Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Line Systems SIP Trunk Service with Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 7.0- Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Line Systems and Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 7.0.

Line Systems SIP Trunk Service (Line Systems) provides PSTN access via a SIP trunk between the enterprise and the Line Systems 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.

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

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between Line Systems and Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of an Avaya IP Office 500v2 Release 9.1, Avaya embedded Voicemail, Avaya IP Office Application Server (with WebRTC and one-X Portal services enabled), Avaya Communicator for Windows (SIP), Avaya Communicator for Web, Avaya H.323, Avaya SIP, digital and analog endpoints. The enterprise solution connects to the Line Systems network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

The Line Systems 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 connecting to Line Systems via Avaya SBCE.
This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**. Note: NAT devices added between Avaya IP Office and the Line Systems network should be transparent to the SIP signaling.

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

2.1. Interoperability Compliance Testing

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

- 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 from/to the Avaya Communicator for Windows (SIP).
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Web (WebRTC) with basic telephony features (transfer/hold).
- Inbound and outbound long hold time call stability.
- Various call types including: local, long distance, international call, outbound toll-free, inbound toll-free, 411, and 911 services.
- Codec G.729A and G.711MU.

- Caller number/ID presentation.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- Telephony features such as hold and resume, transfer, and conference.
- FAX using T.38 and G.711 pass-through.
- Off-net call forwarding.
- Twinning to mobile phones on inbound calls.
- Authentication.
- Use both of the SIP re-Invite and SIP Refer method for network redirection (transferring/ forwarding calls with the PSTN back to another PSTN).
- Remote Worker (using Avaya Communicator for Windows (SIP)) which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Item not supported include the following:

- Line Systems does not support the outbound calls to Assisted Operator during the compliance testing.

2.2. Test Results

Interoperability testing of Line Systems was completed with successful results for all test cases with the exception of the limitation described below:

- **Blind Call Transfer using Avaya 1140E SIP phone did not complete until transferee picked up the call** - The expected behavior of the SIP phone was after transferring, the phone should display "Transfer successful". But in this case, user pressed "Trnsfr" button, answered question of "Consult with party?", and the answer was "No", which implied the blind transfer, the transferee phone was ringing and the SIP phone should be released and displayed "Transfer successful". Instead, the SIP phone was still displayed "Transferring" and not released until the transferee phone answered the call. This is very minor known limitation on Avaya 1140E SIP phone. There was no user impact. Transfer was still completed with 2-way audio.

2.3. Support

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

For technical support on the Line Systems SIP Trunk Service, please contact customer service at 1-888-808-6111 or visit: http://www.linesystems.com/services/voice/.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to Line Systems 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.

The Avaya components used to create the simulated customer site including:

- Avaya IP Office 500v2.
- Avaya micro Session Border Controller for Enterprise.
- Avaya embedded Voicemail for IP Office.
- Avaya Application Server (Enabled WebRTC and one-X Portal services)
- Avaya 9600 Series IP Deskphones (H.323).
- Avaya 11x0 Series IP Deskphones (SIP).
- Avaya 1408 Digital phones.
- Avaya Analog phones.
- Avaya Communicator for Windows (SIP).
- Avaya Communicator for Web (WebRTC)
- Avaya Communicator for Windows (SIP) for remote worker

Located at the enterprise site is an Avaya IP Office 500v2 with the MOD DGTL STA16 expansion module which provides connections for 16 digital stations to the PSTN, and 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 LAN2 port of Avaya IP Office is connected to Avaya SBCE. A separate Windows XP PC runs Avaya IP Office Manager to configure and administer Avaya IP Office.

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

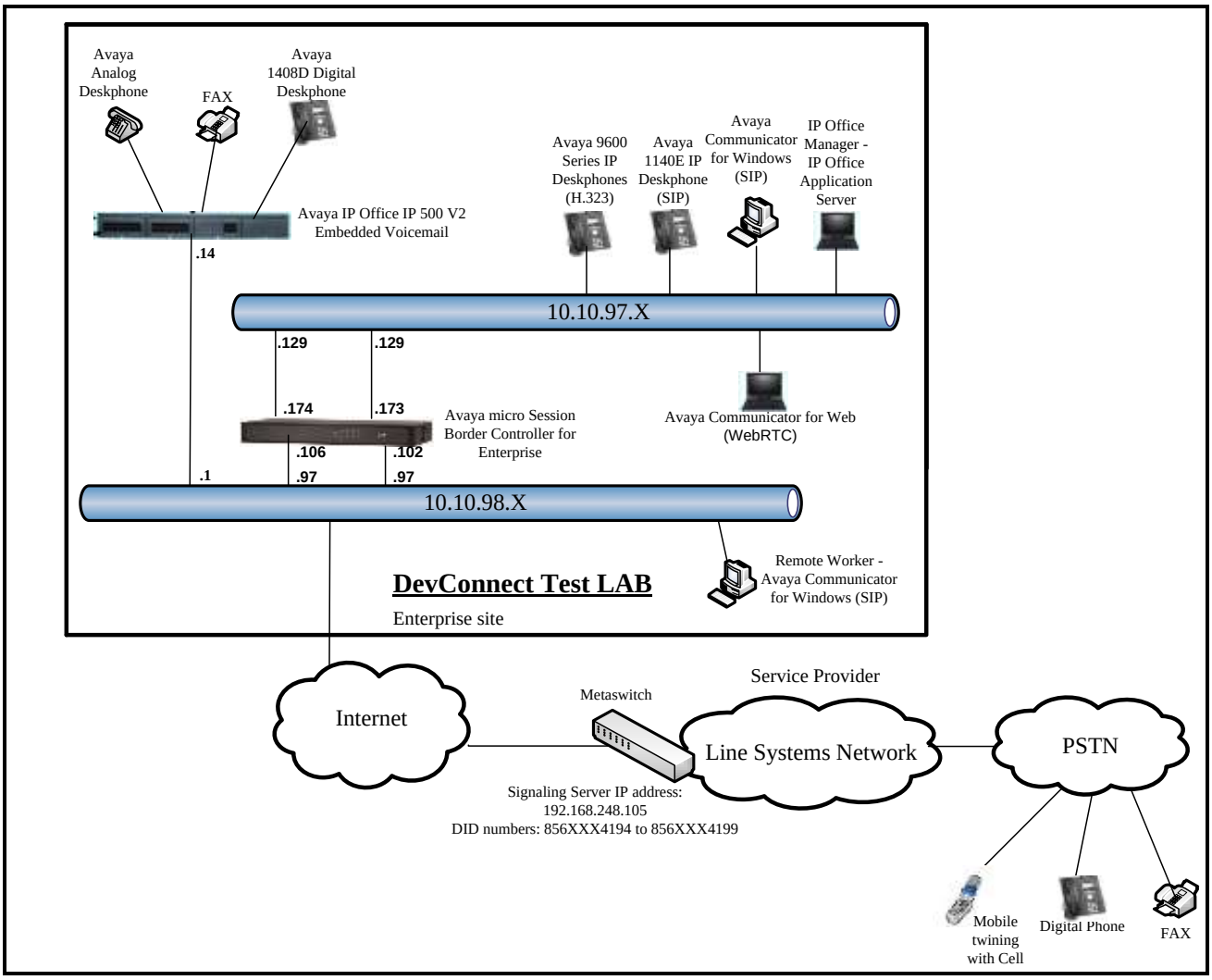

Figure 1: Test Configuration for Avaya IP Office with Line Systems SIP Trunk Service

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 6 + N digits to send digits across the SIP trunk to Line Systems. The short code of 6 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Line Systems. 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, Line Systems sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the Avaya IP Office such as data firewall. 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 Avaya IP Office 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 provided:

Component	Version
Avaya	
Avaya IP Office solution: Avaya IP Office 500v2 Embedded Voicemail Avaya IP Office Analogue PHONE 8 Avaya IP Office VCM64/PRID U Avaya IP Office DIG DCPx16 V2 Avaya IP Office Manager Avaya IP Office Application Server Avaya Web RTC Gateway Avaya one-X Portal	 9.1.5.0.145 9.1.5.0.145 9.1.5.0.145 9.1.5.0.145 9.1.5.0.145 9.1.5.0.145 9.1.4.0.137 9.1.4.0.102 9.1.4.0.24
Avaya micro Session Border Controller for Enterprise	7.0.1.03-8739
Avaya 1140E IP Deskphone (SIP)	04.04.18.00
Avaya IP 9641G	6.6029
Avaya IP 9621G	6.6029
Avaya Communicator for Windows (SIP)	2.0.3.33
Avaya Communicator for Web	1.0.16.1217
Avaya 1408D Digital Deskphone	R40
Avaya Analog Deskphone	N/A
HP Officejet 4500 (fax)	N/A
Service Provider	
Metaswitch's Perimeta Session Border Controller (SBC)	8.3.11

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 without T.38 Fax Service.

5. Configure Avaya IP Office

This section describes the Avaya IP Office solution configuration necessary to support connectivity to the Avaya SBCE. It is assumed that the initial installation and provisioning of the Avaya IP Office has been previously completed and therefore is not covered in these Application Notes. For information on the installation, refer to Additional References **Section 10**.

This section describes the Avaya IP Office configuration to support connectivity to Avaya SBCE. Avaya IP Office is configured through the Avaya IP 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** (not shown), select the proper Avaya IP Office system from the pop-up window. Click **OK** button.

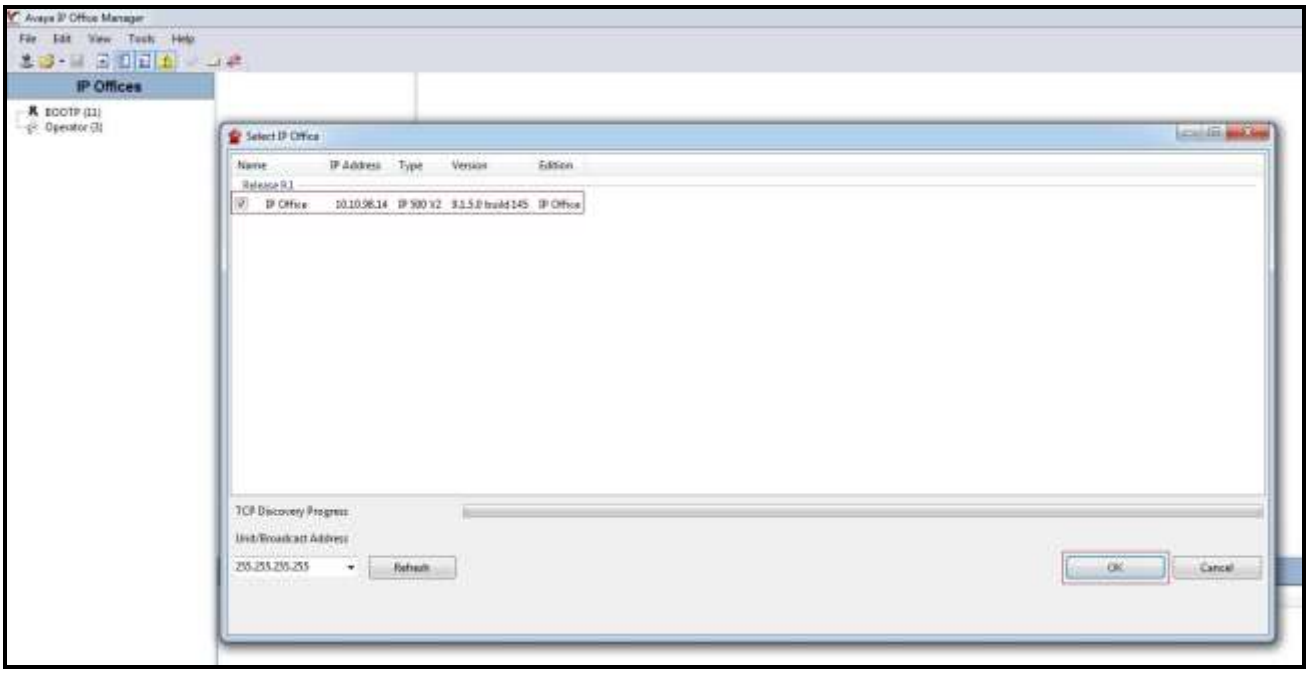

Figure 2 – Avaya IP Office Selection

Log in using appropriate credentials.

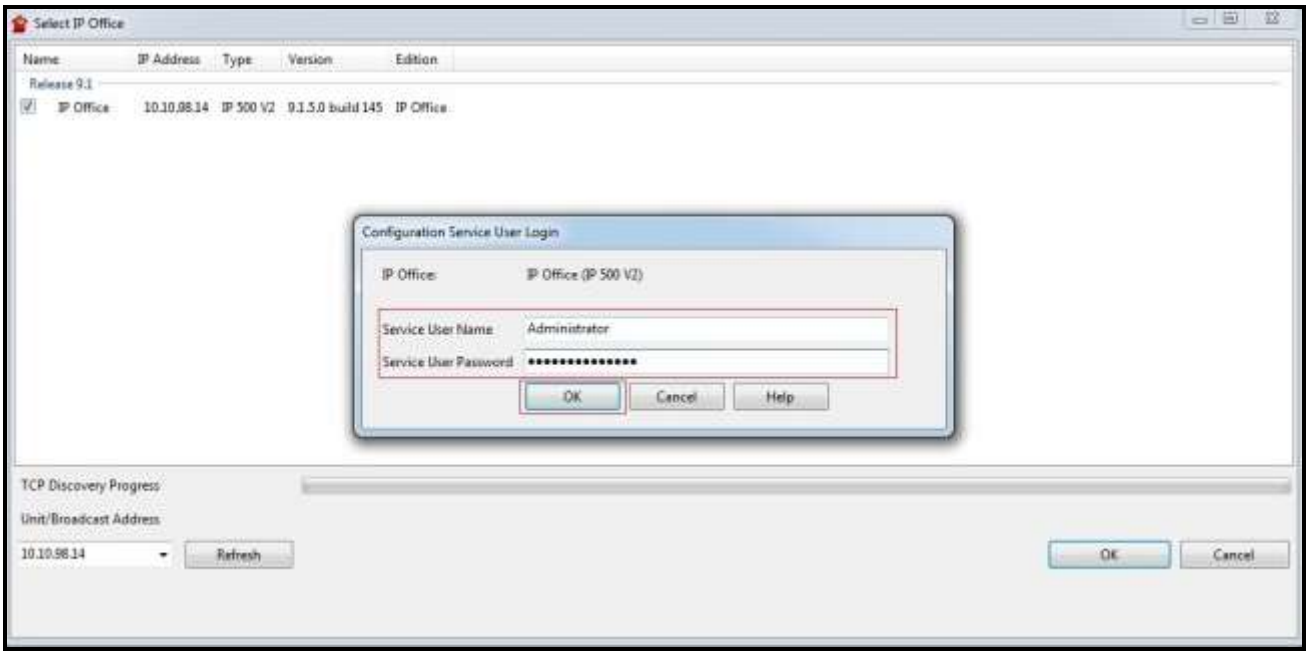

Figure 3 – Avaya IP Office Log In

5.1. Licensing

The configuration and features described in these Application Notes require the Avaya 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.

5.2. System Tab

Navigate to **System (1)** under the **IP Office** on the left pane and select the **System** tab in the Details pane. The Name field can be used to enter a descriptive name for the system. In the reference configuration, **IP Office** was used as the name in Avaya IP Office. Make sure to check the **Enable Softphone HTTP Provisioning** box to enable the support of Avaya IP Office Softphone.

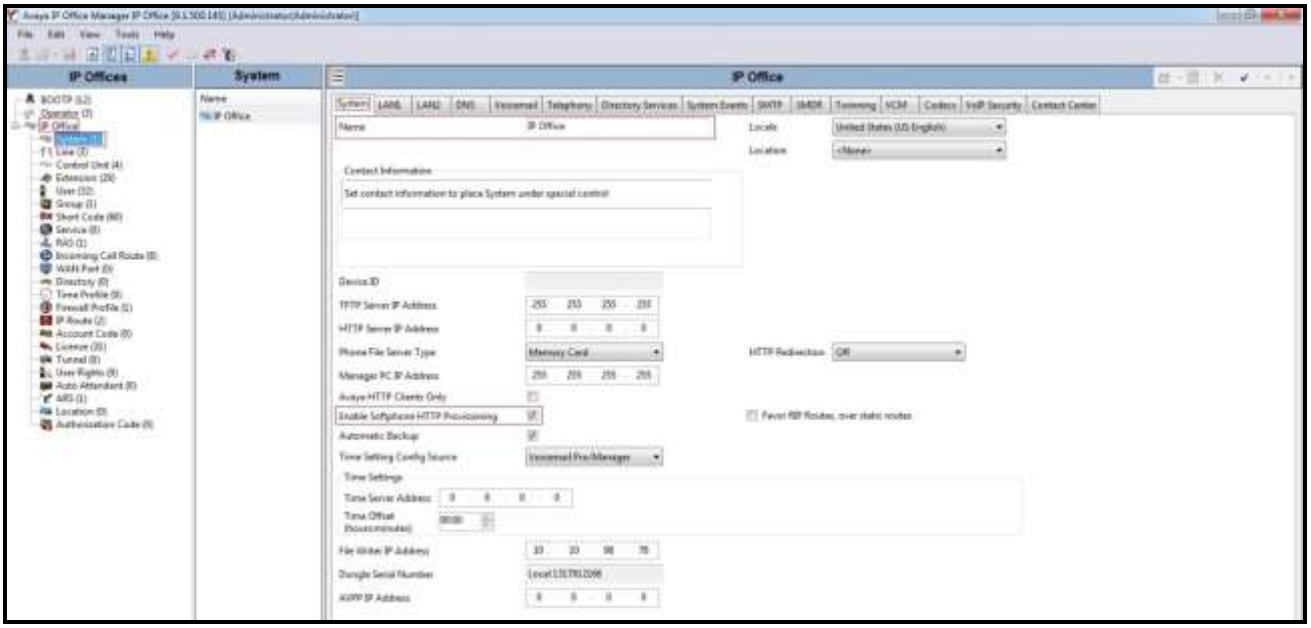

Figure 4 - Avaya IP Office System Configuration

5.3. LAN2 Settings

In the sample configuration, the LAN2 port of Avaya IP Office was used to connect to Avaya SBCE. To access the LAN2 settings, first navigate to **IP Office → System (1)** 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 LAN 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** to submit the change.

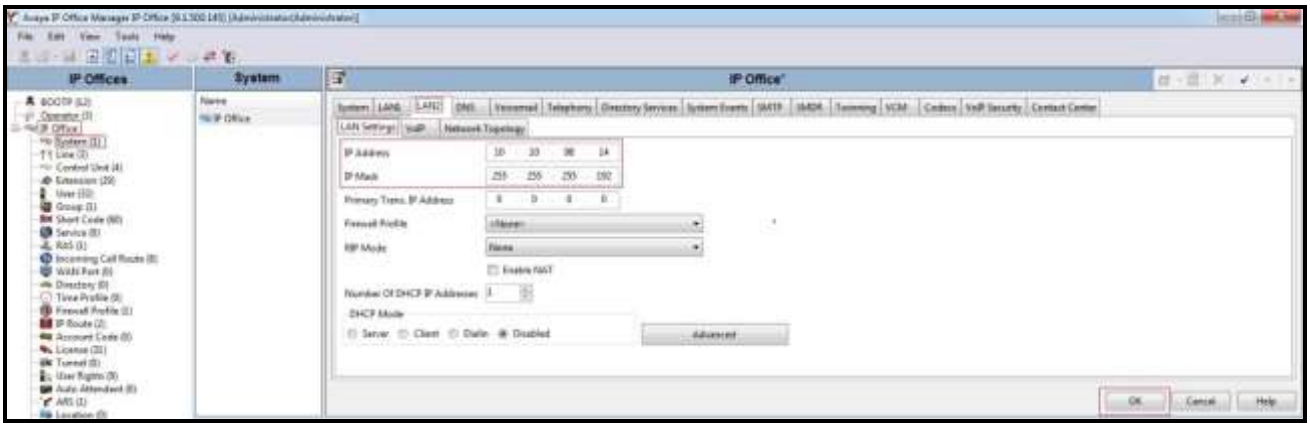

Figure 5 - Avaya IP Office LAN2 Settings

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

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Deskphones/Softphones using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Avaya SBCE.
- Check the **SIP Registrar Enable** to allow Avaya IP Deskphones/Softphones to register using the SIP protocol.
- Input **Domain Name** as **10.10.98.14**.
- The **Layer 4 Protocol** use **UDP** with **UDP Port** as **5060**, and **TCP** with **TCP Port** as **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.
- Verify the **DiffServ Settings** were kept as default for the Differentiated Services Code Point (DSCP) parameters in the IP packet headers to support Quality of Services policies for both signaling and media, the **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling.
- All other parameters should be set according to customer requirements.
- Click **OK** to submit the changes.

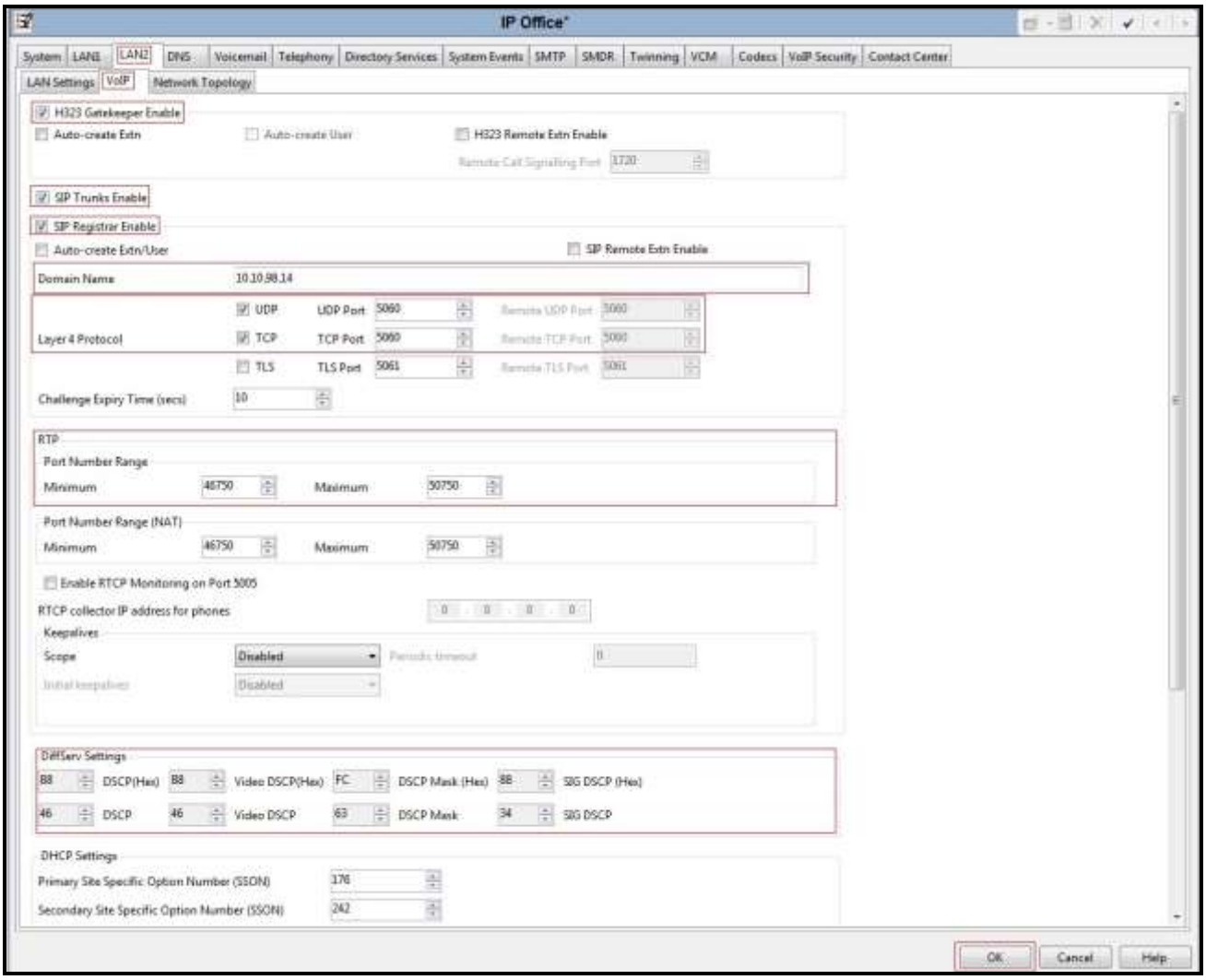

Figure 6 - Avaya IP Office LAN2 VoIP

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 the **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 OPTION messages to the service provider.
- Set **Public IP Address** to the IP address of the Avaya IP Office LAN2 port.
- Set **Public Port** for **UDP** as **5060**, and **TCP** as **5060**.
- All other parameters should be set according to customer requirements.
- Click **OK** to submit the changes.

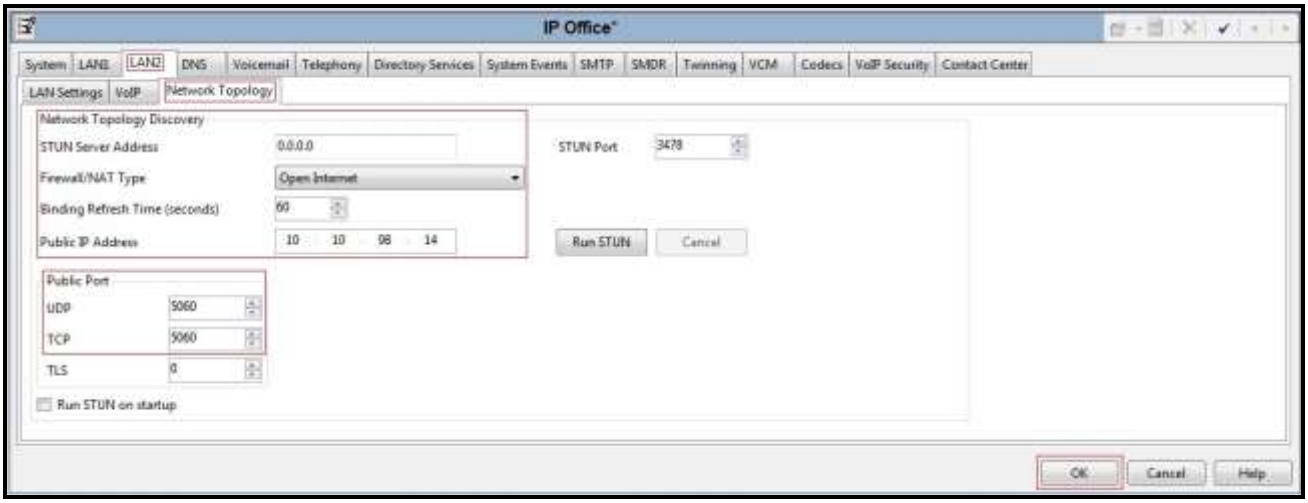

Figure 7 - Avaya IP Office LAN2 Network Topology

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 Line Systems, and therefore is not described in these Application Notes.

5.4. System Telephony Settings

Navigate to **IP Office → System (1)** in the Navigation and Group Panes and then navigate to the **Telephony → Telephony** tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. For North America, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the service provider across the SIP trunk. Set **Hold Timeout (secs)** to **1200** and **Default Name Priority** to **Favor Trunk**. Defaults were used for all other settings. Click **OK** to submit the changes.

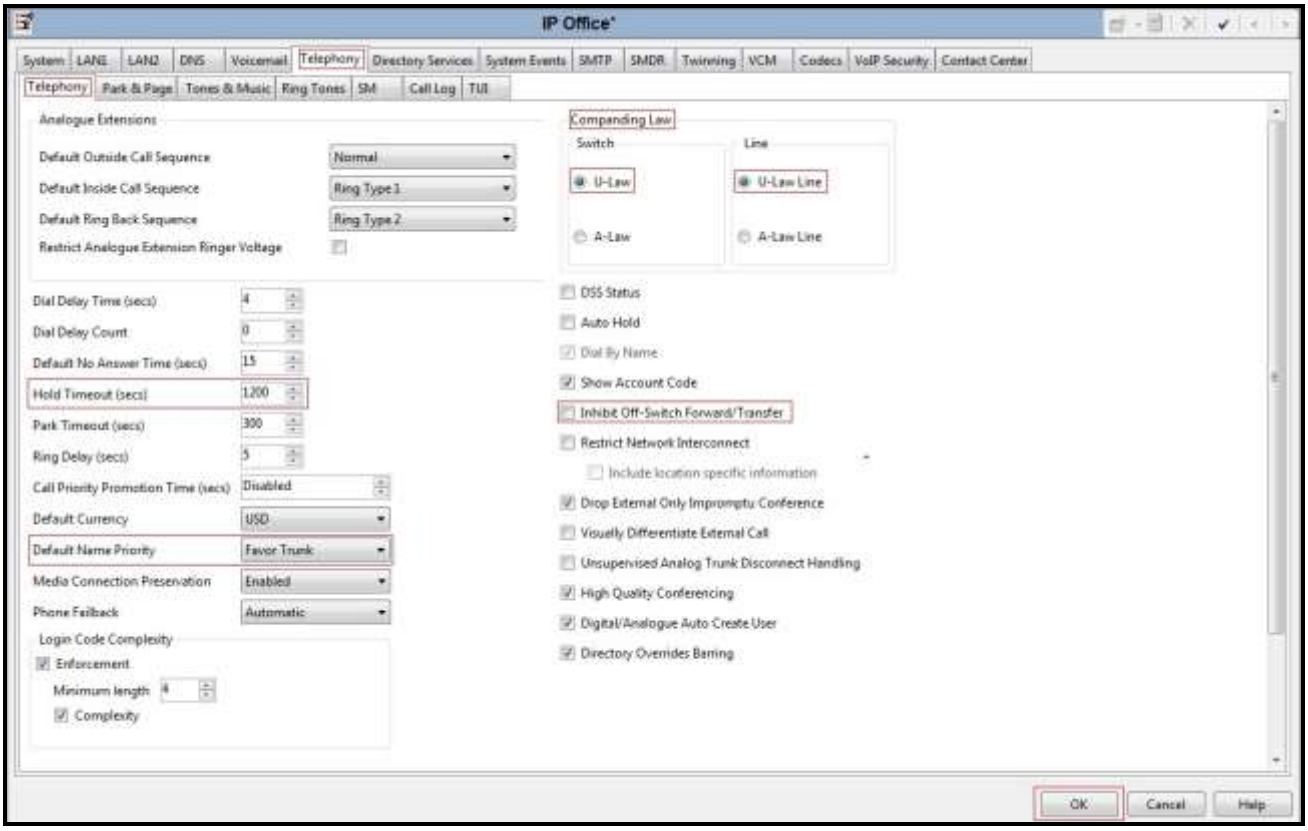

Figure 8 - Avaya IP Office Telephony

5.5. System Codec Settings

Navigate to **IP Office → System (1)** in the Navigation and Group Panes and then navigate to the **Codecs** tab in the Details Pane. Choose the **RFC2833 Default Payload** as IP Office default of **101**. Select codecs **G.711 ULAW 64K**, and **G.729(a) 8K CS-ACELP** that Line Systems supports. Click **OK** to submit the changes.

Figure 9 - Avaya IP Office Codecs

5.6. Twinning Calling Party Settings

When using twinning, the calling party number displayed on the twinned phone is controlled by two parameters. These parameters only affect 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 **Twinning** tab, as shown below. The second parameter is the **Send Caller ID** parameter on the **SIP Line** form (shown in **Section 5.7.2**).

If **Send original calling party information for Mobile Twinning** on the **Twinning** tab is checked, the setting of the second parameter is ignored and Avaya IP Office will send the following in the SIP From Header:

- On calls from an internal extension to a twinned phone, Avaya IP Office will send the calling party number of the originating extension.
- On calls from the PSTN to a twinned phone, Avaya IP Office will send the calling party number of the host phone associated with the twinned destination (instead of the number of the originating caller).

If this option is unchecked, the value sent in the SIP From header is determined by the setting of the second parameter mentioned above.

- For the compliance test, the **Send original calling party information for Mobile Twinning** box in the **IP Office → System (1) →Twinning** tab was unchecked. The value sent in the SIP From header is determined by the setting of the **Send Caller ID** parameter on the **SIP Line** form**.**

Figure 10 - Avaya IP Office Twinning

5.7. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Avaya SBCE. 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 **Section 5.7.2.**

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.
- SIP Advanced Engineering.

Alternatively, a SIP Line can be created manually. To do so right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.7.2.**
In the compliance test, SIP Line 17 was used as trunks for incoming and outgoing calls.

5.7.1. 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_Line-System_SIPTrunk.xml** (for SIP Line 17). 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** to submit the changes.

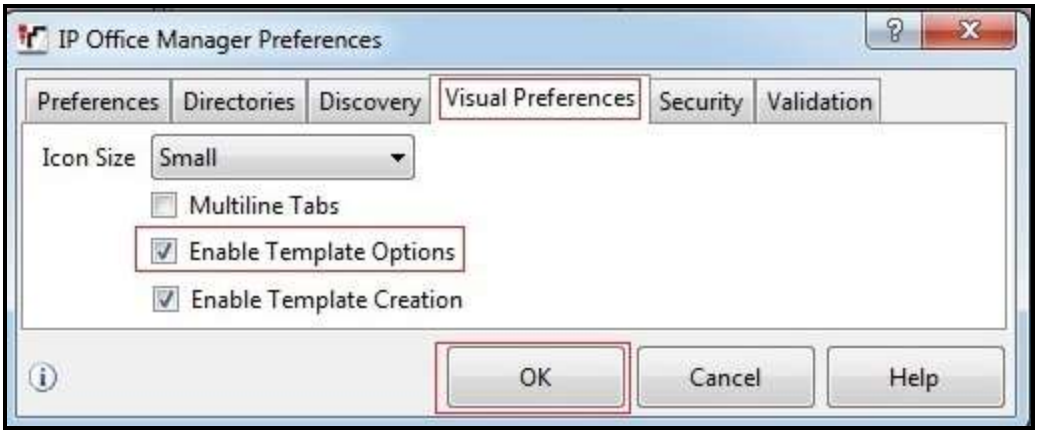

Figure 11 – Enable Template for SIP Line

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.

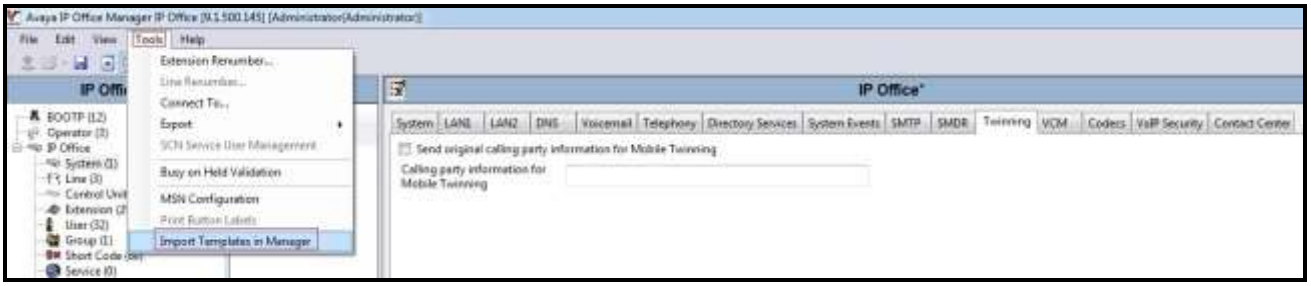

Figure 12 – Import Template for SIP Line

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 below will appear stating success (or failure). Then click **OK** to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

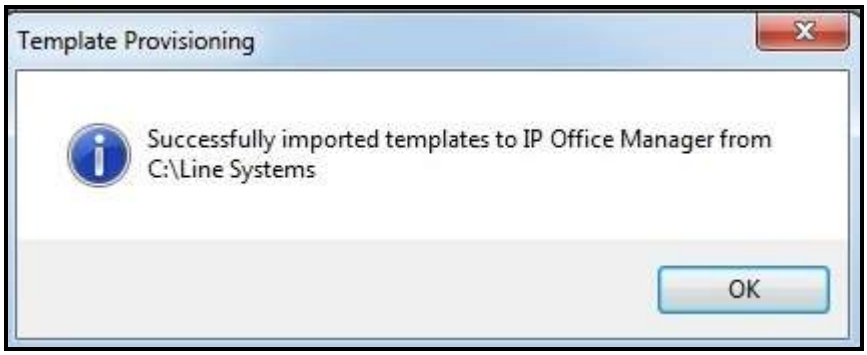

Figure 13 – Import Template successfully for SIP Line

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

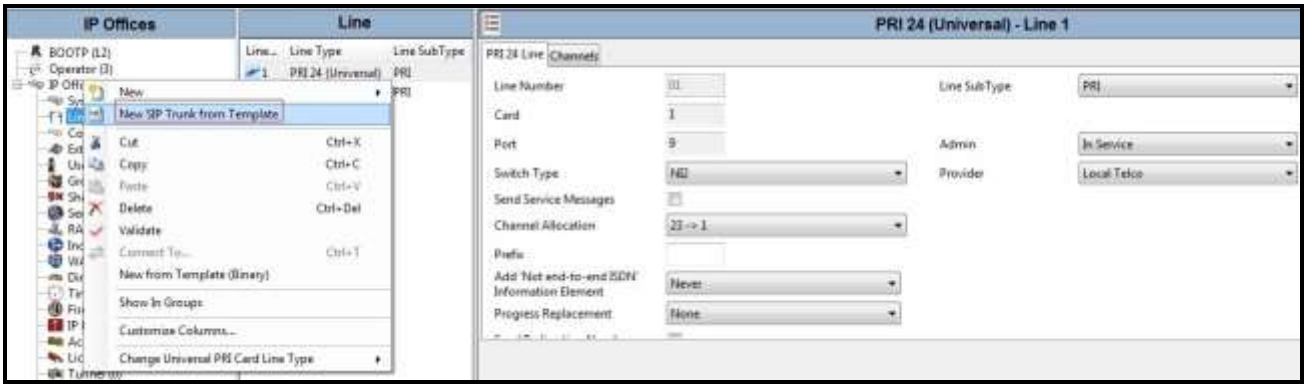

Figure 14 – Create SIP Line from Template

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

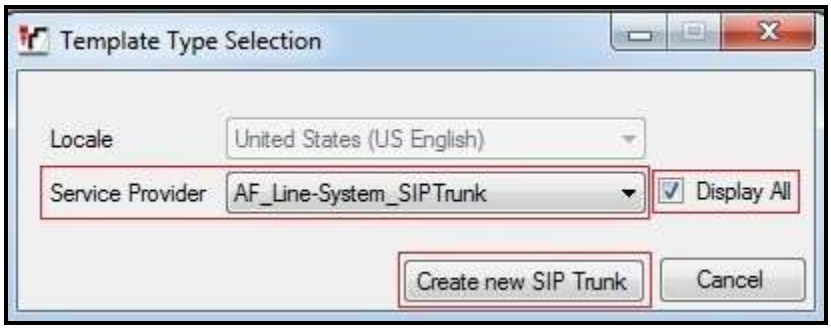

Figure 15 – Select Template for creating SIP

6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Section 5.7.2**.

5.7.2. 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** (not shown).

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

- Set **ITSP Domain Name** to the IP address of Avaya IP Office LAN2 port.
- Set **URI Type** to **SIP**.
- Check the **In Service** and **Check OOS** boxes.
- For **Session Timers**, set **Refresh Method** to **Reinvite** with **Timer (seconds)** to **1200**.
- For **Forwarding and Twinning**, set **Send Caller ID** to **Diversion Header**.
- For **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Auto**. Note: In the compliance testing, Line Systems supports both SIP re-Invite and SIP Refer.
- Set **Name Priority** to **Favor Trunk**. As described in **Section 5.4**, the **Default Name Priority** parameter may retain the default **Favor Trunk** setting, or can be configured to **Favor Directory**. As shown below, the default **Favor Trunk** setting was used in the reference configuration
- Default values may be used for all other parameters.
- Click **OK** to commit then press Ctrl + S to save.

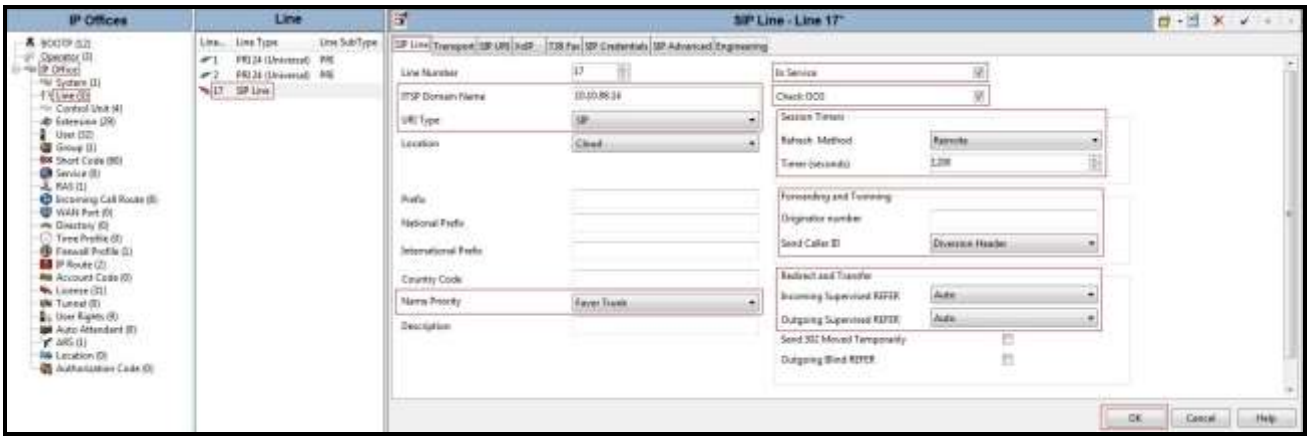

Figure 16 – SIP Line Configuration

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

- The **ITSP Proxy Address** was set to the IP Address of Avaya SBCE internal interface **10.10.97.174** as shown in **Figure 1**.
- In the **Network Configuration** area, **UDP** was selected as the **Layer 4 Protocol** and the **Send Port** was set to **5060** which is the port number supported by Line Systems.
- The **Use Network Topology Info** parameter was set to **LAN 2**. This associates the SIP Line 17 with the parameters in the **System (1) → LAN2**
- The **Calls Route via Registrar** was unchecked. In this certification testing, Line Systems did not support the dynamic Registration on the SIP Trunk.
- Other parameters retain default values.
- Click **OK** to commit then press Ctrl + S to save.

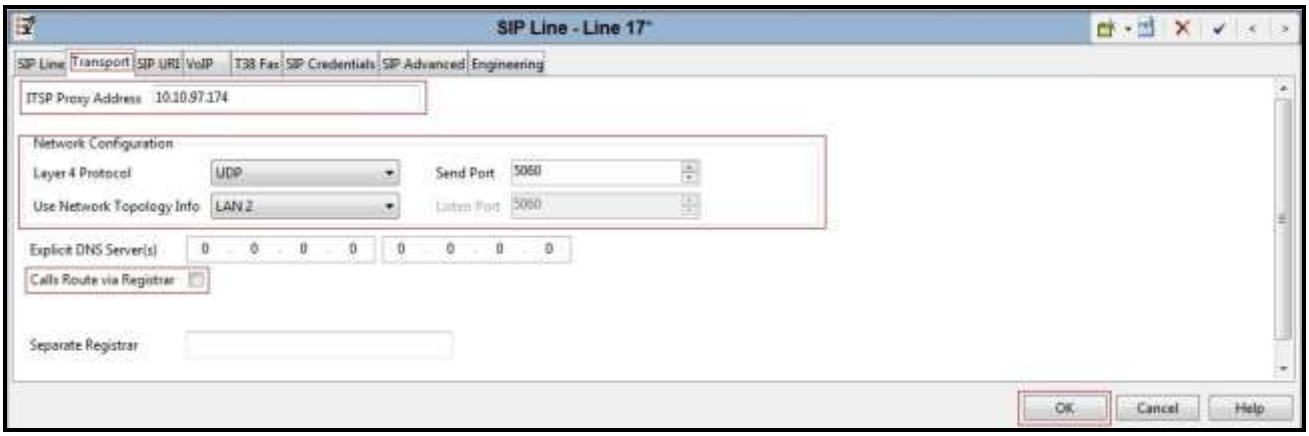

Figure 17 – SIP Line Transport Configuration

A SIP URI (Uniform Resource Identifier) is similar to an internet email address and represents the source or destination for SIP connection. Select the **SIP URI** tab; click the **Add** button and the **New Channel** area will appear at the bottom of the pane (not shown). To edit an existing entry, click an entry in the list at the top, and click **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:

- Set **Local URI**, **Contact**, **Display Name**, and **PAI** 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 5.9**.
- Set **Registration** to **0: <None>** as Line Systems does not require registration.
- Associate this line with an incoming line group in the **Incoming Group** field and an outgoing line group in the **Outgoing Group** field. This line group number will be used in defining incoming and outgoing call routes for this line. In the compliance test, a new line 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 submit the changes.

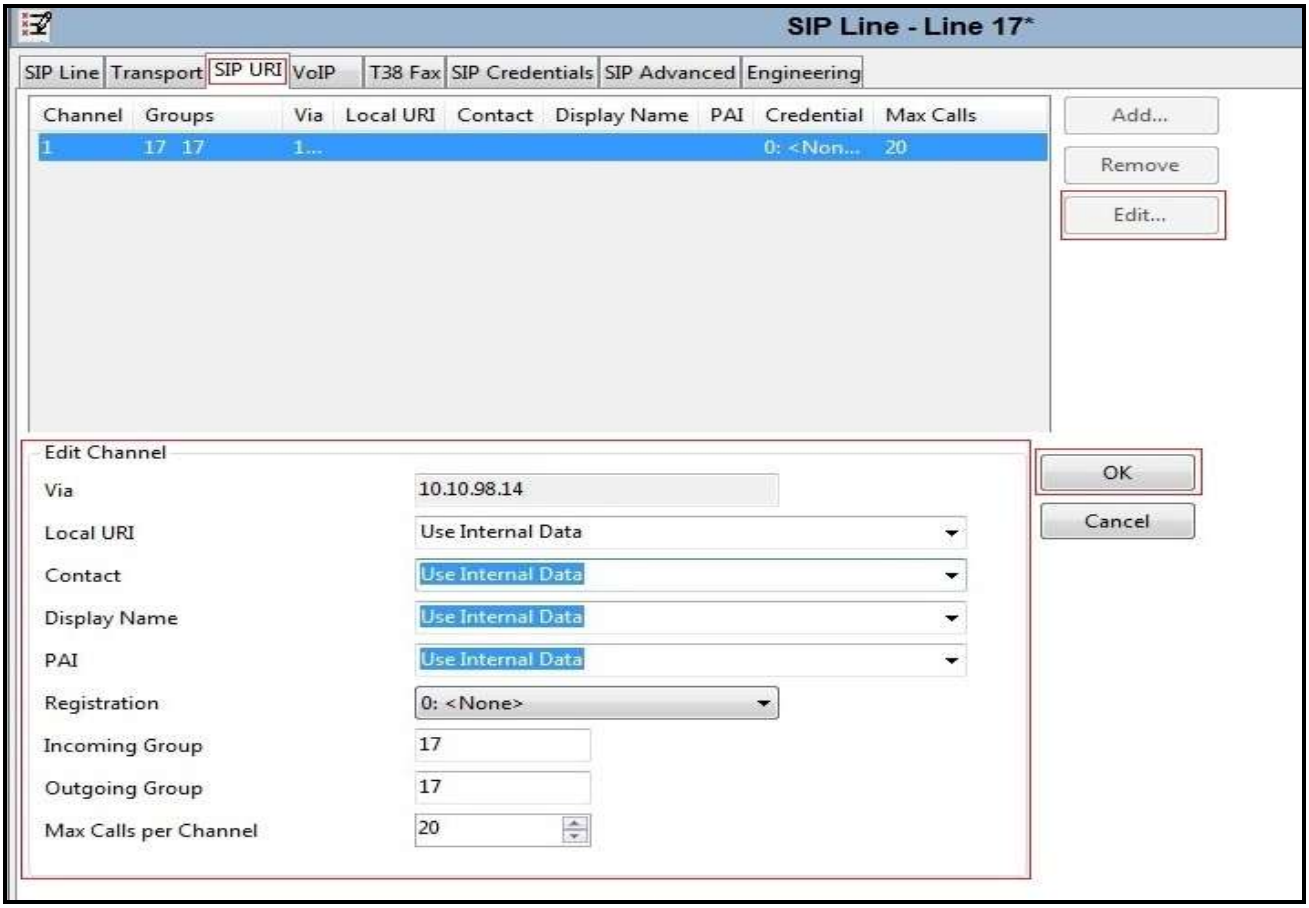

Figure 18 – SIP Line SIP URI Configuration

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. The **G.711 ULAW 64K** and **G.729(a) 8K CS –ACELP** codecs are selected. Avaya IP Office supports these codecs, which are sent to Line Systems, in the Session Description Protocol (SDP) offer, in that order.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Set **Fax Transport Support** to **T38 fallback** from the pull-down menu. In the compliance testing, Line Systems supports both Fax T.38 and Fax G.711 pass-through modes.
- Set the **DTMF Support** to **RFC2833** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Default values may be used for all other parameters**.**
- Click **OK** to submit the changes.

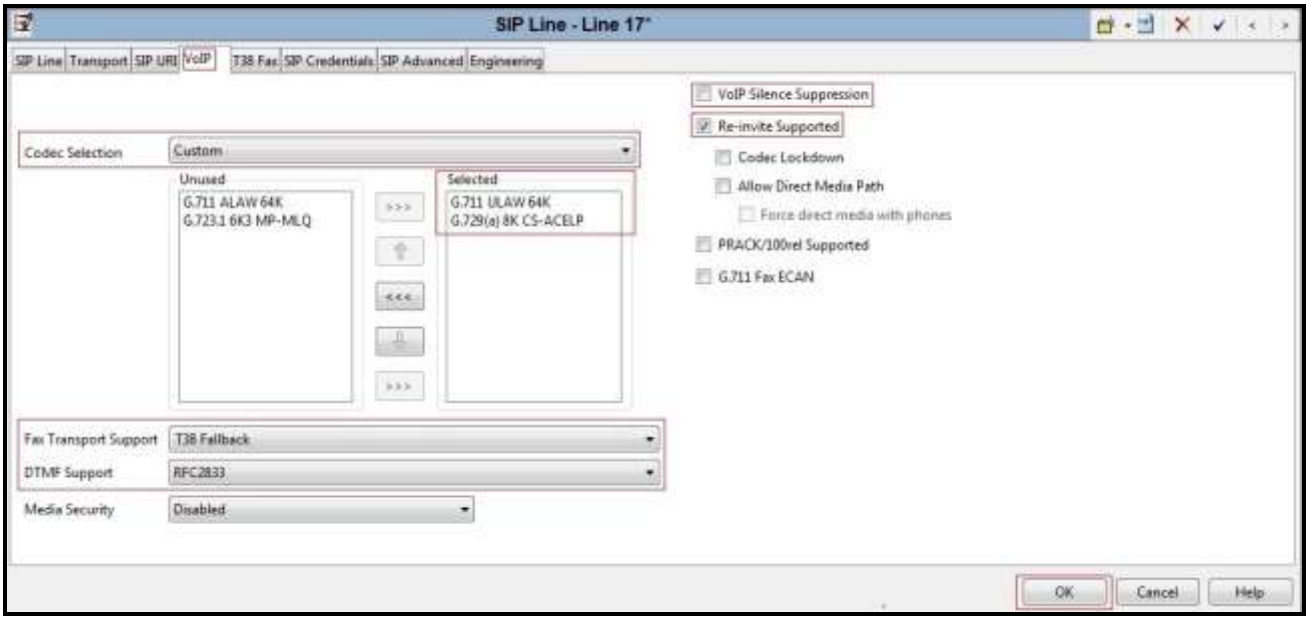

Figure 19 – SIP Line VoIP Configuration

5.8. Short Code

Define a short code to route outbound traffic on the SIP line to Line Systems. To create a short code, select **Short Code** in the left Navigation Pane, then right-click in the Group Pane and select **New** (Not shown). 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 "6N;" 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, **6N;**, this short code will be invoked when the user dials 6 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N"@10.10.97.174"**. 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 IP address of Avaya SBCE internal interface.
- Set the **Line Group ID** to the **Outgoing Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 5.7.2**. This short code will use this line group when placing the outbound call.
- Set the **Locale** to **United States (US English)**.
- Default values may be used for all other parameters**.**
- Click **OK** to submit the changes.

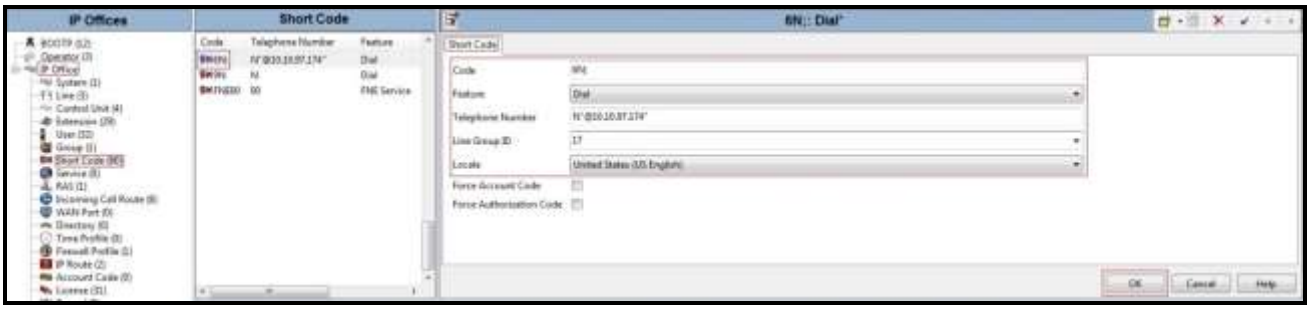

Figure 20 – Short Code 6N

The feature of incoming calls from mobility extension to idle-appearance FNE (Feature Name Extension) is hosted by Avaya IP Office. The Short Code **FNE00** was configured with following parameters:

- For **Code** field, enter FNE feature code as **FNE00** for dial tone.
- Set **Feature** to **FNE Service**.
- Set **Telephone Number** to **00**.
- Set **Line Group ID** to **0**.
- Set the **Locale** to **United States (US English)**.
- Default values may be used for other parameters.
- Click **OK** to submit the changes.

Figure 21 – Short Code FNE

5.9. User

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 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 **4194**. 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. The example below shows the settings for user **4194**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise provided by Line Systems. 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.

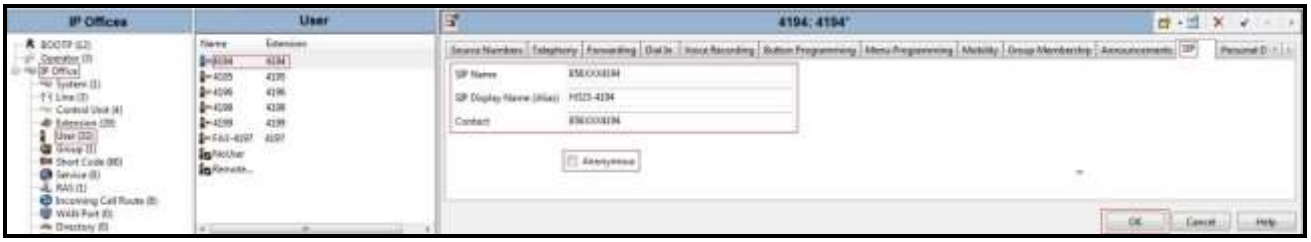

Figure 22 – User Configuration

One of the H.323 IP Deskphones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for **User 4194**. 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 **61613XXX5205**. Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (see **Section 5.8**). Other options can be set according to customer requirements.

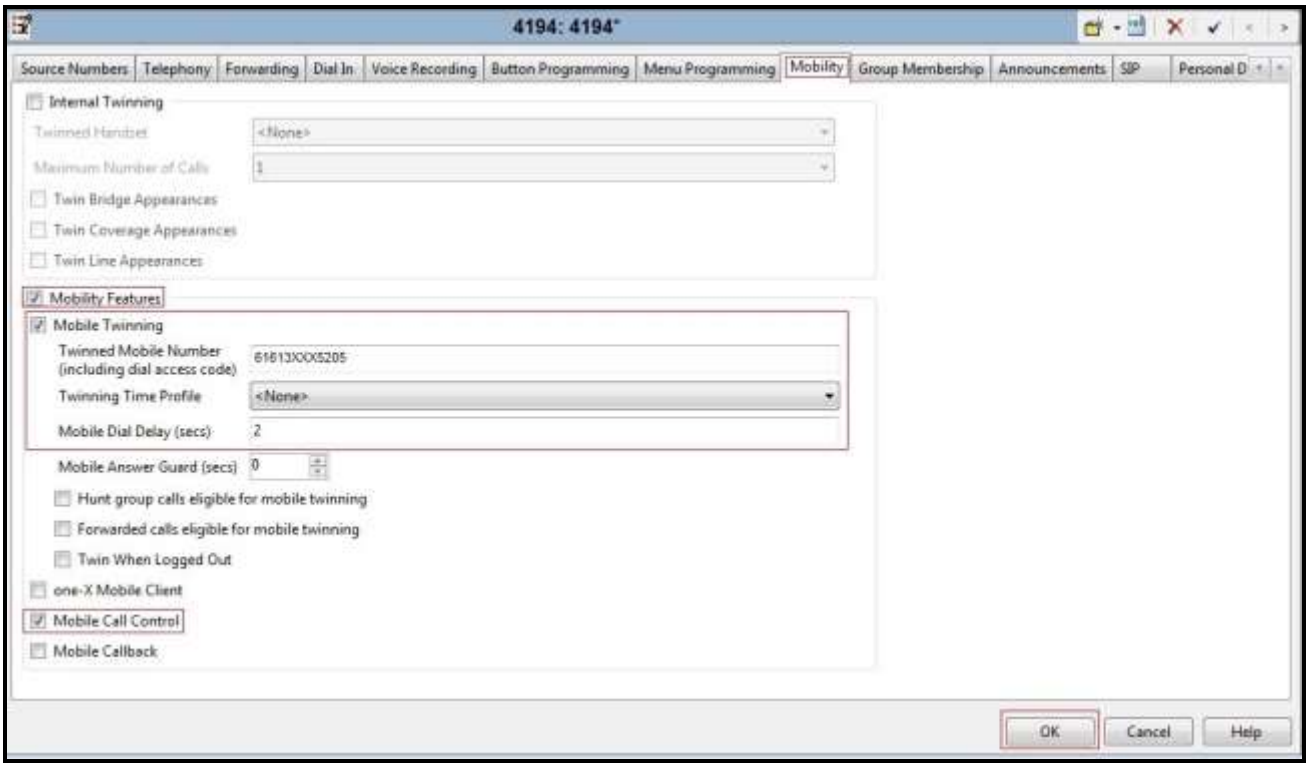

Figure 23 – Mobility Configuration for User

5.10. 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 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** (Not shown). On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group ID** to the **Incoming Group 17** defined on the **SIP URI** tab on the **SIP Line** in **Section 5.7.2**.
- Set the **Incoming Number** to the incoming DID number on which this route should match.
- Default values can be used for all other fields.

Figure 24 – Incoming Call Route Configuration

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **856XXX4194** on line 17 are routed to extension **4194**.

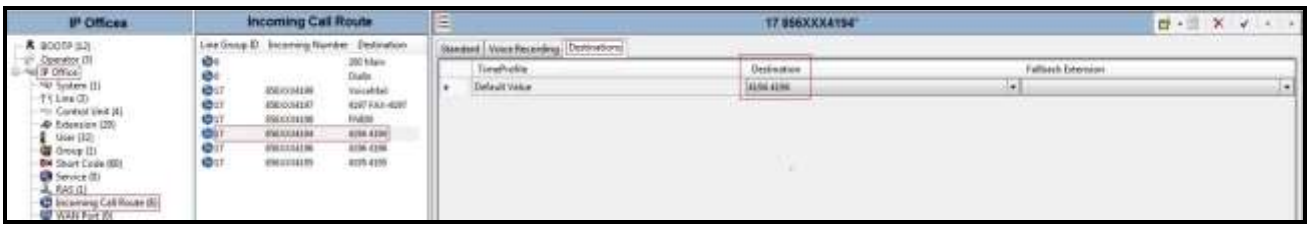

Figure 25 – Incoming Call Route for Destination H323-4194

For testing purpose, the incoming calls to DID number **856XXX4198** were configured to access **FNE00**. The **Destination** was appropriately defined as **FNE00** as below screenshot:

Figure 26 – Incoming Call Route for Destination FNE

For testing purpose, the incoming calls to DID number **856XXX4199** were also configured to access **VoiceMail**. The **Destination** was appropriately defined as **VoiceMail** as below screenshot:

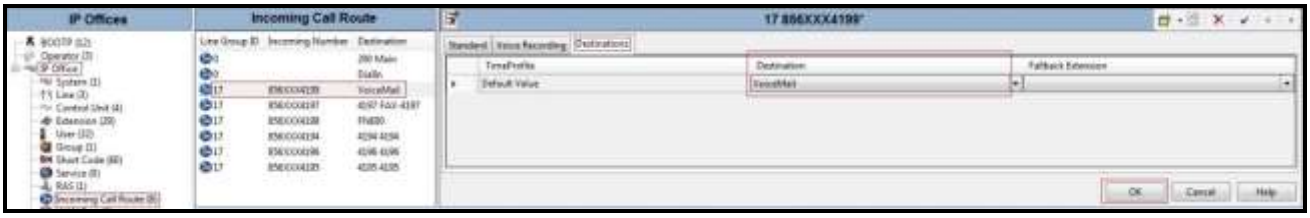

Figure 27 – Incoming Call Route for Destination VoiceMail

5.11. Save Configuration

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

6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of Avaya SBCE necessary for interoperability with the Avaya IP Office and Line Systems SIP Trunk Service.

Avaya elements reside on the Private side and the Line Systems SIP Trunk Service resides on the Public side of the network, as illustrated in **Figure 1**.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see relevant product documentation references in **Section 10** of these Application Notes.

6.1. Log in to the Avaya SBCE

Access the web interface by typing "**https://x.x.x.x/sbc/**" (where x.x.x.x is the management IP address of the Avaya SBCE).

Enter the **Username** and **Password**.

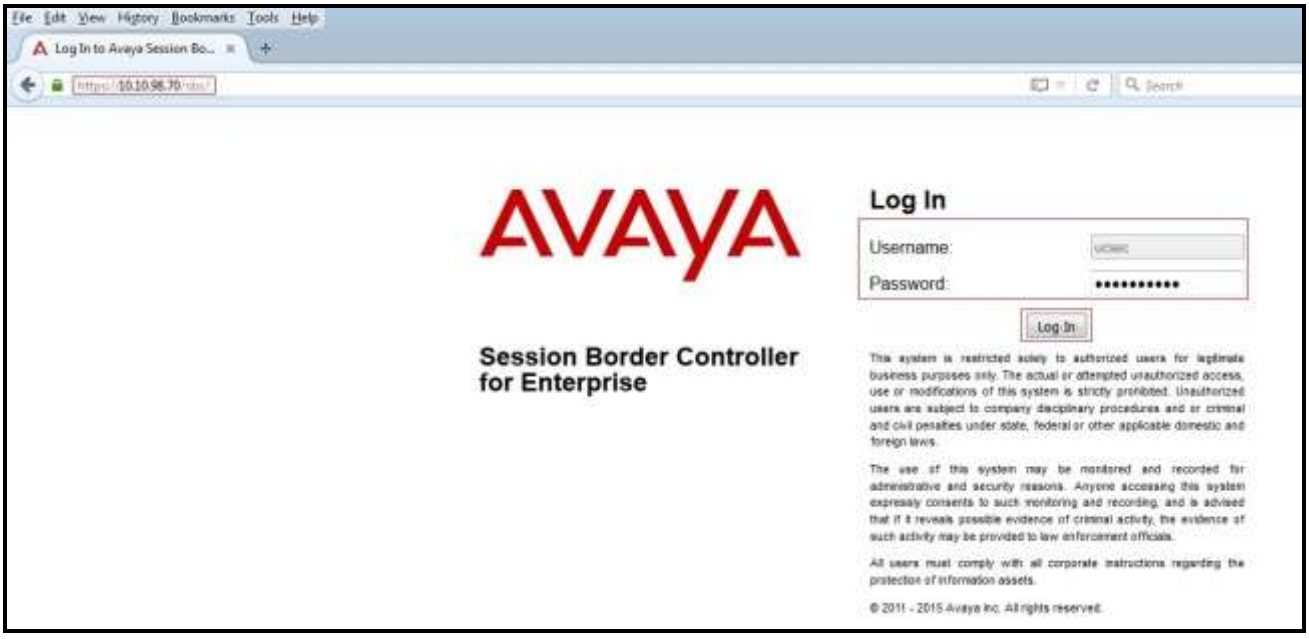

Figure 28 – Avaya SBCE Login

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

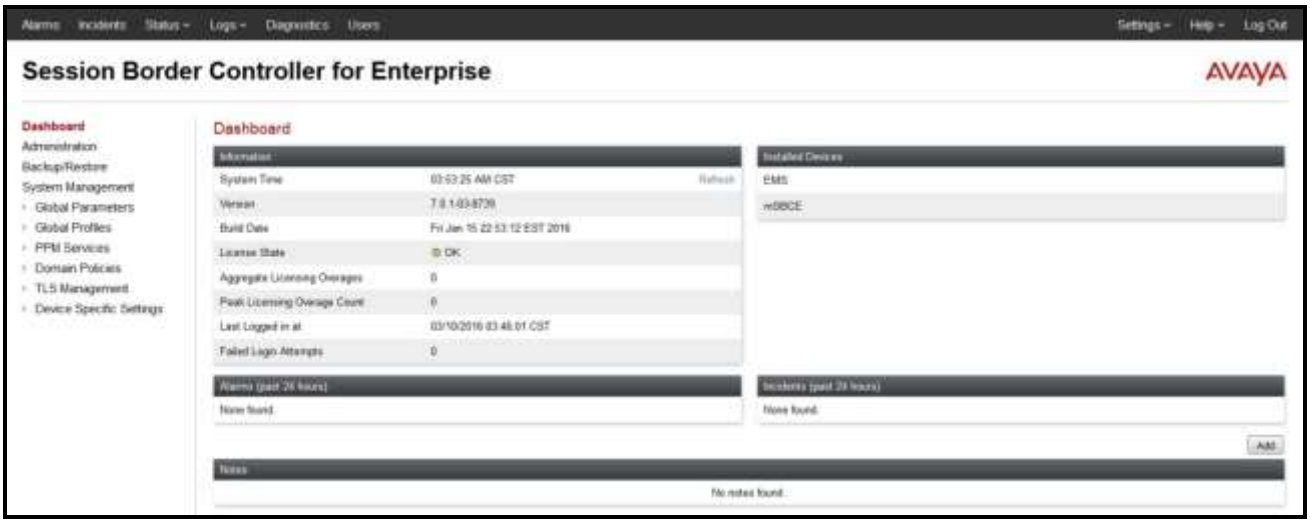

Figure 29 - Avaya SBCE Dashboard

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

Figure 30 - Avaya SBCE System Management

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**.

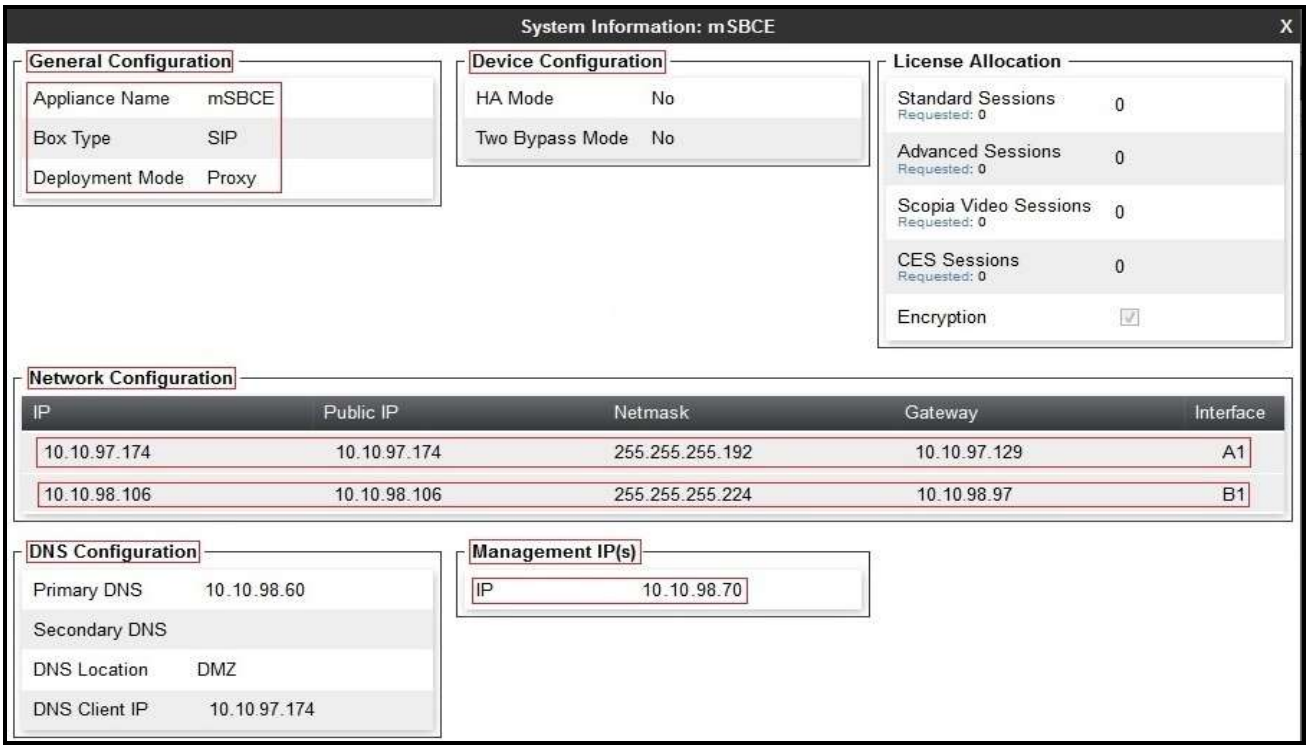

Figure 31 - Avaya SBCE System Information

6.2. Global Profiles

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

6.2.1. Configure Server Interworking Profile – Avaya IP Office

Server Interworking profile allows administrator to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.
From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- Select **avaya-ru** in **Interworking Profiles**.
- Click **Clone**.
- Enter **Clone Name**: **IPO_14** and click **Finish** (not shown).

From the list of **Interworking Profiles**, click on **IPO_14** to edit.

- On the **General** tab, set **T.38 Support** to **Yes**. Note: In the compliance testing, Line Systems supports both Fax T.38 and G.711 pass-through modes. Other options can be left at default.
- On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** tabs, all options can be left at default. Click **Finish** (not shown).

The following screen shows that Avaya IP Office server interworking profile (named: **IPO_14**) was added.

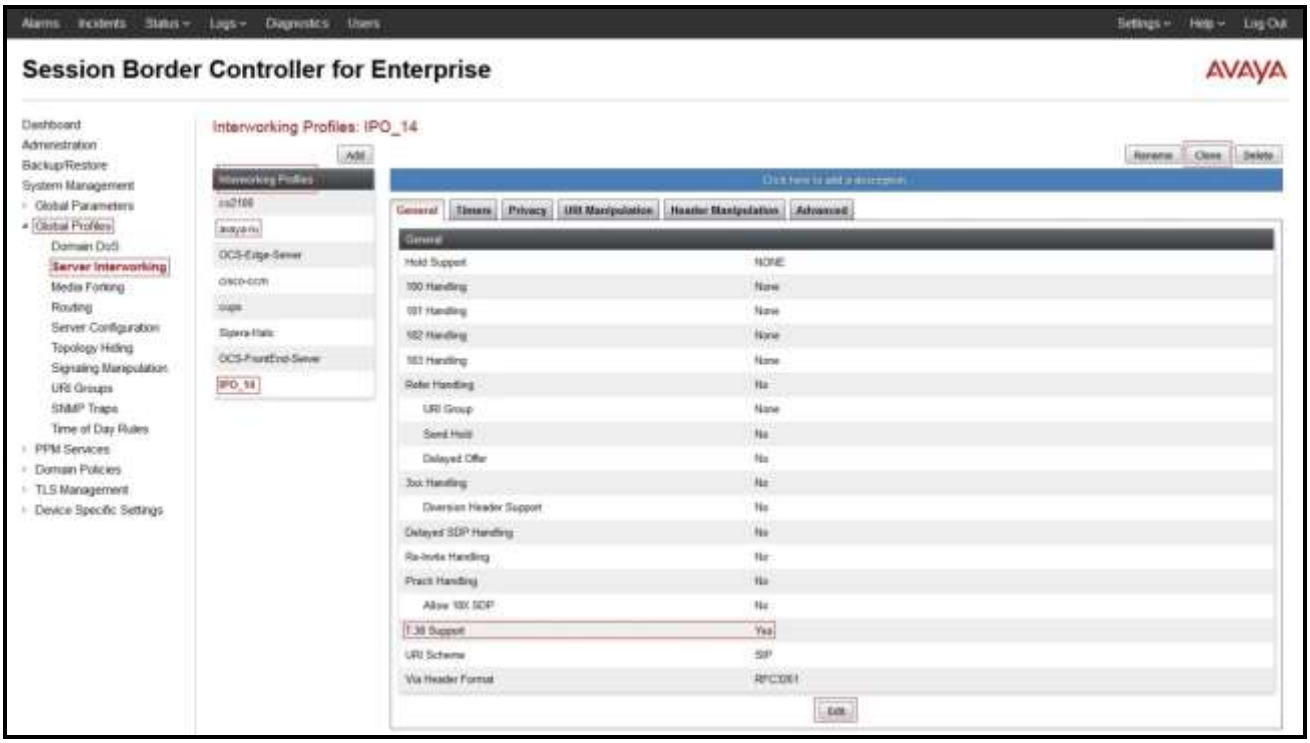

Figure 32 - Server Interworking – Avaya

6.2.2. Configure Server Interworking Profile – Line Systems

From the menu on the left-hand side, select **Global Profiles → Server Interworking → Add**

- Enter **Profile Name**: **SP4** (not shown).
- Click **Next** button to leave all options at default.
- Click **Finish** (not shown).

From the list of **Interworking Profiles**, click on **SP4** to edit.

- On the **General** tab, set **T.38 Support** to **Yes**. Note: In the compliance testing, Line Systems supports both Fax T.38 and G.711 pass-through modes. Other options can be left at default.
- Click **Finish** (not shown).

The following screen shows that Line Systems server interworking profile (named: **SP4**) was added.

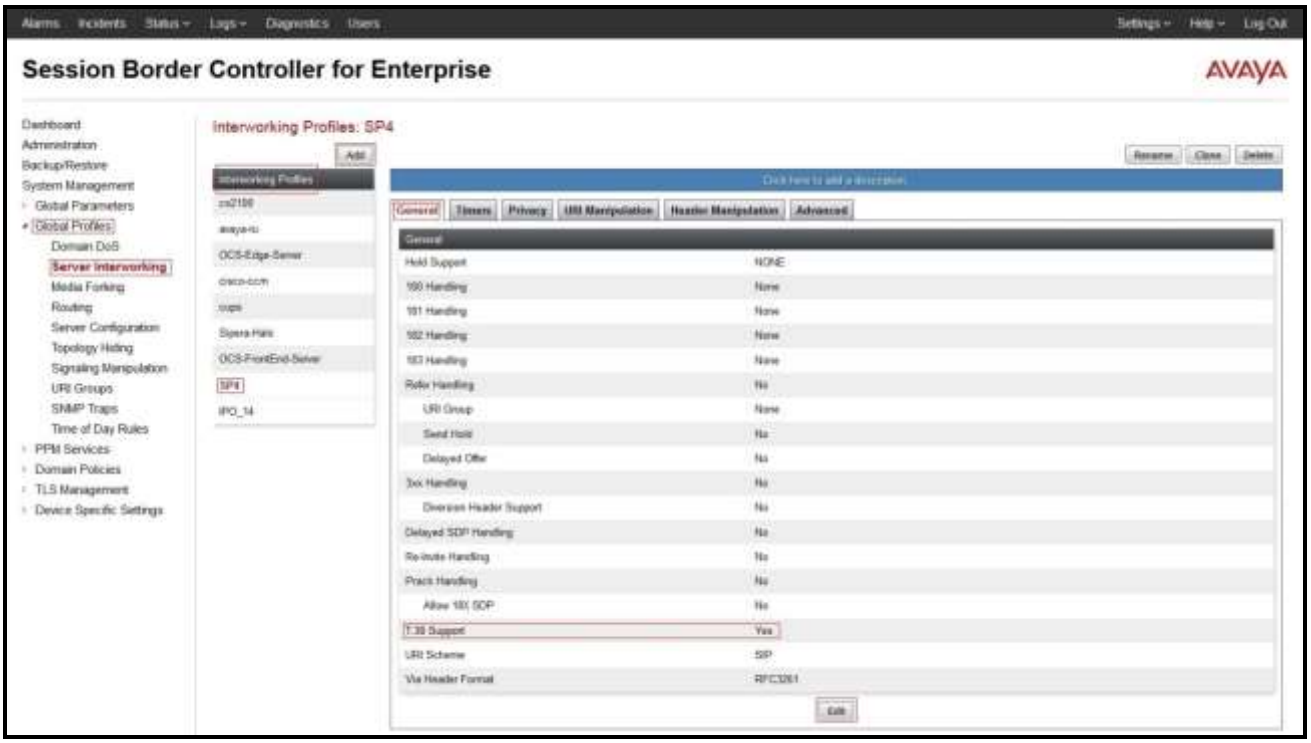

Figure 33 - Server Interworking – Line Systems

6.2.3. Configure Server – Avaya IP Office

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server-specific parameters such as UDP port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**.

Enter **Profile Name**: **IPO_14** (not shown).

On **General** tab, enter the following:

- **Server Type**: Select **Call Server**.

- **IP Address/FQDN**: **10.10.98.14** (Avaya IP Office IP LAN2 port IP address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).

Figure 34 – Avaya Server Configuration – General

On the **Advanced** tab:

- Select **IPO_14** for **Interworking Profile** (see **Section 6.2.1**).
- Click **Finish** (not shown).

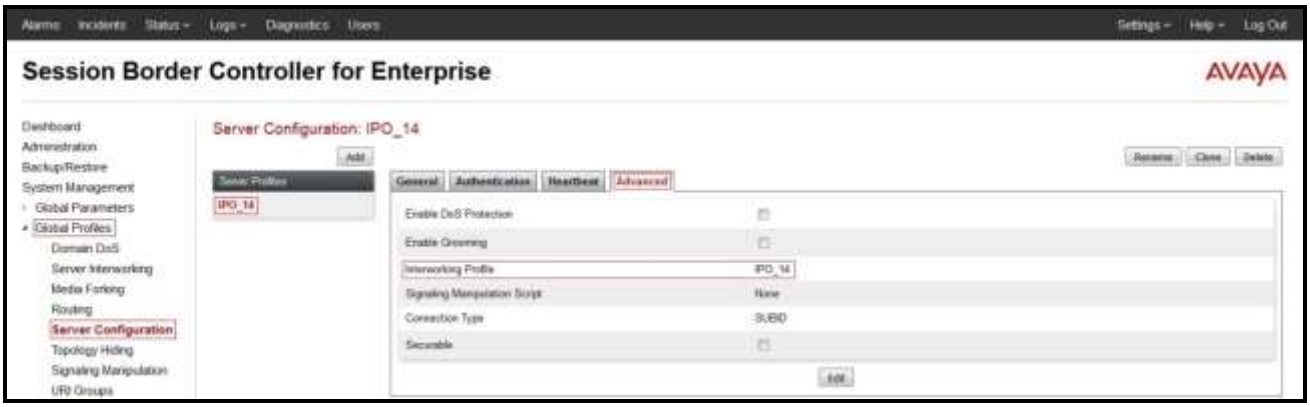

Figure 35 – Avaya Server Configuration – Advanced

6.2.4. Configure Server – Line Systems

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**.

Enter **Profile Name**: **SP4** (not shown).
On **General** tab, enter the following:

- **Server Type**: Select **Trunk Server**.
- Add **IP Address/FQDN**: **192.168.248.105** (Line Systems Signaling Server IP address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).

Figure 36 - Line Systems Server Configuration – General

On the **Authentication** tab, click **Edit** button and enter the following:

- Check **Enable Authentication** checkbox.
- Enter **User Name**: Line Systems provides user name.
- Enter **Password** and **Confirm Password**: Line Systems provides the password.
- Click **Finish**.

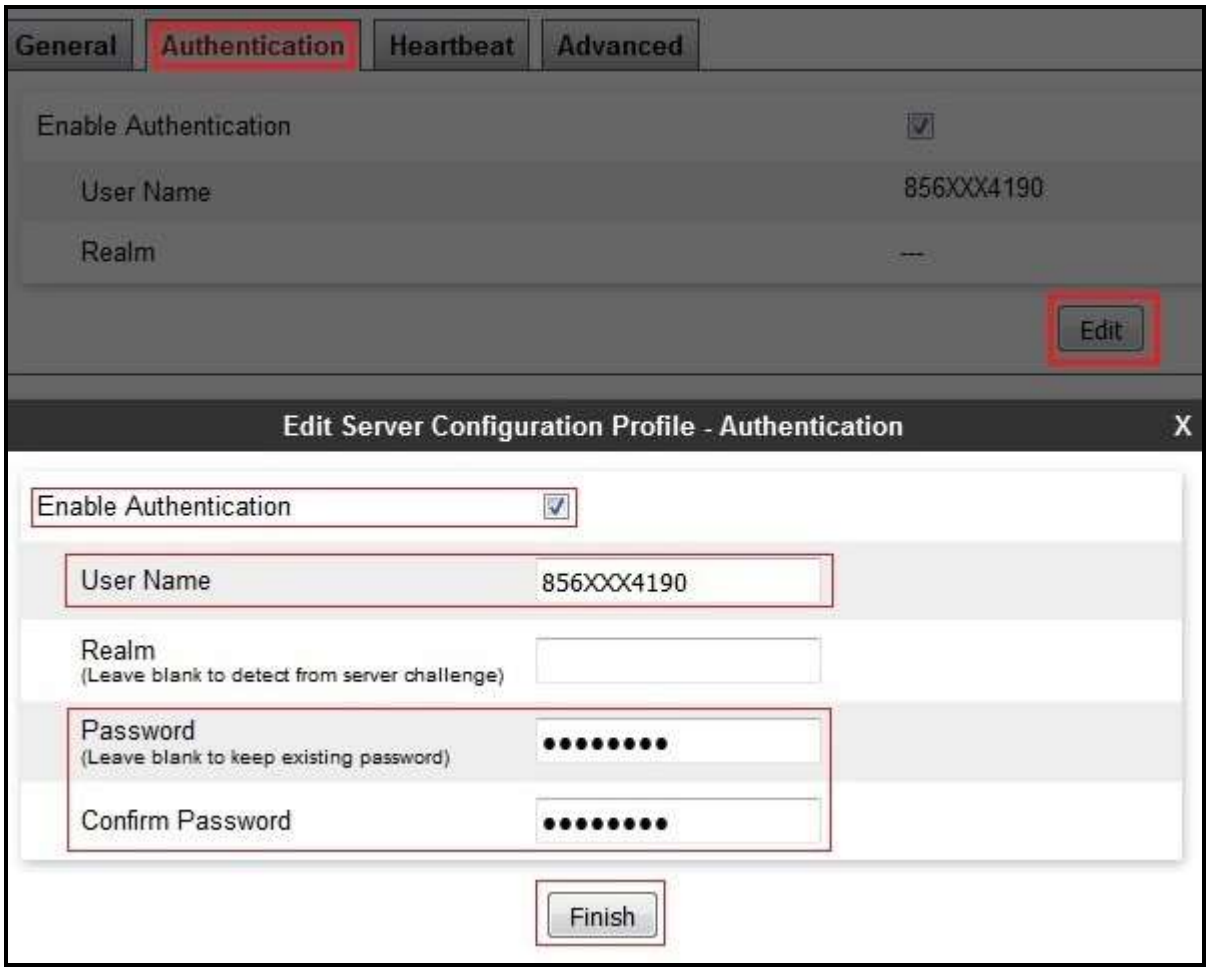

Figure 37 - Line Systems Server Configuration – Authentication

On the **Advanced** tab, click **Edit** button and enter the following:

- **Interworking Profile**: select **SP4** (see **Section 6.2.2**).
- Click **Finish** (not shown).

Figure 38 - Line Systems Server Configuration – Advanced

6.2.5. Configure Routing – Avaya IP Office

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.

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **To_IPO_14** and click **Next** button (not shown).

- Select **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight**: **1**.
- **Server Configuration**: **IPO_14** (see **Section 6.2.3**). This selection will automatically populate the **Next Hop Address** field with **10.10.98.14:5060 (UDP)** (Avaya IP Office IP address).
- Click **Finish**.

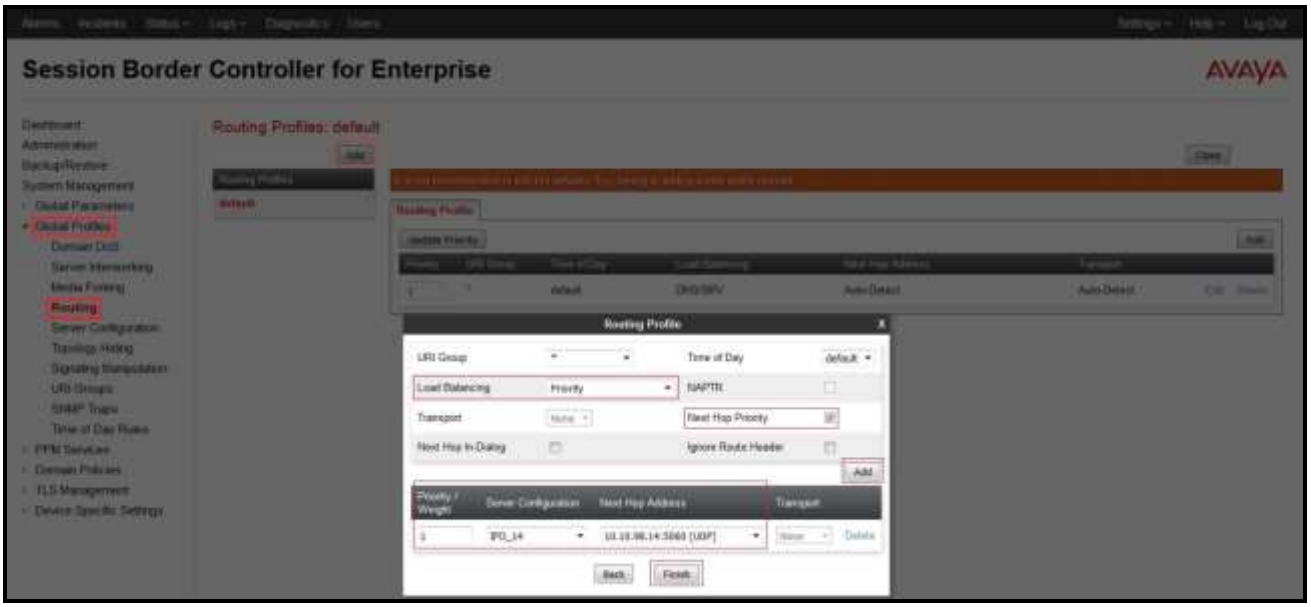

Figure 39 - Routing to Avaya IP Office

6.2.6. Configure Routing – Line Systems

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **To_SP4** (not shown).

- **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight**: **1**.
- **Server Configuration**: **SP4** (see **Section 6.2.4**). This selection will automatically populate the **Next Hop Address** field. Select **192.168.248.105:5060 (UDP)** (Line Systems Signaling IP address).
- Click **Finish**.

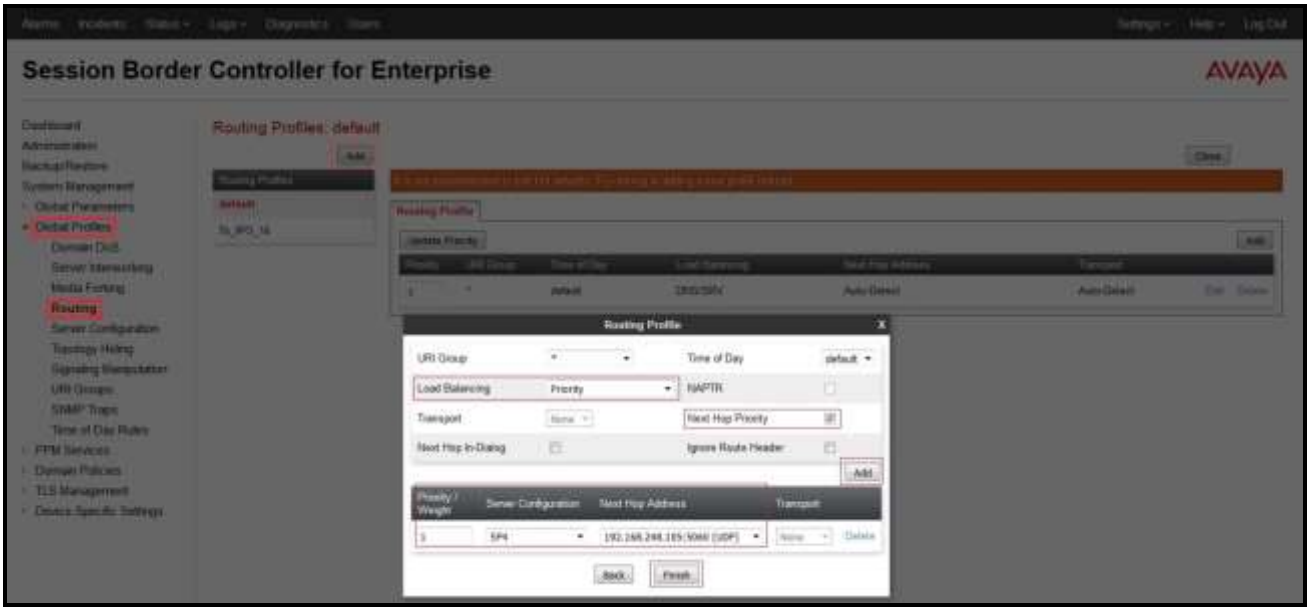

Figure 40 - Routing to Line Systems

6.2.7. Configure Topology Hiding – Avaya IP Office

The **Topology Hiding** screen allows an administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. From the menu on the left-hand side, select **Global Profiles → Topology Hiding**.

- Select **default** in **Topology Hiding Profiles**.
- Click **Clone**.
- Enter **Clone Name**: **From_IPO_14** and click **Finish** (not shown).
- Select **To_IPO_14** in **Topology Hiding Profiles** and click **Edit** button to modify as below:
  For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **10.10.97.174**

  For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **10.10.98.14**

  For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **10.10.98.14**
- Click **Finish** (not shown).

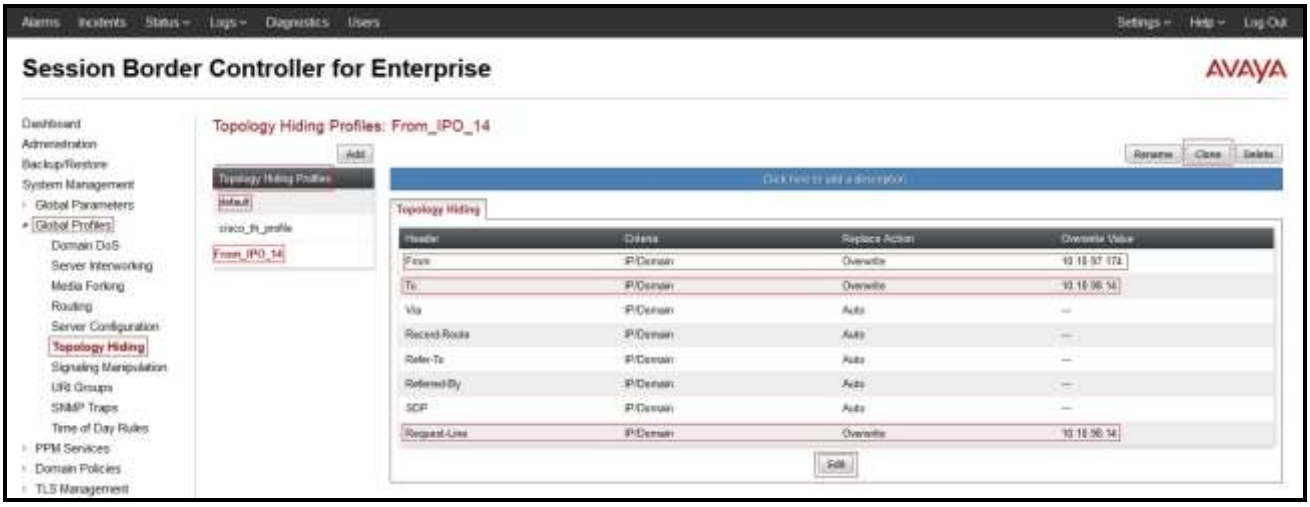

Figure 41 - Topology Hiding Avaya IP Office

6.3. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

6.3.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - **Name**: **Network_A1**.
  - **Default Gateway**: **10.10.97.129**.
  - **Subnet Mask**: **255.255.255.192**.
  - **Interface**: **A1** (This is the Avaya SBCE inside interface).
  - Click the **Add** button to add the **IP Address** for inside interface: **10.10.97.174**.
  - Click the **Finish** button to save the changes.

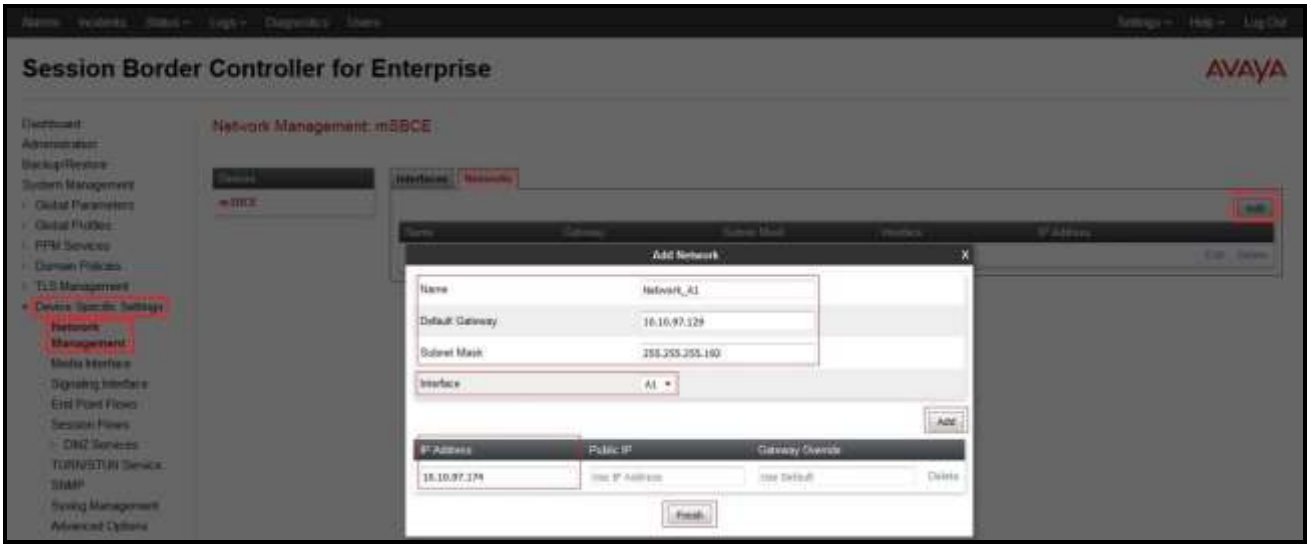

Figure 42 - Network Management – Inside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- Select **Networks** tab and click the **Add** button to add a network for the outside interface as follows:
  - **Name**: **Network_B1**.
  - **Default Gateway**: **10.10.98.97**.
  - **Subnet Mask**: **255.255.255.224**.
  - **Interface**: **B1** (This is the Avaya SBCE outside interface).
  - Click the **Add** button to add the **IP Address** for outside interface: **10.10.98.106**.
  - Click the **Finish** button to save the changes.

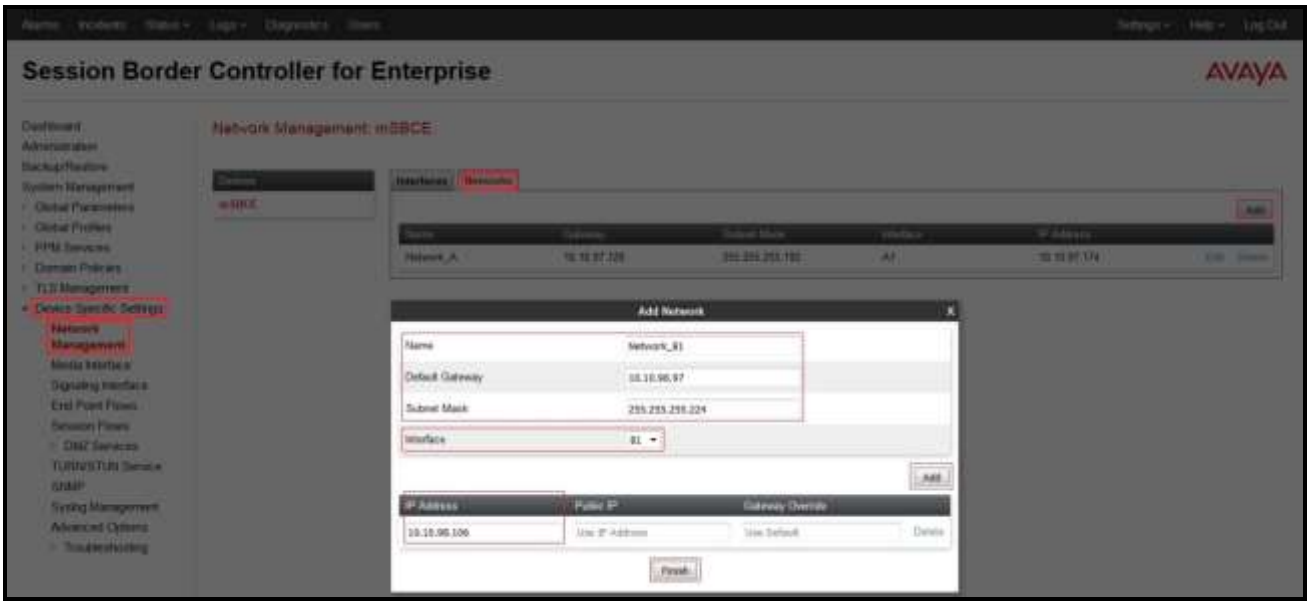

Figure 43 - Network Management – Outside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- Select the **Interfaces** tab.
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state.

Figure 44 - Network Management – Interface Status

6.3.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya SBCE can be used for both inside and outside ports.
From the menu on the left-hand side, **Device Specific Settings → Media Interface**.

- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **InsideMedia**.
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.97.174** (Avaya SBCE internal IP address toward Avaya IP Office).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).
- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **OutsideMedia**.
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.106** (Avaya SBCE external IP address toward Line Systems SIP Trunk).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).

The screen below shows the configured media interfaces:

Figure 45 - Media Interface

6.3.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.
From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**.

- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **InsideSIP**.
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.97.174** (Avaya SBCE internal IP address toward Avaya IP Office).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).

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

- Select the **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **OutsideSIP**.
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.106** (Avaya SBCE external IP address toward Line Systems SIP trunk).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).

Note: For the internal interface, the Avaya SBCE was configured to listen for UDP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 as same by Line Systems.

The screen below shows the configured signaling interfaces:

Figure 46 - Signaling Interface

6.3.4. Configuration Server Flows

Server Flows allow an administrator to categorize signaling and apply various policies.

6.3.4.1 Create End Point Flows – Avaya IP Office

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter the followings:
  - **Flow Name**: **IPO Flow**.
  - **Server Configuration**: **IPO_14** (see **Section 6.2.3**).
  - **URI Group**: *****.
  - **Transport**: *****.
  - **Remote Subnet**: *****.
  - **Received Interface**: **OutsideSIP** (see **Section 6.3.3**).
  - **Signaling Interface**: **InsideSIP** (see **Section 6.3.3**).
  - **Media Interface**: **InsideMedia** (see **Section 6.3.2**).
  - **End Point Policy Group**: **default-med**.
  - **Routing Profile**: **To_SP4** (see **Section 6.2.6**).
  - **Topology Hiding Profile**: **From_IPO_14** (see **Section 6.2.7**).
  - Click **Finish**.

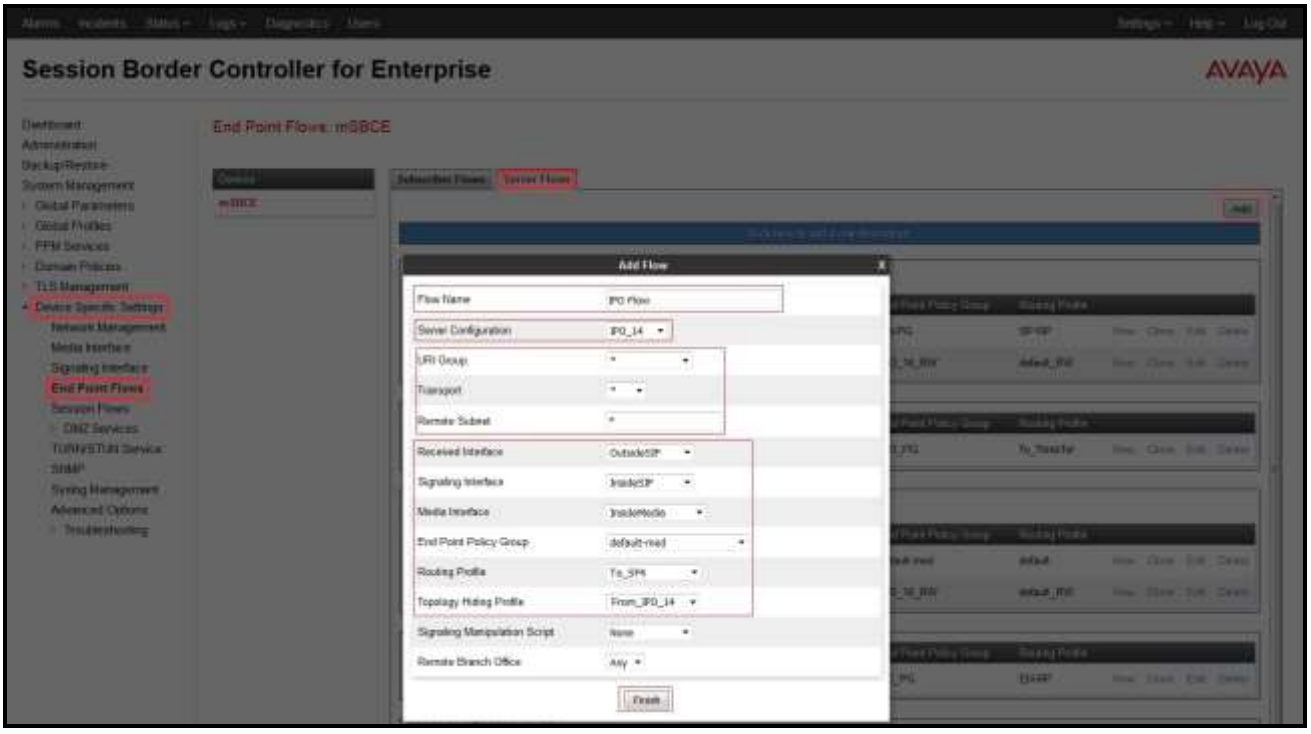

Figure 47 - End Point Flow to Line Systems

6.3.4.2 Create End Point Flows – Line Systems

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter the followings:
  - **Flow Name**: **SP4 Flow**.
  - **Server Configuration**: **SP4** (see **Section 6.2.4**).
  - **URI Group**: *****.
  - **Transport**: *****.
  - **Remote Subnet**: *****.
  - **Received Interface**: **InsideSIP** (see **Section 6.3.3**).
  - **Signaling Interface**: **OutsideSIP** (see **Section 6.3.3**).
  - **Media Interface**: **OutsideMedia** (see **Section 6.3.2**).
  - **End Point Policy Group**: **default-med**.
  - **Routing Profile**: **To_IPO_14** (see **Section 6.2.5**).
  - **Topology Hiding Profile**: **default**.
  - Click **Finish**.

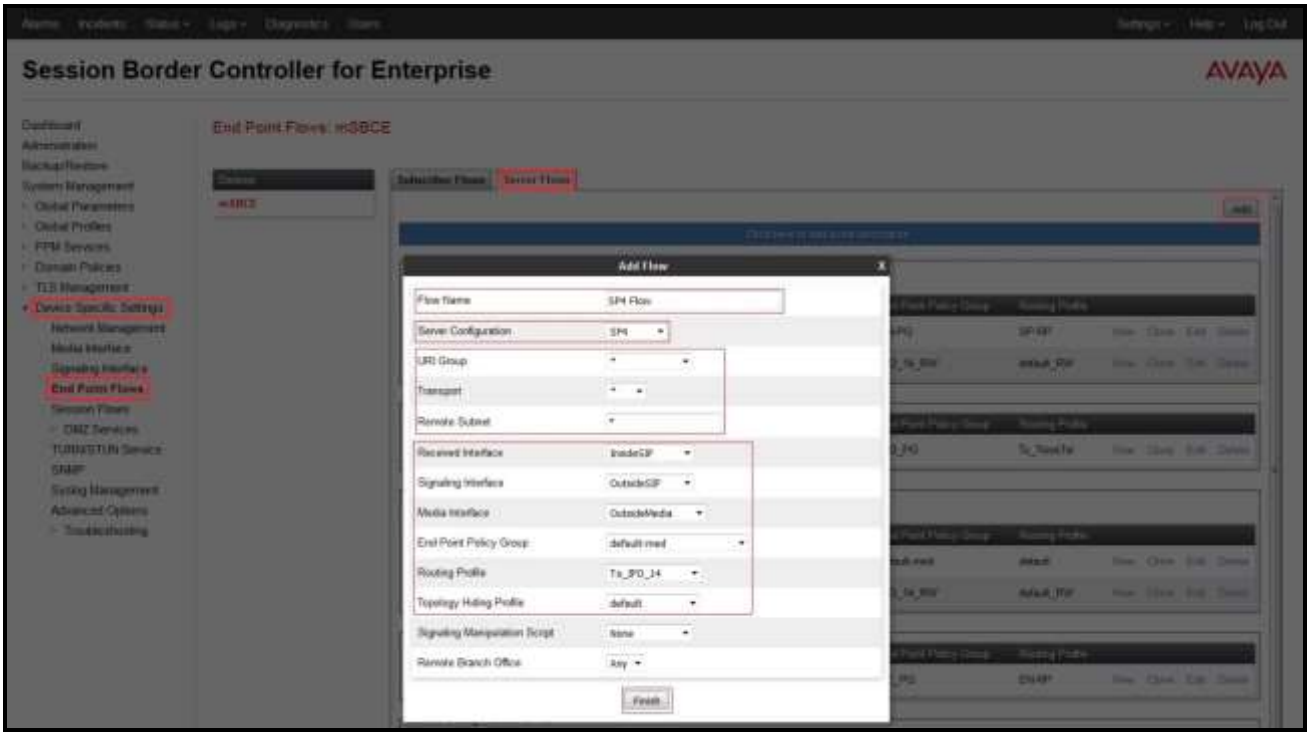

Figure 48 - End Point Flow from Line Systems

7. Line Systems SIP Trunk Configuration

Line Systems is responsible for the configuration of Line Systems SIP Trunk Service. The customer must provide the IP address used to reach the Avaya SBCE at the enterprise. Line Systems will provide the customer necessary information to configure the SIP connection between Avaya SBCE and Line Systems. The provided information from Line Systems includes:

- IP address and port number used for signaling or media servers through any security.
- DID numbers.
- Line Systems SIP Trunk Specification (If applicable).

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** for each channel (The below screen shot showed 2 active calls at present time).

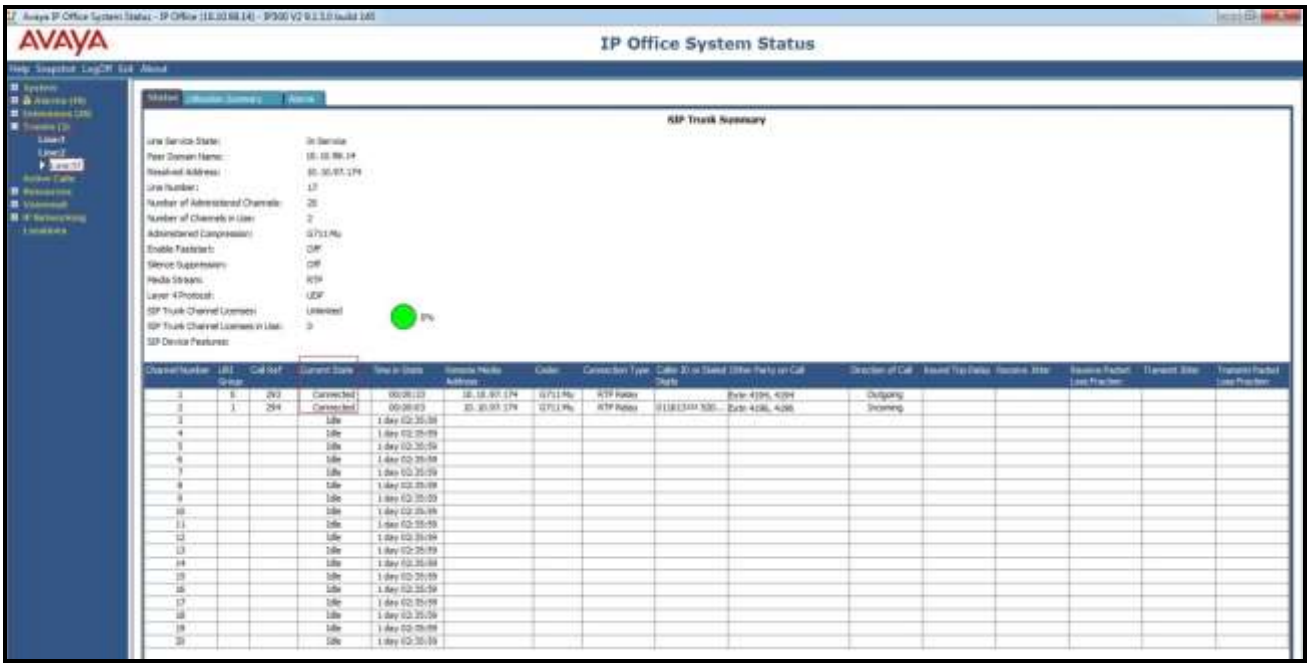

Figure 49 – SIP Trunk status

- Use the Avaya IP Office System Status application to verify that no alarms are active on the SIP line. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select **Alarm → Trunks** to verify that no alarms are active on the SIP line.

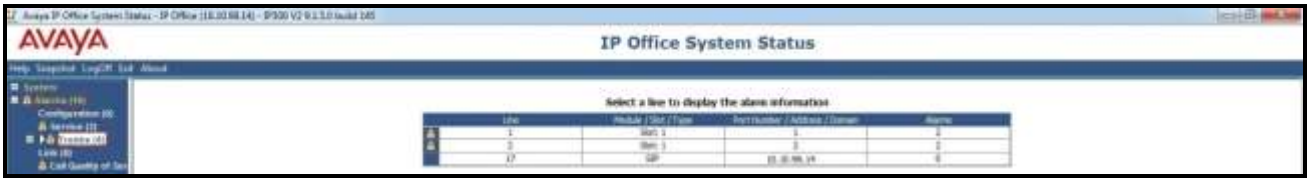

Figure 50 – SIP Trunk alarm

- Verify that a phone connected to the PSTN can successfully place a call to 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.
- Use a network sniffing tool e.g. Wireshark to monitor the SIP signaling between the enterprise and Line Systems. The sniffer traces are captured at the public interface of the Avaya SBCE.

9. Conclusion

Line Systems passed compliance testing excepting the limitation in **Section 2.2**. These Application Notes describe the procedures required to configure the SIP connections between Avaya IP Office and Avaya SBCE, Avaya SBCE and the Line Systems system as shown in **Figure 1**.

10. Additional References

[1] IP Office 9.1 Administering Avaya IP Office Platform with Manager, Release 9.1, Issue 10.32, November 2015.
[2] Deploying Avaya IP Office™ Platform Solution, Release 9.1, Issue 02.13, October 2015.
[3] Using Avaya Communicator for Web, Release 1.0, Issue 1.0.4, October 2015.
[4] Using Avaya Communicator for Windows on IP Office, Release 9.1.2, April 2015.
[5] Avaya Session Border Controller for Enterprise Overview and Specification, Release 7.0, Issue 1, August 2015
[6] Administering Avaya Session Border Controller for Enterprise, Release 7.0, Issue 3, January 2016
[7] Avaya Session Border Controller for Enterprise 7.0 Release Notes, Issue 1, August 2015
[8] 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/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html

Product documentation for Line Systems SIP Trunking may be found at:
http://www.linesystems.com/services/voice/.

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, refer to **Section 10**.

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 (SIP mode) 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 Line Systems Internet Service located between the Remote Worker private LAN and the public Internet.

Provisioning of the Line Systems router is beyond the scope of this document.

11.1. Provisioning Avaya SBCE for Remote Worker

Provisioning of the Avaya SBCE to support Avaya IP Office SIP connection to the service provider is described in **Section 6**. The following sections build on that provisioning.

11.1.1. Network Management

This section shows the **Network Management** configuration of the Avaya SBCE to support Remote Worker. For this purpose, the Avaya SBCE is configured with a second outside IP address assigned to physical interface B1, and a second inside IP address assigned to physical interface A1.

The following IP addresses were used on the Avaya SBCE in the configuration used for the compliance test:
10.10.97.174 is the inside IP address previously provisioned for SIP Trunking with Avaya IP Office (see **Section 6.3.1**).
10.10.97.173 is the new inside IP address for Remote Worker.
10.10.98.106 is the outside IP address previously provisioned for SIP Trunking with Line Systems (see **Section 6.3.1**).
10.10.98.102 is the new outside IP address for Remote Worker.

On the **Networks** tab, select **Add** to create an entry for **10.10.97.173** on interface **A1**, then select **Save** (not shown).
On the **Networks** tab, select **Add** to create an entry for **10.10.98.102** on interface **B1**, then select **Save** (not shown).

Figure 51 – Remote Worker Network Management

11.1.2. Signaling Interfaces

Two new Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Both interfaces **InsideSIPRW** and **OutsideSIPRW** support **TCP Port 5060**.
From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **InsideSIPRW**.

- **Signaling IP** = **10.10.97.173**.
- **TCP Port** = **5060**.

From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **OutsideSIPRW**.

- **Signaling IP** = **10.10.98.102**.
- **TCP Port** = **5060**.

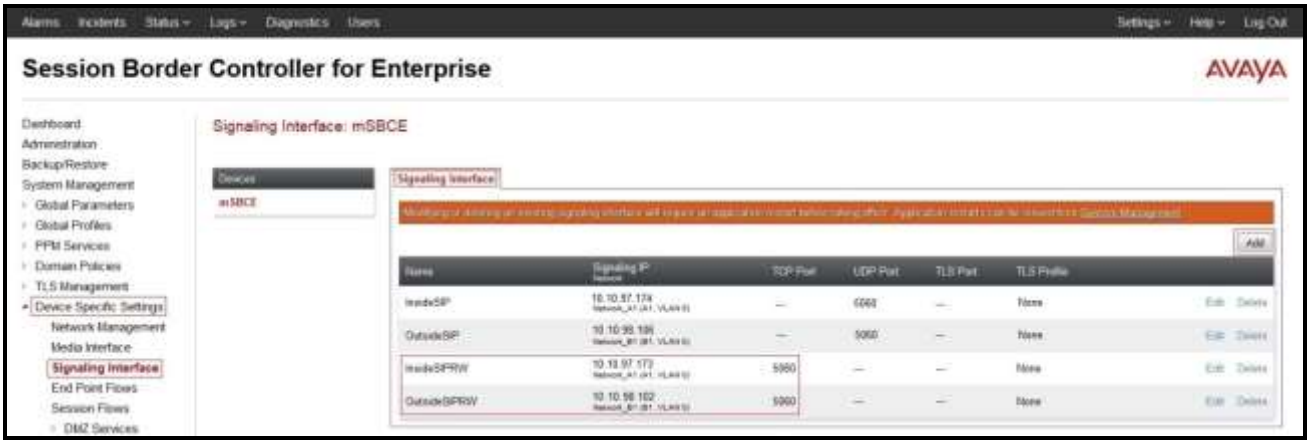

Figure 52 – Remote Worker Signaling Interface

Signaling Interface **InsideSIPRW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.8.2**). Signaling Interface **OutsideSIPRW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.8.1**), and in the Remote Worker Server Flow (Refer to **Section 11.1.8.2**).

11.1.3. Media Interface

Two new Media interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **InsideMediaRW** using the parameters shown below:

- **Media IP** = **10.10.97.173**.
- **Port Range** = **35000 – 55000**.

From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **OutsideMediaRW** using the parameters shown below:

- **Media IP** = **10.10.98.102**.
- **Port Range** = **35000 – 55000**.

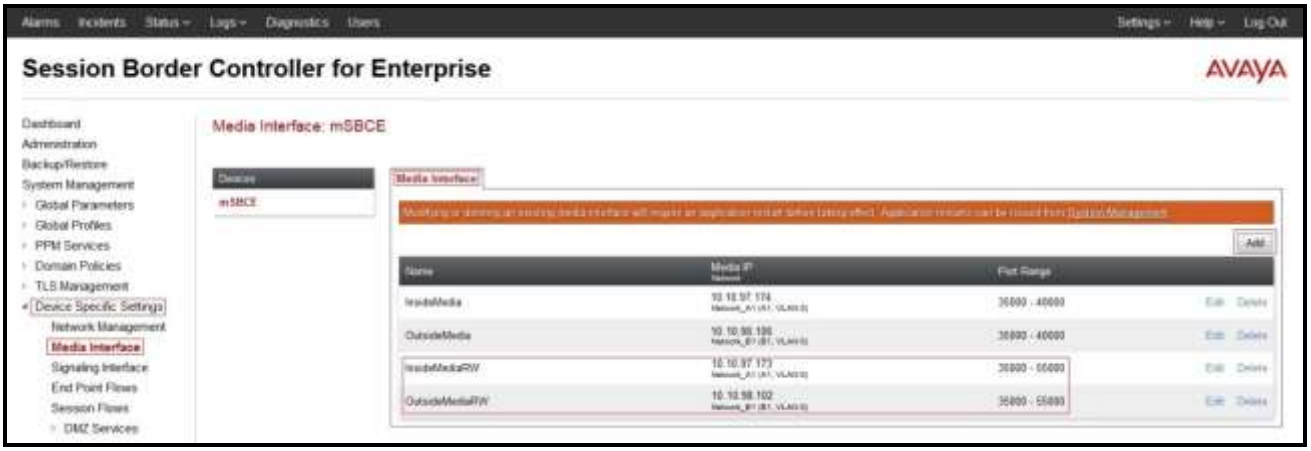

Figure 53 – Remote Worker Media Interface

Media Interface **InsideMediaRW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.8.2**). Media Interface **OutsideMediaRW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.8.1**).

11.1.4. Server Profile for Avaya IP Office

TCP transport protocol (which is required for the Remote Worker connection between the Avaya SBCE and Avaya IP Office) needs to be added to the existing **IPO_14** Server Profile (see **Section 6.2.3**).

From **Global Profiles** on the left-hand menu, select **Server Configuration**

- Select the existing **IPO_14** in **Sever Profiles** and click on **Edit**.
- On **General** tab, enter the following:
  - **IP Address/FQDN**: **10.10.98.14** (Avaya IP Office LAN2 port interface IP address).
  - **Port**: **5060**.
  - **Transport**: **TCP**.

Figure 54 – Remote Worker Server Configuration

11.1.5. Routing Profiles

Two new Routing Profiles are required to support Remote Worker.
From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **To_IPO_14_RW** (not shown).

- **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**.
- **Server Configuration**: **IPO_14** (Refer to **Section 11.1.4**).
- **Next Hop Address**: Select **10.10.98.14:5060 (TCP)** (Avaya IP Office LAN2 port interface IP address).
- Click **Finish** to submit the changes.

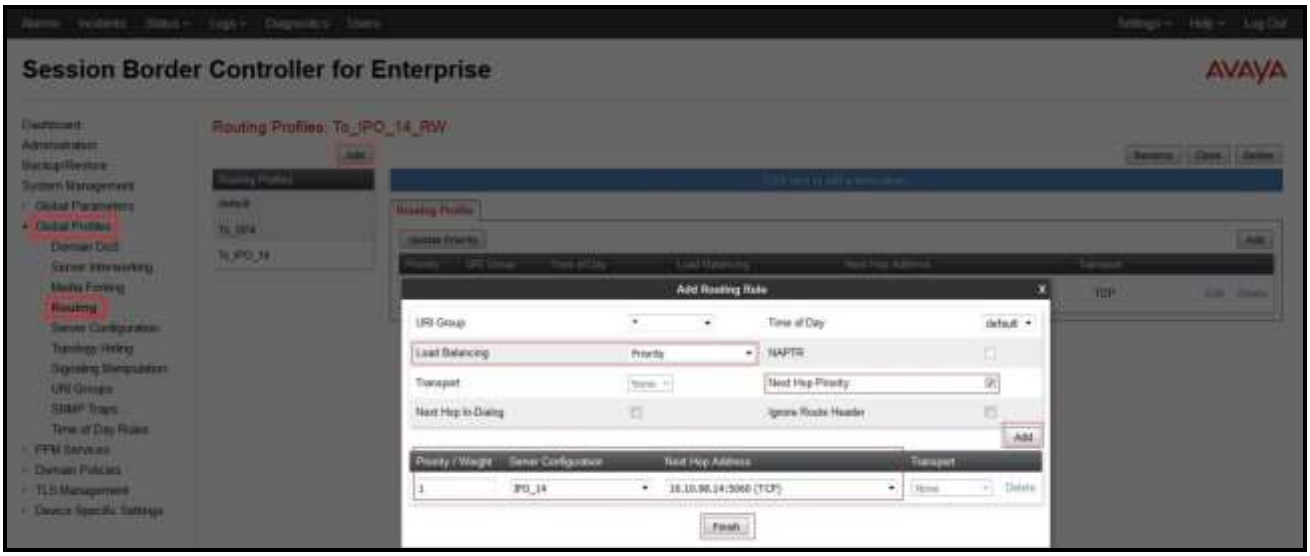

Figure 55 – Remote Worker Routing

From the menu on the left-hand side, select **Global Profiles → Routing**, select the existing **default Routing Profiles** and click on the **Clone** button, and name it **default_RW** and click **Finish** (not shown) to submit the changes. The **default_RW** was created as below.

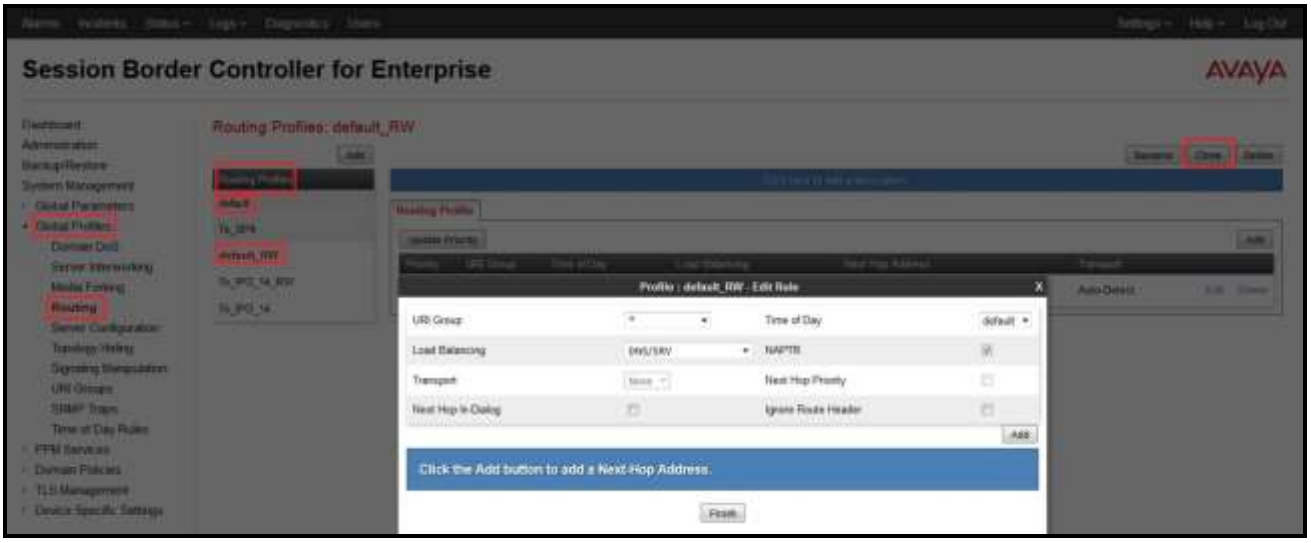

Figure 56 – Remote Worker Default Routing

The Routing Profile **To_IPO_14_RW** is used in the Remote Worker Subscriber Flow (Refer to **Section 11.1.8.1**). The Routing Profile **default_RW** is used in the Remote Worker Server Flow (Refer to **Section 11.1.8.2**).

11.1.6. User Agent

User Agents are created for each type of Remote Worker endpoint used. In the configuration for the compliance test, the Avaya Communicator for Windows (SIP) softphone was used, and its configuration is shown below.

From the menu on the left-hand side, select **Global Parameters → User Agents**, and click **Add** button to create a new User Agent.

- Enter the following:
- **Name** = **Avaya Communicator**
- **Regular Expression = Avaya Flare.***

In this expression, "Avaya Flare.*" will match any software version listed after the user agent name.

Figure 57 – Remote Worker User Agent

The **Avaya Communicator** User Agent is defined in the Remote Worker Subscriber Flow (see **Section 11.1.8.1**).

11.1.7. End Point Policy Groups

The End Point Policy Group is defined for Remote Worker. Group **IPO_14_RW** is defined for the RTP connection.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add** button to create a new End Point Policy Group.
- Enter a name (e.g., **IPO_14_RW**), and click on **Next** (not shown).
- The **Policy Group** window will open. Select the information as shown in capture below.

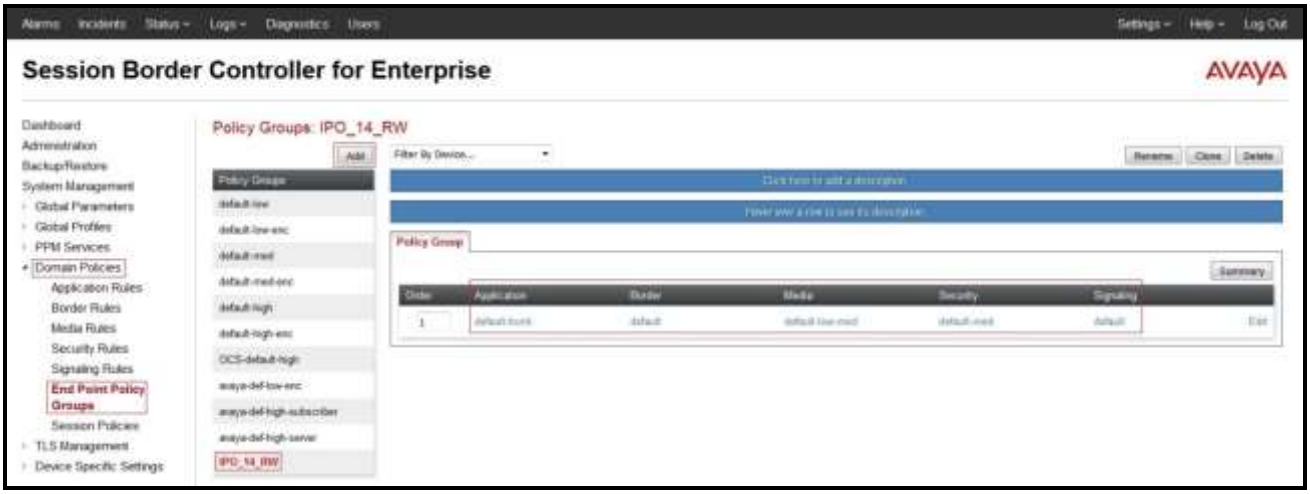

Figure 58 – Remote Worker Endpoint Policy Group

End Point Policy Group **IPO_14_RW** is used in the Subscriber Flow (Refer to **Section 11.1.8.1**) and in the Server Flow (Refer to **Section 11.1.8.2**).

11.1.8. End Point Flows

A Subscriber Flow and a Server Flow are created for Remote Worker.

11.1.8.1 Subscriber Flow

A **Subscriber Flow** is defined as follows:

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**.

On **Subscriber Flows** tab, click on **Add** and the **Criteria** window will open.

- Enter **Flow Name** (e.g., **Avaya Communicator**).
- **URI Group** = *****.
- **User Agent** = **Avaya Communicator** (Refer to **Section 11.1.6**).
- **Source Subnet** = ***** (default).
- **Via Host** = ***** (default).
- **Contact Host** = ***** (default).
- **Signaling Interface** = **OutsideSIPRW** (Refer to **Section 11.1.2**).

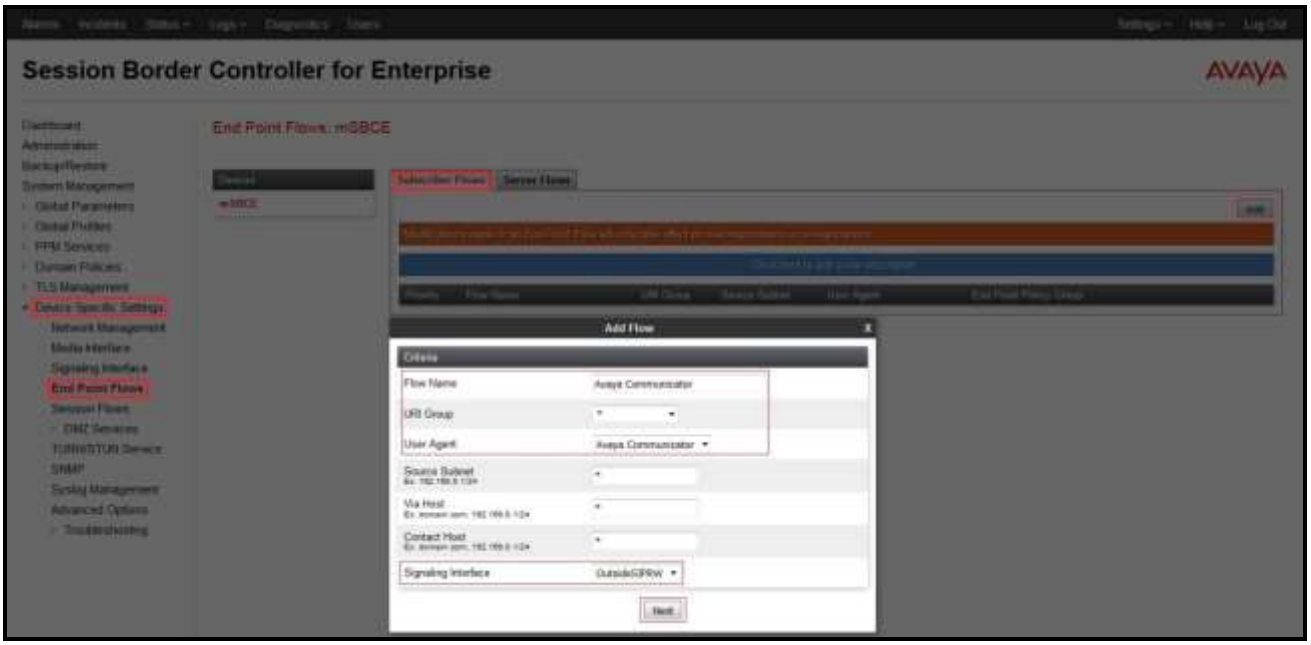

Figure 59 – Remote Worker Subscriber Flow 1

Click on **Next** and the **Profile** window will open. Enter the followings:

- **Source** = **Subscriber**
- **Methods Allowed Before REGISTER**: Leave as default.
- **Media Interface** = **OutsideMediaRW** (Refer to **Section 11.1.3**).
- **End Point Policy Group = IPO_14_RW** (Refer to **Section 11.1.7**).
- **Routing Profile = To_IPO_14_RW** (Refer to **Section 11.1.5**).
- **Topology Hiding Profile** = **None**.
- **TLS Client Profile** = **None**.
- **Signaling Manipulation Script** = **None**.
- **Presence Server Address** = **Blank**.
- Click **Finish** to submit the changes.

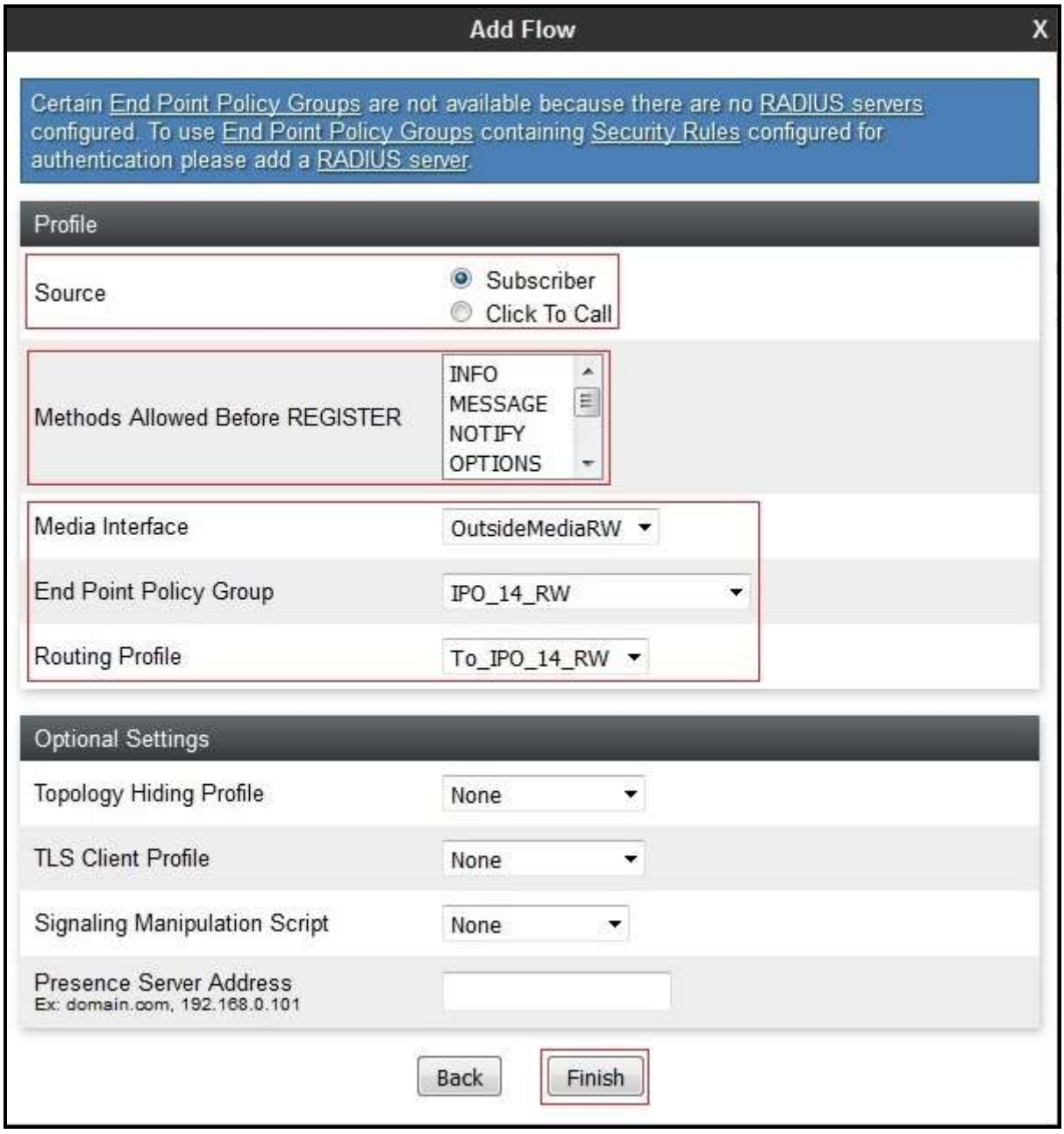

Figure 60 – Remote Worker Subscriber Flow 2

The **Subscriber Flows** tab shown below displays the finished Subscribe Flow **Avaya Communicator**:

Figure 61 – Remote Worker Subscriber Flow 3

Click on the highlighted **View** link brings up the following **View Flow** window.

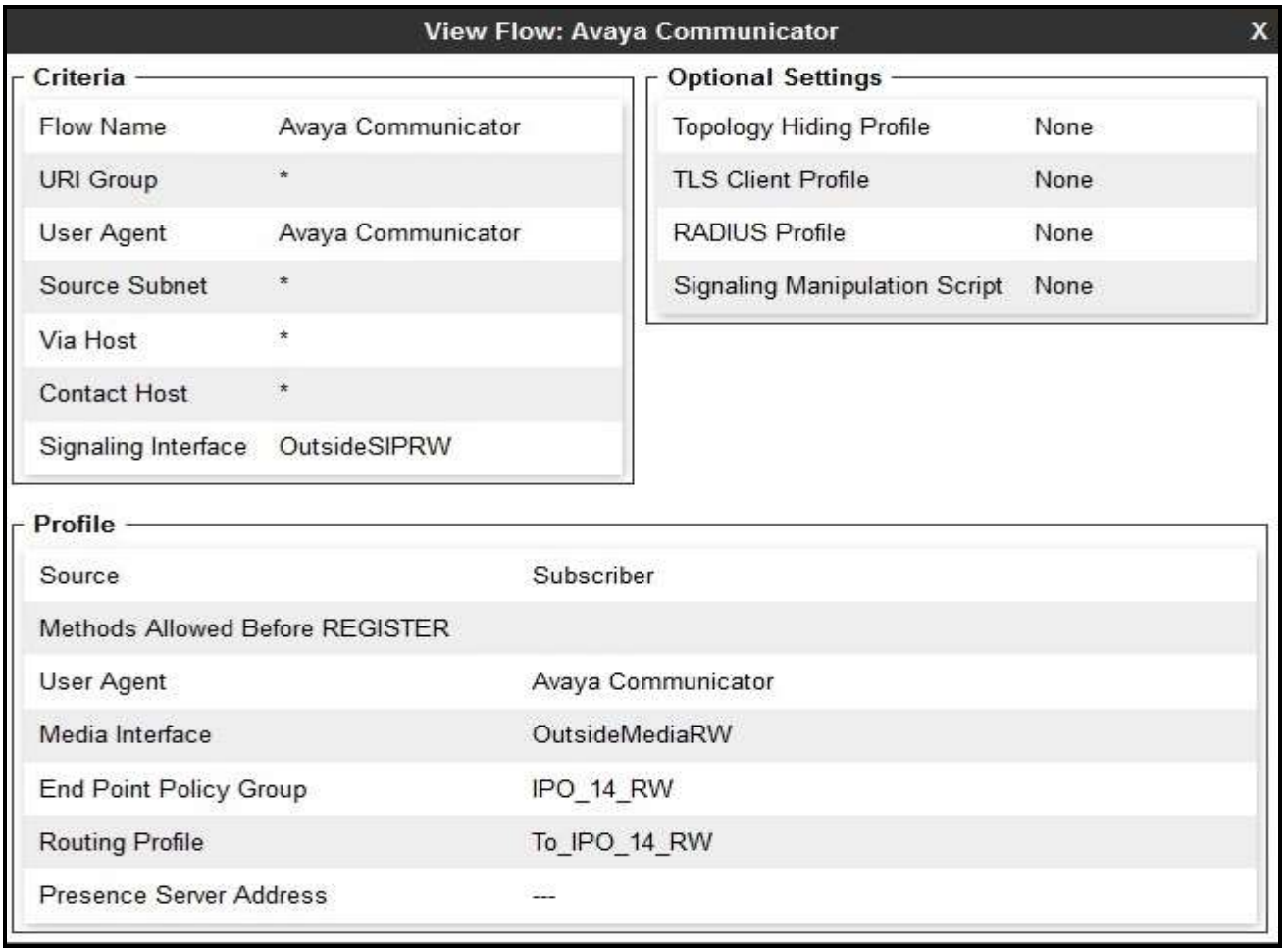

Figure 62 – Remote Worker Subscriber Flow 4

11.1.8.2 Server Flow

The following section shows the new **Server Flow** settings for Remote Worker.
From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**.
On **Server Flows** tab, click on **Add** to create a new server flow for Remote Worker.
Enter the following:

- **Flow Name = IPO_14_RW**
- **Server Configuration** = **IPO_14** (Refer to **Section 11.1.4**).
- **URI Group** = ***** (default).
- **Transport** = ***** (default).
- **Remote Subnet** = ***** (default).
- **Received Interface** = **OutsideSIPRW** (Refer to **Section 11.1.2**).
- **Signaling Interface** = **InsideSIPRW** (Refer to **Section 11.1.2**).
- **Media Interface** = **InsideMediaRW** (Refer to **Section 11.1.3**).
- **End Point Policy Group** = **IPO_14_RW** (Refer to **Section 11.1.7**).
- **Routing Profile** = **default_RW** (Refer to **Section 11.1.5**).
- **Topology Hiding Profile** = **None** (default).
- **Signaling Manipulation Script** = **None** (default).
- **Remote Branch Office = Any** (default).
- Click **Finish** to submit the changes.

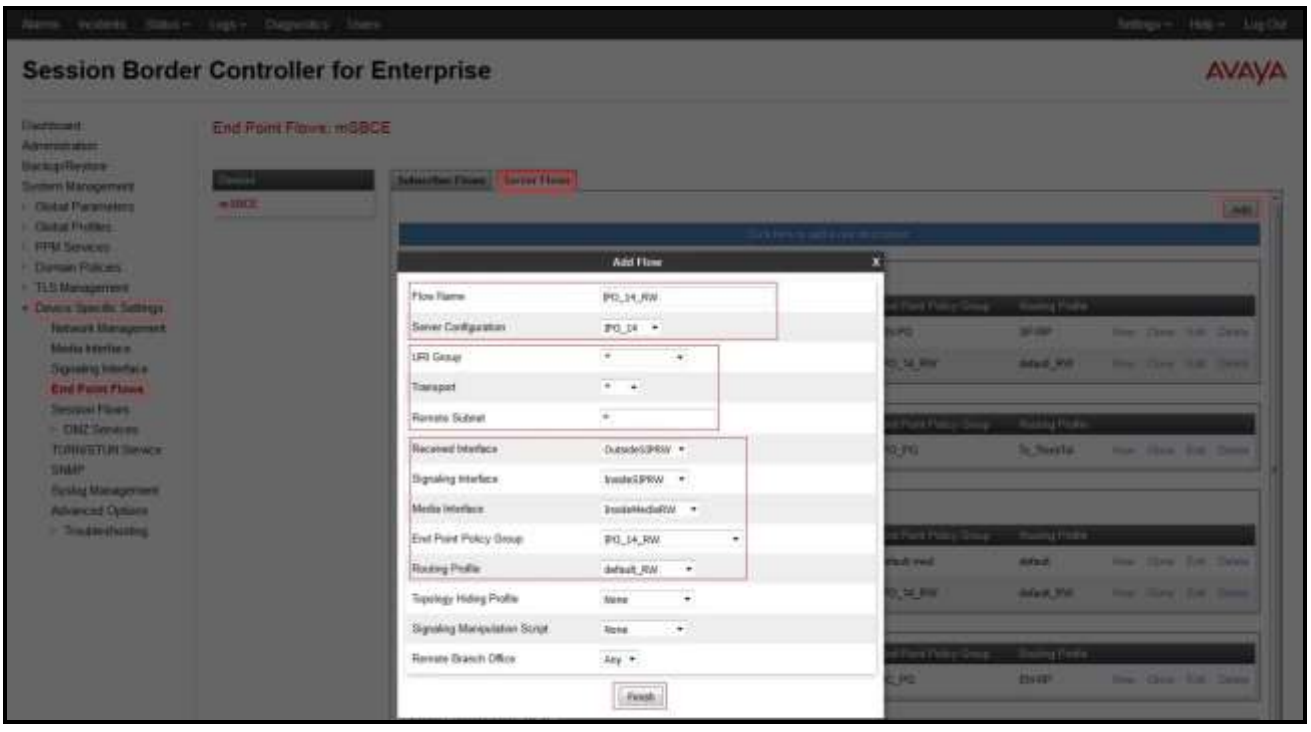

Figure 63 – Remote Worker Server Flow 1

If this Remote Worker server flow is listed ahead of the flow for SIP Trunking (**IPO Flow** as created in **Section 6.3.4.1**), enter **2** in the **Priority** box at the start of the Remote Worker flow entry and click the **Update** button under the server name. The completed flow should show up in the **Server Flows** tab as below.

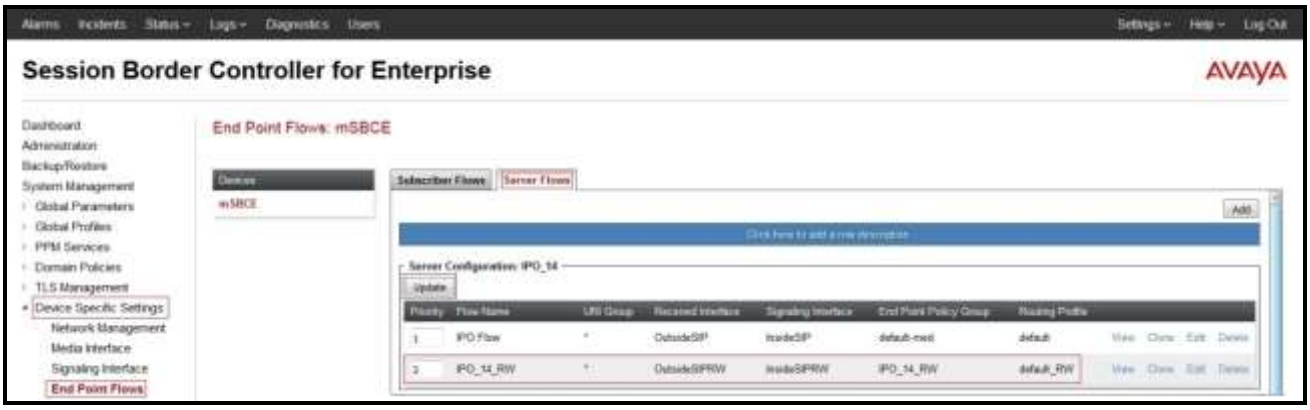

Figure 64 – Remote Worker Server Flow 2

11.2. Remote Worker Endpoint Configuration on Avaya IP Office

The Remote Worker - Avaya Communicator for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration.

11.2.1. Extension and User Configuration

No special configurations are required to create the Remote Worker extension and user in Avaya IP Office. Follow the same standard procedures for creating a local extension and user for Avaya Communicator for Windows.

The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Communicator for Windows, the **Enable Softphone** and **Enable Communicator** options are selected.

Note: Do not check the **Enable Remote Worker** option. This is only enabled for Avaya IP Office "native" Remote Worker configurations, not for Remote Worker configurations utilizing the Avaya SBCE.

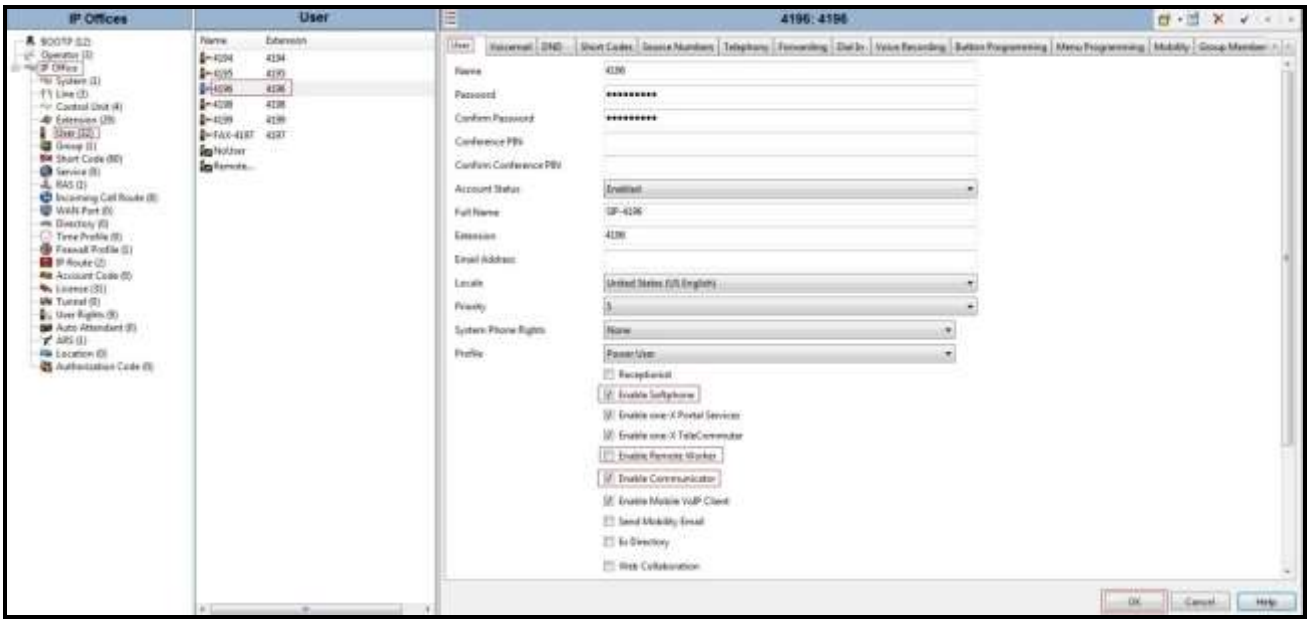

Figure 65 – Remote Worker User Configuration 1

The **SIP** tab for the Remote User is configured the same way as with local Avaya IP Office user (see **Section 5.9**).

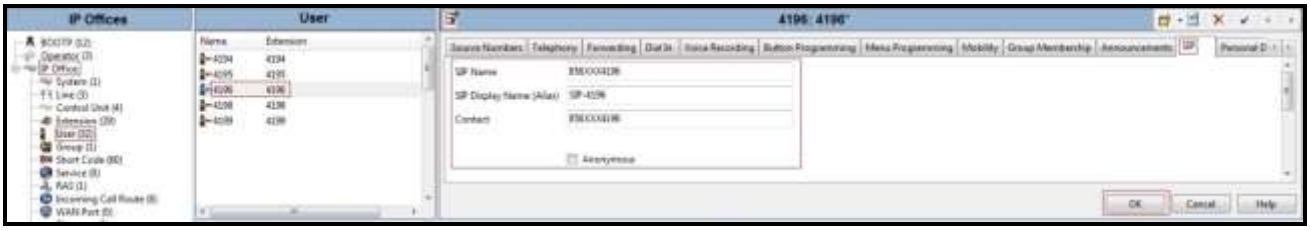

Figure 66 – Remote Worker User Configuration 2

11.2.2. Incoming Call Route

Follow the same procedures described in **Section 5.10** for defining an Incoming Call Route to the Remote Worker.

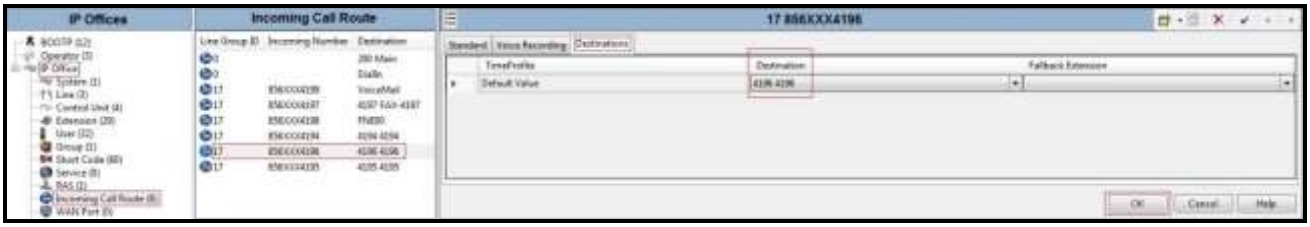

Figure 67 – Remote Worker Incoming Call Route

11.3. Remote Worker - Avaya Communicator for Windows Settings

The following screen illustrates Avaya Communicator for Windows administration settings for Remote Worker as used in the reference configuration.
After opening the Avaya Communicator for Windows application, select the Settings icon, select **Server** from the Settings menu, and enter the following:

- **Server address** = **10.10.98.102** (IP address of Remote Worker outside interface B1 on Avaya SBCE (see **Section 11.1.1**).
- **Server port** = **5060**.
- **Transport type** = **TCP**.
- **Domain** = **10.10.98.14 (**Domain name was defined in LAN2→ VoIP tab in **Section 5.3**).
- Click **OK** the save the changes.

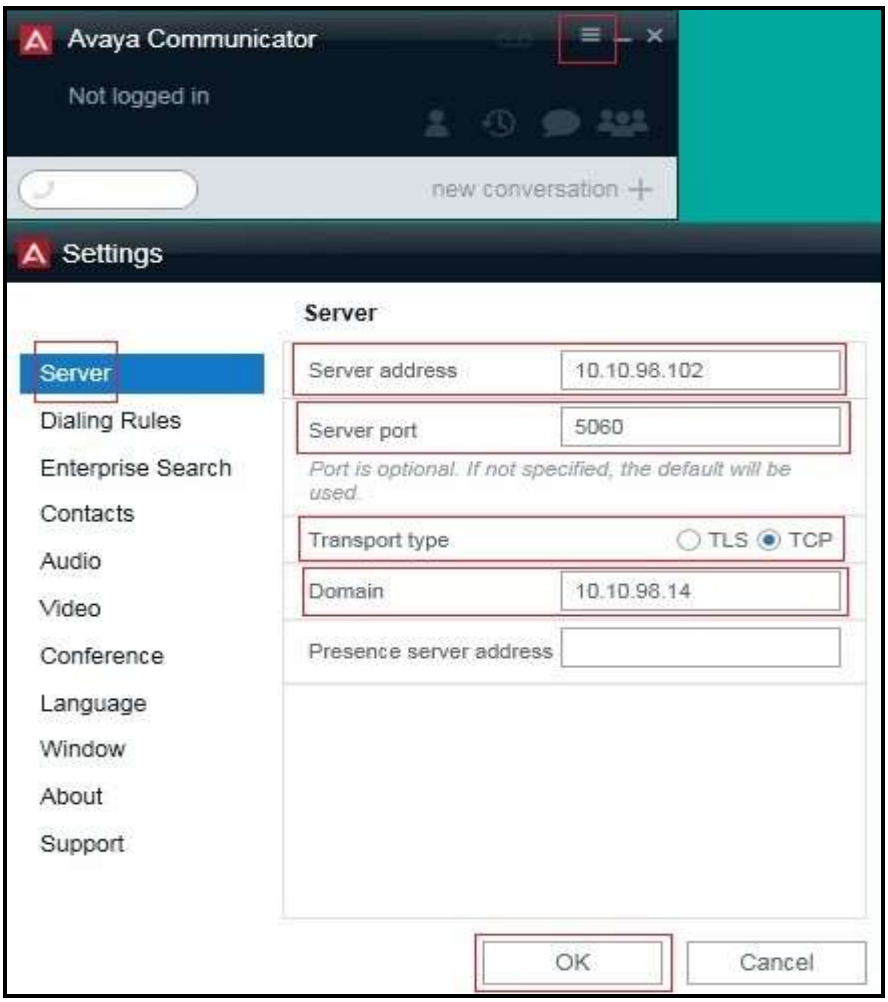

Figure 68 – Remote Worker - Avaya Communicator for Windows Settings

Note: In the compliance testing, only audio calls were tested with RTP media for Avaya Communicator for Windows.

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.