



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Bell Canada SIP Trunking with Avaya IP Office 8.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Bell Canada and Avaya IP Office 8.1.

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 8.1, 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 IP Office). 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. 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. 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
- ◆ 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.

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 Binding Refresh Time of sending OPTIONS to monitor the SIP trunk connectivity is configured on Avaya IP Office to be larger than the Binding Refresh Time 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. This problem was reported to Avaya IP Office for further investigation since release 7.0.
- ◆ **DTMF tone transmission**: Bell Canada SIP Trunking service does not use out-of-band RTP events for DTMF tone transmissions as per RFC 2833 for inbound calls to the enterprise. Instead, DTMF tones were passed in-band using G.711MU on inbound calls. This configuration is on “purpose to avoid double conversion between in-band and RTP event when a call initiated from PSTN is forwarded back to PSTN by PBX” (quoted from Bell Canada support). Outbound calls from the enterprise use out-of-band DTMF tone transmission as configured on IP Office.

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 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 1408D Digital Telephone, 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.

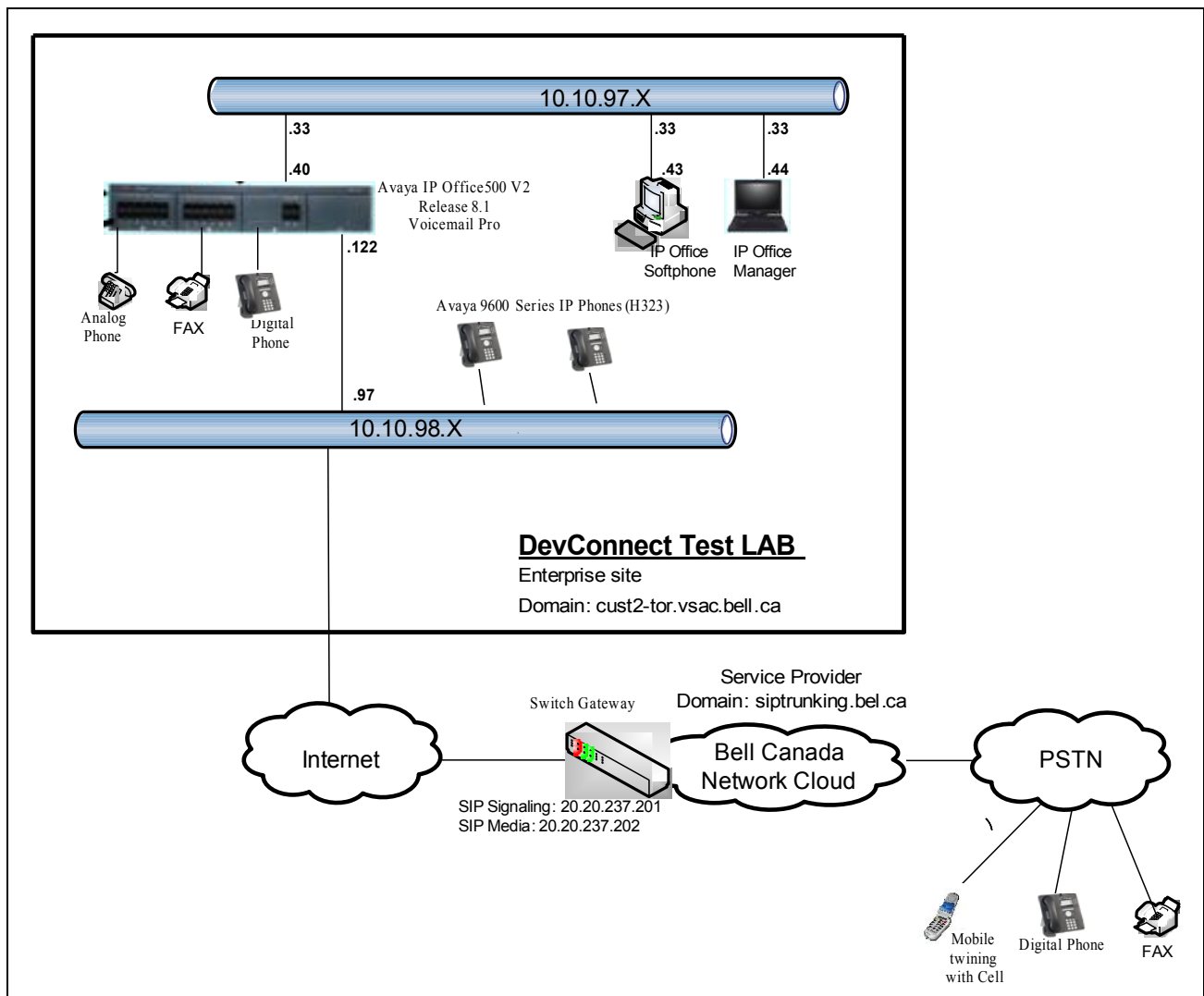


Figure 1: Test Configuration for Avaya IP Office with Bell Canada SIP Trunking Service

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. By default, Avaya IP Office is 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 of a SIP INVITE message. 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.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the Avaya IP Office such as a Session Border Controller or Data Firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and the Avaya IP Office must be allowed to pass through these devices.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	Release
Avaya IP Office 500v2	8.1 (43)
Avaya IP Office DIG DCP*16 V2	8.1 (43)
Avaya IP Office Ext Card Phone 8	8.1
Avaya IP Office Manager	10.1 (43)
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition S3.110b
Avaya Digital Telephones (1408D)	N/A
Avaya Symphony 2000 Analog Telephone	N/A
Avaya IP Office Softphone	3.2.3.15 64595
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

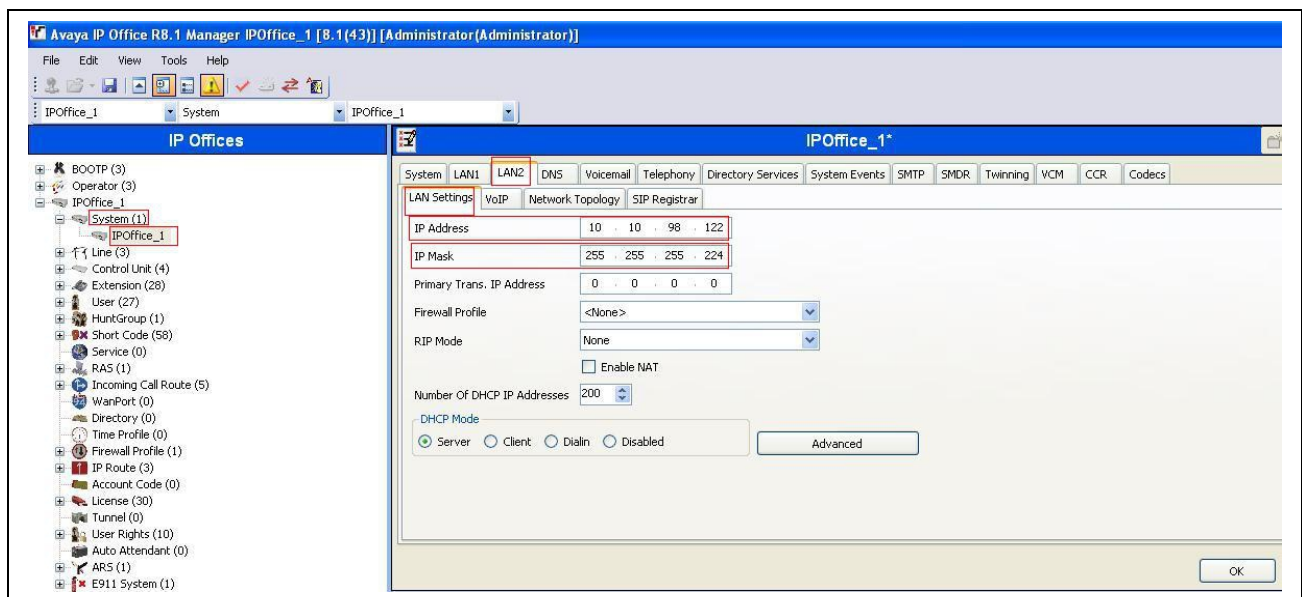
5. Configure IP Office

This section describes the Avaya IP Office configuration to support connectivity to Bell Canada SIP Trunking service. 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

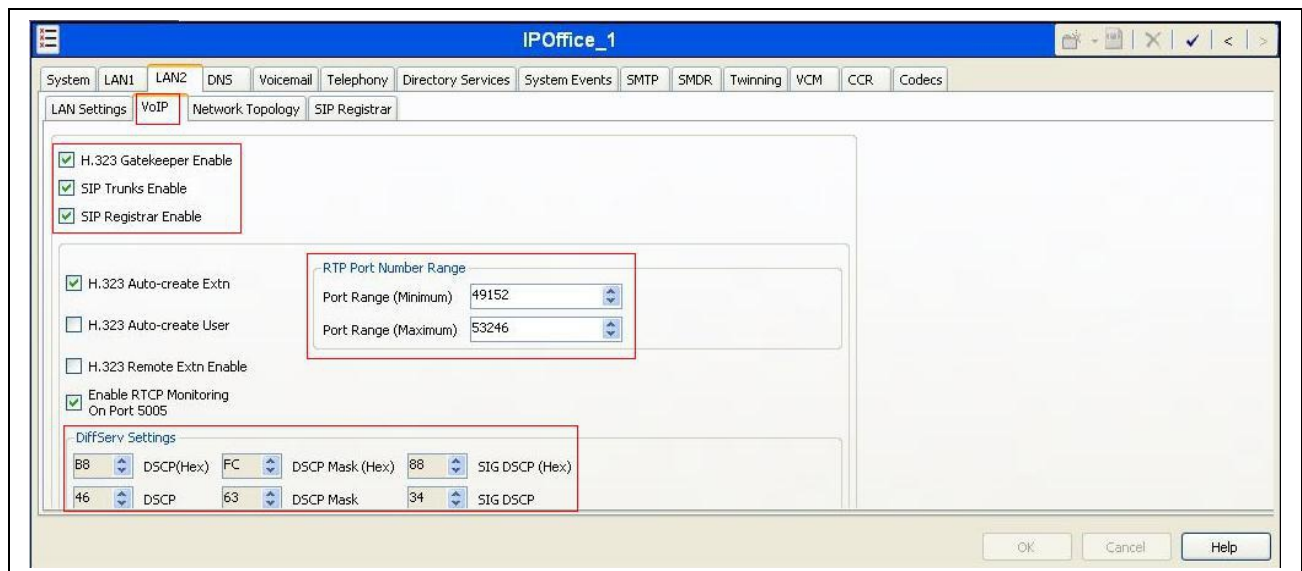
side, the Group pane in the center, and the Details pane on the right side. These panes will be referenced throughout the Avaya IP Office configuration. Proper licensing as well as standard feature configurations that are not directly related to the interface with the service provider (such as LAN interface to the enterprise site and IP Office Softphone support) is assumed to be already in place.

5.1. LAN2 Settings

In the sample configuration, **IPOffice_1** was used as the system name and the WAN port was used to connect the Avaya IP Office to the public network. The LAN2 settings correspond to the WAN port on the Avaya IP Office. To access the LAN2 settings, first navigate to **System (1) → IPOffice_1** in the Navigation and Group Panes and then navigate to the **LAN2 → LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office 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.

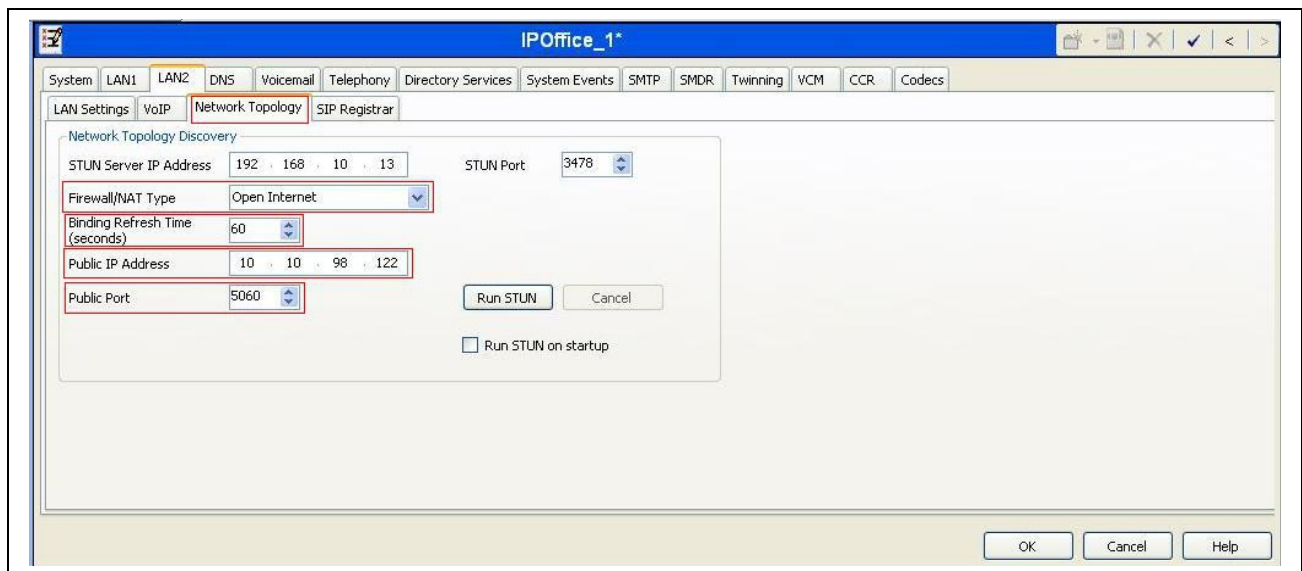


Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such the 9600-Series IP Telephones used in the sample configuration. The **SIP Trunks Enable** box must be checked to enable the configuration 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. Avaya IP Office can also 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 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:

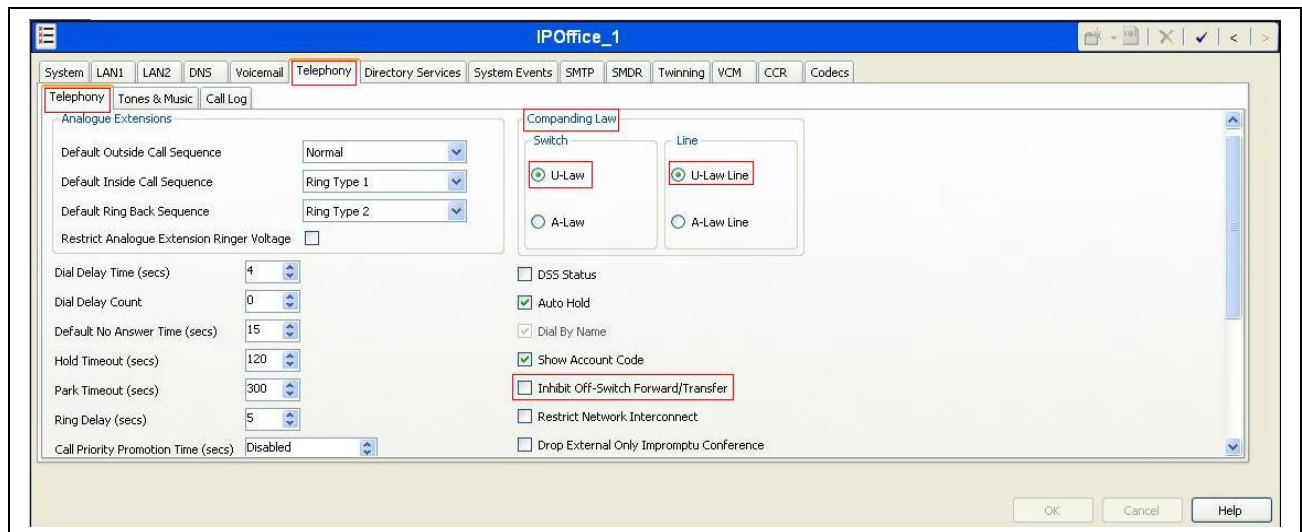
- ◆ Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. No firewall or network address translation (NAT) device was used in the compliance test as shown in **Figure 1**, so the parameter was set to **Open Internet**. With this configuration, STUN will not 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

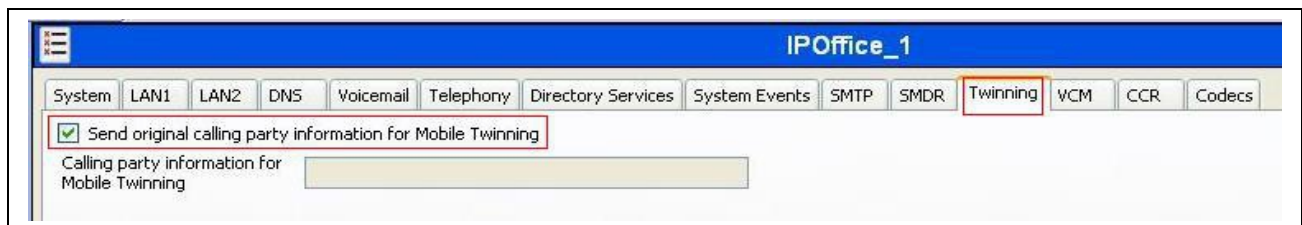
When using twinning, the calling party number displayed on the twinned phone is controlled by two parameters. These parameters only affect twinning and do not impact the messaging or operation of other redirected calls such as forwarded calls. The first parameter is the **Send original calling party 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**.

If **Send original calling party information for Mobile Twinning** is checked as shown below, the setting of the **Send Caller ID** parameter on the **SIP Line** form is ignored and Avaya IP Office will send the following in the SIP From Header:

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

If this parameter is unchecked, the value sent in the SIP From header is determined by the setting of the **Send Caller ID** parameter on the **SIP Line** form in **Section 5.4**.

For the compliance test, the **Send original calling party information for Mobile Twinning** box in the **System→Twinning** tab was checked which overrides any setting of the **Send Caller ID** parameter on the **SIP Line** form.



The screenshot shows the Avaya IP Office configuration window titled 'IPOffice_1'. The 'Twinning' tab is selected and highlighted with a red box. Within this tab, the checkbox 'Send original calling party information for Mobile Twinning' is checked and also highlighted with a red box. Below this checkbox, there is a text label 'Calling party information for Mobile Twinning' followed by an empty text input field.

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. To create a SIP line, begin by navigating to **Line** in the left Navigation Pane, then right-click in the Group Pane and select **New → SIP Line** (not shown). On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

- ◆ Set **ITSP Domain Name** to the 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 **None**. For the compliance test, this parameter was ignored since **Send original calling party information for Mobile Twinning** is checked 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 shows the 'SIP Line - Line 17' configuration window. The left pane shows the 'IP Offices' tree with 'Line(3)' selected. The main pane has tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', and 'SIP Credentials'. The 'SIP Line' tab is active, showing the following configuration:

- Line Number: 17
- ITSP Domain Name: cust2-tor.vtac.bell.ca
- In Service: ☒
- Use Tel URI: ☐
- Check OOS: ☒
- Call Routing Method: Request URI
- Originator number for Forwarded and twinning calls:
- Name Priority: System Default
- Caller ID from From header: ☒
- Send From In Clear: ☐
- User-Agent and Server Headers:
- Send Caller ID: None
- Association Method: By Source IP address
- REFER Support: ☒
- Incoming: Always
- Outgoing: Always

Select the **Transport** tab. The **ITSP Proxy Address** is set to the Bell Canada SIP Proxy IP Address provided by Bell Canada. As shown in **Figure 1**, this IP Address is **20.20.237.201**. In the **Network Configuration** area, **UDP** is selected as the **Layer 4 Protocol**, and the **Send Port** is set to the port number provided by Bell Canada. 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.

SIP Line - Line 17*

SIP Line **Transport** SIP URI VoIP T38 Fax SIP Credentials

ITSP Proxy Address 20.20.237.201

Network Configuration

Layer 4 Protocol UDP Send Port 5060

Use Network Topology Info LAN 2 Listen Port 5060

Explicit DNS Server(s) 0 0 0 0 0 0

Calls Route via Registrar ☒

Separate Registrar

A SIP Credentials entry must be created for Digest Authentication used by Bell Canada SIP trunking service to authenticate calls from the enterprise to the PSTN. To create a SIP Credentials entry, first select the **SIP Credentials** tab. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane (not shown) . To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the bottom of the screen, the Edit Channel area will be opened. In the example screen below, a previously configured entry is edited. The entry was created with the parameters shown below:

- ◆ Set **User name** and **Authentication Name** to the value provided by the service provider.
- ◆ Set **Password** to the value provided by the service provider. **Expiry (mins)** is set to **60**
- ◆ Uncheck the **Registration required** option. Bell Canada does not require registration for Digest Authentication.

The screenshot shows the 'SIP Line - Line 17' configuration window. The 'SIP Credentials' tab is selected. A table lists the credentials, and an 'Edit SIP Credentials' dialog box is open at the bottom.

Index	UserName	Authentication Name	Contact	Expiry (mins)	Register
1	4167751396	4167751396		60	False

Edit SIP Credentials

User name: 4167751396

Authentication Name: 4167751396

Contact:

Password: *****

Expiry (mins): 60

Registration required: ☐

Buttons: Add..., Remove, Edit..., OK, Cancel

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, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane (not shown). To edit an existing entry, click an entry in the list at the top, and click 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 will allow calls on this line if the 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 **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 **17** was defined that only contains this line (line 17).
- ♦ Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

The screenshot shows the 'SIP Line - Line 17' configuration window. The 'SIP URI' tab is selected. Below the tab, there is a table with columns: Channel, Groups, Via, Local URI, Contact, Display Name, PAI, Credential, and Max Calls. The table contains one entry with Channel 1, Groups 17 17, Via 1..., Local URI, Contact, Display Name, PAI, Credential 1: 4167..., and Max Calls 10. To the right of the table are buttons: Add..., Remove, and Edit... (highlighted with a red box). Below the table is the 'Edit Channel' dialog. The dialog has fields for: Via (10.10.98.122), Local URI (Use Internal Data), Contact (Use Internal Data), Display Name (Use Internal Data), PAI (Use Internal Data), Registration (1: 4167751396), Incoming Group (17), Outgoing Group (17), and Max Calls per Channel (10). The 'Edit Channel' dialog has OK and Cancel buttons.

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**, **G.711 ALAW 64K** and **G.729(a) 8K CS-ACELP** codecs which are supported by the Bell Canada SIP Trunking Service. Avaya IP Office will include these codes 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.
- ✦ Check **Use Offerer's Preferred Codec**.
- ✦ Default values may be used for all other parameters.

SIP Line - Line 17

SIP Line | Transport | SIP URI | **VoIP** | T38 Fax | SIP Credentials

Codec Selection: Custom

Unused

Selected

- G.711 ULAW 64K
- G.711 ALAW 64K
- G.729(a) 8K CS-ACELP

Fax Transport Support: G.711

Call Initiation Timeout (s): 4

DTMF Support: RFC2833

☐ VoIP Silence Suppression
☒ Re-invite Supported
☒ Use Offerer's Preferred Codec
☐ Codec Lockdown
☐ PRACK/100rel Supported

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 (not shown)**. On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created. The screen below shows the details of the previously administered “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 feature that the short code will invoke.
- ✦ Set **Telephone Number** to **N"@siptrunking.bell.ca: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 SIP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'Short Code (58)' selected. The main area is divided into two panes. The left pane, titled 'Short Code', contains a table with columns 'Code' and 'Telephone Number'. The right pane, titled '9N;; Dial', shows the configuration details for the selected short code.

Code	Telephone Number
*71*N#	N
9000	"MAINTENANCE"
*91N;	N".1"
*92N;	N".2"
*DSSN	";[0]151/ERR - "N
*SDN	";[0]151/ERR - "N
*SKN	";[0]151/ERR - "N
*6N	N
*9N;	N"@siptrunking.bell.ca:5060"

The configuration details for the '9N;; Dial' short code are as follows:

- Code:** 9N;
- Feature:** Dial
- Telephone Number:** N"@siptrunking.bell.ca:5060"
- Line Group ID:** 17
- Locale:** United States (US English)
- Force Account Code:** ☐

The “9N;” short codes illustrated above do 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 digits following the short code are desired, the Automatic Route Selection (ARS) feature may be used. In the following example screen, the short code 6N is illustrated for access to ARS. When the Avaya IP Office user dials 6 plus any number N, rather than being directed to a specific **Line Group Id**, the call is directed to **Line Group Id** “50: Main”, configurable via ARS. See **Section 5.8** for example ARS route configuration for “50: Main” as well as a backup route.

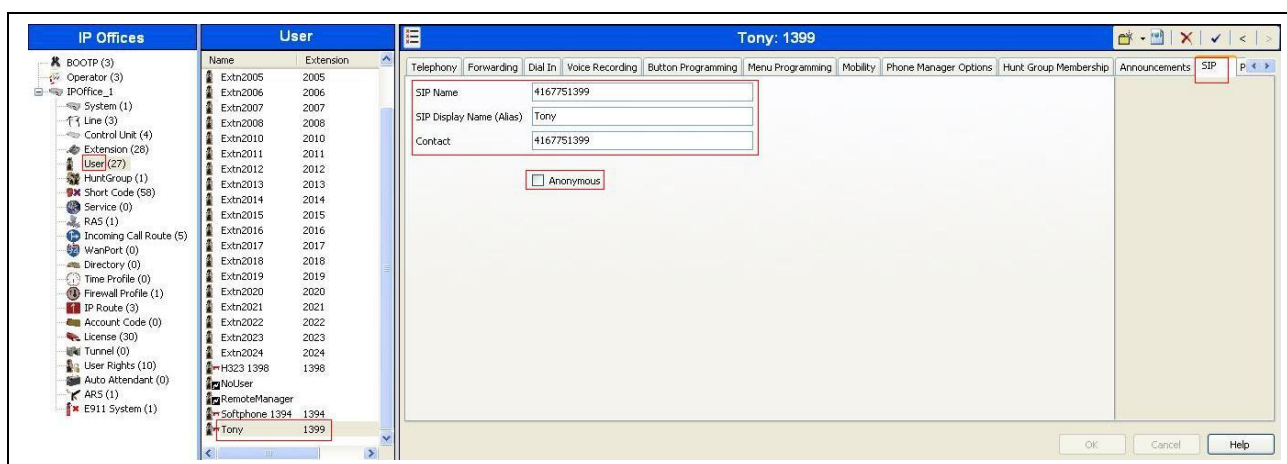
The screenshot shows a configuration window titled "6N: Dial". It contains the following fields and controls:

- Short Code** (tab):
- Code**: Text field containing "6N".
- Feature**: Dropdown menu set to "Dial".
- Telephone Number**: Text field containing "N".
- Line Group Id**: Dropdown menu set to "50: Main". This field is highlighted with a red rectangular box.
- Locale**: Dropdown menu.
- Force Account Code**: Check box, currently unchecked.
- Buttons**: "OK", "Cancel", and "Help" buttons at the bottom right.

5.6. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line as 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 “Tony”. 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 **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 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. 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 916132423648. Other options can be set according to customer requirements.

The screenshot shows the 'Mobility' tab configuration for a device named 'Tony: 1399*'. The 'Internal Twinning' section is disabled. The 'Mobility Features' and 'Mobile Twinning' checkboxes are checked. The 'Twinned Mobile Number (including dial access code)' is set to '916132423648'. Other settings include 'Twinning Time Profile' set to '<None>', 'Mobile Dial Delay (secs)' set to '1', and 'Mobile Answer Guard (secs)' set to '0'. There are also three unchecked checkboxes: 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', and 'Twin When Logged Out'.

Section	Field/Option	Value
Internal Twinning	Internal Twinning	<input type="checkbox"/>
	Twinned Handset	<None>
	Maximum Number of Calls	1
	Twin Bridge Appearances	<input type="checkbox"/>
Mobility Features	Mobility Features	<input checked="" type="checkbox"/>
	Mobile Twinning	<input checked="" type="checkbox"/>
Mobile Twinning	Twinned Mobile Number (including dial access code)	916132423648
	Twinning Time Profile	<None>
	Mobile Dial Delay (secs)	1
	Mobile Answer Guard (secs)	0
	Hunt group calls eligible for mobile twinning	<input type="checkbox"/>
	Forwarded calls eligible for mobile twinning	<input type="checkbox"/>
	Twin When Logged Out	<input type="checkbox"/>

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

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

The screenshot shows the 'IP Offices' configuration window. On the left, the 'Navigation Pane' lists various system components, with 'Incoming Call Route (5)' selected. The main area displays the 'Standard' tab for a specific route (ID 17 4167751399). The fields are as follows:

Field	Value
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	4167751399
Incoming Sub Address	
Incoming CLI	
Locale	United States (US English)
Priority	1 - Low
Tag	
Hold Music Source	System Source

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to 416-775-1399 on line 17 are routed to extension **1399 Tony**.

The screenshot shows the 'Destinations' tab for the same route. It contains a table with two columns: 'Destination' and 'Fallback Extension'.

Destination	Fallback Extension
1399 Tony	

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 illustrations and considerations. ARS is illustrated here to demonstrate alternate routing configuration should the SIP Line be out of service or temporarily not responding.

Optionally, ARS can be used rather than the simple “9N;” short code approach as documented in **Section 5.5**. With ARS, a 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. Although not shown in this section, 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 1+10 digit calls following an access code should use the SIP Line preferentially, but other local or service numbers following the access code should prefer a different outgoing line group, ARS can be used to distinguish the call behaviors.

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, select **ARS** in the Navigation pane, and select the appropriate route name in the Group pane.

The following screen shows an example ARS configuration for the route named “Main”. The **In Service** parameter refers to the ARS form itself. 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 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.

The screenshot displays the IP Office configuration interface for the ARS (Automatic Route Selection) configuration of the 'Main' route. The left pane shows the navigation tree with 'ARS' selected under 'Main'. The main pane shows the configuration details for the 'Main' route.

ARS Configuration Details:

- ARS Route Id: 50
- Route Name: Main
- Dial Delay Time: System Default (4)
- In Service: ☒ (checked)
- Time Profile: <None>
- Secondary Dial tone: ☒ (checked), SystemTone
- Check User Call Barring: ☒ (checked)
- Out of Service Route: S1: backup
- Out of Hours Route: <None>

Code Table:

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0N;	0N	Dial SK1	0
1N;	1N;siptrunking.bell.ca:5060	Dial SK1	17
XN;	N	Dial SK1	0
XXXXXXXXXXN	N	Dial SK1	0

Alternate Routing Configuration:

- Alternate Route Priority Level: 3
- Alternate Route Wait Time: 30
- Alternate Route: S1: backup

Buttons: Add..., Remove, Edit..., OK, Cancel, Help

Assuming the primary route is in-service, the number passed from the short code used to access ARS (e.g., 6N 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 6-1-613-242-3648, the call would be directed to **Line Group 17**. Line Group 17 is the SIP Line configured and described in these Application Notes. If Line Group 17 cannot be used, the call can automatically be routed to the route name configured in the **Alternate Route** parameter in the lower right of the screen. Since alternate routing can be considered a privilege not available to all callers, IP Office can control access to the alternate route by comparing the calling user priority to the value in the **Alternate Route Priority Level** field.

The following screen shows an example ARS configuration for the route named “backup” with ARS Route ID 51. Continuing from the prior example, if the user dialed 6-1-613-242-3648, and the call could not be routed via the primary route “50: Main” as described above, the call will be delivered to the alternate route “backup”. Per the configuration shown below, the call will be delivered to Line Group 1, using an analog trunk connecting Avaya IP Office to the PSTN as a backup connection. In this case, the originally dialed number (sans the short code 6) will be dialed as is through the analog/PRI trunk to the PSTN. Additional codes (e.g., 411, 0+10, etc.) can be added to the ARS route by pressing the **Add...** button to the right of the list of previously configured codes.

The screenshot displays the configuration window for the 'backup' ARS route. The left sidebar shows the navigation tree with 'ARS (2)' expanded, showing '50: Main' and '51: backup'. The main configuration area includes the following fields and options:

- ARS Route Id:** 51
- Route Name:** backup
- Dial Delay Time:** System Default (4)
- In Service:** ☒ (checked)
- Time Profile:** <None>
- Secondary Dial tone:** ☒ (checked)
- SystemTone:** SystemTone
- Check User Call Barring:** ☒ (checked)
- Out of Service Route:** <None>
- Out of Hours Route:** <None>
- Code List:**

Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
1N	1N	Dial	1
- Alternate Route Priority Level:** 3
- Alternate Route Wait Time:** 30
- Alternate Route:** <None>

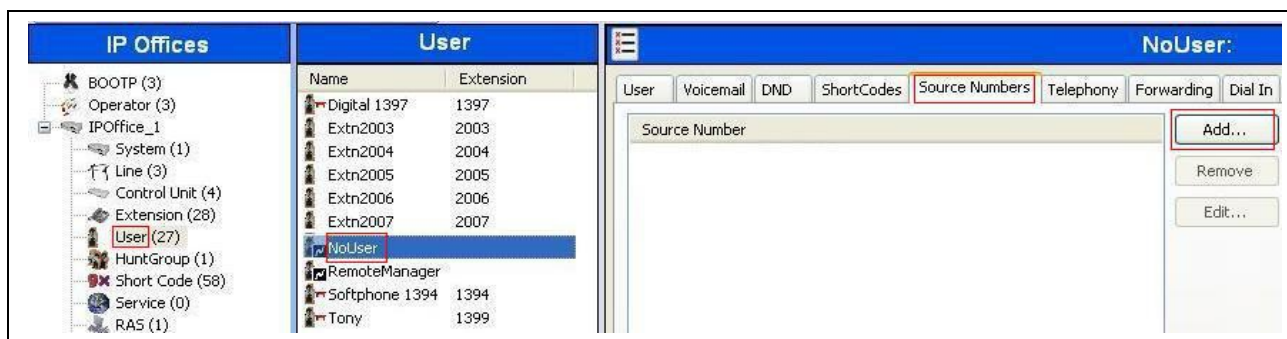
The 'Add...' button is highlighted in the code list area.

In the testing associated with the configuration, calls were successfully delivered to SIP Line 17 via the primary ARS route “50: Main”. When the primary route experiences a network outage, Avaya IP Office successfully routed the call via the backup route (This alternate route was not tested).

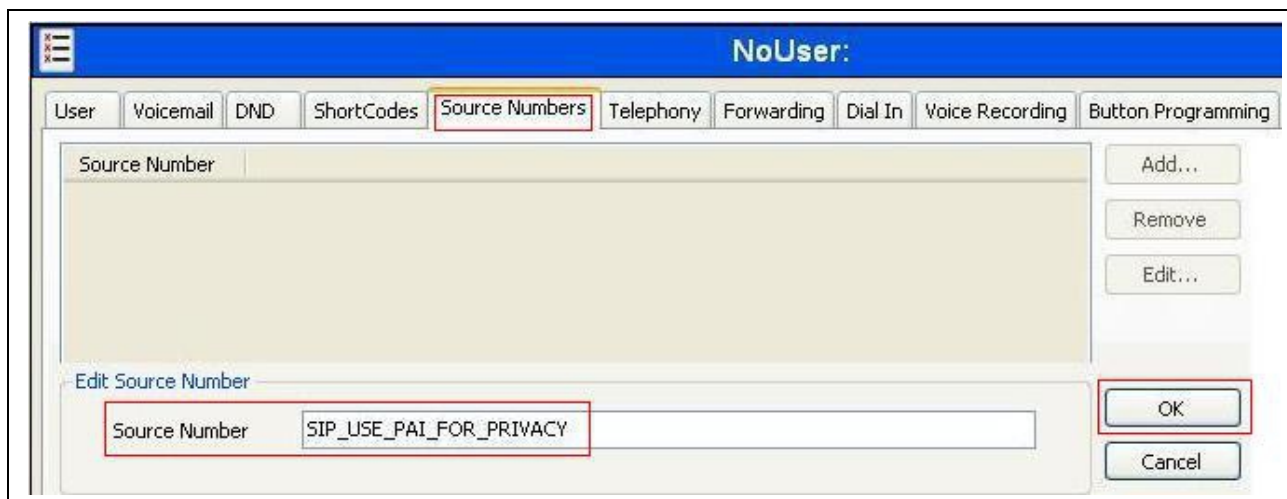
5.9. Privacy/Anonymous Calls

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.

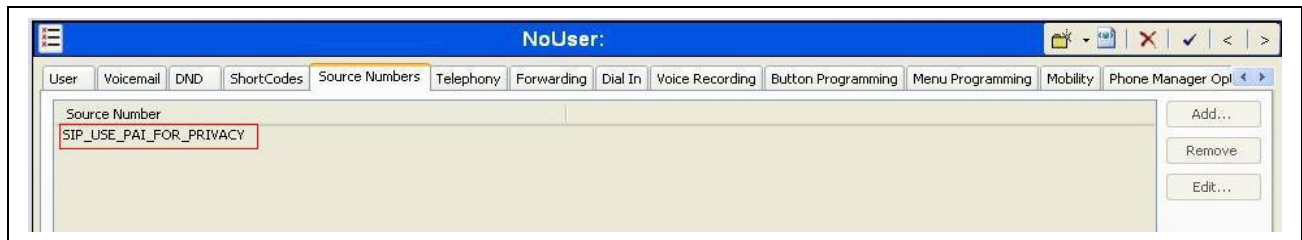
To configure Avaya IP Office to use PAI for privacy calls, navigate to **User → noUser** in the Navigation / Group Panes. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



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



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

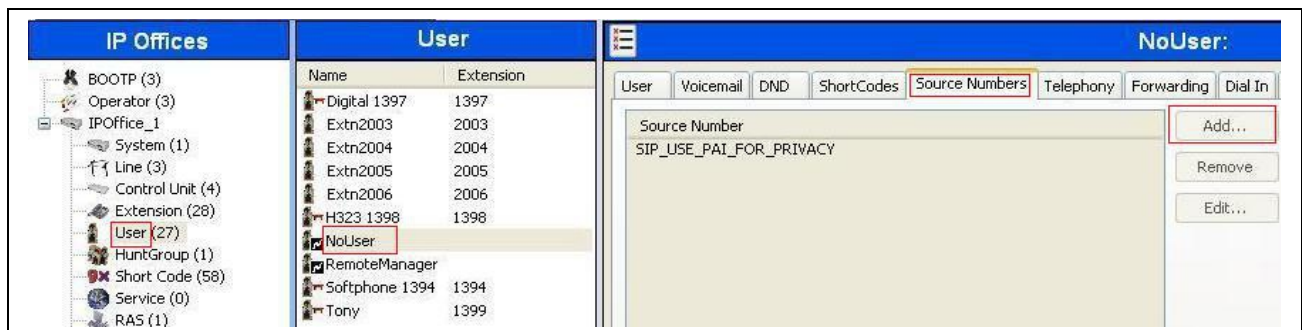


5.10. SIP Options

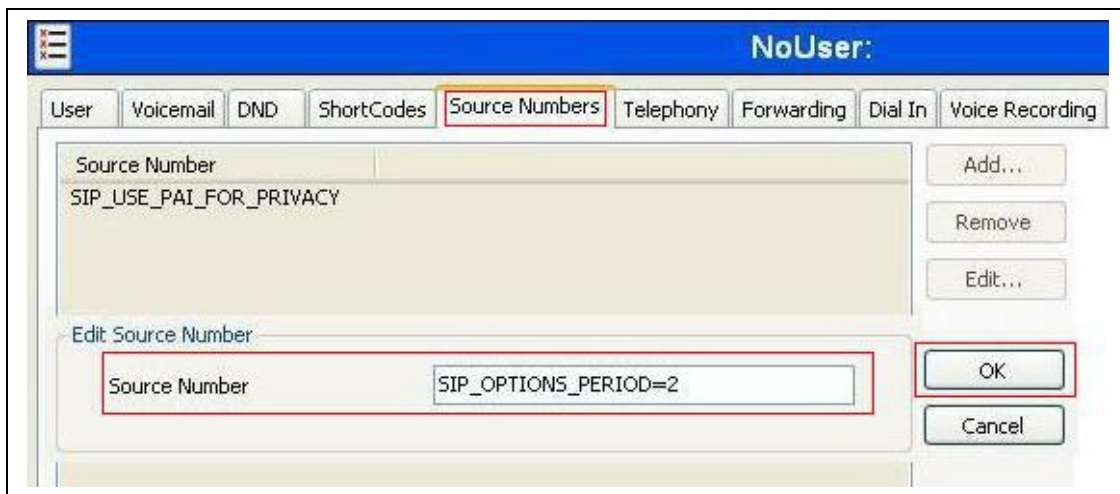
Avaya IP Office sends SIP OPTIONS messages periodically to determine if the SIP connection is active. The rate at which the messages are sent is determined by the combination of the **Binding Refresh Time** (in seconds) set on the **Network Topology** tab in **Section 5.1** and the **SIP_OPTIONS_PERIOD** 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 seconds. 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 seconds. The OPTIONS message period will be the **Binding Refresh Time** and smaller than the **SIP_OPTIONS_PERIOD**.

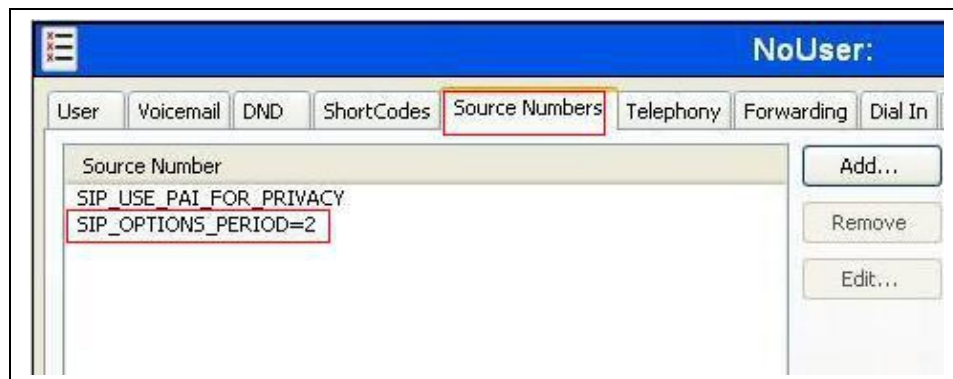
To configure the **SIP_OPTIONS_PERIOD** parameter, navigate to **User → noUser** in the Navigation / Group Panes. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



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 selects the lowest value of these two parameters (1 minute) to determine the actual OPTIONS interval. Click the **OK** button (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 (not shown).

6. 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.

7. 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 is installed. Select the SIP line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** is *Idle* for each channel (assuming no active calls at present time).

The screenshot shows the Avaya IP Office System Status application. The left pane displays a tree view with the following items: System, Alarms (1), Extensions (10), Trunks (5), Lines: 1 - 4, Line: 17, Active Calls, Resources, Voicemail, and IP Networking. The right pane shows the Status tab with the SIP Trunk Summary section. The summary includes the following information:

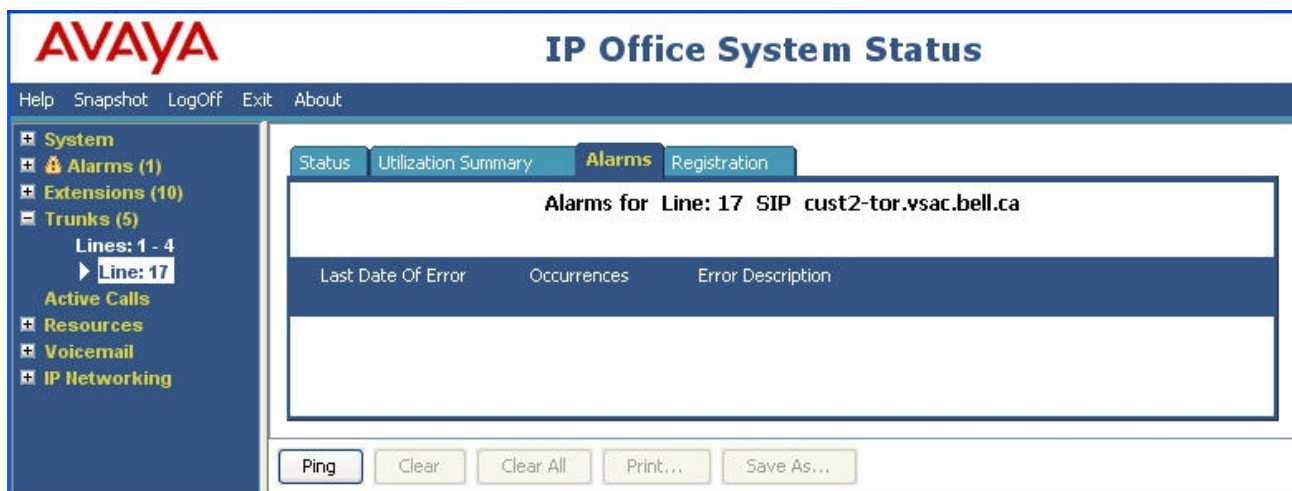
- Peer Domain Name: cust2-tor.vtac.bell.ca
- Resolved Address: 20.20.237.201
- Line Number: 17
- Number of Administered Channels: 10
- Number of Channels in Use: 0
- Administered Compression: Auto
- Silence Suppression: Off
- SIP Trunk Channel Licences: Unlimited
- SIP Trunk Channel Licences in Use: 0
- SIP Device Features: REFER (incoming and outgoing)

A green circle indicates 0% utilization. Below the summary is a table with the following columns: Channel Number, URI, Call Gro, Current State, Time in State, Remote R' Address, Code, Connect Type, Caller ID, Other Party, Direction of Call, Round T Delay, Receive Jitter, Receive Loss Fre, Transmit Jitter, and Transmit Loss Fre. The table contains 10 rows, all showing 'Idle' as the current state and '1 day ...' as the time in state.

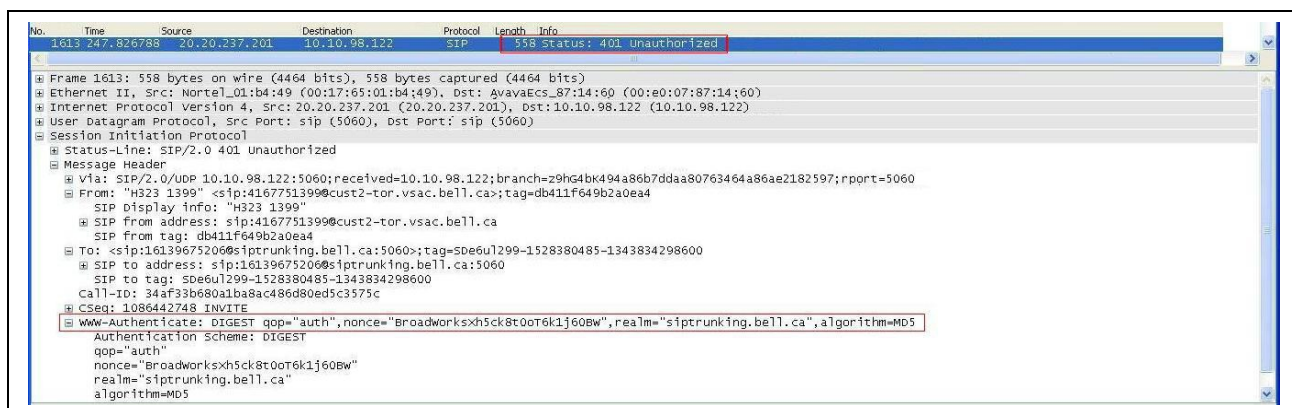
Channel Number	URI	Call Gro	Current State	Time in State	Remote R' Address	Code	Connect Type	Caller ID	Other Party	Direction of Call	Round T Delay	Receive Jitter	Receive Loss Fre	Transmit Jitter	Transmit Loss Fre
1			Idle	1 day ...											
2			Idle	1 day ...											
3			Idle	1 day ...											
4			Idle	1 day ...											
5			Idle	1 day ...											
6			Idle	1 day ...											
7			Idle	1 day ...											
8			Idle	1 day ...											
9			Idle	1 day ...											
10			Idle	1 day ...											

At the bottom of the application, there are buttons for Trace, Trace All, Pause, Ping, Call Details, Print..., and Save As...

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



- ◆ Verify that a phone connected to PSTN can successfully place a call to the Avaya IP Office with two-way audio.
 - ◆ Verify that a phone connected to Avaya IP Office can successfully place a call to the PSTN with two-way audio.
 - ◆ Using a network sniffing tool (e.g., Wireshark), monitor the SIP signaling messages between Bell Canada and Avaya IP Office on an outbound call from the enterprise to the PSTN, and verify the SIP signaling message exchanges for Digest Authentication as shown below:
1. Bell Canada SIP Trunking service returned a “401 Unauthorized” status message to the initial INVITE from the Avaya IP Office, requesting Digest Authentication (see the highlighted **www-Authentication** Header).



2. Avaya IP Office sends an ACK for the 401 message above and then responds by sending a second INVITE containing the highlighted **Authorization** Header supplying the information for successful Digest Authentication.

No.	Time	Source	Destination	Protocol	Length	Info
1618	247.833911	10.10.98.122	20.20.237.201	SIP/SDP	1192	Request: INVITE sip:16139675206@siptrunking.bell.ca:5060, with session description
<div> <div>Session Initiation Protocol</div> <div> <div>Request-Line: INVITE sip:16139675206@siptrunking.bell.ca:5060 SIP/2.0</div> <div>Message Header</div> <div> <div>Via: SIP/2.0/UDP 10.10.98.122:5060;rport;branch=z9hG4bK8325bbb8fdc7c60e7cefd6e77490e562</div> <div>From: "H323 1399" <sip:4167751399@cust2-tor.vtac.bell.ca>;tag=db411f649b2a0ea4</div> <div>SIP Display Info: "H323 1399"</div> <div>SIP from address: sip:4167751399@cust2-tor.vtac.bell.ca</div> <div>SIP from tag: db411f649b2a0ea4</div> <div>To: <sip:16139675206@siptrunking.bell.ca:5060></div> <div>SIP to address: sip:16139675206@siptrunking.bell.ca:5060</div> <div>Call-ID: 344f53b680a1ba8ac486d80ed5c3575c</div> <div>CSeq: 1086442749 INVITE</div> <div>Contact: "H323 1399" <sip:4167751399@10.10.98.122:5060;transport=udp></div> <div>SIP Display Info: "H323 1399"</div> <div>Contact URI: sip:4167751399@10.10.98.122:5060;transport=udp</div> <div>Max-Forwards: 70</div> <div>[truncated] Authorization: Digest username="4167751396",realm="siptrunking.bell.ca",nonce="Broadworksxh5ck8t00t6k1j60Bw",response="8068288d80d39c7de086ef9"</div> <div>Authentication Scheme: Digest</div> <div>username="4167751396"</div> </div> </div> </div>						

8. 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**.

9. Additional References

- [1] IP Office 8.1 Installation, Document number 15-601042 Issue 26j, 19 Sep 2012
- [2] IP Office 8.1 Manager 10.1, Document number 15-601011 Issue 29o, 03 Aug 2012
- [3] IP Office 8.1 Administering Voicemail Pro, Document number 15-601063 Issue 27b, 05 June 2012

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.

10. Change History

Issue	Date	Reason
0.1	3/8/2012	Initial issue

©2012 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.