Avaya Solution & Interoperability Test Lab

Application Notes for Configuring IntelePeer SIP Trunking Service with Avaya IP Office R9.0.1 and Avaya Session Border Controller for Enterprise 6.2.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between IntelePeer and an enterprise solution using Avaya IP Office Release 9.0.1 and Avaya Session Border Controller for Enterprise 6.2.1.

The IntelePeer SIP Trunking Service provides PSTN access via a SIP trunk between the enterprise and the IntelePeer network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

IntelePeer 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 IntelePeer and an enterprise solution using Avaya IP Office Release 9.0.1 and Avaya Session Border Controller for Enterprise 6.2.1.

The IntelePeer SIP Trunking Service referenced within these Application Notes is positioned for customers who have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

The IntelePeer SIP Trunking Service will enable delivery of origination and termination of local, long-distance, Toll-free, international, and other types of calls across a single broadband IP connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE).

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the IntelePeer SIP Trunking Service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site comprised of an Avaya IP Office 500 V2 running Release 9.0.1 software, Avaya Voicemail Pro messaging application, Avaya H.323 and SIP hard phones, and SIP-based Avaya softphones. The enterprise solution connects to the IntelePeer network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

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 covered during the interoperability compliance test:

- Sending/receiving SIP OPTIONS queries to/from the service provider.
- Incoming calls from the PSTN to H.323 and SIP telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing calls to the PSTN from H.323 and SIP telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Various call types including: local, long distance, outbound toll-free and international.
- G.711MU and G.729A codecs.
- Caller ID presentation and Caller ID restriction.
- DTMF transmission using RFC 2833.
- Voicemail access and navigation for inbound and outbound calls.
- Telephony supplementary features such as hold and resume, transfer, and conference.

- Off-net call forwarding and call transfer/conference.
- Twinning on inbound calls to PSTN mobile phones.
- Use of SIP INVITE message for call redirection to the PSTN.
- Inbound and outbound long-duration calls stability.
- Inbound and outbound long hold time call stability.
- Response to incomplete call attempts and trunk busy or error conditions.
- T.38 fax.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Items not supported or not tested include the following:

- Inbound toll-free and emergency calls (911) were not tested as part of the compliance test.
- IntelePeer SIP Trunking does not support use of the SIP REFER method for network redirection (transferring calls with the PSTN back to the PSTN).
- IntelePeer SIP Trunking does not support Operator call (0), Operator-Assisted (0 + 10-digit), and Directory Assistance (411) calls.

2.2. Test Results

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

- **"200 OK" Contact Header –** For outbound calls, the Contact header in the "200 OK" message from IntelePeer to signal call connect contained the caller number instead of the number for the actual connected party (i.e., the callee number). As a consequence, if the call was terminated by the IP Office caller, the BYE message to IntelePeer would contain the caller DID number in its Request URI instead of the PSTN callee number. The call would terminate properly though the signaling was not clean as described. The same problem existed with the “200 OK” response from IntelePeer to the session-refresh re-INVITE messages from IP Office, with no negative impact observed. IntelePeer has been investigating this issue.
- **Codec Lockdown –** For outbound calls with multiple codes offered in the SDP of outbound INVITE, the call connect "200 OK" from IntelePeer contained the same set of codecs in the SDP instead of just the preferred coded (first in the list).
- **Session Refresh –** IntelePeer issued session refresh SIP re-INVITE messages towards the IP Office at 3-minute intervals for both inbound and outbound calls, but SIP messages from IntelePeer contained no information relating to session refresh handshake (e.g., Session-Expires, Min-SE headers).
- **RFC2833 Payload Type –** IntelePeer configured SIP Trunking to match to only one specific RFC2833 payload type. Payload type 101 was used for the compliance test. This static payload type configuration worked well for most of the Avaya IP Office endpoints. However, the Avaya Flare® Experience for Windows softphone used payload type 120 which IntelePeer was not able to match, resulting in failure of out-band DTMF tone transmission from this specific endpoint. IntelePeer was investigating a SIP Trunking

configuration capable of dynamically matching to different RFC2833 payload types from the enterprise site.

- **Outbound T.38 Fax Interworking with G.729A Codec –** IntelePeer did not initiate re-INVITE to switch to T.38. IP Office would time out eventually, failing the outbound fax when the voice codec was G.729A. Outbound T.38 fax interworking with the G.711MU codec worked successfully. Since IntelePeer recommends configuring G.711MU as the preferred codec, this would not be a problem in deployed customer environments.
- **Direct Media –** Starting with R9.0, Avaya IP Office offers a new Direct Media capability on IP Office 500 V2 that allows IP endpoints to send RTP media directly to each other rather than having all the media flow through the IP Office, using up VoIP resources. Though Direct Media was tested and verified for straight inbound / outbound calls during testing, the following issues were experienced when the Direct Media option was enabled:
  - When Direct Media was enabled, Avaya IP Office IP endpoints did not send RTP Events.
  - Only Direct Media *or* T.38 fax is supported on a SIP Line. The use of both features on the same SIP Line is not supported.
  - As a result of these issues, the recommended configuration is to have Direct Media disabled (see **Section 5.4.6**).

2.3. Support

Contact information for technical support on the IntelePeer SIP Trunking service:

- Email: support@intelepeer.com
- Telephone: (877) 780-8639

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

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The sample configuration shows an enterprise site connected to the IntelePeer SIP Trunking Service.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers.

The enterprise endpoints include both local extensions and Remote Worker phones that connect directly to the public Internet. The same Avaya SBCE was configured to connect to both the service provider network and Remote Worker using separate sets of public/private interfaces (**Figure 1** only shows the public/private interfaces used for connecting to the service provider network).

The Avaya IP Office 500 V2 at the enterprise site runs IP Office Release 9.0.1 software. Endpoints include various Avaya IP Telephones (with H.323 and SIP firmware) and SIP-based Avaya softphones (Avaya IP Office Softphone and Avaya Flare® Experience for Windows). The site also has a Windows PC running Avaya Voicemail Pro for providing voice messaging service to the Avaya IP Office users, and Avaya IP Office Manager for administering 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.

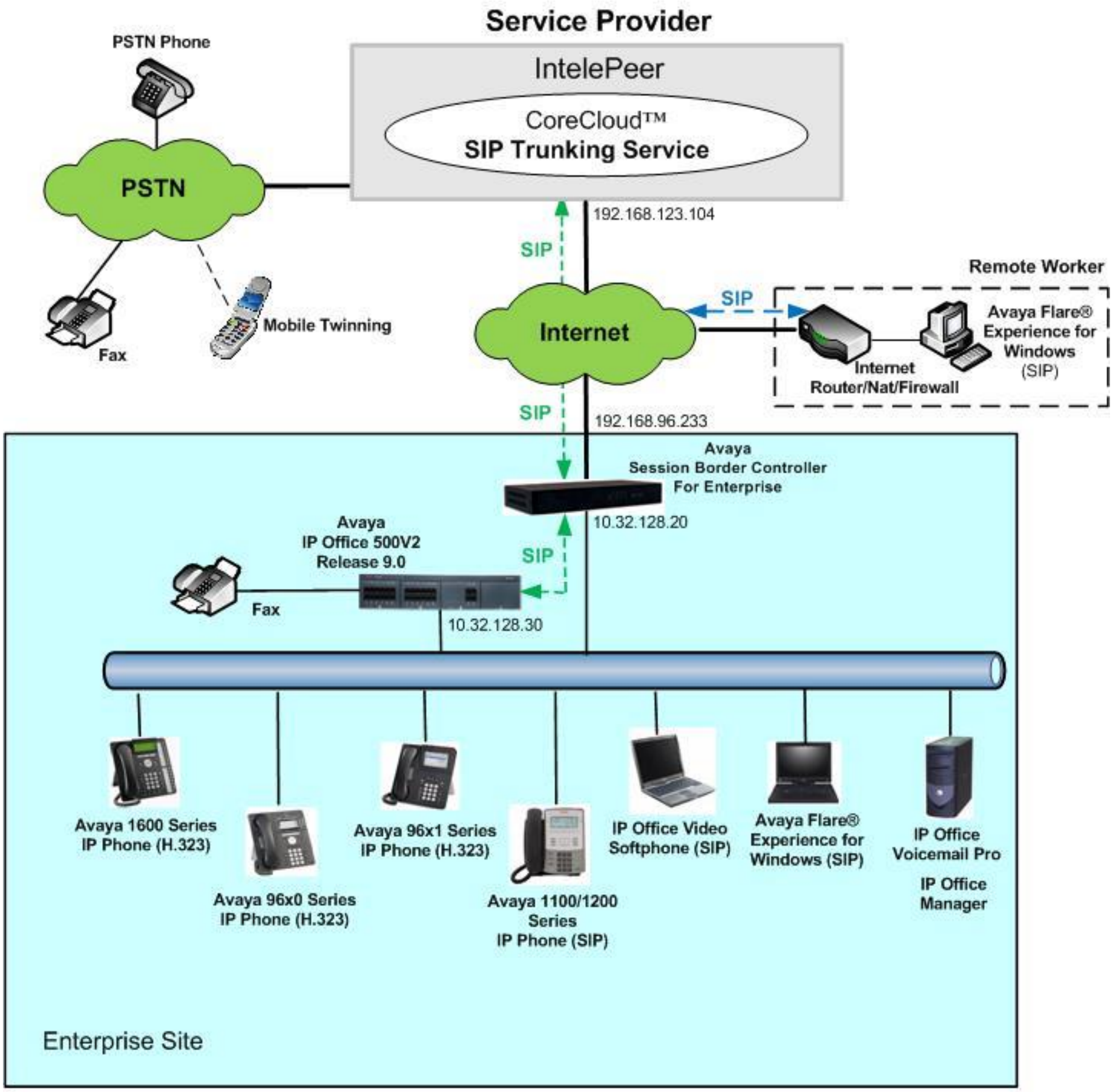


Figure 1: Test Configuration

For security purposes, any actual public IP addresses used in the compliance test were changed to 192.168.x.x throughout these Application Notes.

For the purposes of the compliance test, users dialed a prefix digit 8 or 9 plus N digits to send an outbound call to the number N across the SIP trunk to IntelePeer. The short code of 8 or 9 was stripped off by Avaya IP Office but the remaining N digits were sent to the service provider network. For calls within the North American Numbering Plan (NANP), the user dialed 11 (1 + 10) digits for long distance and local calls. Thus, for these NANP calls, Avaya IP Office sent 11 digits in the

Request URI and the To header of an outbound SIP INVITE message. IntelePeer also sent 10 digits in the Request URI and the To header 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 enterprise network such as a 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 Avaya IP Office must be allowed to pass through these devices.

The administration of the Avaya Voicemail Pro messaging service and endpoints on Avaya IP Office are standard. Since these configuration tasks are not directly related to the inter-operation with the IntelePeer SIP Trunking Service, they are not included in these Application Notes. The configuration for Remote Worker via Avaya SBCE is contained in the Appendix to this document.

4. Equipment and Software Validated

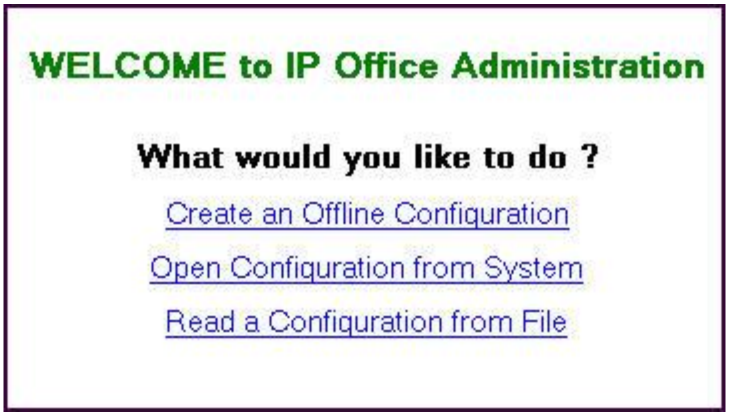
The following equipment and software/firmware were used for the sample configuration provided:

Avaya Telephony Components	
Equipment / Software	**Release / Version**
Avaya IP Office 500V2	9.0.100.845
Avaya IP Office COMBO6210/ATM4 Module	9.0.100.845
Avaya IP Office Manager	9.0.100.845
Avaya Preferred Edition (a.k.a Voicemail Pro)	9.0.1.0.53
Avaya Session Border Controller for Enterprise running on a Portwell CAD-0208 server	6.2.1.Q07
Avaya 1616 IP Telephones (H.323)	Avaya one-X Deskphone 1.3 SP4
Avaya 9611G IP Telephones (H.323)	Avaya one-X Deskphone 6.3.0.37_V452
Avaya 9630G IP Telephones (H.323)	Avaya one-X Deskphone 3.2.1.2A
Avaya 1120E IP Telephone (SIP)	4.03.18.00
Avaya 1140E IP Telephone (SIP)	4.03.18.00
Avaya IP Office Video Softphone (Windows)	3.2.3.49 68975
Avaya Flare® Experience for Windows	1.1.4.23
IntelePeer Components	
Equipment / Software	**Release / Version**
Taqua T7100 Multimedia Controller	3.0.0.29

Testing was performed with IP Office 500 V2 R9.0.1, but this testing also applies to IP Office Server Edition 9.0.1. Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running Avaya IP Office Manager, select **Start → Programs → IP Office → Manager** to launch the application. A screen that includes the following in the center may be displayed:



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

The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the Group Pane has been omitted, its content is shown as submenus in the Navigation pane. These panes (Navigation and Details) will be referenced throughout the Avaya IP Office configuration.

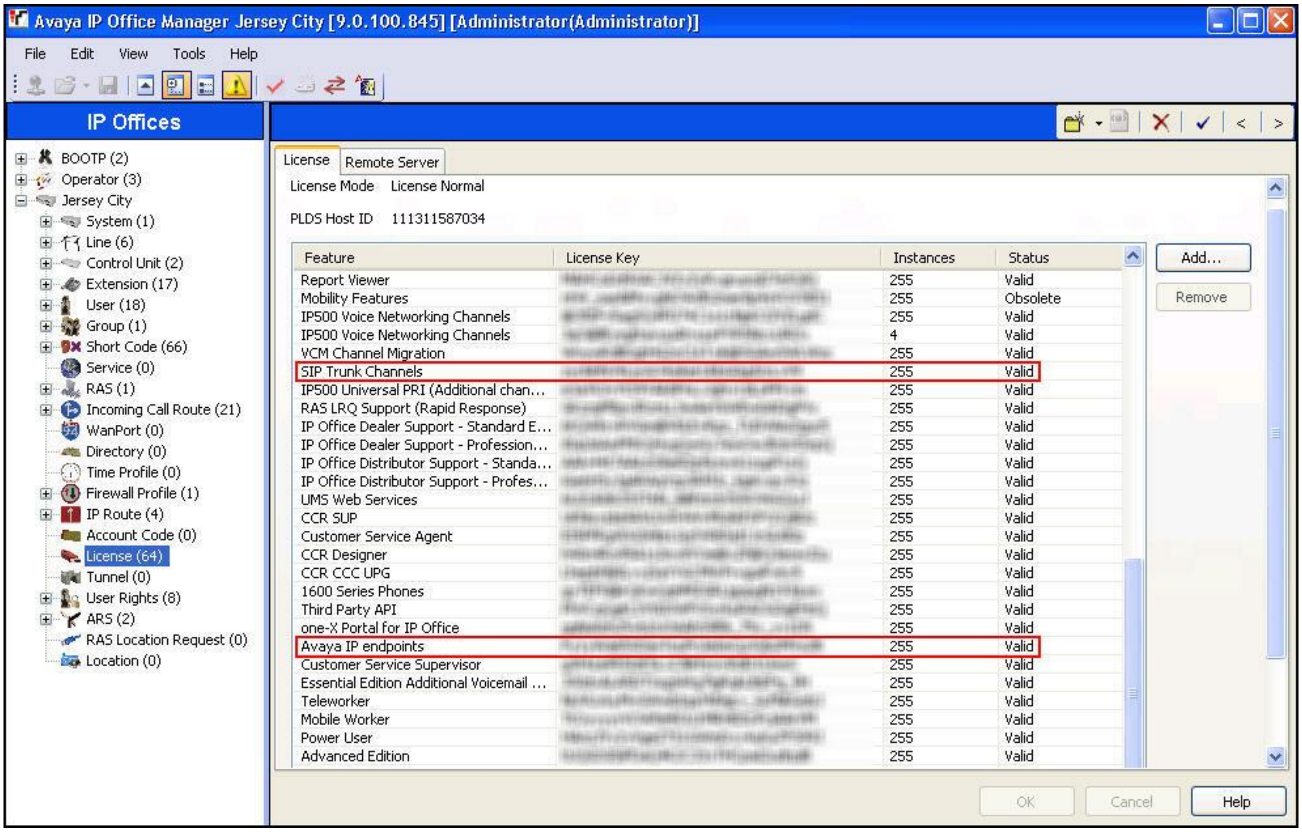
All licensing and feature configuration that is not directly related to the interface with the service provider (such as twinning and IP Office Softphone support) is assumed to already be in place.

In the sample configuration, **Jersey City** was used as the system name. All navigation described in the following sections (e.g., **License → SIP Trunk Channels)** appears as submenus underneath the system name **Jersey City** in the Navigation Pane. The configuration screens only highlight values/settings configured for the compliance test. Defaults were used for other values and may be customized based upon requirements in the field.

5.1. Licensing and Physical Hardware

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

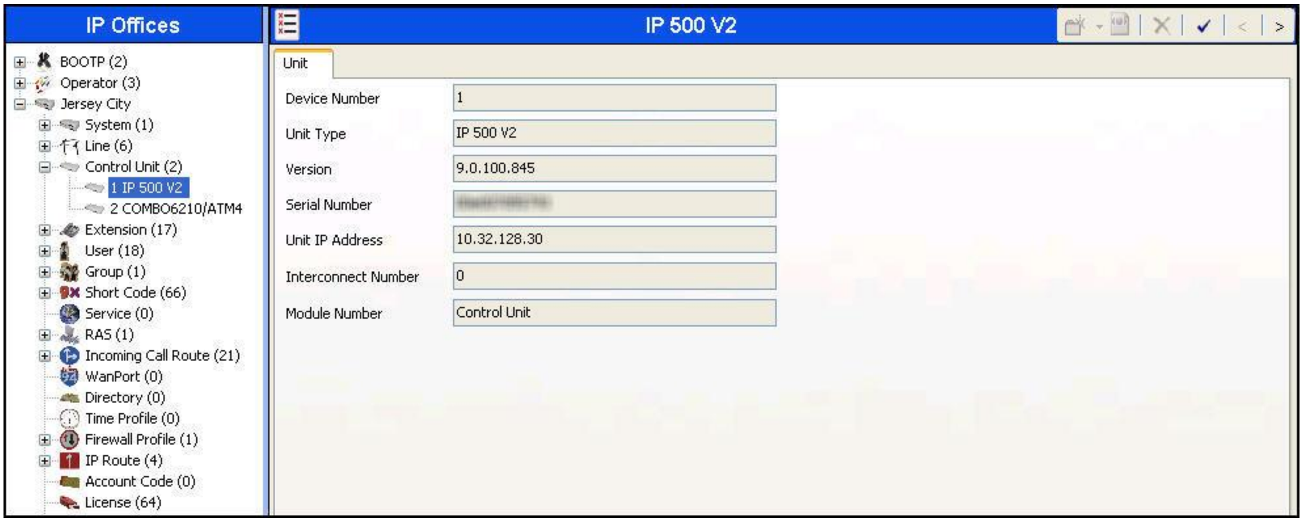
To verify that there is a **SIP Trunk Channels** License with sufficient capacity; click **License** in the Navigation pane. Confirm a valid license with sufficient **Instances** (trunk channels) in the Details pane. The screen below also shows the valid license for **Avaya IP endpoints**.



To view the physical hardware comprising the Avaya IP Office system, expand the components under the **Control Unit** in the Navigation pane. In the sample configuration, the second component listed is a Combination Card. This module has 6 digital station ports, two analog extension ports, 4 analog trunk ports and 10 VCM channels. The VCM is a Voice Compression Module supporting VoIP codecs. An Avaya IP Office hardware configuration with a VCM component is necessary to support SIP trunking.

To view the details of the component, select the component in the Navigation pane.

The screen below shows the details of the IP 500 V2:



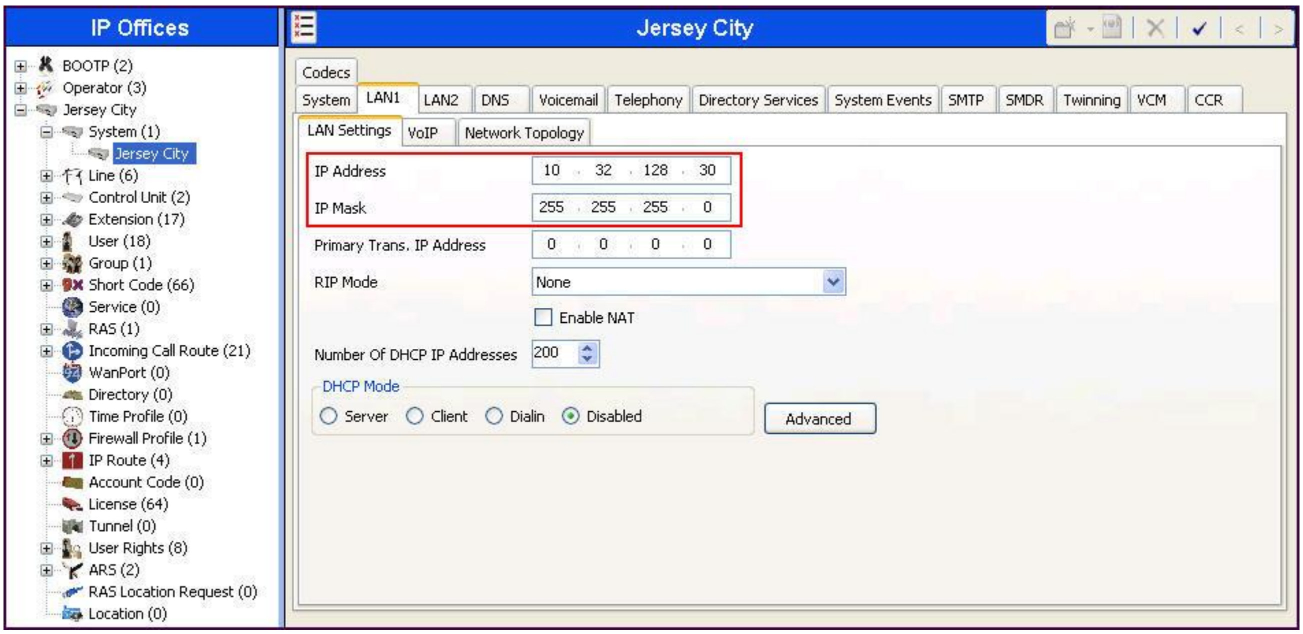
The screen below shows the details of the Combination Card:

5.2. System

This section configures the necessary system settings

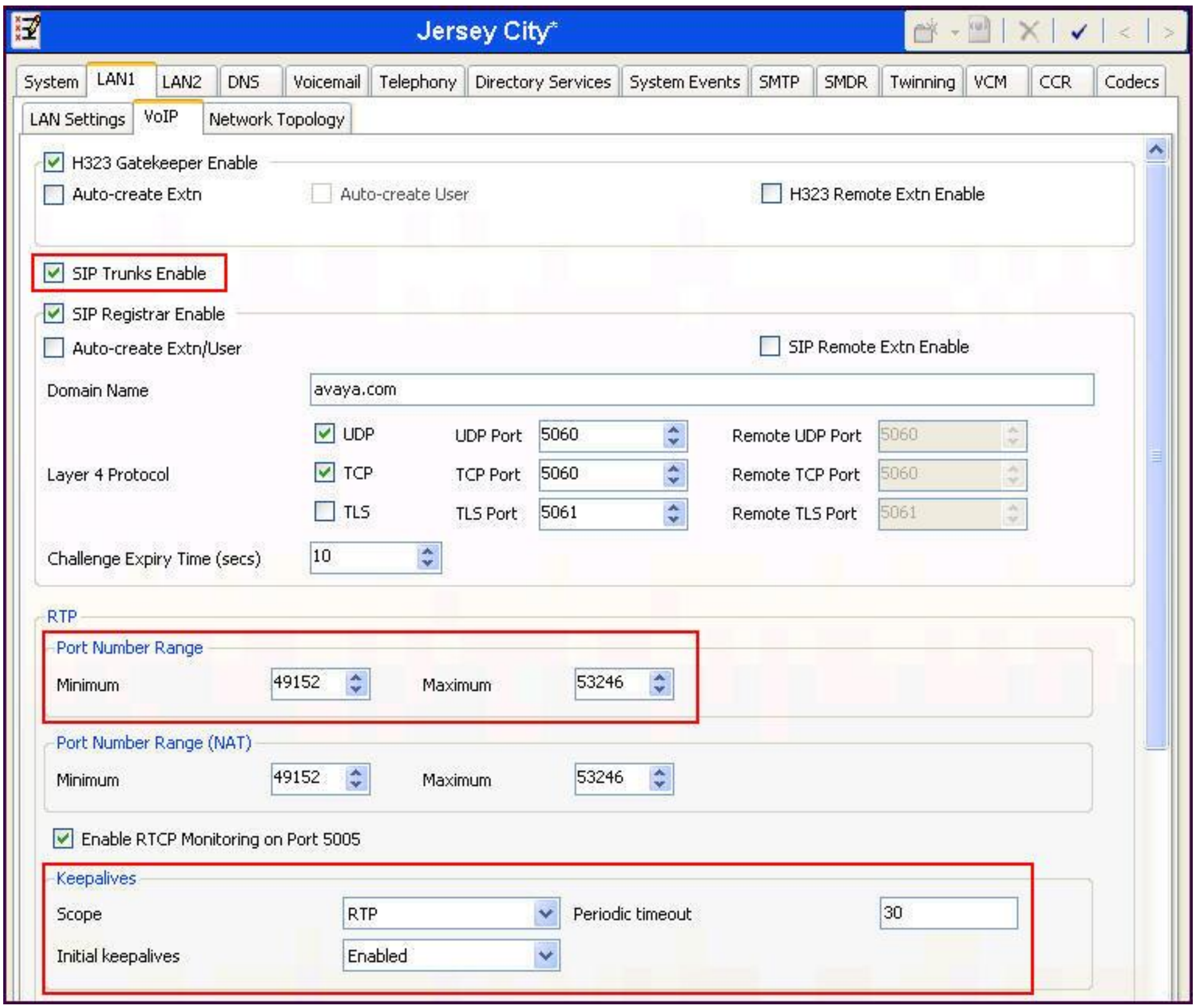
5.2.1. System - LAN1 Tab

In the sample configuration, the Avaya IP Office LAN port was used to connect to the enterprise network. The LAN1 settings correspond to the LAN port on the Avaya IP Office 500 V2. To access the LAN1 settings, first navigate to **System → <*Name*>**, where <*Name*> is the system name assigned to the IP Office. In the case of the compliance test, the system name is **Jersey City**. Next, navigate to the **LAN1 → 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 enterprise network.

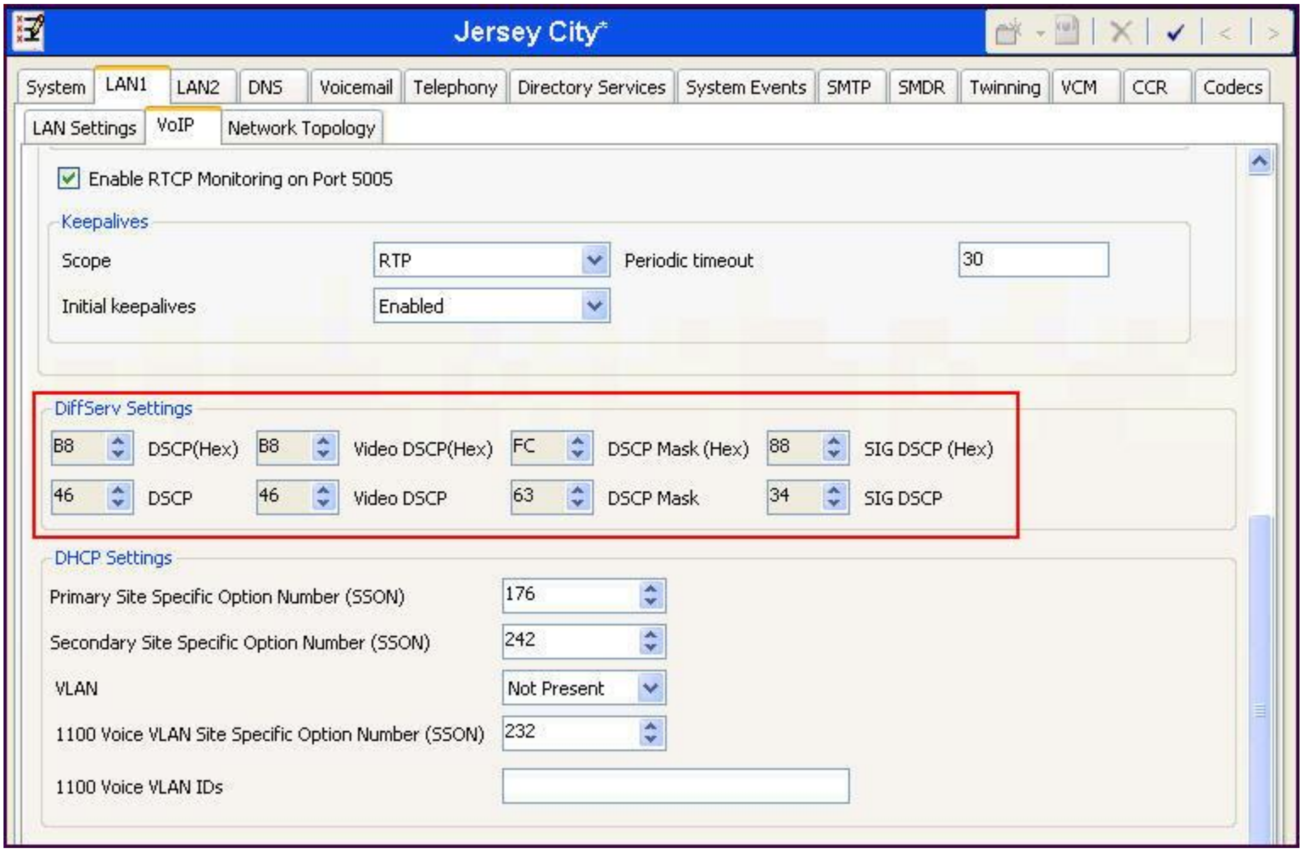


On the **VoIP** tab of LAN1 in the Details Pane, configure the following parameters:

- Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks.
- The **RTP Port Number Range** can be customized to a specific range of receiving ports for the RTP media. Based on this setting, Avaya IP Office would request RTP media be sent to a port in the configurable range for calls using LAN1.
- In the **Keepalives** section. Select ***RTP*** for **Scope**; select ***Enabled*** for **Initial keepalives**; enter ***30*** for **Periodic timeout**. These settings direct IP Office to send a RTP keepalive packet starting at the time of initial connection and every 30 seconds thereafter if no other RTP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting for media from the other, as well as helping to keep firewall ports open for the duration of the call.



Scroll down to the **DiffServ Settings** section. Avaya IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values 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. The specific values used for the compliance test are shown in the screen below and are also the default values. For a customer installation, if the default values are not sufficient, appropriate values should be provided by the customer.

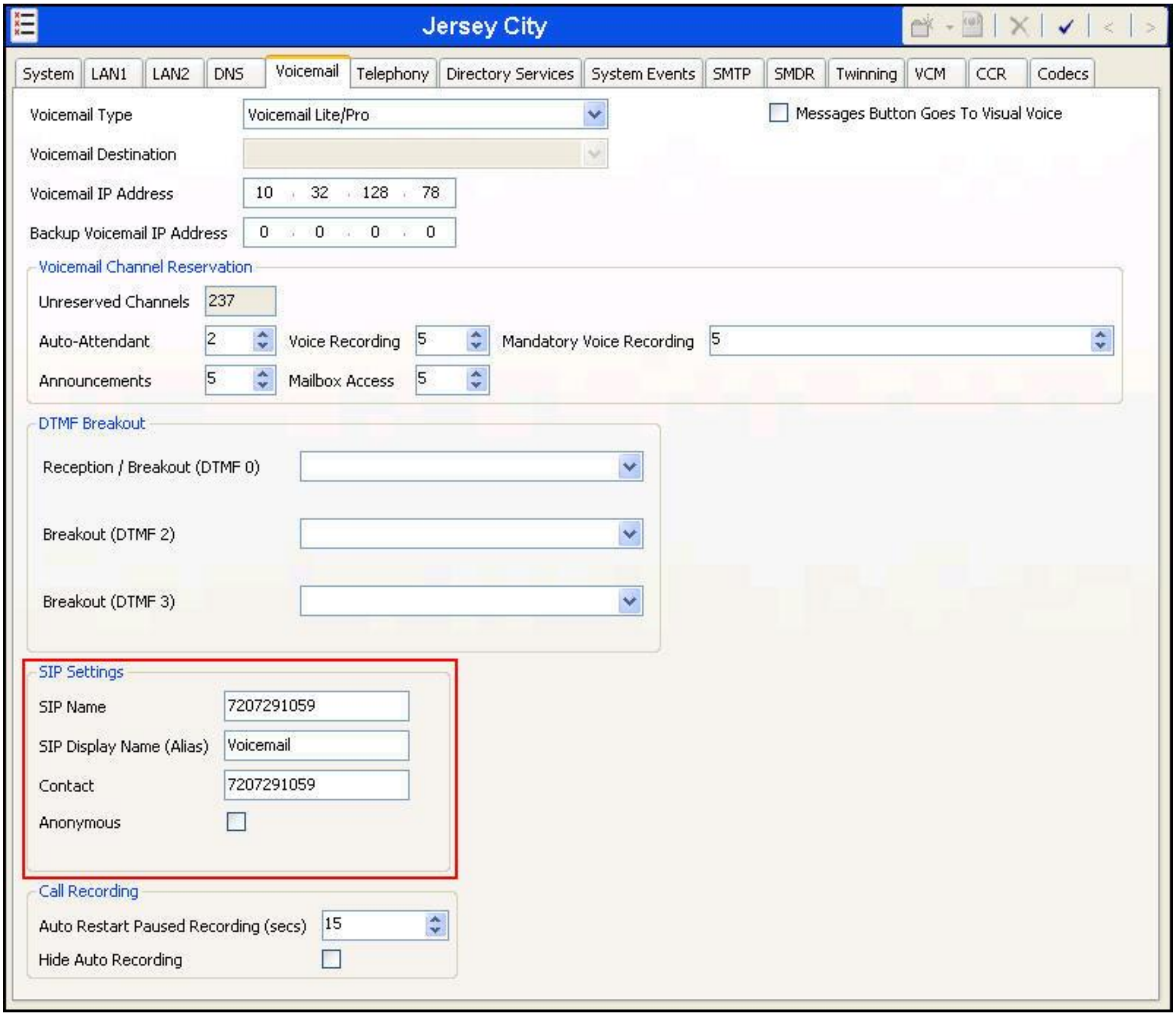


On the **Network Topology** tab of LAN1 in the Details Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. The Avaya SBCE will perform network address translation of SIP traffic but it is not necessary for IP Office to have any knowledge of this translation. Thus, the parameter was set to ***Open Internet***.
- Set **Binding Refresh Time (seconds)** to a desired value. 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. See **Section 5.9** for complete details.
- Set **Public Port** to ***5060*** for **UDP**.

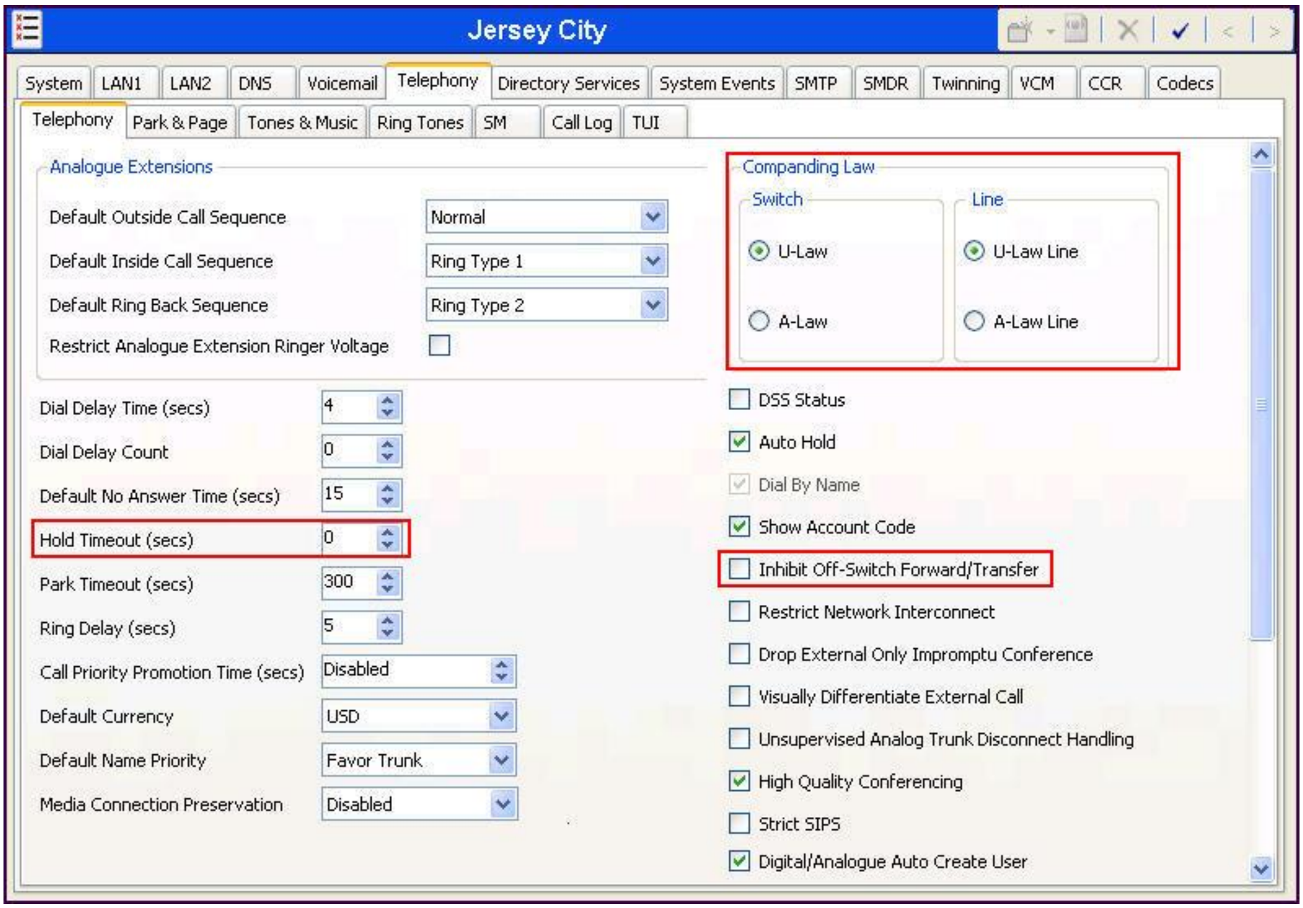
5.2.2. System - Voicemail Tab

In the **Voicemail** tab of the Details Pane, configure the **SIP Settings** section. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from IntelePeer. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. Uncheck the **Anonymous** box to allow the Voicemail Caller ID information to be sent to the network.



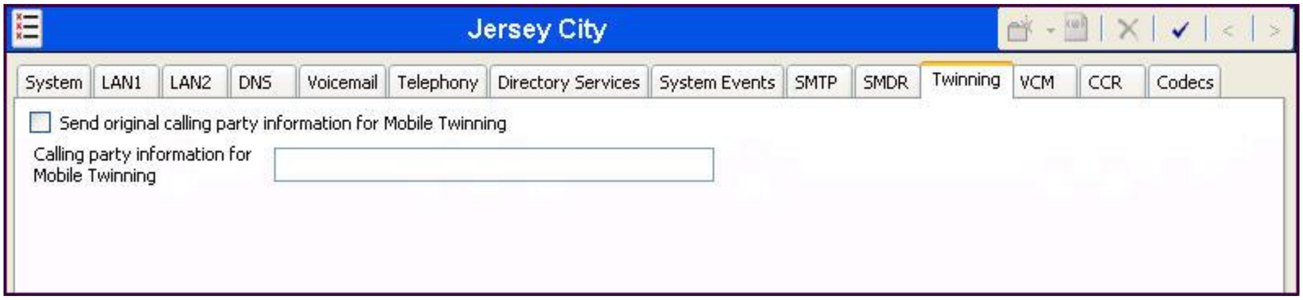
5.2.3. System - Telephony Tab

Navigate to the **Telephony → Telephony** tab in the Details Pane. Enter or select ***0*** for **Hold Timeout (secs)** so that calls on hold will not time out. Choose the **Companding Law** typical for the enterprise site. For the compliance test, ***U-LAW*** was 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 per customer business policies. Note that this configuration might pose a security issue (Toll Fraud). Customers should exercise caution with this configuration.



5.2.4. System - Twinning Tab

To view or change the System Twinning settings, navigate to the **Twinning** tab in the Details Pane as shown in the following screen. The **Send original calling party information for Mobile Twinning** box is not checked in the sample configuration, and the **Calling party information for Mobile Twinning** is left blank.



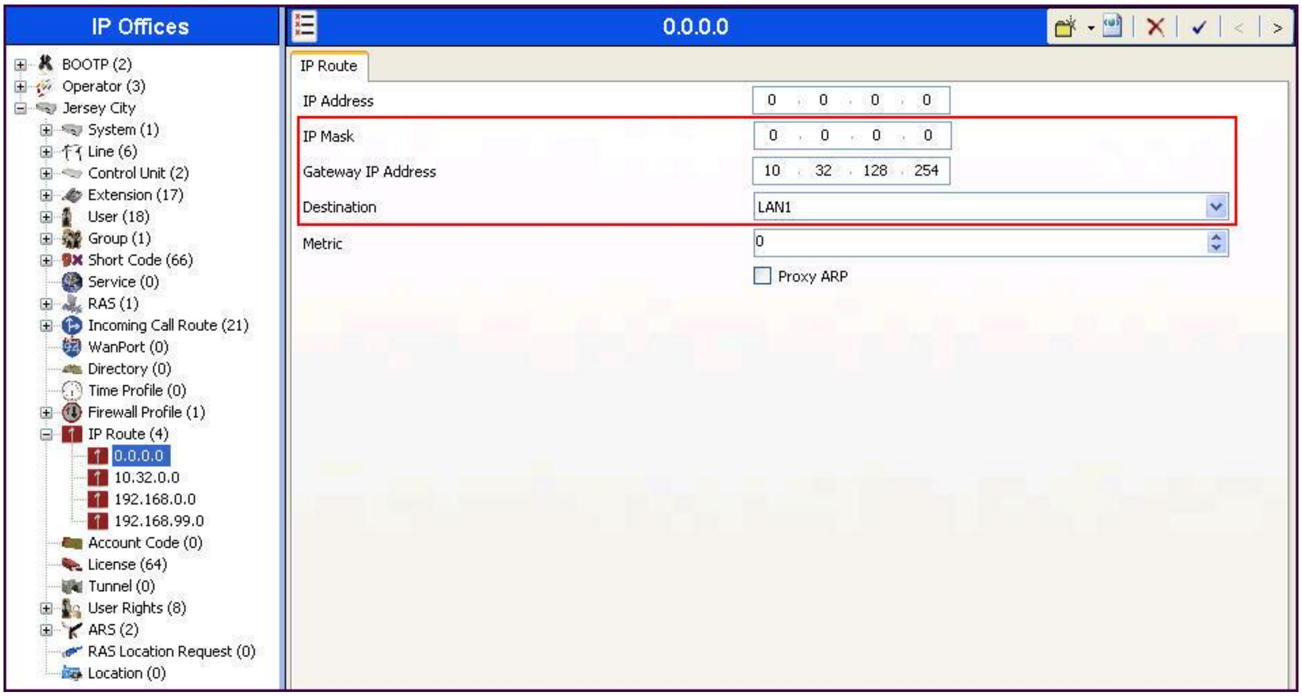
5.2.5. System – Codecs Tab

In the **Codecs** tab of the Details Pane, select or enter ***101*** for **RFC2833 Default Payload**. This setting matched the configuration by IntelePeer for use with out-band DTMF tone transmissions.

5.3. IP Route

Navigate to **IP Route → 0.0.0.0** in the left Navigation Pane if a default route already exists. Otherwise, to create the default route, right-click on **IP Route** and select **New.** Create/verify a default route with the following parameters:

- Set **IP Mask** to ***0.0.0.0***.
- Set **Gateway IP Address** to the IP address of the enterprise LAN gateway for the subnet where the Avaya IP Office is connected.
- Set **Destination** to ***LAN1*** from the drop-down list.



5.4. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the IntelePeer 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 **Sections 5.4.2 – 5.4.7**.

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

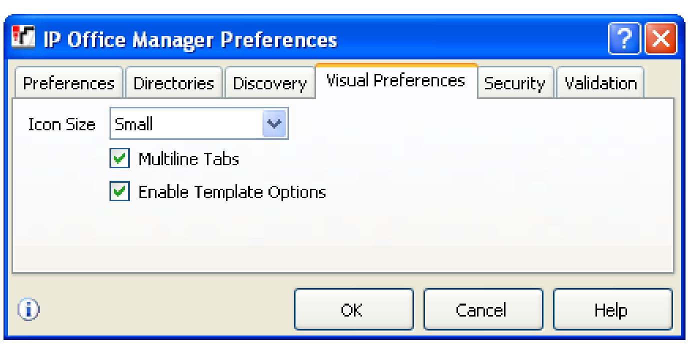
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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 **Sections 5.4.2 – 5.4.7**.

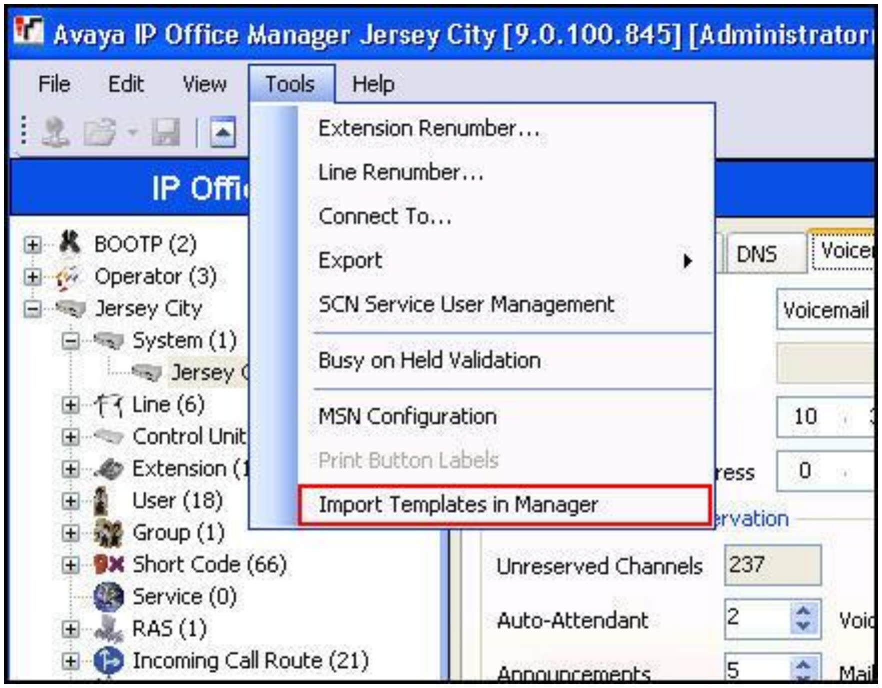
5.4.1. Create SIP Line from Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **US_IntelePeer_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 option box is checked next to **Enable Template Options**. Click **OK**.

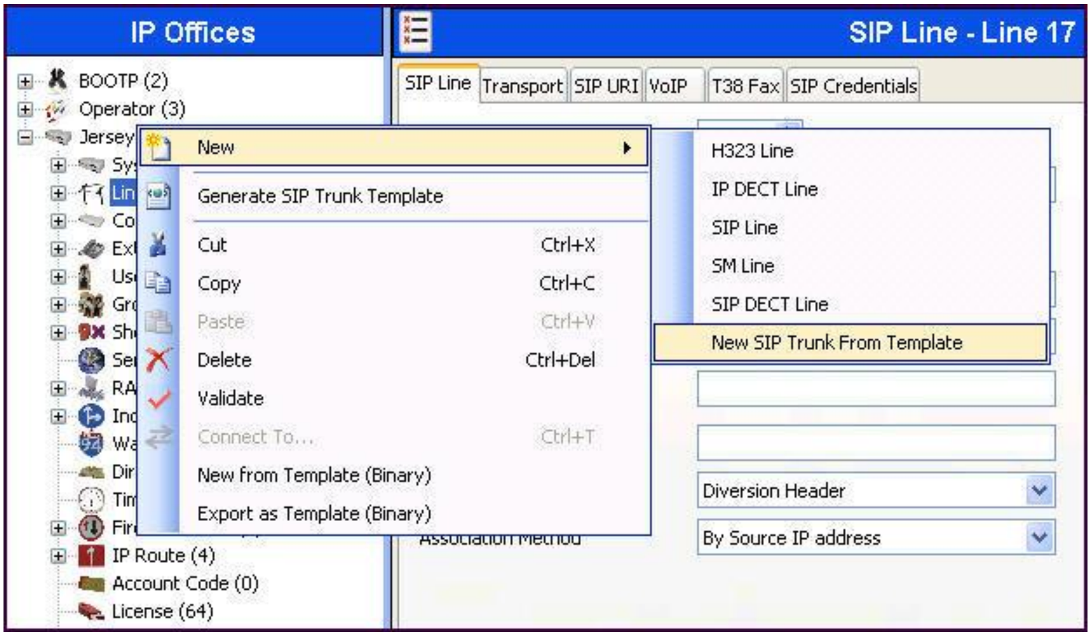


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template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



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

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**.



5. In the subsequent **Template Type Selection** pop-up window, select ***United States*** from the **Country** drop-down list and select ***IntelePeer*** from the **Service Provider** drop-down list as shown below. These values correspond to parts of the file name (**US_IntelePeer_SIPTrunk.xml)** created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.

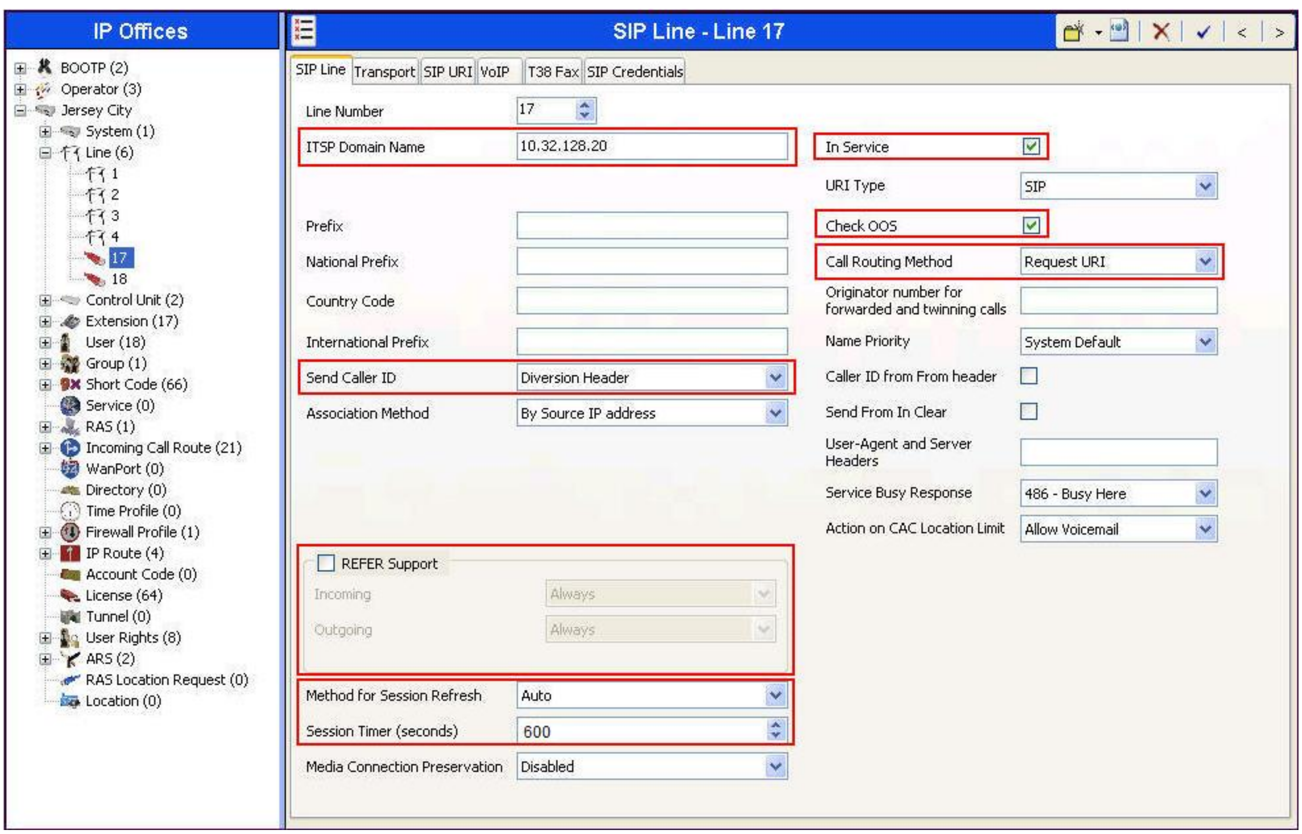
Note that the newly created SIP Line may not immediately appear in the Navigation pane until the configuration was saved, closed and reopened in IP Office Manager.

6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2 – 5.4.7.**

5.4.2. SIP Line – SIP Line Tab

In the **SIP Line** tab of the Details Pane, configure the parameters as shown below...

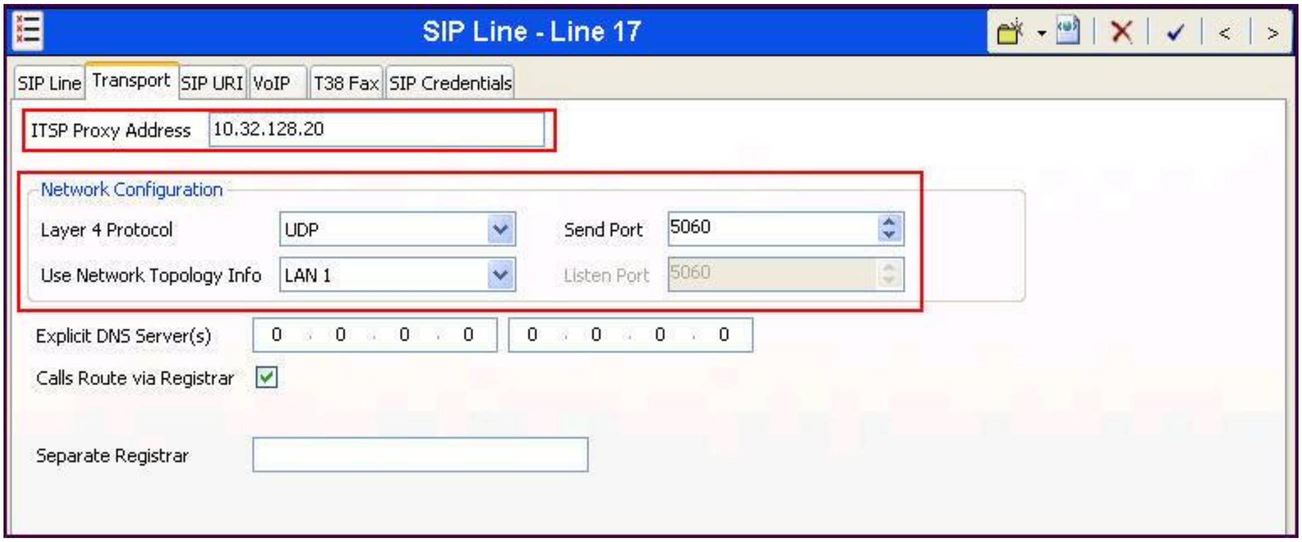
- Set **ITSP Domain Name** to the IP address of the internal signaling interface of the Avaya SBCE.
- Check the **In Service** box. This makes the trunk available to incoming and outgoing calls.
- Check **OOS** box. Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line. See **Section 5.9** for details on time between SIP OPTIONS sent by IP Office.
- Set **Call Routing Method** to ***Request URI***. Avaya IP Office will route inbound calls based on the number in the Request URI.
- Set **Send Caller ID** to ***Diversion Header***. With this setting and the related configuration in **Section 5.2.4**, Avaya IP Office will include the Diversion Header for calls that are forwarded or redirected via Mobile Twinning out the SIP Line to the service provider.
- Uncheck **REFER Support**. IntelePeer SIP Trunking does not support use of REFER for off-net call re-direction as in call transfers.
- Set **Method for Session Refresh** to ***Auto***. With this setting Avaya IP Office will send UPDATE messages for session refresh if the other party supports UPDATE. If UPDATE is not supported, re-INVITE messages are sent.
- Set **Session Timer (seconds)** to a desired value. With the value as shown below, Avaya IP Office will send session refresh UPDATE or re-INVITE to the service provider every 5 minutes (half of the specified value).



5.4.3. SIP Line – Transport Tab

Navigate to the **Transport** tab and set the following:

- Set the **ITSP Proxy Address** to the IP address of the internal signaling interface of the Avaya SBCE.
- Set the **Layer 4 Protocol** to ***UDP***.
- Set **Use Network Topology Info** to the network port used by the SIP line to access the far-end as configured in **Section 5.2.1**.
- Set the **Send Port** to ***5060***.

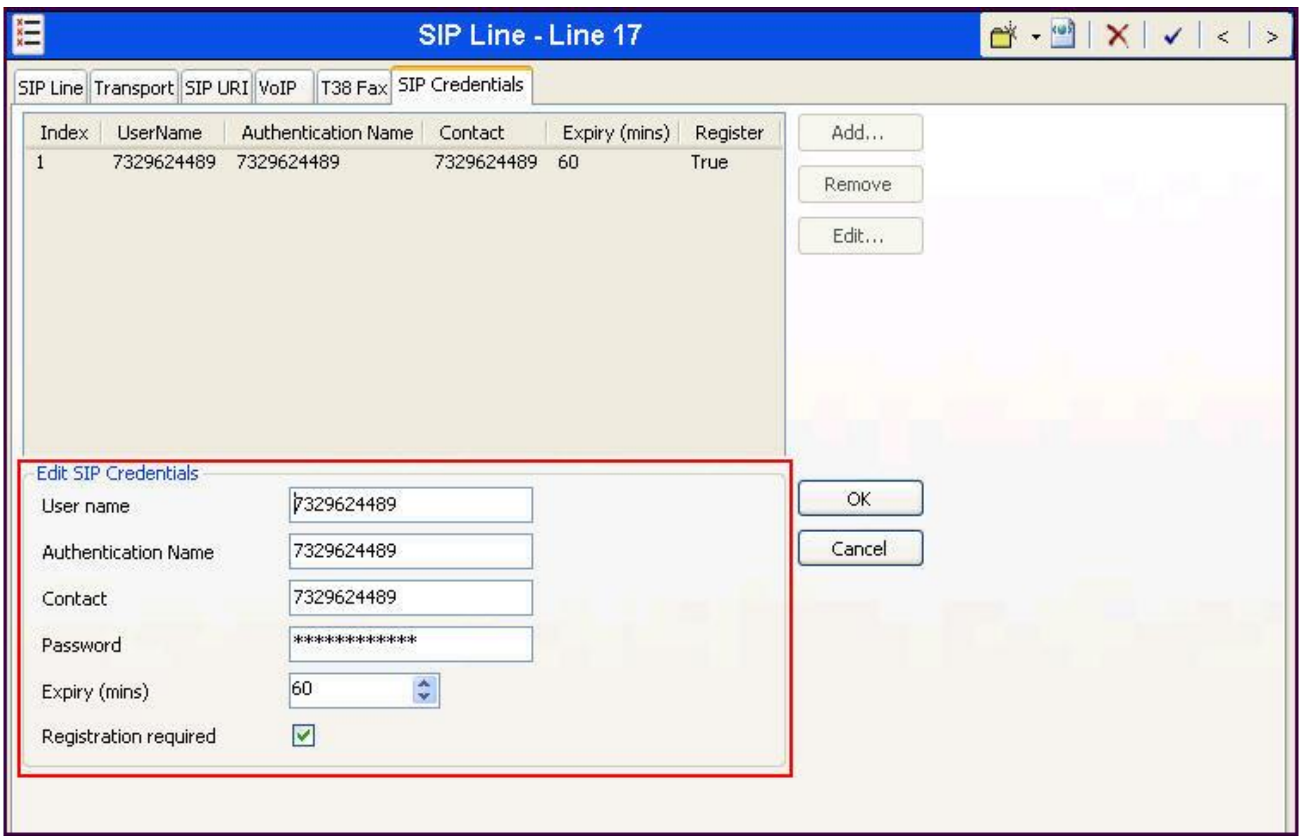


5.4.4. SIP Line – SIP Credentials Tab

SIP Credentials are used to register the SIP Trunk with a service provider that requires SIP Registration. SIP Credentials are unique per customer and therefore customers must contact the service provider to obtain the proper registration credentials for their deployment. IntelePeer uses static IP authentication for the customer account, therefore the SIP Credentials configuration is not needed. This section is included in these application notes for reference and completeness.

Select the **SIP Credentials** tab, and then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button. The screen below shows a previously configured entry being edited. The entry was created with sample settings as shown below:

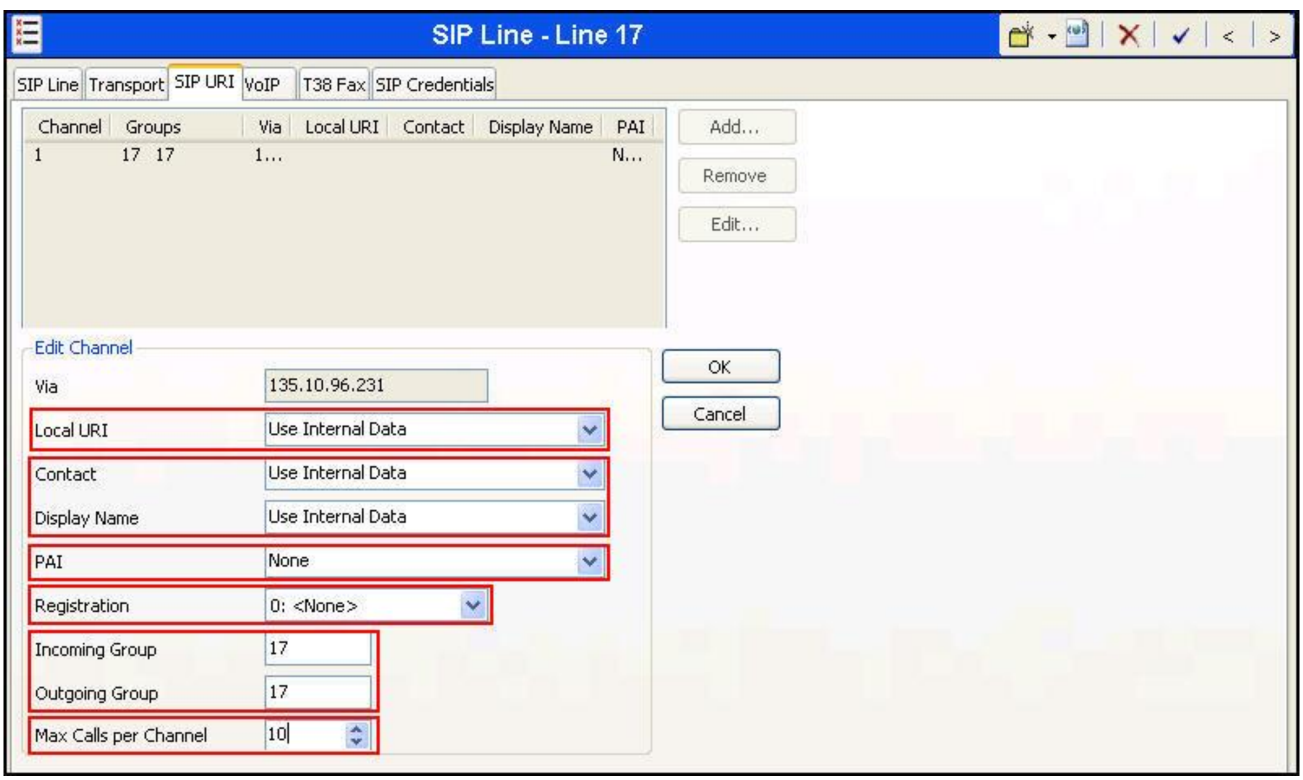
- Set the **User name**, **Authentication Name**, and **Contact** fields to the registration string provided by the service provider. This is generally a 10-digit telephone number like ***7329624489*** as shown below.
- In the **Password** field, enter the registration password provided by the service provider.
- In the **Expiry (mins)** field, enter the time in minutes until the registration expires.
- Check the **Registration required** field if Registration is required for the SIP Trunking customer account.



5.4.5. SIP Line – SIP URI Tab

Select the **SIP URI** tab to create a SIP URI entry or edit an existing entry. A SIP URI entry matches each incoming number that Avaya IP Office will accept on this line. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane. For the compliance test, a single SIP URI entry was created to match any DID number assigned to Avaya IP Office users. The following screen shows the edit window on a previously configured entry for the compliance test.

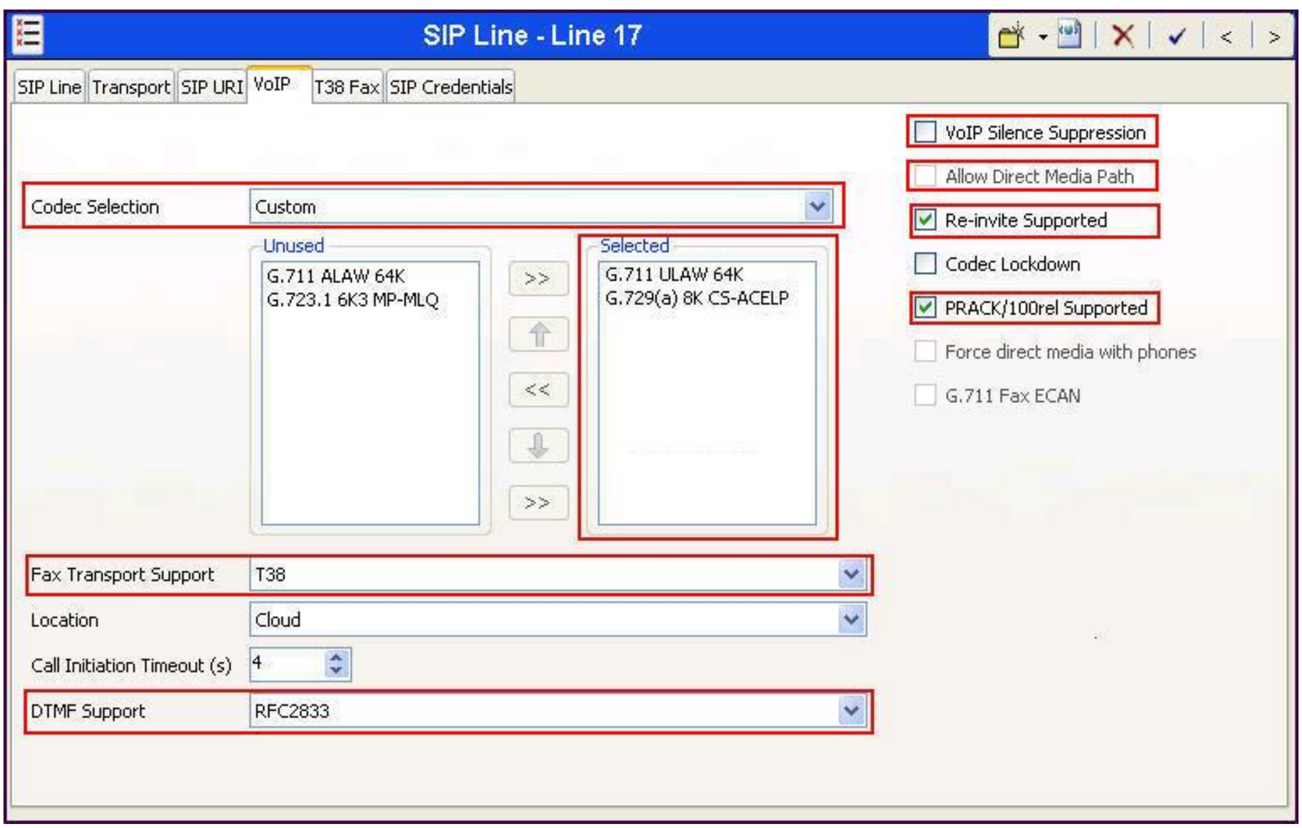
- Set **Local URI**, **Contact**, and **Display Name** to ***Use Internal Data***. This setting allows calls on this line who's SIP URI matches the number set in the **SIP** tab of any User as shown in **Section 5.6**.
- Set **PAI** to ***None***. This setting directs Avaya IP Office to send the PPI (P-Preferred-Identity) header when appropriate instead of the PAI header (P-Asserted-Identity). The PPI header will be populated from the data set in the **SIP** tab of the call initiating **User** as shown in **Section 5.66**.
- Select the **Registration** value that was configured in **Section 5.4.4**, or ***0: <None>*** if the service provider uses static IP authentication (as was the case with the compliance test and shown below).
- Associate this line with an incoming line group by entering line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. For the compliance test, the incoming and outgoing group ***17*** was specified.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls allowed using this SIP URI pattern.



5.4.6. SIP Line – VoIP Tab

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

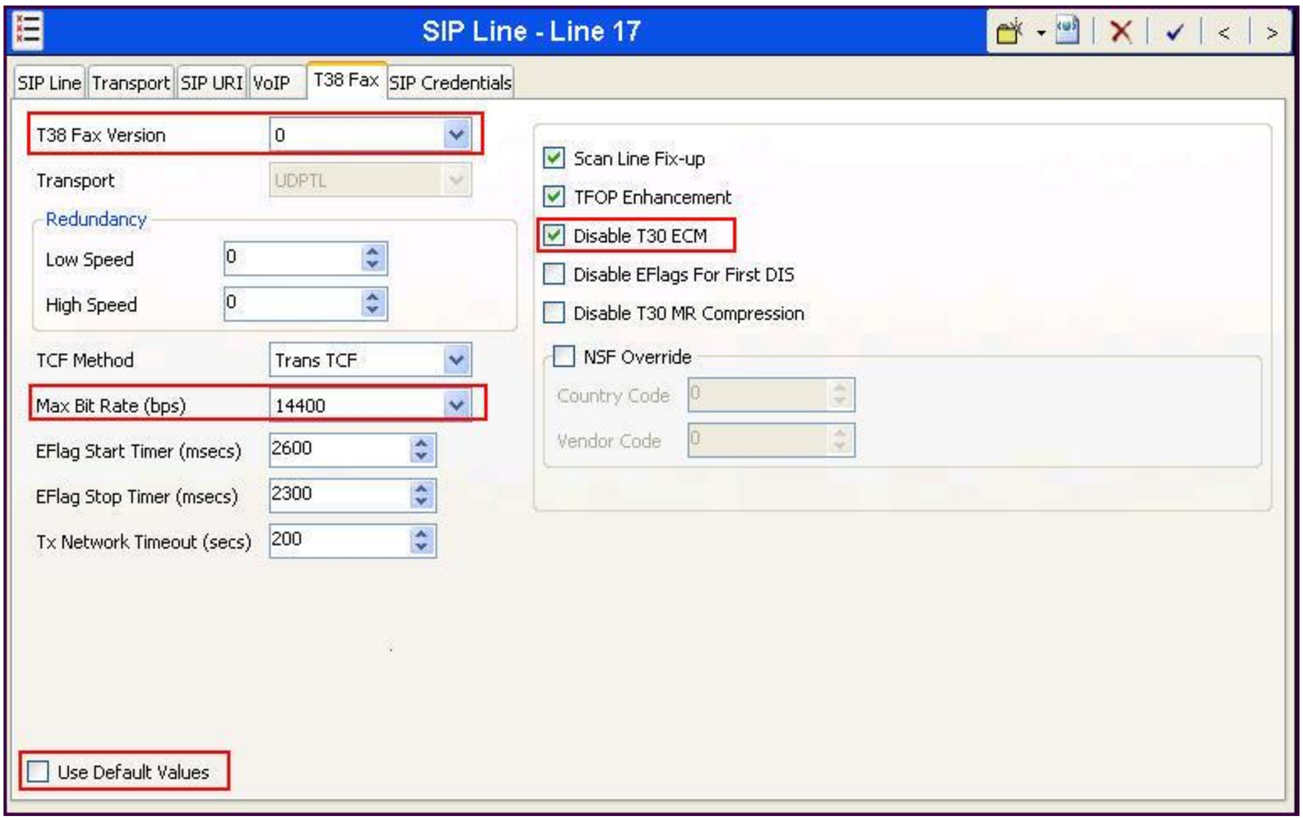
- Set the **Codec Selection** to ***Custom***.
- Choose ***G.711 ULAW 64K*** and ***G.729(a) 8K CS-ACELP*** from the **Unused** box and move these 2 selections to the **Selected** box. These 2 codecs are supported by the IntelePeer SIP Trunking Service. Use the down/up arrows to order the 2 selected codecs as shown. IntelePeer recommends G.711MU as the preferred codec.
- Select ***T38*** for **Fax Transport Support**.
- Set the **DTMF Support** field to ***RFC2833***. This directs Avaya IP Office to send DTMF tones as out-band RTP events as per RFC2833.
- Uncheck the **VoIP Silence Suppression** option box.
- Verify that **Allow Direct Media Path** is disabled (see observation/limitation list in **Section 2.2**).
- Check the **Re-invite Supported** option box.
- Check the **PRACK/100rel Supported** option box. This setting enables support by Avaya IP Office for the PRACK (Provisional Reliable Acknowledgement) message on SIP trunks.



5.4.7. SIP Line – T.38 Fax Tab

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

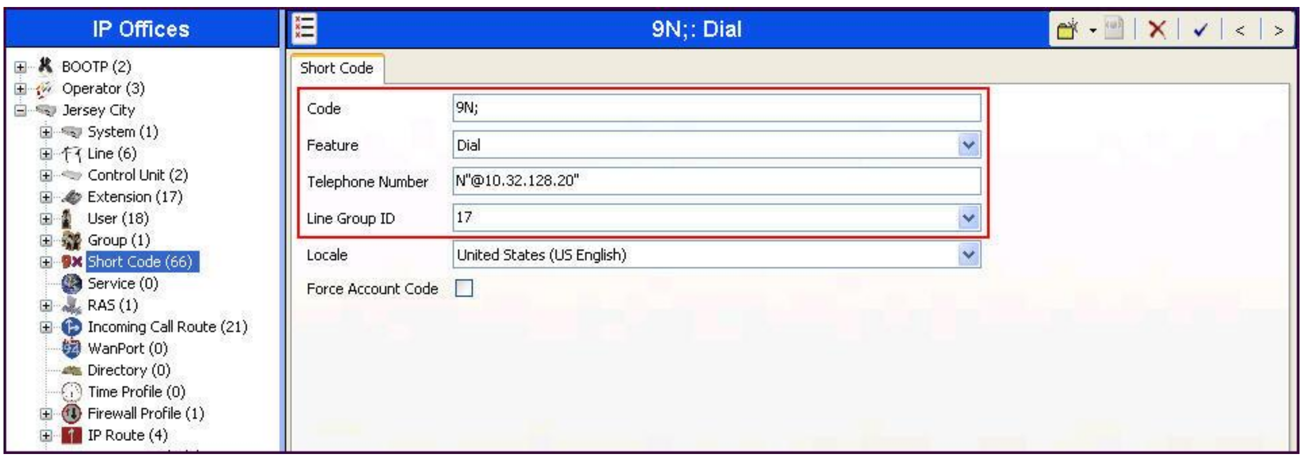
- Uncheck **Use Default Values** at the bottom of the screen.
- Set **T38 Fax Version** to ***0***. IntelePeer SIP Trunking supports T.38 fax version 0.
- Set **Max Bit Rate (bps)** to 14400, the highest fax bit rate that Avaya IP Office supports for T.38 faxing.
- Check the **Disable T30 ECM** option.



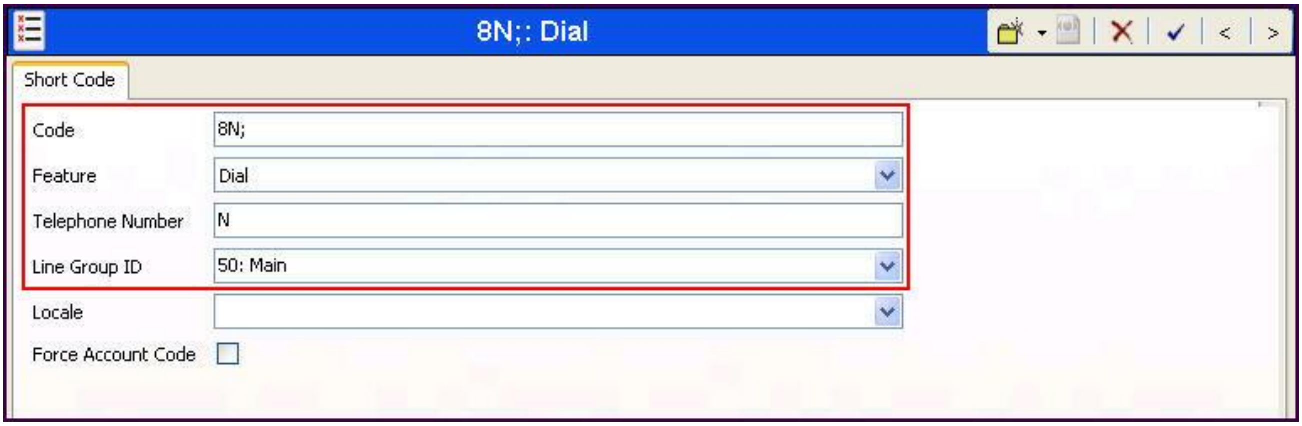
5.5. Short Code

Define a short code to route outbound calls to the SIP line. To create a short code, right-click on **Short Code** in the Navigation Pane and select **New** (not shown). In the Details Pane, configure the parameters as shown below:

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The ***9N;*** short code, used for the compliance test, 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"@10.32.128.20"***. 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 IP address following the **@** sign is the IP address of the private interface of the Avaya SBCE.
- Set the **Line Group Id** to the **Outgoing Group** number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4.5**. This short code will use this line group when placing the outbound calls.



The simple **9N;** short code illustrated above does not provide a means of alternate routing if the configured SIP Line is out of service or temporarily not responding. When alternate routing options and/or more customized analysis of the dialed digits following the short code are desired, the Automatic Route Selection (ARS) feature may be used. In the screen below, the short code ***8N;*** is illustrated for access to ARS. When the Avaya IP Office user dials 8 plus any number ***N***, rather than being directed to a specific **Line Group Id**, the call is directed to ***50: Main***, configurable via ARS. See **Section 5.8** for example ARS route configuration.

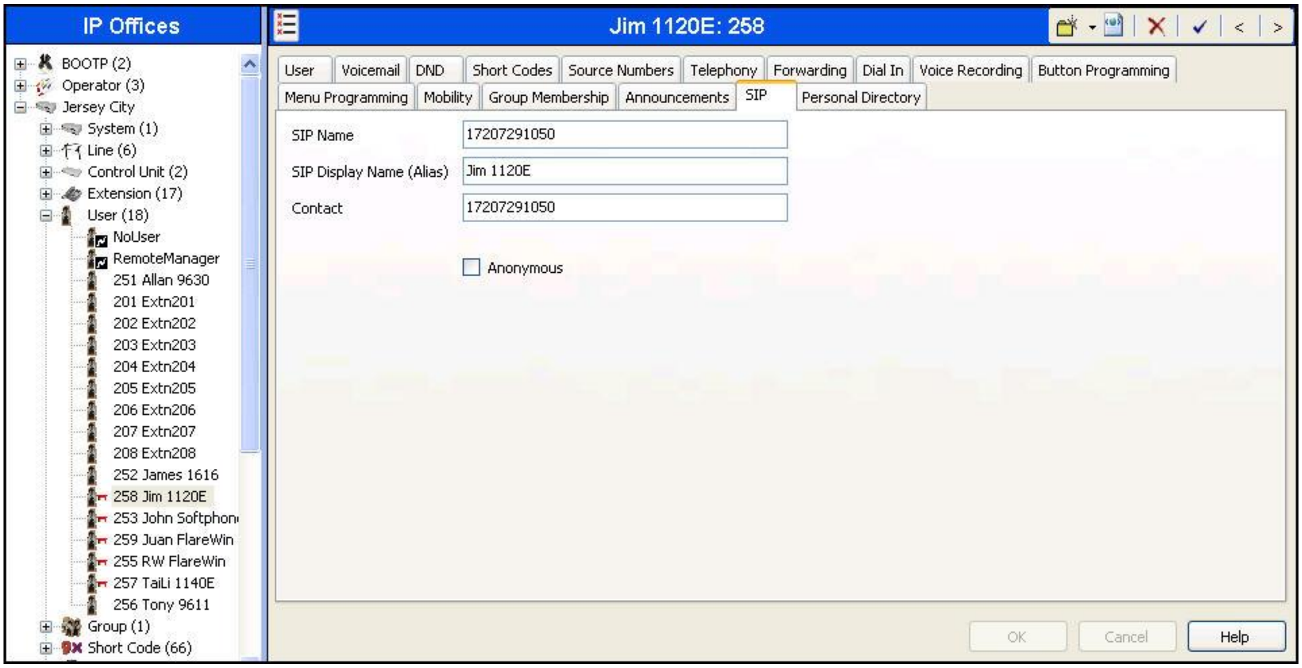


Optionally, add or edit a short code that can be used to access the SIP Line anonymously. In the screen shown below, the short code ***67N;*** is illustrated. This short code is similar to the **9N;** short code except that the **Telephone Number** field begins with the letter ***W***, which means "withhold the outgoing calling line identification". In the case of the compliance test, when a user dialed *67 plus the number, Avaya IP Office would include the user's telephone number (DID number assigned to the user) in the **PPI** (P-Preferred-Identity) or the **PAI** (P-Asserted-Identity) header and would include the **Privacy: id** header in the outbound INVITE message. Consequently IntelePeer would prevent presentation of the caller id to the called PSTN destination.

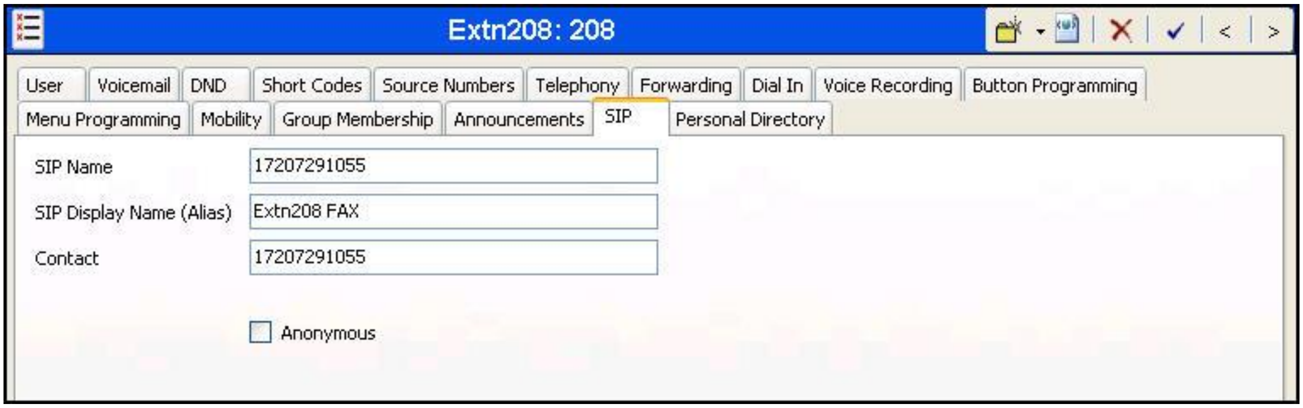
5.6. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line. To configure these settings, first navigate to **User→Name** in the Navigation Pane, where **Name** is the name of the user to be modified. In the example below, the name of the user is ***Jim 1120E***. Select the **SIP** tab in the Details Pane. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by IntelePeer. The **SIP Display Name (Alias)** can optionally be configured with a descriptive text string. The value entered for the **Contact** field will be used in the Contact header for outgoing SIP INVITE to the service provider. The value entered for the **SIP Name** is used as the user part of the SIP URI in the From header for outgoing SIP trunk calls.

If outbound 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 (or alternatively use the *67 short code as defined in **Section 5.5**).



The following screen shows the similar SIP settings for an analog extension user for fax:



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, right-click **Incoming Call Route** in the Navigation Pane and select **New** (not shown). On the **Standard** tab in the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capacity** to ***Any Voice***.
- Set the **Line Group Id** to the **Incoming Group** of the SIP Line defined in **Section 5.4.5**.
- Set the **Incoming Number** to the incoming DID number on which this route should match. Matching is right to left.

On the **Destinations** tab, select the destination from the pull-down list of the **Destination** field. In this example, incoming calls to the DID number 17207291050 on Incoming Group 17 are to be routed to the user “Jim 1120E” at extension 258.

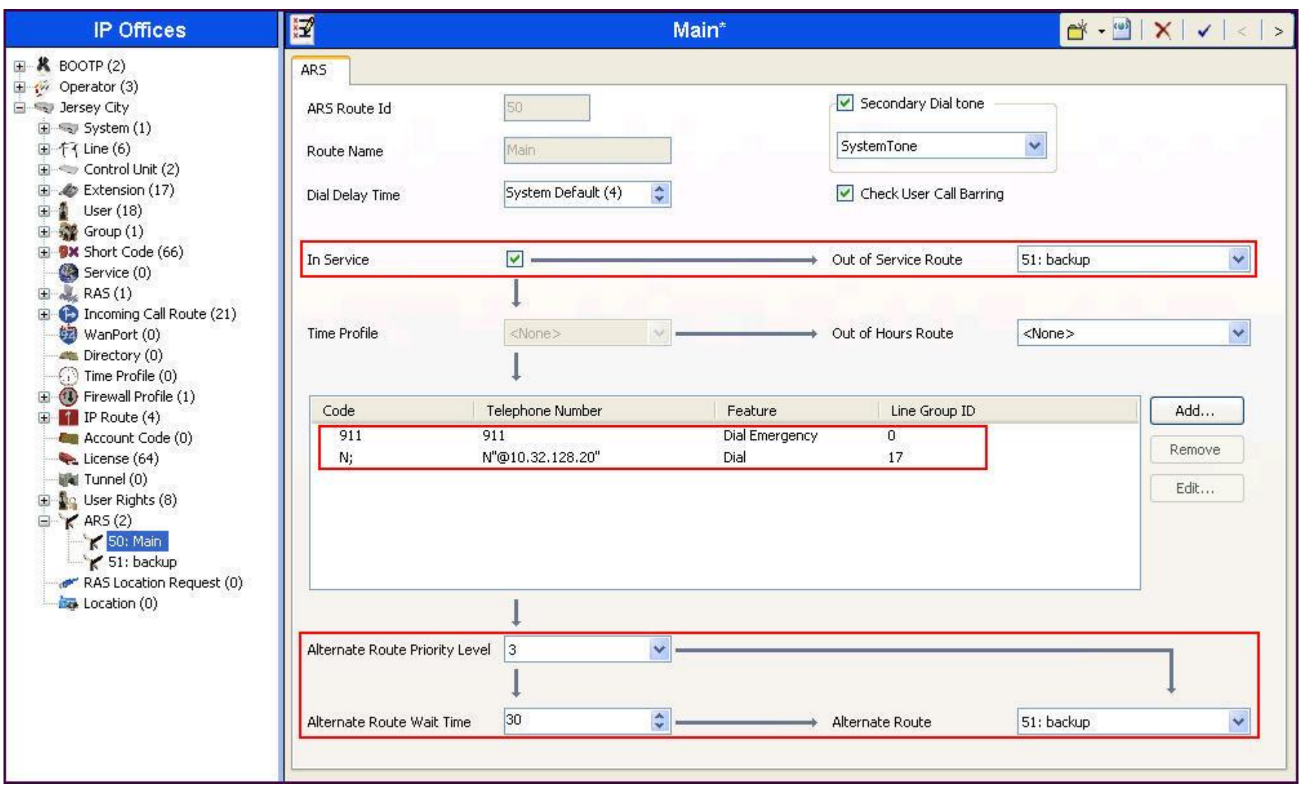
5.8. ARS and Alternate Routing

While detailed coverage of Automatic Route Selection (ARS) is beyond the scope of these Application Notes, this section includes basic ARS screen illustration and considerations. ARS is shown here mainly to illustrate alternate routing should the SIP Line be out of service or temporarily not responding.

Optionally, ARS can be used to supplement or replace the simple **9N;** short code approach documented in **Section 5.5**. With ARS, secondary dial tone can be provided after the access code, time-based routing criteria can be introduced, and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. ARS also facilitates more specific dialed telephone number matching, enabling immediate routing and alternate treatment for different types of numbers following the access code. For example, if all local and long distance calls should use the SIP Line, but service numbers should prefer a different outgoing line group, ARS can be used to distinguish between the two call patterns.

To add a new ARS route, right-click **ARS** in the Navigation pane and select **New** (not shown). To view or edit an existing ARS route, expand ARS in the Navigation pane and select a route name.

The following screen shows an example ARS configuration for the route named ***50: Main***. The **In Service** parameter refers to the ARS form itself, not the Line Groups that may be referenced in the form. If the **In Service** box is un-checked, calls are routed to the ARS route name specified in the **Out of Service Route** parameter. IP Office short codes may also be defined to allow an ARS route to be disabled or enabled from a telephone. The configurable provisioning of an Out of Service Route and the means to manually activate the Out of Service Route can be helpful for scheduled maintenance or other known service-affecting events for the primary route.



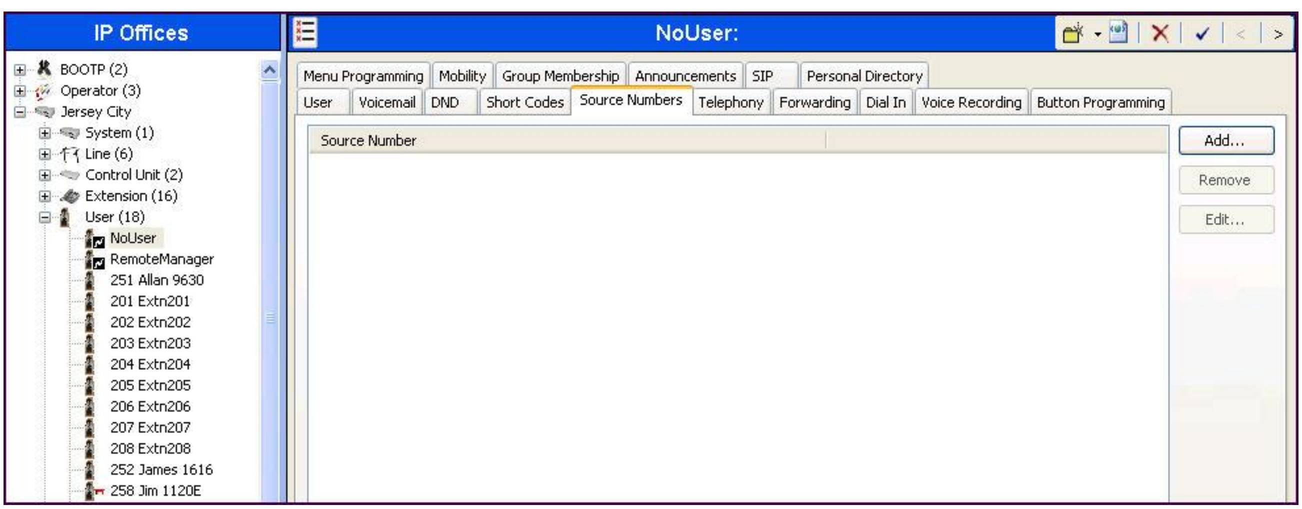
Assuming the primary route is in-service, the number passed from the short code used to access ARS (e.g., **8N;** in **Section 5.5**) can be further analyzed to direct the call to a specific Line Group ID. Per the example screen above, if the user dialed 8-911, the call would be directed to Line Group 0 to be sent out to the local area emergency response center (note that a short code 911 can also be configured to send the emergency call out when the user simply dials 911); if the user dialed 8 + any other number, the call would be directed to Line Group 17 as configured in **Section 5.4.5**. If the primary route cannot be used, the call can automatically route to the route name specified in the **Alternate Route** field in the lower right of the screen (***51: Backup***). Since alternate routing is considered a privilege not available to all callers, IP Office can control access to the alternate route by comparing the calling user's priority, configured in the **User** tab of individual users, to the value in the **Alternate Route Priority Level** field.

5.9. SIP Options

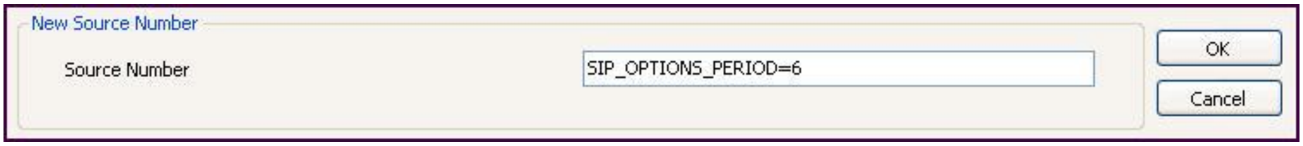
Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. By default, Avaya IP Office Release 9.0 sends out OPTIONS every 300 seconds. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set on the **Network Topology** tab in **Section 5.2.1** and the **SIP_OPTIONS_PERIOD** parameter (in minutes) that can be set on the **Source Number** tab of the **noUser** user. The OPTIONS period is determined in the following manner:

- To use the default value, set **Binding Refresh Time** to 0 or 300. OPTIONS will be sent at the 300 second frequency.
- To establish a period of less than 300 seconds, do not define the **SIP_OPTIONS_PERIOD** parameter and set the **Binding Refresh Time** to a value less than 300 seconds. The OPTIONS message period will be equal to the **Binding Refresh Time** setting.
- To establish a period greater than 300 seconds, a **SIP_OPTIONS_PERIOD** parameter must be defined. The **Binding Refresh Time** must be set to a value greater than 300 seconds. The OPTIONS message period will be the smaller of the **Binding Refresh Time** and the **SIP_OPTIONS_PERIOD** settings.

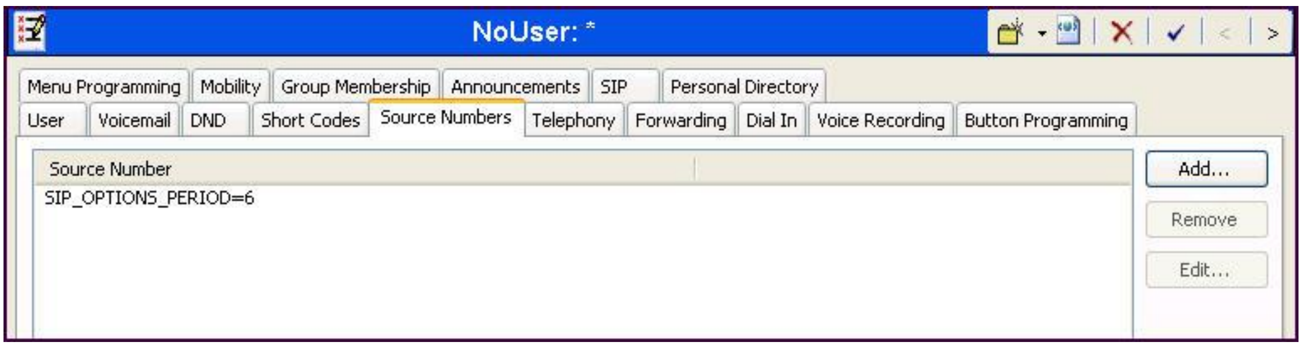
To configure the **SIP_OPTIONS_PERIOD** parameter, navigate to **User → noUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



At the bottom of the Details Pane, the **Source Number** field will appear. Enter ***SIP_OPTIONS_PERIOD=X***, where ***X*** is the desired value in minutes. Click **OK**.



The **SIP_OPTIONS_PERIOD** parameter will appear in the list of Source Numbers as shown below. For the compliance test, an OPTIONS period of 60 seconds was desired. The **Binding Refresh Time** was set to ***60*** seconds on the **Network Topology** tab in **Section 5.2.1**. There was no need to define **SIP_OPTIONS_PERIOD**.

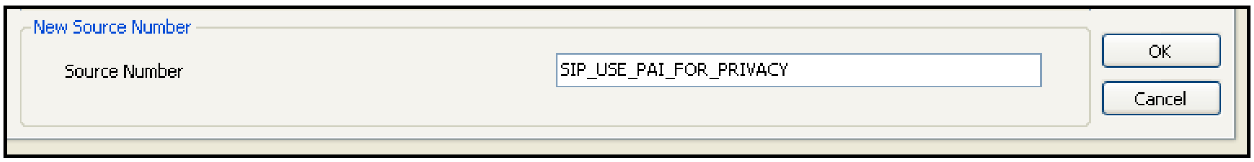


5.10. Privacy/Anonymous Calls

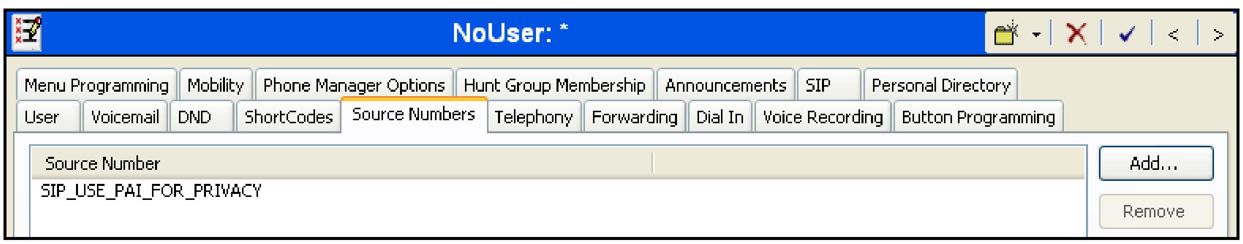
For outbound calls with privacy (anonymous) enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with “anonymous”. Avaya IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity (PAI) header to pass the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

To configure Avaya IP Office to use PAI for privacy calls, select **NoUser** under **User** in the Navigation Pane, then select the **Source Numbers** tab in the Details Pane as shown in the first screen in **Section 5.9**. Click the **Add** button.

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



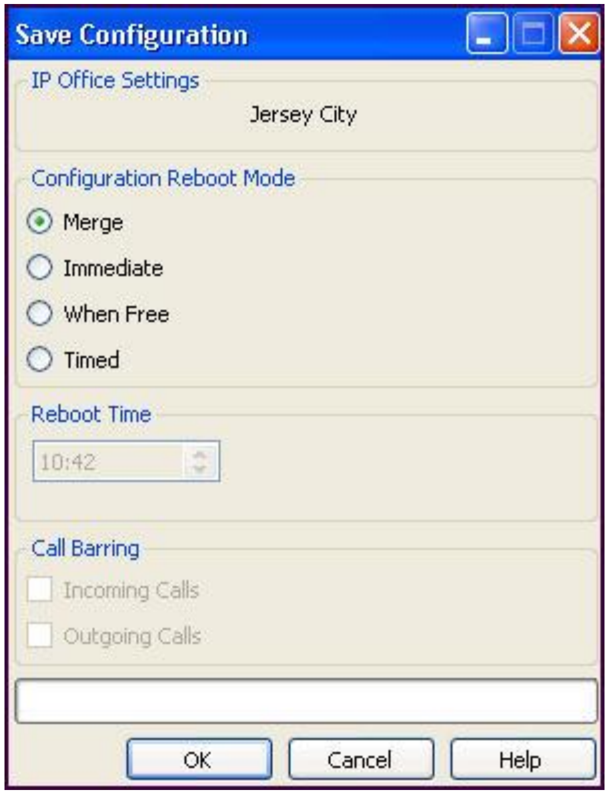
The **SIP_USE_PAI_FOR_PRIVACY** parameter will appear in the list of Source Numbers as shown below. Click **OK** at the bottom of the screen (not shown).



5.11. Save Configuration

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

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



6. Configure Avaya Session Border Controller for Enterprise

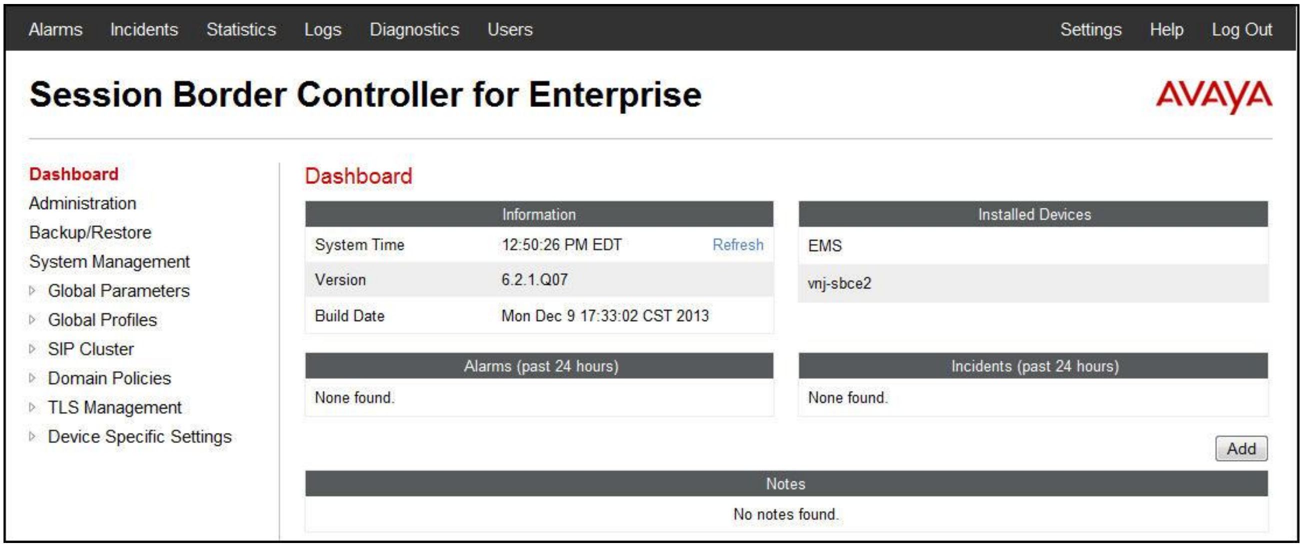
This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

6.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with appropriate credentials.

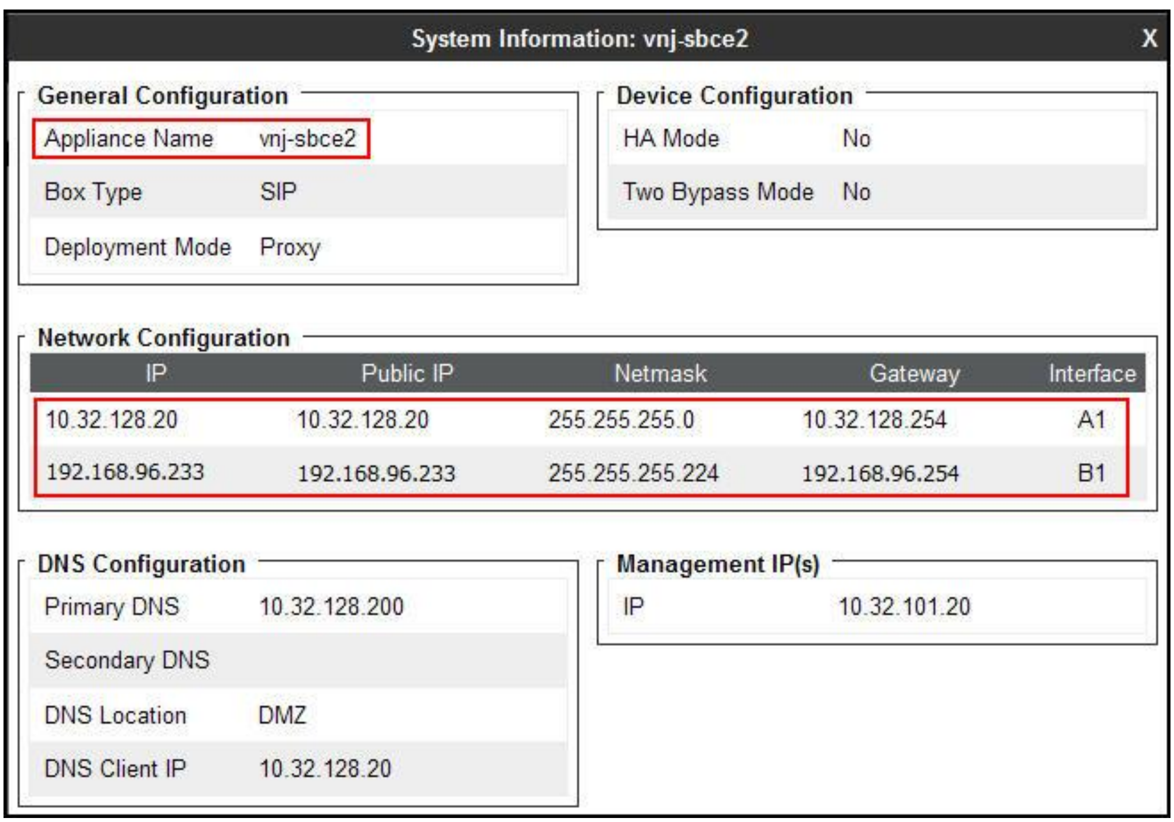
After logging in, the Dashboard screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.



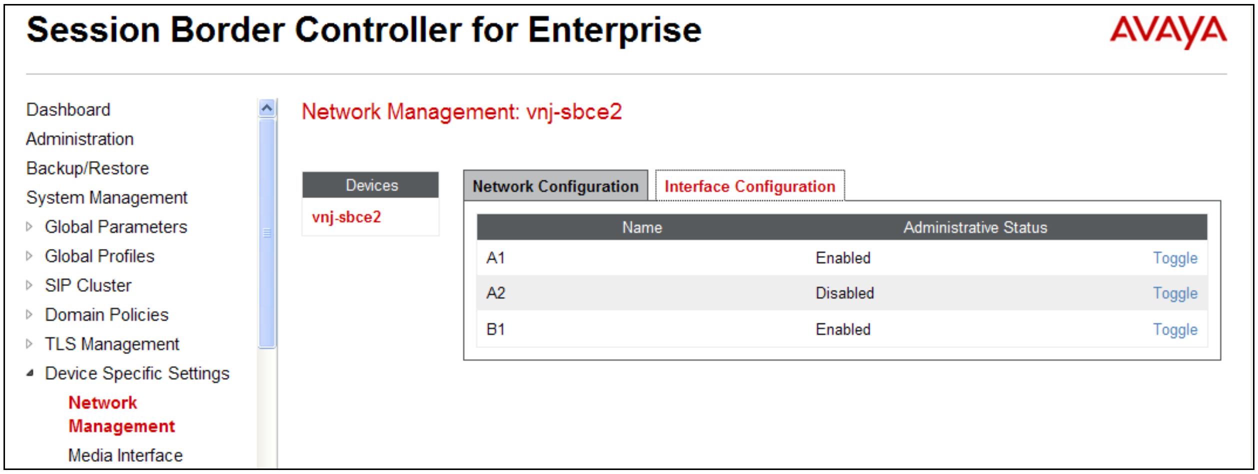
6.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.

A System Information page will appear showing the information provided during installation. The **Appliance Name** field is the name of the device (***vnj-sbce2***). This name will be referenced in other configuration screens. Interfaces **A1** and **B1** highlighted below represent the private and public interfaces of the Avaya SBCE for SIP Trunking. Each of these interfaces must be enabled after installation.



To enable the interfaces, first navigate to **Device Specific Settings → Network Management** in the left pane and select the device being managed in the center pane. In the right pane, click on the **Interface Configuration** tab. Verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click **Toggle** to enable the interface.



6.3. Signaling Interface

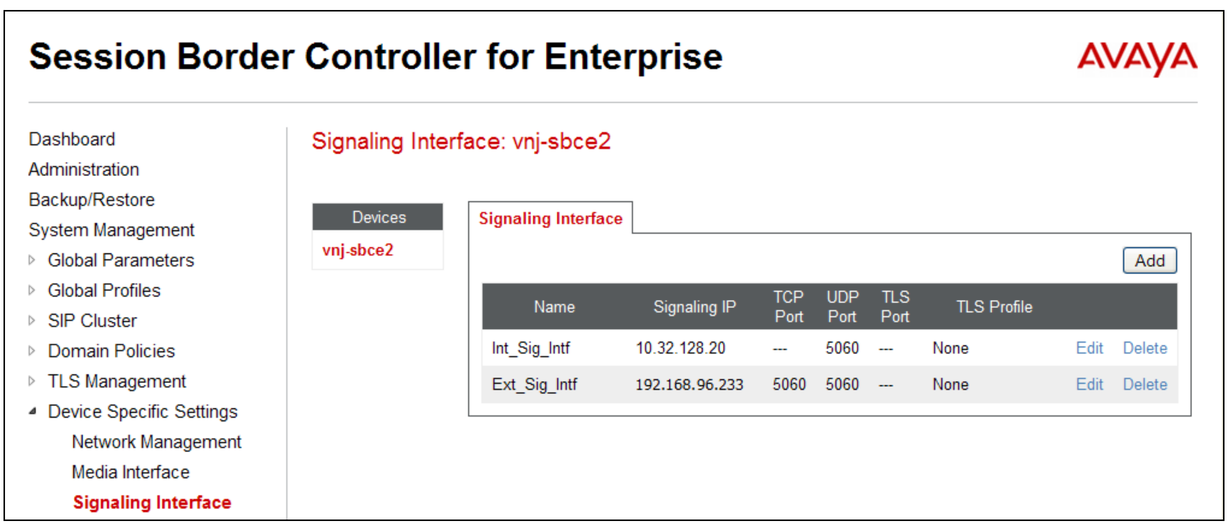
A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface. These two signaling interfaces are shown below.

When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 6.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 6.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. 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 or TCP on port 5060. Since IntelePeer uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.



6.4. Media Interface

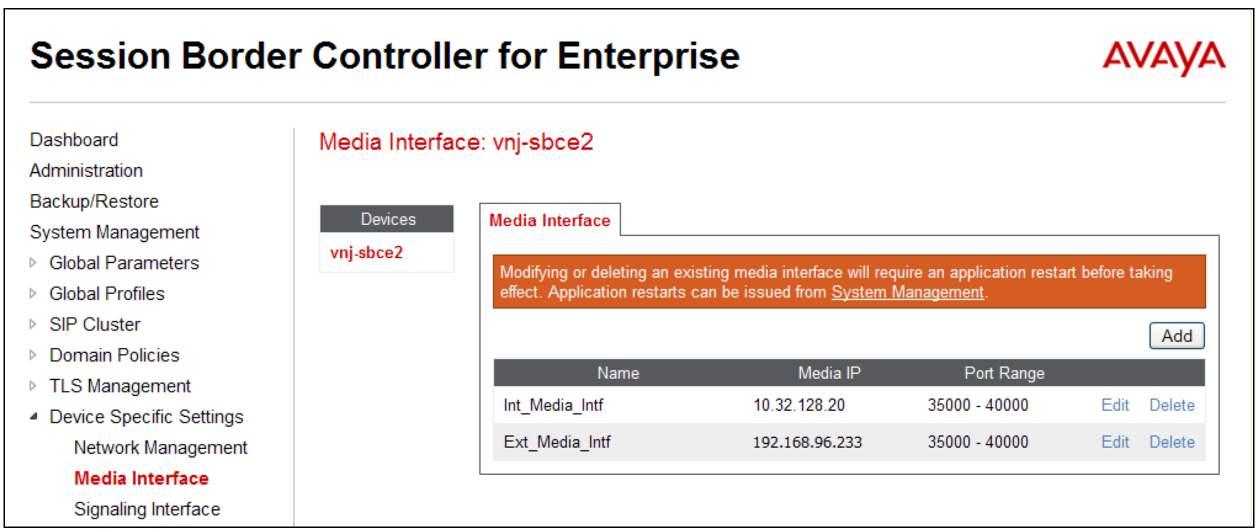
A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int_Media_Intf** was created for the Avaya SBCE internal interface and media interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. Each is shown below.

When configuring the interfaces, configure the parameters as follows:

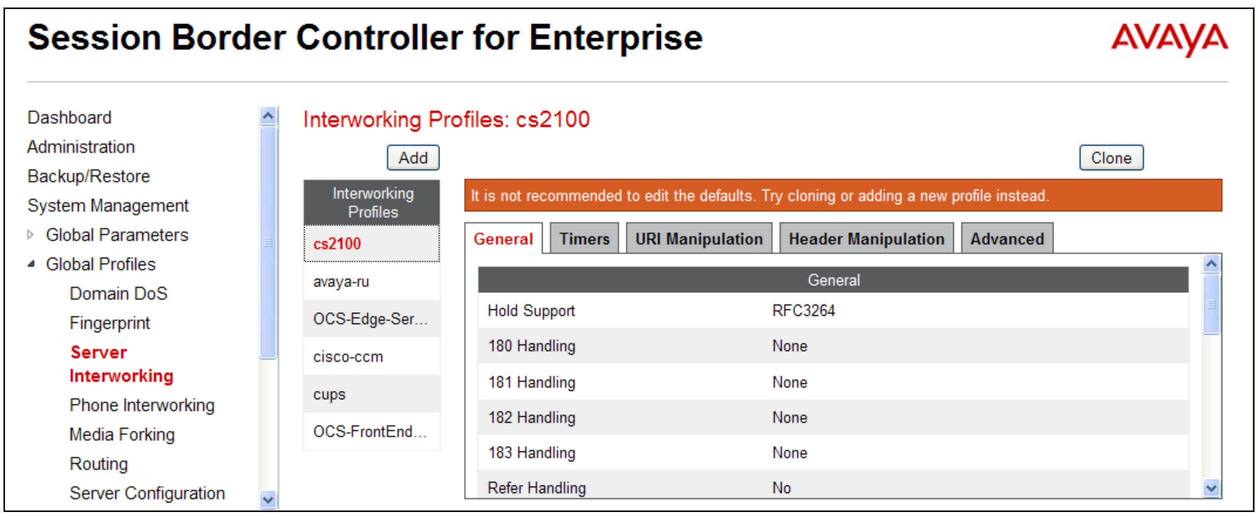
- Set **Name** to a descriptive name.
- For the internal interface, set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 6.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the compliance test, the default port range was used for both interfaces.



6.5. Server Interworking

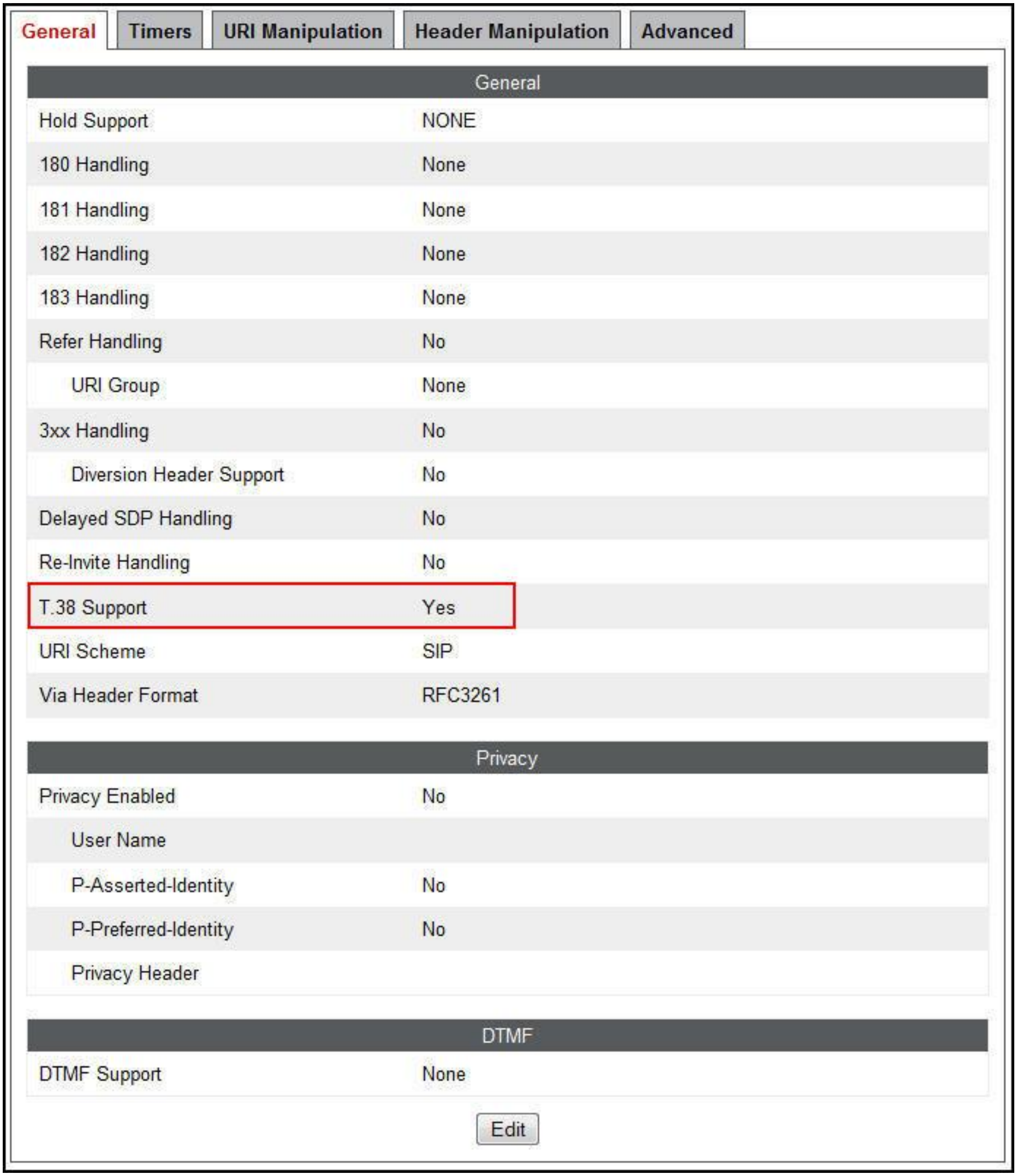
A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create one server interworking profile for Avaya IP Office and another for the service provider SIP server. These profiles will be applied to the appropriate servers in **Section 6.7.1** and **6.7.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



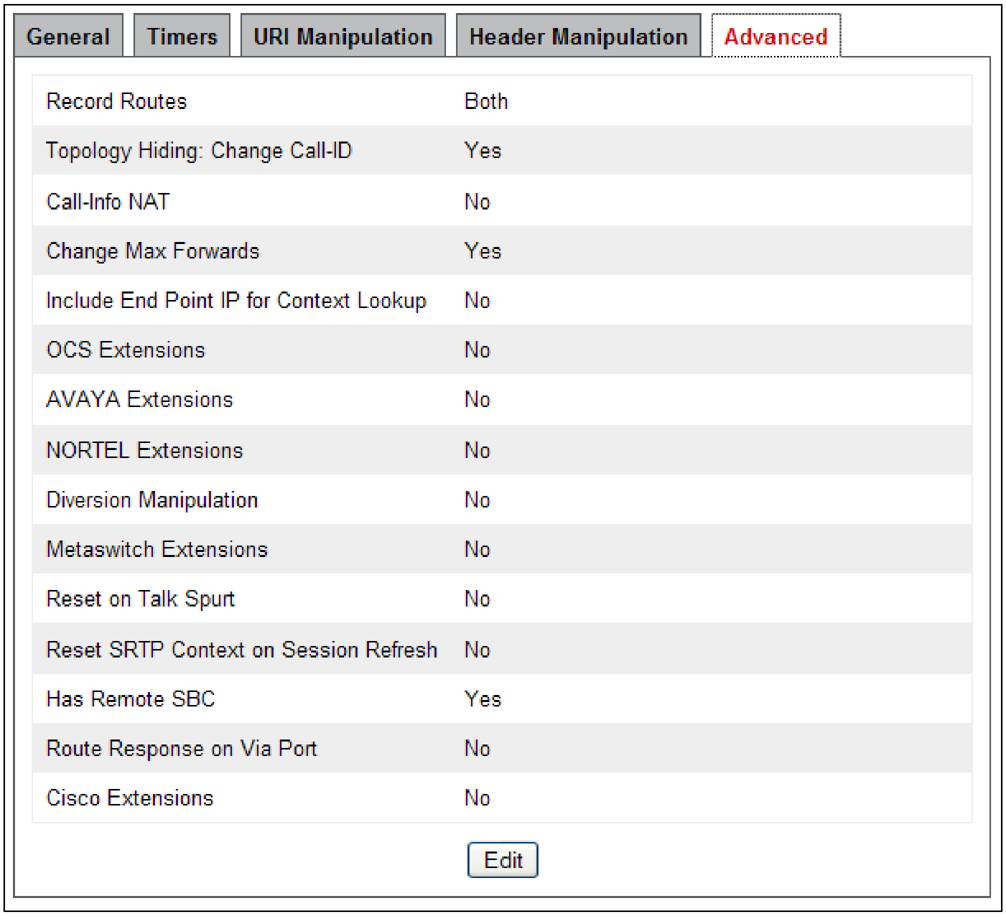
6.5.1. Server Interworking – Avaya IP Office

For the compliance test, server interworking profile ***IPOffice-T38*** was created for Avaya IP Office by creating a new profile and accepting the default values for all settings with the exception of setting the **T.38 Support** to ***Yes***. The **General** tab parameters are shown below.



The **Timers**, **URI Manipulation** and **Header Manipulation** tabs have no entries.

The **Advanced** tab parameters are shown below.



6.5.2. Server Interworking – IntelePeer

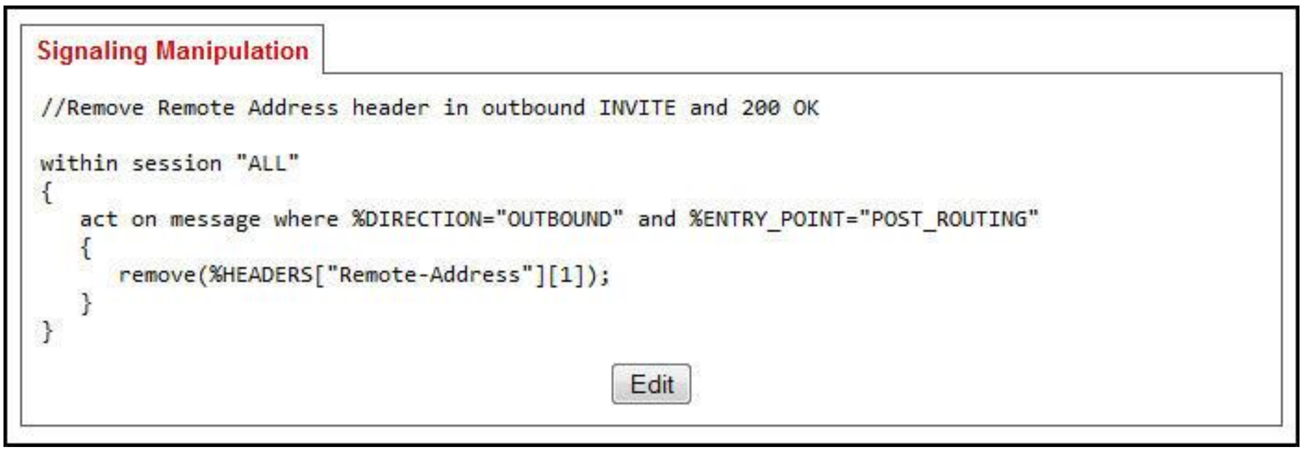
For the compliance test, server interworking profile ***SP-General-T38*** was created for the IntelePeer SIP server. When creating the profile, the default values were used for all parameters with the exception of **T.38 Support** set to ***Yes***. Thus, the **SP-General-T38** profile is identical to the **IPOffice-T38** profile created in **Section 6.5.1**.

6.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be done by other configuration within the Avaya SBCE.

The compliance test used a signaling manipulation script to remove a Remote-Address header from messages (INVITE and 200 OK) originated from the Avaya IP Office. This header needed to be removed since it could contain an IP address on the private enterprise network.

To create a signaling manipulation script, navigate to **Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown), then type in a script title and enter the script statements/commands. Save the script by clicking on **Save** (not shown). For the compliance test, a script named "Remove_Remote-Address" was created. The script is shown below.



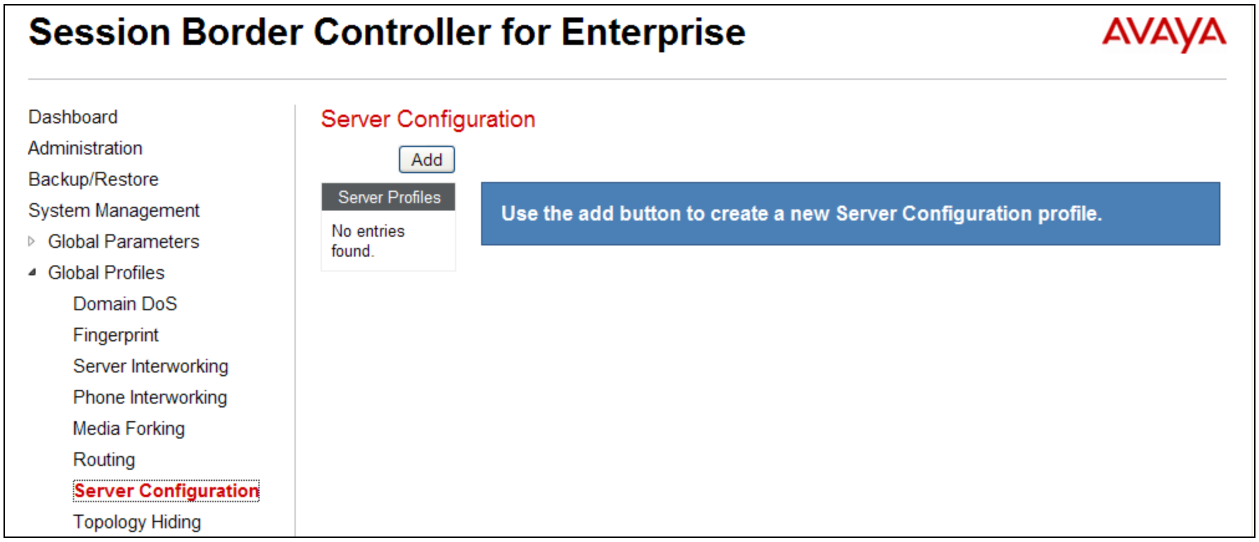
The above script is tied to the IntelPeer trunk server in Server Configuration (**Section 6.7.2**).

Note that use of the Signaling Manipulation scripts demands higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should be used with care and only in cases where the use of Signaling Rules (**Section 6.10**) does not meet the desired result. Refer to **[11]** for information on the Avaya SBCE scripting language

6.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create one server configuration profile for Avaya IP Office and another for the service provider SIP server.

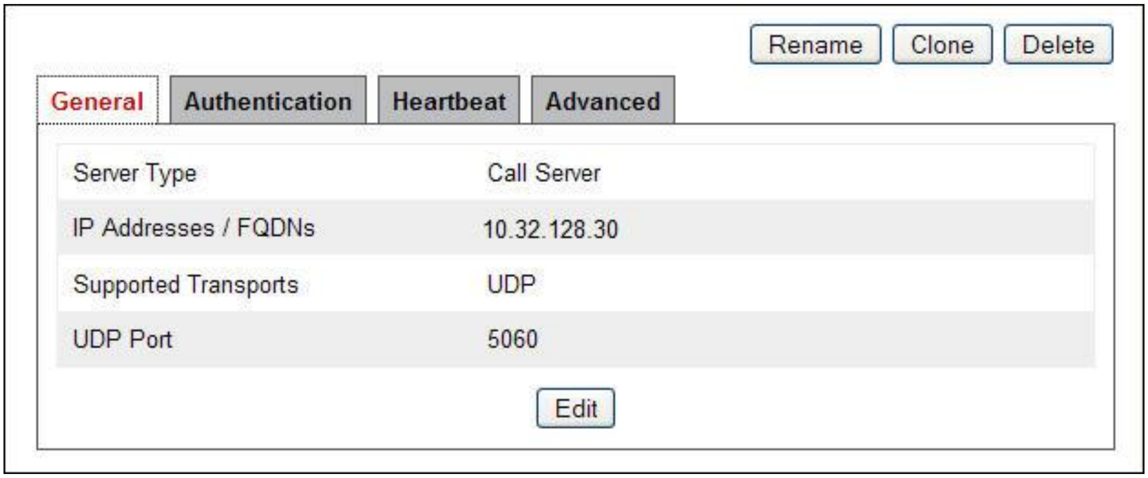
To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



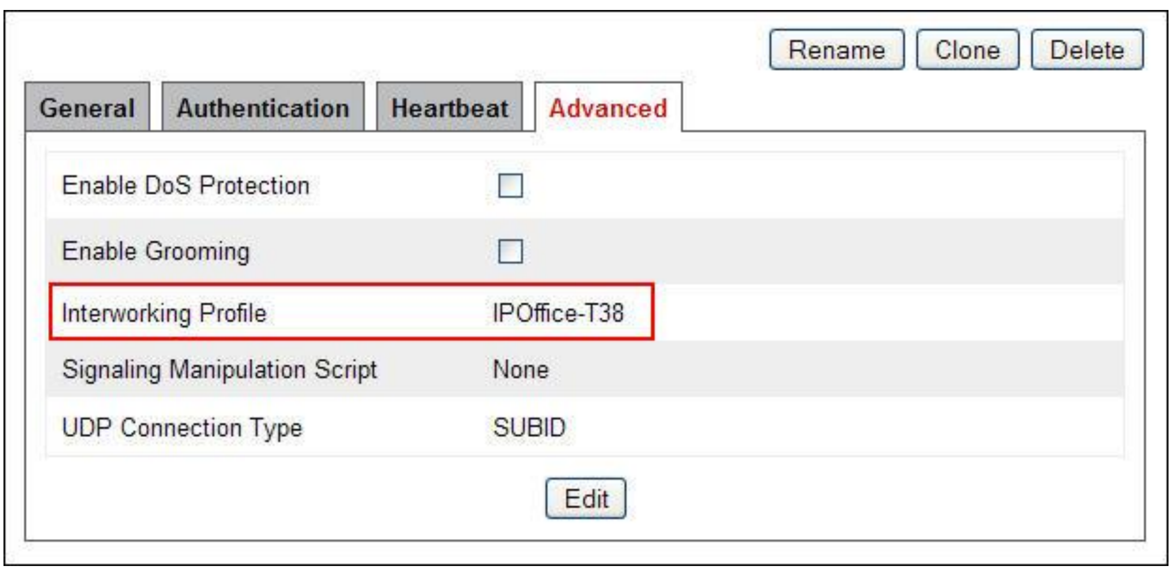
6.7.1. Server Configuration – Avaya IP Office

For the compliance test, server configuration profile **IPO-JCity** was created for Avaya IP Office. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to ***Call Server***.
- Set **IP Addresses / FQDNs** to the IP address of the Avaya IP Office LAN1 port.
- Set **Supported Transports** to the transport protocol used for SIP signaling between Avaya IP Office and the Avaya SBCE.
- Set the **UDP Port** to the port Avaya IP Office will listen on for SIP requests from the Avaya SBCE.



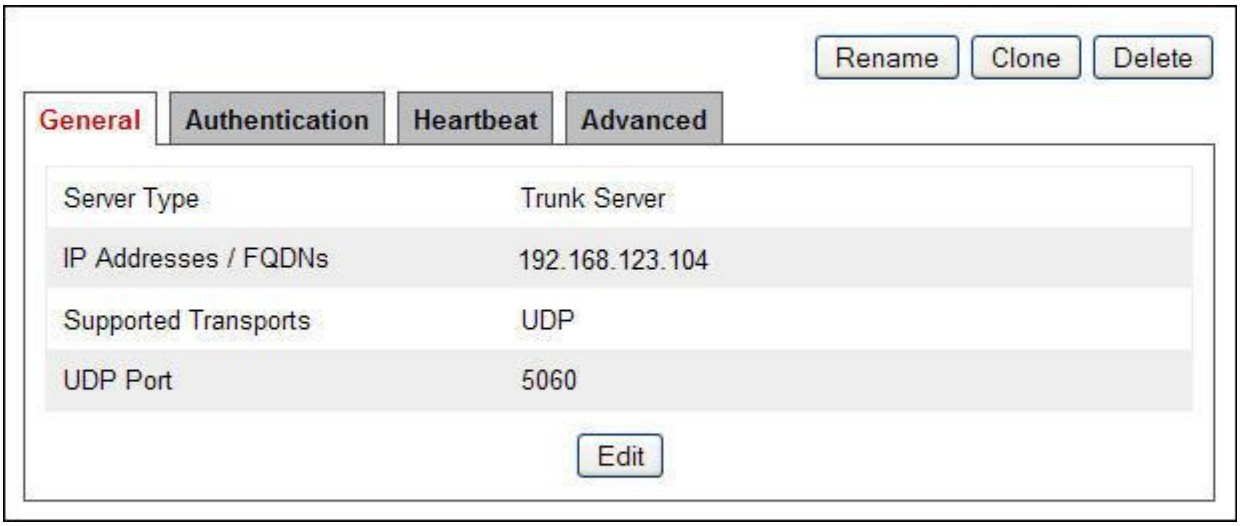
On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Avaya IP Office defined in **Section 6.5.1**.



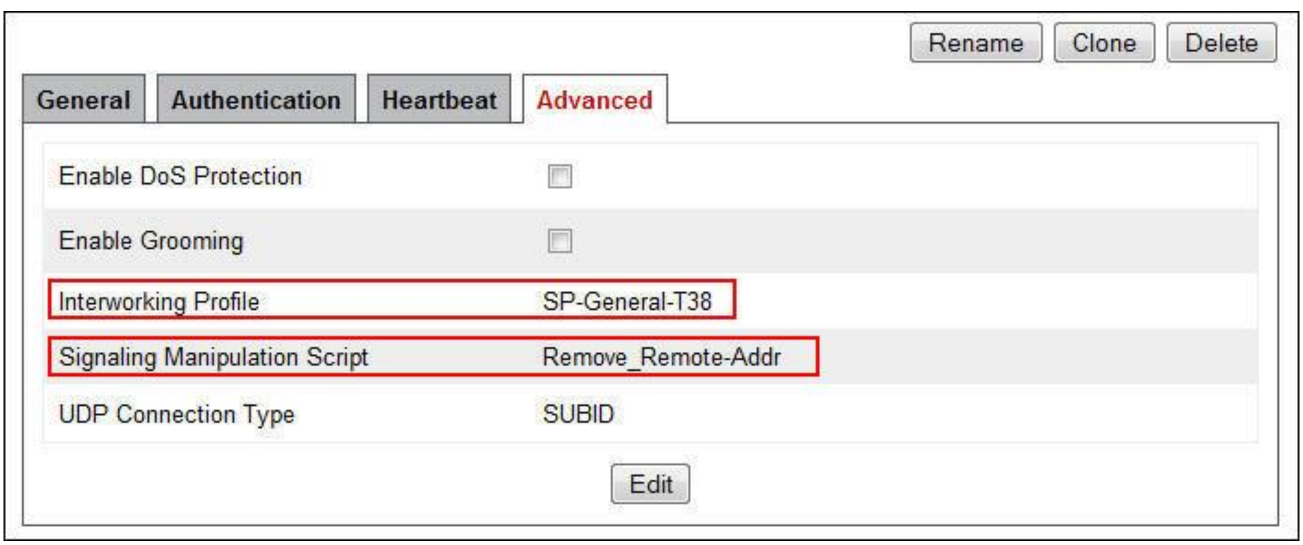
6.7.2. Server Configuration – IntelePeer

For the compliance test, server configuration profile ***IntelePeer*** was created for the IntelePeer SIP Server. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to ***Trunk Server*.**
- Set **IP Addresses / FQDNs** to the IP address of the IntelePeer SIP server.
- Set **Supported Transports** to the transport protocol used for SIP signaling between IntelePeer and the Avaya SBCE. In the compliance test, UDP was used.
- Set the **UDP Port** to the standard SIP port of 5060. This is the port IntelePeer will listen on for SIP requests from the Avaya SBCE.



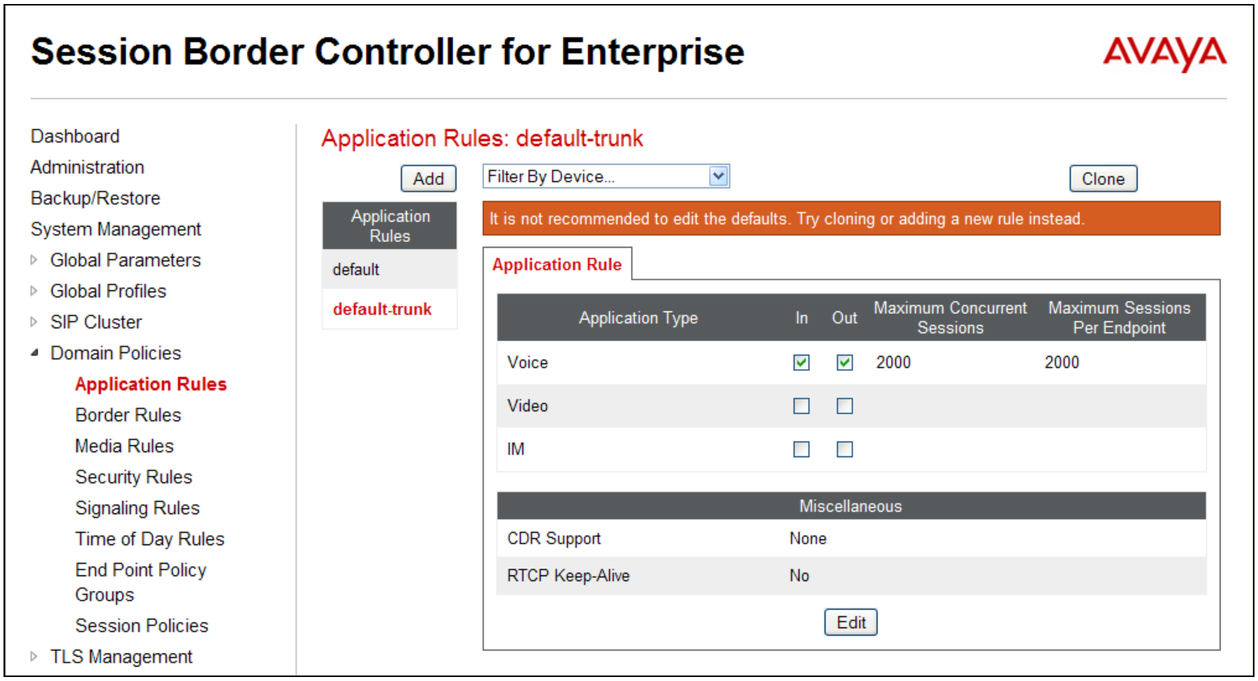
On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for IntelePeer defined in **Section 6.5.2**. For **Signaling Manipulation Script**, select the script created in **Section 6.6**.



6.8. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 6.11**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Avaya IP Office and the IntelePeer SIP server.

To view an existing rule, navigate to **Domain Policies → Application Rules** in the left pane. In the center pane, select the rule (e.g., **default-trunk**) to be viewed.



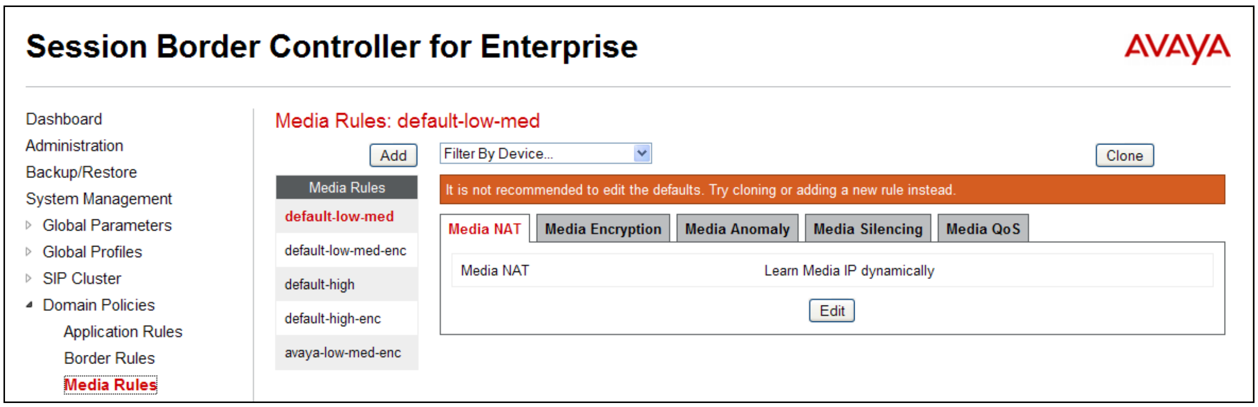
6.9. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 6.11**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Avaya IP Office and the IntelePeer SIP server.

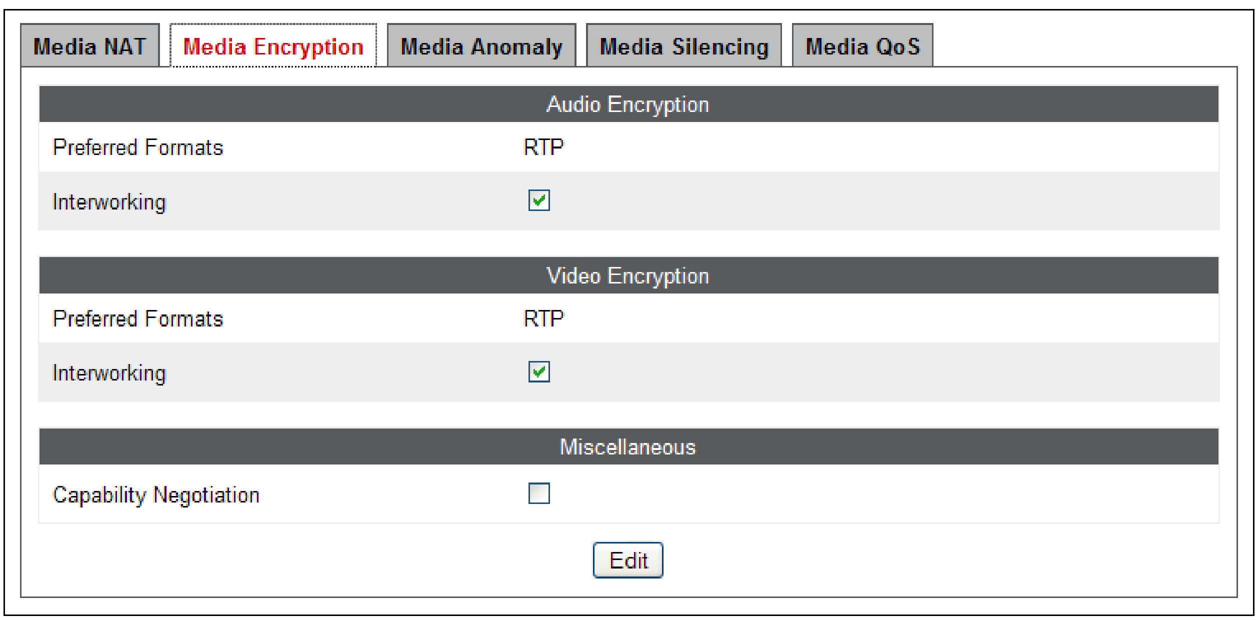
To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed.

Each of the tabs of the **default-low-med** media rule containing data is shown below.

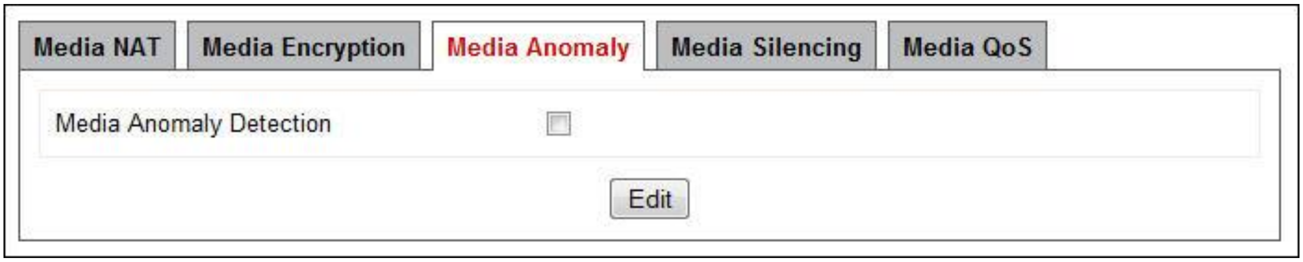
The **Media NAT** tab has no entries.



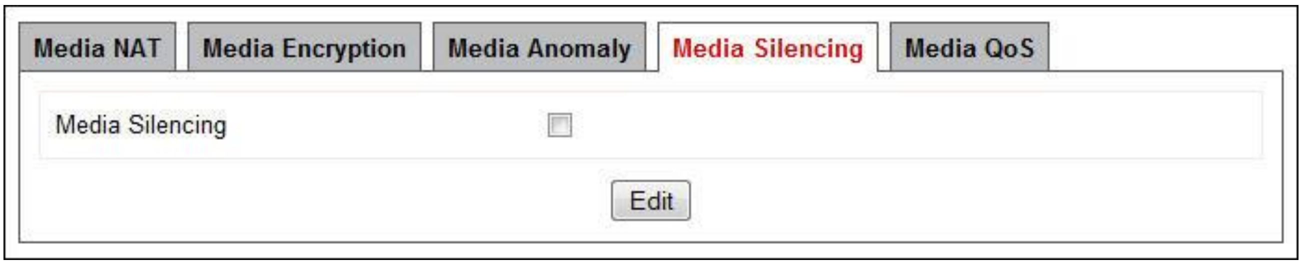
The **Media Encryption** tab indicates that no encryption was used.



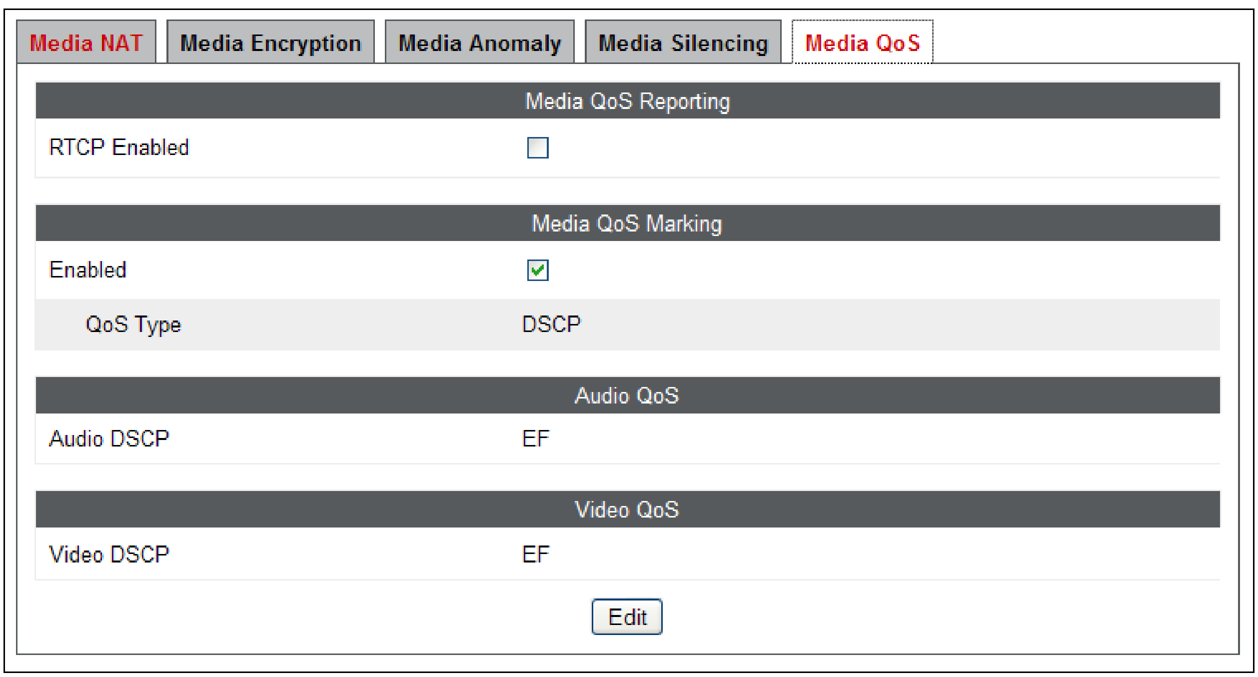
The **Media Anomaly** tab shows **Media Anomaly Detection** was disenabled.



The **Media Silencing** tab shows **Media Silencing** was disenabled.



The **Media QoS** settings are shown below.

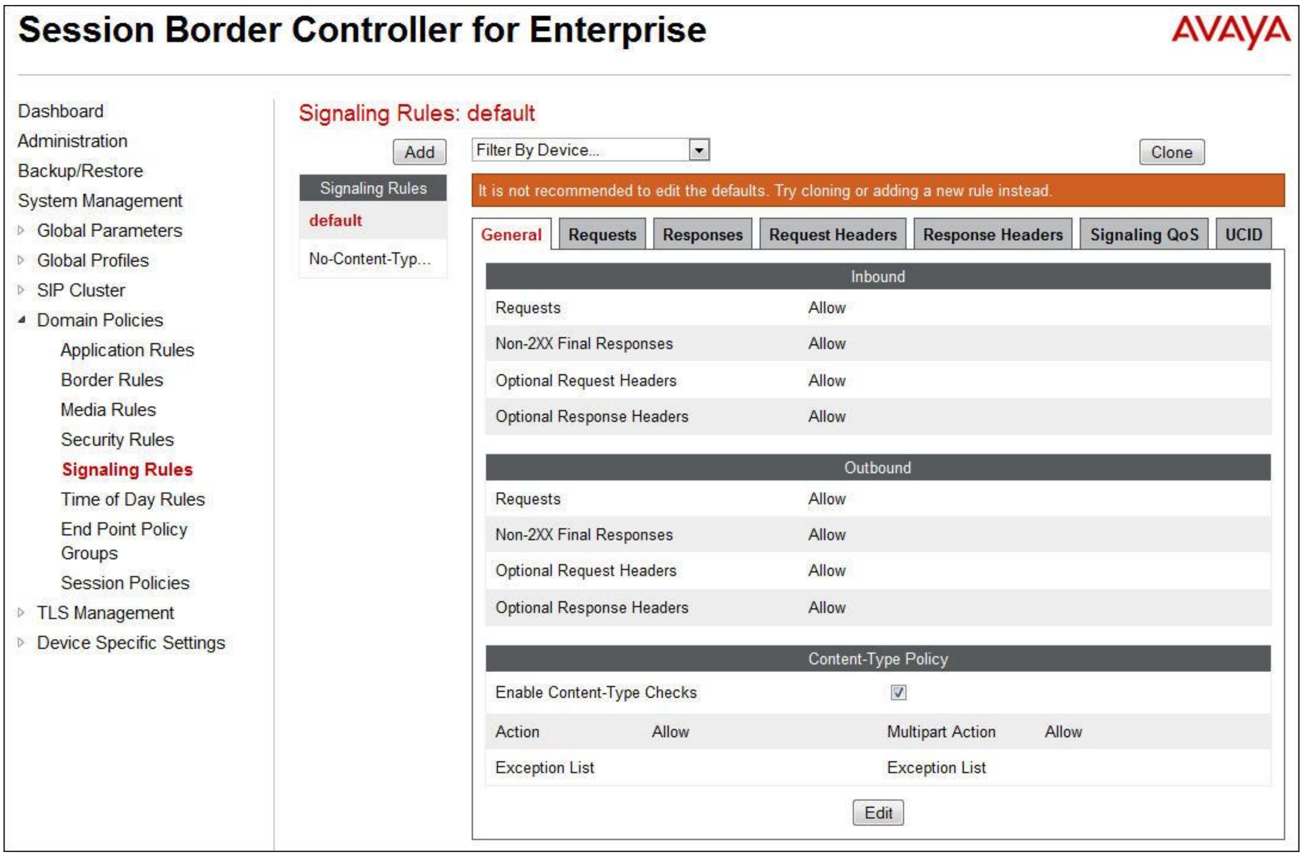


6.10. Signaling Rules

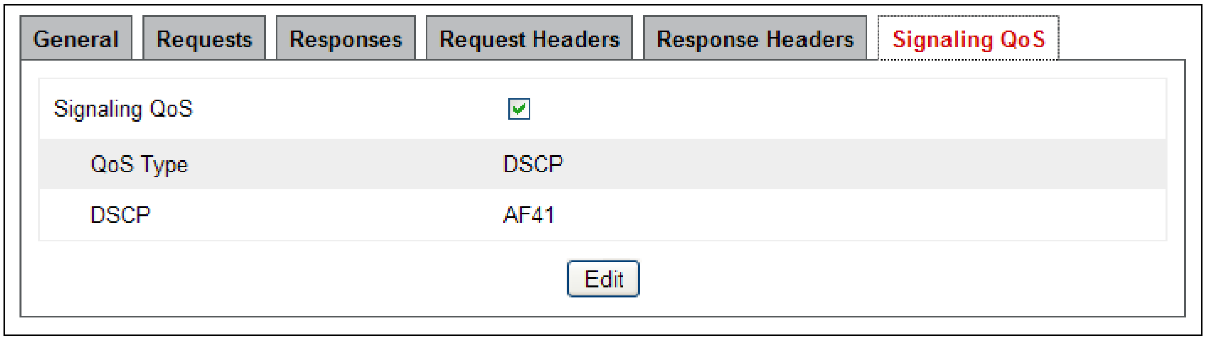
A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 6.11**. For the compliance test, the predefined **default** signaling rule (shown below) was used for both Avaya IP Office and the IntelePeer SIP server.

To view an existing rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select the rule (e.g., **default**) to be viewed.

The **General** tab settings are shown below.



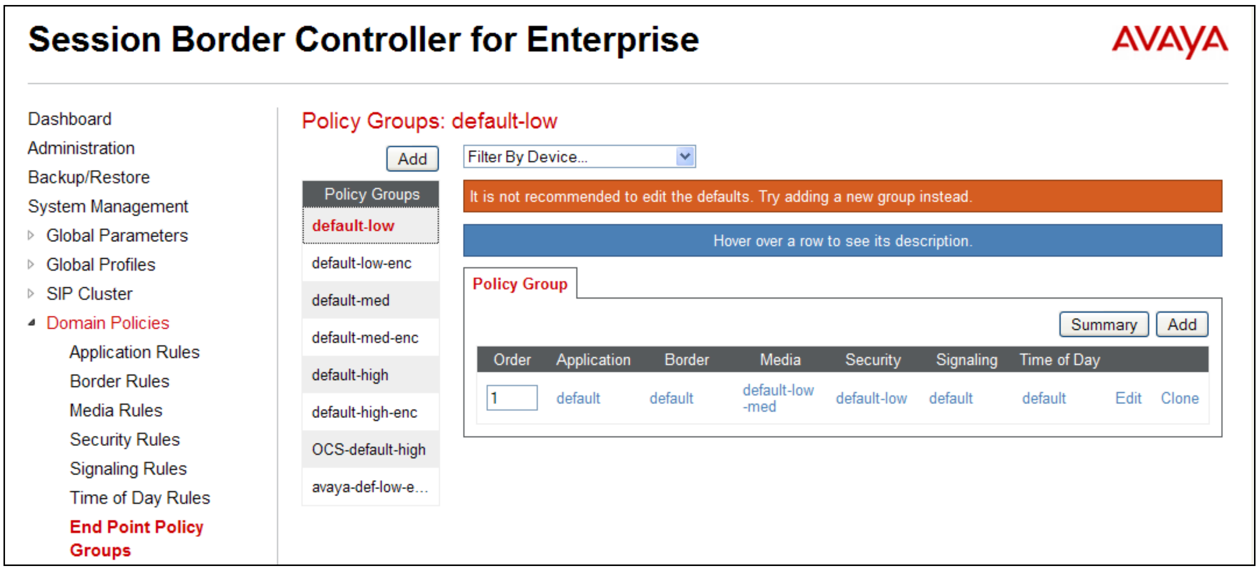
The **Requests**, **Responses**, **Request Headers**, and **Response Headers** tabs have no entries. The **Signaling QoS** tab is shown below.



6.11. Endpoint Policy Groups

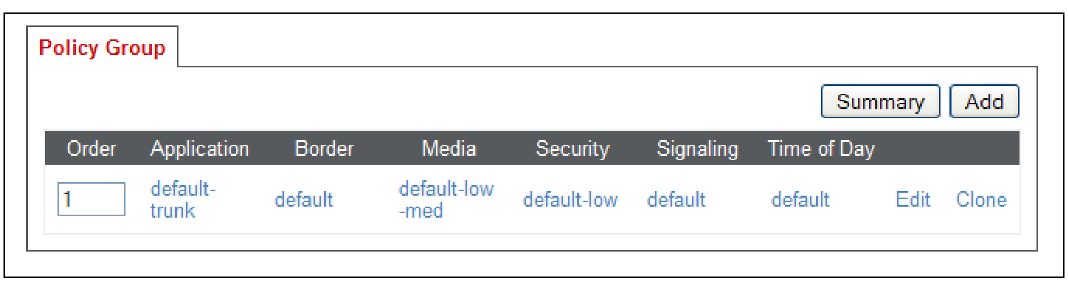
An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one endpoint policy group must be created for Avaya IP Office and another for the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 6.14**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by series of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.



6.11.1. Endpoint Policy Group – Avaya IP Office

For the compliance test, endpoint policy group ***IPO-EP-Policy*** was created for Avaya IP Office. Default values were used for each of the rules which comprise the group with the exception of **Application**. For **Application**, enter the application rule specified in **Section 6.8**. The details of the default settings for **Media** and **Signaling** are showed in **Section 6.9** and **Section 6.10** respectively.



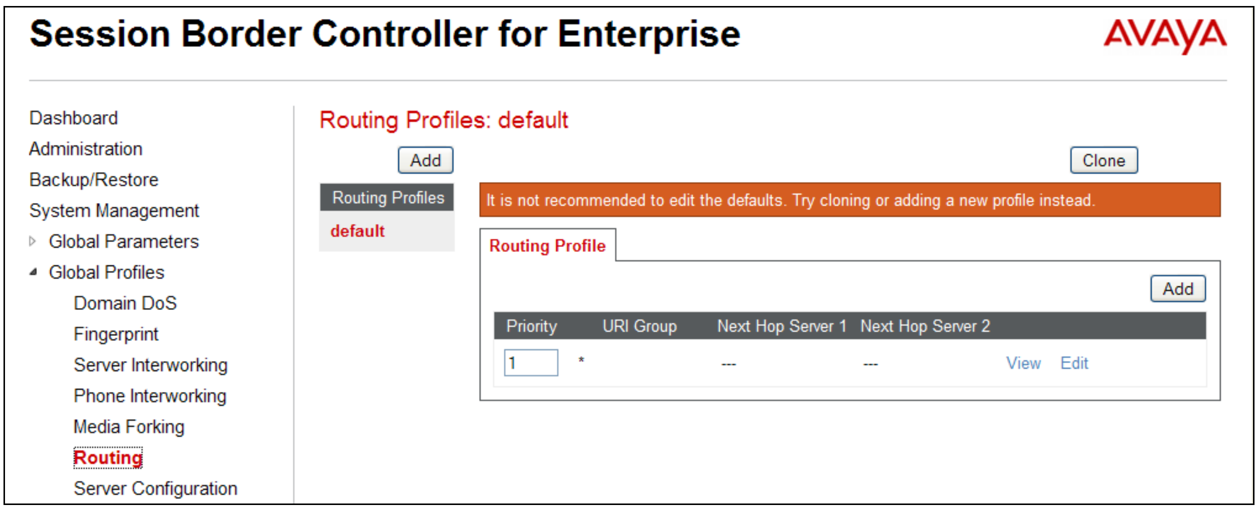
6.11.2. Endpoint Policy Group – IntelePeer

For the compliance test, endpoint policy group ***SP-EP-Policy*** was created for the IntelePeer SIP server. Default values were used for each of the rules which comprise the group with the exception of **Application**. For **Application**, enter the application rule specified in **Section 6.8**. Thus, the **SP-EP-Policy** is identical to the **IPO-EP-Policy** created in **Section 6.11.1**.

6.12. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 6.14**. Create one routing profile for Avaya IP Office and another for the service provider SIP server.

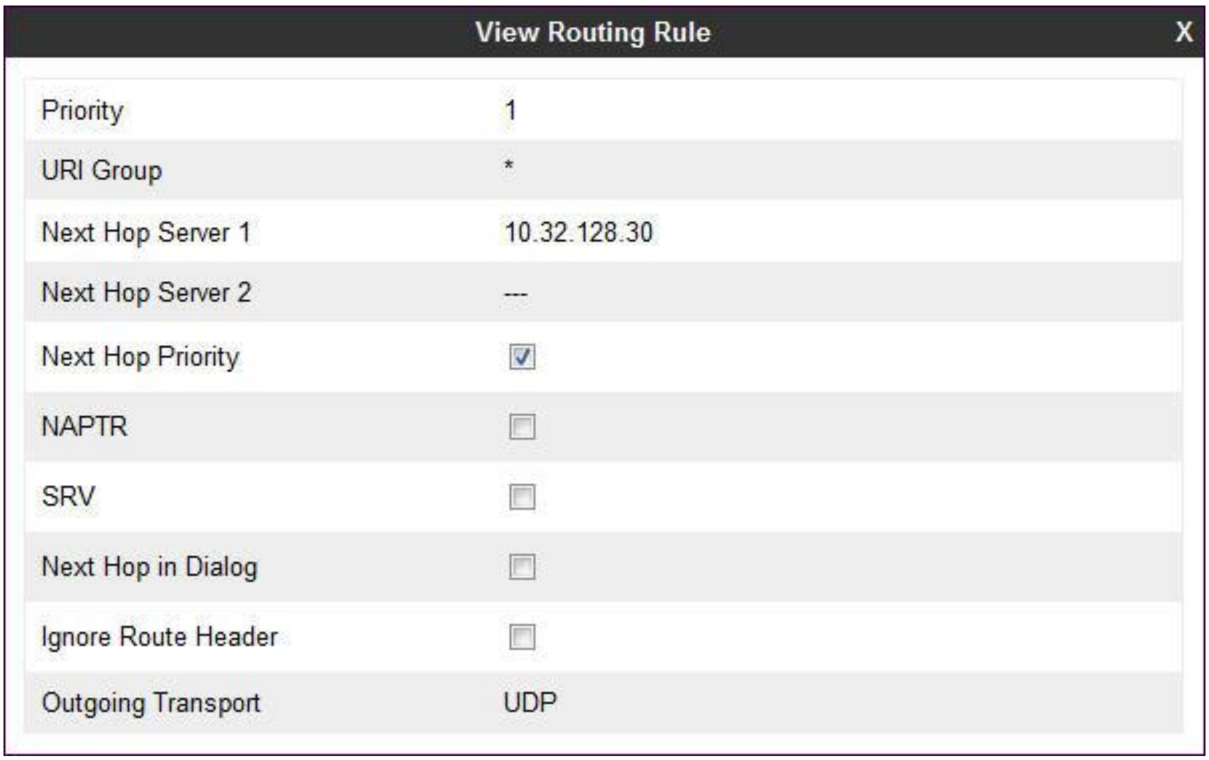
To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



6.12.1. Routing – Avaya IP Office

For the compliance test, routing profile **To-IPO-JCity** was created for Avaya IP Office. When creating the profile, configure the parameters as follows:

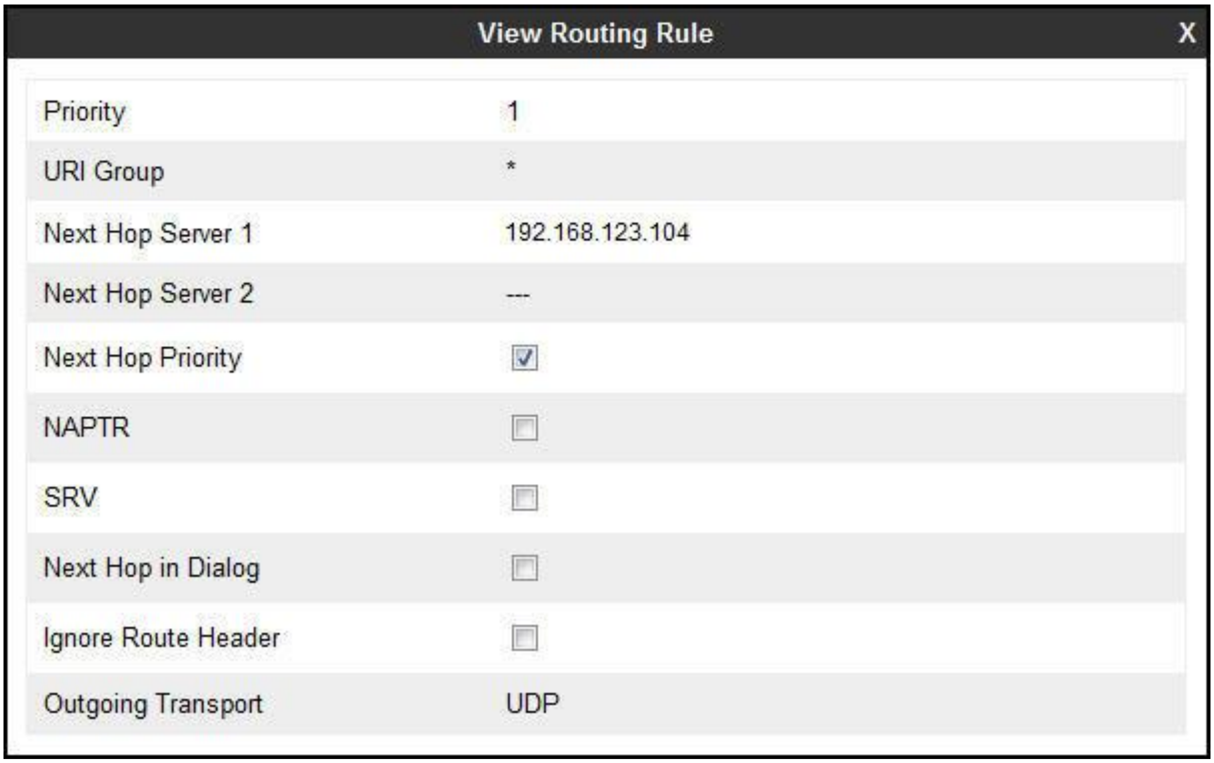
- Set the **URI Group** to the wild card ***** to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of Avaya IP Office LAN1 port.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP**.



6.12.2. Routing – IntelePeer

For the compliance test, routing profile ***To-IntelePeer*** was created for IntelePeer. When creating the profile, configure the parameters as follows:

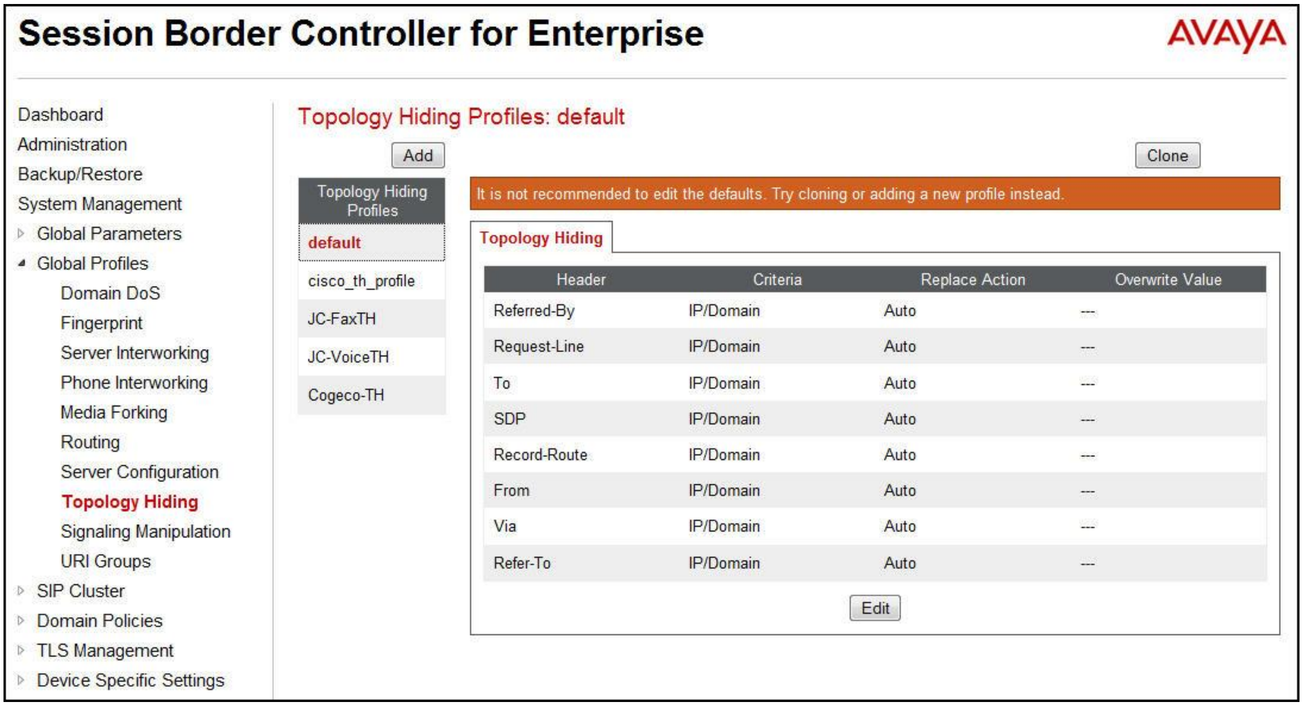
- Set the **URI Group** to the wild card ***** to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the IntelePeer SIP server.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP** as defined by IntelePeer.



6.13. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 6.14**. For the compliance test, the predefined **default** topology hiding profile (shown below) was used for both Avaya IP Office and the IntelePeer SIP server.

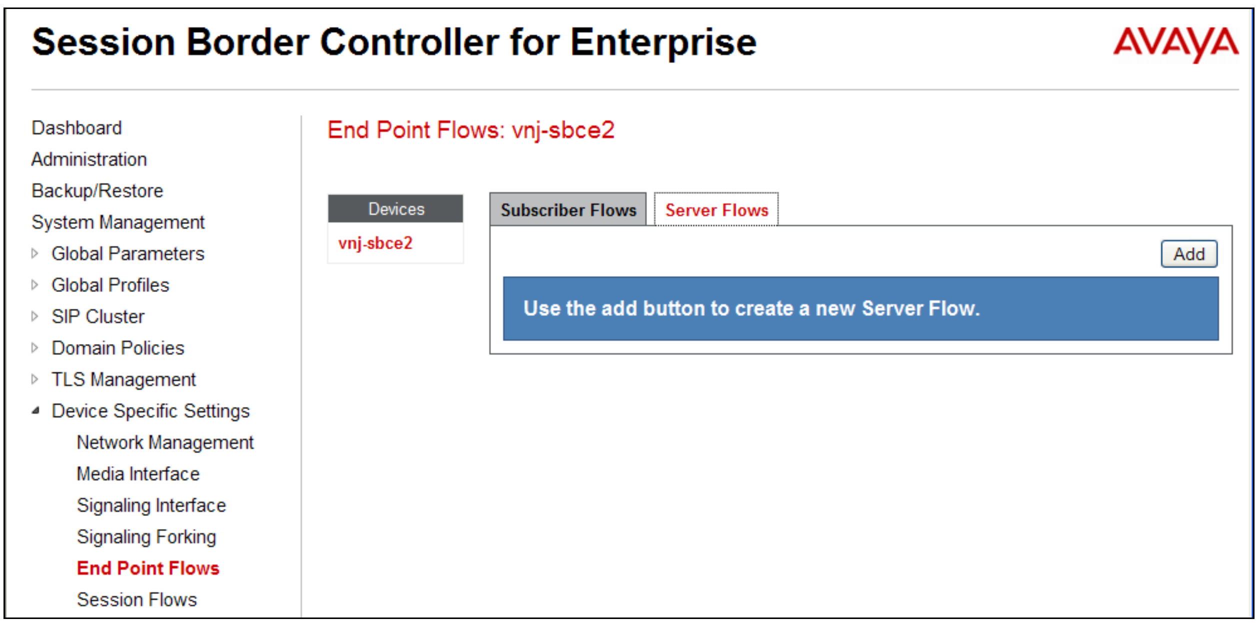
To add a new profile or view an existing profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add** to add a new profile, or select an existing profile (e.g., **default**) to be viewed.



6.14. End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at 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 policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the signaling endpoints are Avaya IP Office and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the far right pane.



6.14.1. End Point Flow – Avaya IP Office

For the compliance test, endpoint flow ***IPO-JCity*** was created for Avaya IP Office. All traffic from Avaya IP Office will match this flow as the source flow and use the specified routing profile **To-IntelePeer** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Avaya IP Office server created in **Section 6.7.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *.
- Set the **Received Interface** to the external signaling interface.
- Set the **Signaling Interface** to the internal signaling interface.
- Set the **Media Interface** to the internal media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Avaya IP Office in **Section 6.11.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.12.2** used to direct traffic to the IntelePeer SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Avaya IP Office in **Section 6.13**.

View Flow: IPO-JCity X

Criteria		Profile	
Flow Name	IPO-JCity	Signaling Interface	Int_Sig_Intf
Server Configuration	IPO-JCity	Media Interface	Int_Media_Intf
URI Group	*	End Point Policy Group	IPO-EP-Policy
Transport	*	Routing Profile	To-IntelePeer
Remote Subnet	*	Topology Hiding Profile	default
Received Interface	Ext_Sig_Intf	File Transfer Profile	None

The screen below shows the saved **IPO-JCity** configuration as a Server Flow. Note that the server name is in the **Server Configuration** heading.

Server Configuration: IPO-JCity

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IPO-JCity	*	Ext_Sig_Intf	Int_Sig_Intf	IPO-EP-Policy	To-IntelePeer	View Clone Edit Delete

6.14.2. End Point Flow – IntelePeer

For the compliance test, endpoint flow ***IntelePeer*** was created for the IntelePeer SIP server. All traffic from IntelePeer will match this flow as the source flow and use the specified routing profile **To-IPO-JCity** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the IntelePeer SIP server created in **Section 6.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set the **Received Interface** to the internal signaling interface.
- Set the **Signaling Interface** to the external signaling interface.
- Set the **Media Interface** to the external media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for IntelePeer in **Section 6.11.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.12.1** used to direct traffic to Avaya IP Office.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for IntelePeer in **Section 6.13**.

View Flow: IntelePeer

Criteria		Profile	
Flow Name	IntelePeer	Signaling Interface	Ext_Sig_Intf
Server Configuration	IntelePeer	Media Interface	Ext_Media_Intf
URI Group	*	End Point Policy Group	SP-EP-Policy
Transport	*	Routing Profile	To-IPO-JCity
Remote Subnet	*	Topology Hiding Profile	default
Received Interface	Int_Sig_Intf	File Transfer Profile	None

The screen below shows the saved **IntelePeer** configuration as a Server Flow. Note that the server name is in the **Server Configuration** heading.

Server Configuration: IntelePeer

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	IntelePeer	*	Int_Sig_Intf	Ext_Sig_Intf	SP-EP-Policy	To-IPO-JCity	View	Clone	Edit	Delete

7. IntelePeer SIP Trunking Configuration

IntelePeer is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise site (i.e., the IP address of the public interface on the Avaya SBCE). IntelePeer will provide the customer the necessary information to configure the Avaya IP Office and Avaya SBCE including:

- Network edge IP addresses of the IntelePeer SIP Trunking Service.
- Transport and port for the IntelePeer SIP Trunking connection to the Avaya SBCE at the enterprise.
- DID numbers to assign to users at the enterprise.
- Supported codecs and their preference order.

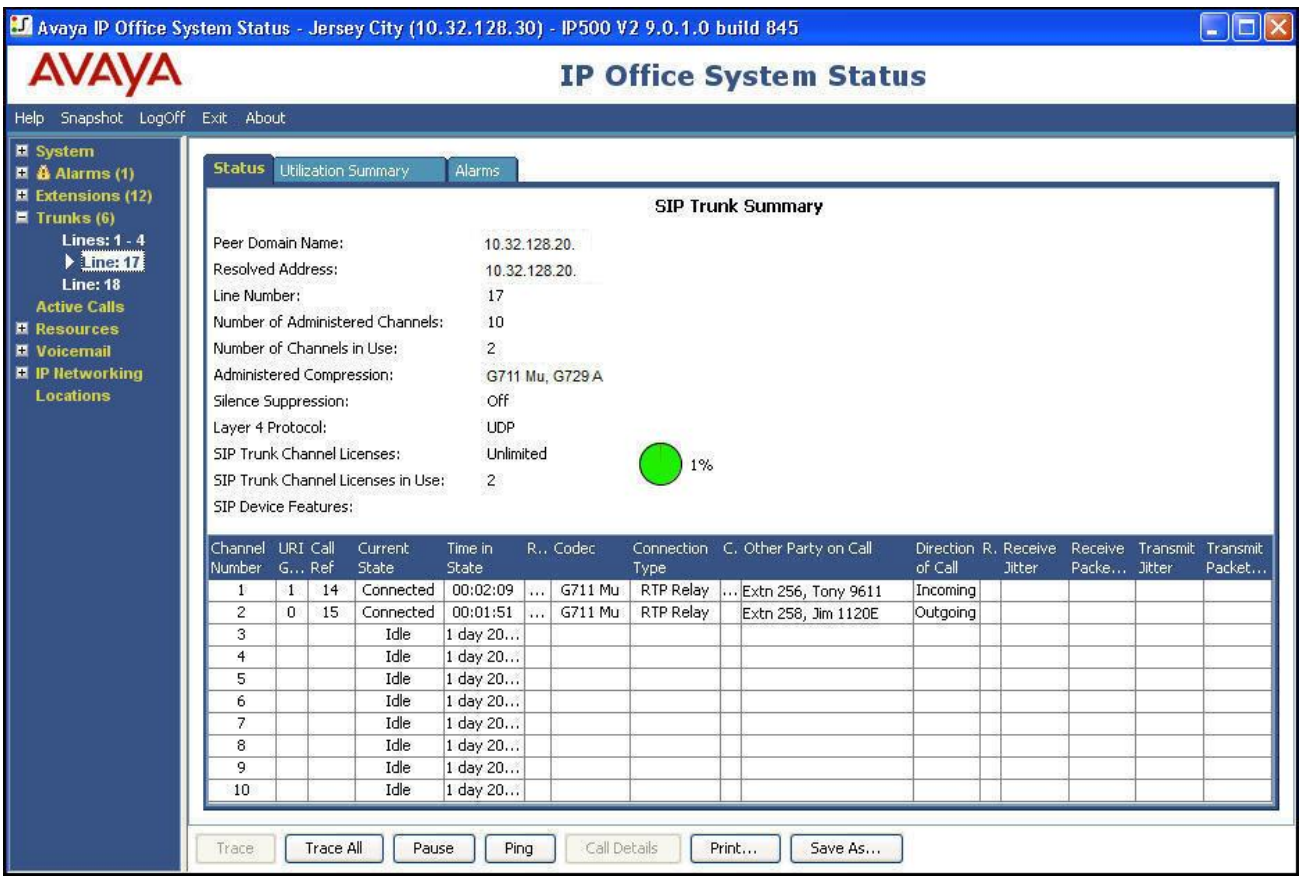
8. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly

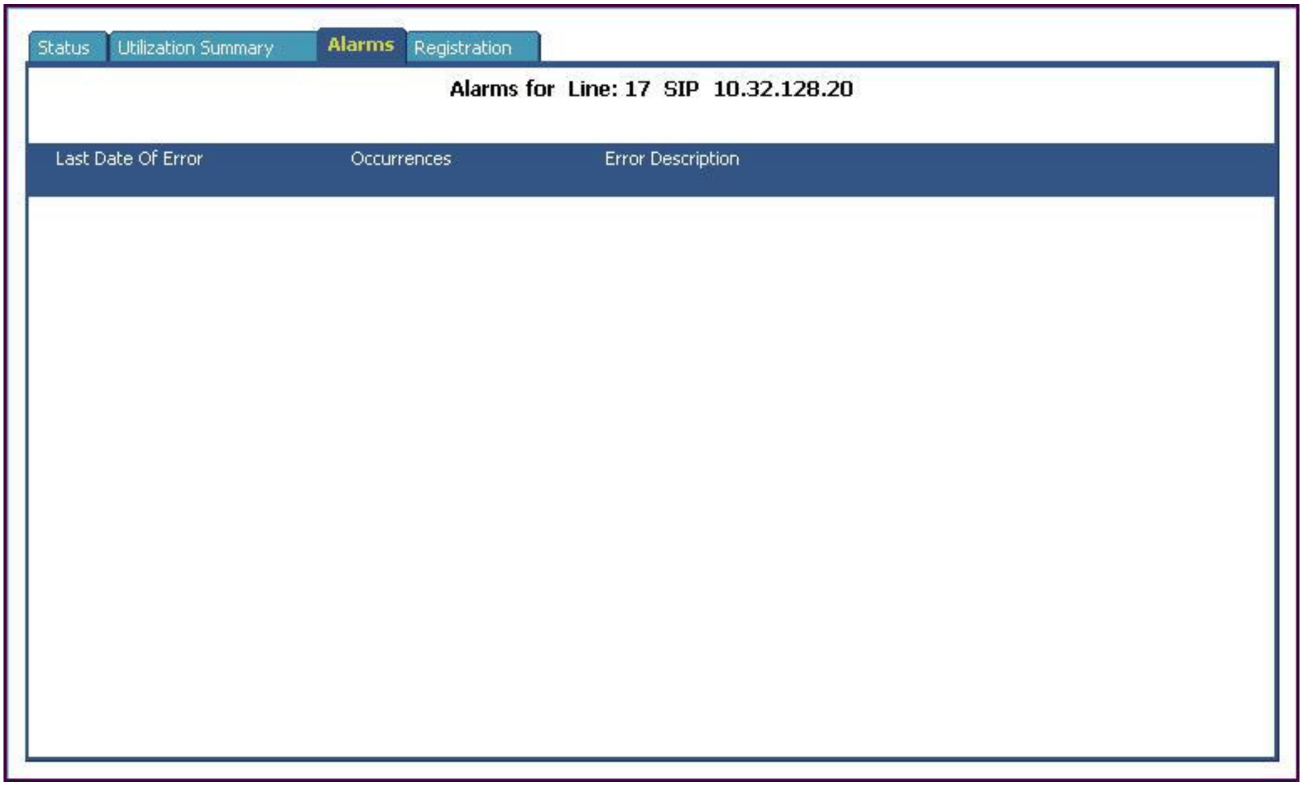
8.1. Avaya IP Office System Status

Use the Avaya IP Office System Status application to verify the SIP Line channels state and to check alarms:

- Launch the application from **Start → Programs → IP Office → System Status** on the Avaya IP Office Manager PC. Select the SIP line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** is **Idle** for channels where no active calls are currently in session; the state should be **Connected** for channels engaged in active calls.

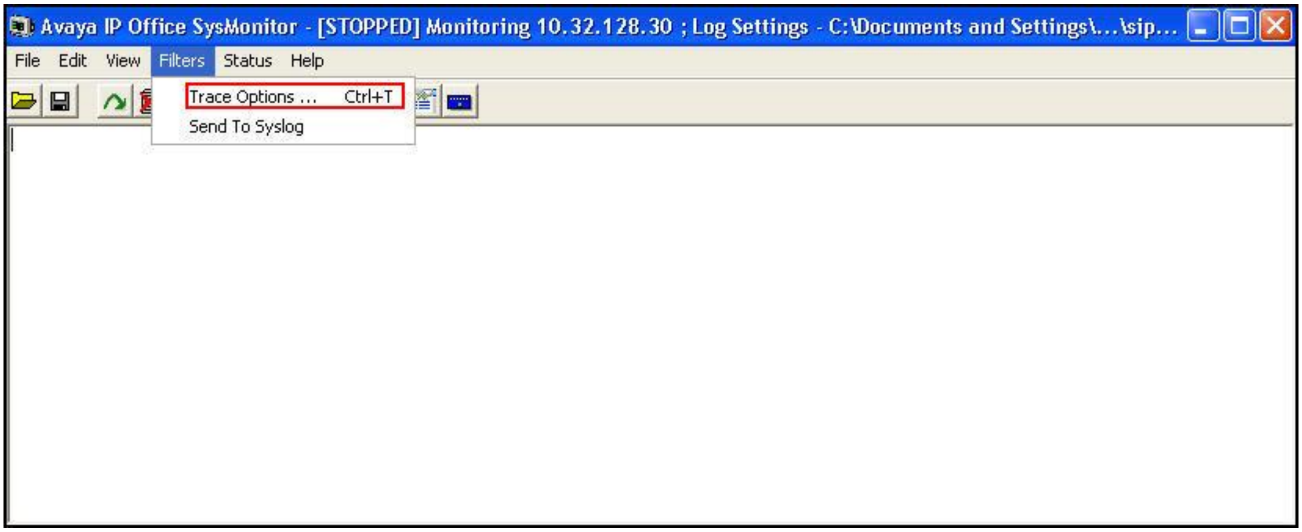


- Select the **Alarms** tab and verify that no alarms are active on the SIP line.

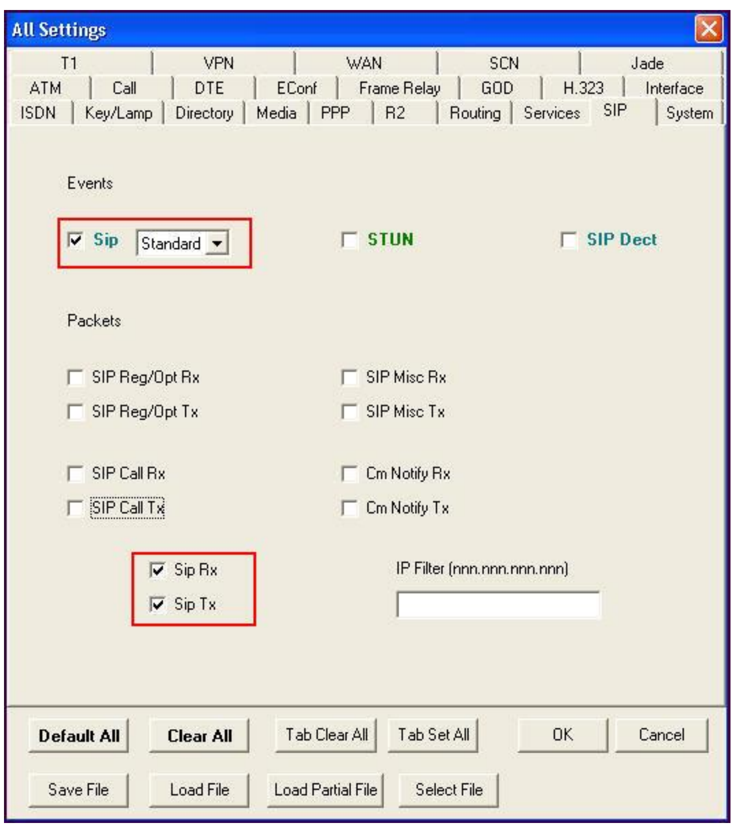


8.2. Avaya IP Office Monitor

The Monitor application can be used to monitor and troubleshoot Avaya IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor** on the Avaya IP Office Manager PC. The application allows the monitored information to be customized. To customize, select **Filters → Trace Options …** as shown below:



The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, ***Standard*** SIP Events and the **SIP Rx** and **SIP Tx** boxes are checked.



8.3. Avaya SBCE Protocol Trace

The Avaya SBCE can take internal traces on specified interfaces. Both SIP signaling crossing interfaces A1 and B1 can be captured for troubleshooting. In the Avaya SBCE web interface, navigate to **Device Specific Settings → Troubleshooting → Trace** to invoke this facility, select or supply the relevant information (e.g., A1 or B1 or any interfaces, IP/port, protocol, number of packets to capture, capture file name, etc.), then start the trace. The captured trace can then be downloaded for examination using a protocol sniffer application such as Wireshark.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office R9.0.1 and the Avaya Session Border Controller for Enterprise R6.2.1 to the IntelePeer SIP Trunking Service. The IntelePeer SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks. The IntelePeer SIP Trunking Service passed compliance testing. Please refer to **Section 2.2** for any exceptions.

10. Additional References

Avaya IP Office R9.0

[1] *IP Office Documentation Library*, Release 9.0, Documentation number 15-604278 Issue 1, September 2013
[2] *IP Office 9.0 Product Description*, Documentation number 15-601041 Issue 27.02.0, January 2014
[3] *Avaya IP Office 9.0 Installing IP500/IP500 V2*, Document number15-601042 Issue 28j, January 2014
[4] *Avaya IP Office 9.0 Administering Voicemail Pro*, Document number15-601063 Issue 9.01.0, September 2013
[5] *Avaya IP Office Manager Release 9.0*, Document number15-601011 Issue 9.02.0, January 2014
[6] *Avaya IP Office 9.0 Using System Status*, Document number15-601758 Issue 09c, August 2013
[7] *Avaya IP Office 9.0 Using IP Office System Monitor*, Document Number 15-601019, Issue 05c, August 2013
[8] *Avaya IP Office 9.0 H.323 Telephone Installation*, Document Number 15-601046, Issue 18b, August 2013
[9] *Avaya IP Office 9.0 SIP Extension Installation*, Issue 3c, August 2013

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

Avaya Session Border Controller for Enterprise

[10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Issue 2, December 2013
[11] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014
[12] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*, September 2013

Product documentation for the IntelePeer SIP Trunking is available from IntelePeer. See **Section 2.3** on how to contact IntelePeer.

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.

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.

Supported Remote Worker endpoints for Avaya IP Office are:

- Flare® Experience for iPad
- Flare® Experience for Windows
- one-X® Mobile Preferred VoIP client for iOS
- one-X® Mobile Preferred VoIP client for Android

For Avaya IP Office R9.0, the following table summarizes encryption support for these remote worker endpoints (see **Section 11.1.8**):

Client type	Uses to the external interface of the SBCE		
	TLS	SRTP Audio	SRTP Video
Flare Experience for iPad	Y*	Y*	N
Flare Experience for Windows	Y*	Y*	N
one-X Mobile Preferred VoIP client for iOS	Y	N	N
one-X Mobile Preferred VoIP client for Android	N	N	N
* If the client is used inside and outside of the IP Office core, the signalling type must be changed. IP Office 9.0 does not support TLS or SRTP connections to these clients on the inside of the SBCE.			

In the configuration for the compliance test, Avaya Flare® Experience 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 Verizon FiOS Internet Service located between the Remote Worker private LAN and the public Internet. The Verizon FiOS router also provides DHCP functionality in the private space. Note that the use of the Verizon FiOS router is for functionality testing only and is not prescriptive.

Provisioning of the Verizon FiOS 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.

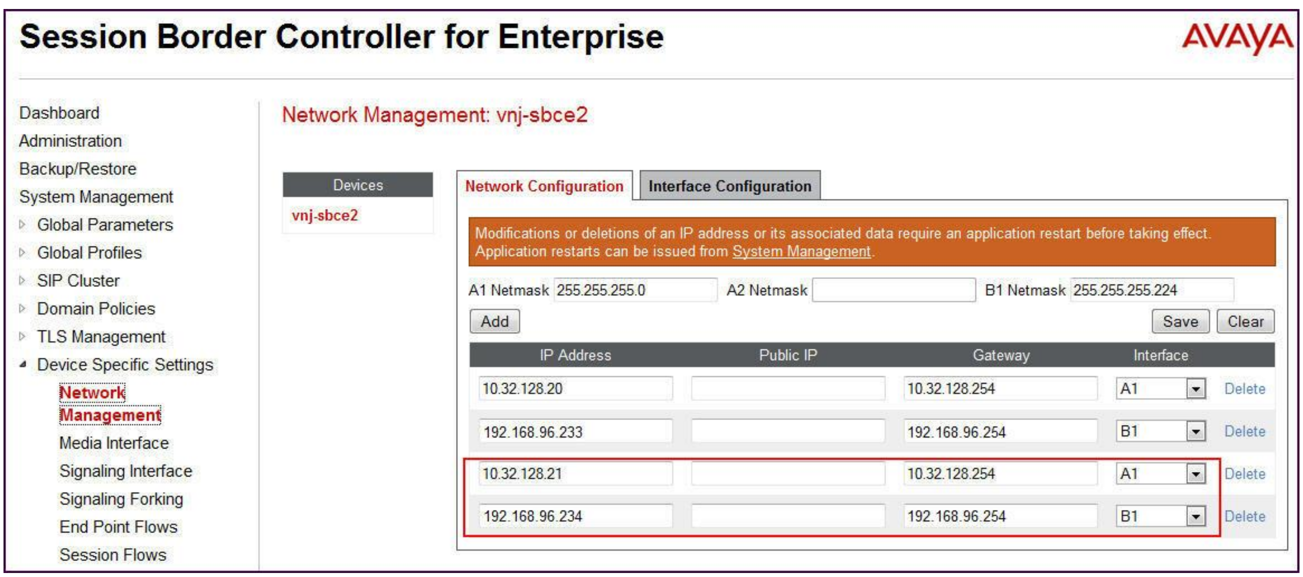
11.1.1. Network Management

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 address assigned to physical interface A1.

The following IP addresses were used on the Avaya SBCE in the configuration used for the compliance test:

- **192.168.128.20** is the inside address previously provisioned for SIP Trunking with the service provider (see **Section 6.2**).
- **192.168.128.21** is the new inside address for Remote Worker.
- **192.168.96.233** is the outside address previously provisioned for SIP Trunking with the service provider (see **Section 6.2**).
- **192.168.96.234** is the new outside address for Remote Worker.

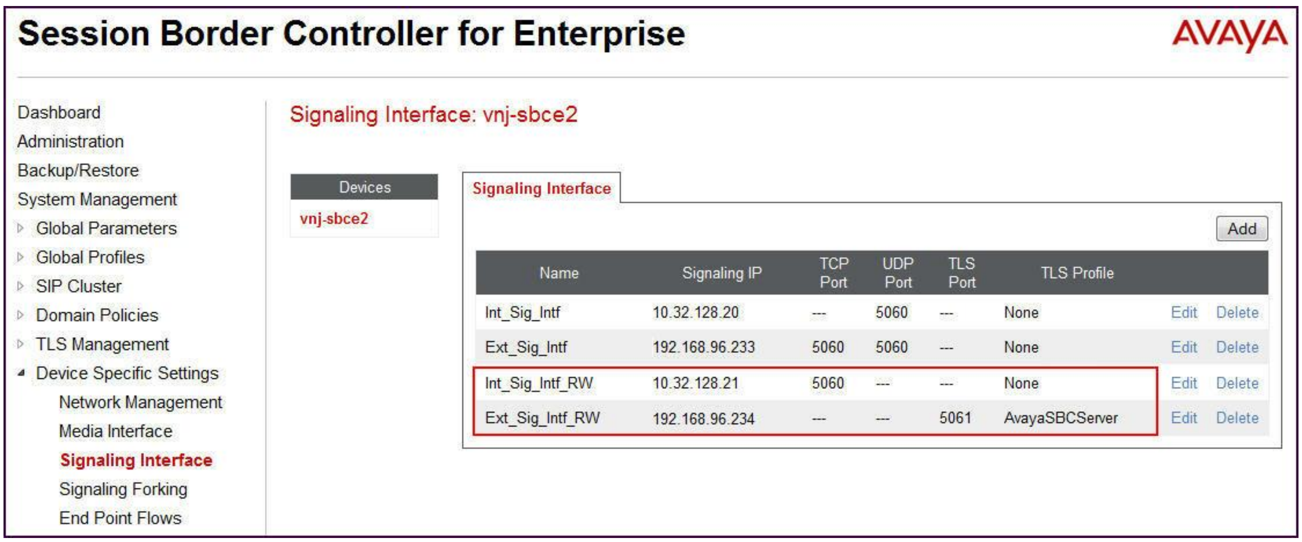
1. On the **Network Configuration** tab, select **Add** to create an entry for **192.168.128.21** on interface **A1**, then select **Save**.
2. Repeat step 1 for adding an entry for **192.168.96.234** on interface **B1**.



11.1.2. Signaling Interfaces

Two new Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Interface **Ext_Sig_Intf_RW** supports TLS, while interface **Int_Sig_Intf_RW** supports TCP.

1. From **Device Specific Settings** on the left-hand menu, select **Signaling Interface**. Click on the **Add** button to create Signaling Interface **Ext_Sig_Intf_RW**
   - Signaling IP = **192.168.96.234**
   - TLS Port = **5061**
   - Select TLS Profile **AvayaSBCServer** from the drop down menu
2. Repeat step 1 to create Signaling Interface **Int_Sig_Intf_RW**
   - Signaling IP = **192.168.128.21**
   - TCP Port = **5060**

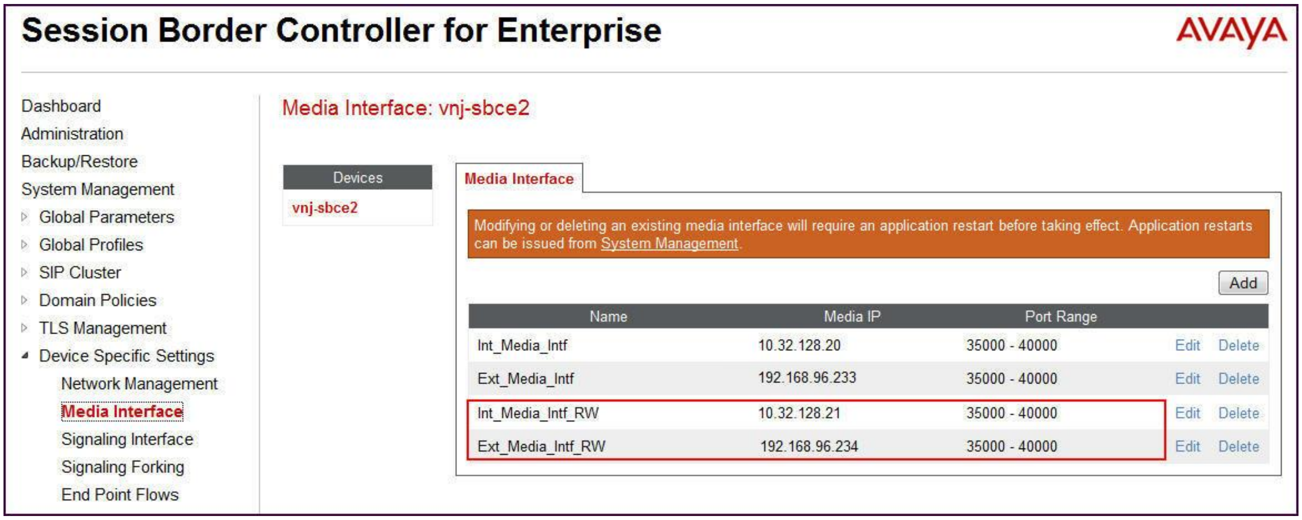


Signaling Interface **Int_Sig_Intf_RW** is used in the Remote Worker Server Flow (**Section 11.1.10.2**). Signaling Interface **Ext_Sig_Intf_RW** is used in the Remote Worker Subscriber Flow (**Section 11.1.10.1**), and in the Remote Worker Server Flow (**Section 11.1.10.2**).

11.1.3. Media Interfaces

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

1. From **Device Specific Settings** on the left-hand menu, select **Media Interface**. Click on the **Add** button to create Media Interface **Int_Media_Intf_RW** using the parameters shown below.
2. Repeat step **1** to create Media Interface **Ext_Media_Intf_RW**.

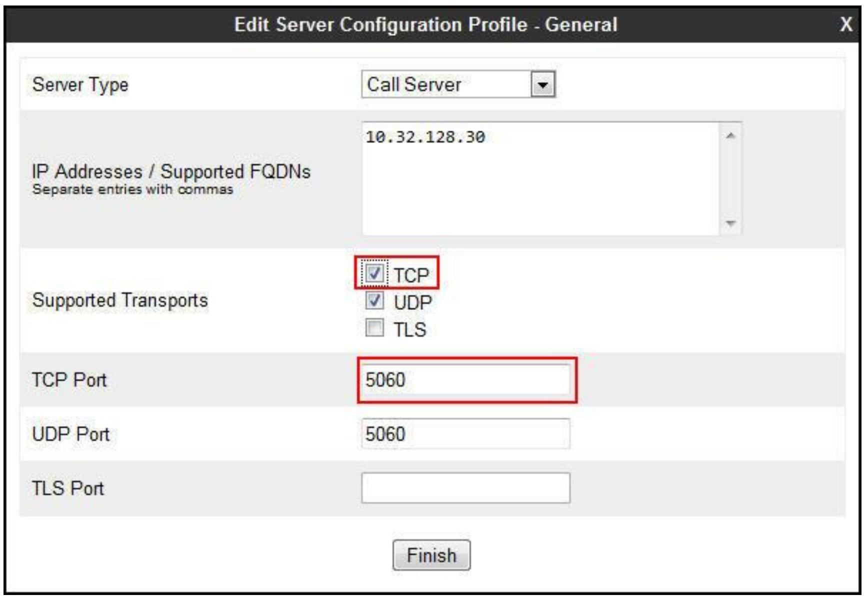


Media Interface **Int_Media_Intf_RW** is used in the Remote Worker Server Flow (**Section 11.1.10.2**). Media Interface **Ext_Media_Intf_RW** is used in the Remote Worker Subscriber Flow (**Section 11.1.10.1**).

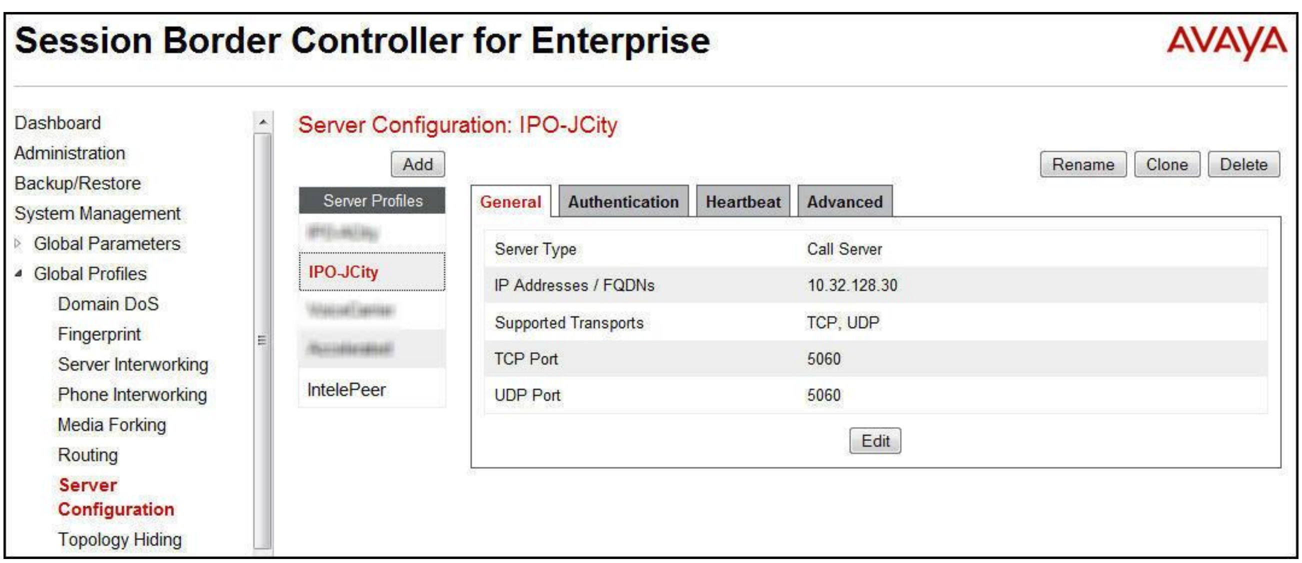
11.1.4. Server Profile for Avaya IP Office

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-JCity** Server Profile (see **Section 6.7.1**).

1. From **Global Profiles** on the left-hand menu, select **Server Configuration**
2. Select the existing **IPO-JCity** profile and click on **Edit**.
3. In the **Edit Server Configuration Profile - General** window, perform the following additional configurations:
   - **Supported Transports**: Check **TCP**
   - **TCP Port**: **5060**



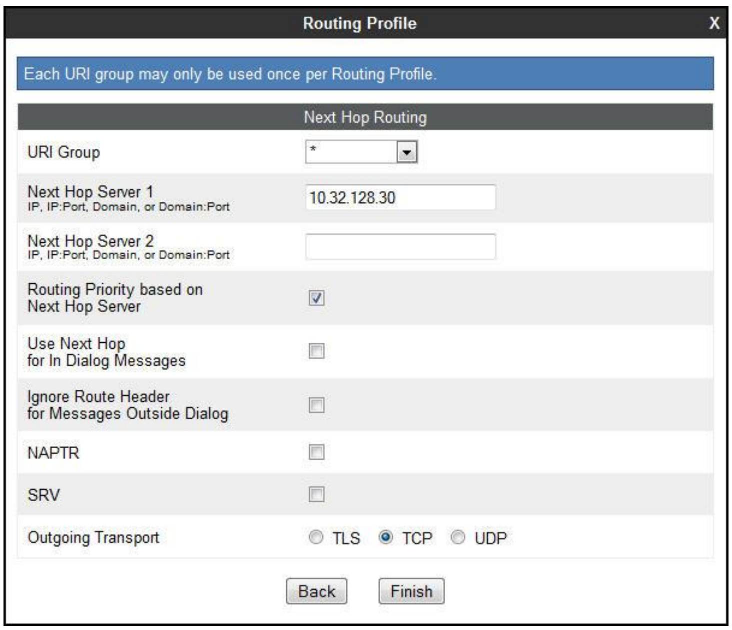
The **General** tab of the completed server profile is shown below.



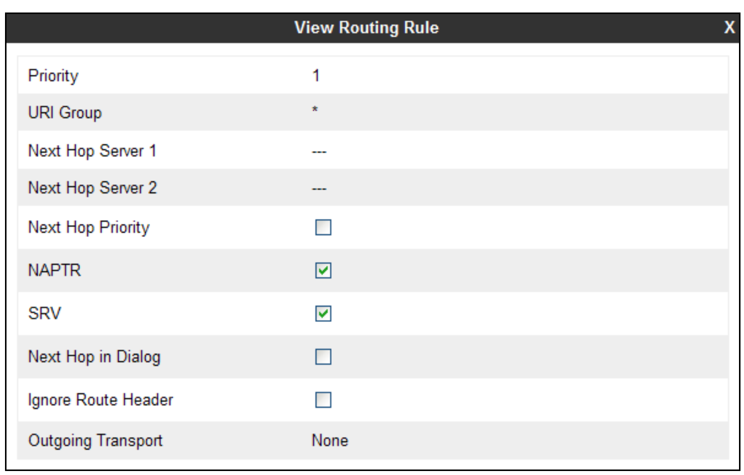
11.1.5. Routing Profiles

Two new Routing Profiles are required to support Remote Worker.

1. From **Global Profiles** on the left-hand menu, select **Routing**.
2. Select the **Add** button to create Routing Profile **To-IPO-JCity_RW**, select **Next** (not shown).
3. Enter the following:
   a. **URI Group** = * (default)
   b. **Next Hop Server 1** = **10.32.128.30** (IP Office LAN1 interface defined in **Section 5.2.1**)
   c. Verify **Routing Priority based on Next Hop Server** is checked.
   d. Select **TCP**.



4. Select the existing **default** Routing Profile and click on the **Clone** button, and name it **default_RW**, then select **Next** (not shown). Keep all the default values.



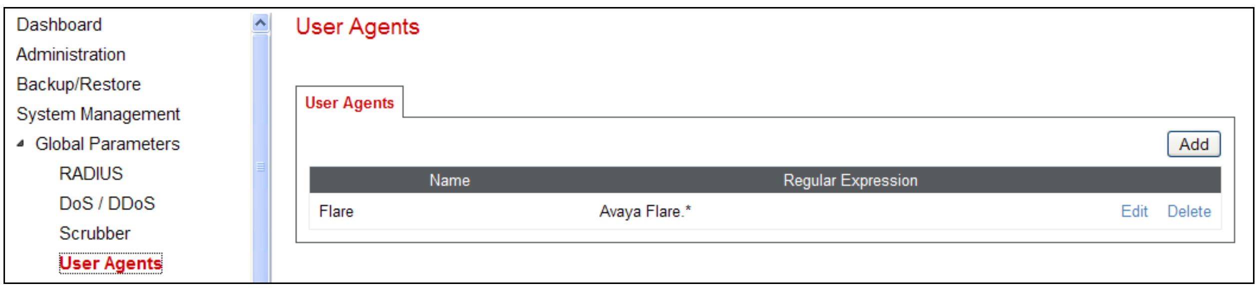
The Routing Profile **To-IPO-JCity_RW** is used in the Remote Worker Subscriber Flow (**Section 11.1.10.1**). The Routing Profile **default_RW** is used in the Remote Worker Server Flow (**Section 11.1.10.2**).

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 Flare® Experience for Windows SIP softphone was used, and its configuration is shown below.

1. From **Global Parameters** on the left-hand menu, select **User Agents**.
2. Select the **Add** button to create a new User Agent.
3. Enter the following:
    - **User Agent** = **Flare**
    - **Regular expression = Avaya Flare.***

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

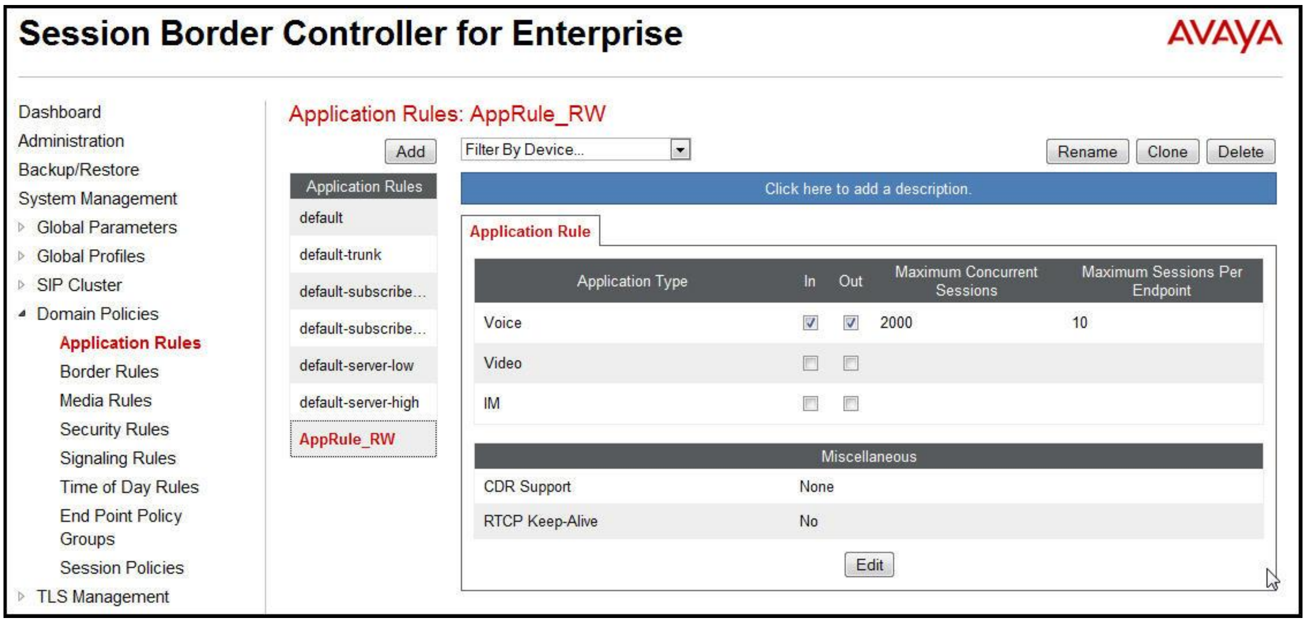


The **Flare** User Agent is defined in the Remote Worker Subscriber Flow (**Section 11.1.10.1**).

11.1.7. Application Rules

Application Rule **AppRule_RW** is created for Remote Worker.

1. From **Domain Policies** on the left-hand menu, select **Application Rules**.
2. Select **Add** button to create a new Application Rule.
3. Enter a name (e.g., **AppRule_RW**), and click on **Next** (not shown).
4. In the **Voice** field:
   - Check **In** and **Out**.
   - Enter an appropriate value in the **Maximum Concurrent Sessions** field, (e.g., **2000**).
   - Enter **10** in the **Maximum Session per Endpoint** field.
   - Leave the **CDR** field at **None** and the **RTCP Keep-Alive** field unchecked (**No)**.

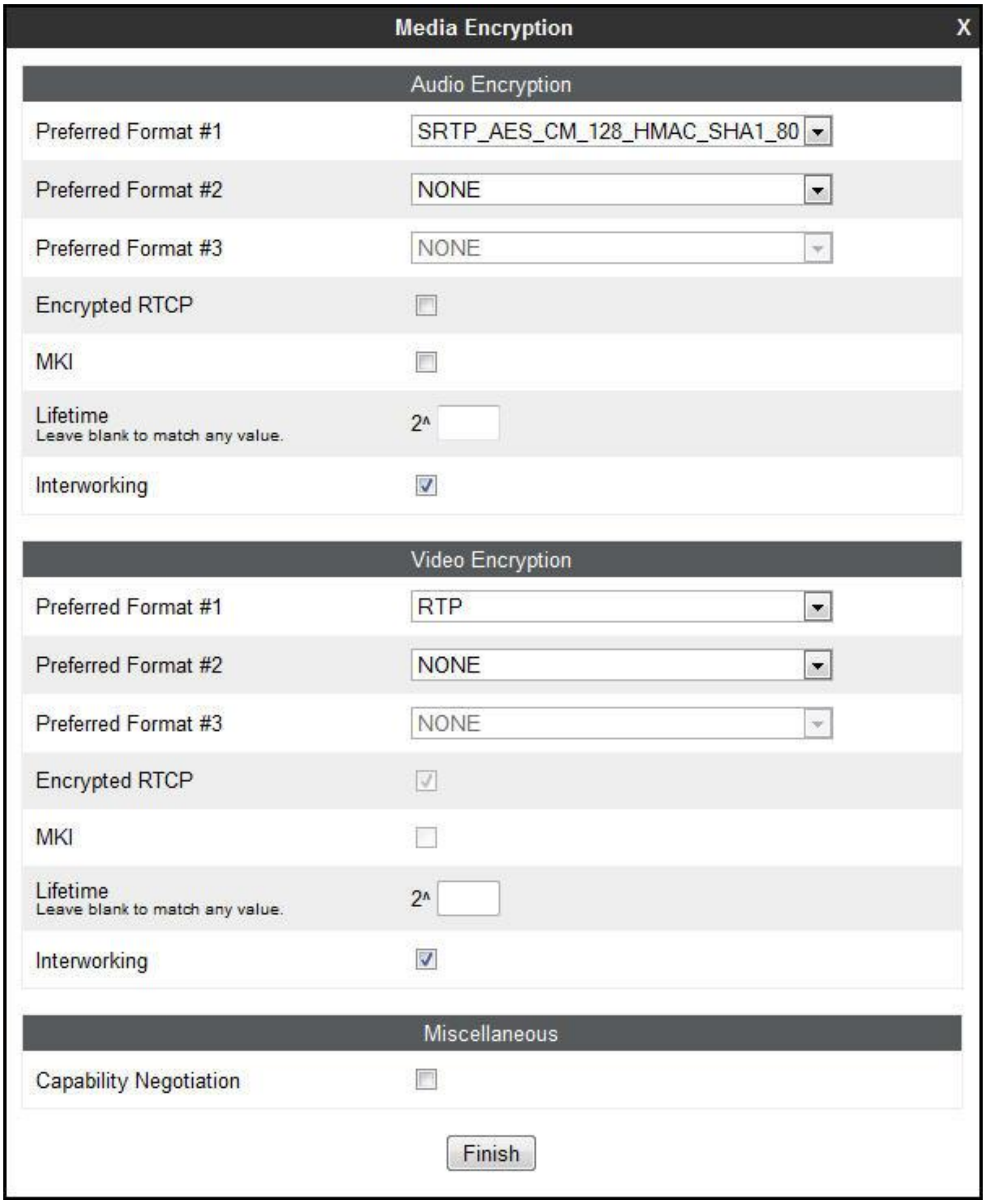


The rule **AppRule_RW** is assigned to the End Point Policy Groups (**Section 11.1.9**).

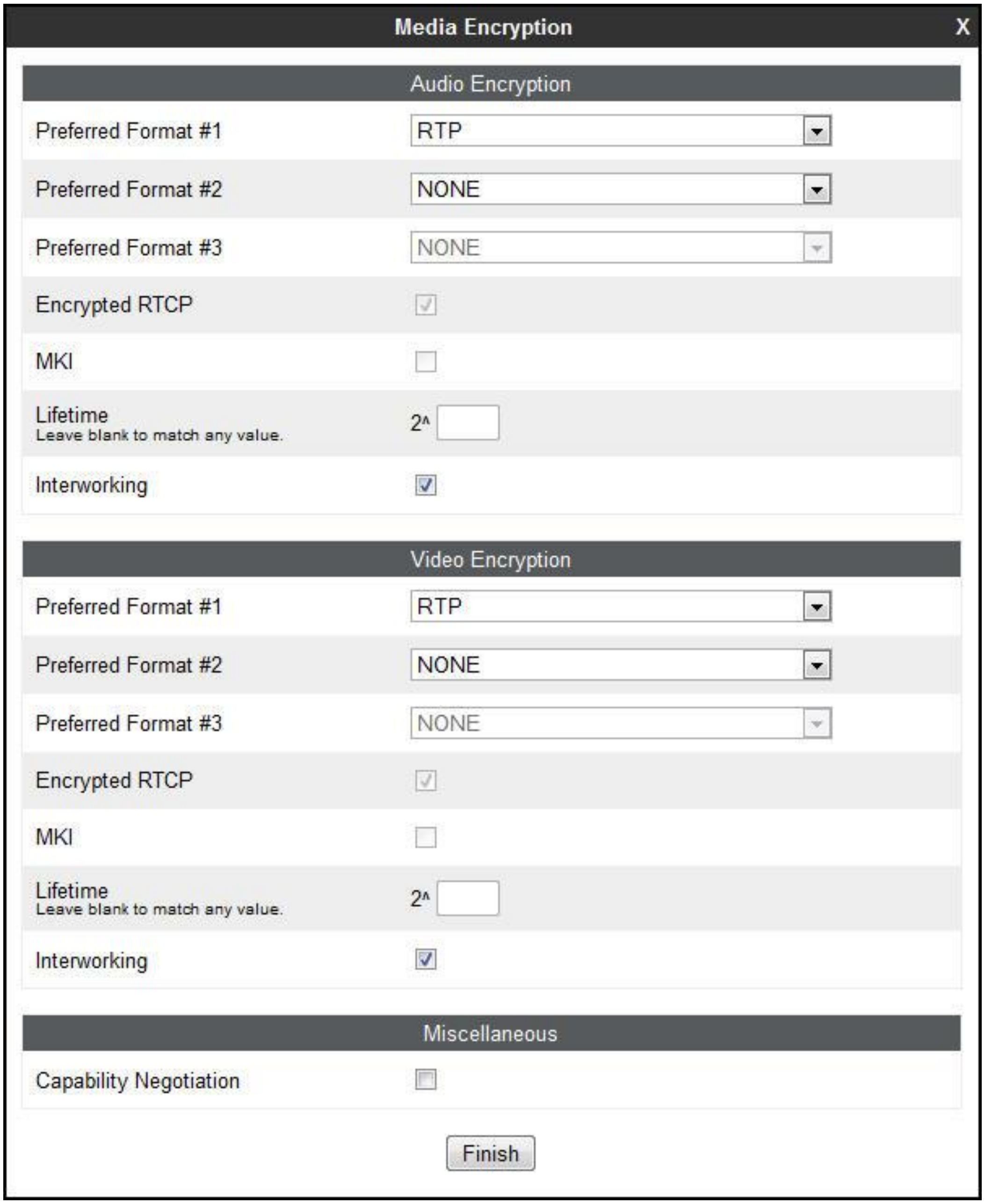
11.1.8. Media Rules

Two Media Rules are defined. Rule **SRTP_RW** is defined to enable the use of SRTP between the Avaya Flare® Experience for Windows Remote Worker (which also uses TLS for transport; see **Section 11.3.1**) and the Avaya SBCE. Rule **RTP_RW** is created for the Remote Worker connection from the Avaya SBCE to Avaya IP Office.

1. From **Domain Policies** on the left-hand menu, select **Media Rules**
2. To create the **SRTP_RW** rule, select the **default-low-med** and click on the **Clone** button.
3. Enter a name (e.g., **SRTP_RW**) and click **Finish** (not shown).
4. Edit the created Media Rule to populate the fields in the **Media Encryption** tab as shown below.



Create the Media Rule **RTP_RW** from cloning the **default-low-med** again. The screen below shows the rule’s Media encryption tab.

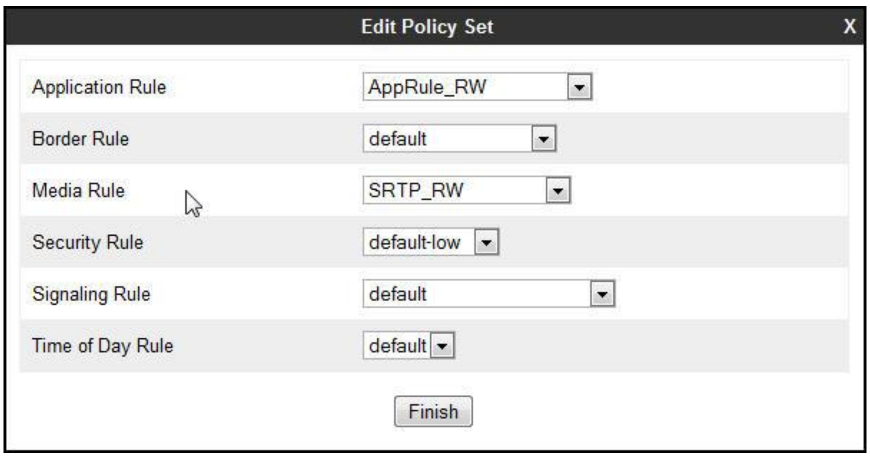


Media Rule **SRTP_RW** is assigned to the End Point Policy Group **SRTP-Policy_RW** (**Section 11.1.9**). Media Rule **RTP_RW** is assigned to the End Point Policy Group **RTP-Policy_RW** (**Section 11.1.9**).

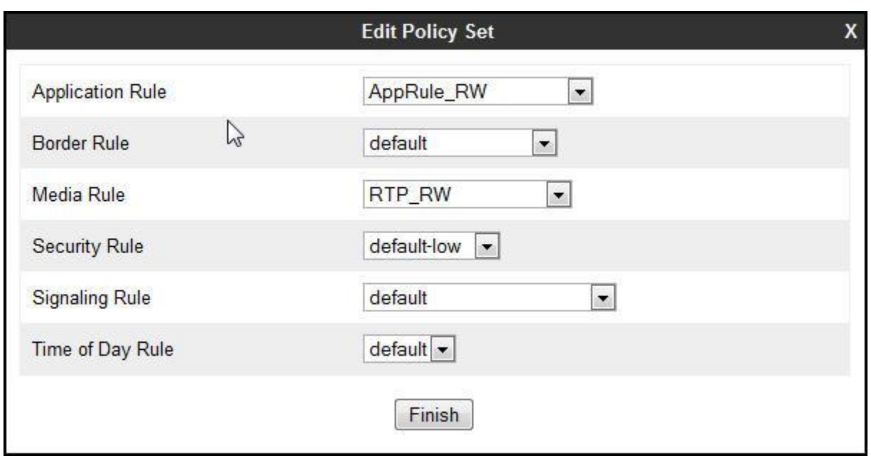
11.1.9. End Point Policy Groups

Two new End Point Policy Groups are defined for Remote Worker. Group **SRTP-Policy_RW** is defined for the SRTP connection and **RTP-Policy_RW** is defined for the RTP connection.

1. From **Domain Policies** on the left-hand menu, select **End Point Policy**.
2. Select **Add** button to create a new End Point Policy Group.
3. Enter a name (e.g., **SRTP-Policy_RW**), and click on **Next** (not shown).
4. The **Policy Group** window will open. Enter the following:
    - **Application Rule** = **AppRule_RW** (**Section 11.1.7**)
    - **Border Rule** = **default**
    - **Media Rule** = **SRTP_RW** (**Section 11.1.8**)
    - **Security Rule** = **default-low**
    - **Signaling Rule** = **default**
    - **Time of Day Rule** = **default**



5. End Point Policy Group **RTP-Policy_RW** is similarly created with Media Rule **RTP_RW** (**Section 11.1.8**):



End Point Policy Group **SRTP-Policy_RW** is used in the Subscriber Flow (**Section 11.1.10.1**). End Point Policy Group **RTP-Policy_RW** is used in the Server Flow (**Section 11.1.10.2**).

11.1.10. End Point Flows

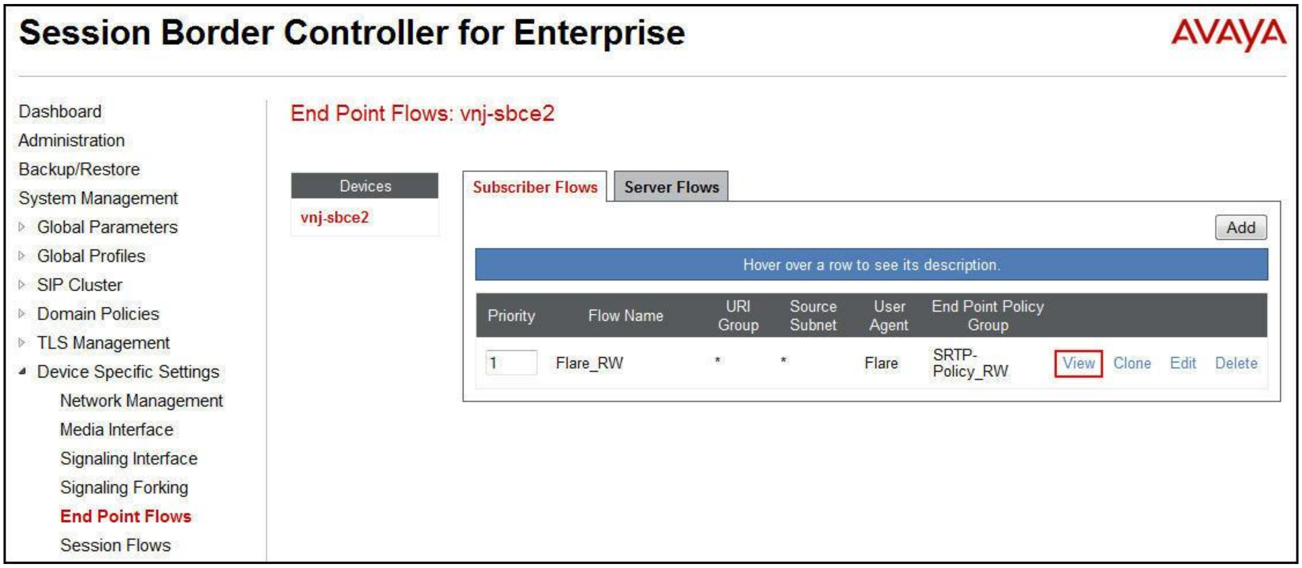
A Subscriber Flow and a Server Flow are created for Remote Worker.

11.1.10.1 Subscriber Flow

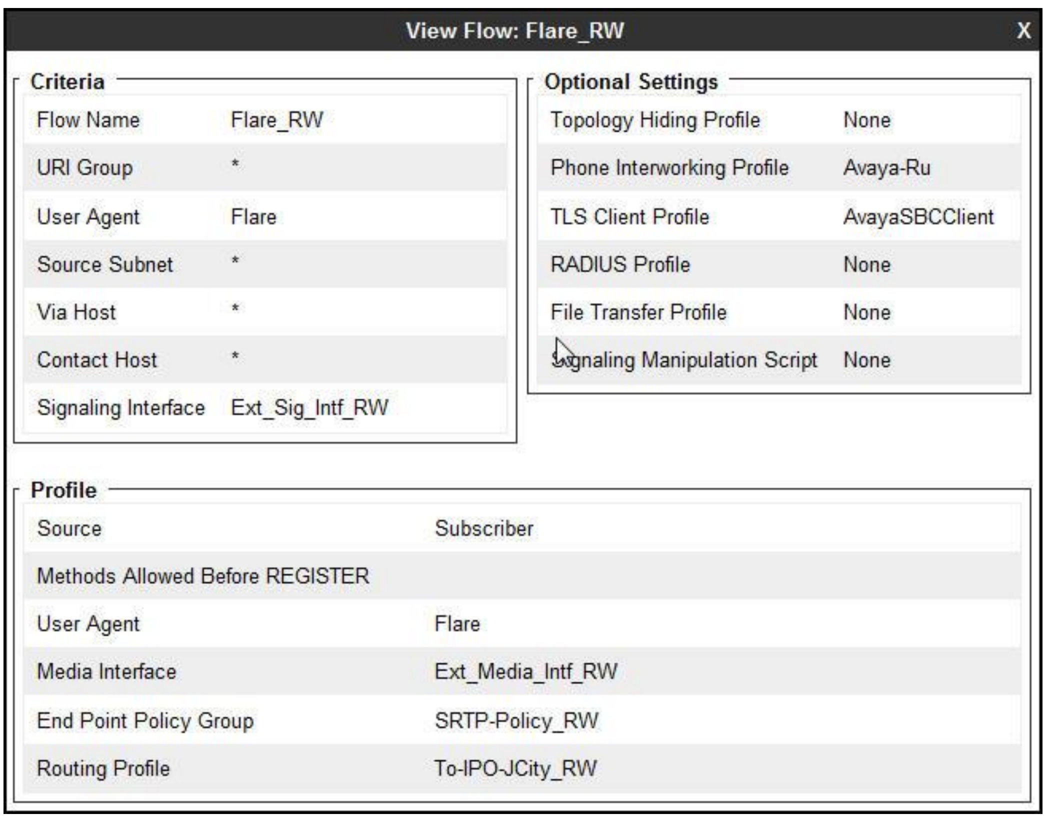
A **Subscriber Flow** is defined as follows:

1. From **Device Specific Settings** on the left-hand menu, select **End Point Flows**. Click on **Add** and the **Criteria** window will open (not shown).
    - Enter a name (e.g., **Flare_RW**)
    - **URI Group** = ***** (default)
    - **User Agent** = **Flare**
    - **Source Subnet** = ***** (default)
    - **Via Host** = ***** (default)
    - **Contact Host** = ***** (default)
    - **Signaling Interface** = **Ext_Sig_Intf_RW** (**Section 11.1.2**)
2. Click on **Next** (not shown) and the **Profile** window will open (not shown).
    - **Source** = **Subscriber**
    - **Methods Allowed Before REGISTER**: Leave as default
    - **Media Interface** = **Ext_Media_Intf_RW** (**Section 11.1.3**)
    - **End Point Policy Group = SRTP-Policy_RW** (**Section 11.1.9**).
    - **SIP Cluster Flow**: unchecked
    - **Routing Profile = To-IPO-JCity_RW** (**Section 11.1.5**)
    - **Topology Hiding Profile** = **None**
    - **Phone Interworking Profile** = **Avaya-Ru**
    - **TLS Client Profile** = **AvayaSBCClient**
    - **Radius Profile = None**
    - **File Transfer Profile** = **None**
    - **Signaling Manipulation Script** = **None**

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



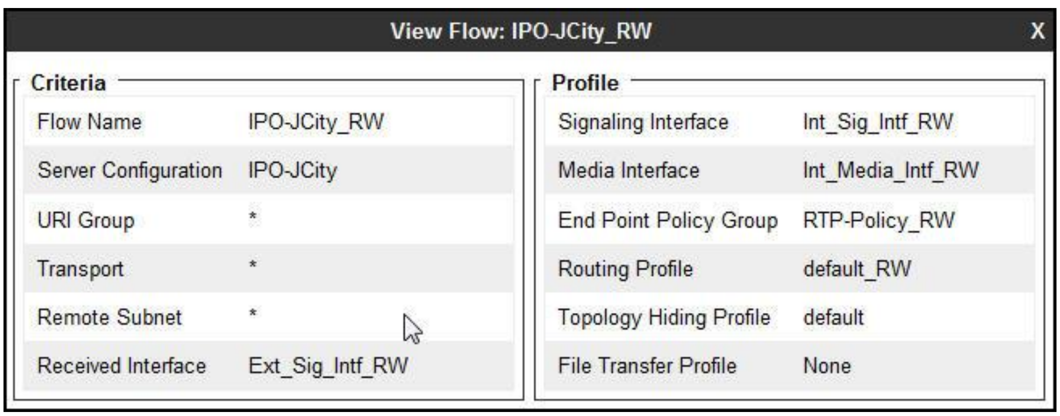
Clicking on the highlighted View link brings up the following **View Flow** window:



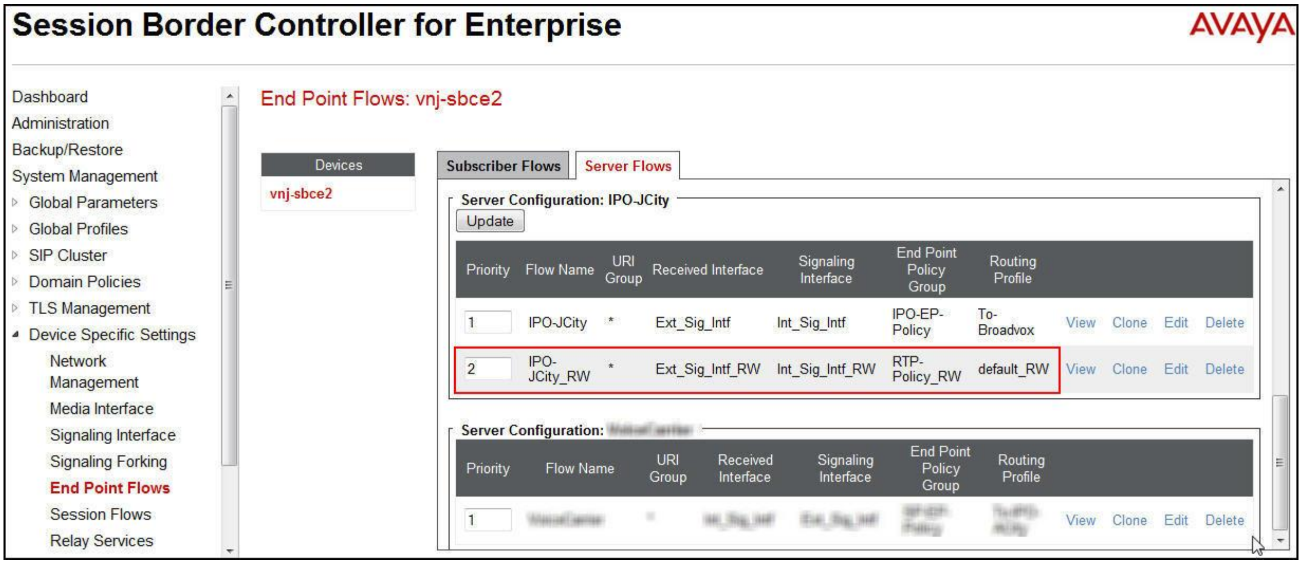
11.1.10.2 Server Flow

The following section shows the new **Server Flow** settings for Remote Worker.

1. From **Device Specific Settings** on the left-hand menu, select **End Point Flows**, then the **Server Flows** tab
2. Select **Add** (not shown), and enter the following:
    - **Name = IPO-JCity_RW**
    - **Server Configuration** = **IPO-JCity** (**Section 6.7.1**)
    - **URI Group** = ***** (default)
    - **Transport** = ***** (default)
    - **Remote Subnet** = ***** (default)
    - **Received Interface** = **Ext_Sig_Intf_RW** (**Section 11.1.2**)
    - **Signaling Interface** = **Int_Sig_Intf_RW** (**Section 11.1.2**)
    - **Media Interface** = **Int_Media_Intf_RW** (**Section 11.1.3**)
    - **End Point Policy Group** = **RTP-Policy_RW** (**Section 11.1.9**)
    - **Routing Profile** = **default_RW (Section 11.1.5)**
    - **Topology Hiding Profile** = **default**
    - **File Transfer Profile** = **None** (default)



If this Remote Worker server flow is listed ahead of the flow for SIP Trunking (**IPO-JCity** as created in **Section 6.14.1**), 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.



11.2. Remote Worker Endpoint Configuration on Avaya IP Office

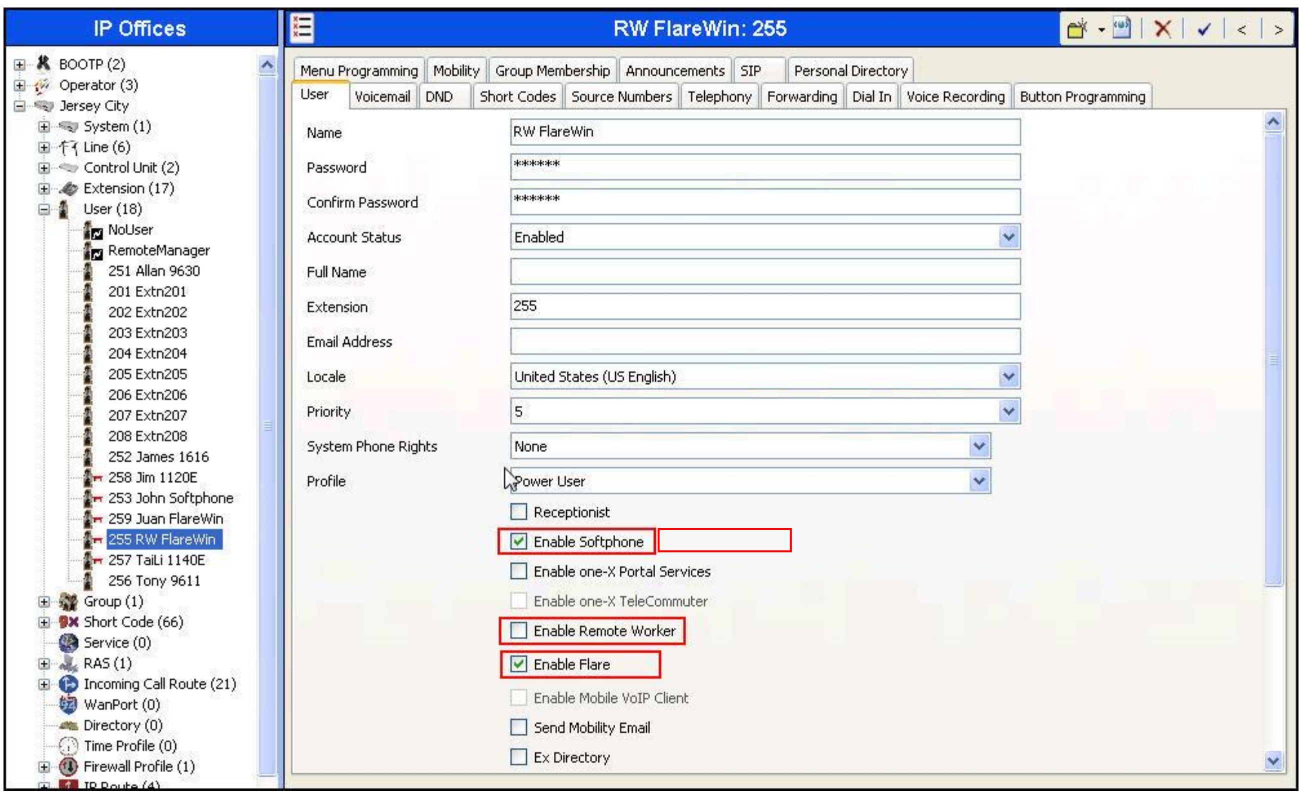
The Remote Worker Avaya Flare® Experience for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration.

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 Flare® Experience for Windows.

The Remote Worker user provisioned is shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Flare® Experience for Windows, the **Enable Softphone** and **Enable Flare** 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.



The **SIP** tab for the Remote User is configured the same way as with local IP Office user (see **Section 5.6**).

11.2.2. Incoming Call Route

Follow the same procedures described in **Section 5.7** for defining an Incoming Call Route to the Remote Worker.

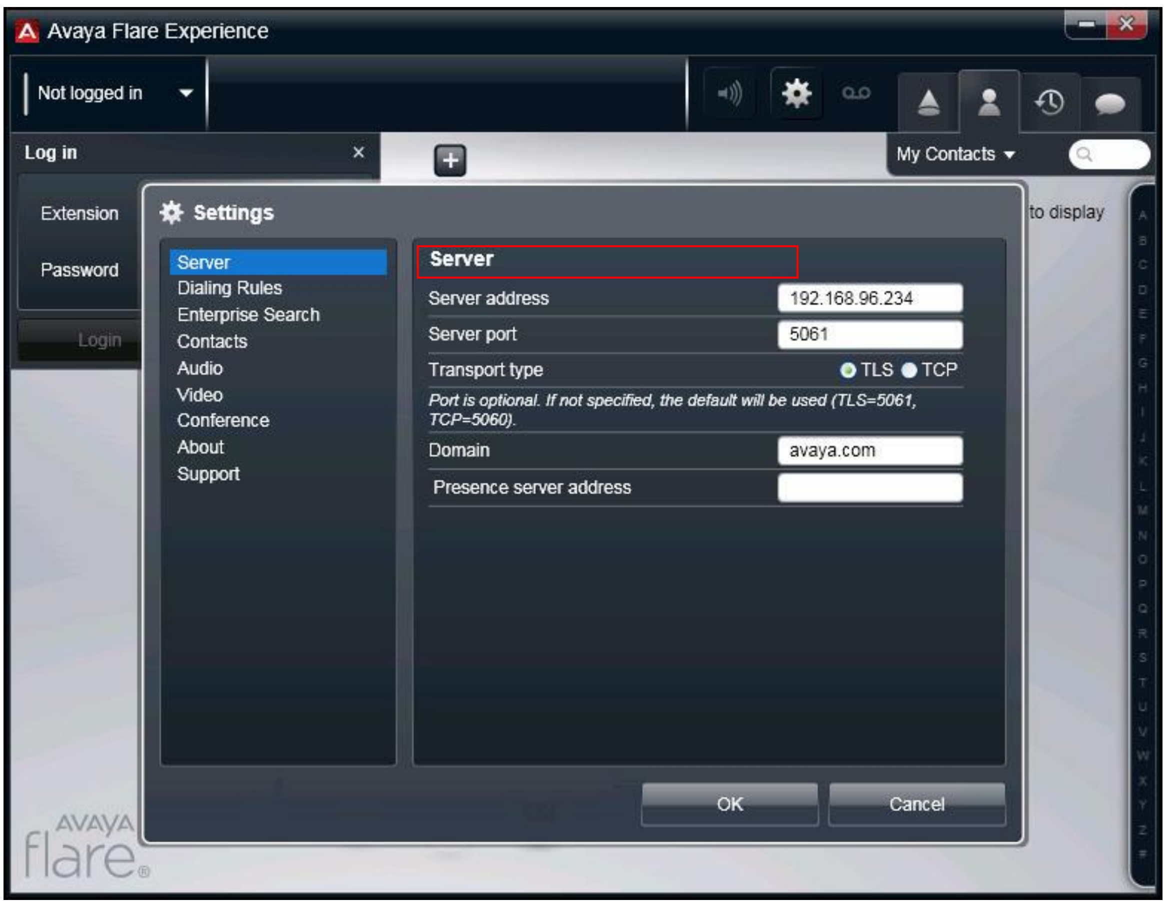
11.3. Remote Worker Avaya Flare® Experience for Windows Configuration

The following screens illustrate Avaya Flare® Experience for Windows administration settings for Remote Worker as used in the reference configuration.

11.3.1. Settings - Server Screen

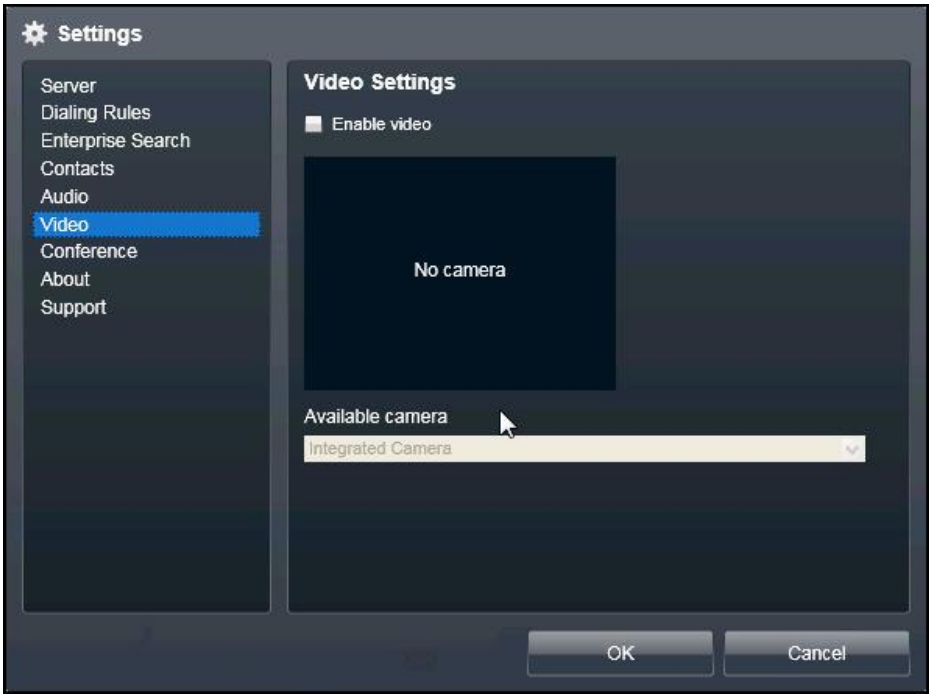
After opening the Avaya Flare® Experience for Windows application, select the Settings icon, select **Server** from the Settings menu, and enter the following:

- **Server address** = **192.168.96.234** (the IP address of Remote Worker outside interface B1on Avaya SBCE (see **Section 11.1.1**).
- **Server port = 5061** (note that the **Transport type** will automatically change to TLS).
- **Domain =** IP Office SIP Registrar domain name (**avaya.com** was used for the compliance test, see the VoIP tab screenshot in **Section 5.2.1**).



11.3.2. Settings - Video Screen

Select **Video** from the Settings menu, *unselect* the **Enable Video** option. In Release 1.1 of Avaya Flare® Experience for Windows, only audio calls are supported with SRTP media encryption (see **Section 11.1.8**).



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.