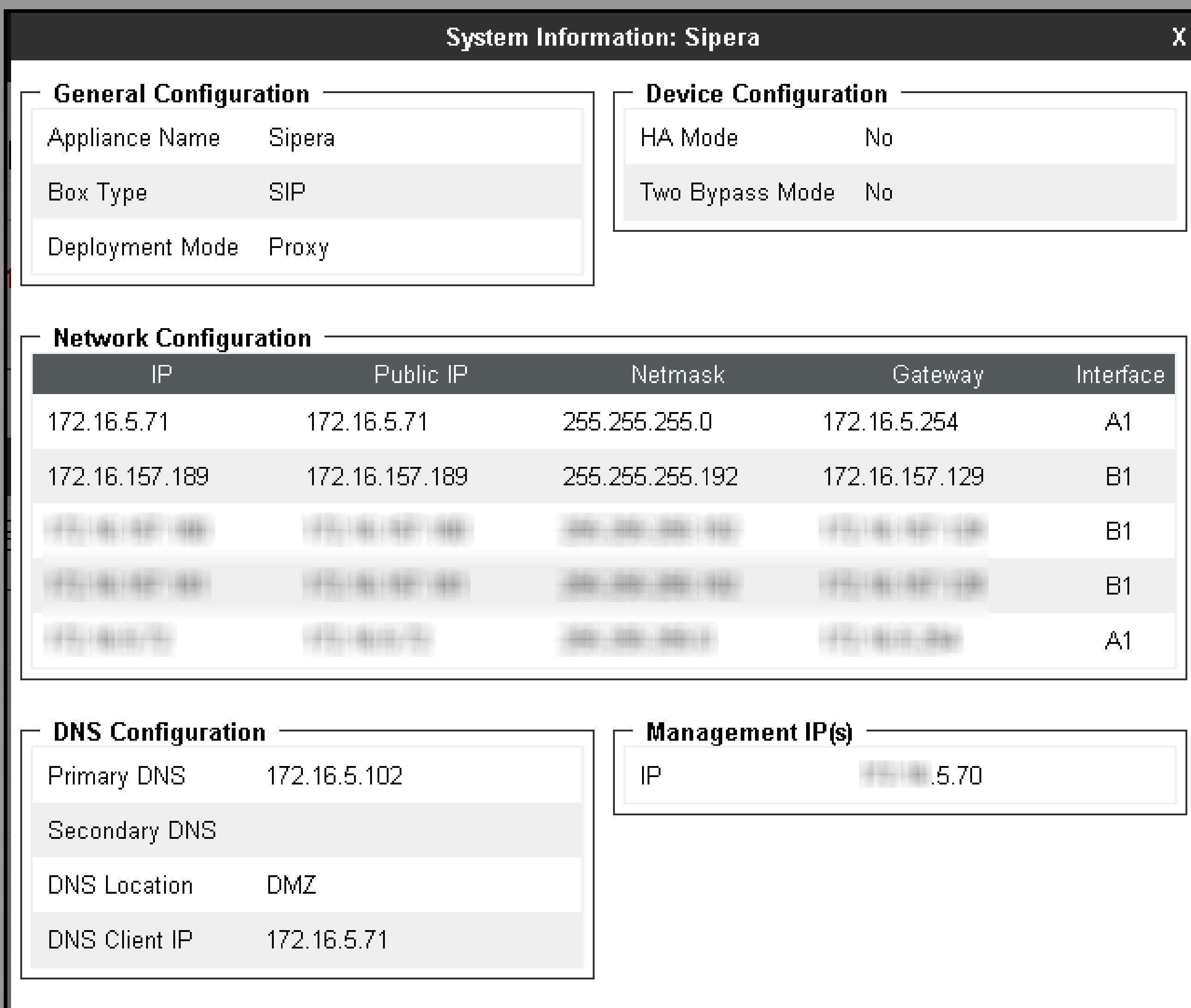


©2014 Avaya Inc. All Rights Reserved.

The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponded 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.

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.

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



©2014 Avaya Inc. All Rights Reserved.

On the previous screen, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces for the Avaya SBCE. The **A1** and **B1** interfaces and IP addresses shown are the ones relevant to the configuration of the SIP trunk to MTS Allstream. Other IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document, these IPs have been blurred out.

6.2 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the UC-Sec control Center.

6.2.1 Server Interworking profile - 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 modifying a default profile is generally not recommended, for the Avaya-IPO interworking profile the default **avaya-ru** profile was duplicated, or “cloned”, and then modified to meet specific requirements for the enterprise SIP-enabled solution.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru.** Click **Clone Profile.**

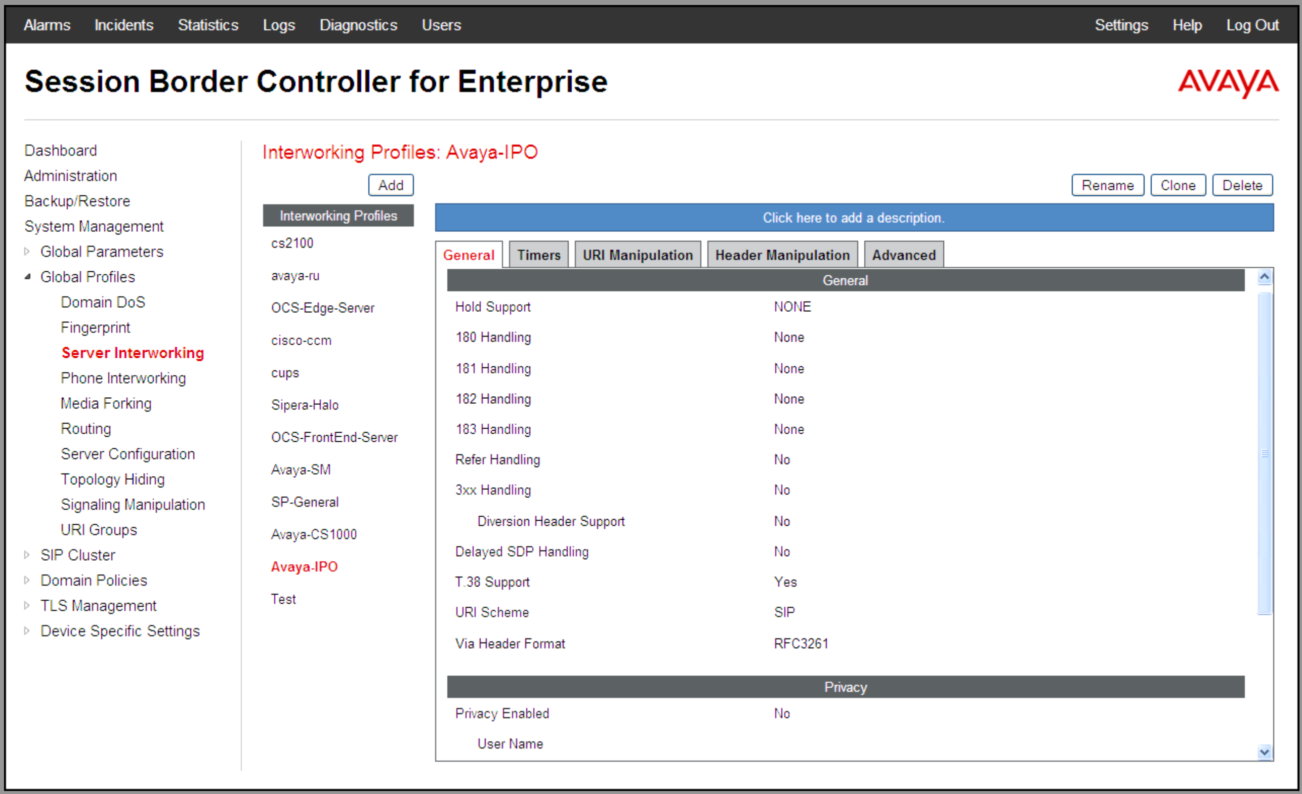
Enter the new profile name in the **Clone Name** field, the name of **Avaya-IPO** was chosen in this example. Click **Finish**.

For the newly created **Avaya-IPO** profile, click **Edit** at the bottom of the General tab.

- Check **T.38 Support**
- Click **Next**.
- Click **Finish** on the **Privacy** tab.
- Leave other fields with their default values.

©2014 Avaya Inc. All Rights Reserved.

The following screen capture shows the newly added **Avaya-IPO** Profile.



©2014 Avaya Inc. All Rights Reserved.

6.2.2 Server Interworking profile – SP General

A second Server Interworking profile named **SP General** was created for the Service Provider, note that the **Add** button was used to add this profile.

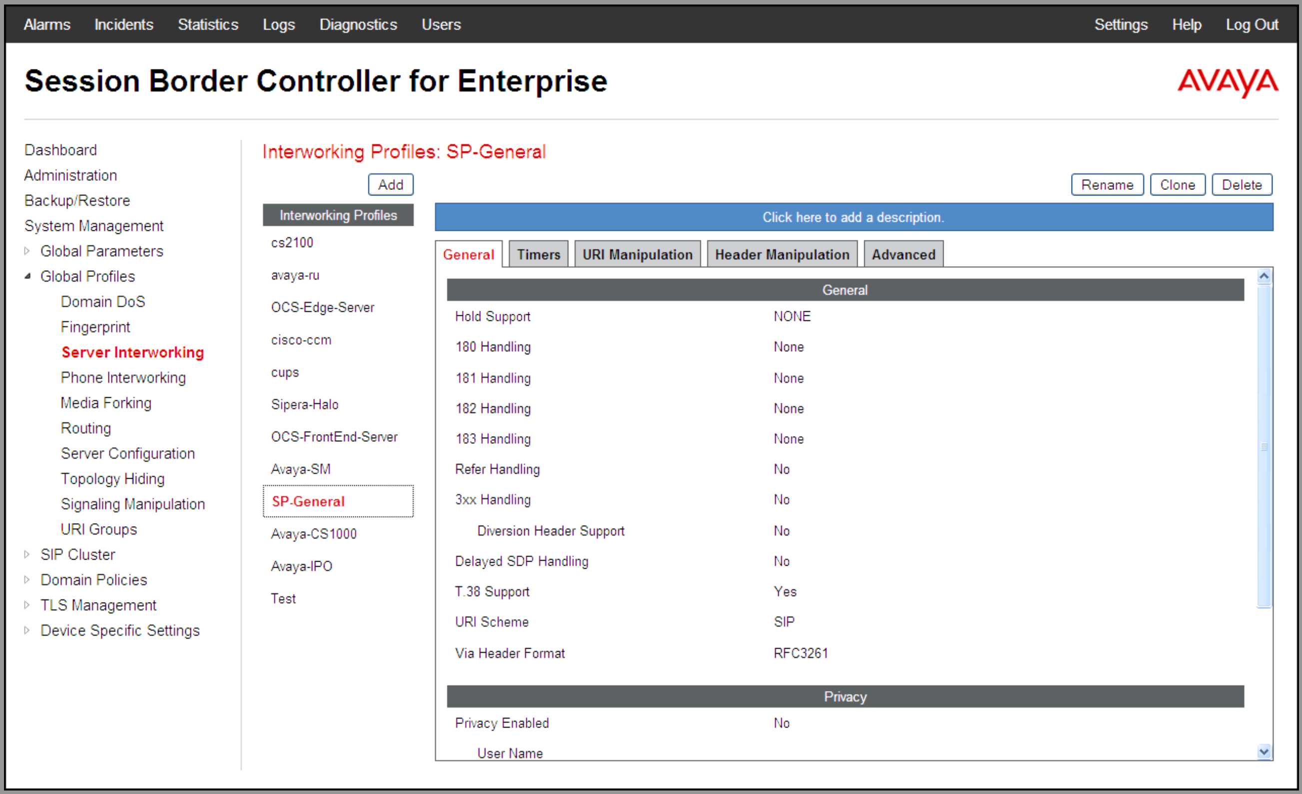
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add.**

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.**

For the newly created **SP General** profile, click **Edit** at the bottom of the General tab.

- Check **T.38 Support**
- Click **Next**.
- Click **Finish** on the **Privacy** tab.
- Leave other fields with their default values

The following screen capture shows the newly added **SP General** Profile.



©2014 Avaya Inc. All Rights Reserved.

6.2.3 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 in the test configuration, 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.

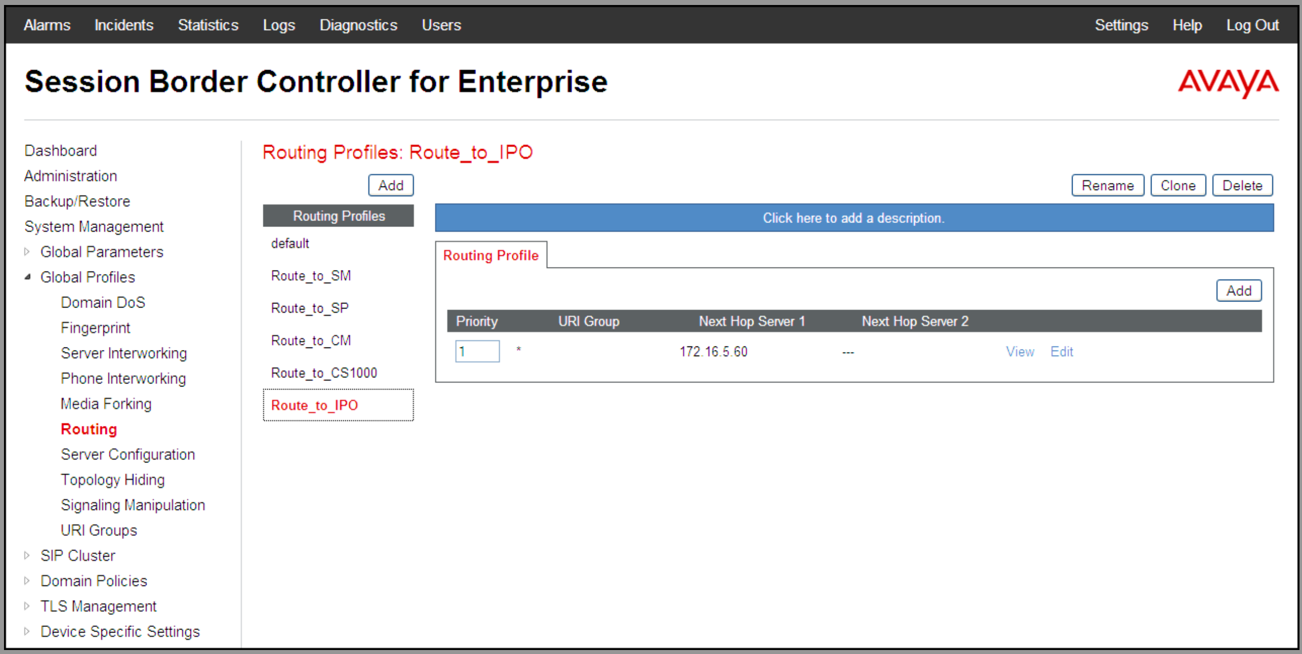
To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select the **Routing** tab.
- Select **Add.**
- Enter Profile Name: **Route_to_IPO**.
- Click **Next.**

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.60** (IP Office IP address).
- Check **Routing Priority Based on Next Hop Server**.
- Check **Outgoing Transport: UDP**.
- Click **Finish.**

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

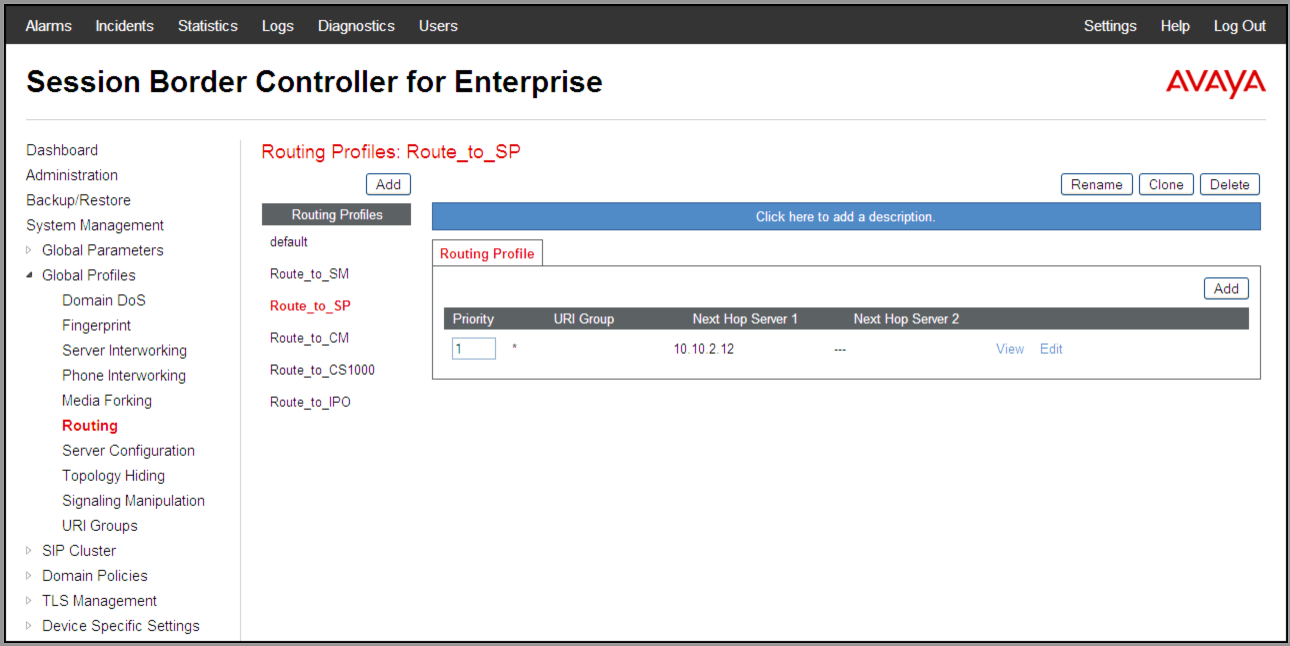


©2014 Avaya Inc. All Rights Reserved.

Similarly, for the outbound route:

- Select **Add.**
- Enter Profile Name: **Route to SP**.
- Click **Next**.
- **Next Hop Server 1: 10.10.2.12** (IP address for Service Provider's SIP Proxy)
- Check **Routing Priority Based on Next Hop Server**.
- Check **Outgoing Transport: UDP**.
- Click **Finish.**

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



©2014 Avaya Inc. All Rights Reserved.

6.2.4 Server Configuration

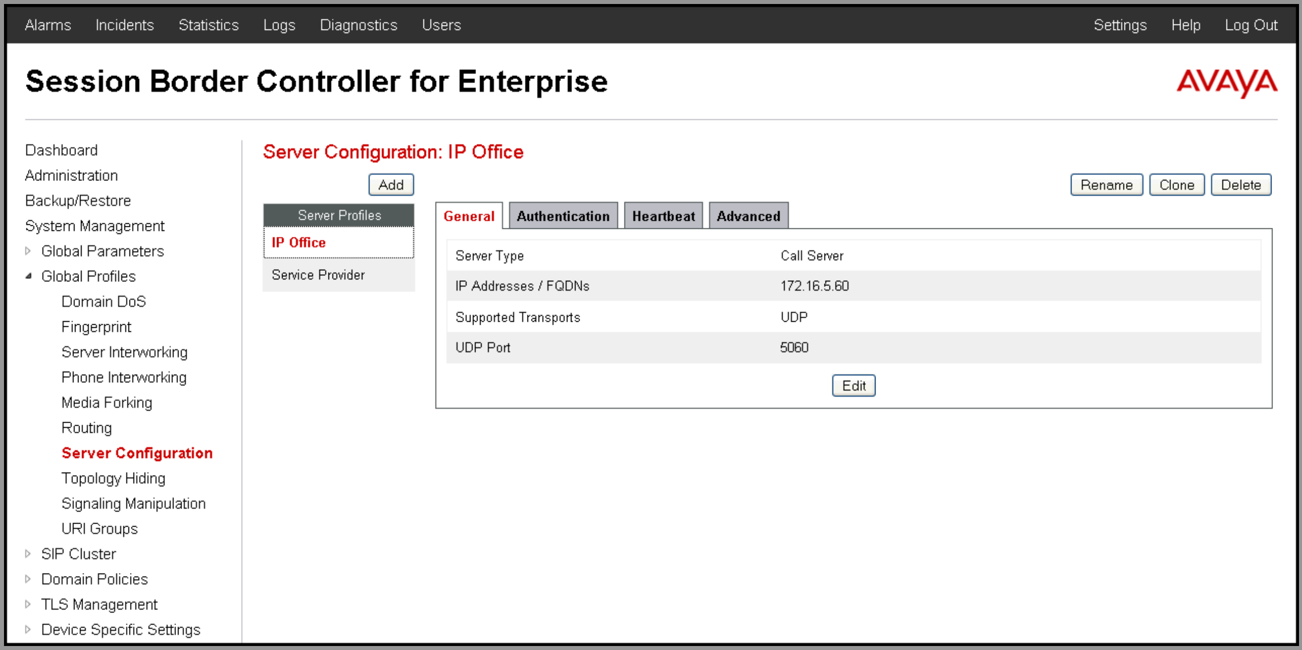
Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (IP Office) and the Trunk Server or SIP Proxy at the service provider's network.

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

On the **Add Server Configuration Profile** Tab:

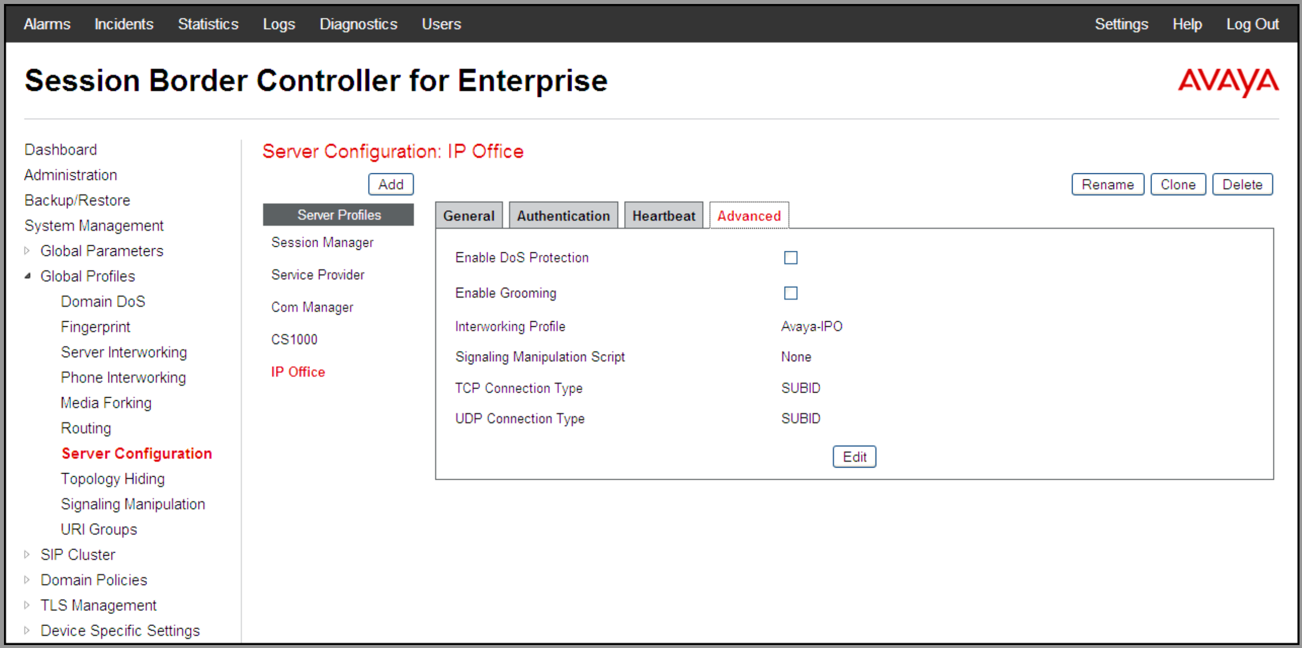
- Select Server Type**: Call Server.**
- **IP Address: 172.16.5.60** (IP Address of IP Office).
- **Supported Transports**: Check **UDP**.
- **TCP Port: 5060.**
- Click **Next.**
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **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 added **IP Office** Profile.



©2014 Avaya Inc. All Rights Reserved.

The following screen capture shows the **Advanced** tab of the added **IP Office** Profile.



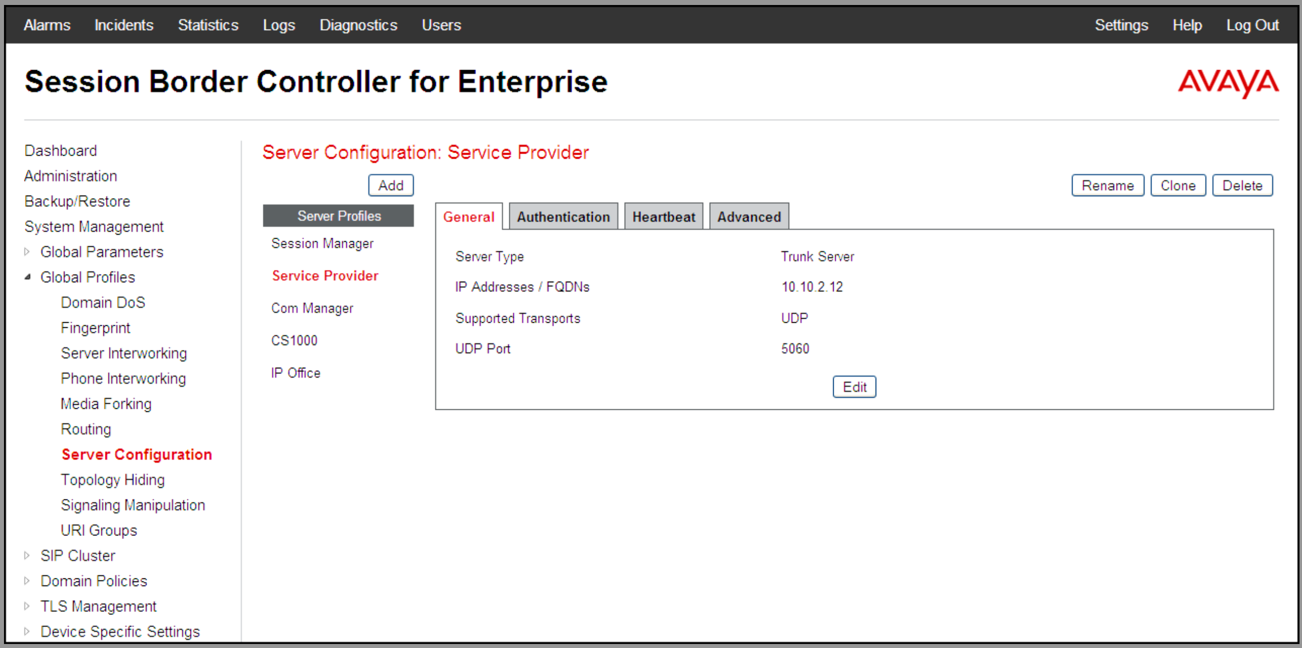
To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** and enter the profile name: **Service Provider.**

On the **Add Server Configuration Profile** Tab:

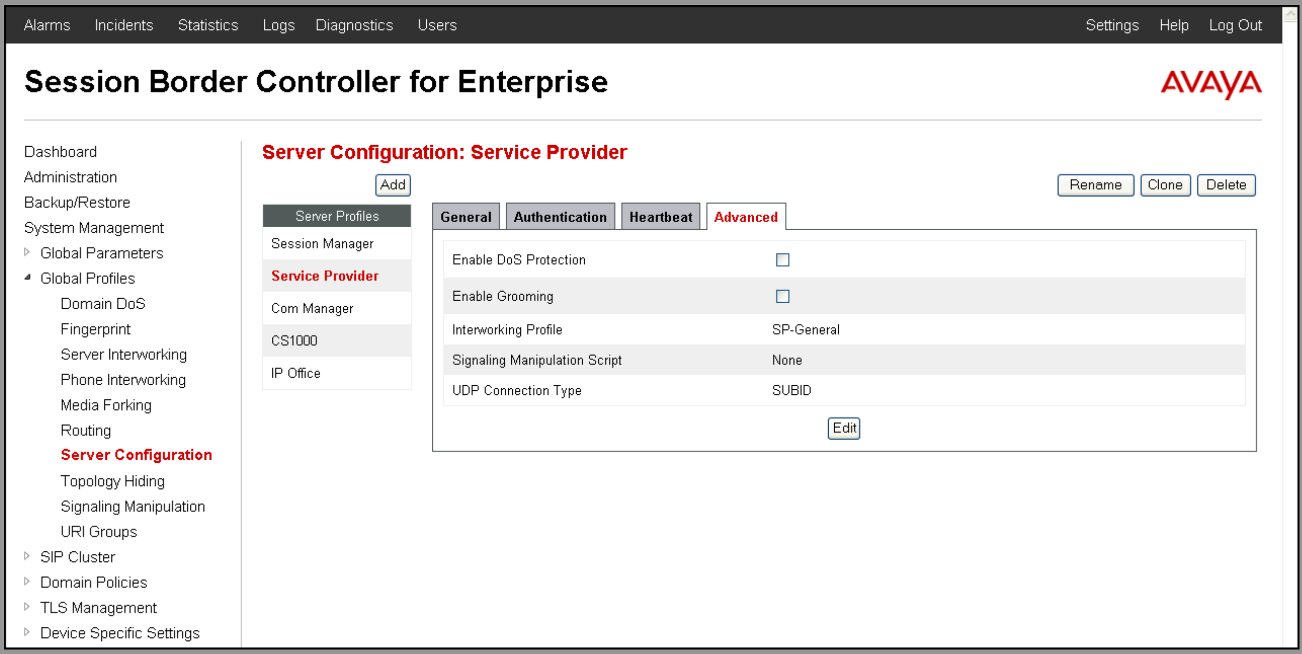
- Select Server Type**: Trunk Server.**
- **IP Address: 10.10.2.12** (IP address for Service Provider's SIP Proxy).
- **Supported Transports**: Check **UDP**.
- **UDP Port: 5060.**
- Click **Next.**
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **SP General** from the **Interworking Profile** drop down menu. Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish.**

©2014 Avaya Inc. All Rights Reserved.

The following screen capture shows the **General** tab of the **Service Provider** Profile.



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



©2014 Avaya Inc. All Rights Reserved.

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.

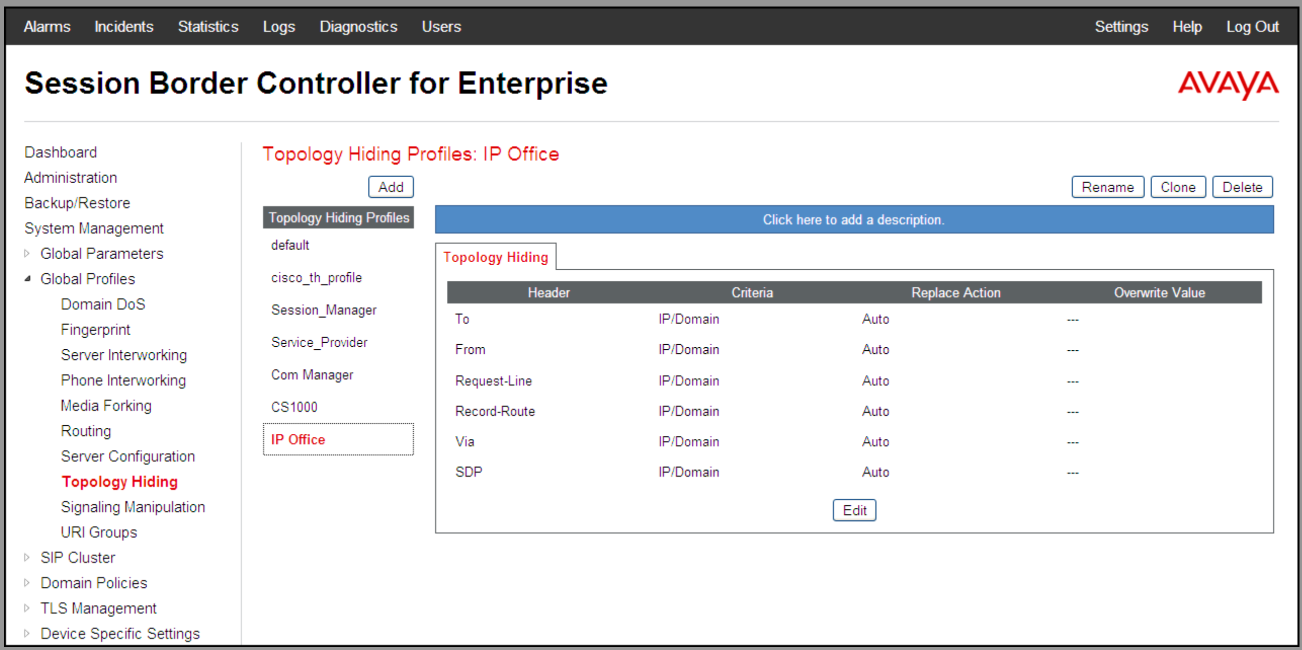
Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

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 no values were overwritten (default).

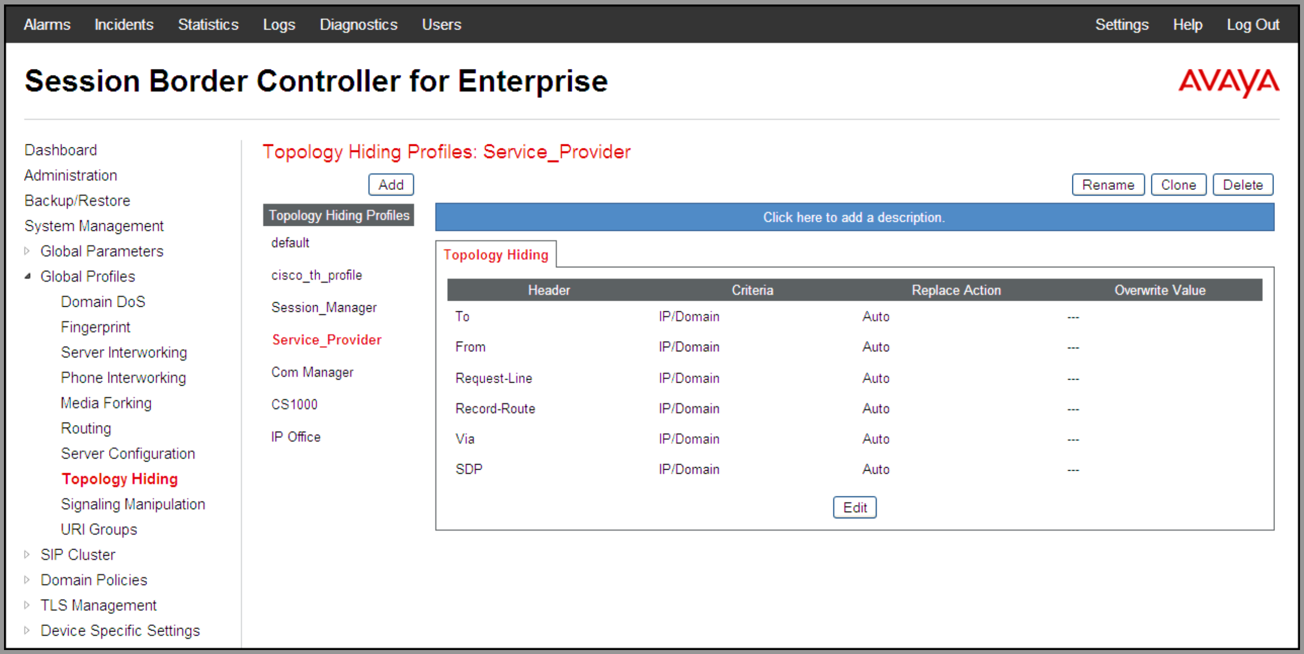


©2014 Avaya Inc. All Rights Reserved.

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 no values were overwritten (default).



©2014 Avaya Inc. All Rights Reserved.

6.2.6 Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows performing a granular header manipulation on the headers in the SIP messages, which sometimes is not possible by direct configuration on the web interface. The ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

Signaling Manipulation was not necessary and was not used during the compliance testing.

6.3 Domain Policies

Domain Policies allow the configuration of 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. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, only a new Application Rule was defined. All other rules under Domain Policies, linked together on End Point Policy Groups, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

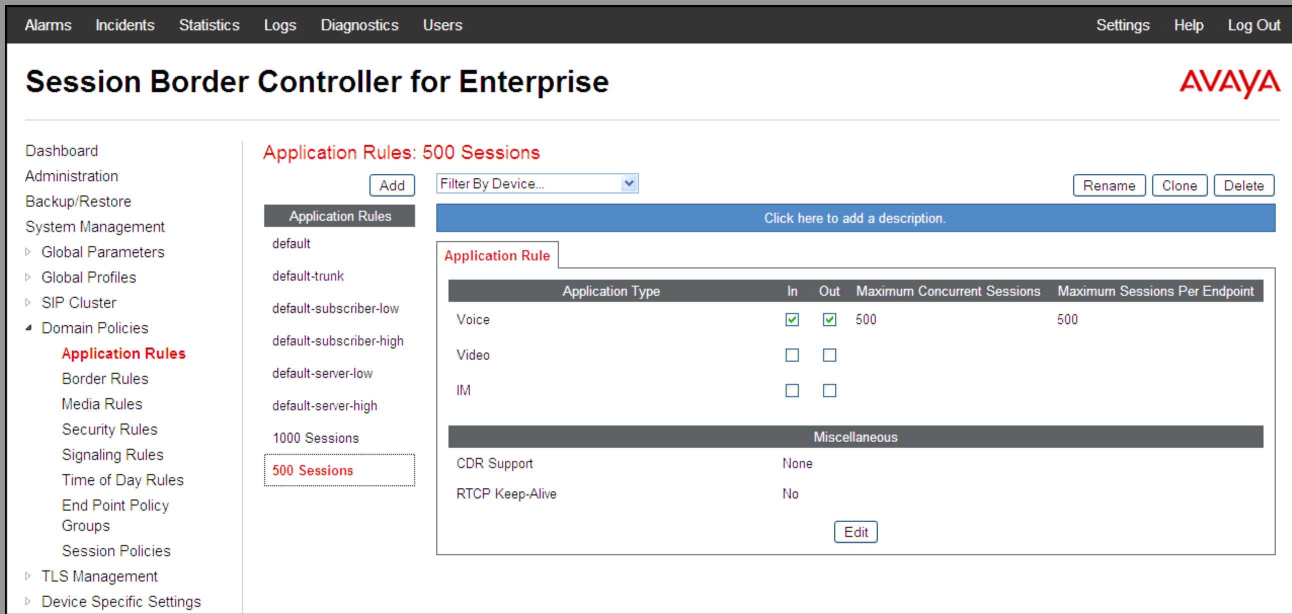
6.3.1 Create Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device 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.

To add a new Application Rule, from the menu on the left-hand side, select **Domain Policies → Application Rules.**

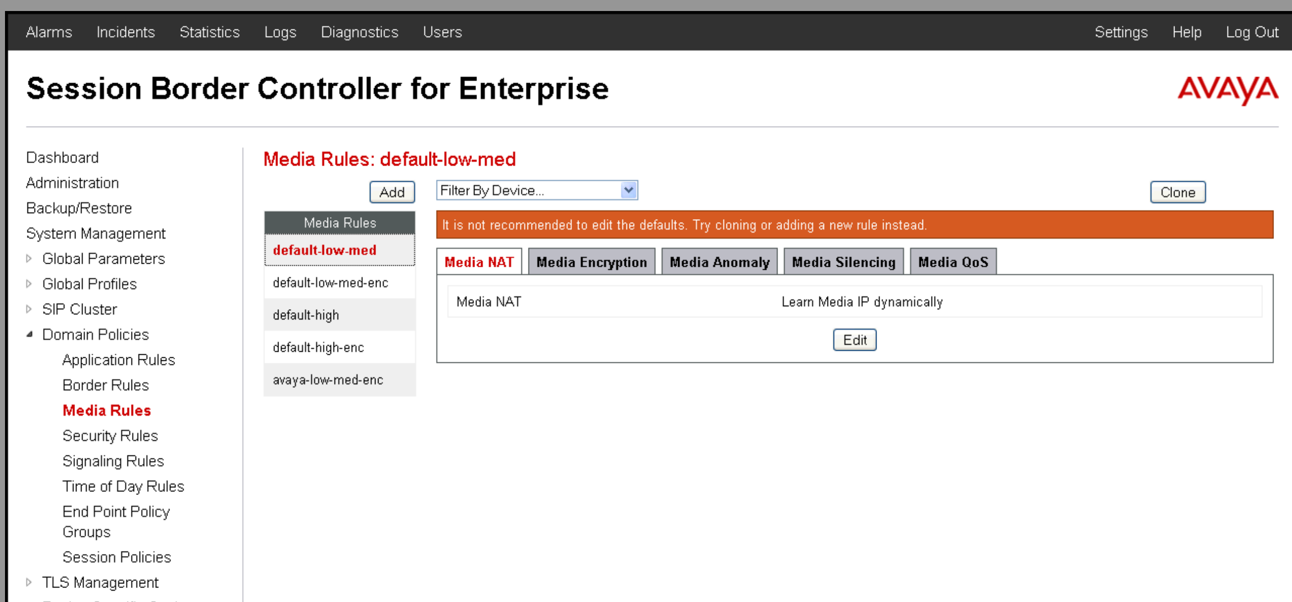
- Select **default trunk** Rule.
- Select **Clone Rule** button.
- Enter the **Application Rule** Name**: 500 Sessions**
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **500** was used in the sample configuration.
- Click Finish.

©2014 Avaya Inc. All Rights Reserved.



6.3.2 Media Rules

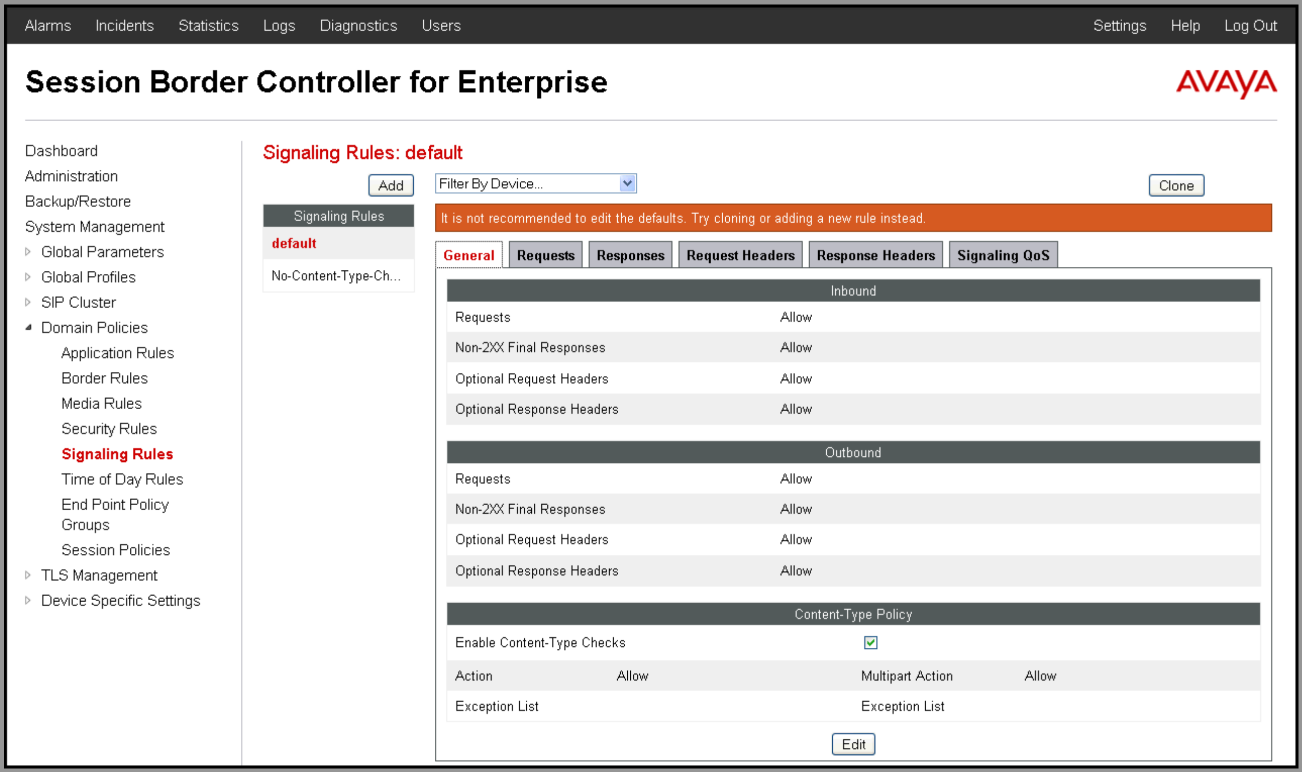
For the compliance test, the existing **default-low-med** Media Rule was used.



©2014 Avaya Inc. All Rights Reserved.

6.3.3 Signaling Rules

For the compliance test, the existing **default** Signaling Rule was used.



©2014 Avaya Inc. All Rights Reserved.

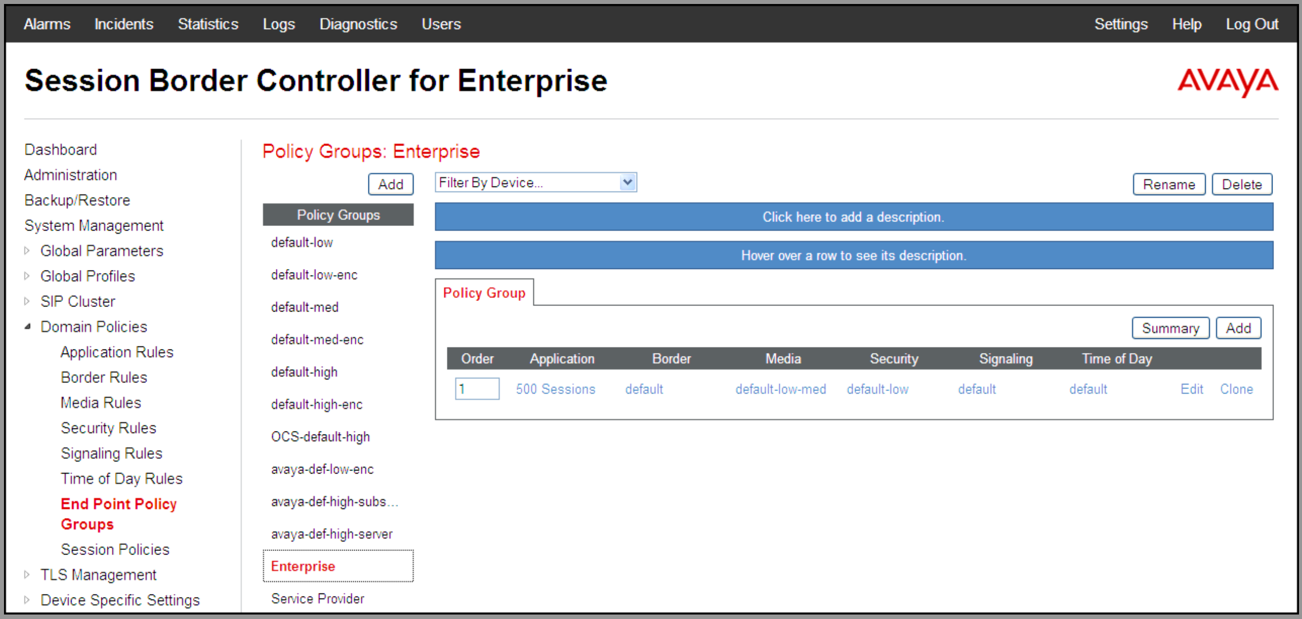
6.3.4 End Point Policy Groups

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**.

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

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

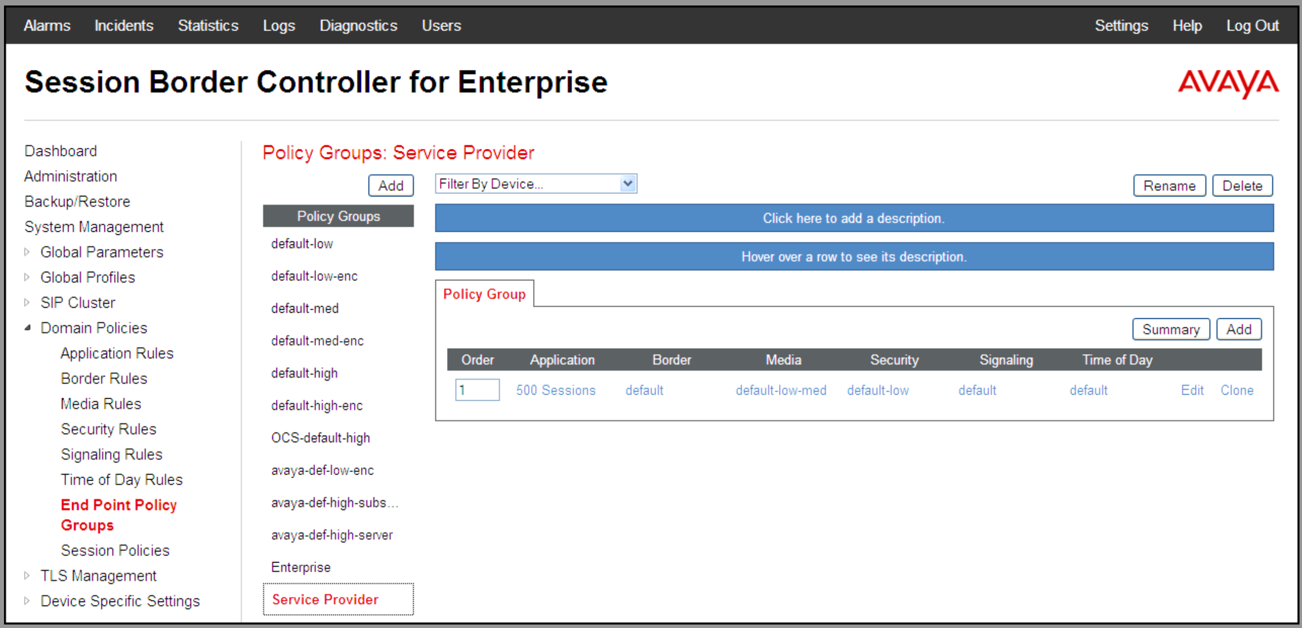


©2014 Avaya Inc. All Rights Reserved.

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

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

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



©2014 Avaya Inc. All Rights Reserved.

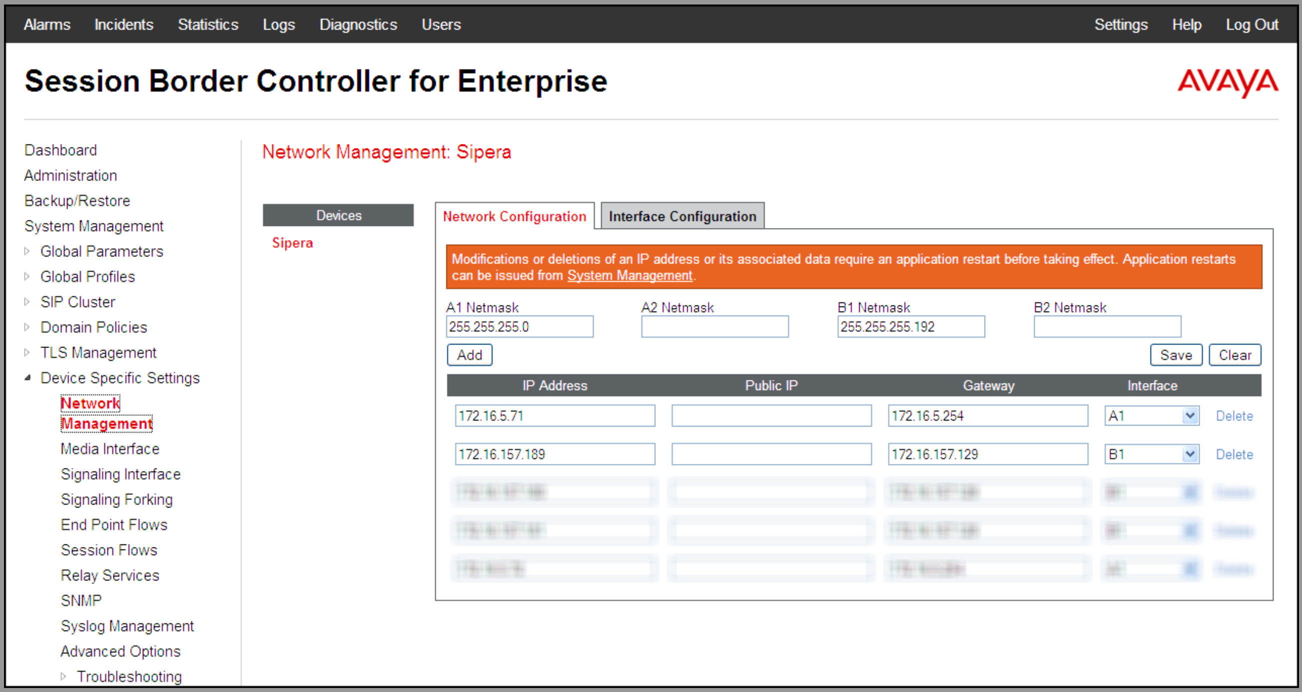
6.4 Device Specific Settings

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

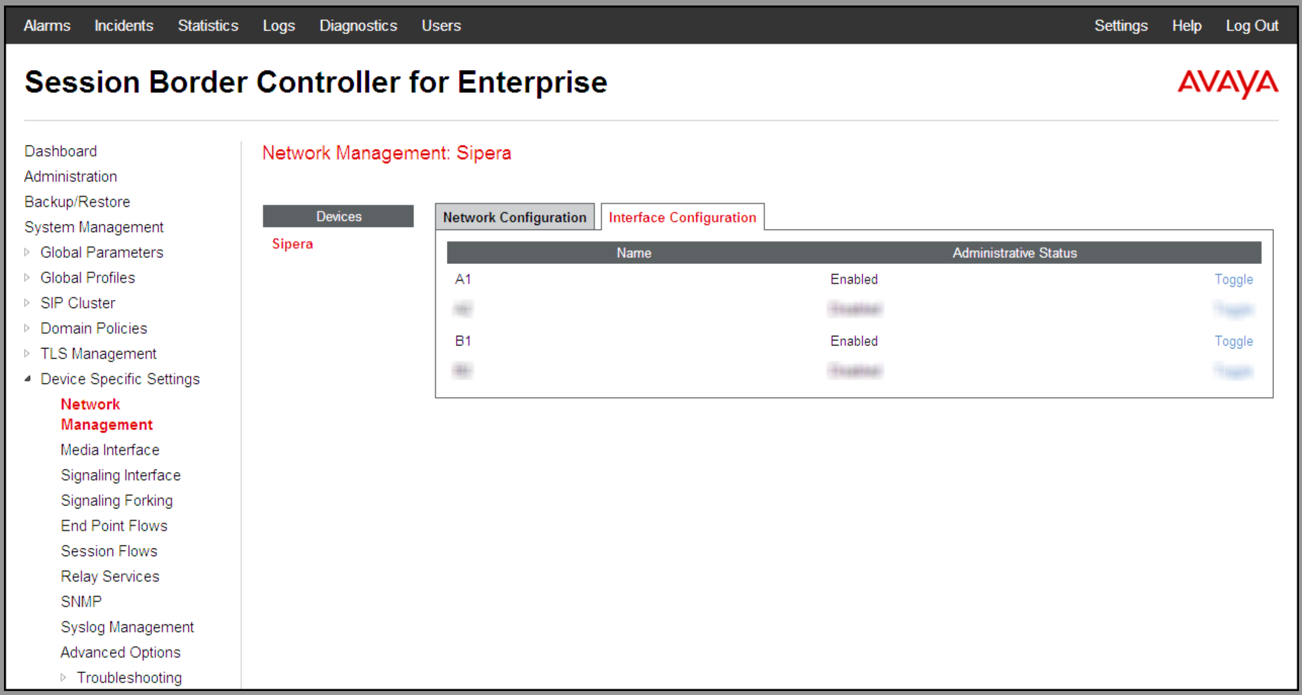
The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** menu on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

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



©2014 Avaya Inc. All Rights Reserved.

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.



©2014 Avaya Inc. All Rights Reserved.

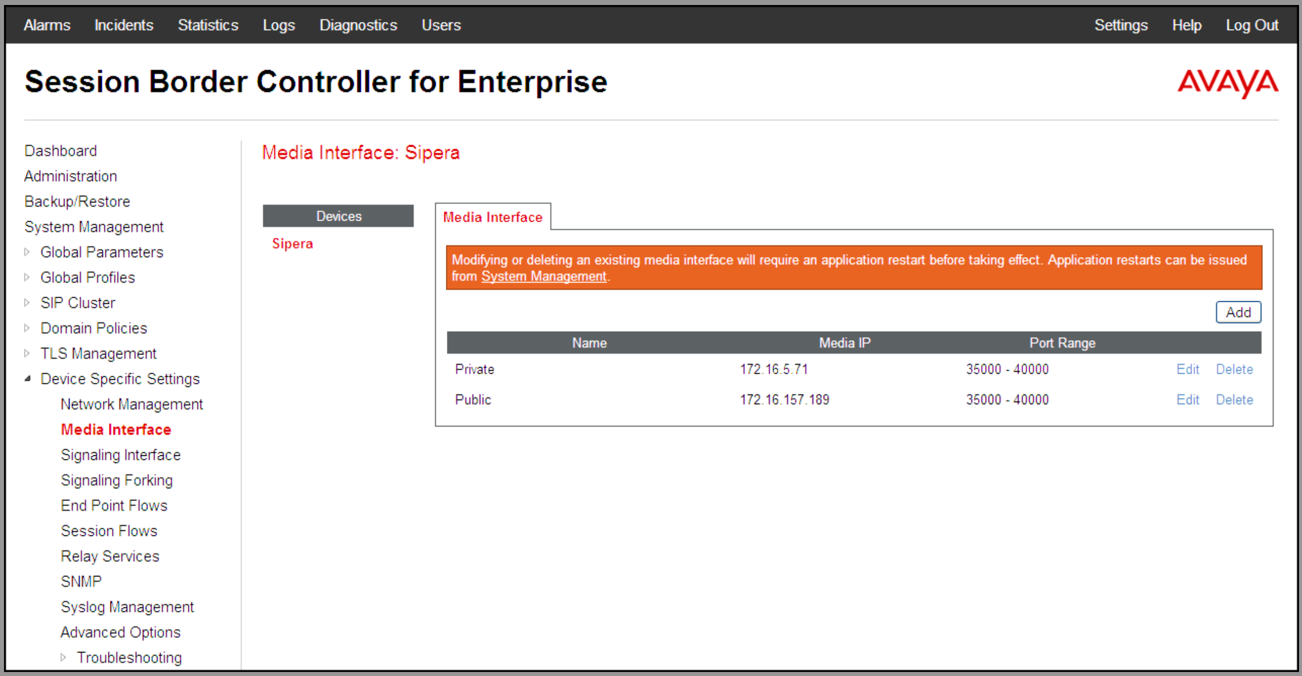
6.4.2 Media Interface

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 ports range 35000 to 40000 was used.

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

- Select **Add.**
- **Name: Private**.
- 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 Media Interface.**
- **Name: Public.**
- Select **IP Address: 172.16.157.189** (Outside IP Address of the Avaya SBCE, toward Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish.**

The following screen capture shows the added **Media Interfaces**.



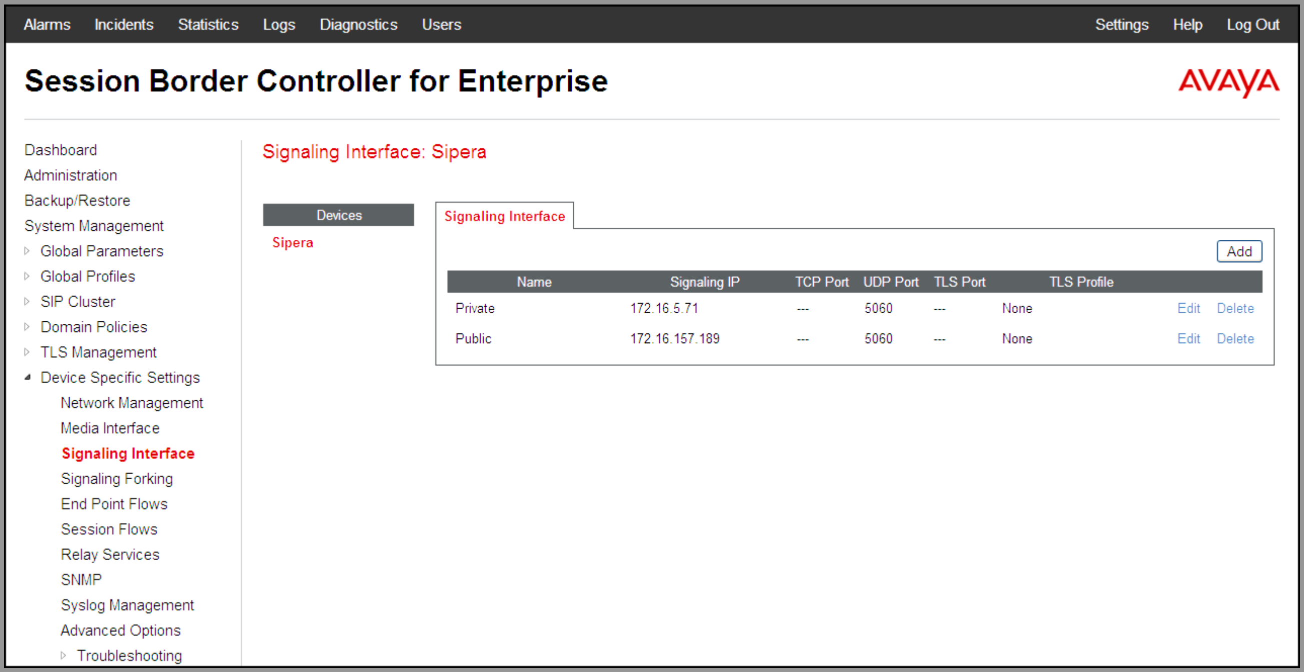
©2014 Avaya Inc. All Rights Reserved.

6.4.3 Signaling Interface

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

- Select **Add Signaling Interface**:
- **Name: Private.**
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port: 5060.**
- Click **Finish.**
- Select **Add Signaling Interface**:
- **Name: Public**
- Select **IP Address: 172.16.157.189** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish.**

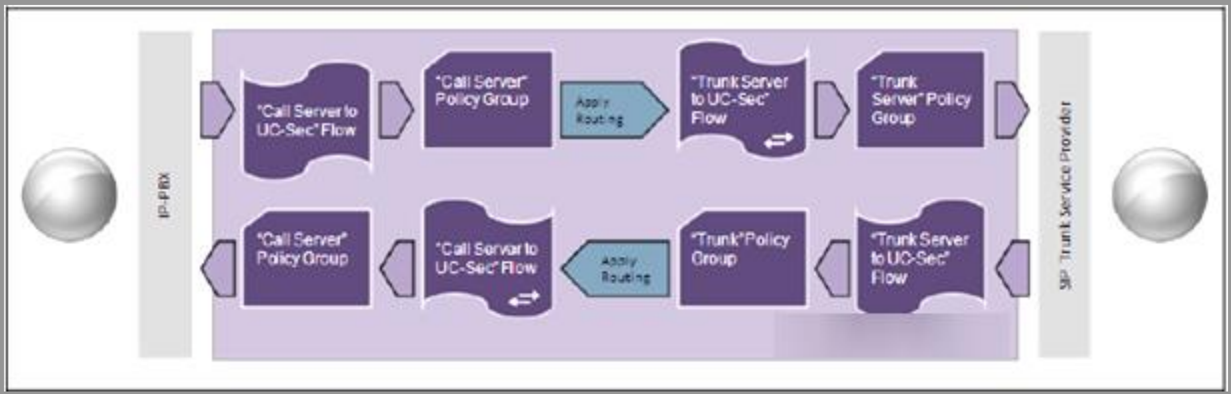
The following screen capture shows the newly added **Signaling Interfaces**.



©2014 Avaya Inc. All Rights Reserved.

6.4.4 End Point Flows

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

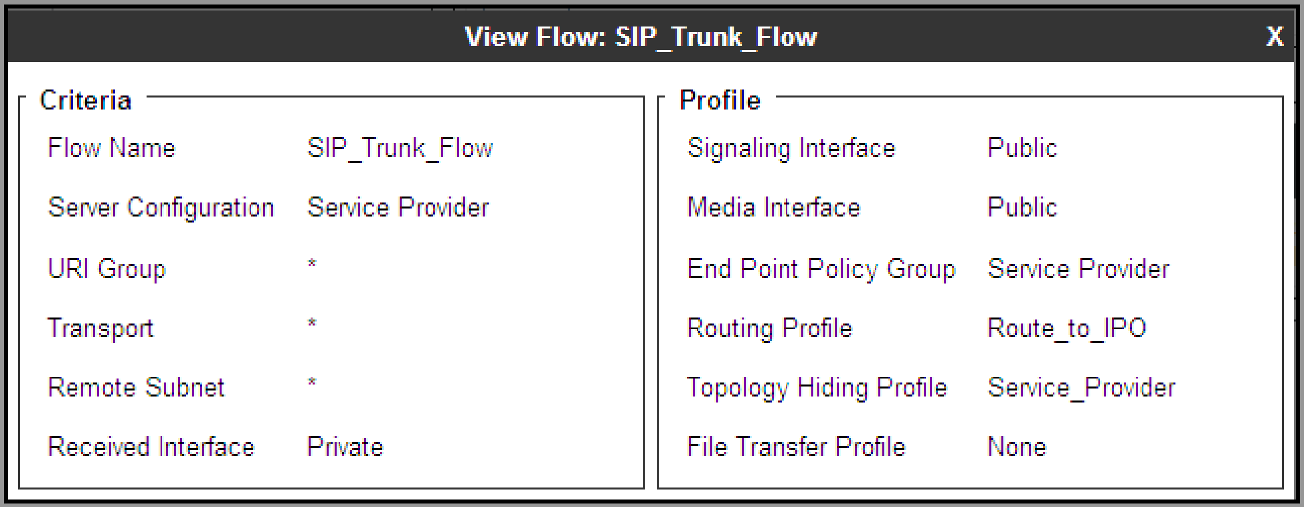


The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

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

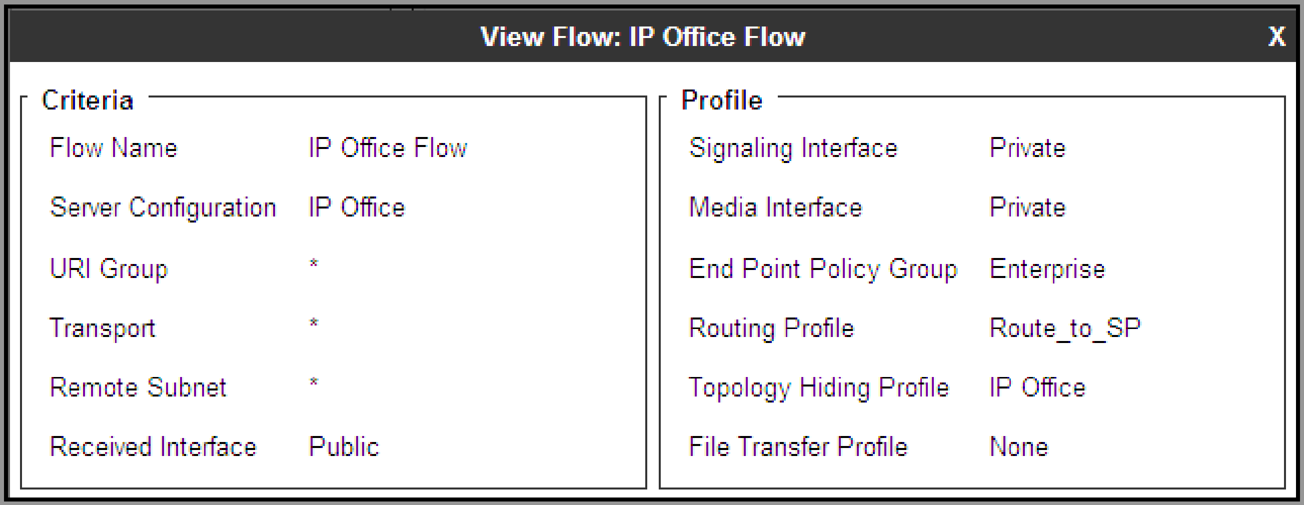
- **Name: SIP Trunk Flow.**
- **Server Configuration**: **Service Provider.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Private**
- **Signaling Interface: Public**
- **Media Interface**: **Public**
- **End Point Policy Group: Service Provider.**
- **Routing Profile: Route_to_IP_Office** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service_Provider.**
- **File Transfer Profile: None.**
- Click **Finish.**

©2014 Avaya Inc. All Rights Reserved.



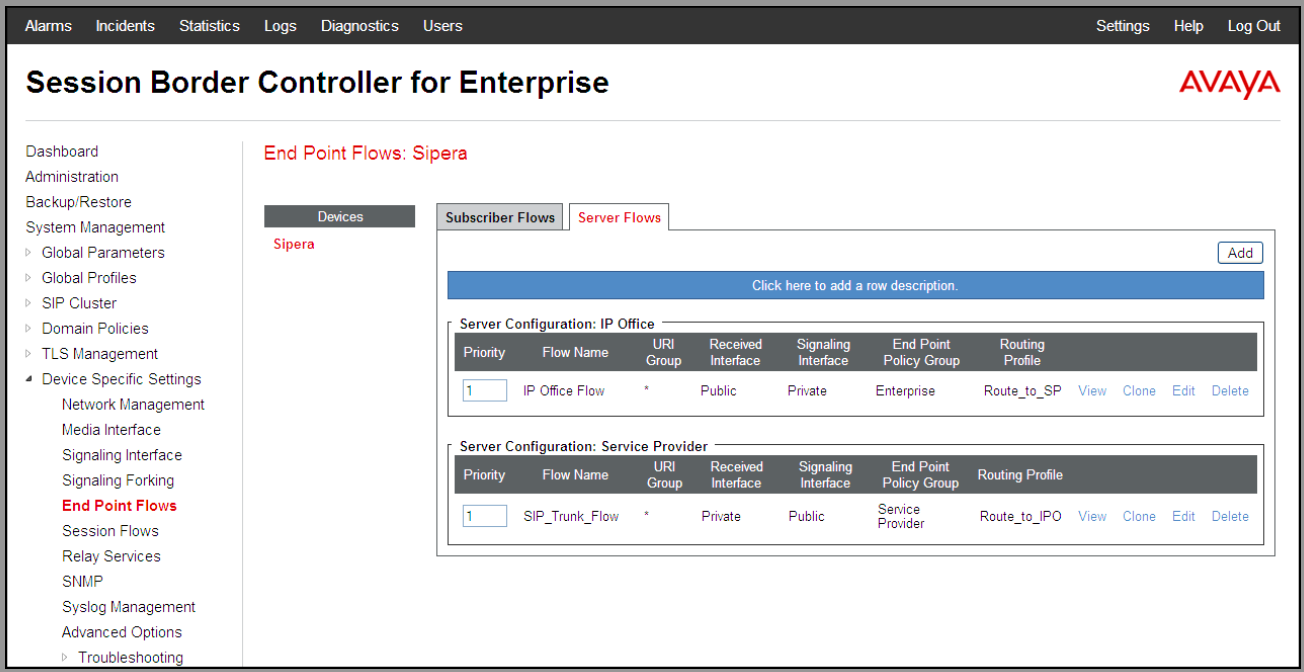
To create the call flow toward the IP Office, click **Add Flow**.

- **Name: IP Office Flow.**
- **Server Configuration**: **IP Office.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface**: **Public**
- **Signaling Interface: Private**
- **Media Interface**: **Private**
- **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.**
- Click **Finish.**



©2014 Avaya Inc. All Rights Reserved.

The following screen capture shows the added **End Point Flows.**



©2014 Avaya Inc. All Rights Reserved.

7. MTS Allstream SIP Trunking Configuration

MTS Allstream is responsible for the configuration of the SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. MTS Allstream will provide the customer the necessary information to configure the Avaya IP Office SIP trunk connection, including:

- IP address of the MTS Allstream SIP Proxy server.
- Supported codec's and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

©2014 Avaya Inc. All Rights Reserved.

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 PSTN and that calls remain active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from PSTN and that calls can remain active for more than 35 seconds.
- Verify that the user on the PSTN side can end an active call by hanging up.
- Verify that an Avaya endpoint at the enterprise site can end an active call by hanging up.

8.2 Protocol Traces

The following SIP message headers are inspected using sniffer trace analysis tool:

- Request-URI: Verify the request number and SIP domain.
- From: Verify the display name and display number.
- To: Verify the display name and display number.
- P-Asserted-Identity: Verify the display name and display number.
- Privacy: Verify privacy masking with "user, id".
- Diversion: Verify the display name and display number.

The following attributes in SIP message body are inspected using sniffer trace analysis tool:

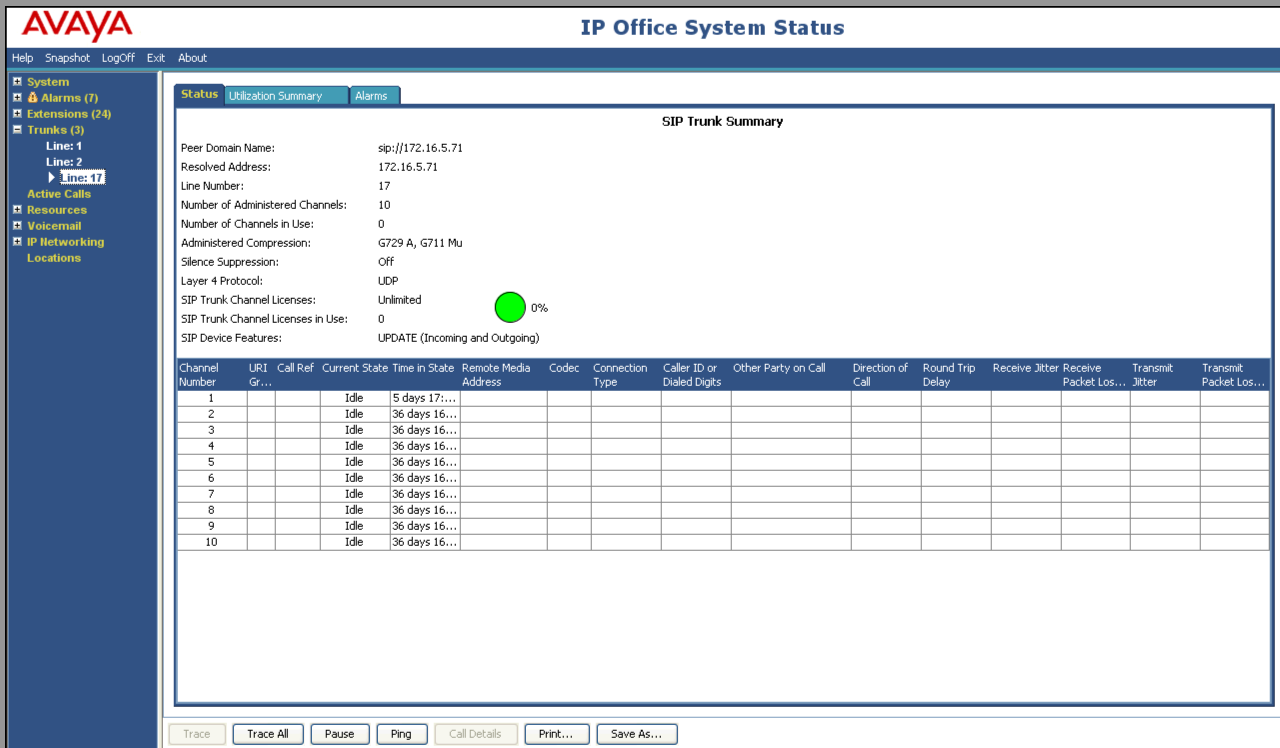
- Connection Information (c line): Verify IP addresses of near end and far end endpoints.
- Time Description (t line): Verify session timeout value of near end and far end endpoints.
- Media Description (m line): Verify audio port, codec, DTMF event description.
- Media Attribute (a line): Verify specific audio port, codec, ptime, send/ receive ability, DTMF event and fax attributes.

8.3 IP Office System Status

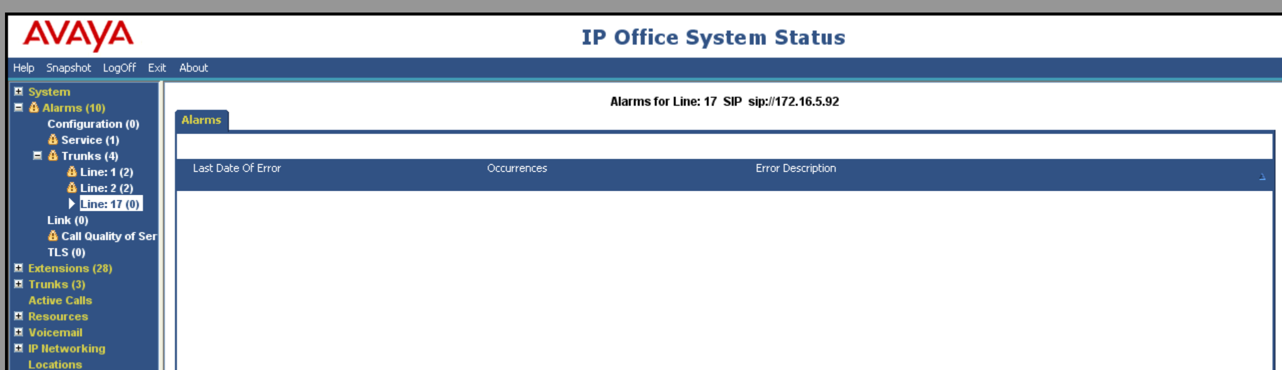
The following steps can also be used to verify the configuration.

- Use the Avaya IP Office **System Status** application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed. 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).

©2014 Avaya Inc. All Rights Reserved.



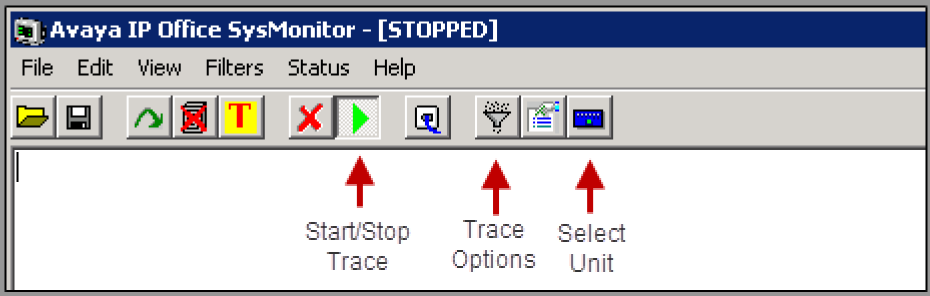
- Select the **Alarms** tab and verify that no alarms are active on the SIP Line.



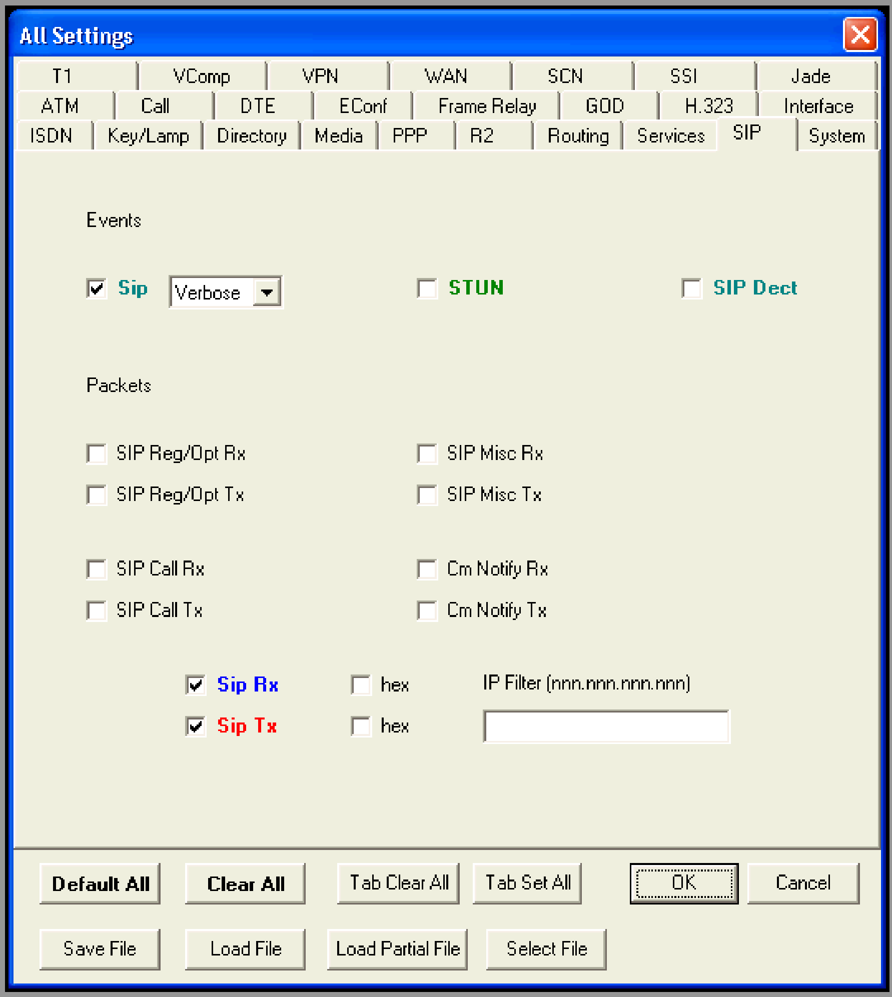
©2014 Avaya Inc. All Rights Reserved.

8.4 IP Office 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 Avaya 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.

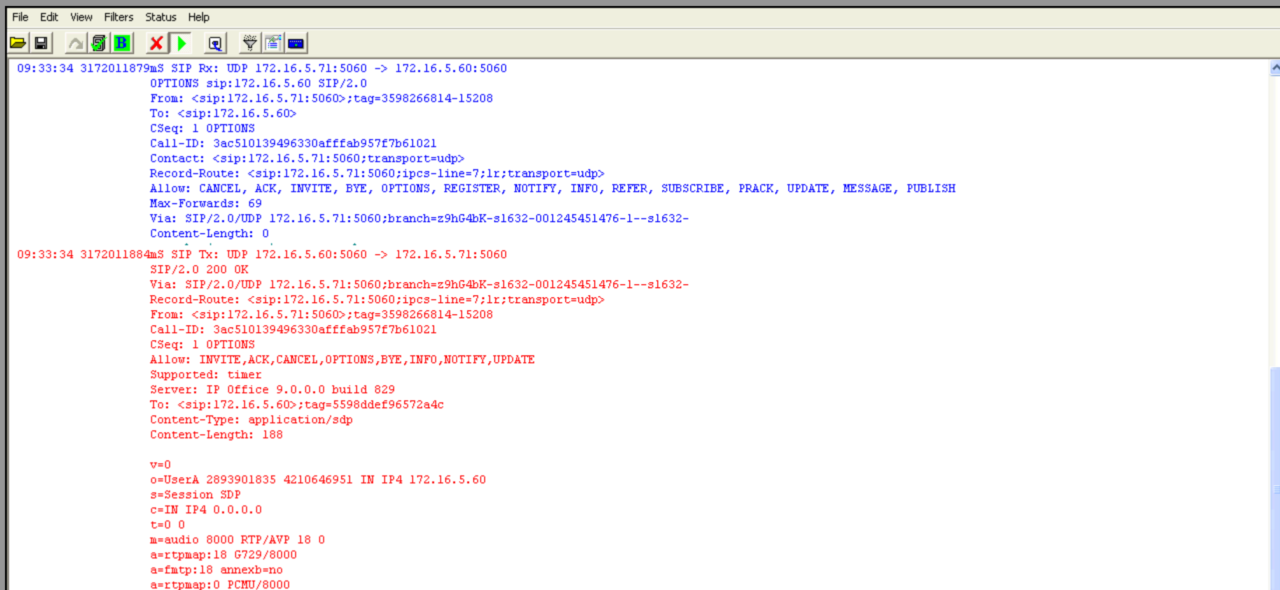


Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type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



©2014 Avaya Inc. All Rights Reserved.

The sample screen below shows an outbound OPTIONS message and the 200 OK response received via the Avaya SBCE.

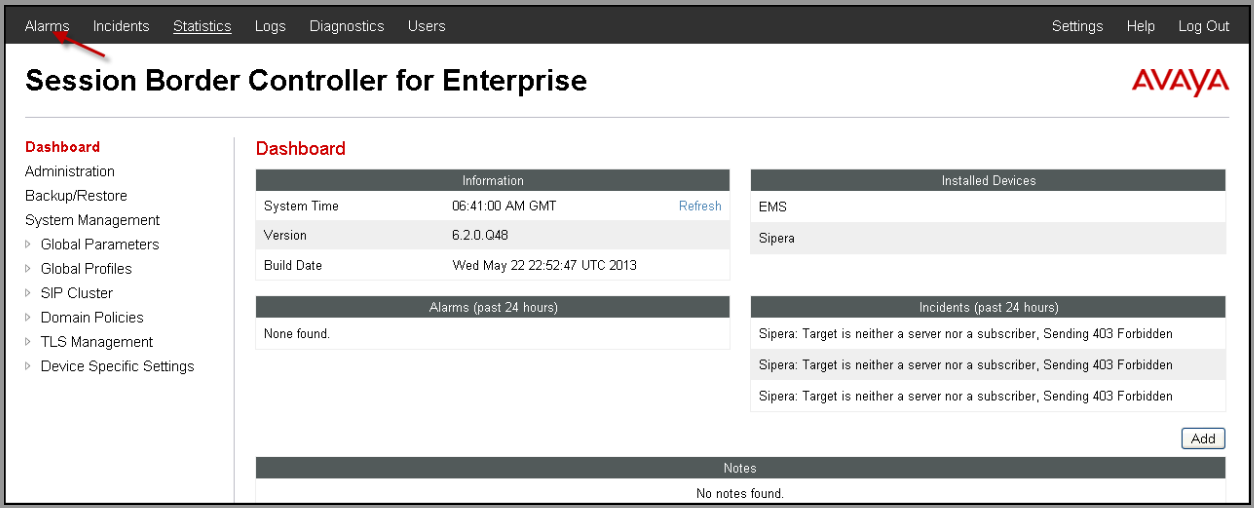


©2014 Avaya Inc. All Rights Reserved.

8.5 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.

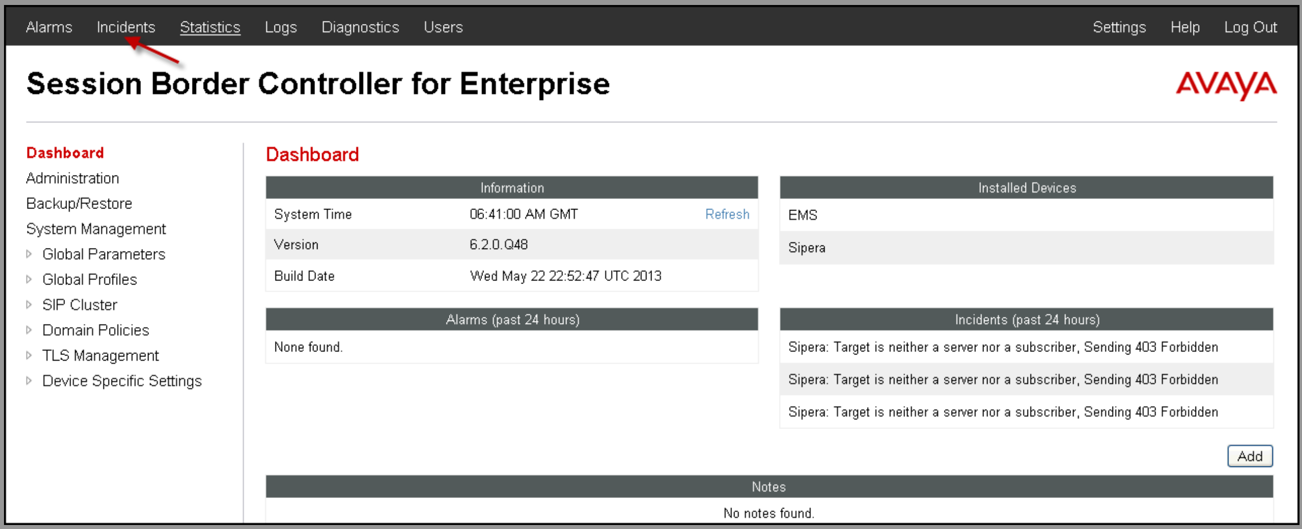
Alarms: Provides information about the health of the SBC.



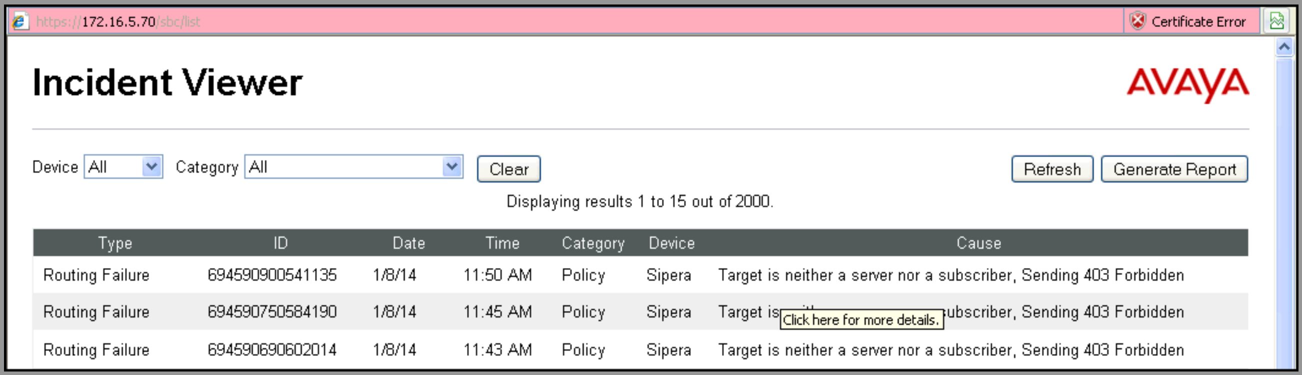
The following screen shows the Alarm Viewer page.

©2014 Avaya Inc. All Rights Reserved.

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

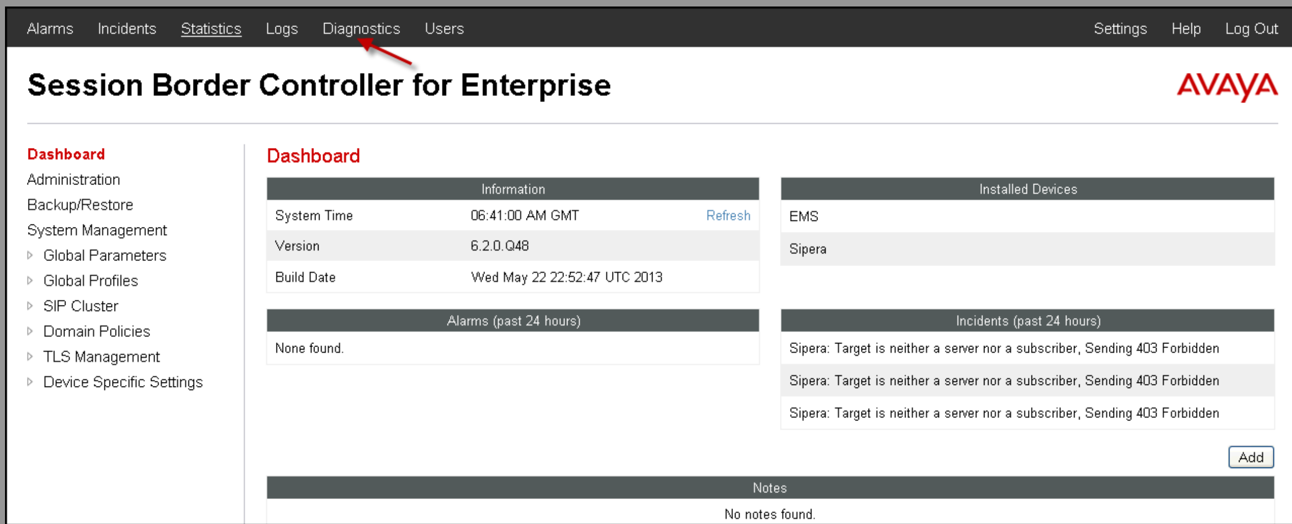


The following screen shows the Incident Viewer page.

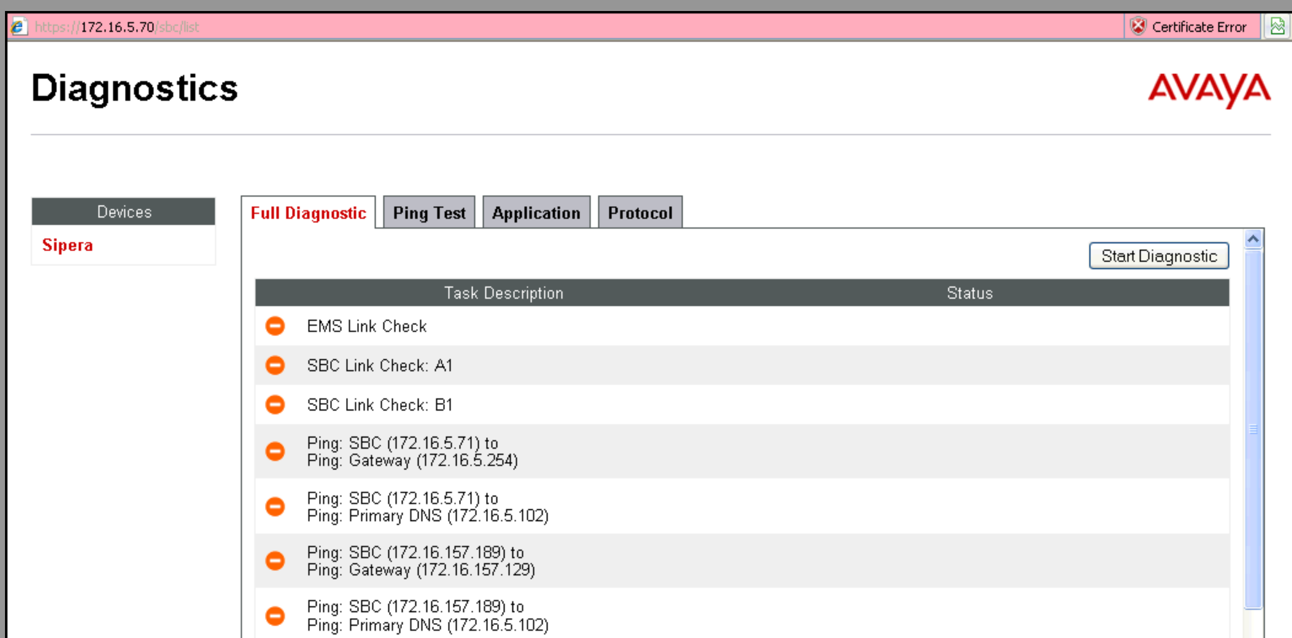


©2014 Avaya Inc. All Rights Reserved.

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

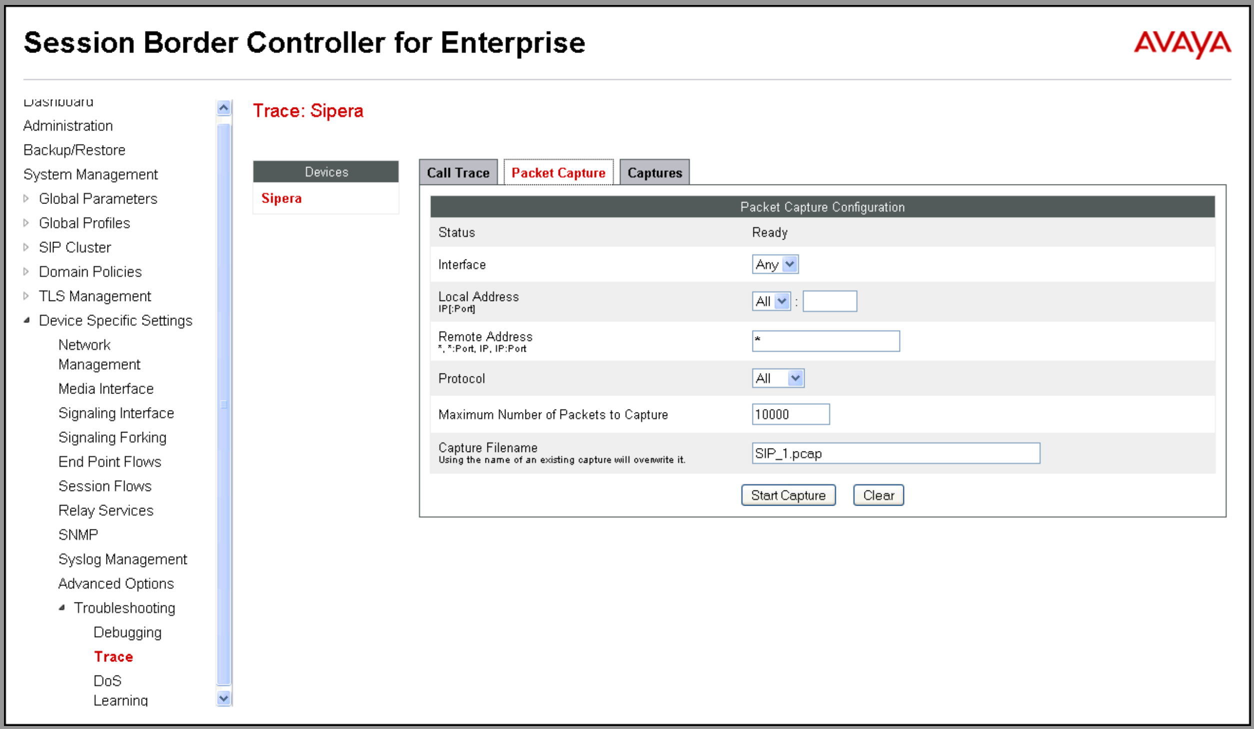


The following screen shows the Diagnostics page.



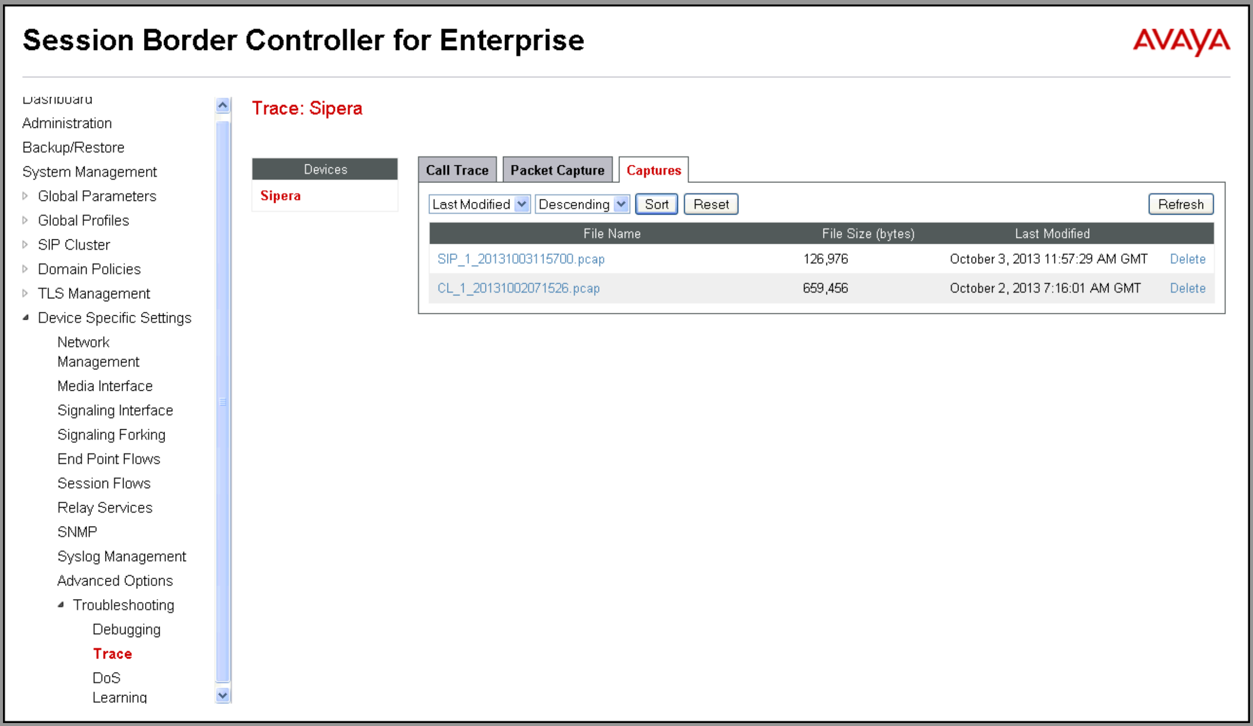
©2014 Avaya Inc. All Rights Reserved.

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**.



©2014 Avaya Inc. All Rights Reserved.

Once the capture is stopped, click 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.



©2014 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 9.0, Avaya Session Border Controller for Enterprise R6.2 and MTS Allstream SIP Trunk Service, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations noted in **Section 2.2**

©2014 Avaya Inc. All Rights Reserved.

10. References

[1] *IP Office 9.0 Installing IP500/IP500 V2*, Document Number 15-601042.
https://downloads.avaya.com/css/P8/documents/100174004

[2] *IP Office Manager Release 9.0*, Document Number 15-601011.
https://downloads.avaya.com/css/P8/documents/100174478

[3] *Administering Avaya Flare® Experience for IPad devices and Windows*.
https://downloads.avaya.com/css/P8/documents/100175132

[4] *IP Office System Status Application*, Document Number 15-601758.
https://downloads.avaya.com/css/P8/documents/100150298

[5] *Avaya IP Office Knowledgebase.*
http://marketingtools.avaya.com/knowledgebase

[6] *Installing Avaya Session Border Controller for Enterprise*.
https://downloads.avaya.com/css/P8/documents/100168983

[7] *Administering Avaya Session Border Controller for Enterprise*.
https://downloads.avaya.com/css/P8/documents/100168982

[8] *Avaya Session Border Controller for Enterprise Release Notes*.
https://downloads.avaya.com/css/P8/documents/100170131

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

Product documentation for Avaya products may be found at http://support.avaya.com.
Product documentation for the Alestra Enlace IP SIP Trunk Service is available from Alestra.
Documentation for Avaya products may be found at http://support.avaya.com.

Product documentation for MTS Allstream SIP Trunking Service is available from MTS Allstream.

©2014 Avaya Inc. All Rights Reserved.

©2014 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.