Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Windstream (Metaswitch Platform) SIP Trunking with Avaya IP Office 9.1.1 and Avaya Session Border Controller for Enterprise Release 6.3.2 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Windstream Metaswitch platform Session Initiation Protocol (SIP) Trunking with Avaya IP Office and Avaya Session Border Controller for Enterprise.

Windstream SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the Windstream network as an alternative to legacy analog or digital 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.

Windstream 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.

©2015 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Windstream and an Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of an Avaya IP Office 500v2 release 9.1.1, Avaya Session Border Controller for Enterprise release 6.3.2 (Avaya SBCE), Avaya Voicemail Pro, Avaya IP Office Video Softphone, and Avaya H.323, SIP, digital, and analog endpoints.

The Windstream SIP Trunking service referenced within these Application Notes is designed for business customers. The service enables local and long distance PSTN calling via standards-based SIP trunks as an alternative to legacy analog or digital trunks, without the need for additional TDM enterprise gateways and the associated maintenance costs.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office to connect to Windstream SIP Trunking service via the Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the features 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

A simulated enterprise site with Avaya IP Office was connected to Windstream SIP Trunking service via the Avaya SBCE. To verify SIP trunking interoperability, the following features and functionality were exercised during the interoperability compliance test:

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from the Avaya Communicator for Windows.
- Inbound and outbound long holding time call stability.
- Various call types including: local, long distance, international, outbound toll-free, operator service and directory assistance.
- Codec G.711MU and G.729.
- Caller number/ID presentation.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.

©2015 Avaya Inc. All Rights Reserved.

- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- Telephony features such as hold and resume, transfer, and conference.
- Use of SIP REFER for call transfer to PSTN.
- G.711 fax pass-through mode.
- Off-net call forwarding.
- Twinning to mobile phones on inbound calls.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

2.2. Test Results

Windstream SIP Trunking passed compliance testing.
Items not supported or not tested included the following:

- Inbound toll-free is supported but was not tested as part of the compliance test.
- Emergency 911 supported but not tested.
- Operator Call (dial 0) and Operator Assisted (dial 0+10digits) are supported but not tested.
- Windstream does not support T.38 fax.

Interoperability testing of Windstream SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **OPTIONS** – Windstream was not configured to send OPTIONS but responded to OPTIONS.
- **Outbound Calling Party Number (CPN) Block from Enterprise Phone** – If IP Office was configured to block Calling Party Number (CPN), the outbound INVITE would receive a "403 Forbidden" response from Windstream, causing the call to fail. This is because Windstream does not support "anonymous" user in the INVITE's From header.
- **Call Redirection using REFER Method** – Windstream prefers use of Re-INVITE for off-net call transfer which was successfully verified in the compliance test. Use of REFER for off-net call transfer was also tested. Though call transfer using REFER succeeded with expected user experience, the signaling was not completely clean: the post-REFER NOTIFY messages from Windstream contained no message body for notification contents, causing IP Office to reject these NOTIFY messages.

2.3. Support

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

For technical support on Windstream SIP Trunking, contact Windstream at http://www.windstream.com.

©2015 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to Windstream SIP Trunking service via Avaya SBCE through the public IP network. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

Located at the enterprise site is an Avaya IP Office 500v2 with the MOD DGTL STA16 expansion which provides connections for 16 digital stations to the PSTN, the extension PHONE 8 card which provides connections for 8 analog stations to the PSTN as well as 64-channel VCM (Voice Compression Module) for supporting VoIP codecs. The LAN port of Avaya IP Office is connected to the enterprise LAN while the WAN port is connected to the public IP network. Endpoints include an Avaya 9600 Series IP Telephone (with H.323 firmware), Avaya 11x0 Series Desk Phone (with SIP firmware), an Avaya 9508 Digital Telephones, an Avaya Symphony 2000 Analog Telephone and an Avaya Communicator for Windows. A separate Windows PC runs Avaya IP Office Manager to configure and administer the Avaya IP Office.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user phones will also ring and can be answered at the configured mobile phones.

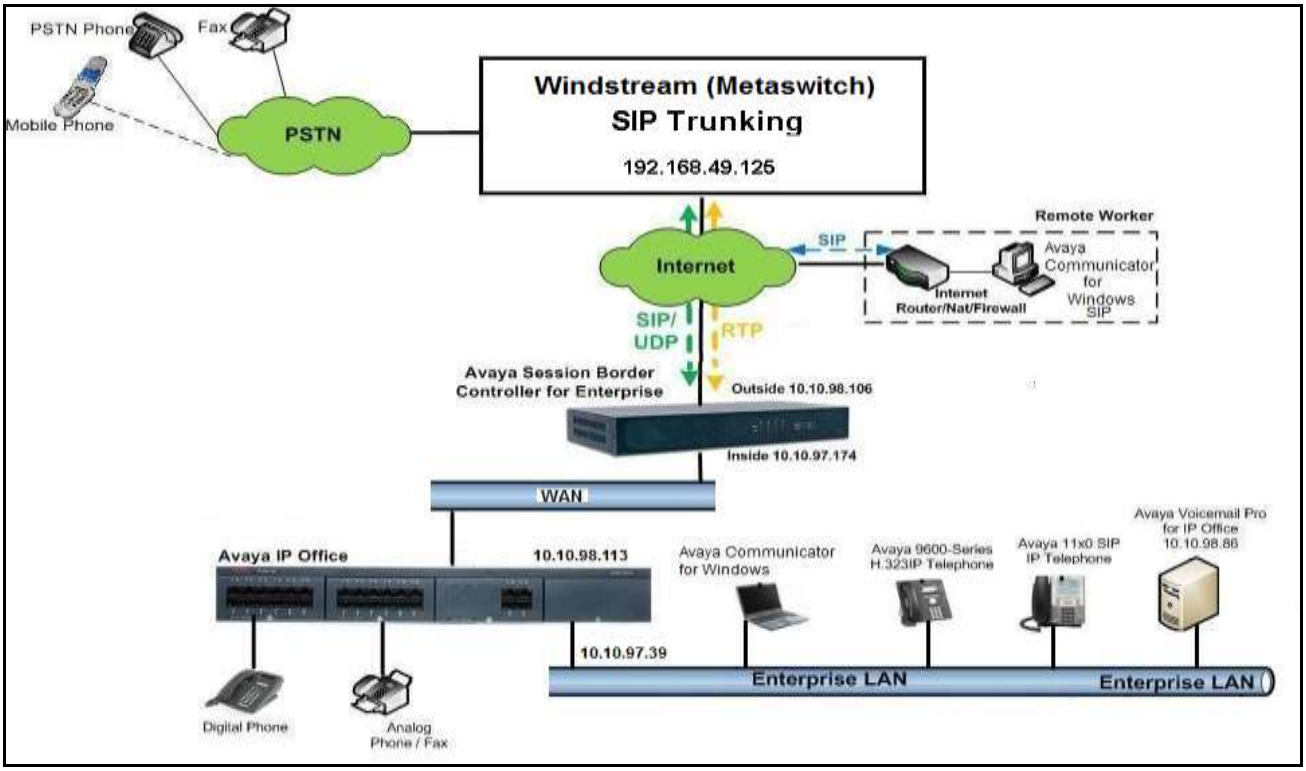


Figure 1: Test Configuration for Avaya IP Office with Windstream (Metaswitch) SIP Trunking Service

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 9 + N digits to send digits across the SIP trunk to Windstream. The short code of 9 was stripped off by Avaya IP

©2015 Avaya Inc. All Rights Reserved.

Office but the remaining N digits were sent unaltered to Windstream. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, Windstream SIP Trunking sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

Additionally, the reference configuration included remote worker functionality, introduced with Avaya IP Office 9.1.1 with Avaya SBCE. A remote worker is a SIP endpoint that resides in the untrusted network, registered to IP Office via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint within the enterprise. This functionality was successfully tested during the compliance test, using the Avaya Communicator for Windows using TLS and SRTP. The configuration tasks required to support remote workers are referenced in **Section 11**.

©2015 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	**Release**
Avaya IP Office 500v2	9.1.1.0 build 10
Avaya IP Office Manager	9.1.1.0 build 10
Avaya Voicemail Pro for IP Office	9.1.1.0 build 10
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.3.2-08-5478
Avaya 11x0 IP Telephone (SIP)	SIP11x0e04.04.18.00
Avaya 9630G IP Telephone (H.323)	Avaya one-X® Deskphone Edition S3.2
Avaya Communicator for Windows	2.0.3.30
Avaya Digital Telephone (9508)	8.44
Avaya Symphony 2000 Analog Telephone	N/A
Windstream SIP Trunking Service Components	
Component	Release
MetaSwitch	8.1.0 Patch B
EdgeMarc 4570 SBC	Version 11-16-13

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.

©2015 Avaya Inc. All Rights Reserved.

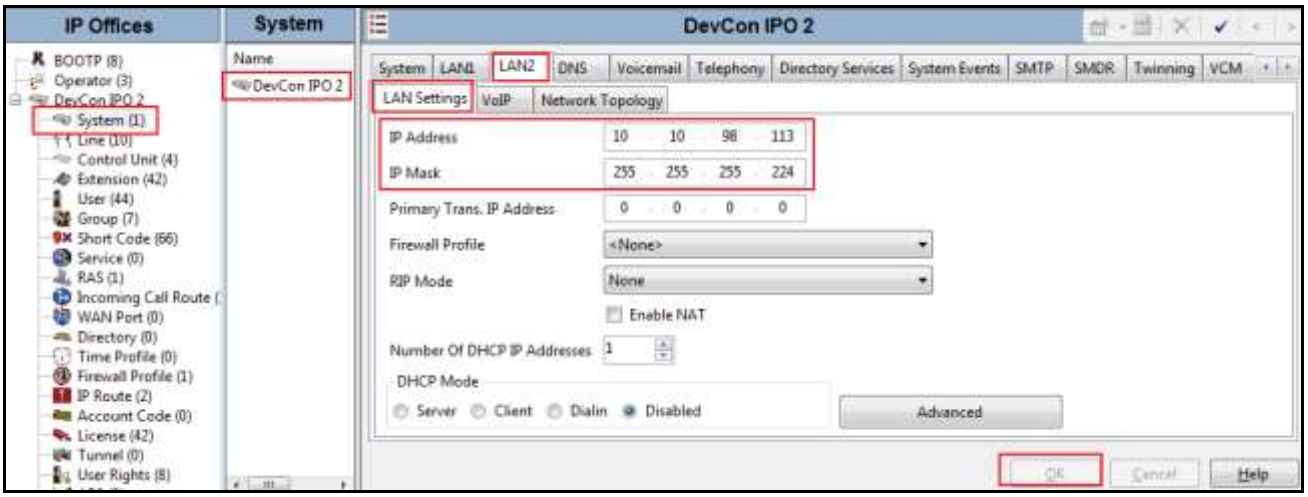
5. Configure IP Office

This section describes the Avaya IP Office configuration to support connectivity to Windstream SIP Trunking service through Avaya SBCE. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one shown in the next section. The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center, and the Details pane on the right side. These panes will be referenced throughout the Avaya IP Office configuration. Proper licensing as well as standard feature configurations that are not directly related to the interface with the service provider (such as LAN interface to the enterprise site and IP Office Video Softphone support) is assumed to be already in place.

5.1. LAN Settings

In the sample configuration, the **DevCon IPO2** was used as the system name and the WAN port was used to connect the Avaya IP Office to the public network. The LAN2 settings correspond to the WAN port on the Avaya IP Office. To access the LAN settings, first navigate to **System (1) → DevCon IPO2** in the Navigation and Group Panes and then navigate to the **LAN2→ LAN Settings** tab in the Details Pane.

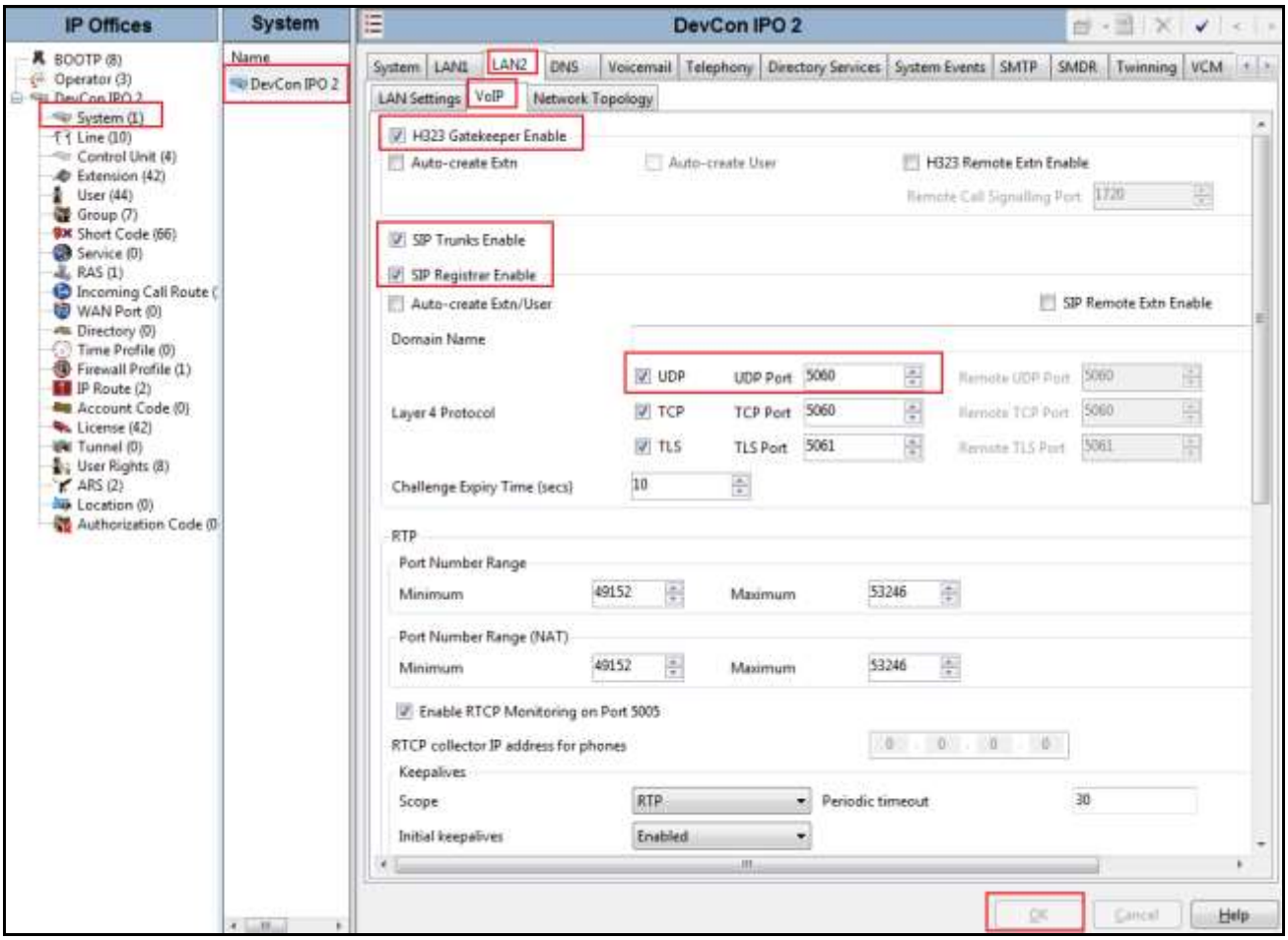
- Set the **IP Address** field to the IP address assigned to the Avaya IP Office WAN port.
- Set the **IP Mask** field to the mask used on the public network.
- All other parameters should be set according to customer requirements.
- Click **OK**.



©2015 Avaya Inc. All Rights Reserved.

Select the **VoIP** tab as shown in the following screen.

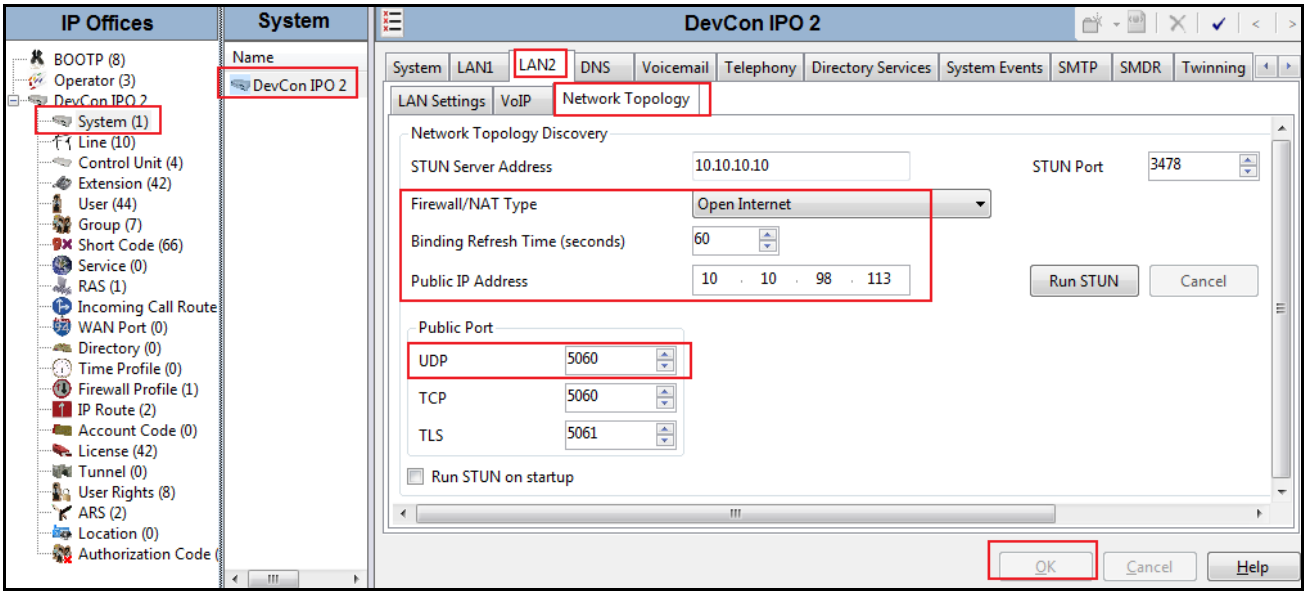
- The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such the 9600-Series IP Telephones used in the sample configuration.
- The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to Windstream.
- The **SIP Registrar Enable** box is checked to allow Avaya IP Office Video Softphone usage.
- The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, Avaya IP Office would request RTP media be sent to a UDP port in the configurable range for calls using LAN2. The specific values used for the compliance test are shown in the example below.
- **Layer 4 Protocol** is set to **UDP** port ***5060***.
- All other parameters should be set according to customer requirements.
- Click **OK.**



©2015 Avaya Inc. All Rights Reserved.

On the **Network Topology** tab in the Details Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test as shown in **Figure 1**, so the parameter was set to ***Open Internet***. With this configuration, STUN will not be used.
- Set **Binding Refresh Time (seconds)** to ***60***. This value is used as one input to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public IP Address** to the IP address of the Avaya IP Office WAN port. **Public Port** is set to ***5060*.**
- All other parameters should be set according to customer requirements.
- Click **OK**.



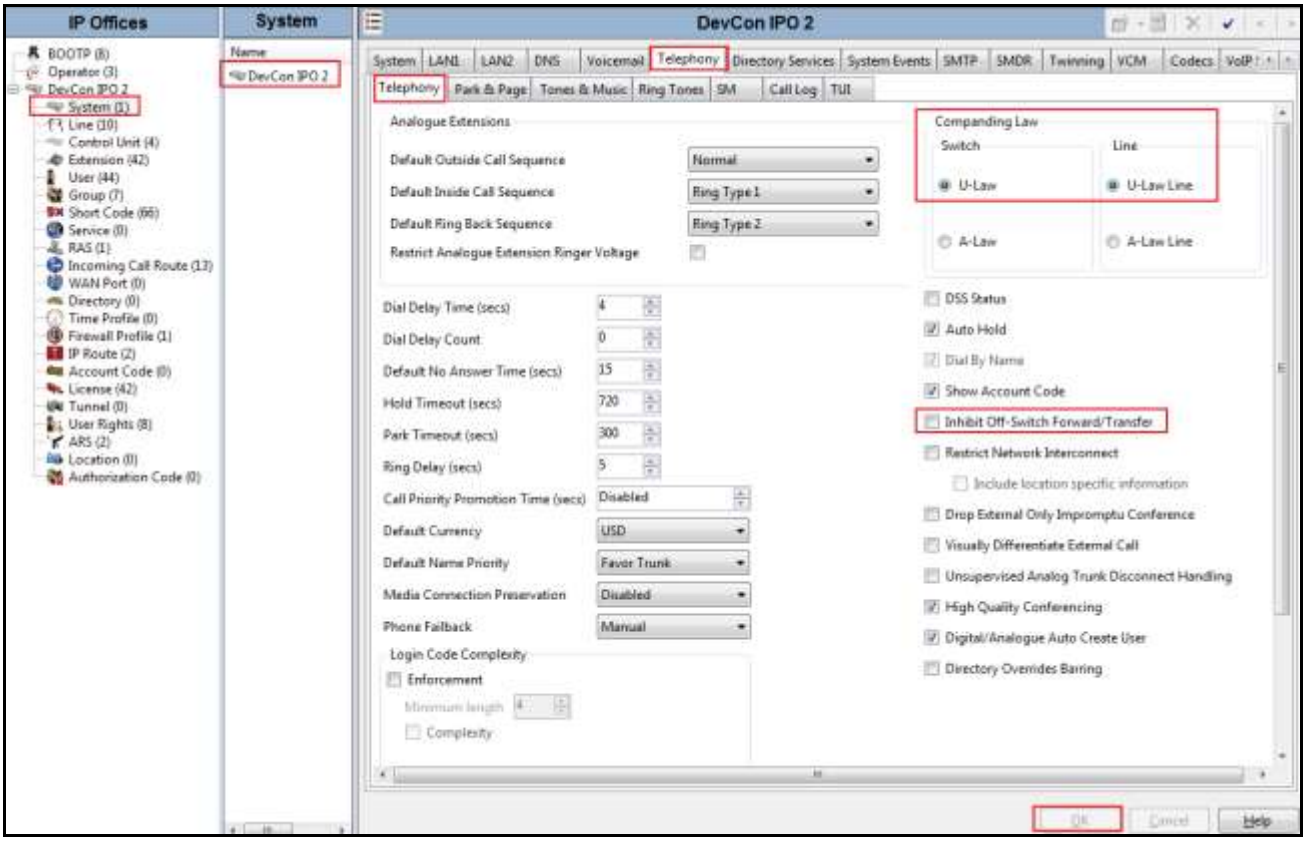
In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network. The LAN1 interface configuration is not directly relevant to the interface with Windstream SIP Trunking service, and therefore is not described in these Application Notes.

©2015 Avaya Inc. All Rights Reserved.

5.2. System Telephony Settings

Navigate to the **Telephony → Telephony** Tab in the Details Pane.

- Choose the **Companding Law** typical for the enterprise location.
- For North America, ***ULAW*** is used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the service provider across the SIP trunk.
- Click **OK**.

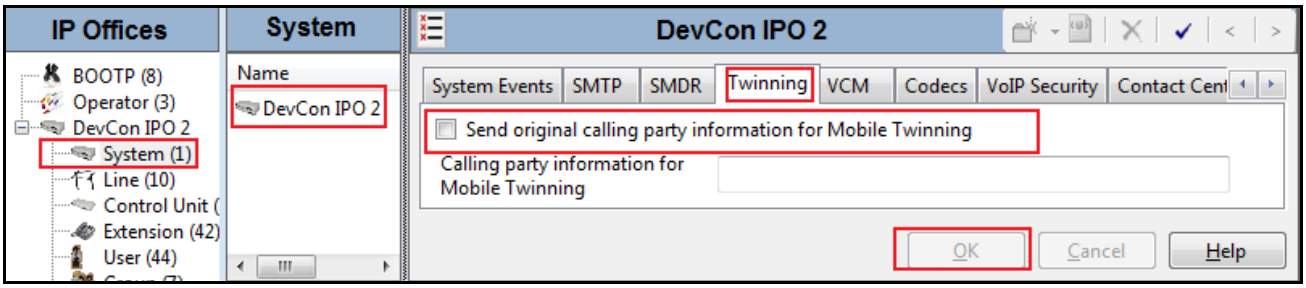


©2015 Avaya Inc. All Rights Reserved.

5.3. Twinning Calling Party Settings

When using twinning, the calling party number displayed on the twinned phone is controlled by two parameters. These parameters only affects twinning and do not impact the messaging or operation of other redirected calls such as forwarded calls. The first parameter is the **Send original calling party information for Mobile Twinning** box on the **System→Twinning** tab. The second parameter is the **Send Caller ID** parameter on the **SIP Line** form (shown in **Section 5.4**).

- For the compliance testing, the **Send original calling party information for Mobile Twinning** as shown below was unchecked. This setting allows **Send Caller ID** parameter that was set in **Section 5.4** to be used.
- Click **OK**.



©2015 Avaya Inc. All Rights Reserved.

5.4. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Windstream 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 IP Office Manager to create a SIP Line. Follow the steps in **Section 5.4.1** 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 **Section 5.4.2**.

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

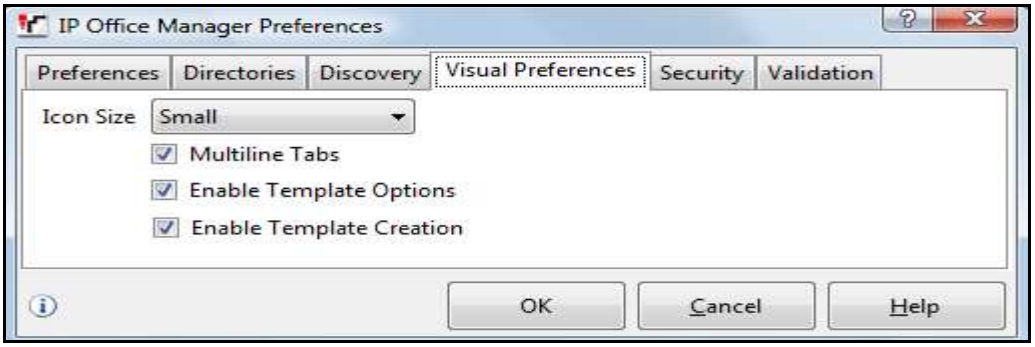
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

Alternatively, a SIP Line can be created manually. To do so right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.4.2**.

5.4.1. Create SIP line from Template

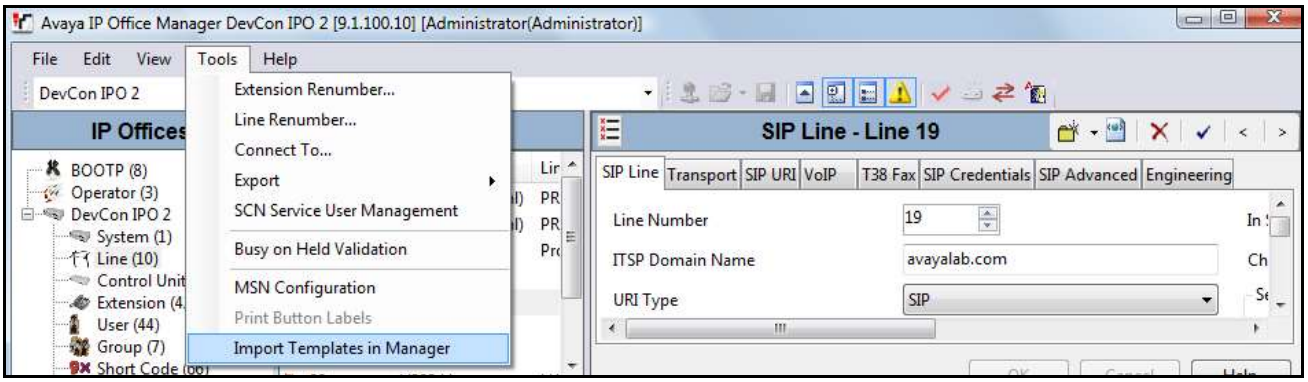
1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **AF_Windstream_Metaswitch_ASBC_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.

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**.



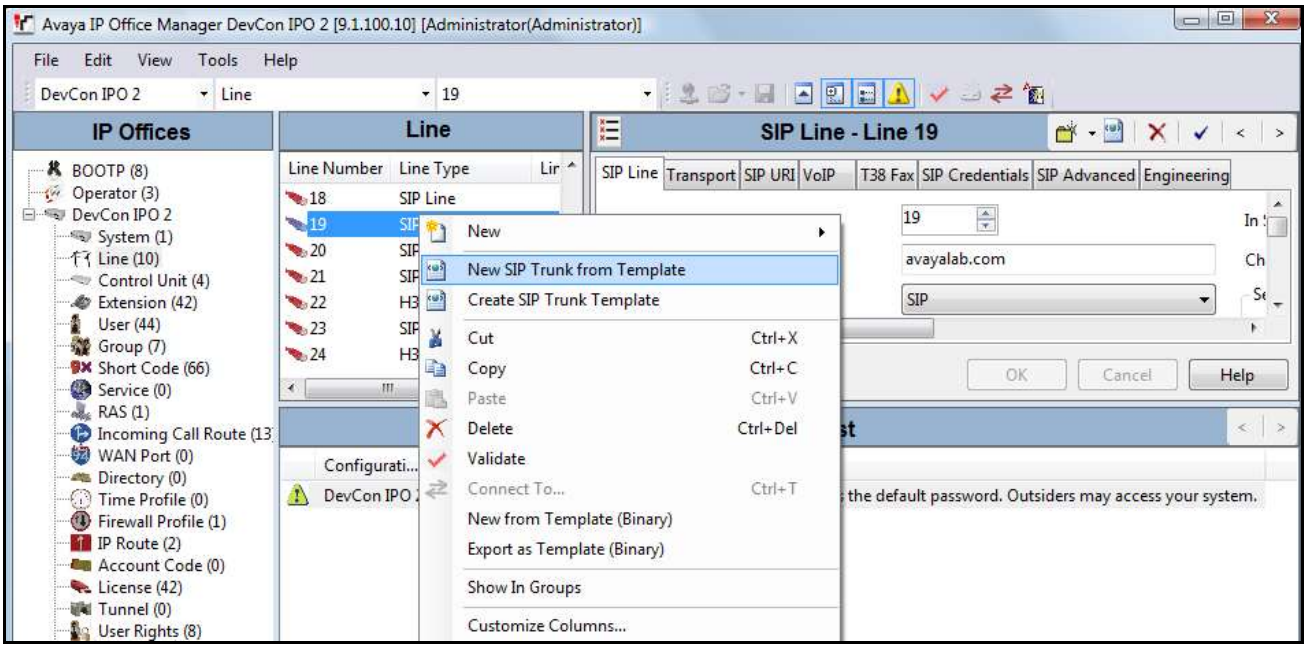
©2015 Avaya Inc. All Rights Reserved.

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**.



   In the pop-up window that appears (not shown), select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window will appear (not shown) stating success or failure. Then 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.

4. 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**.



©2015 Avaya Inc. All Rights Reserved.

5. In the subsequent Template Type Selection pop-up window, select **United State** from the **Locale** pull-down menu and select **Windstream** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**AF_Windstream_Metaswitch_ASBC _SIPTrunk.xml)** created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.

6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2.**

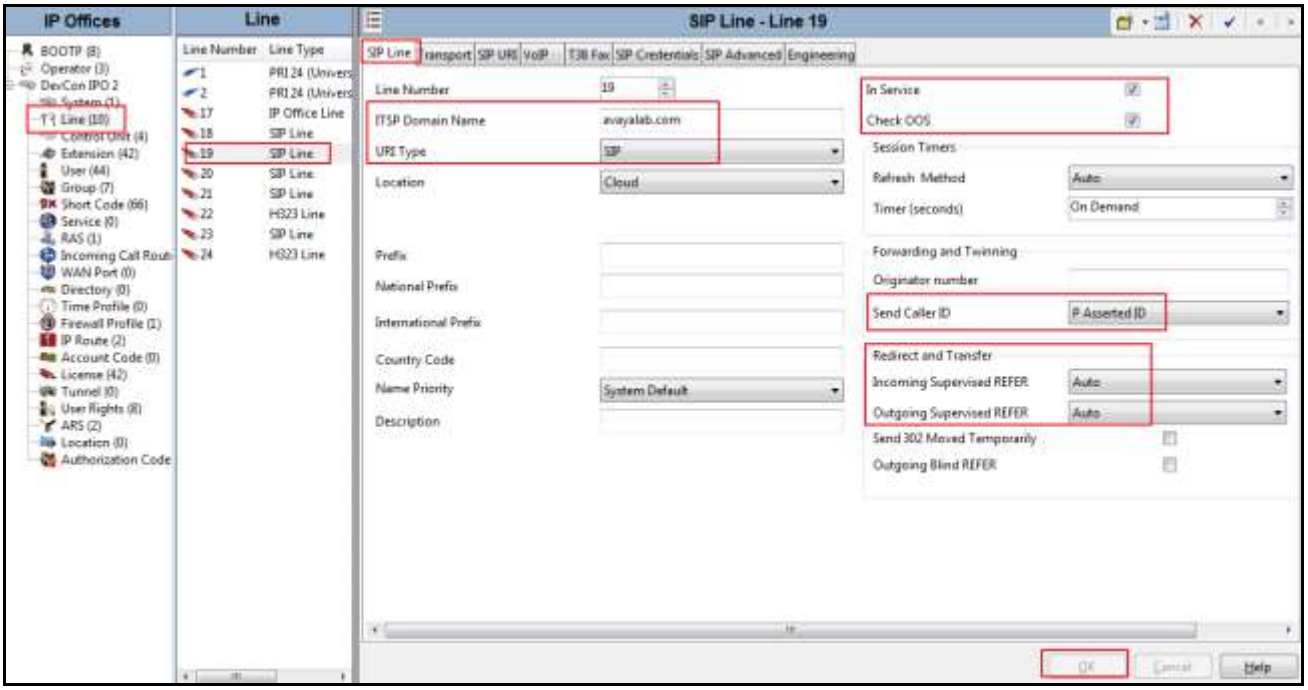
©2015 Avaya Inc. All Rights Reserved.

5.4.2. Create SIP Line Manually

To create a SIP line, begin by navigating to **Line** in the left Navigation Pane, then right-click in the Group Pane and select **New → SIP Line**. On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the enterprise domain so that IP Office uses this domain as the host portion of SIP URI in SIP headers such as the From header.
- Set **Send Caller ID** to ***P Assert ID***. For the compliance test, this parameter was used for caller ID in the case of Call Forwarding and Twinning.
- Check the **In Service** box.
- Set **URI Type** as ***SIP*** for SIP trunk to service provider via Avaya SBCE.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Default values may be used for all other parameters.

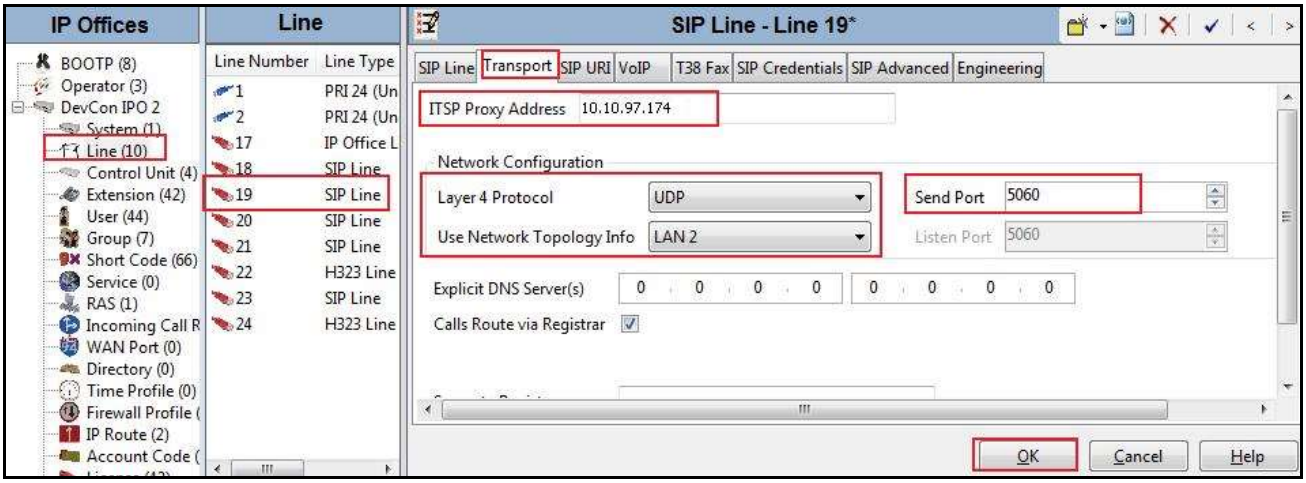
The area of the screen entitled **Redirect and Transfer** is used to enable/disable SIP REFER for call transfers. In the compliance test, Re-INVITE and REFER methods are supported by Windstream. Therefore, the value "**Auto**" is selected from the drop-down menu for **Incoming** and **Outgoing Supervised REFER**. Click **OK**.



©2015 Avaya Inc. All Rights Reserved.

Select the **Transport** tab.

- The **ITSP Proxy Address** is set to internal IP Address of Avaya SBCE. As shown in **Figure 1**, this IP Address is shown in capture below.
- In the **Network Configuration** area, ***UDP*** is selected as the **Layer 4 Protocol**, and the **Send Port** is set to the port number of Avaya SBCE.
- The **Use Network Topology Info** parameter is set to ***LAN 2***. This associates the SIP Line with the parameters in the **System → LAN2 → Network Topology** tab.
- Other parameters retain default values in the screen below.
- Click **OK**.

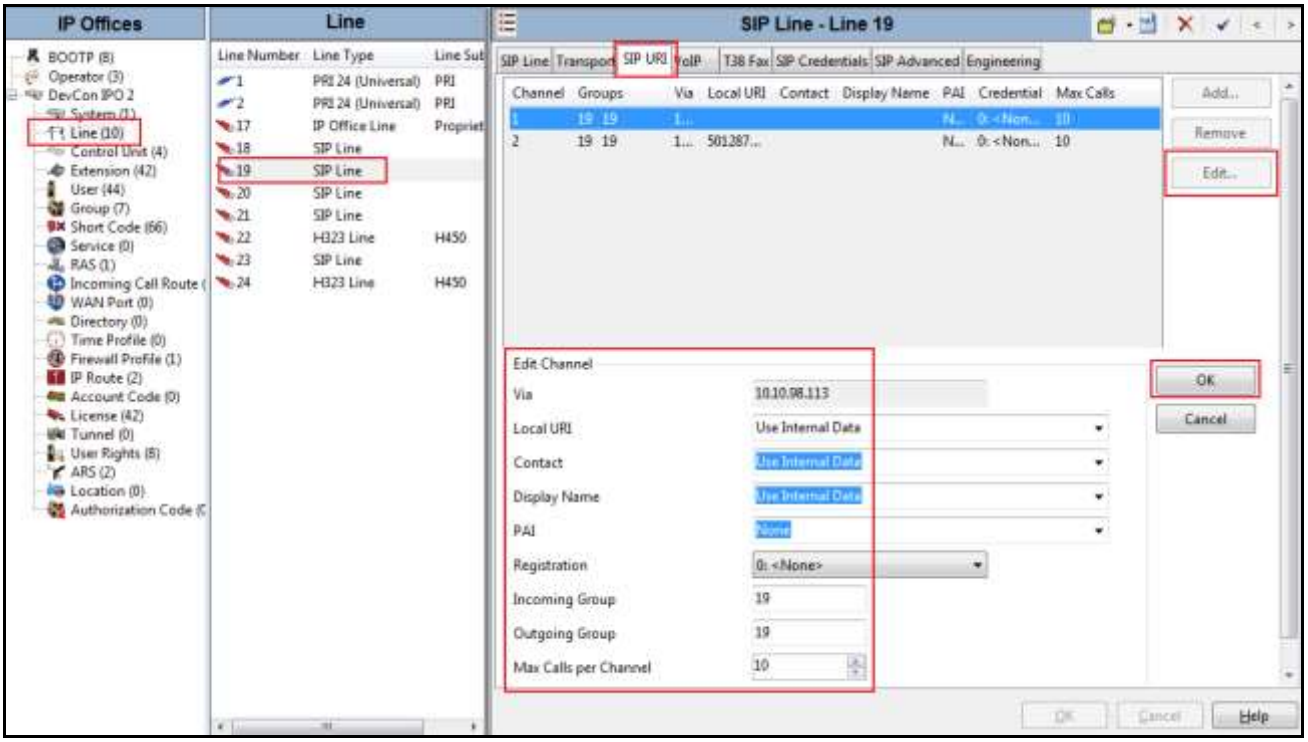


©2015 Avaya Inc. All Rights Reserved.

A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, click the **Add** button, and then **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 is 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:

- **Via** field is pre-populated by IP Office.
- Set **Local URI**, **Contact** and **Display Name** to ***Use Internal Data***. This setting allows calls on this line which SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.6**.
- For **PAI** and **Registration**, select ***None***.
- Associate this line with an incoming line group 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. For the compliance test, a new incoming and outgoing group ***19*** was defined that only contains this line (line 19).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK.**

The following capture is the SIP URI entry for **Channel 1**.



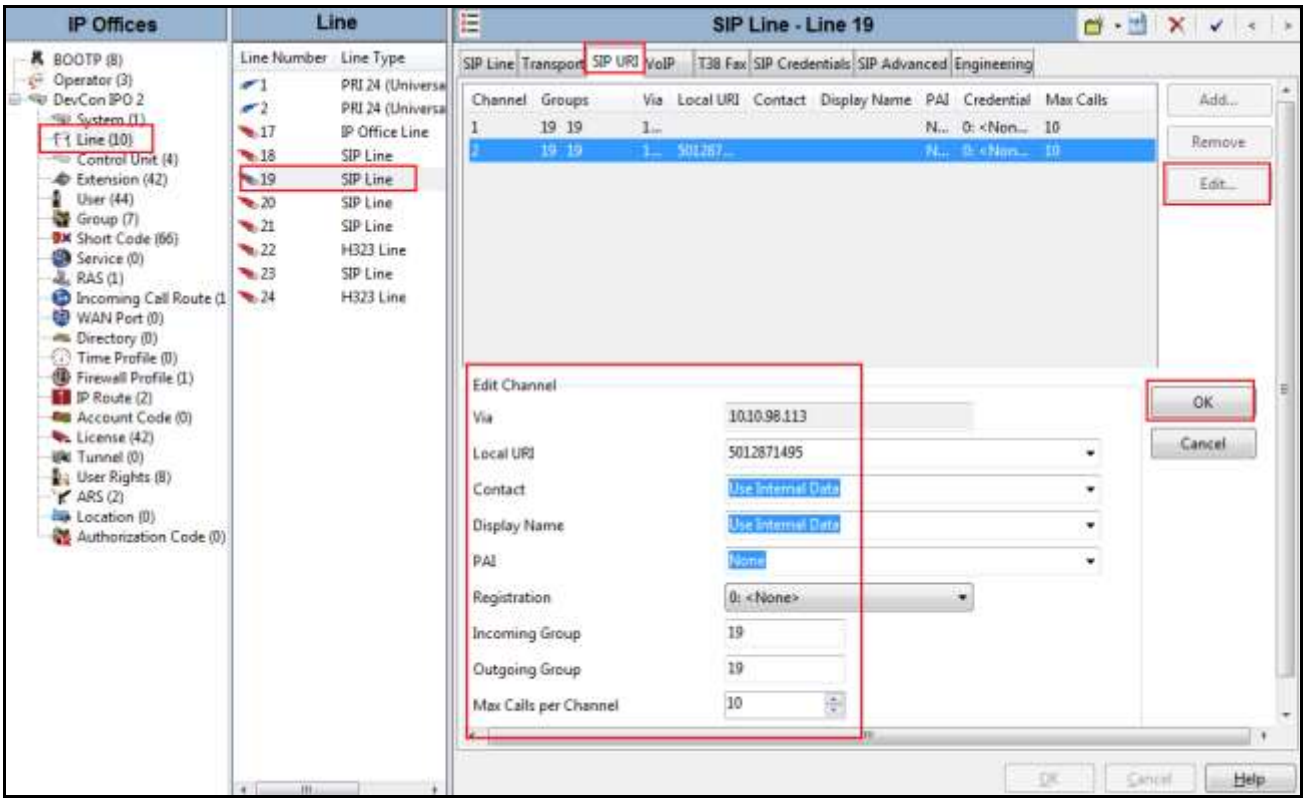
©2015 Avaya Inc. All Rights Reserved.

SIP URI entry **Channel 2** was similarly created for incoming calls to a pre-define DID numbers, as shown in capture below, to access to Feature Name Extension 00 (FNE00. The Short Codes for FNE00 was defined in **Section 5.5** to provide Dial Tone and Mobile Callback for mobility extension.

The **Channel 2,** as shown in the screenshot below, was configured with following parameters.

- **Via** field is pre-populated by IP Office.
- Set the **Local URI** to pre-define DID number.
- Set **Contact** and **Display Name** to ***Use Internal Data***. This setting allows calls on this line which SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.6.**
- For **PAI** and **Registration**, select ***None***.
- Associate **Incoming Group** and **Outgoing Group** to SIP Line ***19***.
- Set the **Max Calls per Channel** field to ***10***.
- Other parameters retain default values.
- Click **OK**.

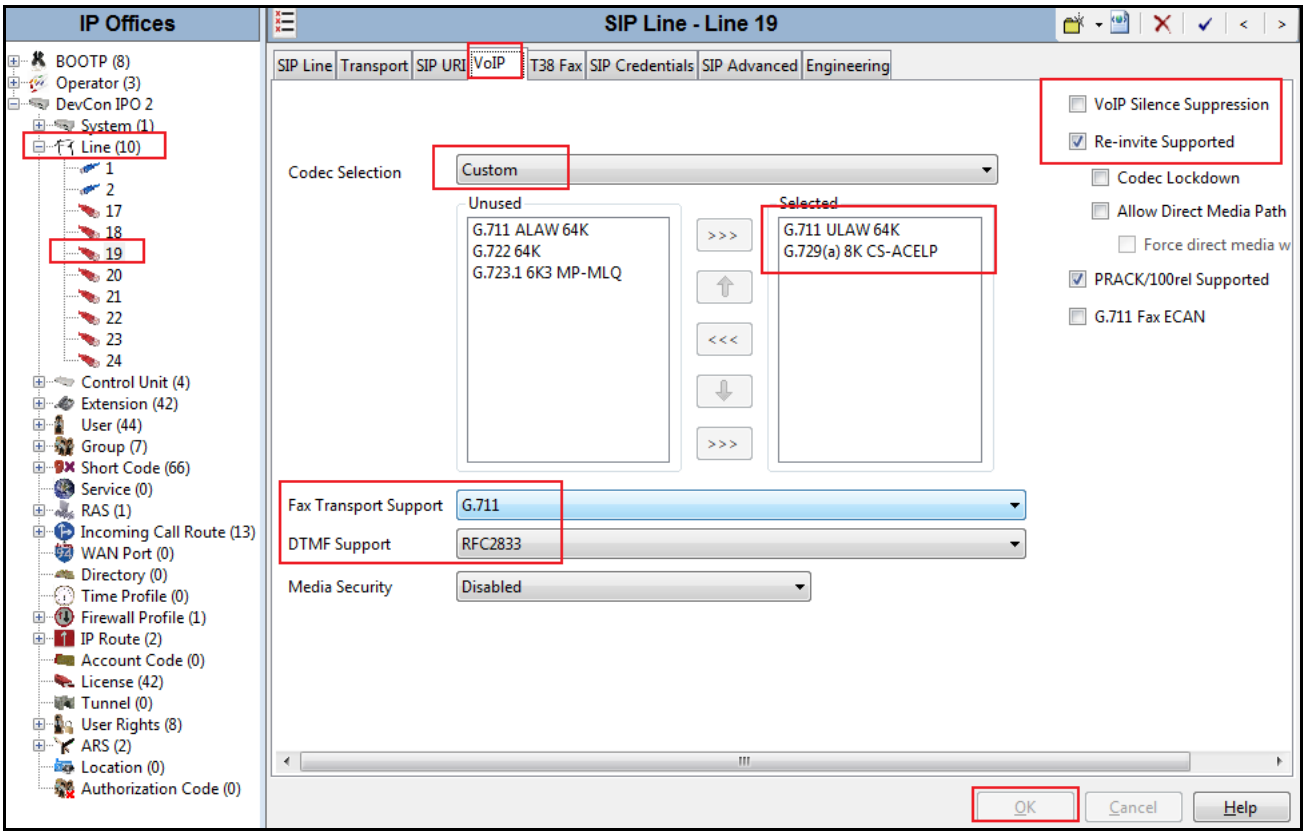
The following capture is the SIP URI entry for **Channel 2**.



©2015 Avaya Inc. All Rights Reserved.

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

- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. Select ***G.711 ULAW*** and ***G.729*** codecs which is supported by the Windstream SIP Trunking service, in the Session Description Protocol (SDP) offer.
- Set **Fax Transport Support** to ***G.711*** from the pull-down menu.
- Set the **DTMF Support** field to ***RFC2833*** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Default values may be used for all other parameters**.**
- Click **OK.**

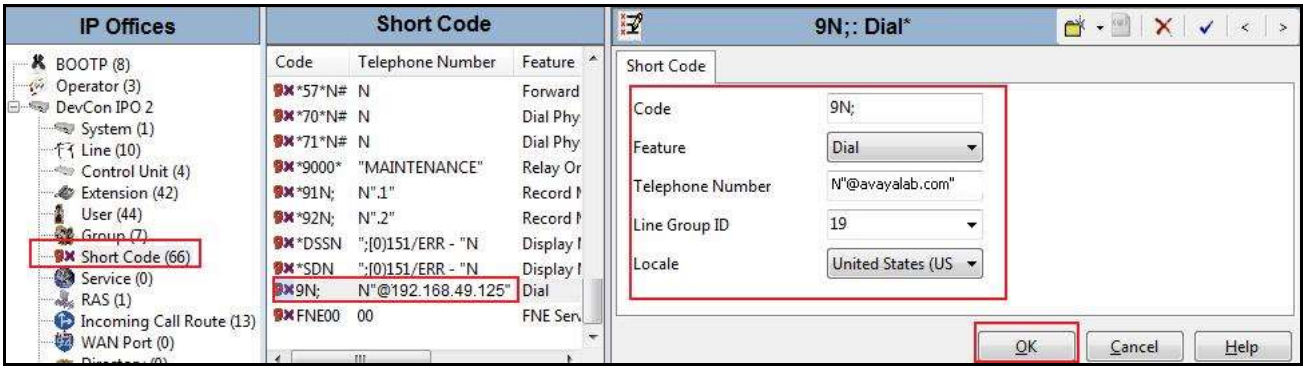


©2015 Avaya Inc. All Rights Reserved.

5.5. Short Code

Define a short code to route outbound traffic to the SIP line. To create a short code, select **Short Code** in the left Navigation Pane, then right-click in the Group Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered "9N;" short code used in the test configuration.

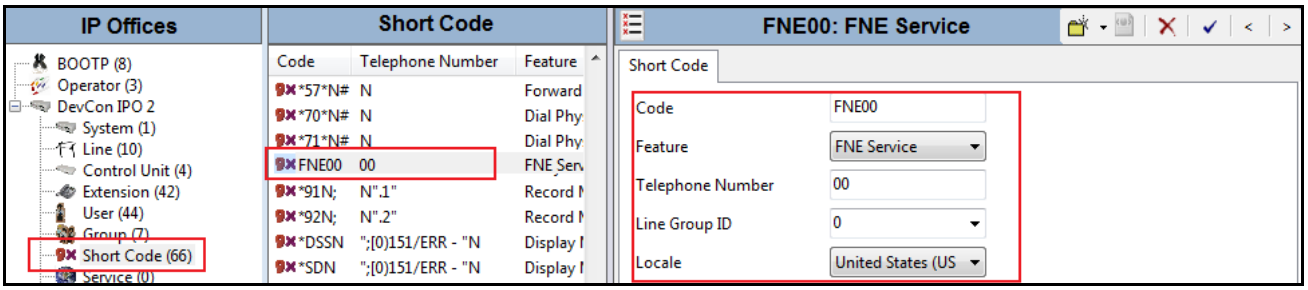
- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, ***9N;*** this short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to ***Dial***. This is the action that the short code will perform.
- Set **Telephone Number** to ***N"@avayalab.com"***. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value ***N*** represents the number dialed by the user. The host part following the "@" is the domain of the service provider network.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4**. This short code will use this line group when placing the outbound call.
- Set **Locale** to ***United State (US English)***.
- Click **OK**.



©2015 Avaya Inc. All Rights Reserved.

For incoming calls from mobility extension to FNE features hosted by IP Office to provide **Dial Tone** functionality, Short Code **FNE00** was created. The **FNE00** was configured with the following parameters.

- In the **Code** field, enter the FNE feature code as ***FNE00*** for **Dial Tone**.
- Set the **Feature** field to ***FNE Service***.
- Set the **Telephone Number** field to ***00*** for **FNE00**.
- Set the **Line Group ID** field to ***0***.
- Retain default values for other fields.
- Click **OK** (not shown).

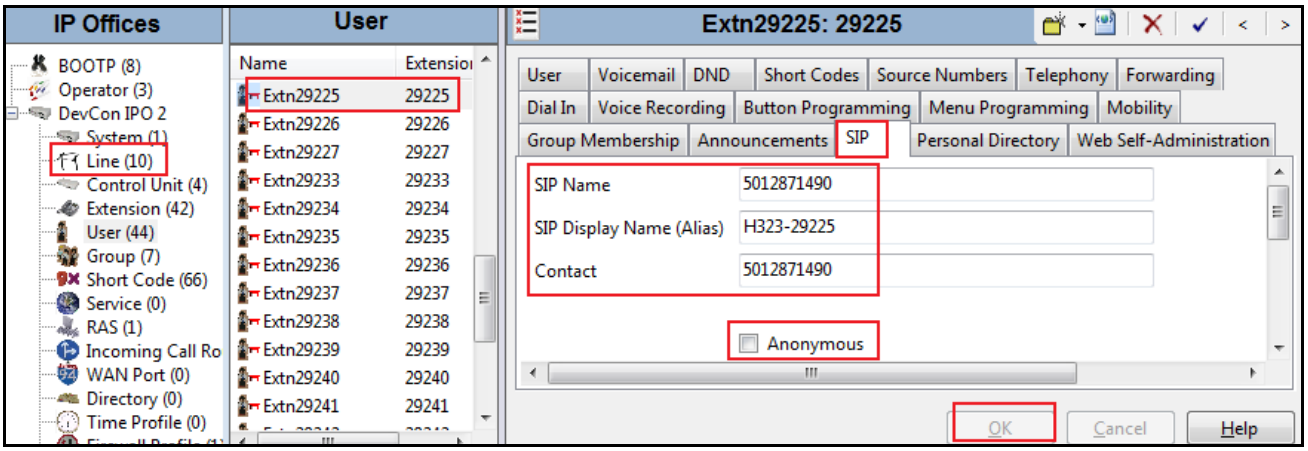


©2015 Avaya Inc. All Rights Reserved.

5.6. User

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 select **User** in the left Navigation Pane, 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 "H323-29225". Select the **SIP** tab in the Details Pane.

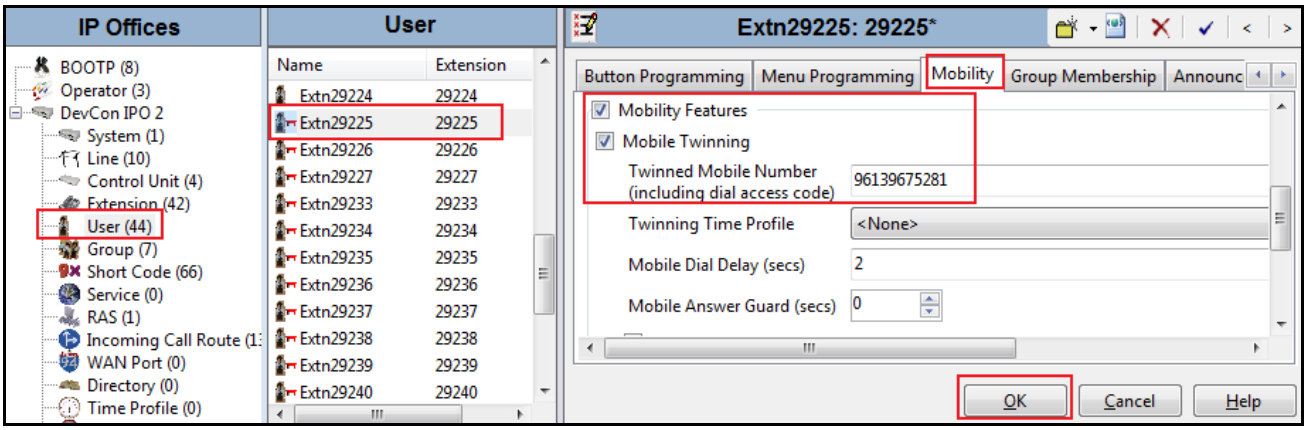
- The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. They also allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4**). The example below shows the settings for user H323-29225. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from Windstream.
- 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.
- Click **OK**.



©2015 Avaya Inc. All Rights Reserved.

One of the H.323 IP Phones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for User H323-29225.

- 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 mobile telephone, in this case 916139675281 including access code of 9.
- Other options can be set according to customer requirements.
- Click **OK**.

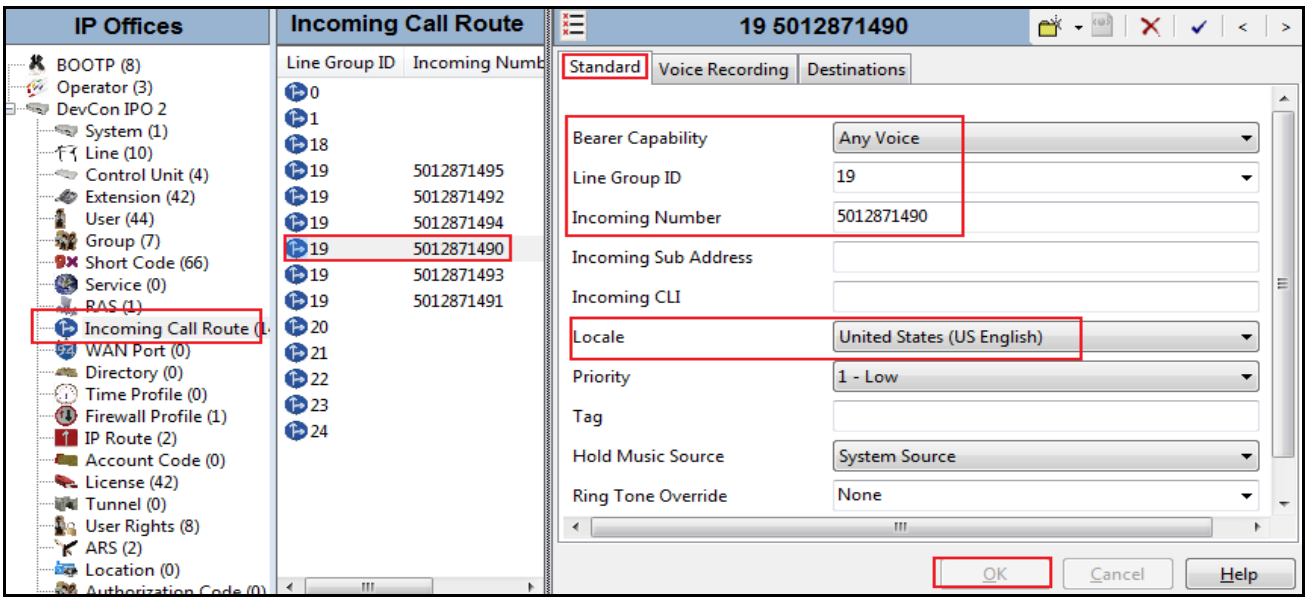


©2015 Avaya Inc. All Rights Reserved.

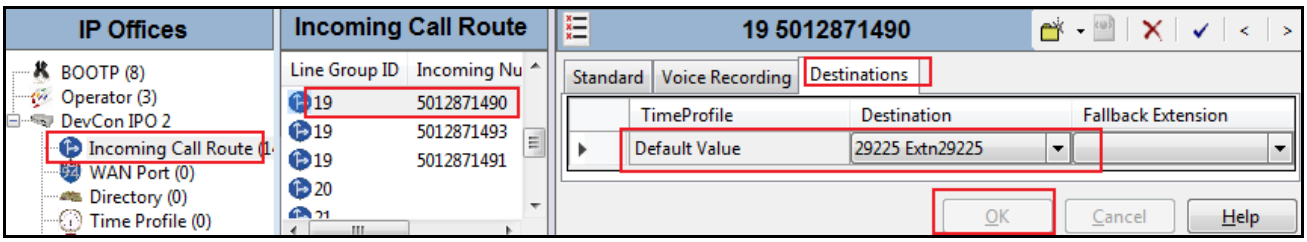
5.7. Incoming Call Route

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 provided by the service provider. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right-click in the center Group Pane and select **New**. 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 number on which this route should match.
- Set **Locale** to ***United State (US English).***
- Default values can be used for all other fields.
- Click **OK**.



On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to 5012871490 on line 19 are routed to extension **29225**. Click **OK**.



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.

©2015 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 software has already been installed. For additional information on these configuration tasks, see reference [4] and [5] in **Section 10**.

The compliance testing comprised the configuration for two major components, 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 in the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - Windstream:

- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Signaling Manipulation
  - Server Configuration
- Domain Policies:
  - Application Rules
  - Media Rules
  - Signaling Rules
  - Endpoint Policy Group
  - Session Policy
- Device Specific Settings:
  - Network Management
  - Media Interface
  - Signaling Interface
  - End Point Flows → Server Flows
  - Session Flows

Call Server configuration elements for the enterprise - IP Office:

- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Server Configuration
- Domain Policies:
  - Application Rules
  - Media Rules
  - Signaling Rules
  - Endpoint Policy Group
  - Session Policy
- Device Specific Settings:

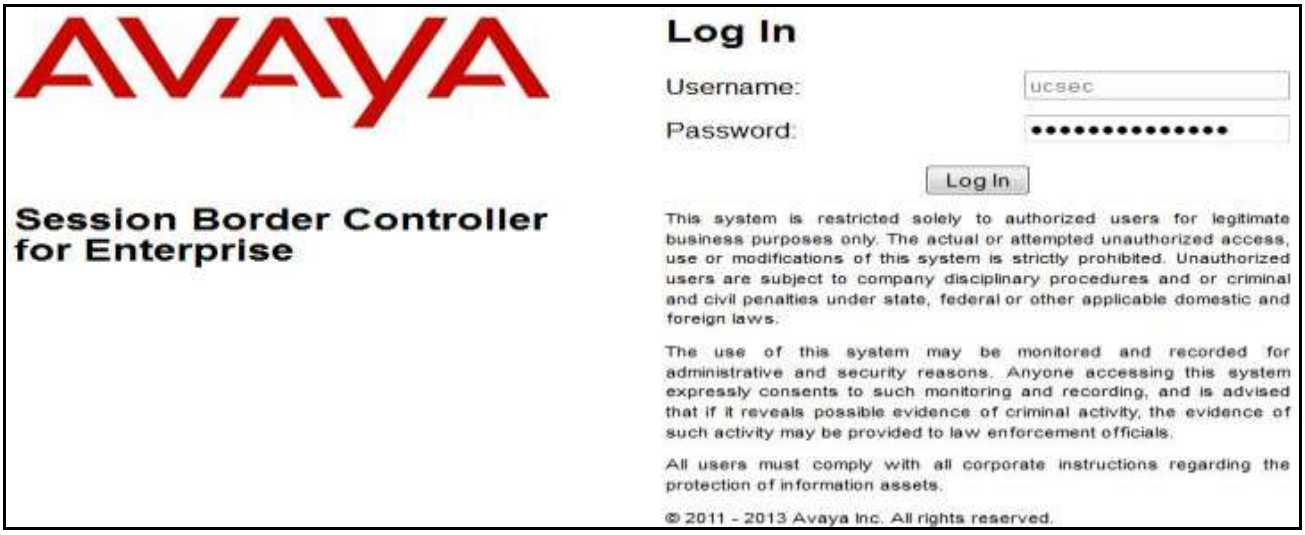
©2015 Avaya Inc. All Rights Reserved.

- Network Management
- Media Interface
- Signaling Interface
- End Point Flows → Server Flows
- Session Flows

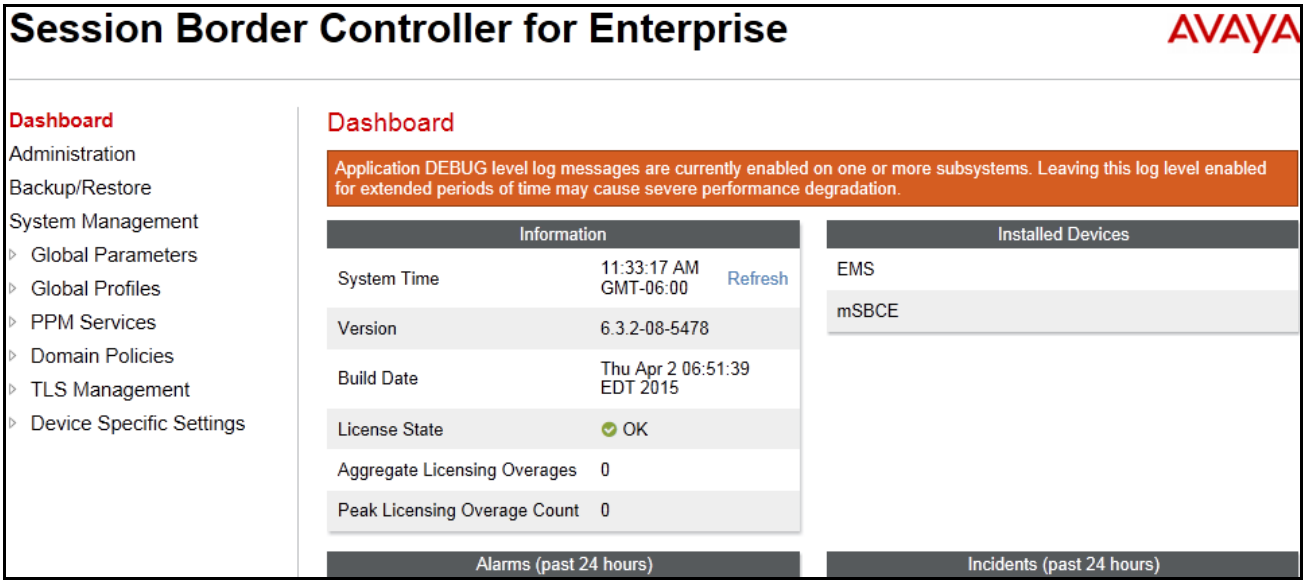
6.1. Log into the Avaya Session Border Controller for Enterprise

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.

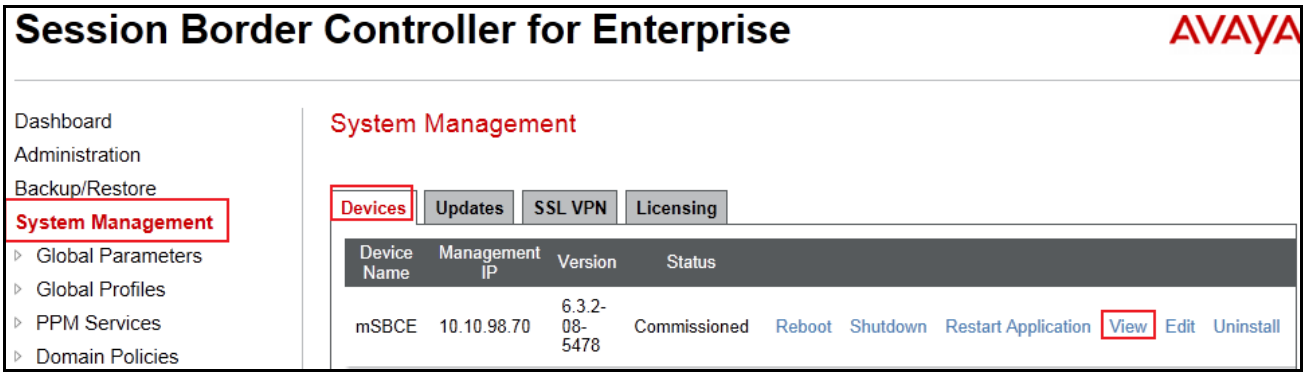
Enter the appropriate credentials then click **Log In**.



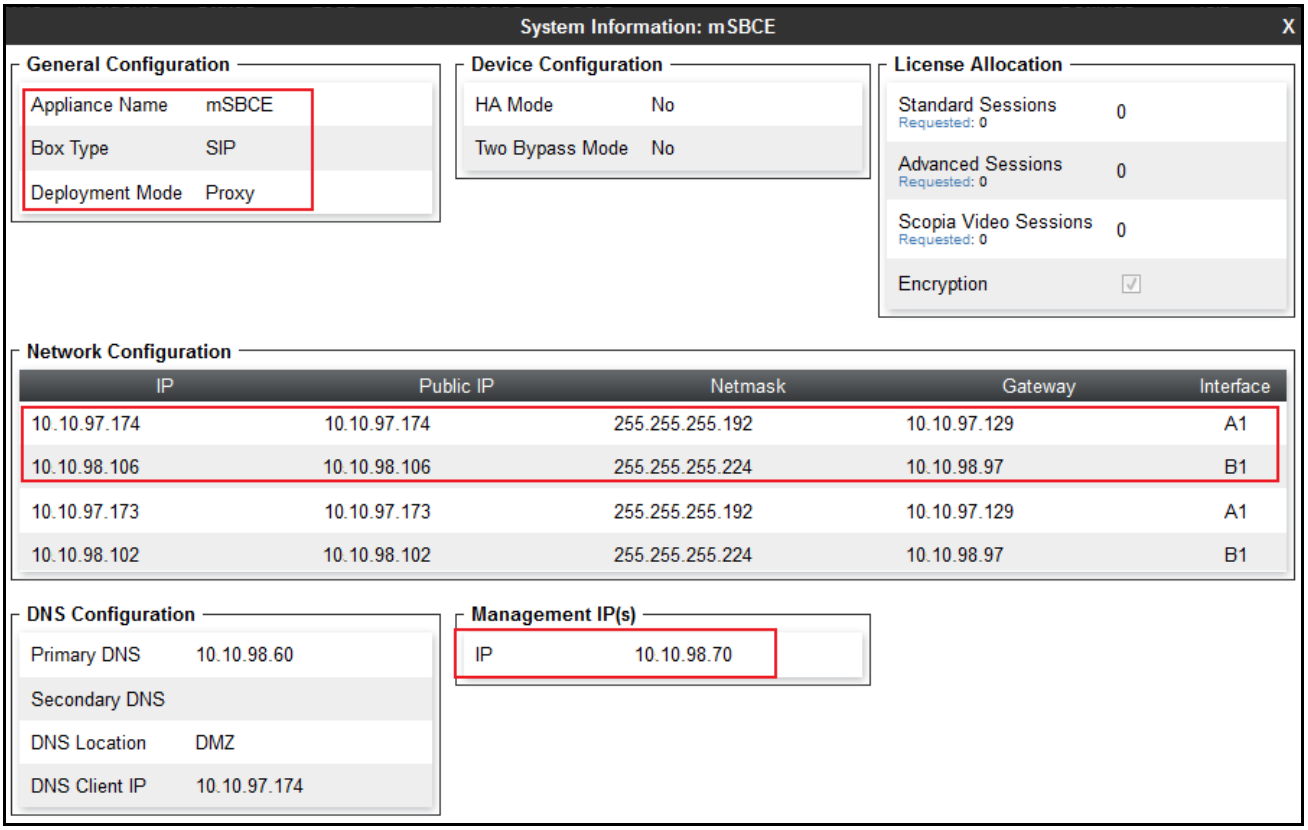
The **Dashboard** main page will appear as shown below.



To view 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 **mSBCE** was already added. To view the configuration of this device, click the **View** as shown in the screenshot below.



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.



©2015 Avaya Inc. All Rights Reserved.

6.2. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.2.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, "*" is used for all incoming and outgoing traffic.

6.2.2. Routing Profiles

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

To create a Routing profile, select **Global Profiles → Routing** then click on the **Add Profile** button (not shown).

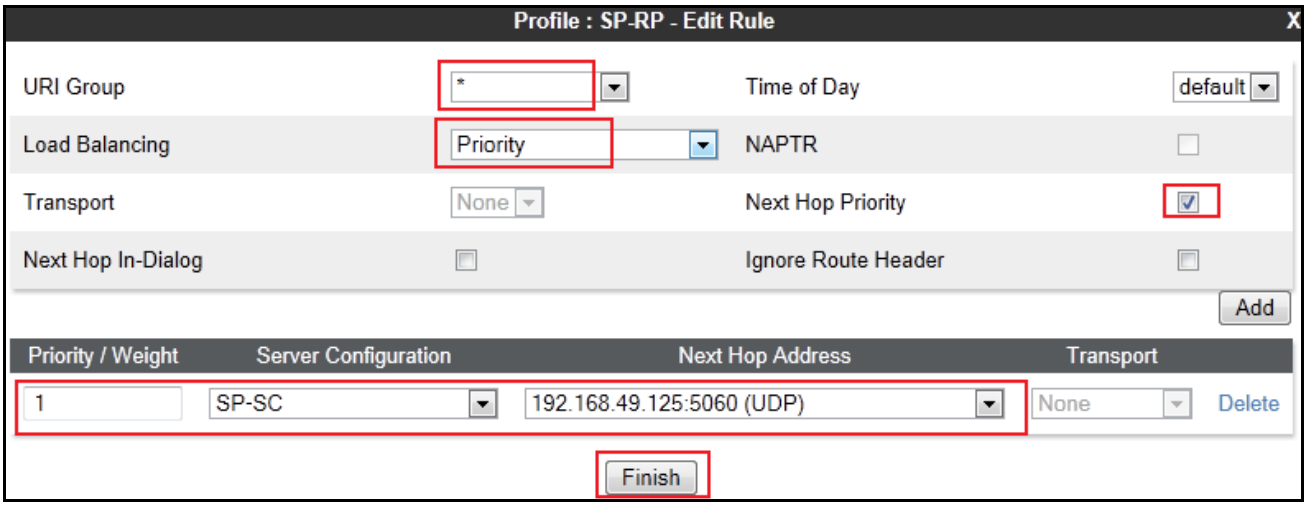
In the compliance testing, Routing profile **SP-SC** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) defined for IP Office. This entry is to route outgoing calls from the enterprise to Windstream.

On the opposite direction, Routing profile **EN-RP** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) defined for Windstream. This entry is to route incoming calls from Windstream to the enterprise.

©2015 Avaya Inc. All Rights Reserved.

6.2.2.1 Routing Profile for Windstream

To display **Edit Routing Rule** dialog of Routing profile **SP-RP**, select **Global Profiles → Routing**: **SP-RP**. As shown in the screenshot below, if there is a match on the SIP domain of the "To" header with the URI Group "*****" defined in **Section 6.2.1**, outgoing calls will be routed to the **Next Hop Server 1** as defined as **192.168.49.125** which is the IP address of Windstream Trunk Server, on port **5060**. As shown in **Figure 1**, Windstream SIP Trunking was connected with transportation protocol **UDP**. The other options were kept as default.



6.2.2.2 Routing Profile for Avaya IP Office

Similarly, Routing profile **EN-RP** was created to route incoming calls to the **Next Hop Server 1** as defined as **10.10.98.113** which is the IP address of IP Office, on port **5060** if there is a match on the SIP domain of the "To" header with the URI Group **"*"** specified in **Section 6.2.1**. As shown in **Figure 1**, IP Office was connected with transportation protocol **UDP**.
To display **Edit Routing Rule** dialog of Routing profile **EN-RP**, select **Global Profiles → Routing**: **EN-RP** then click **Edit** (not shown).

Note: The **Routing Priority based on Next Hop Priority** was checked to use the default settings.

©2015 Avaya Inc. All Rights Reserved.

6.2.3. Topology Hiding

Topology Hiding is a security feature of the Avaya SBCE which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding** then click on the **Add Profile** (not shown).

In the compliance testing, two Topology Hiding profiles were created: **SP-TH** and **EN-TH**.

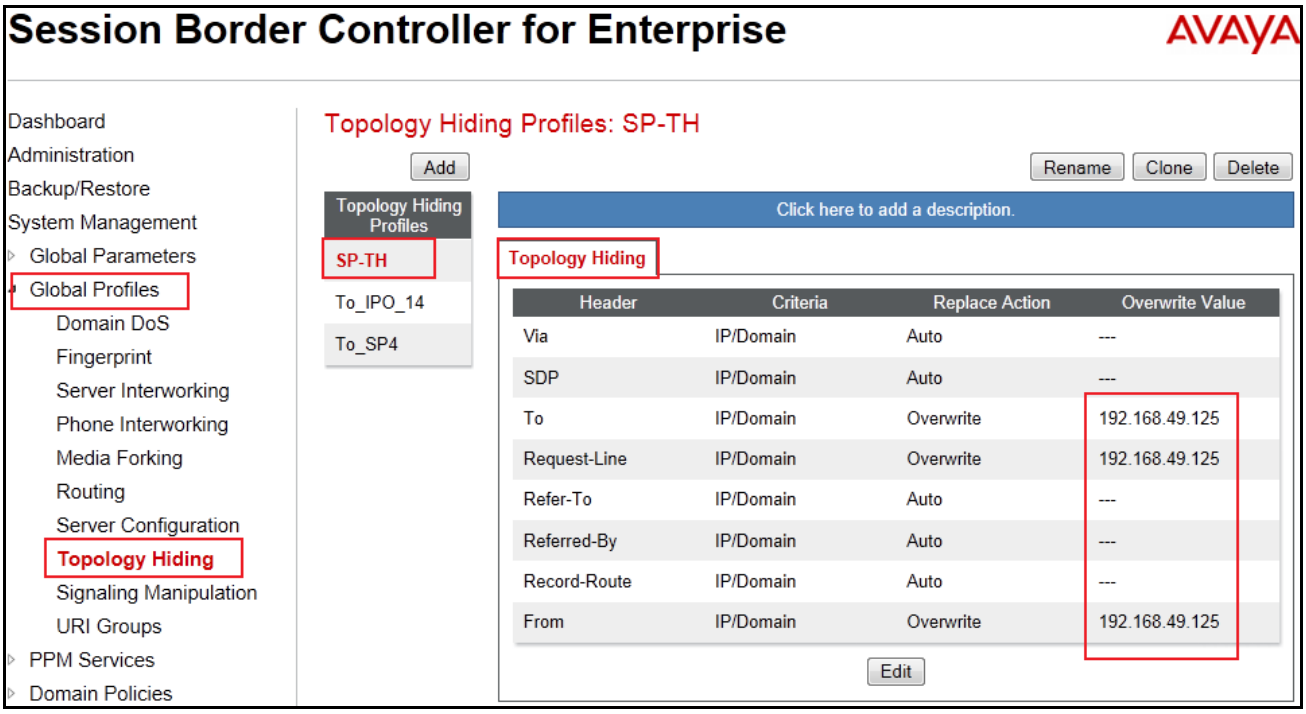
6.2.3.1 Topology Hiding Profile for Windstream

Topology Hiding profile **SP-TH** was defined for outgoing calls to Windstream to:

- Mask URI-Host of the "Request-URI" and "To" headers with service provider SIP domain **192.168.49.125** to meet the requirements of Windstream.
- Mask URI-Host of the "From" header to service provider SIP domain **192.168.49.125.**

This implementation is to secure the enterprise network topology and also to meet the SIP requirements from the service provider.

The screenshots below illustrate the Topology Hiding profile **SP-TH**.



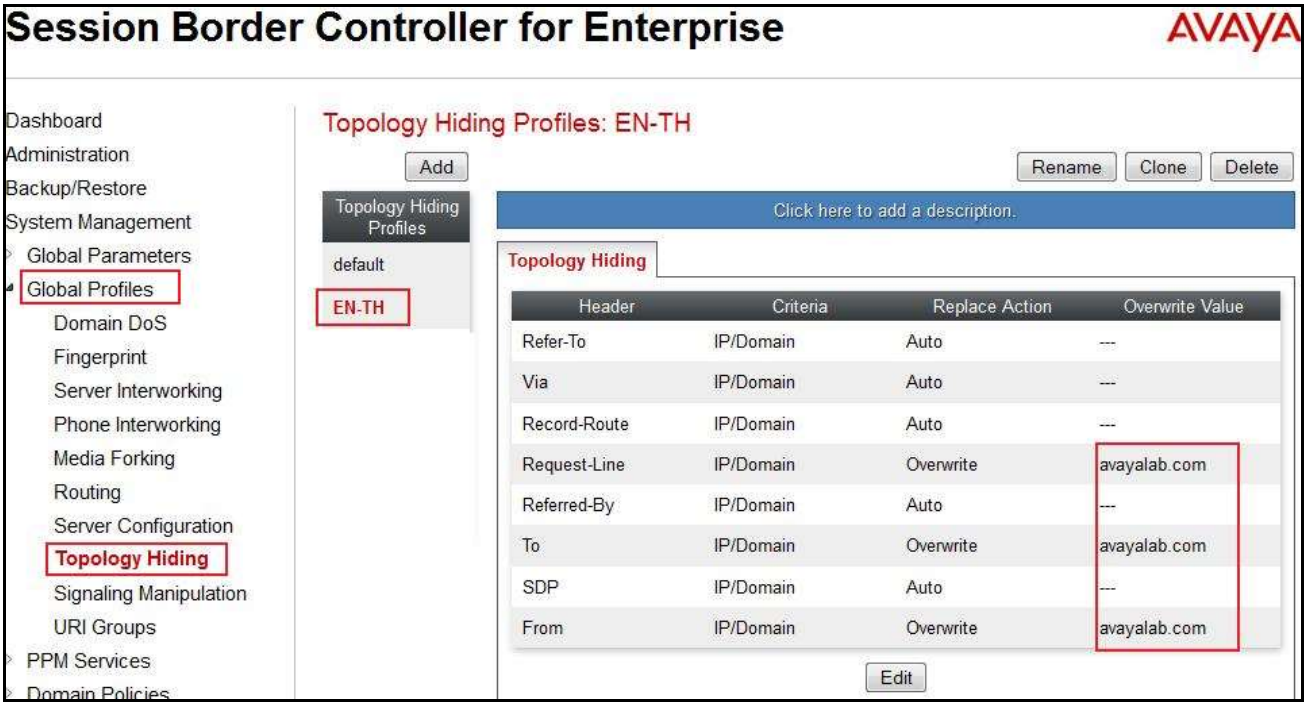
©2015 Avaya Inc. All Rights Reserved.

6.2.3.2 Topology Hiding Profile for IP Office

Topology Hiding profile **EN-TH** was defined for incoming calls to IP Office to:

- Mask URI-Host of the "Request-URI", "To", and "From" headers with the enterprise SIP domain **avayalab.com**.
- Leave the "Record-Route", "Via" headers and SDP to default **Auto**.

The screenshots below illustrate the Topology Hiding profile **EN-TH**.



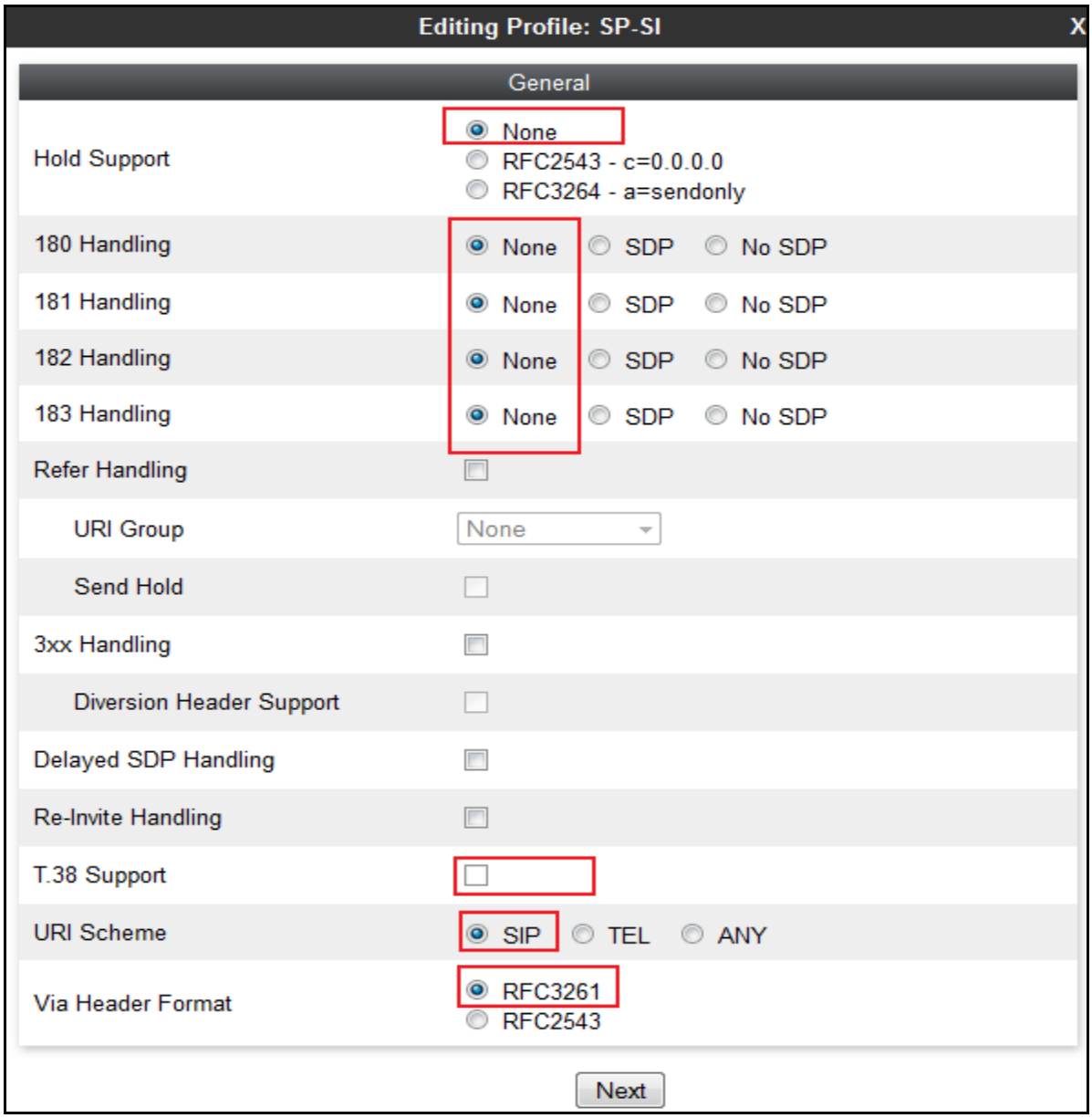
©2015 Avaya Inc. All Rights Reserved.

6.2.4. Server Interworking

The Server Interworking profile features are configured differently for Call Server and Trunk Server. To create a Server Interworking profile, select **Global Profiles → Server Interworking** then click on the **Add Profile** button (not shown). In the compliance testing, two Server Interworking profiles **SP-SI** and **EN-SI** were created for Windstream (Trunk Server) and IP Office (Call Server).

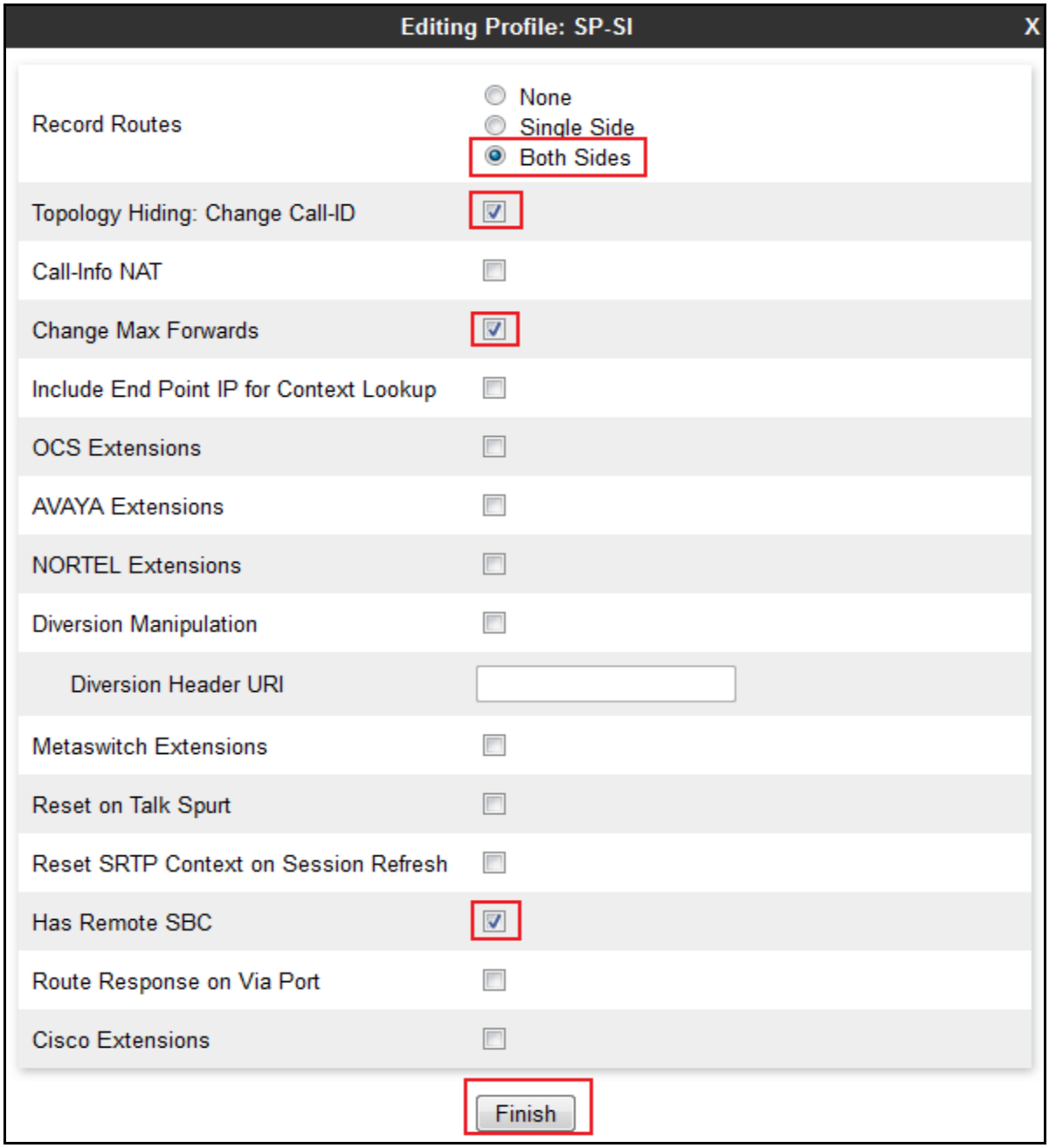
6.2.4.1 Server Interworking Profile for Windstream

Server Interworking profile **SP-SI** was defined to match the specification of Windstream. The **General** and **Advanced** tabs were configured with the following parameters while the other tabs **Timers, URI Manipulation** and **Header Manipulation** were kept as default. **General** settings are being set as shown in capture bellow. Others are left as default.



©2015 Avaya Inc. All Rights Reserved.

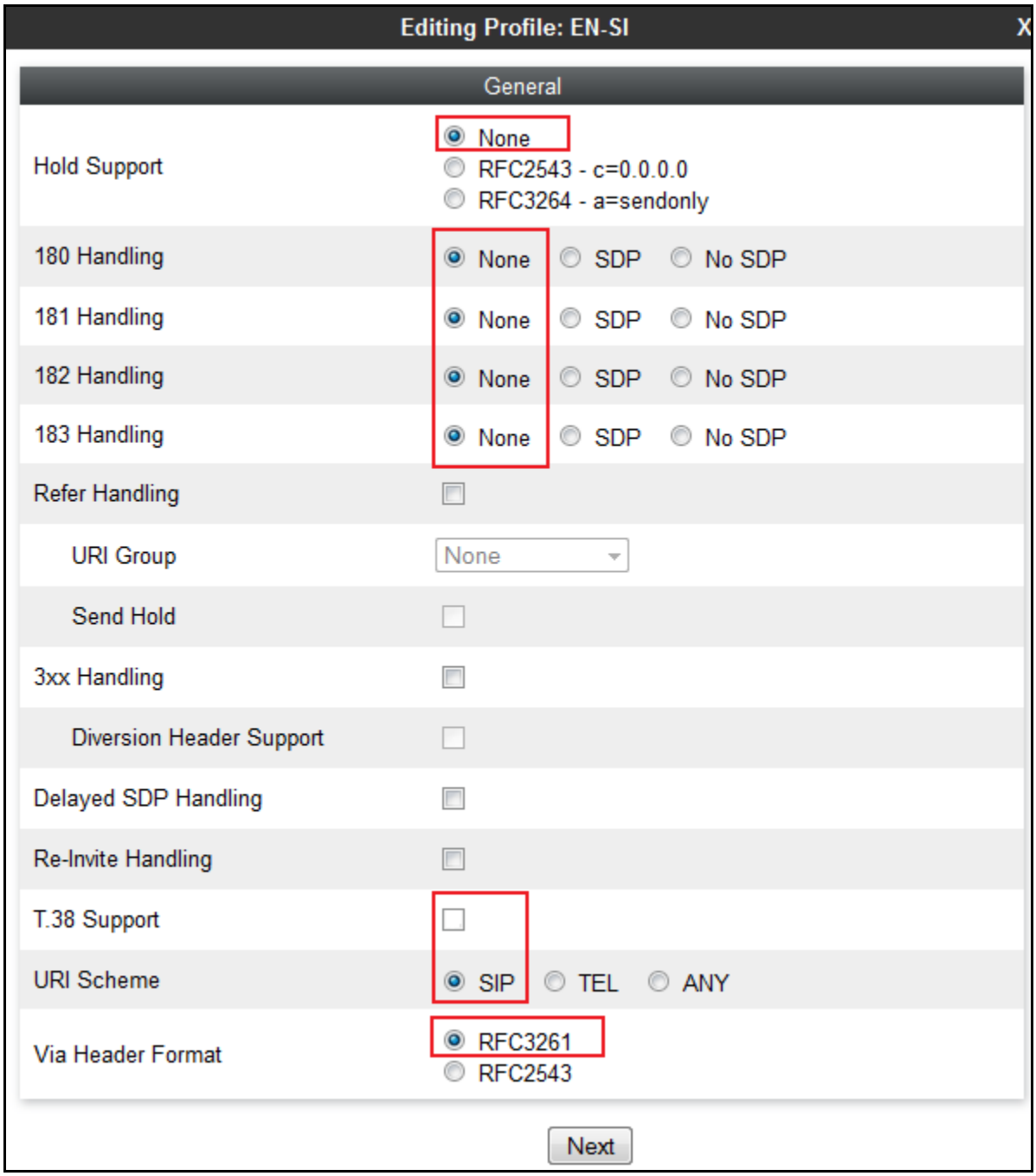
Advanced settings are being set as shown in capture bellow and others are left as default.



©2015 Avaya Inc. All Rights Reserved.

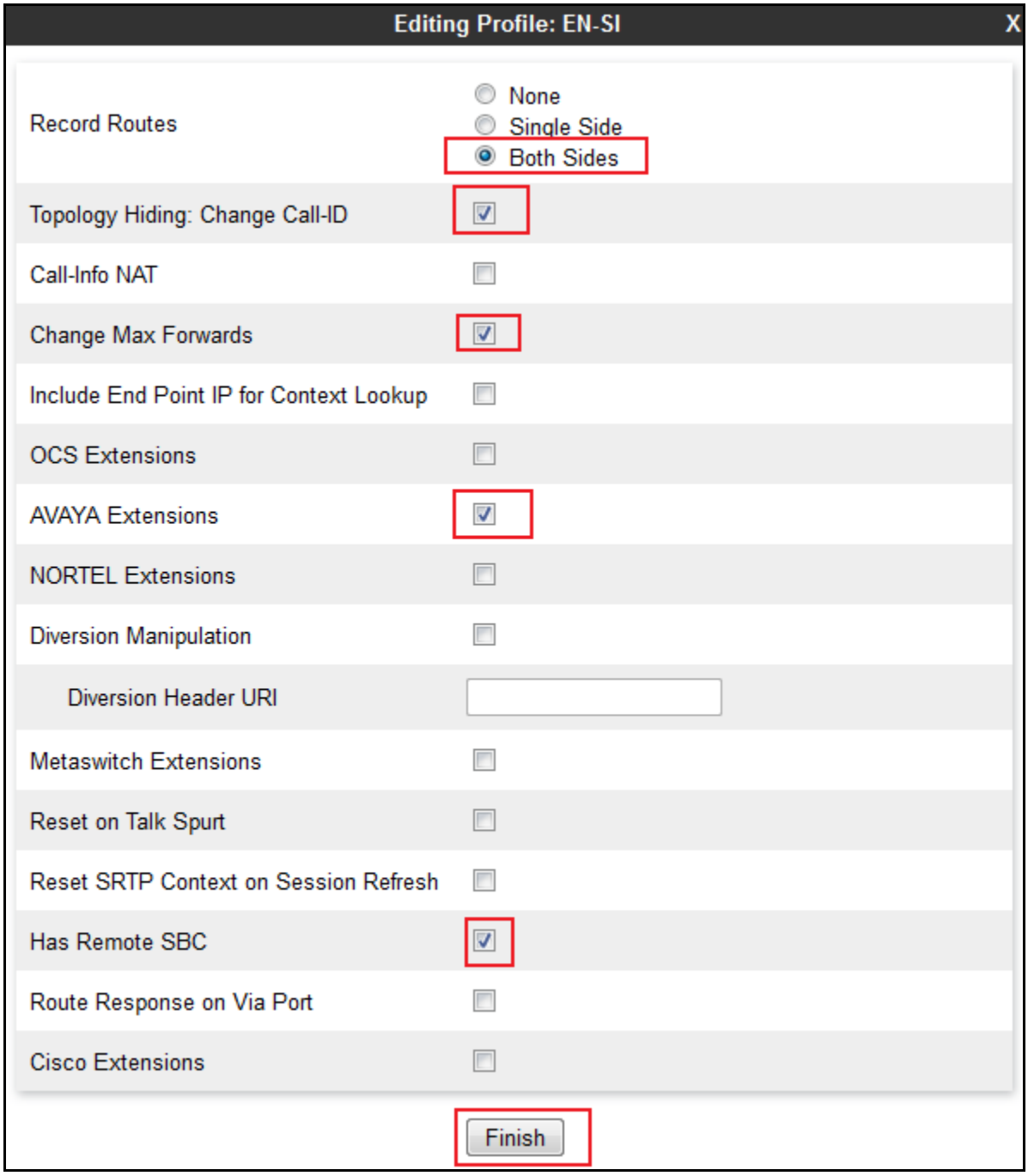
6.2.4.2 Server Interworking Profile for IP Office

Server Interworking profile **EN-SI** shown in the screenshots below, was similarly defined to match the specification of IP Office with the exception of the support for **Avaya Extensions** was enabled. **General** Settings are being set as shown in capture bellow and others are left as default.



©2015 Avaya Inc. All Rights Reserved.

Advanced settings are being set as shown in capture below and others are left as default.



©2015 Avaya Inc. All Rights Reserved.

6.2.5. Server Configuration

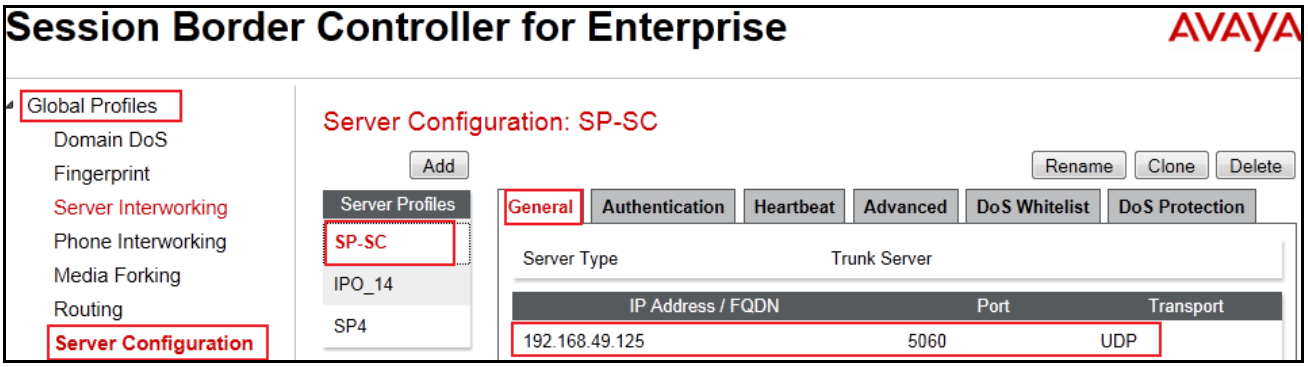
The Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create a Server Configuration entry, select **Global Profiles →Server Configuration** then click on the **Add Profile** button (not shown).

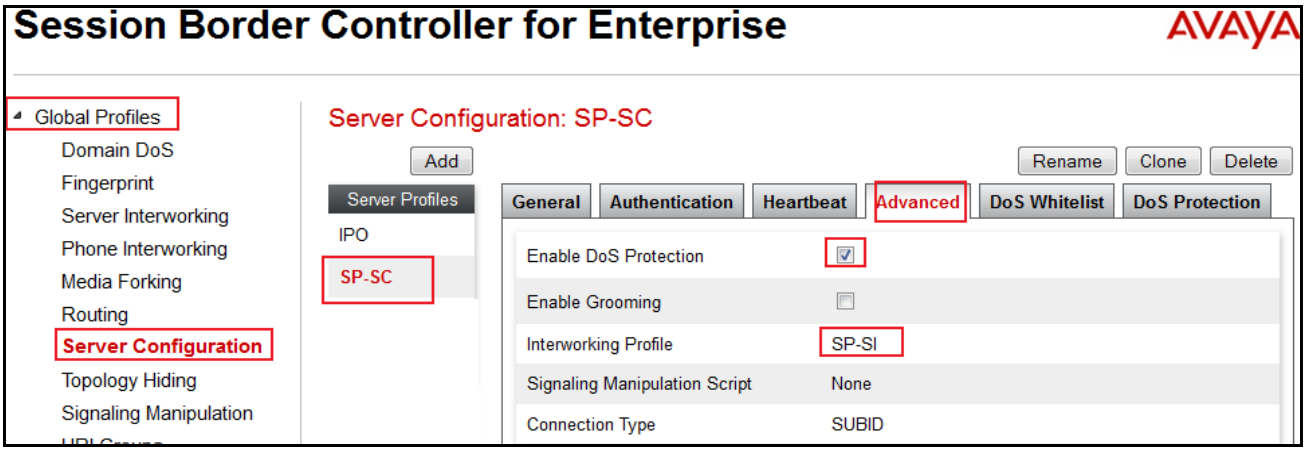
In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for Windstream and server entry **EN-SC** for IP Office.

6.2.5.1 Server Configuration for Windstream

The Server Configuration **SP-SC** was added for Windstream, it is discussed in detail below. The **General** and **Advanced** tabs were provisioned. The **Heartbeat** tab, however, was disabled (default) to allow the Avaya SBCE to forward the OPTIONS heartbeat originated from IP Office to Windstream, to query for the status of the SIP Trunk. The **Authentication** tab was also kept disabled (default). The **General** setting for Server Configuration **SP-SC** is being set as shown in the following capture.



The **Advanced** setting is being set as shown in capture. Where the **SP-SI** Interworking Profile is selected as defined in **Section 6.2.4.1.**

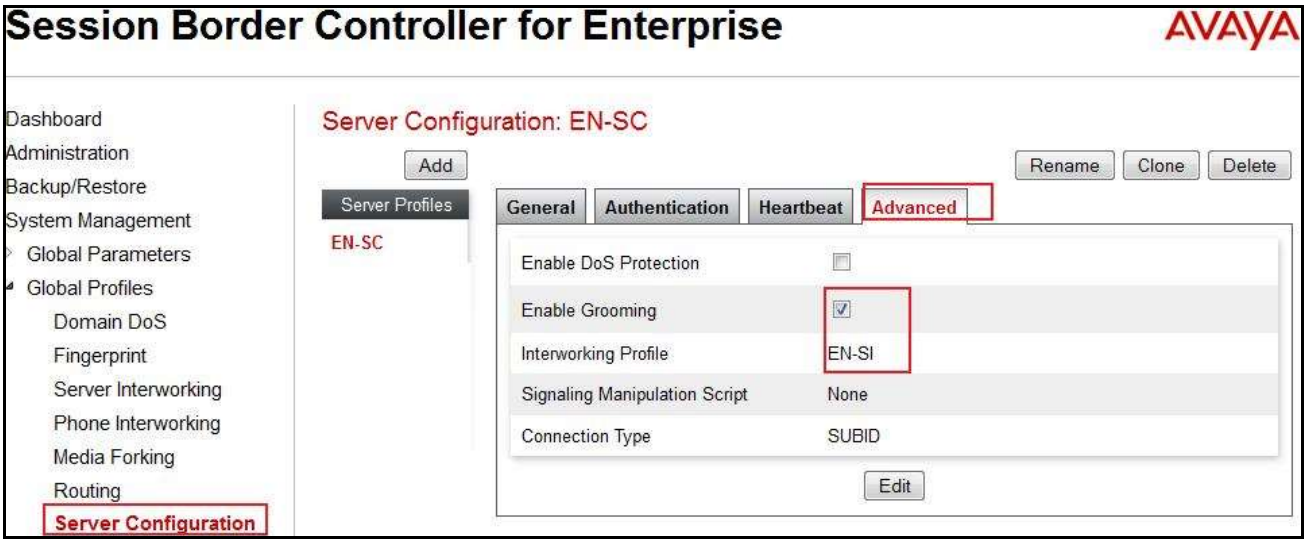


©2015 Avaya Inc. All Rights Reserved.

6.2.5.2 Server Configuration for Avaya IP Office

The Server Configuration **EN-SC** was similarly created for IP Office. It is discussed in detail below. Only the **General** and **Advanced** tabs required provisioning. The **Heartbeat** tab was kept disabled (default) to allow the Avaya SBCE to forward the OPTIONS heartbeat from Windstream, to IP Office, to query for the status of the SIP Trunk. The **General** setting for Server Configuration **EN-SC** is being set as shown in the following capture.

The **Advanced** setting is set, as shown in the following capture. The **EN-SI** Interworking Profile is selected as defined in **Section 6.2.4.2.**



©2015 Avaya Inc. All Rights Reserved.

6.3. Domain Policies

The Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

6.3.1. Signaling Rules

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

To clone a signaling rule, navigate to **Domain Policies → Signaling Rules**, select the **default** rule then click on the **Clone Rule** button (not shown).

In the compliance testing, two **Signaling Rules** were created for Windstream and IP Office.

6.3.1.1 Signaling Rule for Windstream

Cloning the Signaling Rule **default** with a descriptive name e.g. **SP-SR** and click on the **Finish** button (not shown). Verify that **General** settings of **SP-SR** with **Inbound** and **Outbound Request** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** (not shown).

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for signaling.

The following screen shows the QoS value used for the compliance testing.

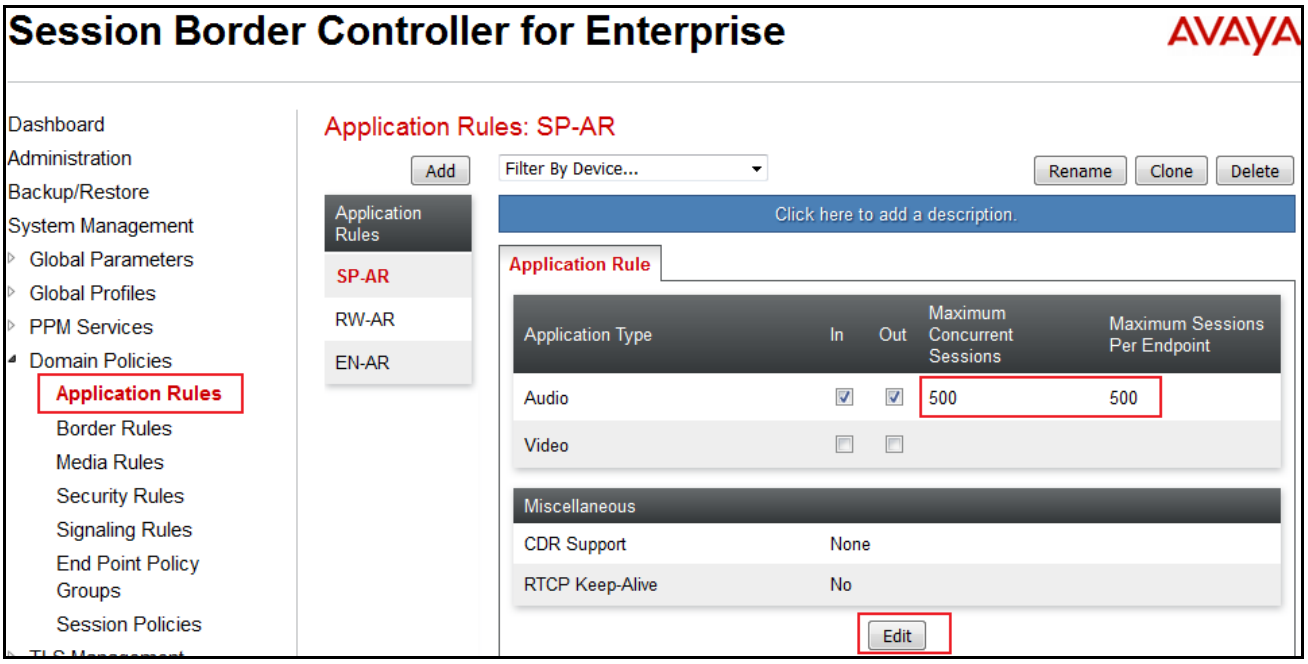
©2015 Avaya Inc. All Rights Reserved.

6.3.1.2 Signaling Rule for IP Office

Cloning the Signaling Rule **default** with a descriptive name e.g. **EN-SR** for IP Office and click on the **Finish** button (not shown). Verify that **General** settings of **EN-SR** with **Inbound** and **Outbound Request** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** (not shown). Similarly the Signaling QoS rules are set as shown in Figure below.

6.3.1.3 Application Rule for Windstream

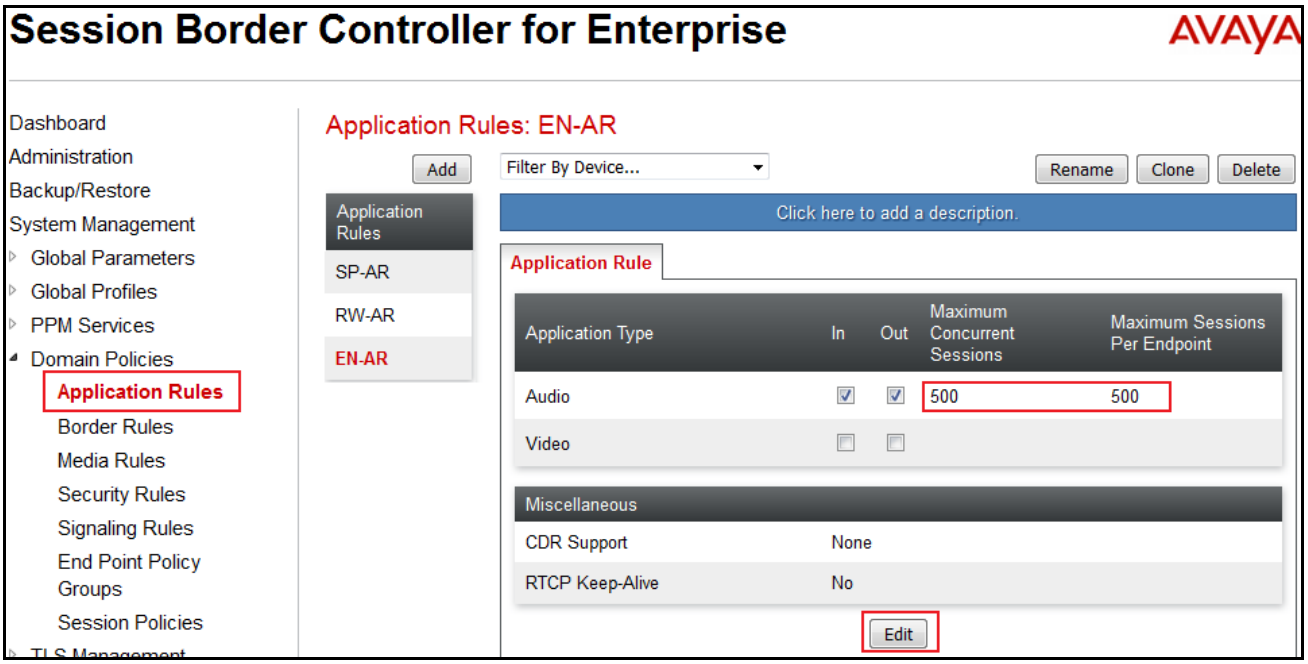
Cloning the Application Rule default with a descriptive name e.g. SP-AR for service provider and click Edit button to change value of Maximum Concurrent Sessions and Maximum Session Per Endpoint to 500 respectively as shown and then click Finish button (not shown).



©2015 Avaya Inc. All Rights Reserved.

6.3.1.4 Application Rule for IP Office

Cloning the Application Rule default with a descriptive name e.g. EN-AR for IP Office and click Edit button to change value of Maximum Concurrent Sessions and Maximum Session Per Endpoint to 500 respectively as shown and then click Finish button (not shown).



©2015 Avaya Inc. All Rights Reserved.

6.3.2. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to Server Flow defined in **Section 6.4.4**.

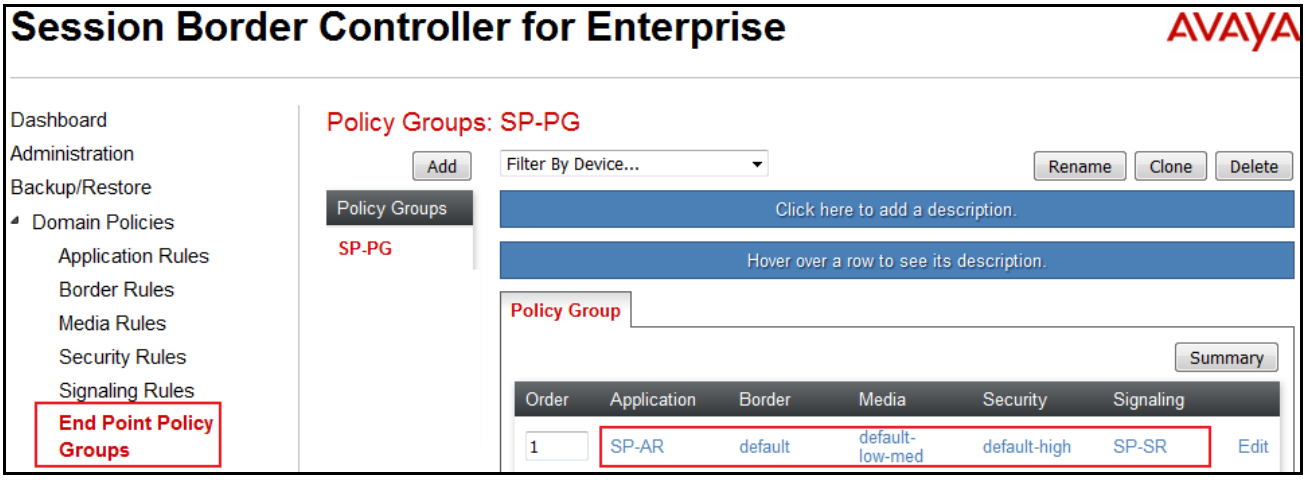
Endpoint Policy Groups were separately created for Windstream and IP Office.

To create a policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on the **Add Group** button (not shown).

6.3.2.1 Endpoint Policy Group for Windstream

The following screen shows **SP-PG** created for Windstream.

- Set Application Rule to **SP-AR** which was created in **Section 6.3.1.3.**
- Set Media Rule to **default-low-med**.
- Set Signaling Rule to **SP-SR** which was created in **Section 6.3.1.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.

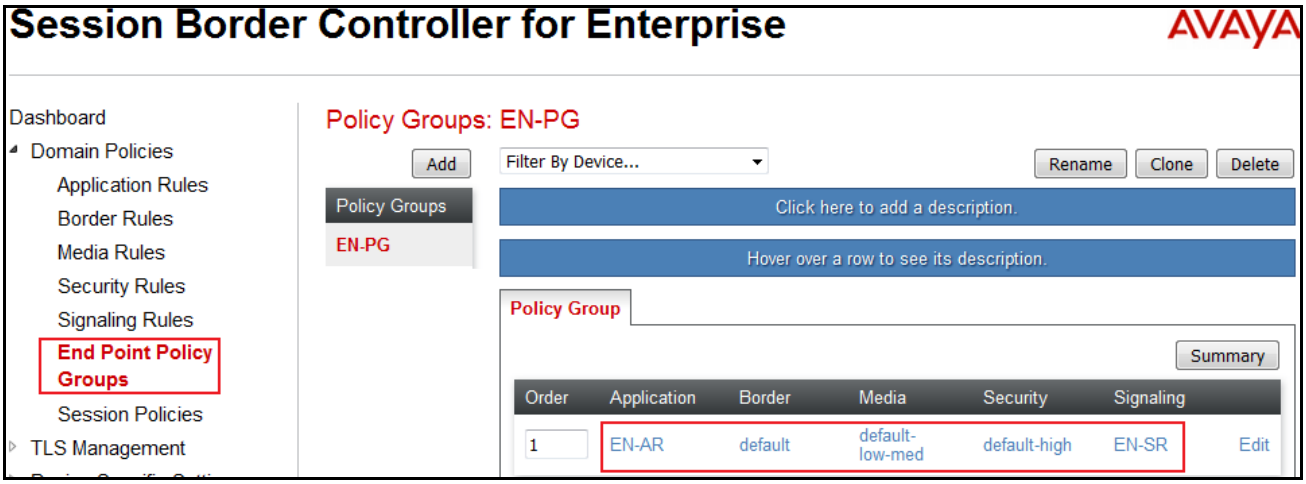


©2015 Avaya Inc. All Rights Reserved.

6.3.2.2 Endpoint Policy Group for IP Office

The following screen shows policy group **EN-PG** created for IP Office.

- Set Application Rule to **EN-AR** which was created **in Section 6.3.1.4.**
- Set Media Rule to **default-low-med**.
- Set Signaling Rule **EN-SR** which was created in **Section 6.3.1.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-high**.



©2015 Avaya Inc. All Rights Reserved.

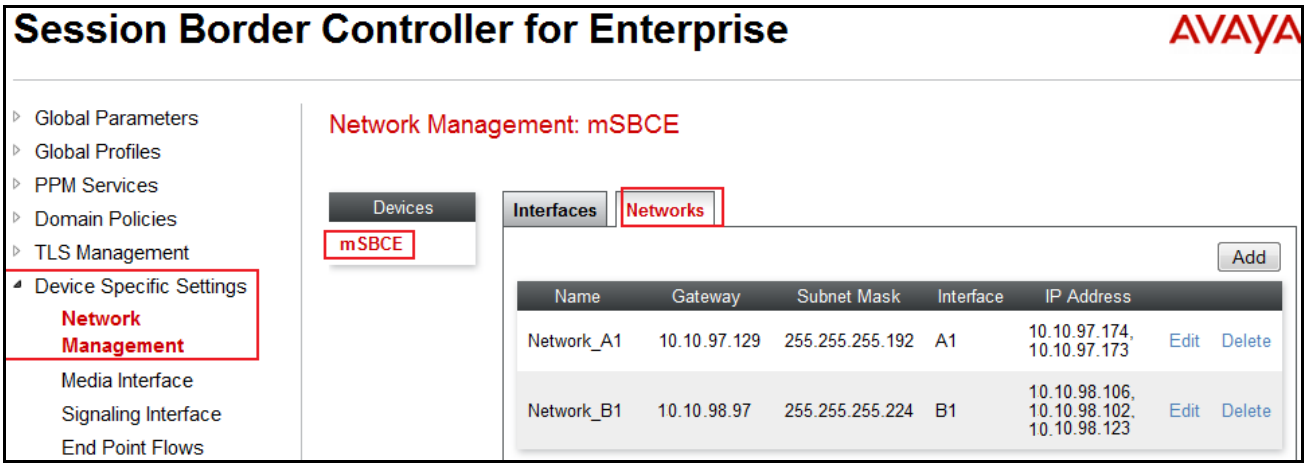
6.4. Device Specific Settings

The Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

6.4.1. Network Management

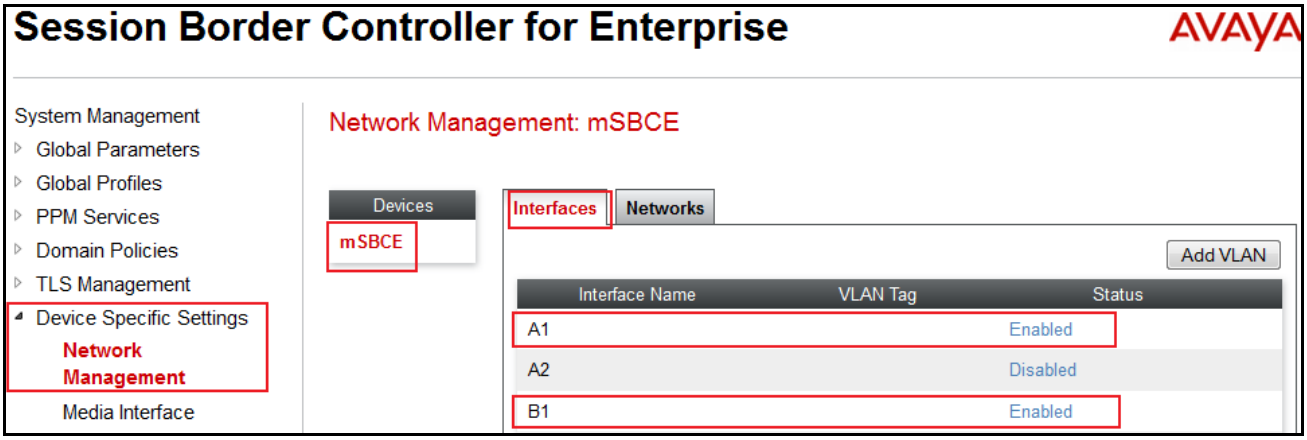
The Network Management page is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address, public IP address, subnet mask, gateway, etc. to interface the device to the networks. This information populates the various Network Management tabs which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Networks**, under **Networks** tab and verify the IP addresses assigned to the interfaces and that the interfaces were enabled. The following screen shows the private interface was assigned to **A1** and the public interface was assigned to **B1** appropriate to the parameters shown in the **Figure 1**.



©2015 Avaya Inc. All Rights Reserved.

On the **Interfaces** tab, enable the interfaces connecting to the inside enterprise and outside service provider networks. To enable an interface, click on "Disable" Status. The following screen shows interface **A1** and **B1** were **Enabled**.



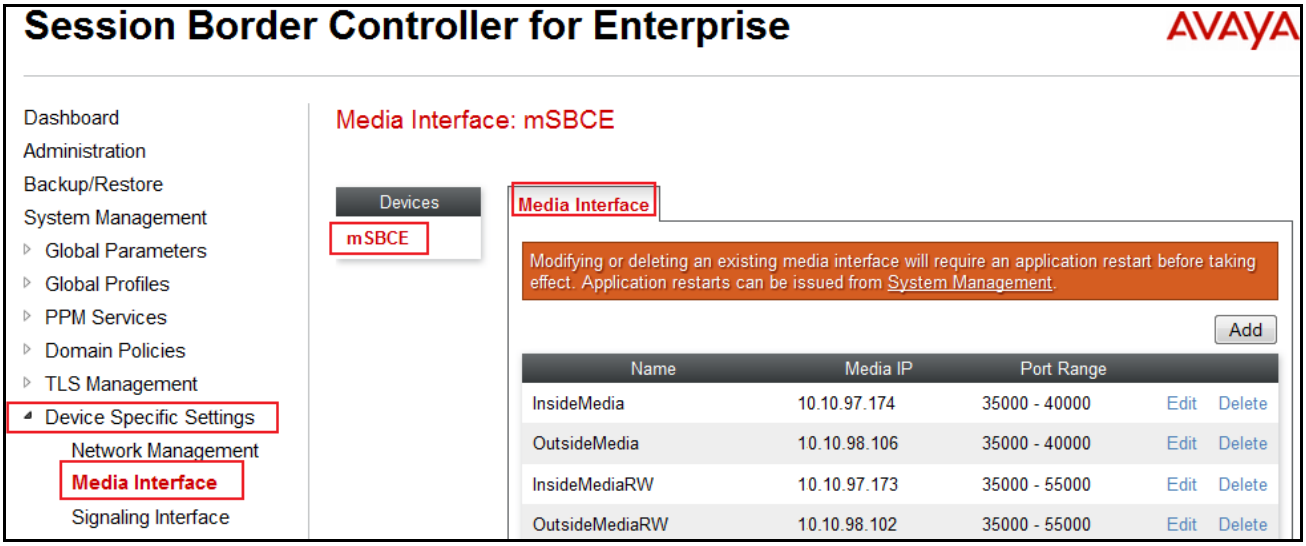
6.4.2. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will open connection for RTP traffic on the defined ports.

To create a new **Media Interface**, navigate to **Device Specific Settings → Media Interface** and click on the **Add Media Interface** button (not shown).

Two separate Media Interfaces are needed for both the inside and outside interfaces. The following screen shows the Media Interfaces **InsideMedia** and **OutsideMedia** were created for the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.



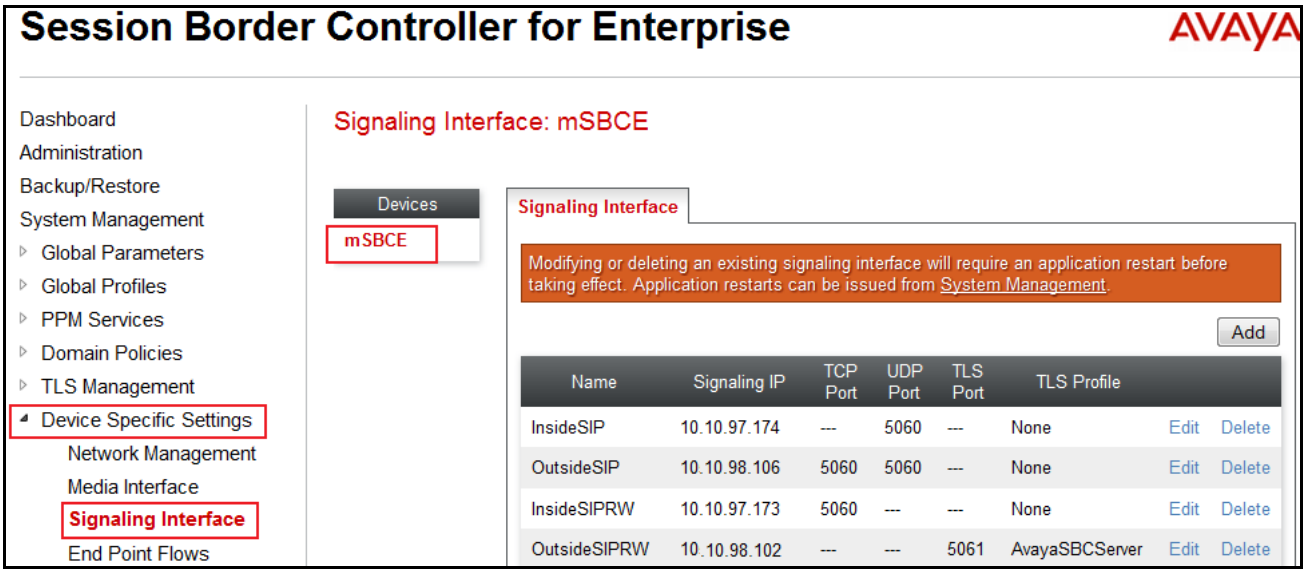
©2015 Avaya Inc. All Rights Reserved.

6.4.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

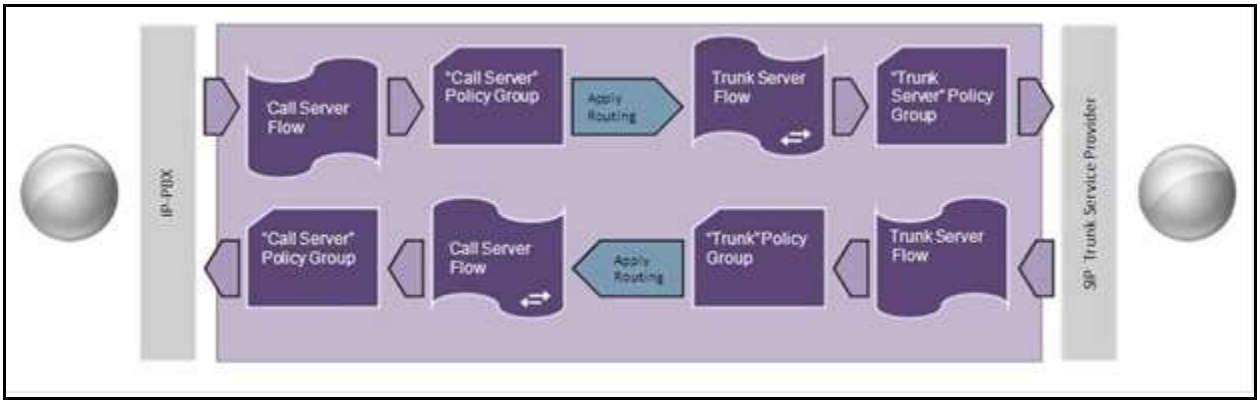
To create a new **Signaling Interface**, navigate to **Device Specific Settings → Signaling Interface** and click on the **Add Signaling Interface** button (not shown).

Two separate Signaling Interfaces are needed for both inside and outside interfaces. The following screen shows the Signaling Interfaces **InsideSIP** and **OutsideSIP** were created in the compliance testing with **UDP/5060** configured for inside and outside interfaces.



6.4.4. End Point Flows - Server Flow

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



©2015 Avaya Inc. All Rights Reserved.

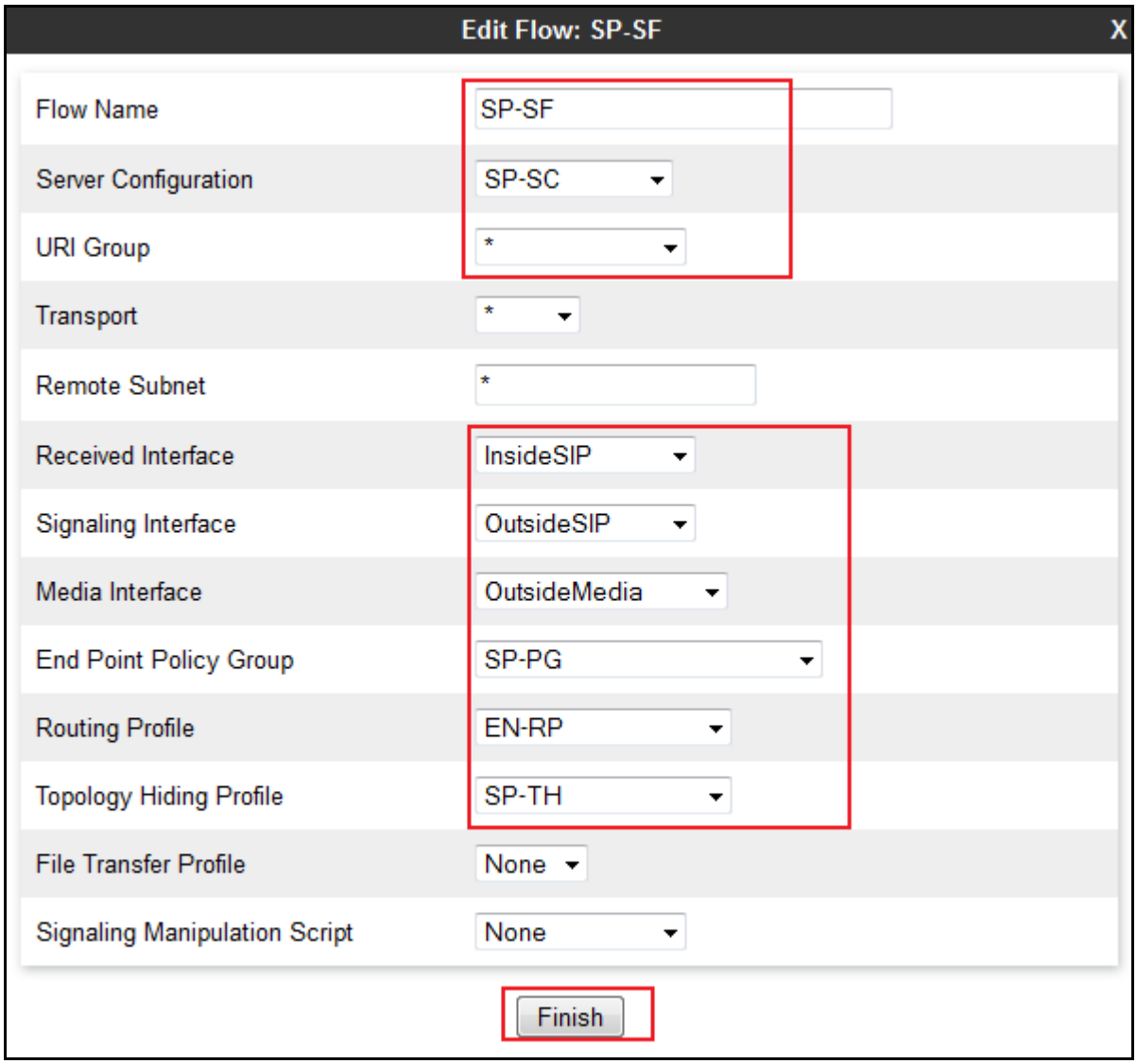
In the compliance testing, two separate Server Flows were created for Windstream and IP Office.

To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the other fields were kept as default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select Server Configuration created in **Section 6.2.5.1** which the Server Flow associates to.
- **URI Group**: Select "*****".
- **Received Interface**: Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface**: Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to send the SIP signaling to.
- **Media Interface**: Select the Media Interface created in **Section 6.4.2** which is the Server Configuration is designed to send the RTP to.
- **End Point Policy Group**: Select the End Point Policy Group created in **Section 6.3.2.1**.
- **Routing Profile**: Select the Routing Profile created in **Section 6.2.2.2**.
- **Topology Hiding Profile**: Select the Topology Hiding profile created in **Section 6.2.3** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

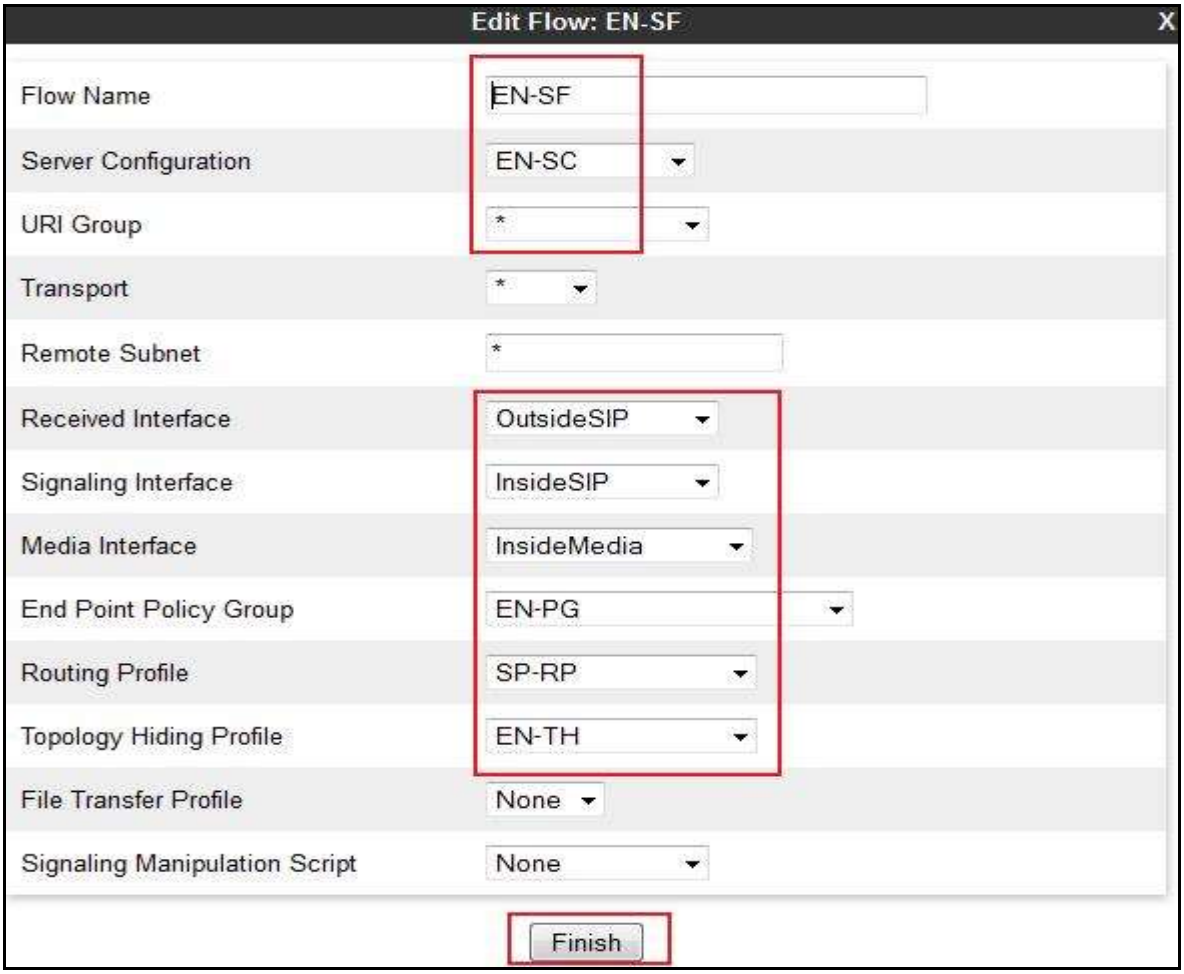
©2015 Avaya Inc. All Rights Reserved.

The following screen shows the Server Flow **SP-SF** for Windstream.



©2015 Avaya Inc. All Rights Reserved.

Similarly, the following screen shows the Server Flow **EN-SF** for IP Office.



6.4.5. Session Flows

The Session Flows feature allows defining certain parameters that pertain to the media portions of a call, whether it originates from the enterprise or outside the enterprise. This feature provides the complete and unparalleled flexibility to monitor, identify and control very specific types of calls based upon these user-definable parameters. Session Flows profiles SDP media parameters, to completely identify and characterize a call placed through the network.

A common Session Flow **SP-SF** was created for both the Windstream and IP Office.

To create a Session Flow, navigate to **Device Specific Settings → Session Flows** then click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the remaining fields were kept as default.

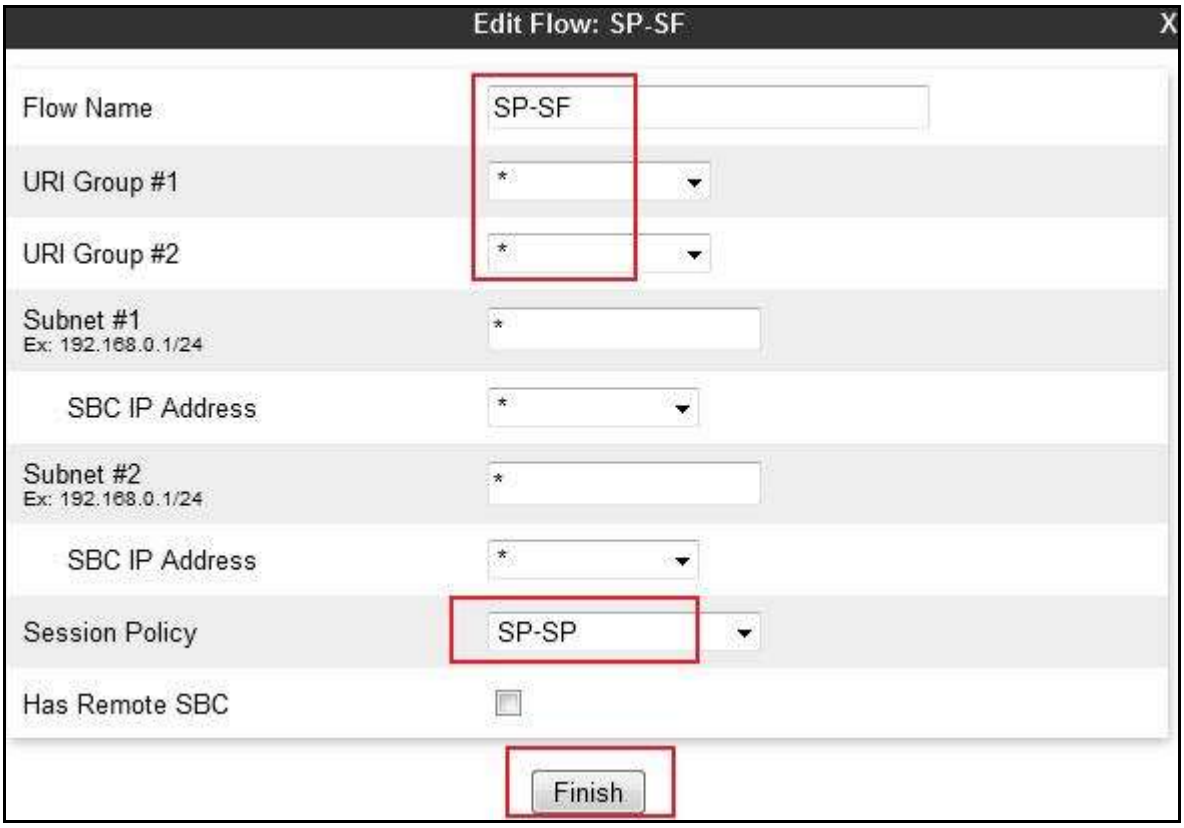
- **Flow Name**: Enter a descriptive name.
- **URI Group #1**: Select the URI Group **"*"**.
- **URI Group #2**: Select the URI Group **"*"**.
- **Session Policy**: Select the Session Policy **SP-SP**, which is clone from **default** (not shown), to assign to the Session Flow.

©2015 Avaya Inc. All Rights Reserved.

- Click on the **Finish** button.

Note: A unique URI Group is used for source and destination, since it contains multiple URIs defined for the source as well as for the destination.

The following screen shows the Session Flow named **SP-SF**.



7. Windstream SIP Trunking Configuration

Windstream is responsible for the configuration of Windstream SIP Trunking service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise, this address will be the outside interface of the Avaya SBCE. Windstream will provide the customer the necessary information to configure the Avaya IP Office SIP connection to Windstream. The provided information from Windstream includes:

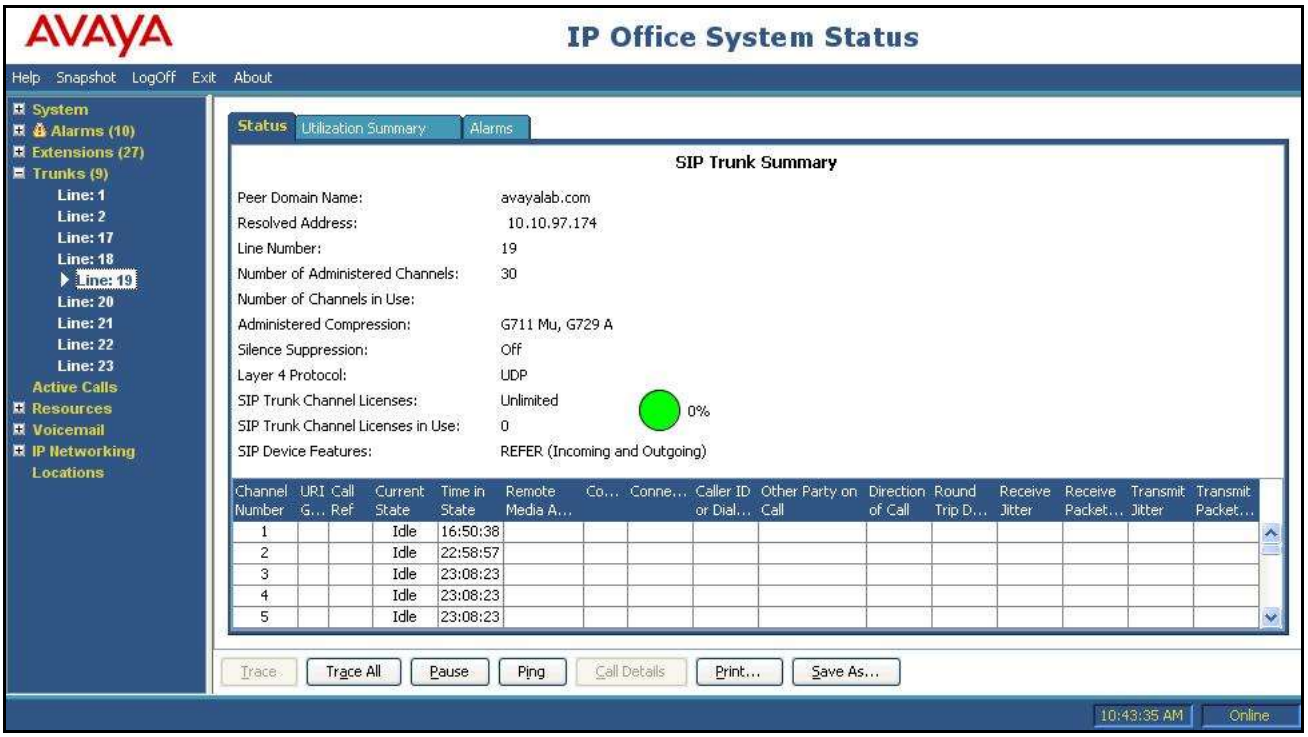
- IP address of the Windstream SIP proxy.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.

©2015 Avaya Inc. All Rights Reserved.

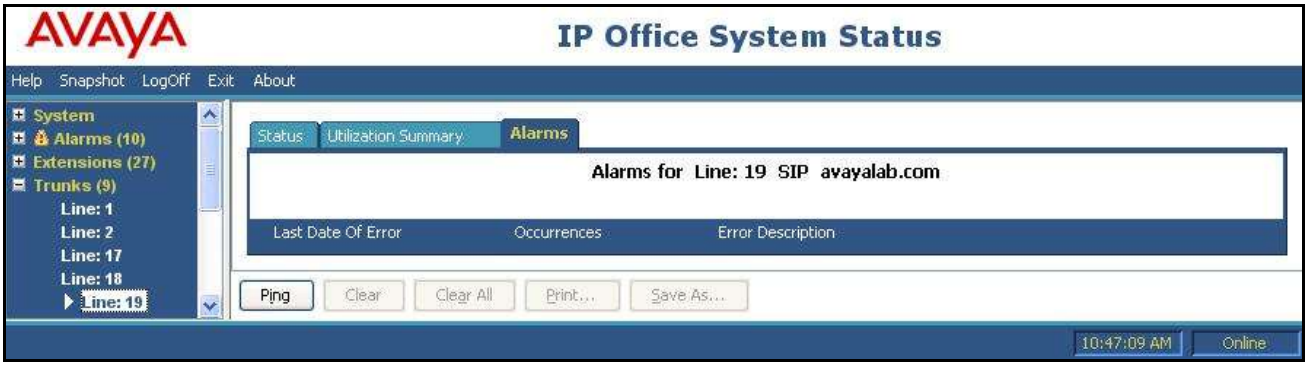
8. Verification Steps

The following steps may 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 Avaya IP Office Manager was 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).



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



- Verify that a phone connected to PSTN can successfully place a call to the Avaya IP Office with two-way audio.
- Verify that a phone connected to Avaya IP Office can successfully place a call to the PSTN with two-way audio.

©2015 Avaya Inc. All Rights Reserved.

- Using a network sniffing tool e.g. Wireshark to monitor the SIP signaling between the enterprise and Windstream. The sniffer traces are captured at the public interface of the Avaya SBCE.

9. Conclusion

The Windstream SIP Trunking passed compliance testing. These Application Notes describe the procedures required to configure the SIP connection between Avaya IP Office, Avaya SBCE and the Windstream SIP Trunking service as shown in **Figure 1**.

©2015 Avaya Inc. All Rights Reserved.

10. Additional References

[1] *IP Office 9.1 Administering Avaya IP Office Platform with Manager*, Release 9.1.0, Issue 10.11, May 2015.
[2] *Administering Avaya IP Office™, Platform Voicemail Pro IP Office™ Platform 9.115-601063*, Issue 10c - (09 December 2014).
Additional Avaya IP Office information can be found at:
[3] http://marketingtools.avaya.com/knowledgebase/
[4] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 5, October 2015.
[5] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2015.
[6] *Application Notes for configuring Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers*– Issue 1.0

Product documentation for Avaya products may be found at http://support.avaya.com. Additional IP Office documentation can be found at:
http://marketingtools.avaya.com/knowledgebase/

Product documentation for Windstream SIP Trunking is available from Windstream.

©2015 Avaya Inc. All Rights Reserved.

11. Appendix – Remote Worker Configuration via Avaya SBCE

This section describes the process for connecting select remote Avaya SIP endpoints on the public Internet to Avaya IP Office on the private enterprise network via the Avaya SBCE. The provisioning builds on the reference configuration described in previous sections of this document.

For more information on how to provision the of ***Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.3 to support Remote Workers,*** refer to reference [6].

Note – This Remote Worker configuration is based on provisioning the Avaya SBCE. It is not to be confused with "native" Avaya IP Office Remote Worker configurations.

In the configuration for the compliance test, Avaya Communicator for Windows was used as the Remote Worker SIP endpoint.

The reference configuration for the compliance test, including the Remote Worker endpoint, is shown in **Figure 1** in **Section 3**. Internet access by the Remote Worker endpoint is through a Router/NAT/Firewall/Default Gateway provided by the Bell Internet Service located between the Remote Worker private LAN and the public Internet. The Bell router also provides DHCP functionality in the private space. Note that the use of the Bell router is for functionality testing only and is not prescriptive.

Provisioning of the Bell router is beyond the scope of this document.

©2015 Avaya Inc. All Rights Reserved.

©2015 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.