



Application Notes for Configuring Bell Canada SIP Trunking with Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.1

Abstract

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

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

Bell Canada 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.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Bell Canada and an Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of an Avaya IP Office 500v2 Release 9.0, Avaya micro Session Border Controller for Enterprise Release 6.2 (Avaya SBCE), Avaya Voicemail Pro, Avaya IP Office Softphone, and Avaya H.323, digital, and analog endpoints.

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

The Bell Canada SIP Trunking service uses Digest Authentication for outbound calls from the enterprise, using challenge-response authentication for each call to the Bell Canada network based on a configured user name and password (provided by Bell Canada and configured in Avaya SBCE). This call authentication scheme as specified in SIP RFC 3261 provides security and integrity protection for SIP signaling.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office to connect to Bell Canada SIP Trunking service via Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**.

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

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from the Avaya IP Office Softphone.

- Inbound and outbound long holding time call stability.
- Various call types including: local, long distance, international, outbound toll-free, operator service and directory assistance.
- Codec G.711MU and G.729A.
- Caller number/ID presentation.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- Telephony features such as hold and resume, transfer, and conference.
- Use of SIP REFER for call transfer to PSTN.
- Fax G.711 Pass Through mode.
- Off-net call forwarding.
- Twinning to mobile phones on inbound calls.

2.2. Test Results

Bell Canada SIP Trunking passed compliance testing.

Items not supported or not tested included the following:

- Inbound toll-free and outbound emergency calls (911) are supported but were not tested as part of the compliance test.
- T.38 Fax is not support.

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

- **OPTIONS from IP Office** – If the periodicity of sending OPTIONS to monitor the SIP trunk connectivity is configured on Avaya IP Office to be larger than the periodicity of OPTIONS from Bell Canada, IP Office would effectively cease to send OPTIONS to Bell Canada. This is expected behavior on Avaya IP Office since it resets the timer for sending OPTIONS starting from the most recently received OPTIONS from the network.
- **Call Display on PSTN Phone** – Call display was not properly updated on PSTN phone involved in a call transfer. After the call transfer was completed, the PSTN phone did not display the actual connected party but instead showed the party that initiated the transfer. SIP signaling trace showed that the enterprise IP Office did not send an UPDATE message to the network to update the call display of the PSTN phone in call transfer. However, it does not affect the end user.
- **Blind Transfer using REFER** – Bell network sent “401 unauthorized” message, at the end of the call transfer sequence after Avaya IP Office sent CANCEL, to second call leg on a blind transfer call. There is no user impact. Notifying Bell’s team on this issue.
- **Call Display on PSTN Phone on PSTN Hold and Resume** – Call display was not properly updated on PSTN phone involved in PSTN Hold and Resume operation. After the inbound call from PSTN to Avaya IP Office was hold on PSTN phone, when the call was resumed on the PSTN phone, the PSTN phone displayed trunk number instead of the calling party ID. No user impact.

2.3. Support

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

For technical support on Bell Canada SIP Trunking, contact Bell Canada at http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page.

3. Reference Configuration

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

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

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

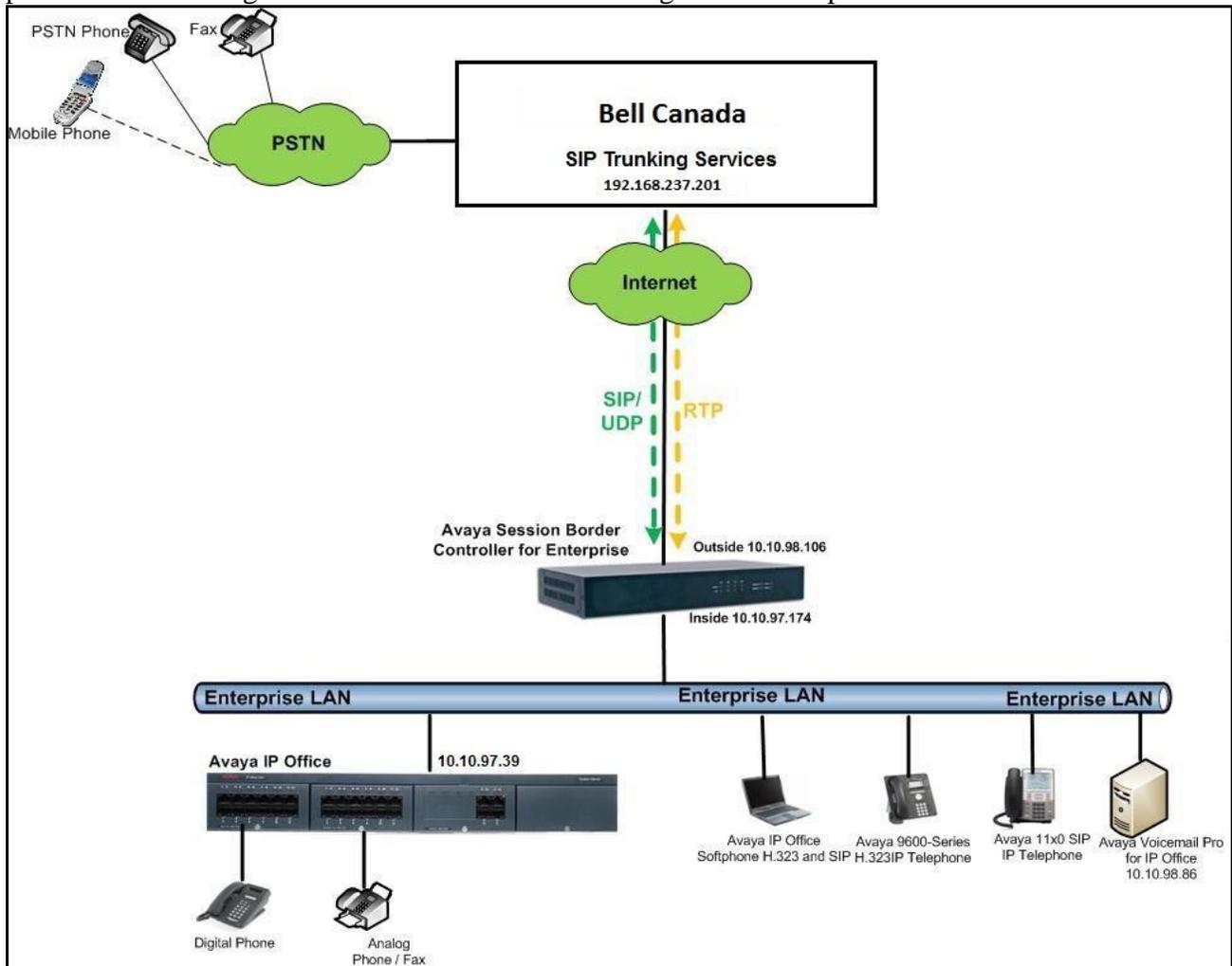


Figure 1: Test Configuration for Avaya IP Office with Bell Canada SIP Trunking Service

For the purposes of the compliance test, Avaya IP Office users dialed a short code of 9 + N digits to send digits across the SIP trunk to Bell Canada. The short code of 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to Bell Canada. For calls within the North American Numbering Plan (NANP), the user would dial 11 (1 + 10) digits. Thus for these NANP calls, Avaya IP Office would send 11 digits in the Request URI and the To field of an outbound SIP INVITE message. It was configured to send 10 digits in the From field. For inbound calls, Bell Canada SIP Trunking sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

Bell Canada uses the phone number in the From header of a SIP INVITE message to authenticate the calling party. Thus, a call will be rejected by the network unless the From header contains a number known to Bell Canada. This is especially important for calls inbound from the PSTN which are redirected back to the PSTN by call forwarding or twinning. For call forwarding, Avaya IP Office sends the number of the forwarding phone in the From header. This is a number known to Bell Canada. As a result, the call display on the destination phone shows the forwarding party not the original caller. For twinning, this behavior can be slightly altered through configuration. See **Sections 5.3 and 5.4** for details.

Note that the calling party authentication using the phone number by Bell Canada, as mentioned above, is in addition to the Digest Authentication by Bell Canada during call setup SIP signaling exchanges using a user name and password as configured in Avaya IP Office for all calls from the enterprise to Bell Canada.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	Release
Avaya IP Office 500v2	9.0.0.829
Avaya IP Office Manager	9.0.0.829
Avaya Voicemail Pro for IP Office	9.0.0.829
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2 (6.2.0 Q30)
Avaya 11x0 IP Telephone (SIP)	SIP11x0e04.03.12.00
Avaya 9630G IP Telephone (H.323)	Avaya one-X® Deskphone Edition S3.2
Avaya IP Office Softphone	3.2.3.20 64770
Avaya Digital Telephone (9508)	N/A
Avaya Symphony 2000 Analog Telephone	N/A
Bell Canada SIP Trunking Service Components	
Component	Release
Acme Packet Net-Net 4250 SBC	Firmware SC6.2.0 MR-4 Patch 1 (Build 718)
Broadsoft SoftSwitch	Rel18
Legacy Nortel CS2K Media Gateway	SN10 PVG/IW-SPM

5. Configure IP Office

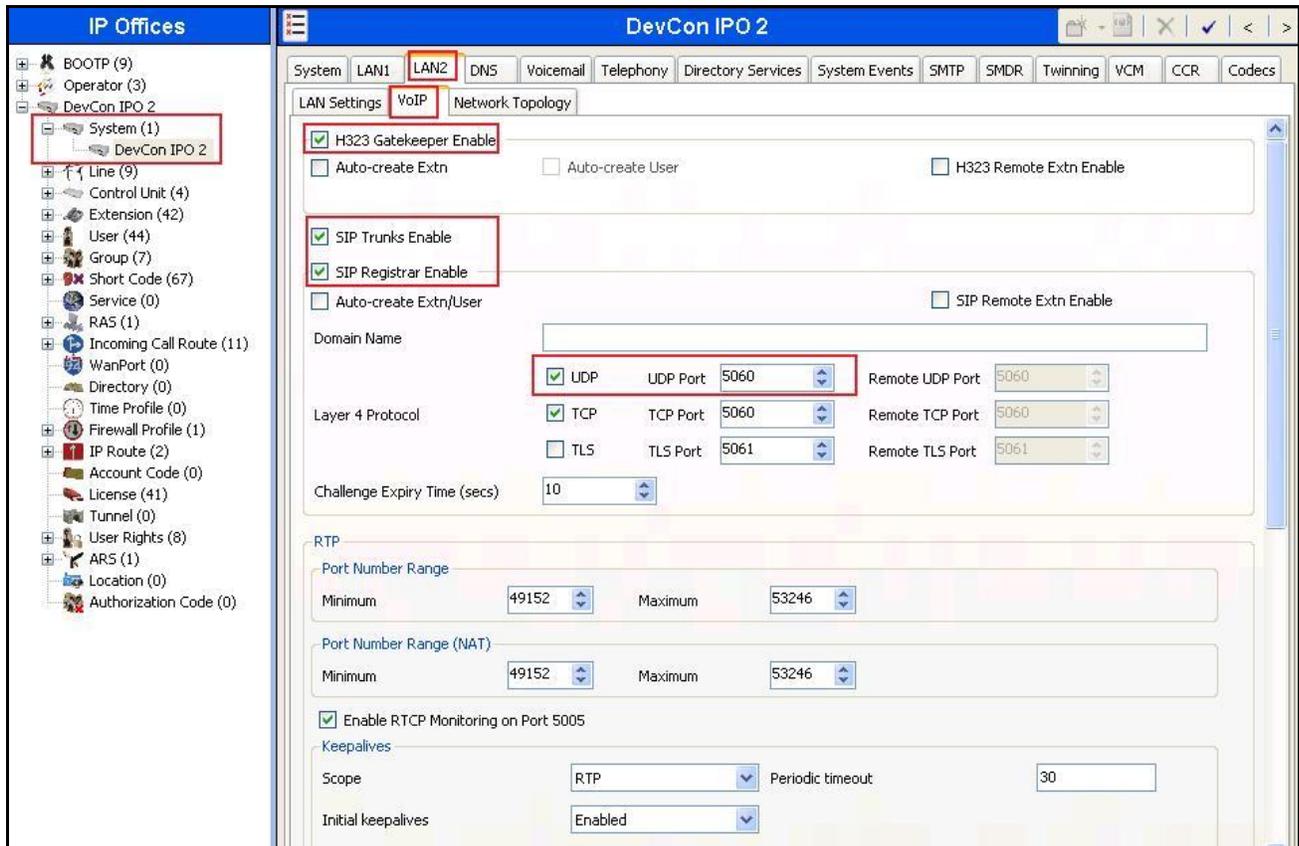
This section describes the Avaya IP Office configuration to support connectivity to Bell Canada SIP Trunking service through Avaya SBCE. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs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

5.1. LAN Settings

In the sample configuration, the **DevCon IPO2** was used as the system name and the WAN port was used to connect the Avaya IP Office to the public network. The LAN1 settings correspond to the WAN port on the Avaya IP Office. To access the LAN settings, first navigate to **System (1) → DevCon IPO2** in the Navigation and Group Panes and then navigate to the **LAN2 → LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office WAN port. Set the **IP Mask** field to the mask used on the public network. All other parameters should be set according to customer requirements.

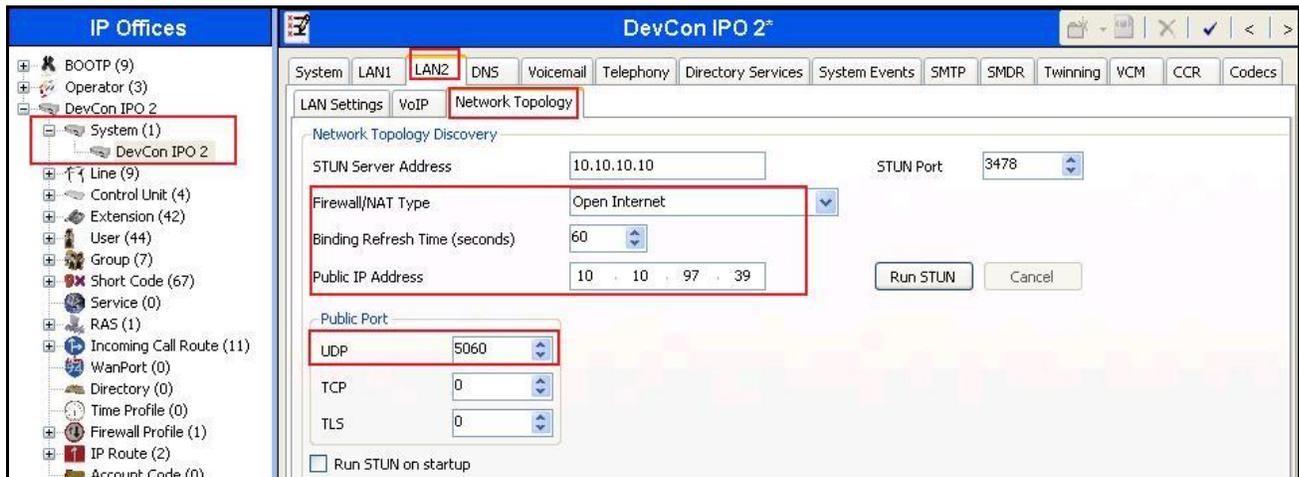
The screenshot displays the Avaya IP Office Manager configuration interface for a system named "DevCon IPO 2". The interface is divided into three main panes: a navigation pane on the left, a group pane in the center, and a details pane on the right. The navigation pane shows a tree structure with "System (1)" expanded to "DevCon IPO 2". The group pane shows "LAN2" selected. The details pane shows the "LAN Settings" tab for "LAN2". The "IP Address" field is set to "10 . 10 . 97 . 39" and the "IP Mask" field is set to "255 . 255 . 255 . 240". Other fields include "Primary Trans. IP Address" (0 . 0 . 0 . 0), "Firewall Profile" (<None>), "RIP Mode" (None), "Enable NAT" (unchecked), and "Number Of DHCP IP Addresses" (1). The "DHCP Mode" section has "Server", "Client", and "Dialin" unselected, and "Disabled" selected. An "Advanced" button is visible at the bottom right.

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



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

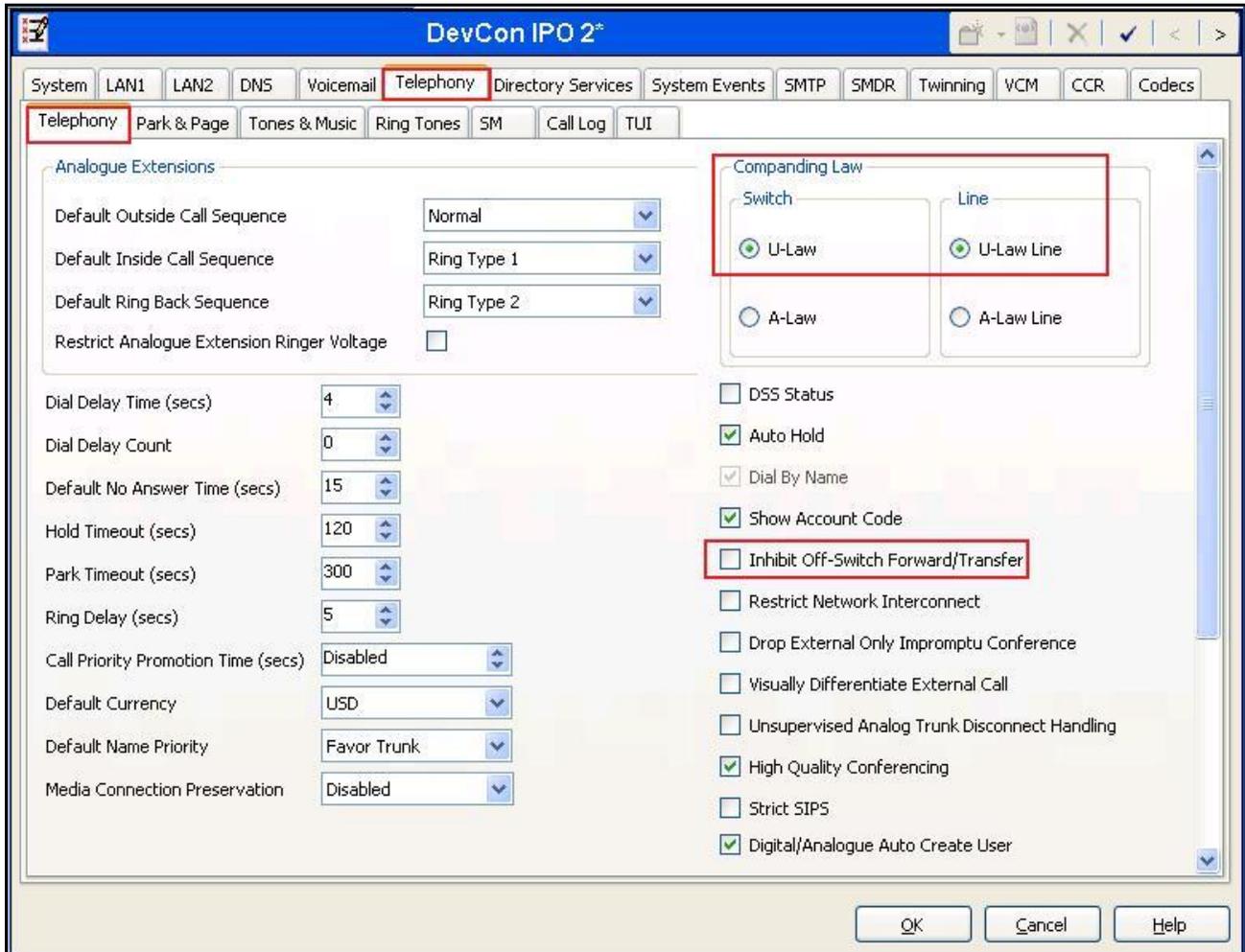
- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test as shown in **Figure 1**, so the parameter was set to **Open Internet**. With this configuration, STUN will not be used.
- Set **Binding Refresh Time (seconds)** to **60**. This value is used as one input to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. See **Section 5.10** for complete details.
- Set **Public IP Address** to the IP address of the Avaya IP Office WAN port. **Public Port** is set to **5060**.
- All other parameters should be set according to customer requirements.



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

5.2. System Telephony Settings

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



5.3. Twinning Calling Party Settings

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

For the compliance testing, the **Send original calling party information for Mobile Twinning** as shown below was unchecked. This setting allows **Send Caller ID** parameter that was set to **P Asserted ID** in [Section 4](#) to be used. IP Office will send the following in the “From” header:

- On calls from an internal extension to a twinned phone, IP Office sends Calling Party Number of the originating extension.
- On calls from the PSTN to a twinned phone, IP Office sends Calling Party Number of the originating PSTN party.



5.4. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Bell Canada 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**.

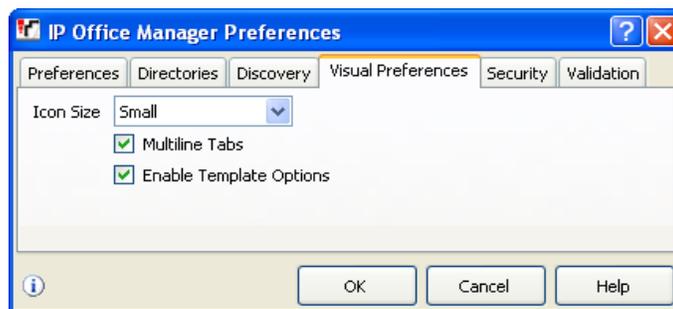
Also, the following SIP Line settings are not supported on Basic Edition:

- 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**.

5.4.1. Create SIP line from Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **CA_Bell Canada_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.
2. Verify that template options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the Visual Preferences tab. Verify that the box is checked next to **Enable Template Options**. Click **OK**.



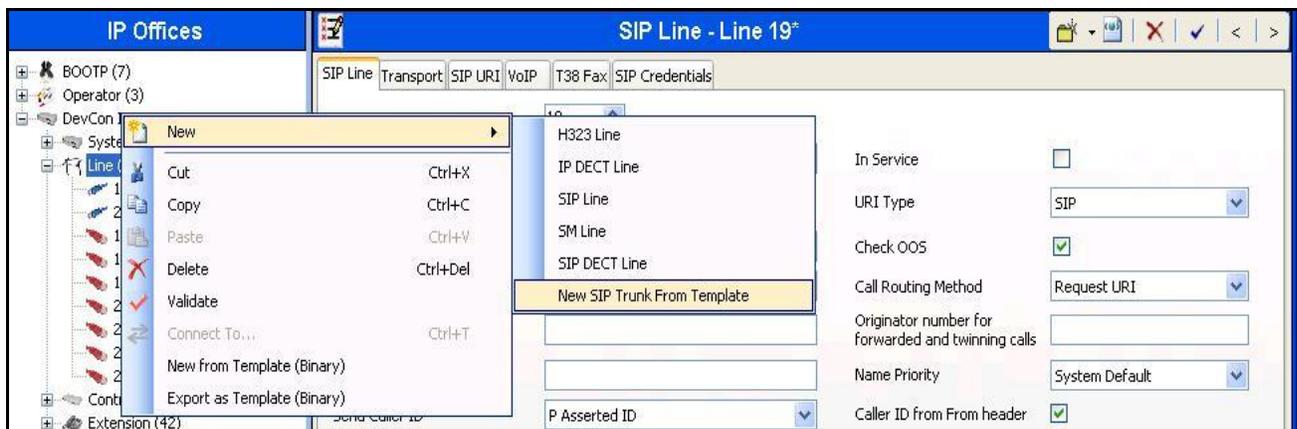
3. Import the template into IP Office Manager.

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 **Canada** from the **Country** pull-down menu and select **Bell Canada** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**CA_Bell Canada_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



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

5.4.2. Create SIP Line Manually

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

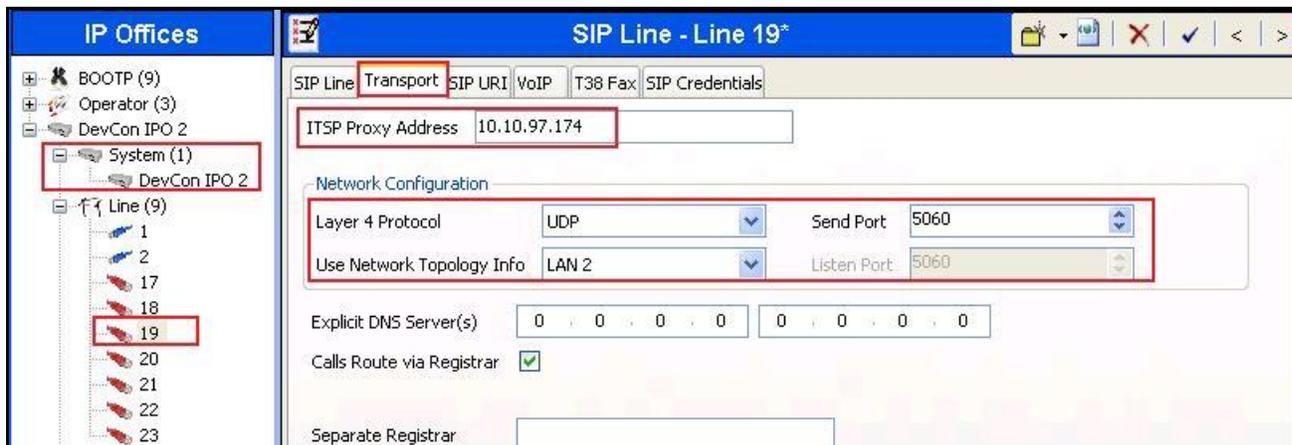
- Set **ITSP Domain Name** to the enterprise domain so that IP Office uses this domain as the host portion of SIP URI in SIP headers such as the From header.
- Set **Send Caller ID** to **P Asserted ID**. For the compliance test, this parameter was ignored since **Send original calling party information for Mobile Twinning** is optioned in **Section 5.3**.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Default values may be used for all other parameters.

The area of the screen entitled **REFER Support** is used to enable/disable SIP REFER for call transfers. The default values of “Auto” for **Incoming** and **Outgoing** effectively disable use of SIP REFER. To enable SIP REFER, select “**Always**” from the drop-down menu for **Incoming** and **Outgoing**. In the compliance test, both configurations were successfully tested to transfer a call between a PSTN phone and an enterprise phone to a second PSTN phone.

The screenshot displays the configuration interface for a SIP Line in IP Office. The left pane shows the navigation tree with 'Line (9)' selected. The main pane shows the configuration for 'SIP Line - Line 19'. The configuration fields are as follows:

Field	Value
Line Number	19
ITSP Domain Name	avayalab.com
Prefix	
National Prefix	
Country Code	
International Prefix	
Send Caller ID	P Asserted ID
Association Method	By Source IP address
In Service	<input checked="" type="checkbox"/>
URI Type	SIP
Check OOS	<input checked="" type="checkbox"/>
Call Routing Method	Request URI
Originator number for forwarded and twinning calls	
Name Priority	System Default
Caller ID from From header	<input checked="" type="checkbox"/>
Send From In Clear	<input type="checkbox"/>
User-Agent and Server Headers	
Service Busy Response	503 - Service Unavailable
Action on CAC Location Limit	Allow Voicemail
REFER Support	<input checked="" type="checkbox"/>
Incoming	Always
Outgoing	Always
Method for Session Refresh	Update
Session Timer (seconds)	On Demand
Media Connection Preservation	Disabled

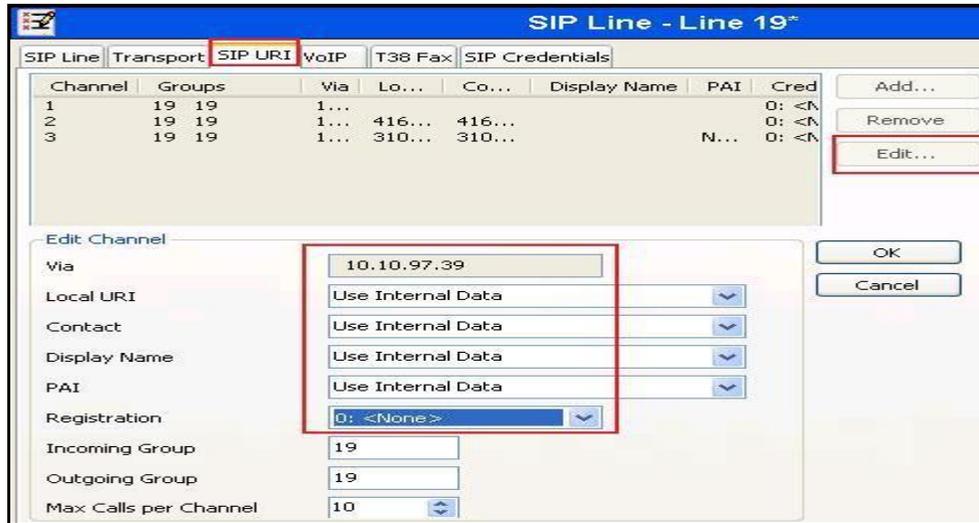
Select the **Transport** tab. The **ITSP Proxy Address** is set to internal IP Address of Avaya SBCE. As shown in **Figure 1**, this IP Address is **10.10.97.174**. In the **Network Configuration** area, **UDP** is selected as the **Layer 4 Protocol**, and the **Send Port** is set to the port number of Avaya SBCE. The **Use Network Topology Info** parameter is set to **LAN 2**. This associates the SIP Line with the parameters in the **System → LAN2 → Network Topology** tab. Other parameters retain default values in the screen below.



A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, click the **Add** button and then **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the example screen below, a previously configured entry is edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Internal Data**. This setting allows calls on this line which SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.6**.
- Set **PAI** to **Internal Data**. With this setting IP Office will populate the SIP P-Asserted-Identity header on outgoing calls with the data set in the **SIP** tab of the call initiating **User** as shown in **Section 5.6**.
- For **Registration**, select the account credentials previously configured on the line's **SIP Credentials** tab.
- Associate this line with an incoming line group in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. For the compliance test, a new incoming and outgoing group **19** was defined that only contains this line (line 19).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

SIP URI entry for Channel 1



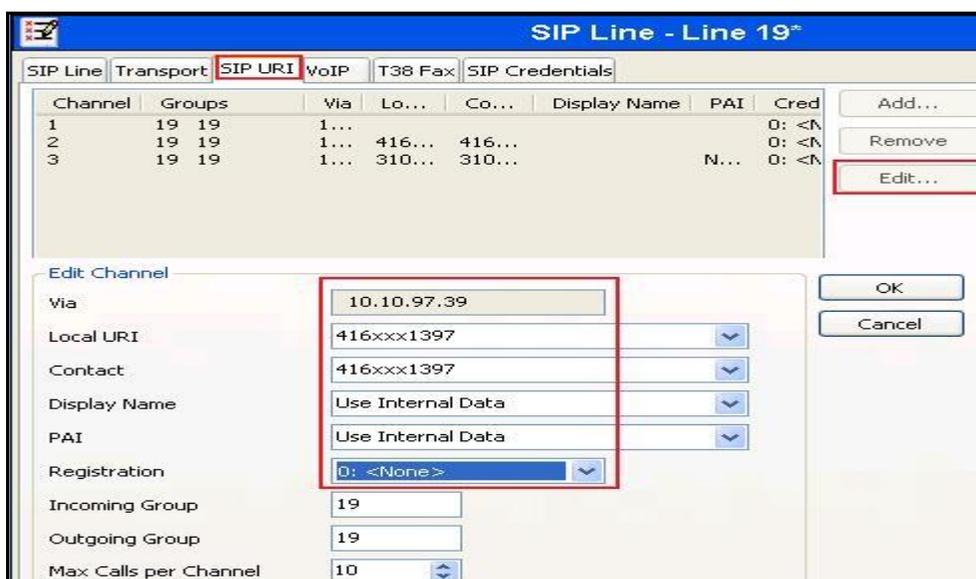
SIP URI entry **Channel 2** was similarly created for incoming calls appropriately to pre-define DID numbers **416xxx1397** to access to Feature Name Extension 00 (FNE00. The Short Codes for FNE00 was defined in **Section 5.5** to provide Dial Tone and Mobile Callback for mobility extension.

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

- Set the **Local URI** and **Contact** fields to pre-define DID number **416xxx1397** appropriately for **Channel 2**.
- Associate **Incoming Group** and **Outgoing Group** to SIP Line 19.
- Set the **Max Calls per Channel** field to **10**.
- Other parameters retain default values.

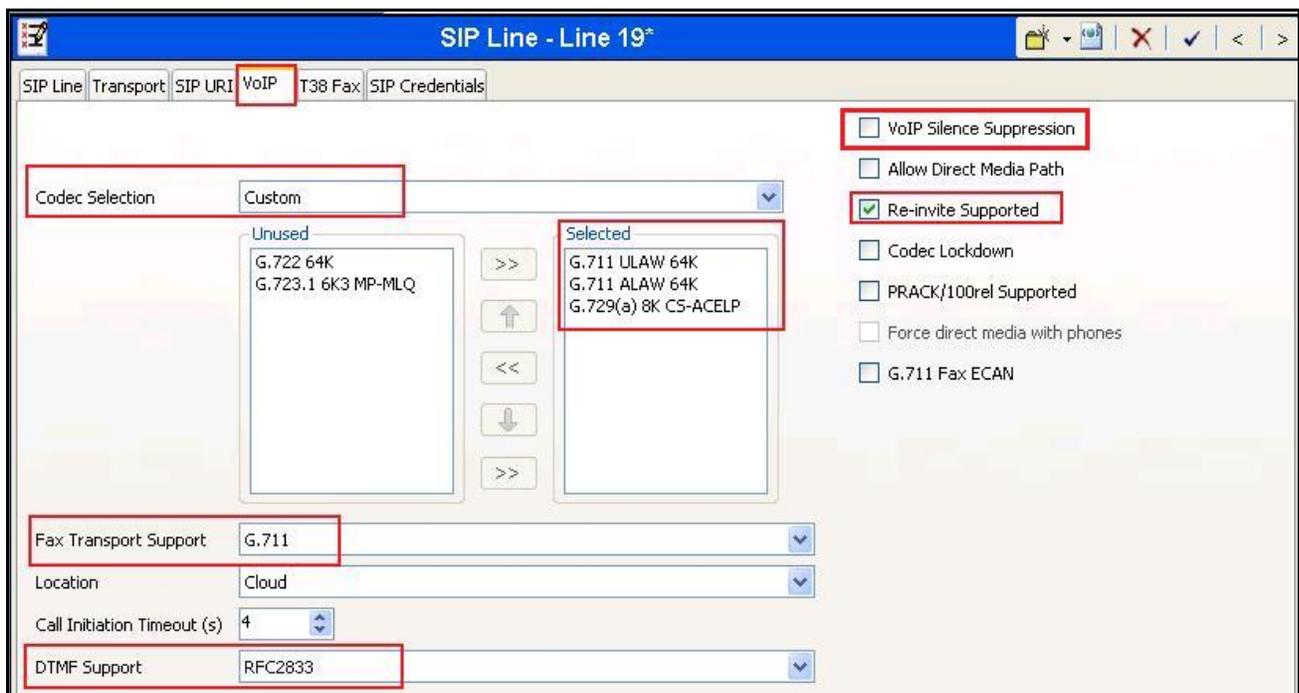
Click OK to commit.

SIP URI entry for Channel 2



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

- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. Select **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** codecs cause Avaya IP Office to include these codes, supported by the Bell Canada SIP Trunking service, in the Session Description Protocol (SDP) offer, in that order.
- Set **Fax Transport Support** to **G711** from the pull-down menu (T.38 faxing is not currently supported by Bell Canada).
- Set the **DTMF Support** field to **RFC2833** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box. By unchecking the **VoIP Silence Suppression** box, calls can be established with the G.729 codec but without silence suppression.
- Check the **Re-invite Supported** box.
- Default values may be used for all other parameters.



5.5. Short Code

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

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**, this short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N"@avayalab.com:5060"**. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value **N** represents the number dialed by the user. The host part following the “@” is the domain of the service provider network.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4**. This short code will use this line group when placing the outbound call.
- Set **Locale** to **United State (US English)**.

The screenshot displays the Avaya configuration interface. On the left, the 'IP Offices' tree shows 'Short Code (67)' selected. The main area is divided into two panes. The left pane, titled 'Short Code', shows a list of codes with '9N;' selected. The right pane, titled '9N;; Dial', shows the configuration details for this short code:

Field	Value
Code	9N;
Feature	Dial
Telephone Number	N"@avayalab.com"
Line Group ID	19
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

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

- In the **Code** field, enter the FNE feature code as **FNE00** for **Dial Tone**.
- Set the **Feature** field to **FNE Service**.
- Set the **Telephone Number** field to **00** for **FNE00**.
- Set the **Line Group ID** field to **0**.
- Retain default values for other fields.

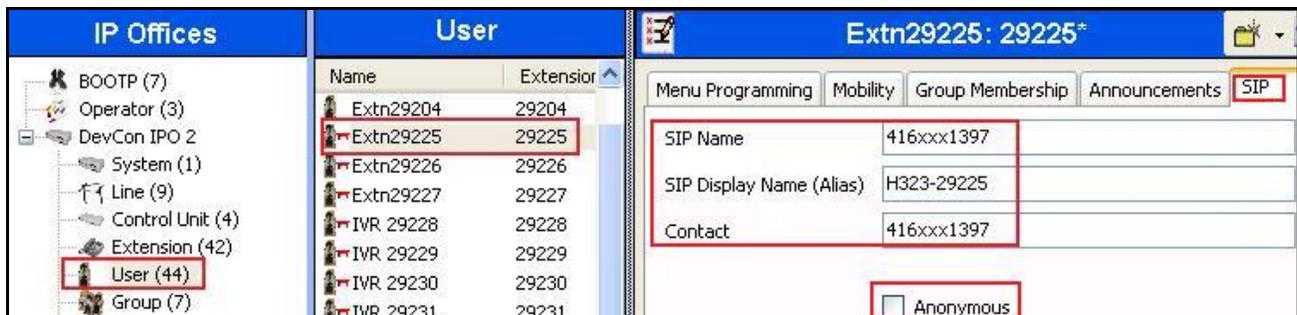
The screenshot displays the Avaya configuration interface. On the left, the 'Short Code' list shows 'FNE00' selected. The right pane, titled 'FNE00: FNE Service', shows the configuration details for this short code:

Field	Value
Code	FNE00
Feature	FNE Service
Telephone Number	00
Line Group ID	0
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

5.6. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first select **User** in the left Navigation Pane, then select the name of the user to be modified in the center Group Pane. In the example below, the name of the user is “H323-29225”. Select the **SIP** tab in the Details Pane.

The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. They also allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4**). The example below shows the settings for user H323-29225. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from Bell Canada. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user’s information from the network.



One of the H.323 IP Phones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for User H323-29225. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case 916139675279. Other options can be set according to customer requirements.



5.7. Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, select **Incoming Call Route** in the left Navigation Pane, then right-click in the center Group Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

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

Line Gr...	Incoming Number	Destin
19	416xxx1397	29225
20		
21		
22		
23		

Bearer Capacity	Any Voice
Line Group ID	19
Incoming Number	416xxx1397
Incoming Sub Address	
Incoming CLI	
Locale	United States (US English)
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to 416xxx1397 on line 19 are routed to extension **29225**.

TimeProfile	Destination	Fallback Extension
Default Value	29225 Extn29225	

5.8. Privacy/Anonymous Calls

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

To configure Avaya IP Office to use PAI for privacy calls, navigate to **User** → **noUser** in the Navigation / Group Panes. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button (not shown).

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



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



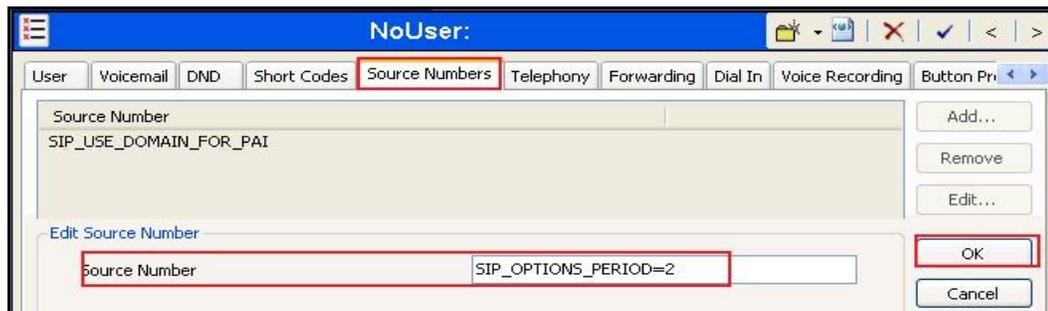
5.9. SIP Options

Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. 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 5.1** 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:

- If no **SIP_OPTIONS_PERIOD** parameter is defined and the **Binding Refresh Time** is 0, then the default value of 44 seconds is used.

- To establish a period less than 42 seconds, do not define a **SIP_OPTIONS_PERIOD** parameter and set the **Binding Refresh Time** to a value less than 42 secs. The **OPTIONS** message period will be equal to the **Binding Refresh Time**.
- To establish a period greater than 42 seconds, a **SIP_OPTIONS_PERIOD** parameter must be defined. The **Binding Refresh Time** must be set to a value greater than 42 secs. The **OPTIONS** message period will be the smaller of the **Binding Refresh Time** and the **SIP_OPTIONS_PERIOD**.

To configure the **SIP_OPTIONS_PERIOD** parameter, navigate to **User** → **noUser** in the Navigation / Group Panes. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button (not shown). 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 1 minute was desired. The **Binding Refresh Time** was set to **60** seconds (1 minute) in **Section 5.1**. The **SIP_OPTIONS_PERIOD** was set to **2** minutes. Avaya IP Office chose the **OPTIONS** period as the smaller of these two values (1 minute). Click the **OK** button (not shown).



5.10. Save Configuration

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

6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see Error! Reference source not found. [5], [6] and [7].

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

Trunk Server configuration elements for the service provider - Bell:

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

Call Server configuration elements for the enterprise - IP Office:

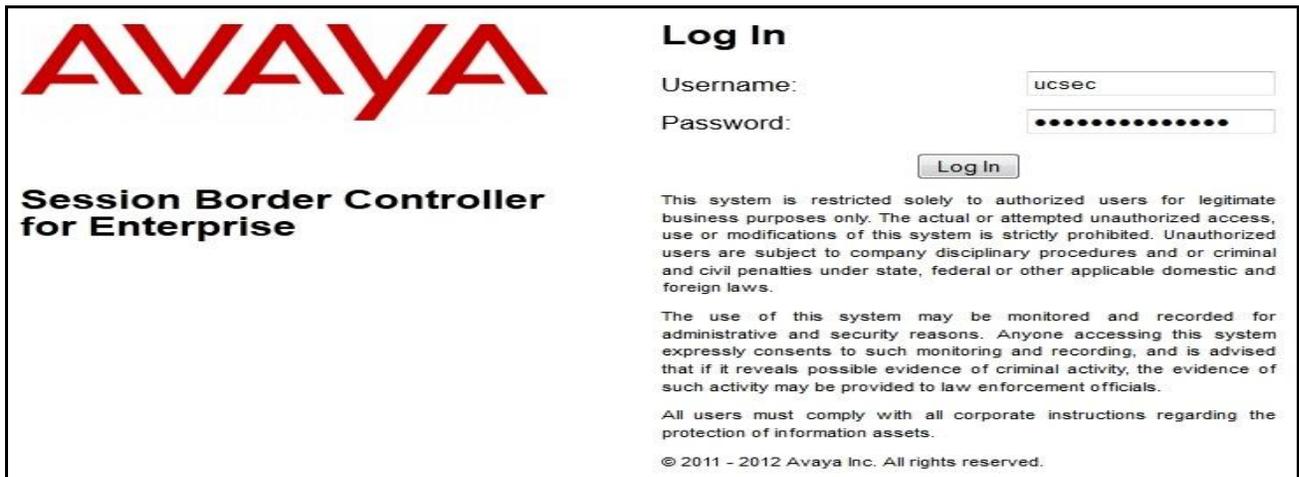
- Global Profiles:
 - URI Groups
 - Routing
 - Topology Hiding
 - Server Interworking
 - Server Configuration
- Domain Policies:
 - Application Rules
 - Media Rules
 - Signaling Rules
 - Endpoint Policy Group
 - Session Policy

- Device Specific Settings:
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows → Server Flows
 - Session Flows

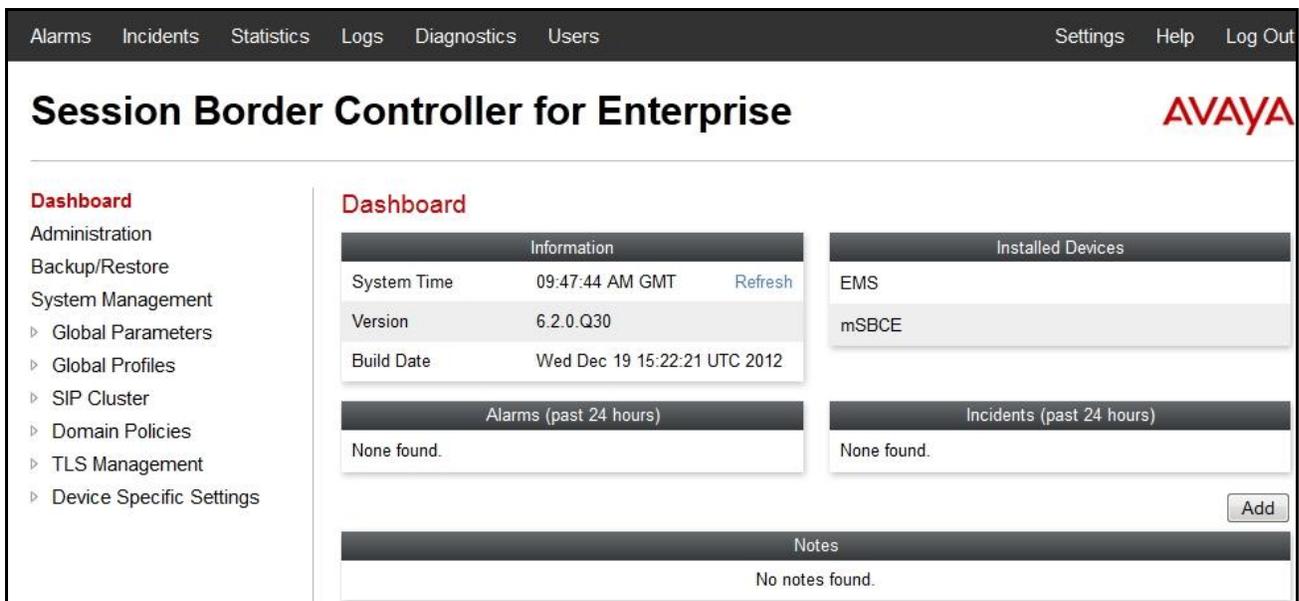
6.1. Log into the Avaya Session Border Controller for Enterprise

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

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



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



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

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies

System Management

Devices Updates SSL VPN Licensing

Device Name (Serial Number)	Management IP	Version	Status					
mSBCE (IFCS21020002)	10.10.98.70	6.2.0.Q30	Commissioned	Reboot	Shutdown	Restart Application	View	Edit Delete

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

System Information: mSBCE [X]

General Configuration

Appliance Name	mSBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.97.174	10.10.97.174	255.255.255.192	10.10.97.129	A1
10.10.98.106	10.10.98.106	255.255.255.224	10.10.98.97	B1

DNS Configuration

Primary DNS	10.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.10.97.174

Management IP(s)

IP	10.10.98.70
----	-------------

6.2. Global Profiles

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

6.2.1. Uniform Resource Identifier (URI) Groups

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

To add an URI Group, select **Global Profiles** → **URI Groups** and click on the **Add Group** button (not shown).

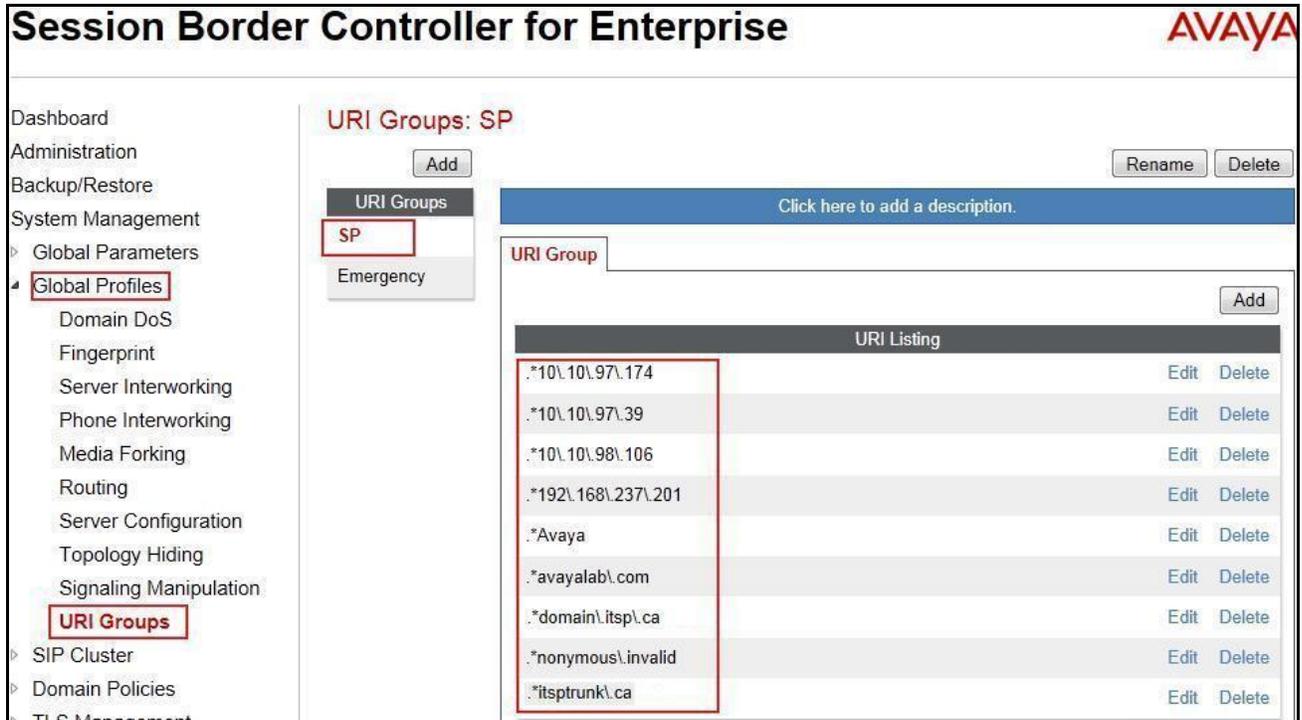
In the compliance testing, URI Group **SP** was added with URI type as **Regular Expression**. It consists of the following:

- Enterprise SIP domains “***avayalab**.com” for regular calls
- “***nonymous\invalid**” for private calls
- IP address based service provider SIP domains “***192\168\237\201**” and “***10\10\98\106**”
- IP addresses based URI-Host of the OPTIONS heartbeat originated by IP Office “***10\10\97\39**” and “***10\10\97\174**”.
- “***Avaya**” for receiving OPTIONS sent by Bell network.

The URI-Group **SP** was used to match the “From” and “To” headers in a SIP call dialog received from both IP Office and Bell. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see Section 6.2.2) and Server Flow (see Section 6.4.4) to route incoming and outgoing calls to the right destinations.

Note: In a normal configuration, URI Group is not needed for deployment of this solution. The reason it is being used in this testing is due to the fact that in this lab environment, single Avaya SBCE is being used for multiple service provider testing.

The screenshot below illustrates the URI listing for URI Group SP.



6.2.2. Routing Profiles

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

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

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

On the opposite direction, Routing profile **To_IPO_97_39** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) defined for Bell. This entry is to route incoming calls from Bell to the enterprise.

6.2.2.1 Routing Profile for Bell

To display **Edit Routing Rule** dialog of Routing profile **To-SP**, select **Global Profiles** → **Routing: To-SP**. As shown in the screenshot below, if there is a match on the SIP domain of the “To” header with the URI Group **SP** defined in **Section 6.2.1**, outgoing calls will be routed to the **Next Hop Server 1** as defined as **192.168.237.201** which is the IP address of Bell Trunk Server, on port **5060**.

As shown in **Figure 1**, Bell SIP Trunking was connected with transportation protocol **UDP**. The other options were kept as default.

Edit Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group: SP

Next Hop Server 1: 192.168.237.201:5060

Next Hop Server 2:

Routing Priority based on Next Hop Server:

Use Next Hop for In Dialog Messages:

Ignore Route Header for Messages Outside Dialog:

NAPTR:

SRV:

Outgoing Transport: TLS TCP UDP

Finish

6.2.2.2 Routing Profile for Avaya IP Office

Similarly, Routing profile **To_IPO_97_39** was created to route incoming calls to the **Next Hop Server 1** as defined as **10.10.97.39** which is the IP address of IP Office, on port **5060** if there is a match on the SIP domain of the “To” header with the URI Group **SP** defined in **Section 6.2.1**. As shown in **Figure 1**, IP Office was connected with transportation protocol **UDP**.

To display **Edit Routing Rule** dialog of Routing profile **To_IPO_97_39**, select **Global Profiles** → **Routing: To_IPO_97_39** then click **Edit** (not shown).

Edit Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group: SP

Next Hop Server 1: 10|10.97.39:5060

Next Hop Server 2:

Routing Priority based on Next Hop Server:

Use Next Hop for In Dialog Messages:

Ignore Route Header for Messages Outside Dialog:

NAPTR:

SRV:

Outgoing Transport: TLS TCP UDP

Finish

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

6.2.3. Topology Hiding

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

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

In the compliance testing, two Topology Hiding profiles were created: **To-SP** and **To_IPO_97_39**.

6.2.3.1 Topology Hiding Profile for Bell

Topology Hiding profile **To-SP** was defined for outgoing calls to Bell to:

- Mask URI-Host of the “Request-URI” and “To” headers with service provider SIP domain **itsptrunk.ca** to meet the requirements of Bell.
- Mask URI-Host of the “From” header to service provider SIP domain **domain.itsp.ca**.
- Change the “Record-Route”, “Via” headers and SDP added by IP Office with external IP address known to Bell.

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'Topology Hiding' highlighted. The main content area is titled 'Topology Hiding Profiles: To-SP' and contains a table with the following configuration:

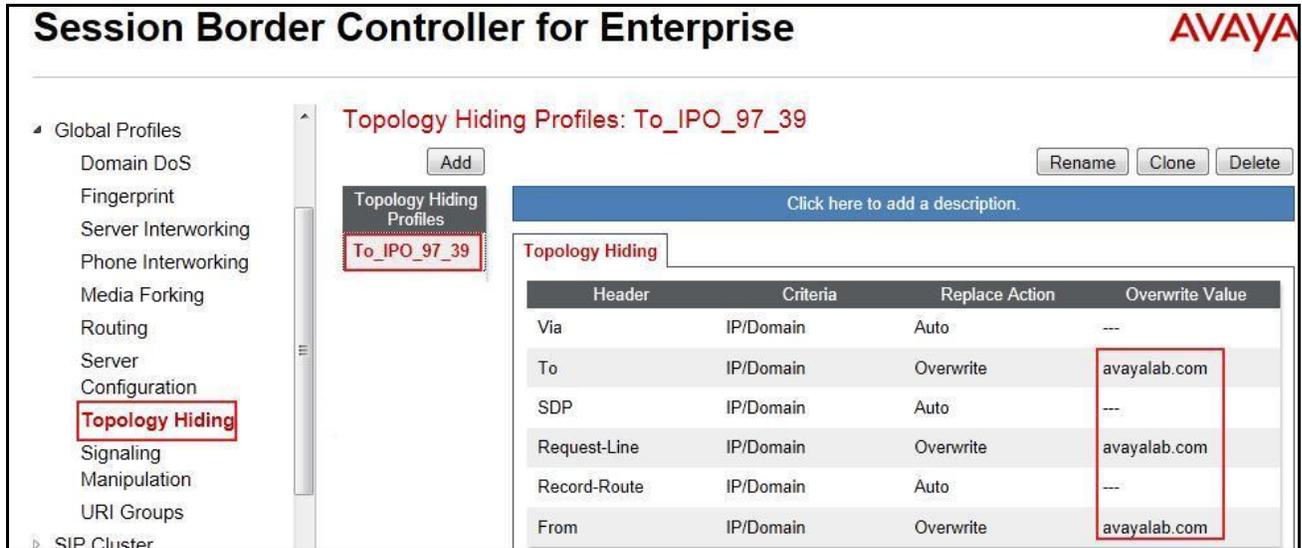
Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	domain.itsp.ca
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	itsptrunk.ca
To	IP/Domain	Overwrite	itsptrunk.ca

6.2.3.2 Topology Hiding Profile for IP Office

Topology Hiding profile **To_IPO_97_39** was defined for incoming calls to IP Office to:

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

The screenshots below illustrate the Topology Hiding profile **To_IPO_97_39**.

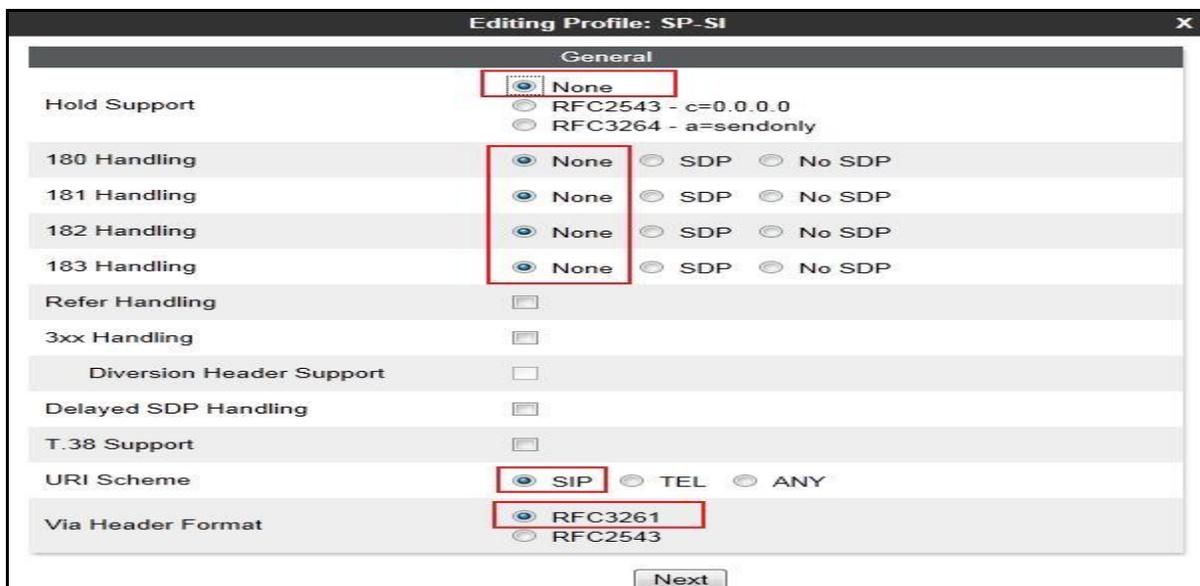


6.2.4. Server Interworking

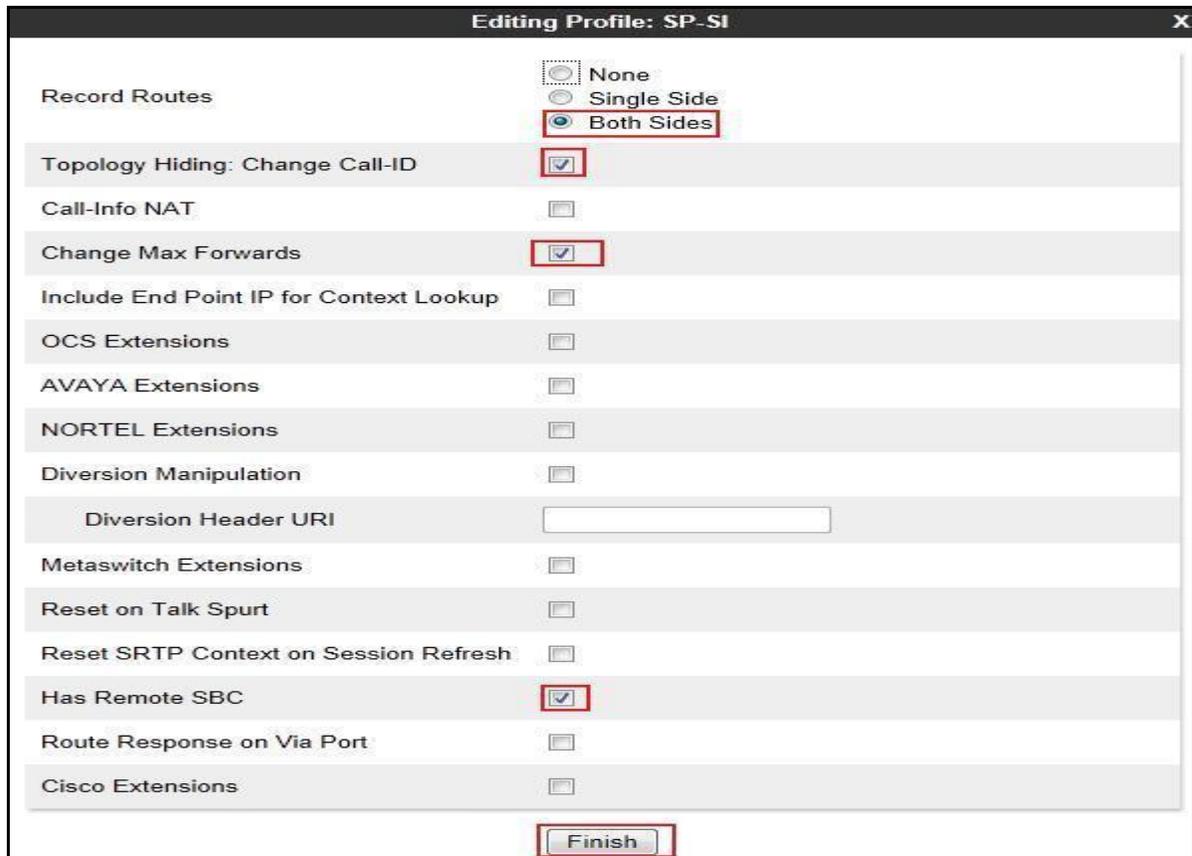
Server Interworking profile features are configured differently for Call Server and Trunk Server. To create a Server Interworking profile, select **Global Profiles** → **Server Interworking** then click on the **Add Profile** button (not shown). In the compliance testing, two Server Interworking profiles **SP-SI** and **IPO_97_39** were created for Bell (Trunk Server) and IP Office (Call Server).

6.2.4.1 Server Interworking Profile for Bell

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

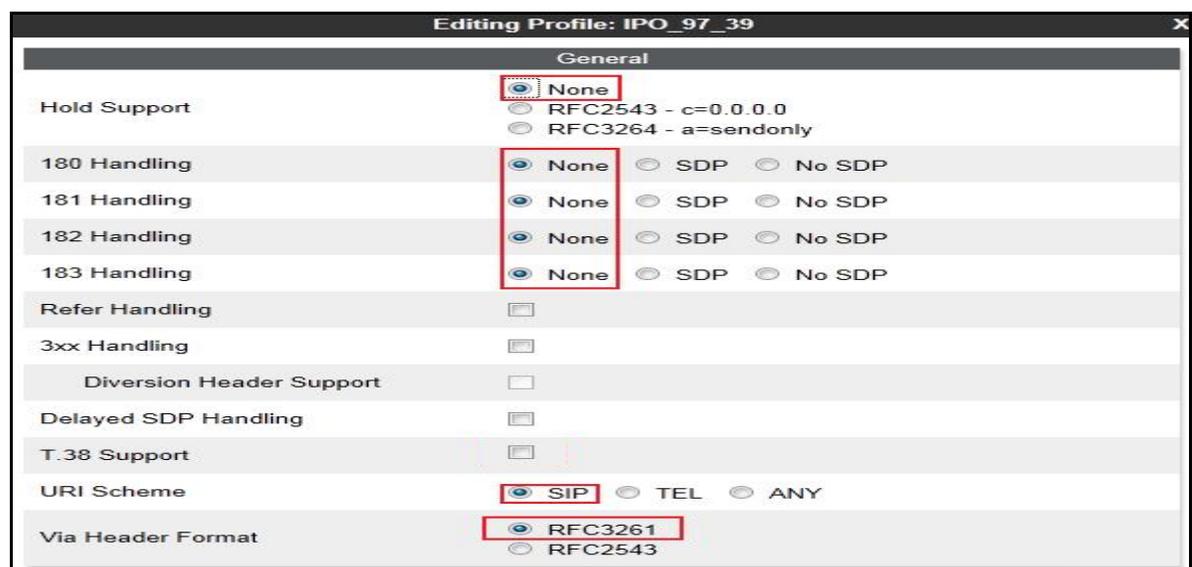


Advanced settings are being set as shown in capture bellow and others are left as default.



6.2.4.2 Server Interworking Profile for IP Office

Server Interworking profile **IPO_97_39** shown in the screenshots below, was similarly defined to match the specification of IP Office with the exception of the support for **Avaya Extensions** was enabled.



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

Setting	Value
Record Routes	Both Sides
Topology Hiding: Change Call-ID	Checked
Call-Info NAT	Unchecked
Change Max Forwards	Checked
Include End Point IP for Context Lookup	Unchecked
OCS Extensions	Unchecked
AVAYA Extensions	Checked
NORTEL Extensions	Unchecked
Diversion Manipulation	Unchecked
Diversion Header URI	
Metaswitch Extensions	Unchecked
Reset on Talk Spurt	Unchecked
Reset SRTP Context on Session Refresh	Unchecked
Has Remote SBC	Checked
Route Response on Via Port	Unchecked
Cisco Extensions	Unchecked

6.2.5. Server Configuration

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

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

In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for Bell and server entry **IPO_97_39** for IP Office.

6.2.5.1 Server Configuration for Bell

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

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and Routing. The "Server Configuration" option is highlighted in red. The main content area is titled "Server Configuration: SP-SC" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below these are tabs for "General", "Authentication", "Heartbeat", "Advanced", "DoS Whitelist", and "DoS Protection". The "General" tab is selected and highlighted in red. It contains a table with the following data:

Server Type	Trunk Server
IP Addresses / FQDNs	192.168.237.201
Supported Transports	UDP
UDP Port	5060

An "Edit" button is located at the bottom right of the table.

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

The screenshot shows the Avaya Session Border Controller for Enterprise interface, similar to the previous one. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. The navigation menu on the left is the same. The "Server Configuration" option is highlighted in red. The main content area is titled "Server Configuration: SP-SC" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below these are tabs for "General", "Authentication", "Heartbeat", "Advanced", "DoS Whitelist", and "DoS Protection". The "Advanced" tab is selected and highlighted in red. It contains a table with the following data:

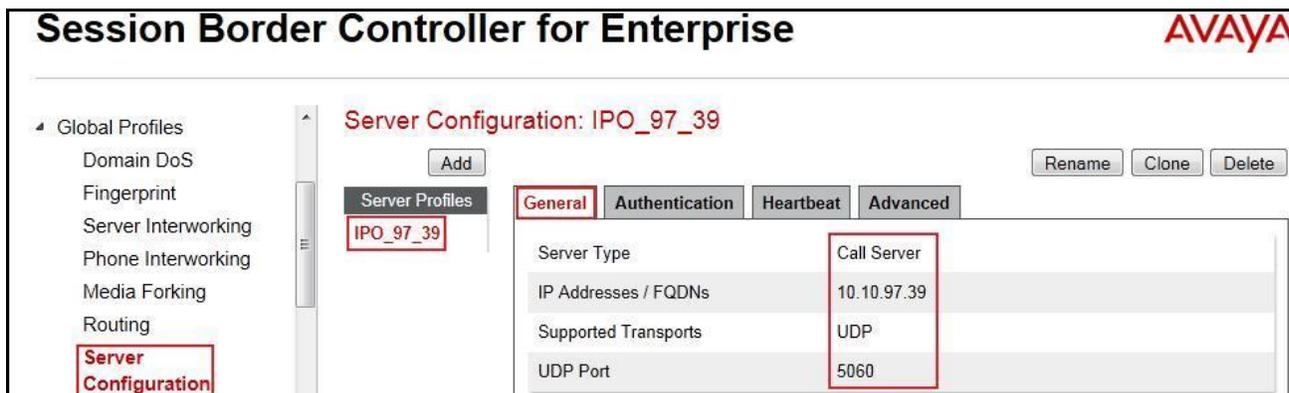
Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-SI
Signaling Manipulation Script	None
UDP Connection Type	SUBID

An "Edit" button is located at the bottom right of the table.

6.2.5.2 Server Configuration for Avaya IP Office

The Server Configuration **IPO_97_39** was similarly created for IP Office. It is discussed in detail as below. Only the **General** and **Advanced** tabs required provisioning. The **Heartbeat** tab was kept disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Bell to IP

Office to query for the status of the SIP Trunk. The **General** setting for Server Configuration **IPO_97_39** is being set as shown in following capture.



The Advanced setting is being set as shown in capture. Where the **IPO_97_39** Interworking Profile is selected as defined in **Section 6.2.4.2**.



6.3. Domain Policies

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

6.3.1. Application Rules

Application Rules define which types of SIP-based applications the Avaya SBCE security device will protect: voice, video, and/or instant messaging (IM). In addition, it is possible to configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

For the certification testing, Application Rule was created to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

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

Enter a descriptive name e.g. **SP-AR** for the new rule, then click on the **Finish** button (not shown). Click **Edit** button to modify the rule. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified Application Rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main content area is titled "Application Rules: SP-AR". It features a table of application rules and a miscellaneous section. The table has columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The 'Voice' rule is highlighted with a red box around its session limits. The 'Miscellaneous' section includes 'CDR Support' (None) and 'RTCP Keep-Alive' (No). A red box highlights the 'Edit' button at the bottom right of the configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	1000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

6.3.2. Media Rules

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packet matching the criteria will be handled by the Avaya SBCE security product.

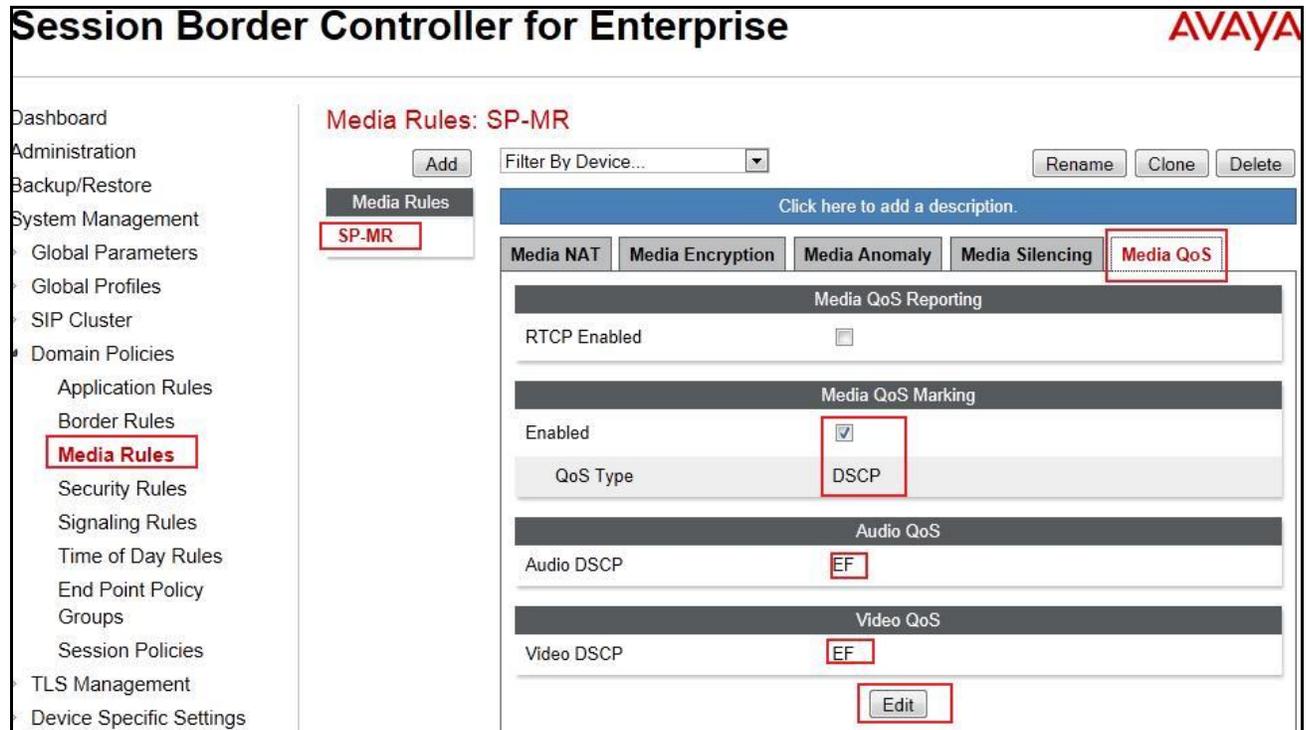
A custom Media Rule was created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration showed Media Rule **SP-MR** which was used for both the enterprise and Bell networks.

To create a **Media Rule**, navigate to **Domain Policies** → **Media Rules**, select the **default-low-med** rule then click on the **Clone Rule** button (not shown).

Enter a descriptive name e.g. **SP-MR** for the new rule, then click on **Finish** button (not shown).

Under **Media QoS** tab, then click on **Edit** button (not shown) to configure the Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policy for the media.

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



6.3.3. Signaling Rules

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

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

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

6.3.3.1 Signaling Rule for Bell

Clone a Signaling Rule with a descriptive name e.g. **SP-SR** and click on the **Finish** button (not shown).

Cloning the Signaling Rule default, verify that **General** settings of **SP-SR** with **Inbound** and **Outbound Request** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** (not shown).

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

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

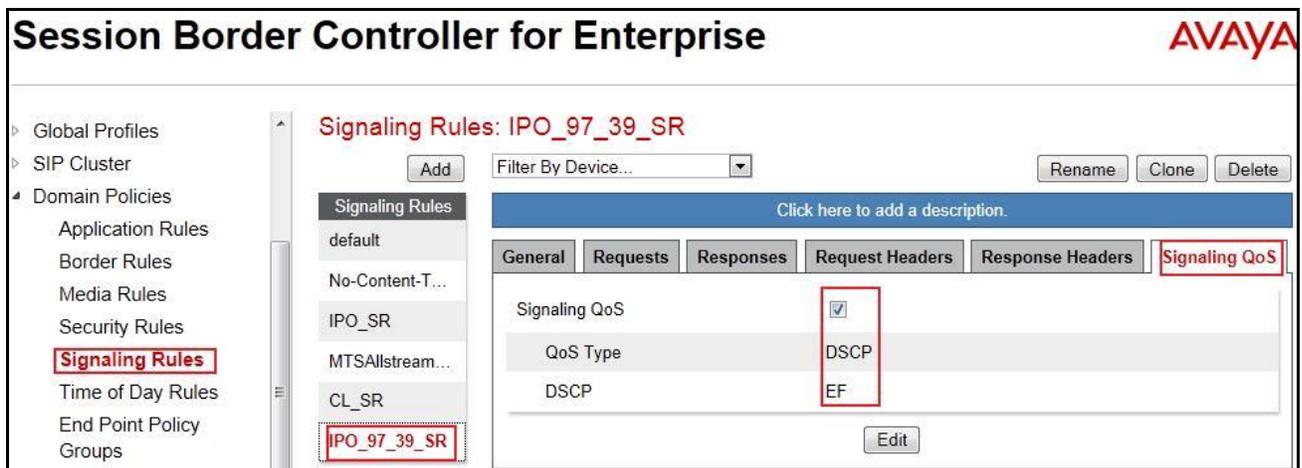


6.3.3.2 Signaling Rule for IP Office

Clone a Signaling Rule with a descriptive name e.g. **IPO_97_39_SR** for IP Office and click on the **Finish** button (not shown).

Cloning the Signaling Rule default, verify that **General** settings of **IPO_97_39_SR** with **Inbound** and **Outbound Request** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** (not shown).

Similarly the Signaling QoS rules are set as shown in Figure bellow.



6.3.4. Endpoint Policy Groups

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

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

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

6.3.4.1 Endpoint Policy Group for Bell

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

- Set Application Rule to **SP-AR** which was created in **Section 6.3.1**.
- Set Media Rule to **SP-MR** which was created in and **Section 6.3.2**.
- Set Signaling Rule to **SP-SR** which was created in **Section 6.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left sidebar lists various policy categories, with 'End Point Policy Groups' highlighted. The main area displays the configuration for 'Policy Groups: SP-PG'. A table lists the rules for this group:

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	SP-AR	default	SP-MR	default-high	SP-SR	default	Edit	Clone

6.3.4.2 Endpoint Policy Group for IP Office

The following screen shows policy group **IPO_97_39_PG** created for IP Office.

- Set Application Rule to **SP-AR** which was created in **Section 6.3.1**.
- Set Media Rule to **SP-MR** which was created in and **Section 6.3.2**.
- Set Signaling Rule **IPO_97_39_SR** which was created in **Section 6.3.3.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left sidebar lists various policy categories, with 'End Point Policy Groups' highlighted. The main area displays the configuration for 'Policy Groups: IPO_97_39_PG'. A table lists the rules for this group:

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	SP-AR	default	SP-MR	default-low	IPO_97_39_SR	default	Edit	Clone

6.4. Device Specific Settings

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

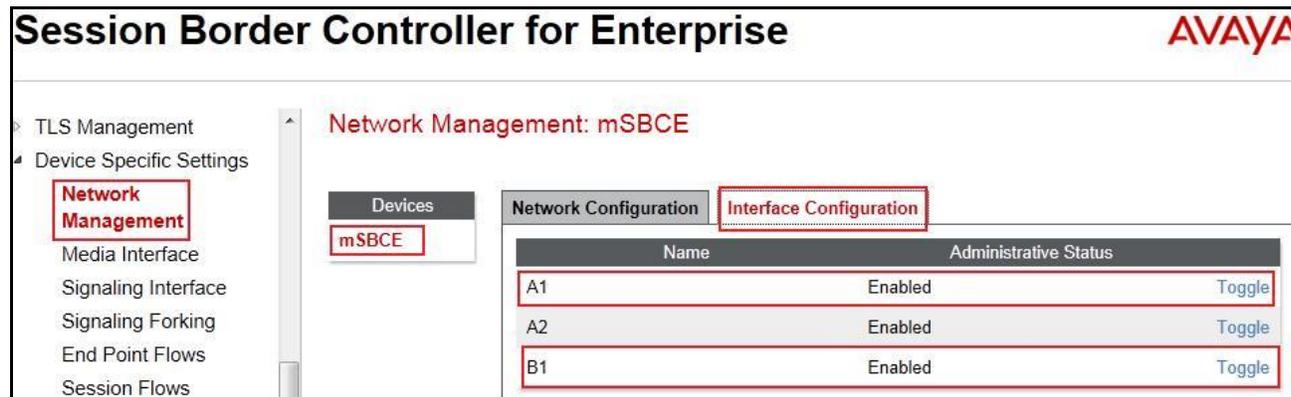
6.4.1. Network Management

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

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

IP Address	Public IP	Gateway	Interface	
10.10.97.174		10.10.97.129	A1	Delete
10.10.98.106		10.10.98.97	B1	Delete

On the **Interface Configuration** tab, enable the interfaces connecting to the inside enterprise and outside service provider networks. To enable an interface click it's **Toggle State** button. The following screen shows interface **A1** and **B1** were **Enabled**.



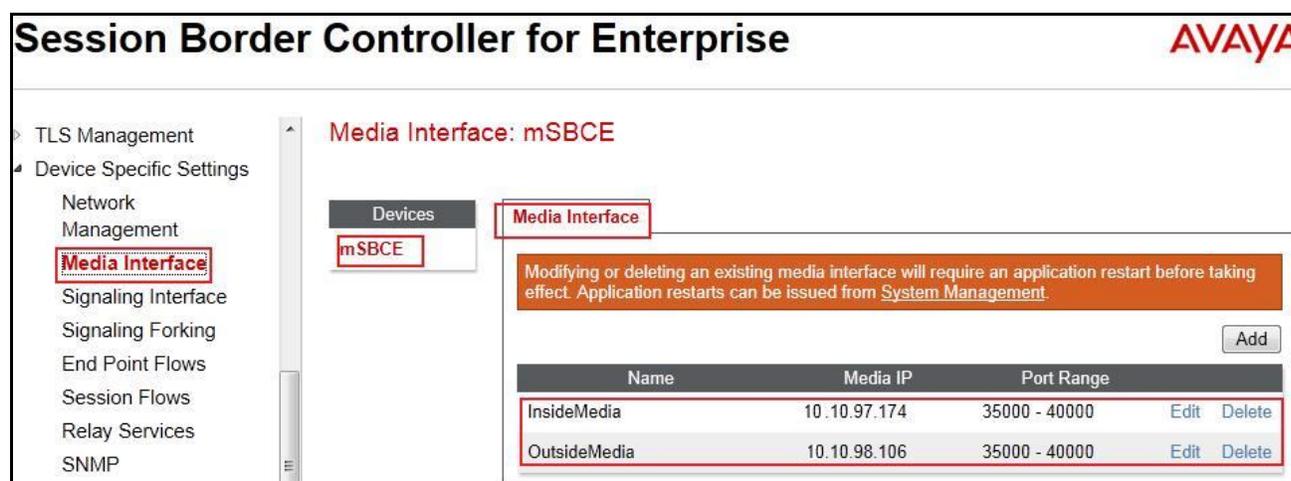
6.4.2. Media Interface

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

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

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

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



6.4.3. Signaling Interface

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

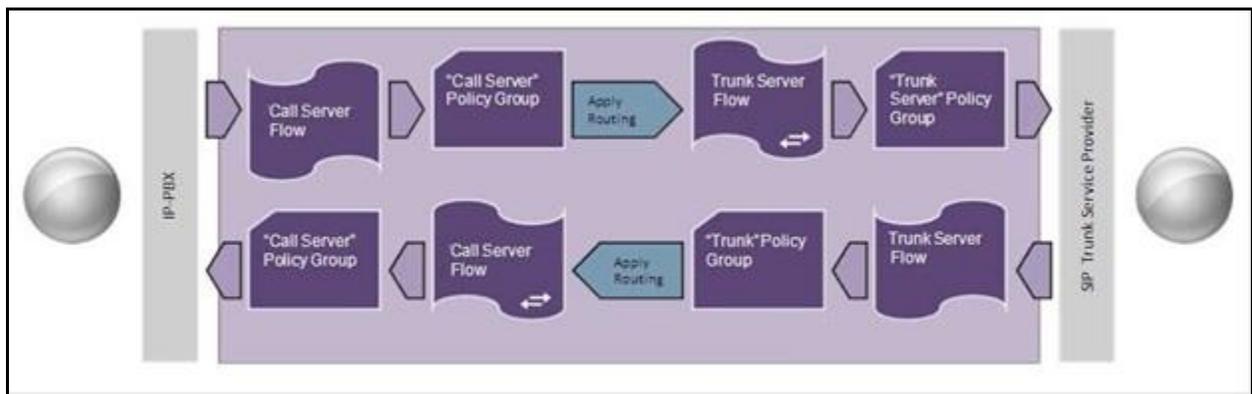
To create a new **Signaling Interface**, navigate to **Device Specific Settings → Signaling Interface** and click on the **Add Signaling Interface** button (not shown).

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

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	10.10.97.174	---	5060	---	None	Edit Delete
OutsideSIP	10.10.98.106	---	5060	---	None	Edit Delete

6.4.4. End Point Flows - Server Flow

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



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

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

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 6.2.5** which the Server Flow associates to.
- **URI Group:** Select the URI Group **SP** created in **Section 6.2.1**.
- **Received Interface:** Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to send the SIP signaling to.
- **Media Interface:** Select the Media Interface created in **Section 6.4.2** which is the Server Configuration is designed to send the RTP to.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 6.3.4**.
- **Routing Profile:** Select the Routing Profile created in **Section 6.2.2** which is used to which is the Server Configuration is designed to route the calls to.
- **Topology Hiding Profile:** Select the Topology Hiding profile created in **Section 6.2.3** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows the Server Flow **SP** for Bell.

Flow Name	SP
Server Configuration	SP-SC
URI Group	SP
Transport	*
Remote Subnet	*
Received Interface	InsideSIP
Signaling Interface	OutsideSIP
Media Interface	OutsideMedia
End Point Policy Group	SP-PG
Routing Profile	To_IPO_97_39
Topology Hiding Profile	To-SP
File Transfer Profile	None

Finish

Similarly, the following screen shows the Server Flow **IPO_97_39** for IP Office.

Edit Flow: IPO_97_39	
Flow Name	IPO_97_39
Server Configuration	IPO_97_39
URI Group	SP
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP
Signaling Interface	InsideSIP
Media Interface	InsideMedia
End Point Policy Group	IPO_97_39_PG
Routing Profile	To-SP
Topology Hiding Profile	To_IPO_97_39
File Transfer Profile	None
Finish	

6.4.5. Session Flows

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

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

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

- **Flow Name:** Enter a descriptive name.
- **URI Group #1:** Select the URI Group **SP** created in **Section 6.2.1** to assign to the Session Flow as the source URI Group.
- **URI Group #2:** Select the URI Group **SP** created in **Section 6.2.1** to assign to the Session Flow as the destination URI Group.

- **Session Policy:** Select the Session Policy **SP-SP**, which is clone from **default**, to assign to the Session Flow.
- Click on the **Finish** button.

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

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

Edit Flow: SP-SF X

Flow Name: SP-SF

URI Group #1: SP

URI Group #2: SP

Subnet #1: *
Ex: 192.168.0.1/24

Subnet #2: *
Ex: 192.168.0.1/24

Session Policy: SP-SP

Finish

7. Bell Canada SIP Trunking Configuration

Bell Canada is responsible for the configuration of Bell Canada SIP Trunking service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. Bell Canada will provide the customer the necessary information to configure the Avaya IP Office SIP connection to Bell Canada. The provided information from Bell Canada includes:

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

8. Verification Steps

The following steps may be used to verify the configuration:

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start** → **Programs** → **IP Office** → **System Status** on the PC where Avaya IP Office Manager was installed. Select the SIP line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** is *Idle* for each channel (assuming no active calls at present time).

The screenshot shows the Avaya IP Office System Status application interface. The left pane displays a tree view with 'Line: 19' selected. The main pane shows the 'SIP Trunk Summary' for Line 19. The summary includes the following details:

- Peer Domain Name: avayalab.com
- Resolved Address: 10.10.97.174
- Line Number: 19
- Number of Administered Channels: 30
- Number of Channels in Use: 0
- Administered Compression: G711 Mu, G729 A
- Silence Suppression: Off
- Layer 4 Protocol: UDP
- SIP Trunk Channel Licenses: Unlimited (0%)
- SIP Trunk Channel Licenses in Use: 0
- SIP Device Features: REFER (Incoming and Outgoing)

Below the summary is a table with the following columns: Channel Number, URI G..., Call Ref, Current State, Time in State, Remote Media A..., Co..., Conne..., Caller ID or Dial..., Other Party on Call, Direction of Call, Round Trip D..., Receive Jitter, Receive Packet..., Transmit Jitter, and Transmit Packet... The table contains five rows of data, all with a 'Current State' of 'Idle'.

At the bottom of the application, there are buttons for 'Trace', 'Trace All', 'Pause', 'Ping', 'Call Details', 'Print...', and 'Save As...'. The status bar at the bottom right shows the time '10:43:35 AM' and the state 'Online'.

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

The screenshot shows the Avaya IP Office System Status application interface with the 'Alarms' tab selected. The main pane displays 'Alarms for Line: 19 SIP avayalab.com'. Below this, there is a table with the following columns: Last Date Of Error, Occurrences, and Error Description. The table is currently empty. At the bottom of the application, there are buttons for 'Ping', 'Clear', 'Clear All', 'Print...', and 'Save As...'. The status bar at the bottom right shows the time '10:47:09 AM' and the state 'Online'.

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

- Verify that a phone connected to Avaya IP Office can successfully place a call to the PSTN with two-way audio.
- Using a network sniffing tool e.g. Wireshark to monitor the SIP signalling between the enterprise and Bell. The sniffer traces are captured at the public interface of the Avaya SBCE.

Following screenshots show an example incoming call from Bell to the enterprise.

- Incoming INVITE request from Bell.

```

INVITE sip:416xxx1397@domain.itsp.ca;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.237.201:5060;branch=z9hG4bKtuaskv10e840pmgh86g1.1
From: <sip:+16139675258@itsptrunk.ca;user=phone>;tag=SDfsh3b01-690686772-1383246642062-
To: "Bell Demo12345"<sip:416xxx1397@domain.itsp.ca>
Call-ID: SDfsh3b01-5c57de64cd1f1b53907a8a2834288c3f-a0n8330
CSeq: 133586376 INVITE
Contact: <sip:+16139675258@192.168.237.201:5060;transport=udp>
Supported: 100rel
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Accept: application/media_control+xml, application/sdp, multipart/mixed
Max-Forwards: 18
Content-Type: application/sdp
Content-Length: 208

v=0
o=BroadWorks 53627190 1 IN IP4 192.168.237.201
s=-
c=IN IP4 192.168.237.201
t=0 0
m=audio 21036 RTP/AVP 0 18 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=fmtp:18 annexb=no

```

- Outgoing 200OK response from the enterprise.

```
SIP/2.0 200 OK
From: <sip:+16139675258@itsptrunk.ca;user=phone>;tag=SDfsh3b01-690686772-1383246642062-
To: "Bell Demo12345" <sip:416xxx1397@domain.itsp.ca>;tag=db644802ae9f002f
CSeq: 133586376 INVITE
Call-ID: SDfsh3b01-5c57de64cd1f1b53907a8a2834288c3f-a0n8330
Contact: "H323-29225" <sip:416xxx1397@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=11825;lr;transport=udp>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,UPDATE
Supported: timer
Via: SIP/2.0/UDP 192.168.237.201:5060;branch=z9hG4bKtuaskv10e840pmgh86g1.1;ms-received-port=5060
Server: IP Office 9.0.0.0 build 829
Content-Type: application/sdp
Content-Length: 432

v=0
o=UserA 3154494098 1724038900 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 35010 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=candidate:aXbjcy37BQY5j+r2bC15HnNnXd9++/7ScRnpPCX16AY= 1 u9M/ImrEz18cEZ0NvqCqOQ==
UDP 0.050 10.10.98.106 35010
a=candidate:aXbjcy37BQY5j+r2bC15HnNnXd9++/7ScRnpPCX16AY= 2 u9M/ImrEz18cEZ0NvqCqOQ==
UDP 0.050 10.10.98.106 35011
```

Following screenshots show an example outgoing call from the enterprise to Bell.

- Outgoing INVITE request from the enterprise.

```
INVITE sip:6139675280@itsptrunk.ca SIP/2.0
From: "H323-29225" <sip:416xxx1397@domain.itsp.ca>;tag=6bf6fc9fd7b93643
To: <sip:6139675280@itsptrunk.ca>
CSeq: 2074542232 INVITE
Call-ID: bce13b3ff918df6f513a5742fd0a1e56
Contact: "H323-29225" <sip:416xxx1397@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=11846;lr;transport=udp>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,UPDATE
Supported: timer
User-Agent: IP Office 9.0.0.0 build 829
Max-Forwards: 69
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-000303249548-1--s1632-
Authorization: Digest username="416xxx1396", realm="itsptrunk.ca",
nonce="BroadWorksXhngdj9lrTs2i1l3BW", uri="sip:avayalab.com",
response="412523a6cxxx912affcb19804bf1047", algorithm=MD5, cnonce="0a4f113b",
qop=auth, nc=00000001
Path: <sip:10.10.98.106:5060;ipcs-line=11846;lr;transport=udp>
P-Asserted-Identity: "H323-29225" <sip:416xxx1397@domain.itsp.ca>
Content-Type: application/sdp
Content-Length: 479

v=0
o=UserA 2283250141 275xxx3746 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 35020 RTP/AVP 0 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=candidate:aXbjcy08SXk1B3+hMmTlTFnpFP91tNIQPG7ojS9IoN0= 1 0e4GT5MctUPB4hxXlYu7IA==
UDP 0.050 10.10.98.106 35020
a=candidate:aXbjcy08SXk1B3+hMmTlTFnpFP91tNIQPG7ojS9IoN0= 2 0e4GT5MctUPB4hxXlYu7IA==
UDP 0.050 10.10.98.106 35021
```

- Incoming 200OK response from Bell.

```
SIP/2.0 200 OK
From: "H323-29225" <sip:416xxx1397@domain.itsp.ca>;tag=6bf6fc9fd7b93643
To: <sip:6139675280@itsptrunk.ca>;tag=SDbuau299-80402914-1383246977275
CSeq: 2074542232 INVITE
Call-ID: bce13b3ff918df6f513a5742fd0a1e56
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-000303249548-1--s1632-
Record-Route: <sip:10.10.98.106:5060;ipcs-line=11846;lr;transport=udp>
Supported:
Contact: <sip:6139675280@192.168.237.201:5060;transport=udp>
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Accept: application/media_control+xml, application/sdp
Content-Type: application/sdp
Content-Length: 184

v=0
o=BroadWorks 53650254 1 IN IP4 192.168.237.201
s=-
c=IN IP4 192.168.237.201
t=0 0
m=audio 21046 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
aptime:20
```

9. Conclusion

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

10. Additional References

- [1] *IP Office 9.0 Installation, Document number 15-601042*, Issue 28, 11 October 2013
- [2] *IP Office 9.0 Manager 9.0, Document number 15-601011*, Issue 9.01, 09 September 2013
- [3] *IP Office 9.0 Administering Voicemail Pro, Document number 15-601063*, Issue 9.0 Release 1.0, September 2013
- [4] *IP Office Embedded Voicemail User Guide (IP Office Mode), Document number 15-604067*, Issue 9.0, 10 September 2013
- [5] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013.
- [6] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013.
- [7] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013.

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

Product documentation for Bell Canada SIP Trunking is available from Bell Canada.

11. Change History

Issue	Date	Reason
0.1	11/12/2013	Initial issue
1.1	04/21/2014	Update to reflect LAN2 configuration

©2014 Avaya Inc. All Rights Reserved.

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

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