Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Bell Canada SIP Trunking Service with Avaya IP Office 10.1 (Using SM Line), Avaya Aura Session Manager 7.1 and Avaya Session Border Controller for Enterprise Release 7.2- 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 Release 10.1, Avaya Aura Session Manager 7.1 and Avaya Session Border Controller for Enterprise Release 7.2 using UDP/RTP.

Bell Canada SIP Trunk Service 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.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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.

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between Bell Canada and an Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of Avaya IP Office Release 10.1, Avaya embedded Voicemail, Avaya IP Office Application Server (with WebRTC and one-X Portal services enabled), Avaya Communicator for Windows (SIP mode), Avaya Communicator for Web, Avaya H.323, Avaya SIP, digital and analog deskphones. The enterprise solution connects to the Bell Canada network via the Avaya Aura Session Manager and Avaya Session Border Controller for Enterprise (Avaya SBCE).

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

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office connecting to Bell Canada via the Avaya Aura Session Manager and Avaya SBCE.

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

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

2.1. Interoperability Compliance Testing

A simulated enterprise site with Avaya IP Office using SM Line, Avaya Aura Session Manager and Avaya SBCE was connected to Bell Canada. This setup is recommended only for specific customers who are subscribed to PBX Call-Offloading with Bell Canada and will require the use of SIP Refer (Instead of Re-Invite with Diversion header) for forwards and blind transfers

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

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog phones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog phones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Windows (SIP)
- Inbound and outbound PSTN calls from/to the Avaya Communicator for Web client (WebRTC) with basic telephony transfer feature
- Inbound and outbound long hold time call stability
- Various call types including: local, long distance, outbound toll-free, 411 local directory assistance, 911 emergency call
- SIP transport UDP/RTP between Bell Canada and the simulated Avaya enterprise site
- 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
- Registration/Authentication
- Voicemail navigation for inbound and outbound calls
- Telephony features such as hold and resume, transfer, and conference
- Fax G.711 pass-through and Fax T38 modes
- Off-net call forwarding using SIP Refer
- Off-net call transfer using of SIP Refer
- Twinning to mobile phones on inbound calls

Note: Avaya Communicator for Web client (WebRTC) was tested as part of this solution. The configuration necessary to support Avaya Communicator for Web client is beyond the scope of these Application Notes and is not included in these Application Notes. For these configuration details, see **Reference [11]**.

Item not supported or not tested include the following:

- Bell Canada does not support TLS/SRTP SIP Transport
- Bell Canada does not support the outbound anonymous call using Party Preferred Identity (PPI)

- Inbound toll-free call is supported but was not available for testing during the compliance test
- The outbound international call is supported but was not available for testing during the compliance test

2.2. Test Results

Interoperability testing of Bell Canada was completed with successful results for all test cases with the exception of the observation described below:

- **OPTIONS from Bell Canada** – Bell Canada was configured to send SIP OPTIONS messages with Max-Forwards header with value equal to 0. This was by design from Bell Canada. Avaya SBCE responded correctly with 483 Too Many Hops. However, Bell would accept this and keep the trunk up
- **Call Redirection (Blind/Consultative Transfer using Refer method) using Avaya SIP endpoints** – When performing call transfer off-net using Avaya SIP endpoints, IP Office system responded to a NOTIFY message from Bell with 405 Method Not Allowed. This NOTIFY message was encapsulating the 100 Trying, following the 202 Accepted. Even though Avaya SIP endpoints displayed "Transfer Failed". The call was being transferred successfully with two-way audio.
- **Bell Canada rejected the anonymous outbound call using Party Preferred Identity (PPI) header and "privacy: id" -** For the anonymous outbound call, IP Office was designed to use SM line to send PPI header with valid DID number instead of Party Asserted Identity (PAI) header. This is IP Office behavior and is not configurable. Bell Canada verified PAI header and rejected the anonymous call. Bell Canada did not verify the PPI header. This was reported to Avaya R&D.
- **We could not define the SIP URI of FROM, CONTACT, PAI, PPI and Diversion headers when using SM Line -** There is no configuration available for SM Line to configure From, Contact, PPI and PAI headers. It is only available in SIP Lines. During the compliance testing, SIP URI Manipulation on Avaya SBCE was used to modify the URI of headers (See **Section 7.2.2**). This was reported to Avaya R&D.
- **IP Office using SM Line does not add the Diversion header for responses, UPDATE and re-Invite's in off-net call forward -** As designed, IP Office using SM Line does not add the Diversion header for responses, UPDATE and re-Invite's in off-net call forward. IP Office used SIP Refer method instead. In order to make off-net call forward work, Bell Canada has to make sure the customer supports SIP Refer before the SIP trunk is implemented. This was reported to Avaya R&D.
- **For off-net transfer/forward calls, the actual functionality of SIP was observed to be always as a consultative transfer -** The observation was that a second INVITE is established for the outbound call and then always followed by a REFER with replaces. The call was being transferred/forwarded successfully with two-way audio. This was reported to Avaya R&D.

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 https://business.bell.ca/shop/enterprise/sip-trunking-service

3. Reference Configuration

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

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

- Avaya IP Office 500V2
- Avaya embedded Voicemail for IP Office
- Avaya Application Server (Enabled WebRTC and one-X Portal services)
- Avaya Aura System Manager
- Avaya Aura Session Manager
- Avaya Session Border Controller for Enterprise
- Avaya 9600 Series IP Deskphones (H.323)
- Avaya 11x0 Series IP Deskphones (SIP)
- Avaya 1408 Digital phones
- Avaya Analog phones
- Avaya Communicator for Windows (SIP)
- Avaya Communicator for Web (WebRTC)

Located at the enterprise site is an Avaya IP Office 500V2 with the MOD DGTL STA16 expansion module which provides connections for 16 digital stations to the PSTN, and the extension PHONE 8 card which provides connections for 8 analog stations to the PSTN as well as 64-channel VCM (Voice Compression Module) for supporting VoIP codecs. The voicemail service is embedded on Avaya IP Office. Endpoints include Avaya 9600 Series IP Telephone (with H.323 firmware), Avaya 1100 Series IP Telephone (with SIP firmware), Avaya 1408D Digital Telephones, Avaya Analog Telephone, Avaya Communicator for Windows and Avaya Communicator for Web Client.

The LAN2 port of Avaya IP Office was connected to Avaya Aura Session Manager while the LAN1 port was not used during the compliance test. The Avaya SBCE internal interface was connected to Avaya Aura Session Manager, while the Avaya SBCE external interface was connected to public internet.

A separate Windows 10 Enterprise PC runs Avaya IP Office Manager to configure and administer Avaya IP Office system.

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

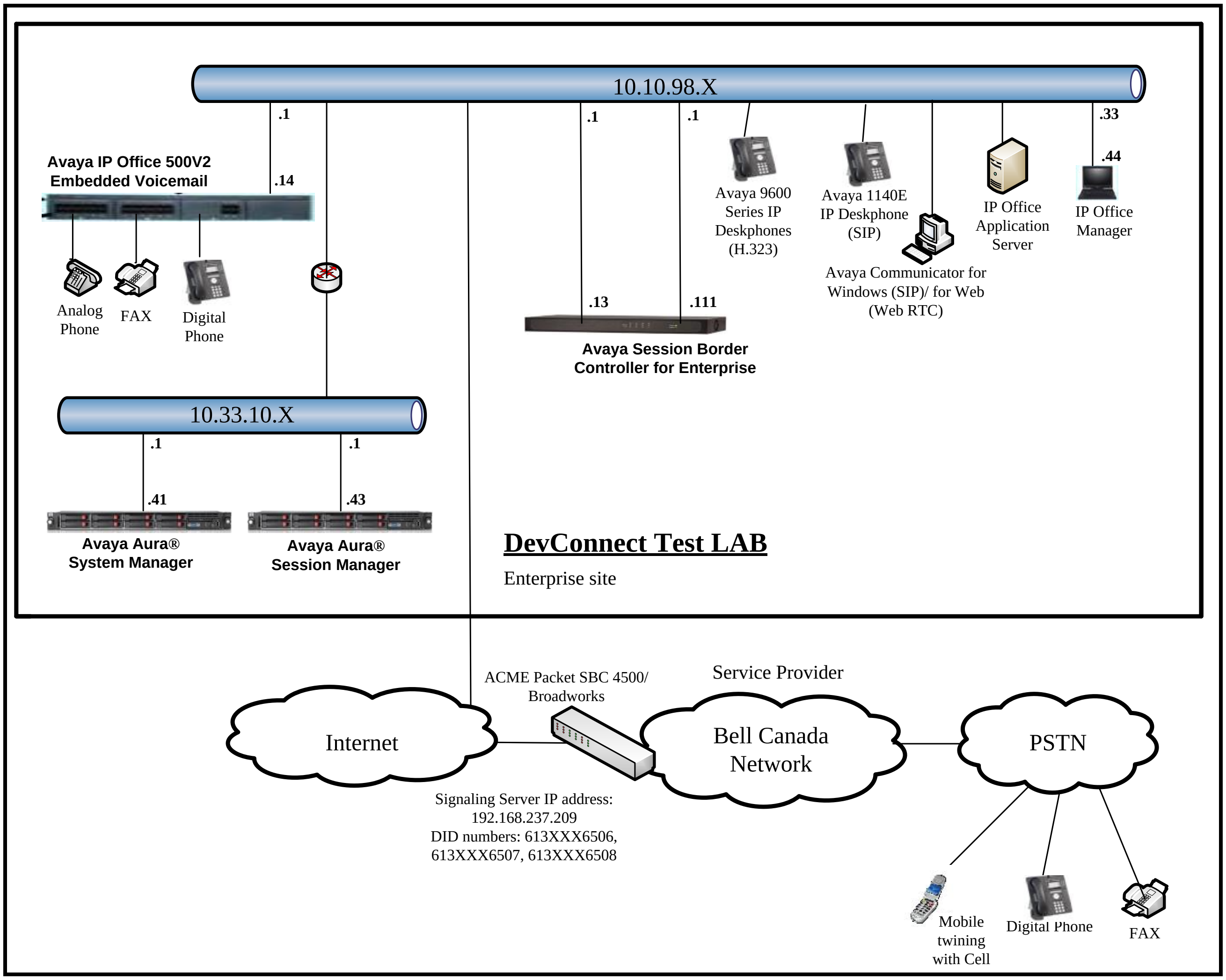

Figure 1 - Test Configuration for Avaya IP Office with Bell Canada SIP Trunk Service

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 sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and Avaya SBCE, such as a data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and Avaya SBCE 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 solution ▪ Avaya IP Office 500V2 ▪ Embedded Voicemail ▪ Avaya Web RTC Gateway ▪ Avaya one-X Portal ▪ Avaya IP Office Manager ▪ Avaya IP Office Analogue PHONE 8 ▪ Avaya IP Office VCM64/PRID U ▪ Avaya IP Office DIG DCPx16 V2	 10.1.0.1.0 build 3 10.1.0.1.0 build 3 10.1.0.1.0 build 3 10.1.0.1.0 build 3 10.1.0.1.0 build 3 10.1.0.1.0 build 3 10.1.0.1.0 build 3 10.1.0.1.0 build 3
Avaya Session Border Controller for Enterprise	7.2.1-05-14222
Avaya Aura System Manager	7.1.2 Build no 7.1.0.0.1125193 Software Update Revision No: 7.1.2.0.057353 FP2
Avaya Aura Session Manager	7.1.2.0.712004
Avaya 1140E IP Deskphone (SIP)	04.04.23
Avaya 9641G IP Deskphone	6.6.4.01
Avaya 9621G IP Deskphone	6.6.4.01
Avaya Communicator for Windows (SIP)	2.1.4.0 - 256
Avaya Communicator for Web	1.0.17.1725
Avaya 1408D Digital Deskphone	R46
Avaya Analog Deskphone	N/A
HP Officejet 4500 (fax)	N/A
Bell Canada Components	
Equipment	**Release**
ACME Packet SBC 4500	7.4.0 MR1 P6
Broadworks	20 SP1.1.606

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500V2 and also when deployed with IP Office in all configurations.

5. Configure Avaya IP Office Solution

This section describes the Avaya IP Office solution configuration necessary to support connectivity to the Avaya Aura Session Manager. It is assumed that the initial installation and provisioning of the Avaya IP Office 500V2 has been previously completed and therefore is not covered in these Application Notes. For information on these installation tasks refer to Additional References **Section 11**.

This section describes the Avaya IP Office configuration required to support connectivity to the Avaya Aura Session Manager. 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 click **OK** button. Log in using appropriate credentials.

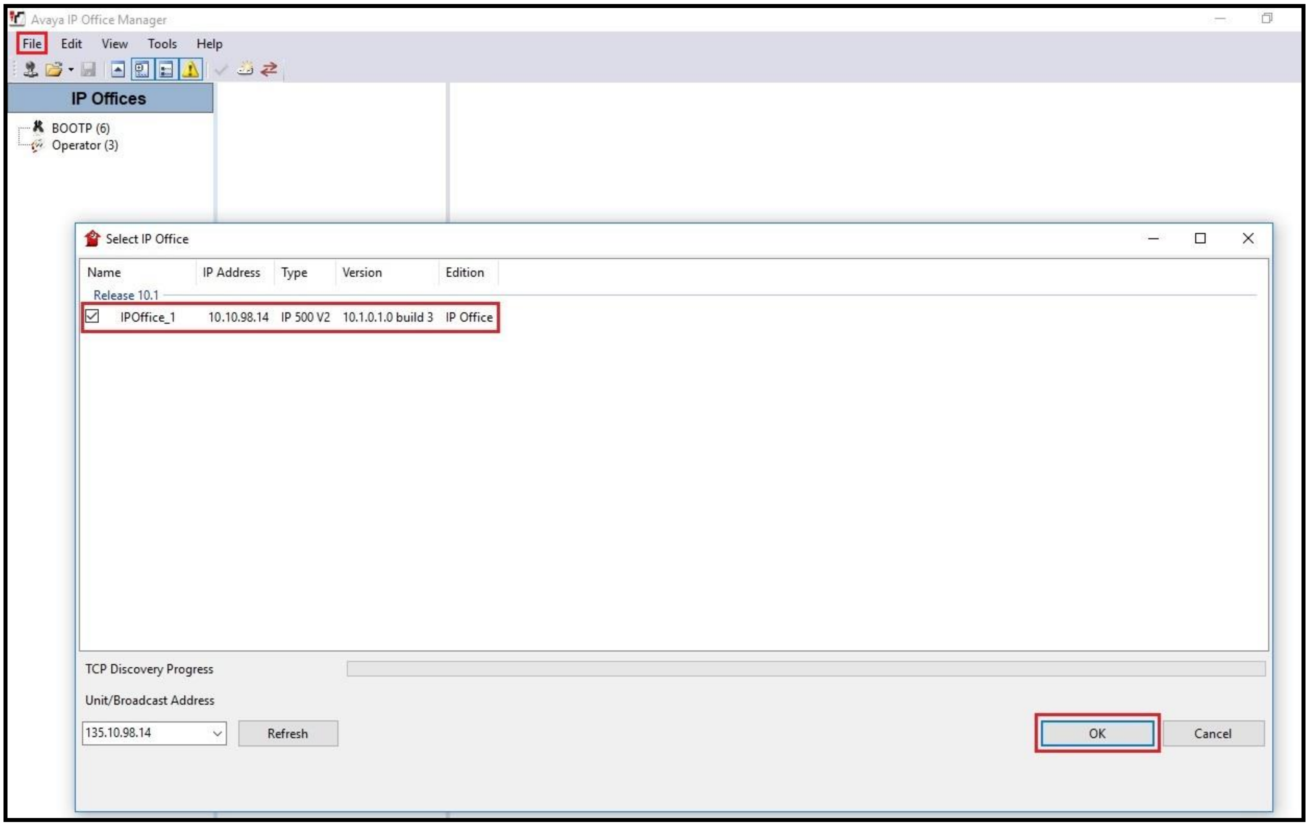

Figure 2 – Avaya IP Office Selection

5.1. Licensing

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

To verify that there is a SIP Trunk Channels license with sufficient capacity, select **IPOffice_1 → License** on the Navigation pane and **SIP Trunk Channels** in the Group pane. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the **Details** pane.

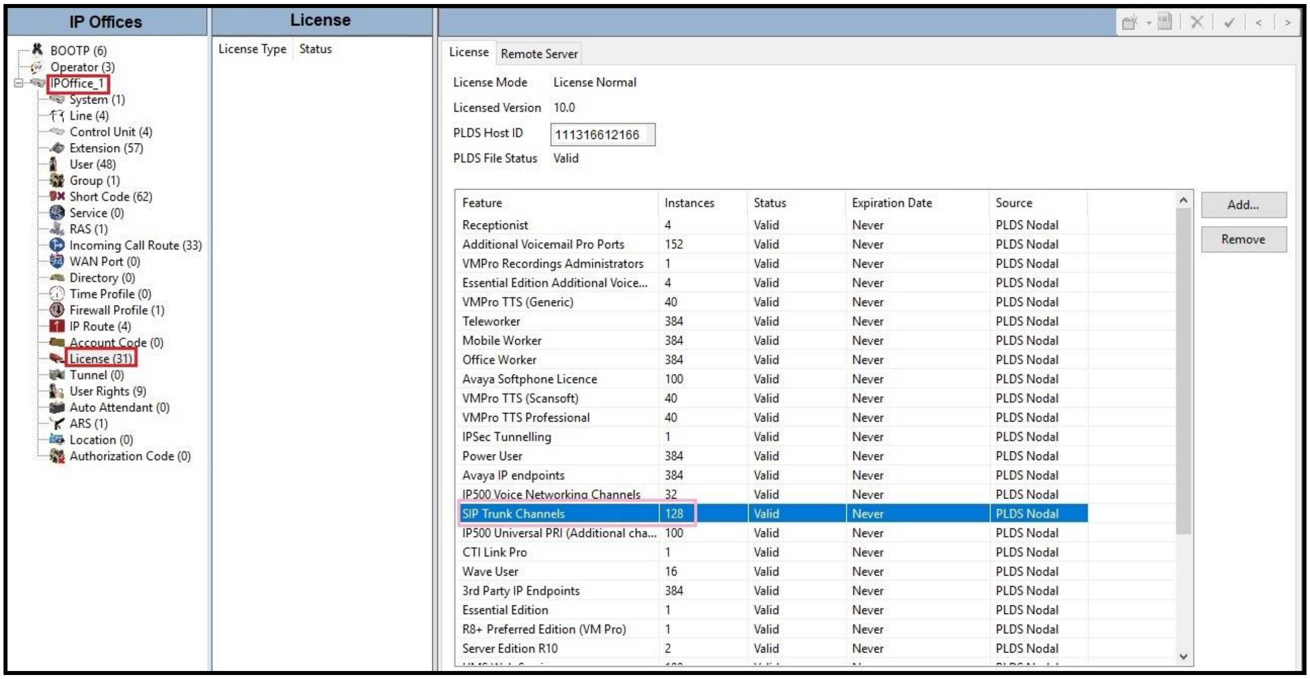

Figure 3 – Avaya IP Office License

5.2. System Tab

Navigate to **System (1)** under **IPOffice_1** on the left pane and select the **System** tab in the **Details** pane. The **Name** field can be used to enter a descriptive name for the system. In the reference configuration, **IPOffice_1** was used as the name in IP Office.

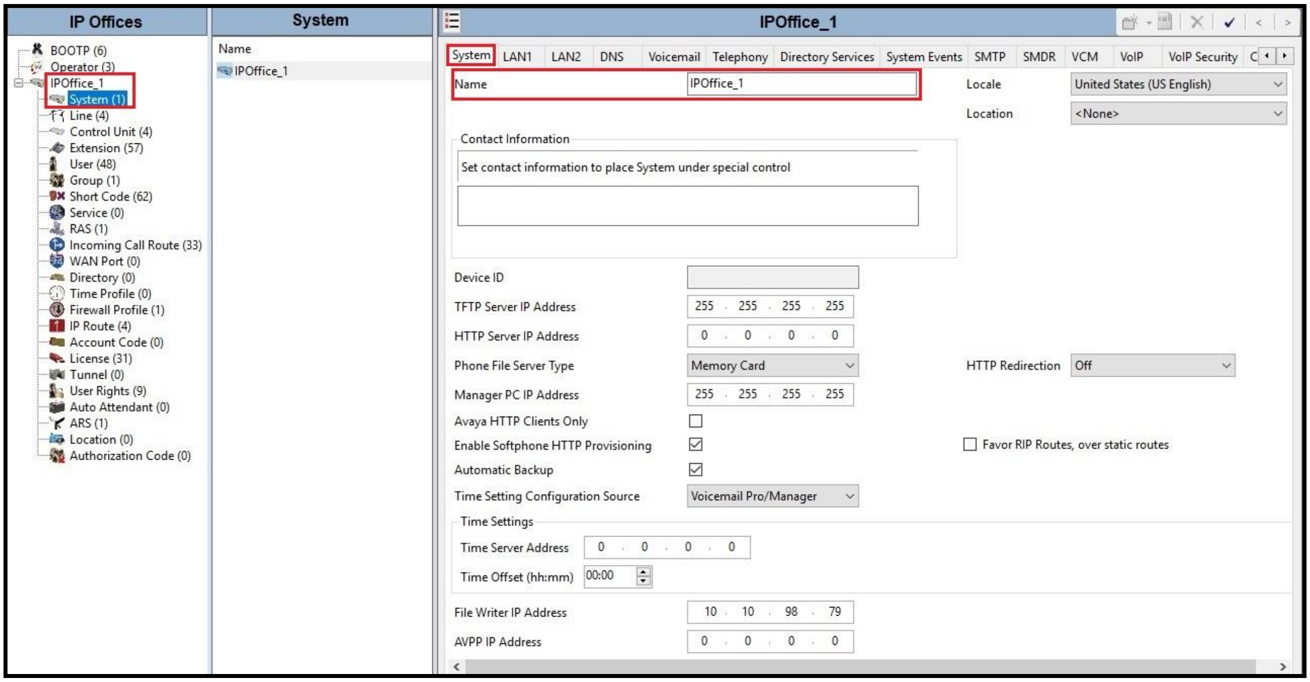

Figure 4 - Avaya IP Office System Configuration

5.3. LAN2 Settings

In the sample configuration, LAN2 is used to connect the enterprise network to Avaya Session Manager.

To configure the LAN2 settings on the IP Office, complete the following steps. Navigate to **IPOffice_1 → System (1)** in the **Navigation** and **Group** panes and then navigate to the **LAN2 → LAN Settings** tab in the **Details** pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office LAN2 port. Set the **IP Mask** field to the mask used on the private network. All other parameters should be set according to customer requirements. Click **OK** to submit the change.

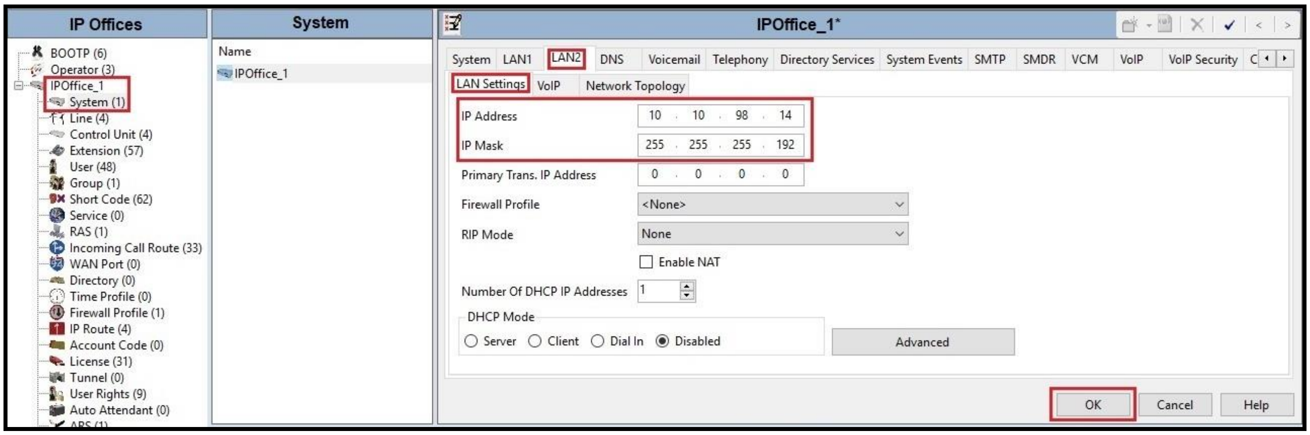

Figure 5 - Avaya IP Office LAN2 Settings

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

- Check the **H323 Gatekeeper Enable** to allow Avaya IP deskphones/softphones using the H.323 protocol to register
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Bell Canada via Avaya Session Manager and Avaya SBCE
- Check the **SIP Registrar Enable** to allow Avaya IP deskphones/softphones to register using the SIP protocol
- Input **SIP Domain Name** as **bvwdev.com**
- The **Layer 4 Protocol** uses **TLS** with **TLS Port** as **5061**
- Verify **Keepalives** to select **Scope** as **RTP-RTCP** with **Periodic timeout 60** and select **Initial keepalives** as **Enabled**
- All other parameters should be set according to customer requirements
- Click **OK** to submit the changes

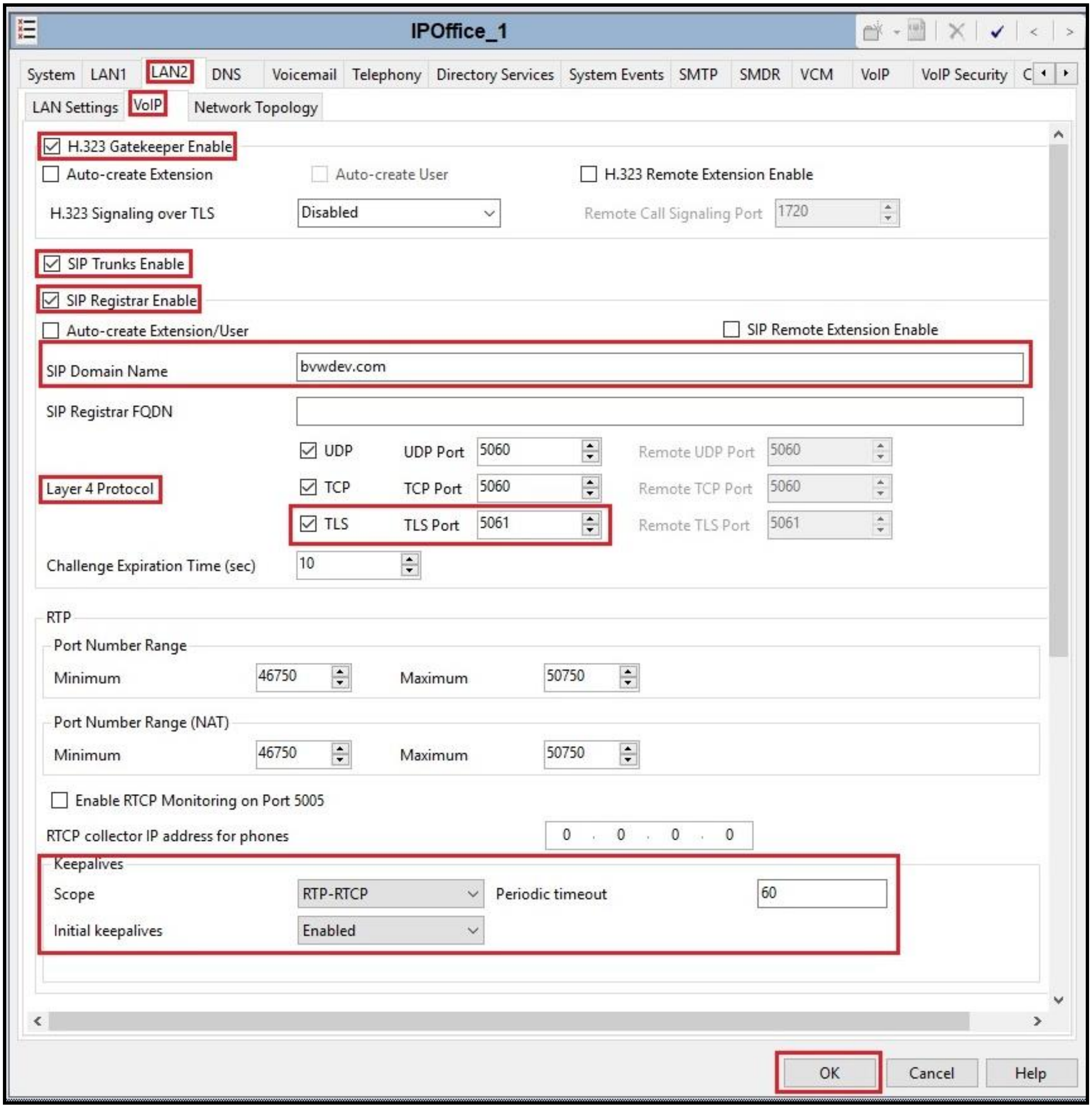

Figure 6 - Avaya IP Office LAN2 VoIP

5.4. System Telephony Settings

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes (not shown) and then navigate to the **Telephony → Telephony** tab in the **Details** pane. Choose the **Companding Law** typical for the enterprise location. For North America, **U-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the service provider across the SIP trunk. Set **Hold Timeout (sec)** to a valid number. Set **Default Name Priority** to **Favor Trunk**. Defaults were used for all other settings. Click **OK** to submit the changes.

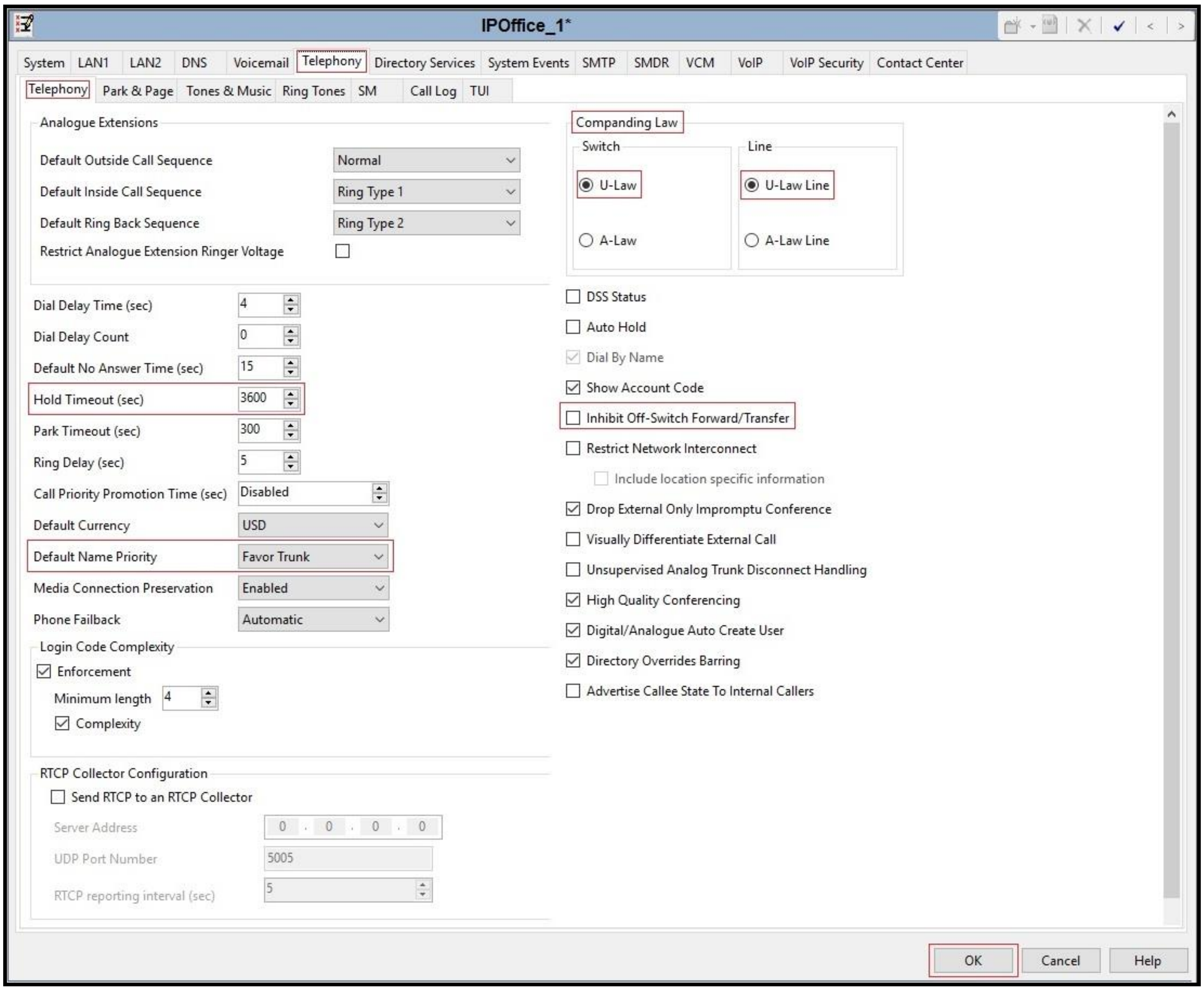

Figure 7 - Avaya IP Office Telephony

5.5. System VoIP Settings

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **VoIP** tab in the **Details** pane. Leave the **RFC2833 Default Payload** as default of **101**. Select codec **G.711 ULAW 64K**, **G.729(a) 8K CS-ACEL**P which Bell Canada supports. Click **OK** to submit the changes.

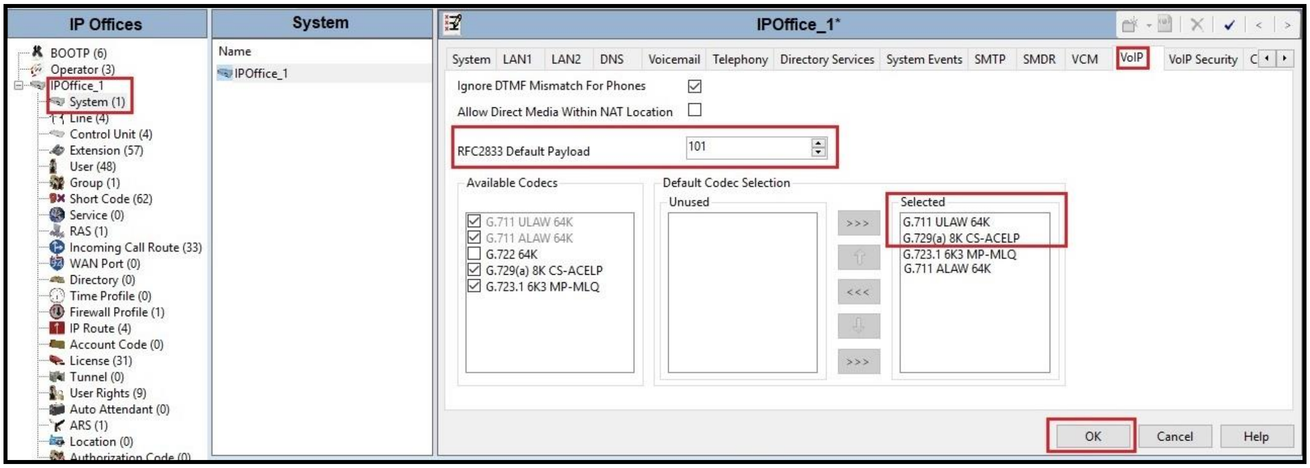

Figure 8 - Avaya IP Office VoIP

Navigate to **IPOffice_1 → System (1)** in the Navigation and Group Panes and then navigate to the **VoIP Security** tab in the **Details** pane. Select **Media** as **Preferred** and select **Media Security Options** as highlights. Click **OK** to submit the changes.

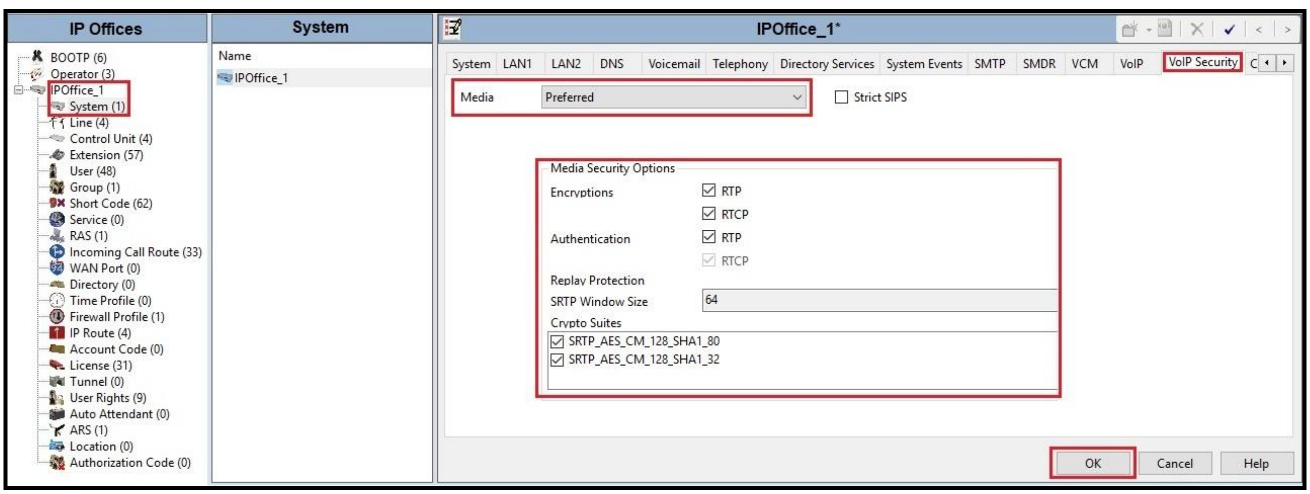

Figure 9 - Avaya IP Office VoIP Security

5.6. Administer SM Line

A SM Line is needed to establish the SIP connection between Avaya IP Office and Avaya Aura Session Manager.

To create a SM line, begin by navigating to **Line** in the left Navigation Pane, then right-click in the Group Pane and select **New → SM Line** (not shown). For the compliance test, SM Line 18 was used as trunk for both outgoing and incoming calls.
Note: There is no configuration available for SM Line to configure From, Contact, PPI, PAI and Diversion headers. It is only available in SIP Lines. In this compliance testing, we used URI manipulation of Server Interworking and SIP Manipulation on SBCE to modify the URI of headers.

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

- Select available **Line Number**: **18**
- Check **In Service** box
- Set **SM Domain Name** to **bvwdev.com**. This field is used to specify the domain name of Avaya Aura Session Manager.
- Set **SM Address** to IP address of Avaya Aura Session Manager.
- Set **Max Calls** to the number of simultaneous SIP calls that are allowed.
- The **Outgoing Group ID** is set to **98888** by default
- Set **URI Type** to **SIP**
- In the **Network Configuration** area, **TLS** was selected as the **Layer 4 Protocol** and the **Send Port** and **Listen Port** were set to **5061**. These values should be matched to the protocol and port on Session Manager (See **Section 6.6** in details)
- Default values may be used for all other parameters
- Click **OK** to commit then press Ctrl + S to save

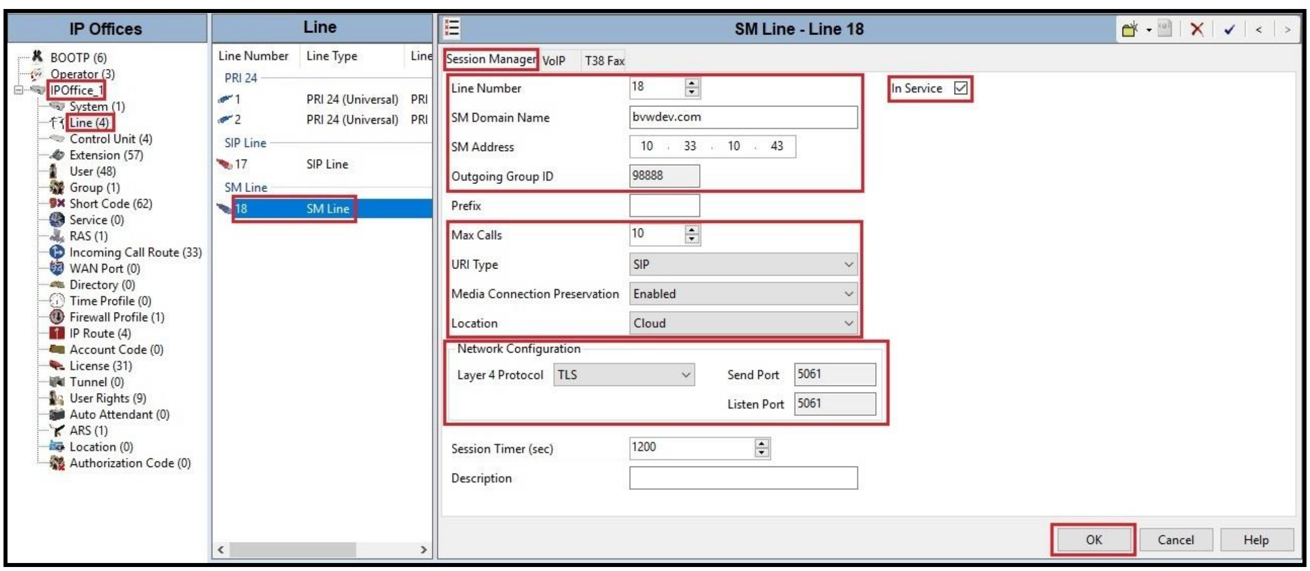

Figure 10 – SM Line Configuration

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

- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. The **G.711 ULAW 64K** and **G.729(a) 8K CS –ACELP** codecs are selected. Avaya IP Office supports these codecs, which are sent to Bell Canada, in the Session Description Protocol (SDP) offer, in that order
- Check the **Re-invite Supported** box
- Set **Fax Transport Support** to **G.711** or **T38** from the pull-down menu. Note: Bell Canada supported both Fax G.711 pass-through and Fax T.38 modes during the compliance testing
- Set the **DTMF Support** to **RFC2833** from the pull-down menu. This directs Avaya IP Office to send DTMF tones using SRTP events messages as defined in RFC2833.
- Set **Media Security** as **Same as System (Preferred)**. Check **Same As System** box
- Default values may be used for all other parameters
- Click **OK** to submit the changes

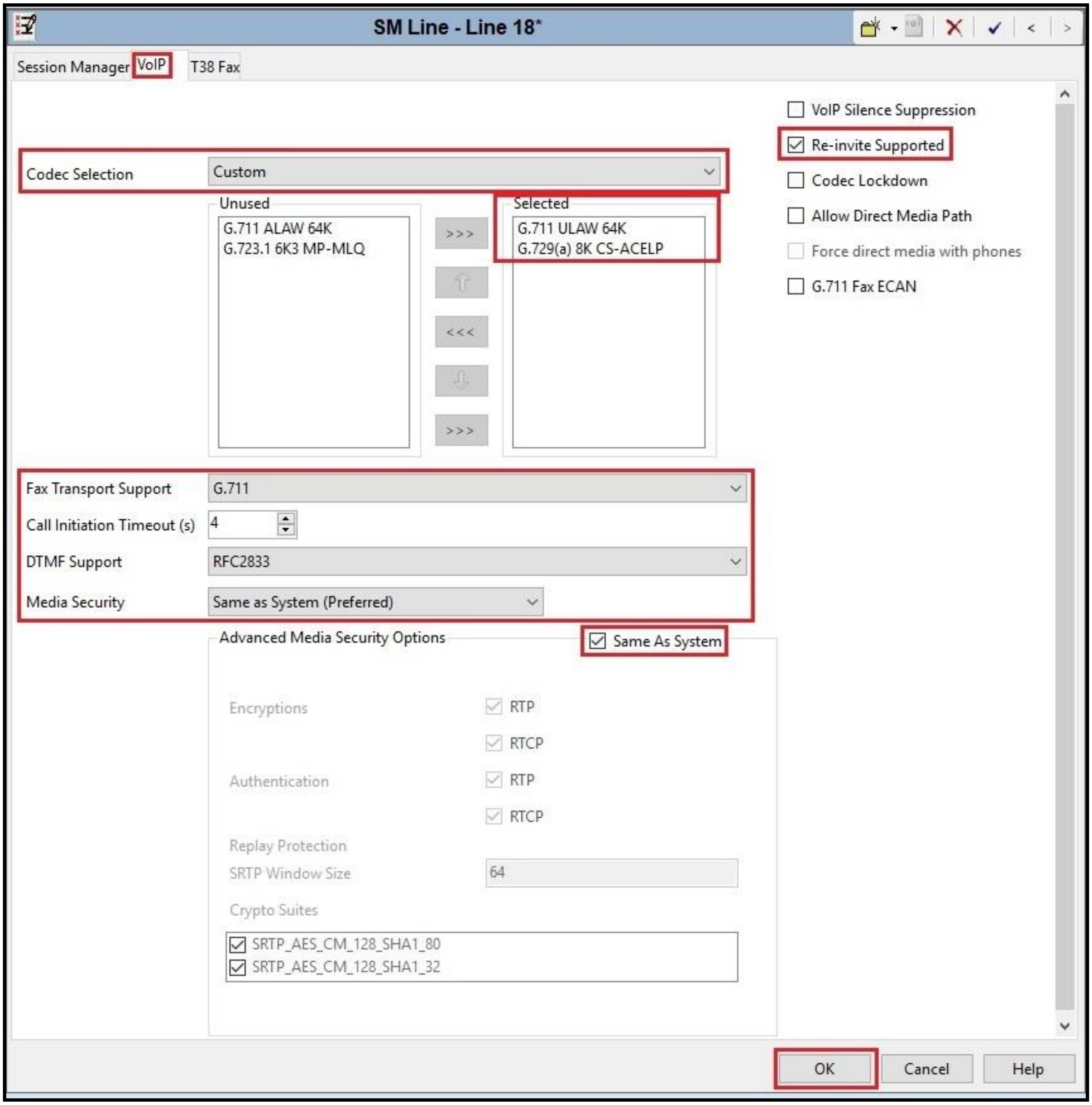

Figure 11 – SM Line VoIP Configuration

Select the **T38 Fax** tab to set the Fax T.38 parameters of the SM line. Note: Whenever T38 is selected for **Fax Transport Support** on **VoIP** tab, T38 Fax tab will be active for configuring the parameters. Set the parameters as shown below:

- Uncheck **Use Default Values** box
- Change **T38 Fax Version** to **0**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

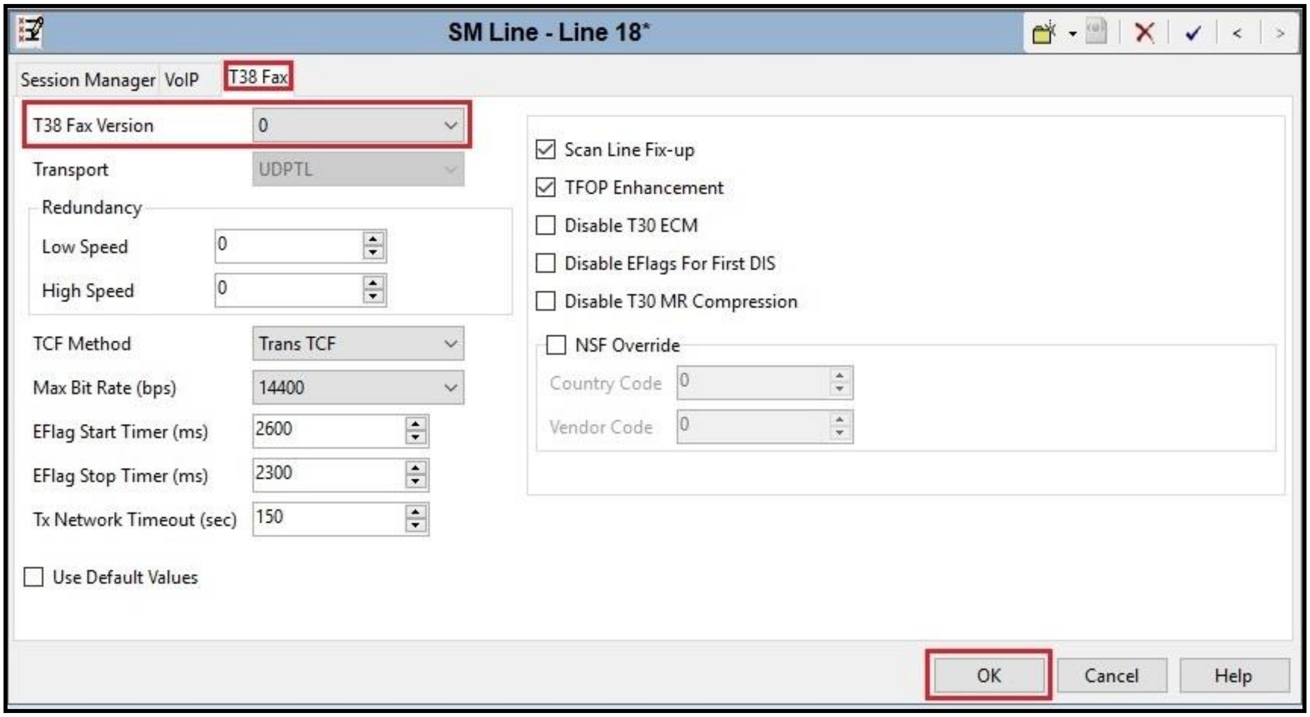

Figure 12 – SM Line T38 Fax Configuration

5.7. Short Code

Define a short code to route outbound traffic on the SM line to Bell Canada via Avaya Aura Session Manager and Avaya SBCE. 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 action that the short code will perform
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user
- Set the **Line Group ID** to **98888**. This is **Outgoing Group ID** defined on **SM Line → Session Manager** tab. This short code will use this line group when placing the outbound call
- Set the **Locale** to **United States (US English)**
- Default values may be used for all other parameters
- Click **OK** to submit the changes

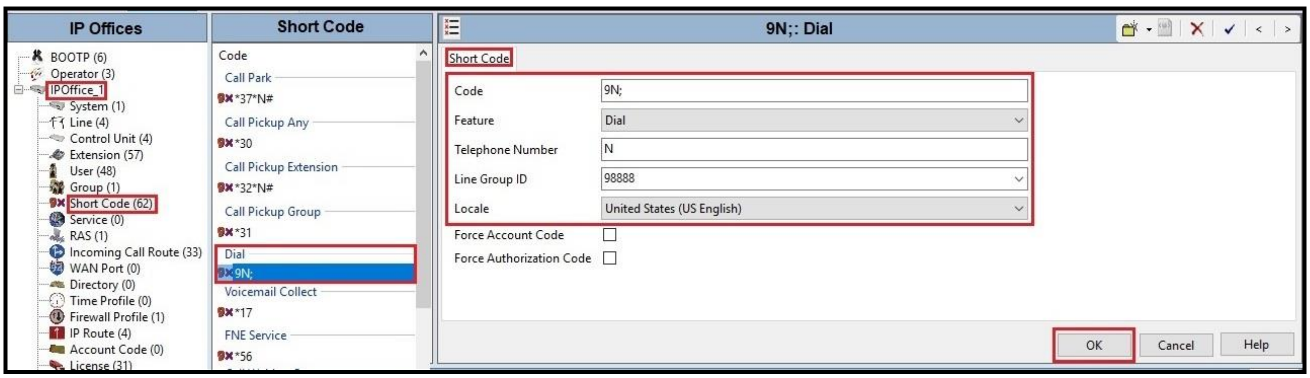

Figure 13 – Short Code 9N

The feature of incoming calls from mobility extension to idle-appearance FNE (Feature Name Extension) is hosted by Avaya IP Office. The Short Code ***56** was configured with following parameters:

- For **Code** field, enter FNE feature code as ***56** for dial tone
- Set **Feature** to **FNE Service**
- Set **Telephone Number** to **FNE00**
- Set **Line Group ID** to **0**
- Default values may be used for other parameters
- Click **OK** to submit the changes

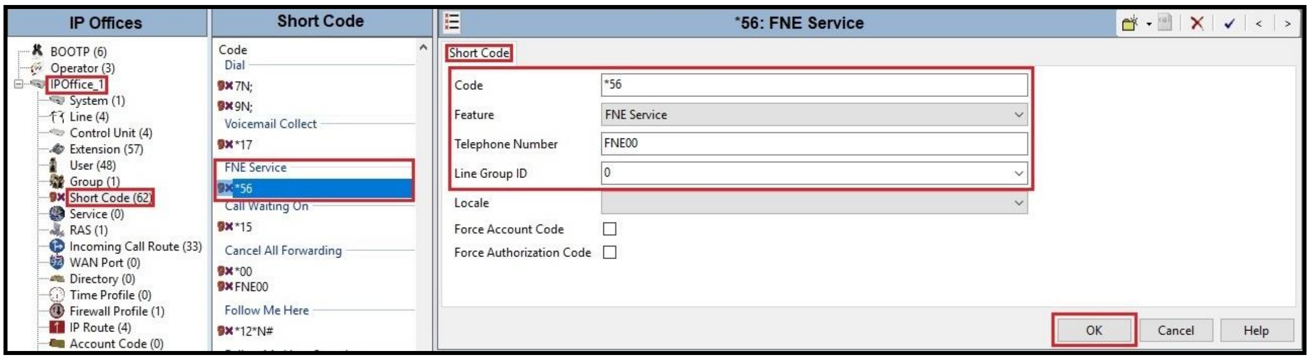

Figure 14 – Short Code for FNE

The feature of incoming calls to Voice Mail is hosted by Avaya IP Office. The Short Code ***17** was configured with following parameters:

- For **Code** field, enter Voicemail Collect feature code as ***17** for dial tone
- Set **Feature** to **Voicemail Collect**
- Set **Telephone Number** to **"?"U**
- Set **Line Group ID** to **0**
- Default values may be used for other parameters
- Click **OK** to submit the changes

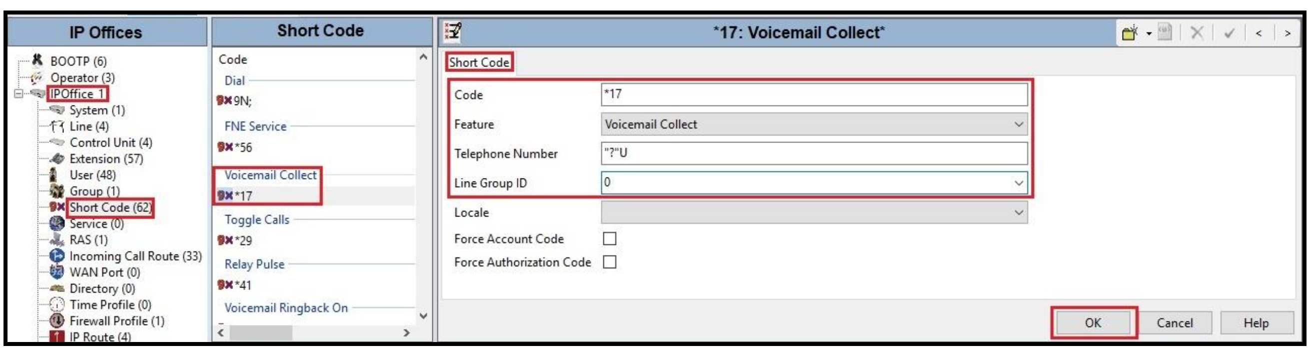

Figure 15 – Short Code for Voice Mail

5.8. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SM Line defined in **Section 5.6**. 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 **613XXX6506**. Select the **User** tab in the Details pane.

The values entered for the **Name** as **613XXX6506** are used to match of the SIP URI for incoming calls. The values entered for the **Extension** as **6506** are used as the user part of the SIP URI in the From, Contact, PAI headers for outgoing calls

The example below shows the settings for user **613XXX6506**. The **Name** is set to one of the DID numbers assigned to the enterprise provided by Bell Canada.

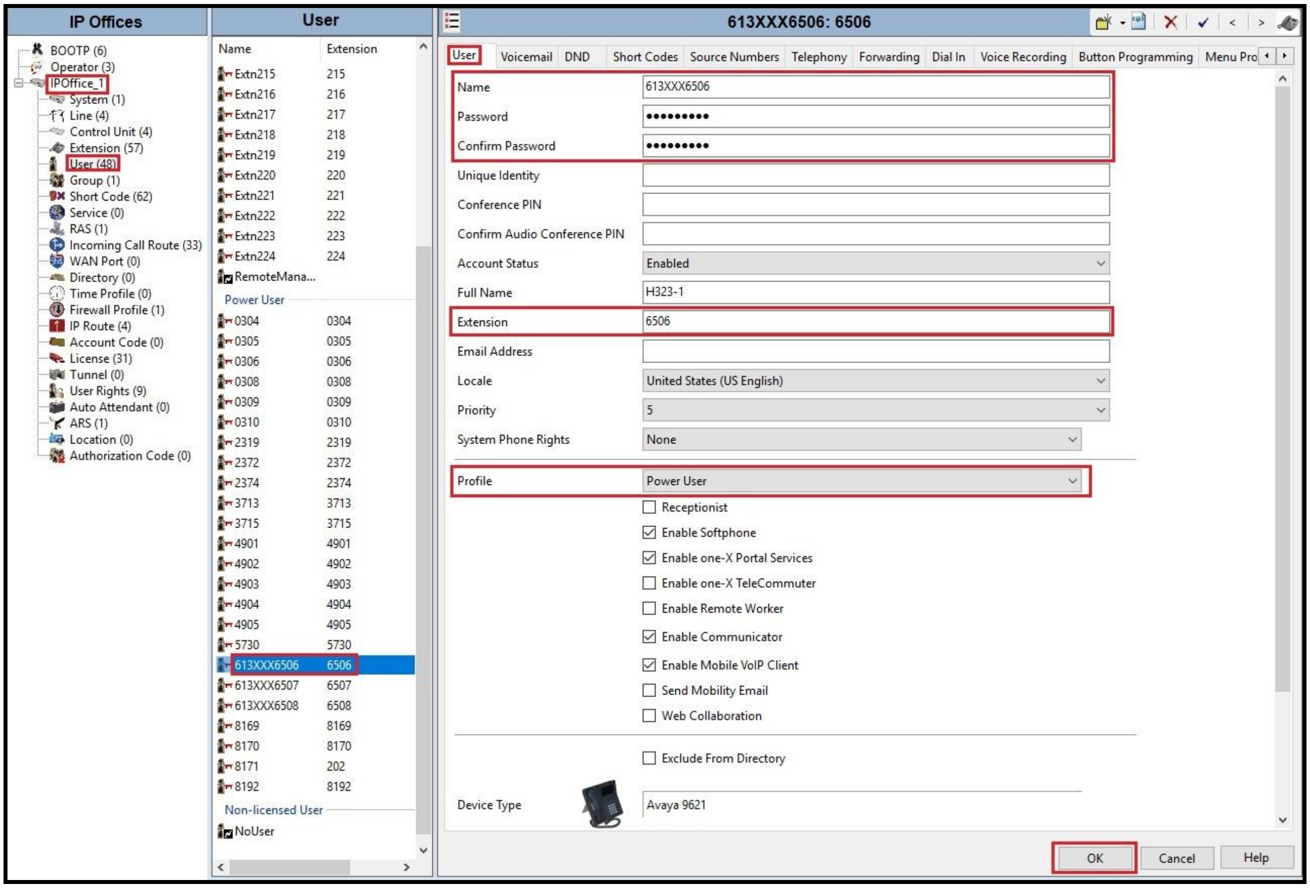

Figure 16 – User Configuration

If all calls involving this user and a SM Line should be considered private, then a short code for specific user should be defined to withhold the user's information from the network.

To create a Short Code for User, select **User** in the left Navigation Pane, then select a specific user. On the **Short Codes** tab in the Details Pane, configure the parameters for the new short code. The screen below shows the details of the previously administered short code used in the test configuration.

- **Code** is set to **9N;**
- **Telephone Number** is set to **WN**
- **Feature** is set to **Dial**
- **Line Group ID** is set to **98888**

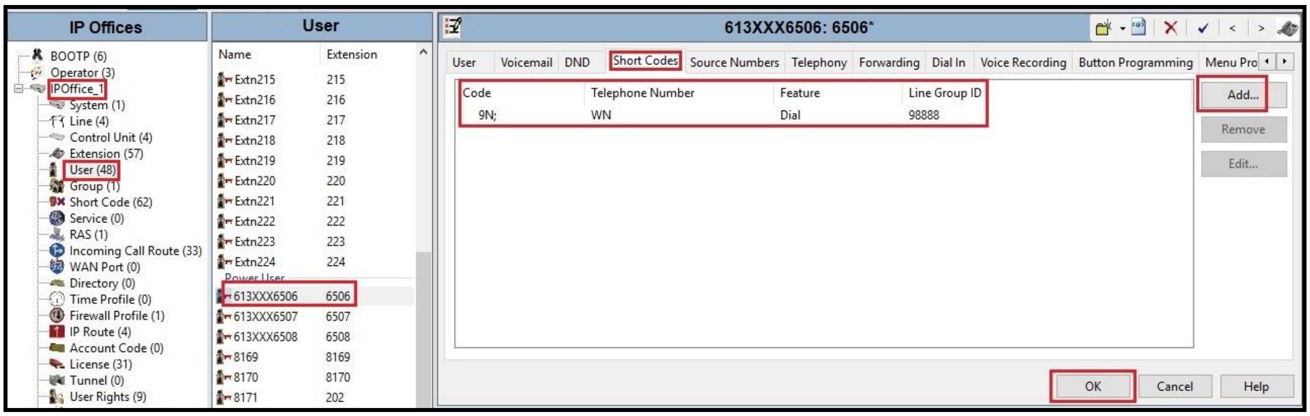

Figure 17 – User Configuration for anonymous outbound call

Note: For the anonymous outbound call, IP Office was designed to use SM line to send PPI header with valid DID number instead of PAI header. This is IP Office behavior and is not configurable. (See **Section 2.2** for more details)

One of the H.323 IP Deskphones at the enterprise site uses the Mobile Twinning feature. The following screen shows the **Mobility** tab for User 613XXX6506. 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 **91613XXX3648**. Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (defined in **Section 5.7**). Other options can be set according to customer requirements.

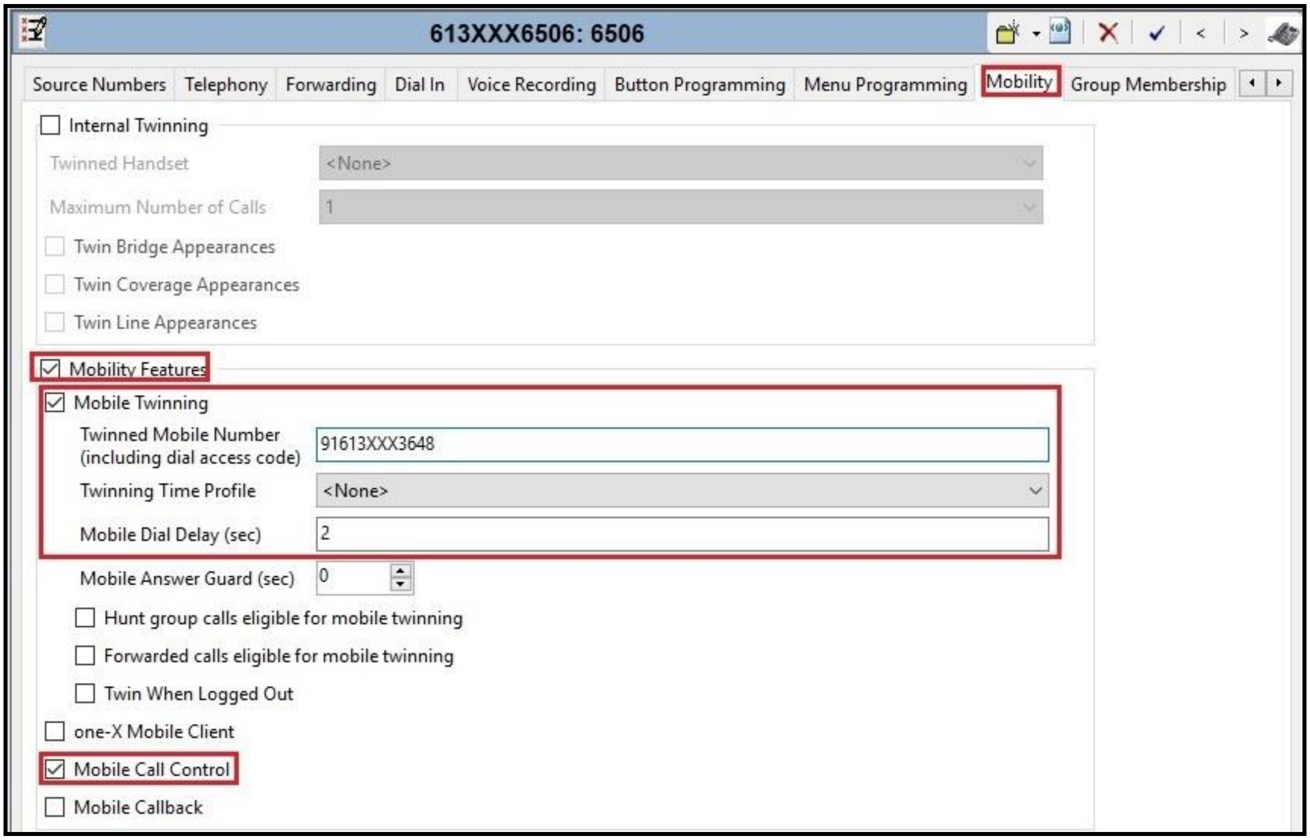

Figure 18 – Mobility Configuration for User

5.9. Save Configuration

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

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Avaya IP Office, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which define route destinations and control call routing between the SIP Entities
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call

It may not be necessary to create all the items above when configuring a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP Domains, Locations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as **https://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

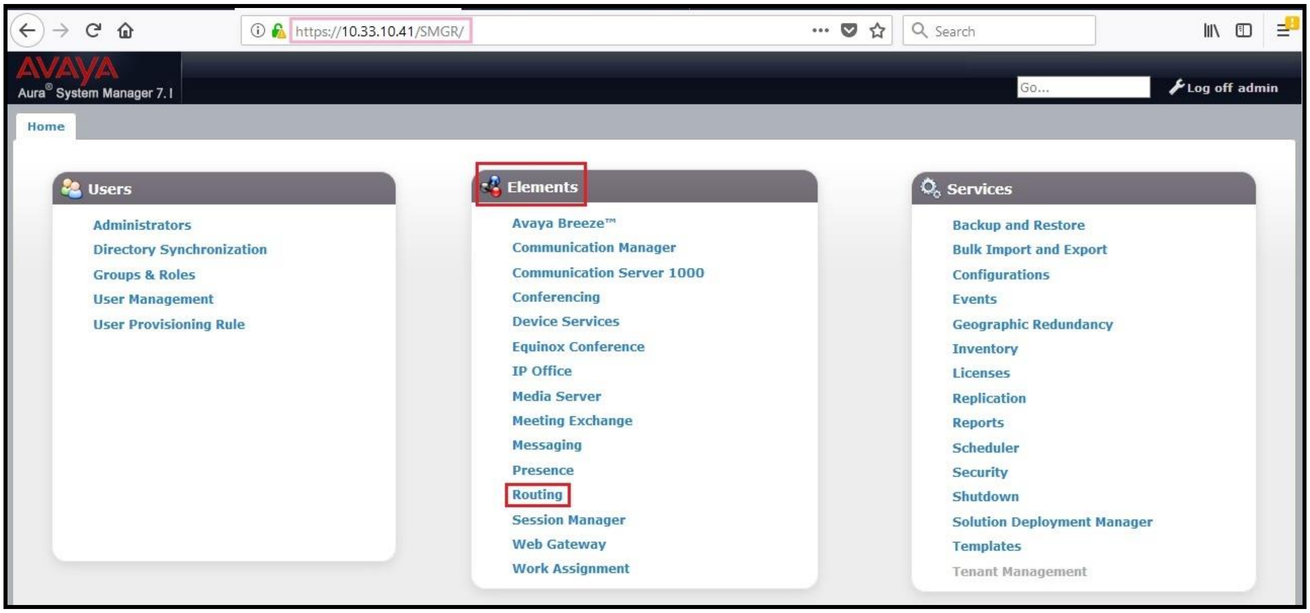

Figure 19: System Manager Home Screen

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

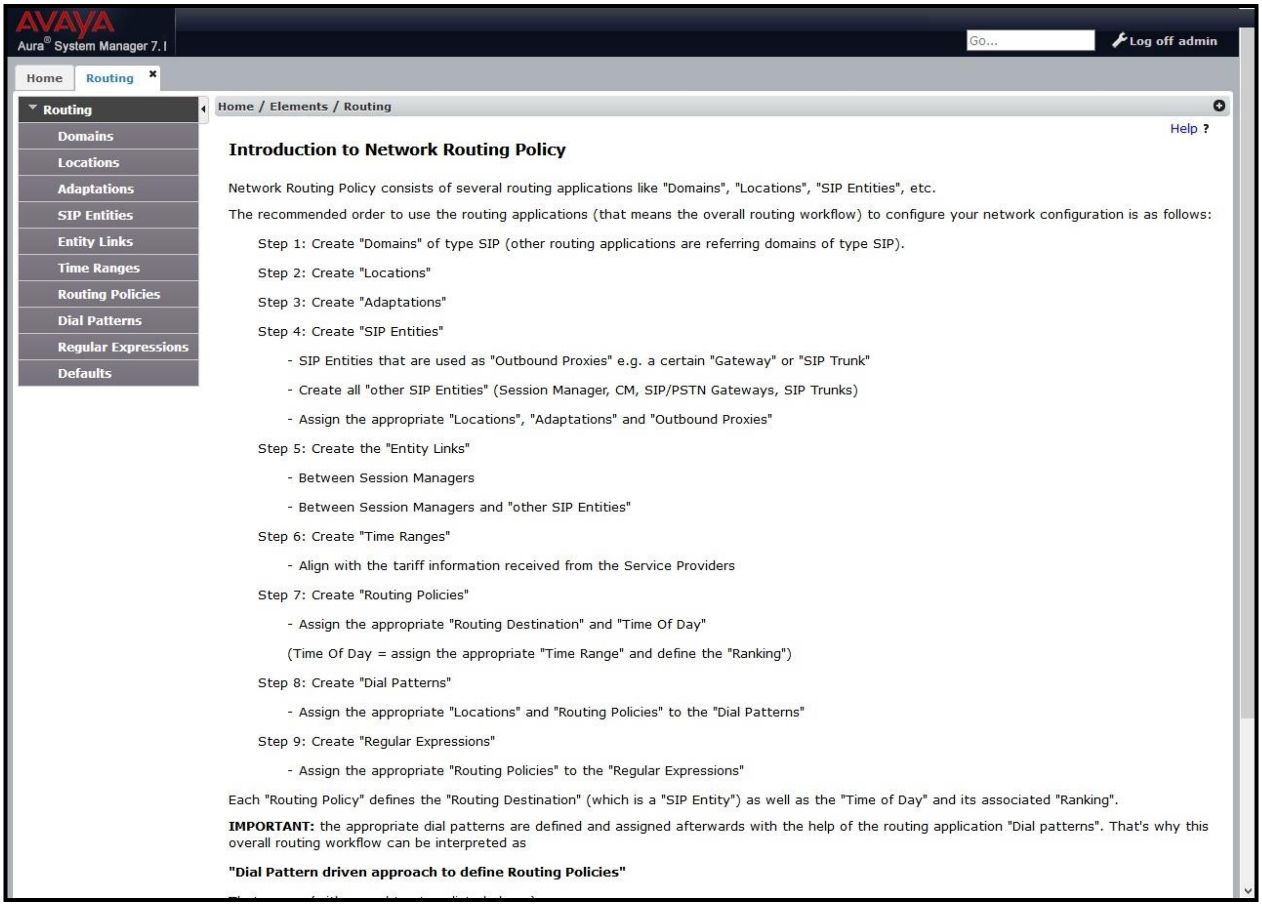

Figure 20: Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev.com**.

Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), fill in the following:

- **Name**: Enter the domain name
- **Type**: Select **sip** from the pull-down menu
- **Notes**: Add a brief description (optional)

Click **Commit** (not shown) to save.

The screen below shows the existing entry for the enterprise domain.

Figure 21: Domain Management

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville-GSSCP**, which includes all equipment in the enterprise including IP Office, Session Manager and Avaya SBCE.

To add a Location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name for the Location
- **Notes:** Add a brief description (optional)

Click **Commit** to save

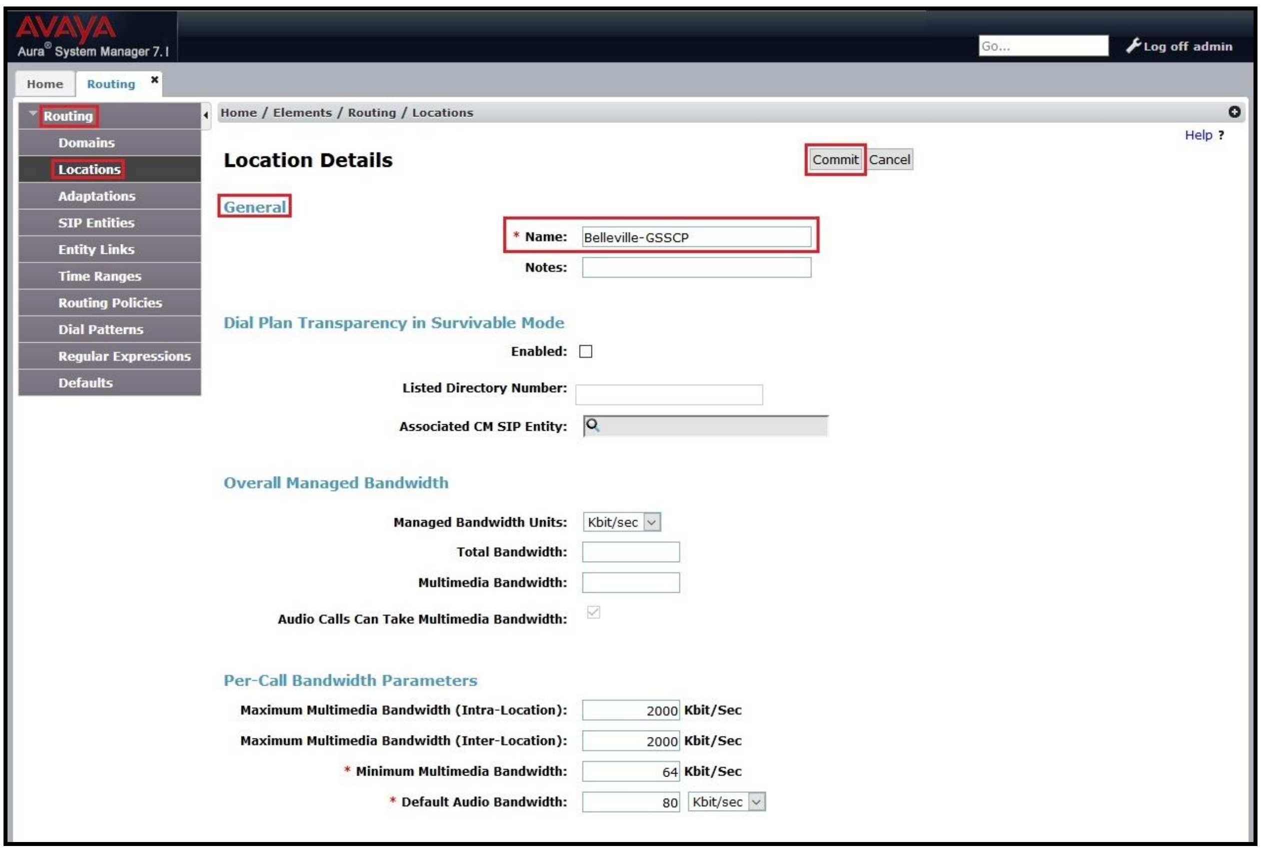

Figure 22: Location Configuration

In the **Location Pattern** section, click **Add** to enter **IP Address Pattern**. The following patterns were used in testing:

- **IP Address Pattern**: **10.33.10.***, **10.33.5.***, **10.10.98.***
- Click **Commit** to save

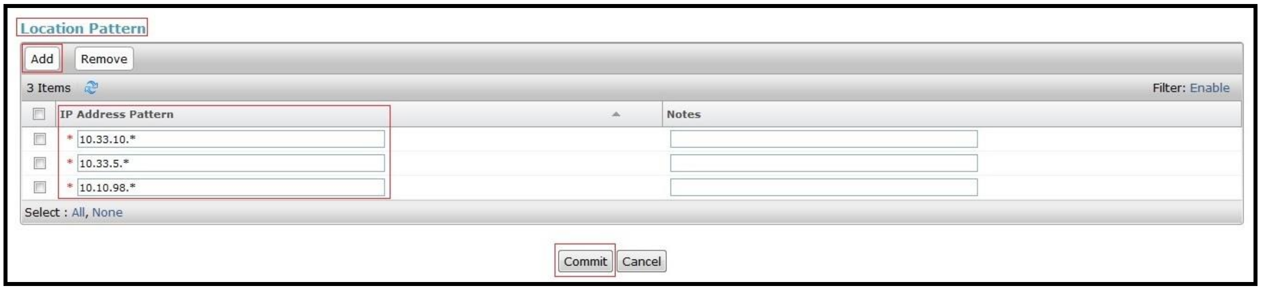

Figure 23: IP Ranges Configuration

Note: Call bandwidth management parameters should be set per customer requirement.

6.4. Configure Adaptations

An adaptation to IP Office is configured to delete + sign on user URI of any inbound calls. This adaptation is also configured to convert inbound calls to FNE Service or VoiceMail which is hosted by IP Office.

To add a new adaptation, select **Routing → Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the adaptation. Select **DigitConversionAdapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu

Click **Add** button and enter **Name** as **fromto** and **Value** as **true**

Click **Add** button under **Digit Conversion for Outgoing Calls from SM** to add **Matching Pattern +** with **Delete Digits 1**.

Click **Add** button under **Digit Conversion for Outgoing Calls from SM** to add **Matching Pattern 613XXX6507** with **Delete Digits 10** and **Insert Digits *56**. This is used for incoming call to FNE Service which is hosted by IP Office (See **Section 5.7** for more details)

Click **Add** button under **Digit Conversion for Outgoing Calls from SM** to add **Matching Pattern 613XXX6508** with **Delete Digits 10** and **Insert Digits *17**. This is used for incoming call to Voicemail Service which is hosted by IP Office (See **Section 5.7** for more details)

Click the **Commit** button after changes are completed.

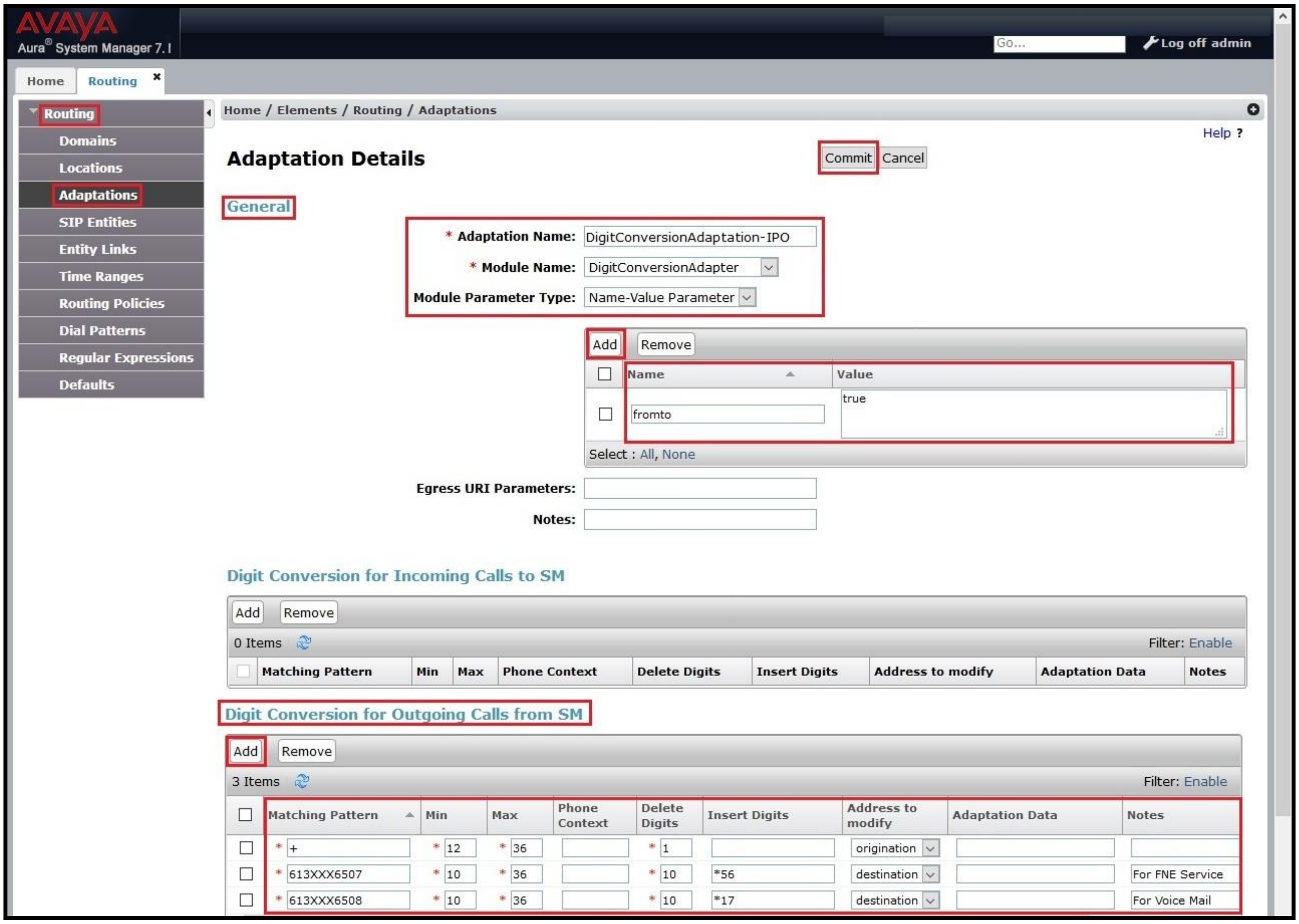

Figure 24 – IP Office Adaptation

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager, which includes IP Office and Avaya SBCE.

Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name**: Enter a descriptive name
- **FQDN or IP Address**: Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling
- **Type**: Select Session Manager for Session Manager; SIP Trunk for Avaya SBCE and IP Office
- **Adaptation**: This field is only present if **Type** is not set to **Session Manager**. Adaptation module was used in this configuration

- **Location**: Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **Belleville-GSSCP**
- **Time Zone**: Select the time zone for the Location above

In this configuration, there are three SIP Entities:

- Session Manager SIP Entity
- IP Office SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.5.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **bvwasm2**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.10.43**. The user will need to select the specific values for the **Location** and **Time Zone**.

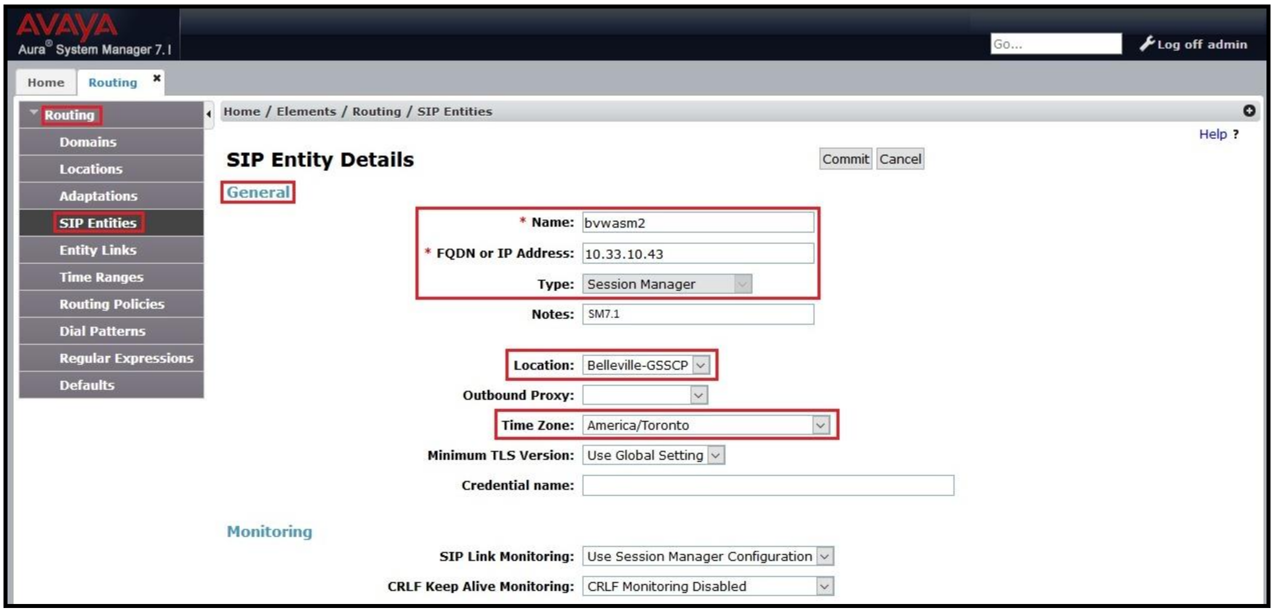

Figure 25: Session Manager SIP Entity

To define the ports used by Session Manager, scroll down to the **Listen Ports** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Listen Ports** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port**: Port number on which Session Manager listens for SIP requests
- **Protocol**: Transport protocol to be used with this port
- **Default Domain**: The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain

Defaults can be used for the remaining fields. Click **Commit** (not shown) to save

The compliance test used port **5061** with **TLS** for connecting to IP Office and Avaya SBCE

Figure 26: Session Manager SIP Entity Port

6.5.2. Configure IP Office SIP Entity

The following screen shows the addition of the IP Office SIP Entity named **IPOffice_1**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to IP Office, it is necessary to create a separate SIP Entity for IP Office in addition to the one created during Session Manager installation. The original SIP entity is used with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of IP Office **10.10.98.14**. The **Adaptation** is set to **DigitConversionAdaptation-IPO** (Defined in **Section 6.4**). Note that **SIP Trunk** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

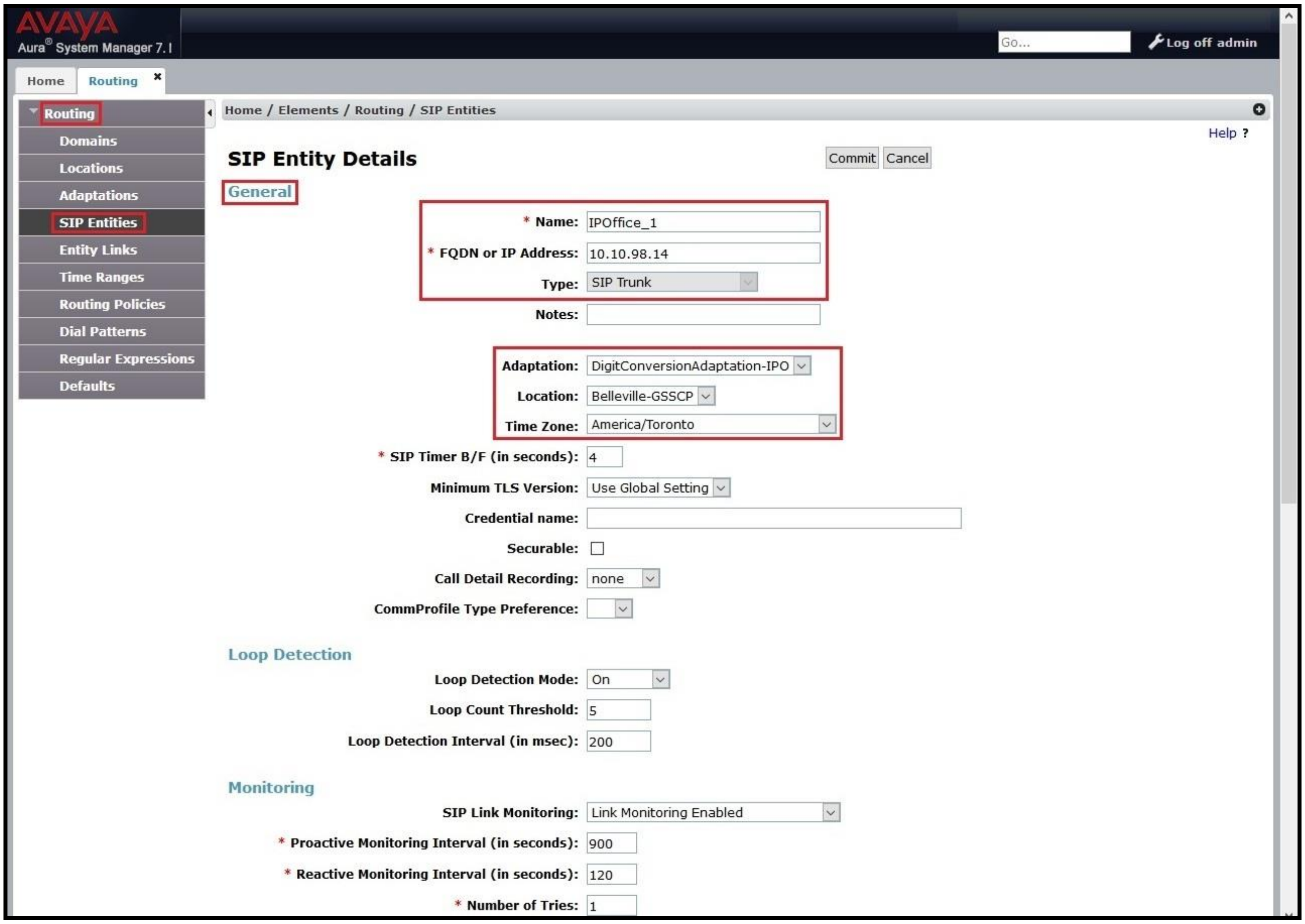

Figure 27: IP Office SIP Entity

6.5.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **SBCE**. The **FQDN** or **IP Address** field is set to the IP address of the SBCE's private network interface **10.10.98.13**. Note that **SIP Trunk** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

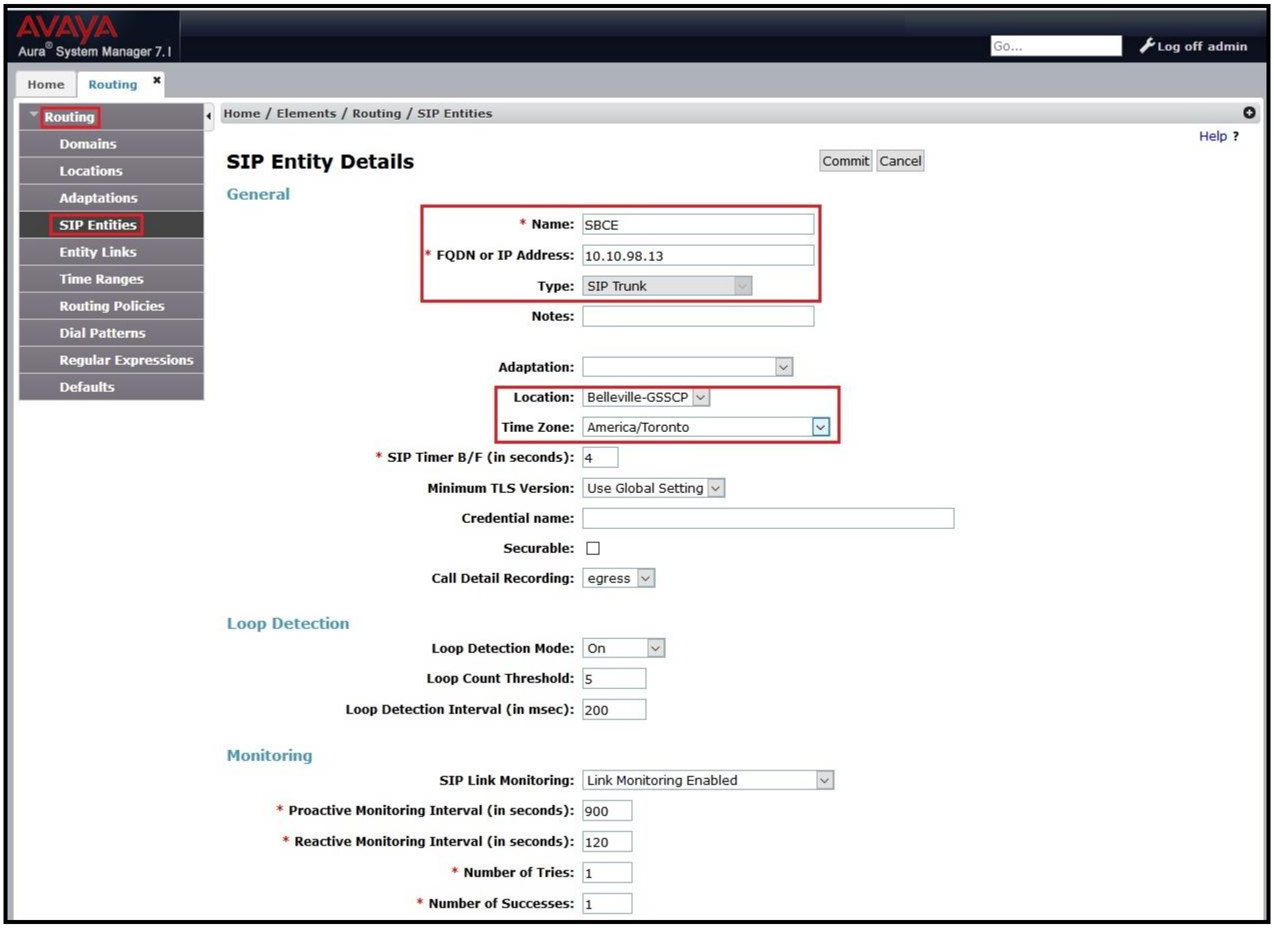

Figure 28: Avaya SBCE SIP Entity

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to IP Office and one to the Avaya SBCE.

To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

- **Name**: Enter a descriptive name
- **SIP Entity 1**: Select the Session Manager being used
- **Protocol**: Select the transport protocol used for this link
- **Port**: Port number on which Session Manager will receive SIP requests from the far-end
- **SIP Entity 2**: Select the name of the other system as defined in **Section 6.5**
- **Port**: Port number on which the other system receives SIP requests from the Session Manager
- **Connection Policy**: Select **trusted**. **Note**: If **trusted** is not selected, calls from the associated SIP Entity specified in **Section 6.5** will be denied

Click **Commit** to save

The following screen illustrates the Entity Link to IP Office. The protocol and ports defined here must match the values used on the IP Office (See SM Line → Session Manager tab → Network Configuration parameters in **Section 5.6**).

Figure 29: IP Office Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.4**, **7.6** and **7.10.3**.

Figure 30: Avaya SBCE Entity Link

6.7. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add a Time Range, select **Routing → Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.

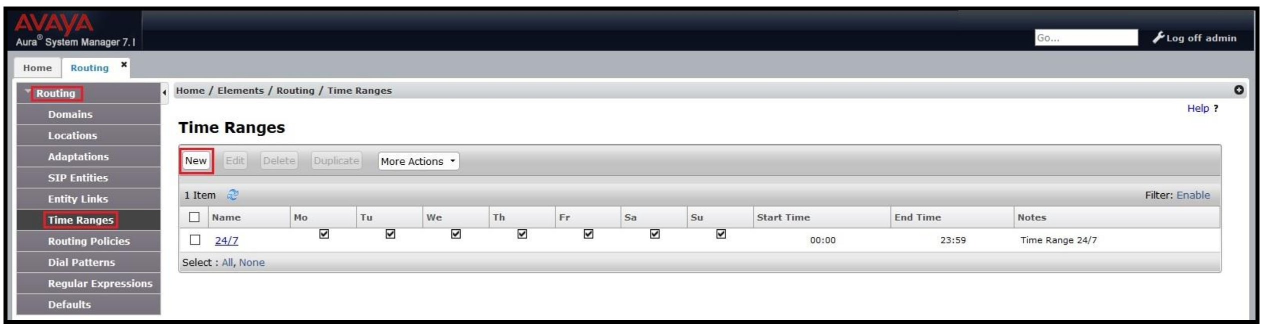

Figure 31: Time Ranges

6.8. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added; one for IP Office and one for Avaya SBCE.

To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name**: Enter a descriptive name
- **Notes**: Add a brief description (optional)

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies and click **Select**. The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields.

Click **Commit** to save

The following screen shows the **Routing Policy Details** for the policy named **Bell Canada Inbound** associated with incoming PSTN calls from Bell Canada to IP Office. Observe the **SIP Entity as Destination** is the entity named **IPOffice_1**.

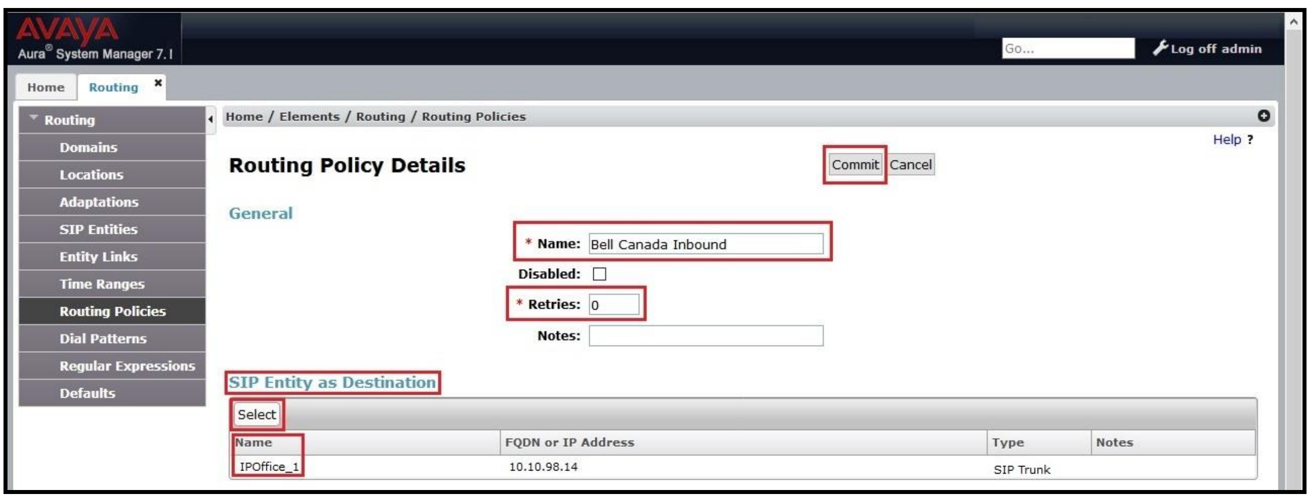

Figure 32: Routing to IP Office

The following screen shows the **Routing Policy Details** for the policy named **Bell Canada Outbound**, associated with outgoing calls from IP Office to the PSTN via Bell Canada SIP Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

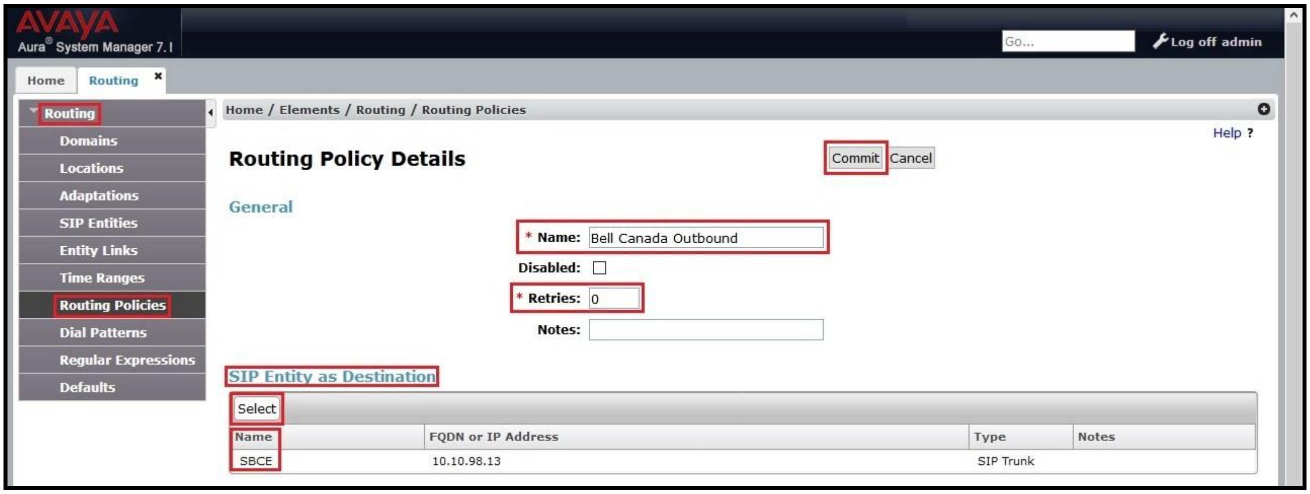

Figure 33: Routing to SBCE

6.9. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from IP Office to Bell Canada SIP Trunk through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination for a particular call based on the dialed digits, destination Domain and originating Location.

To add a Dial Pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Pattern**: Enter a dial string that will be matched against the Request-URI of the call
- **Min**: Enter a minimum length used in the match criteria
- **Max**: Enter a maximum length used in the match criteria
- **SIP Domain**: Enter the destination domain used in the match criteria
- **Notes**: Add a brief description (optional)

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating Location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**

Default values can be used for the remaining fields. Click **Commit** to save

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns were similarly defined.

The first example shows that outbound 11-digit dialed numbers that begin with **1** and have a destination **SIP Domain** of **bvwdev.com** uses **Routing Policy Name** as **Bell Canada Outbound** which is defined in **Section 6.8**.

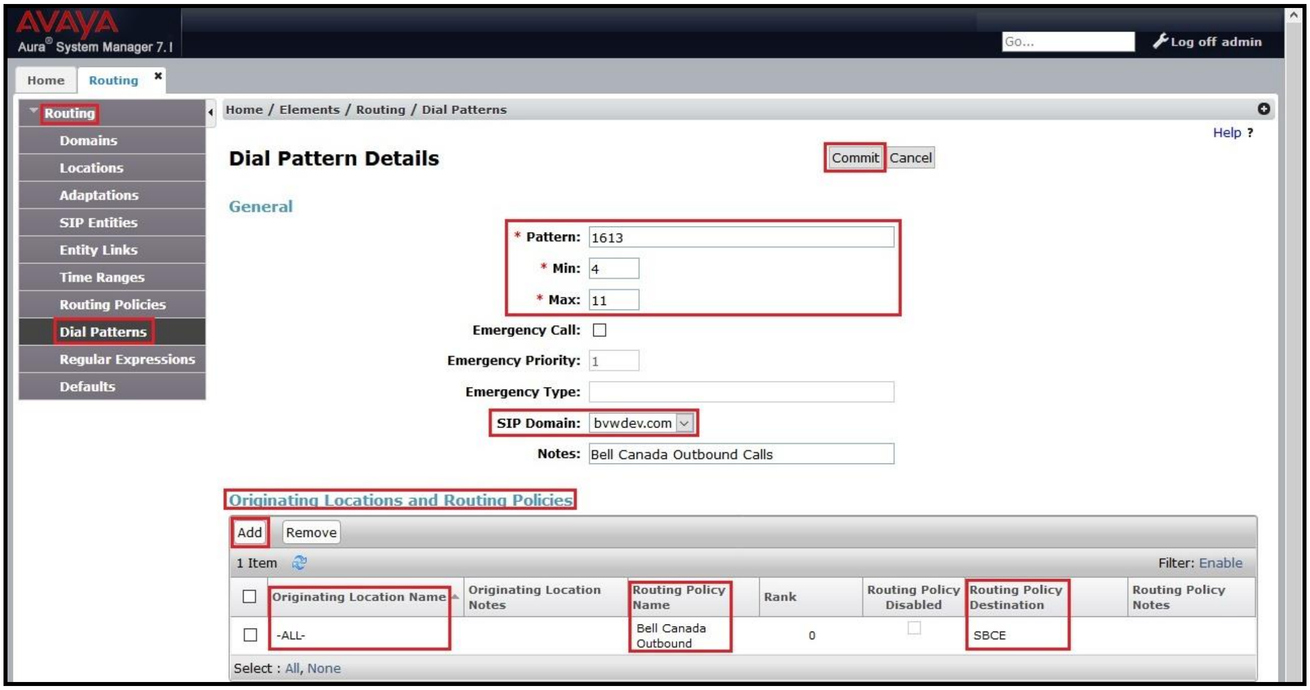

Figure 34: Dial Pattern_1613

Note that with the above Dial Pattern, Bell Canada did not restrict outbound calls to specific US/Canada area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed back to the PSTN.

The second example shows that inbound 10 digit numbers that start with **613** use **Routing Policy Name** as **Bell Canada Inbound** which is defined in **Section 6.8**. This Dial Pattern matches the DID numbers assigned to the enterprise by Bell Canada.

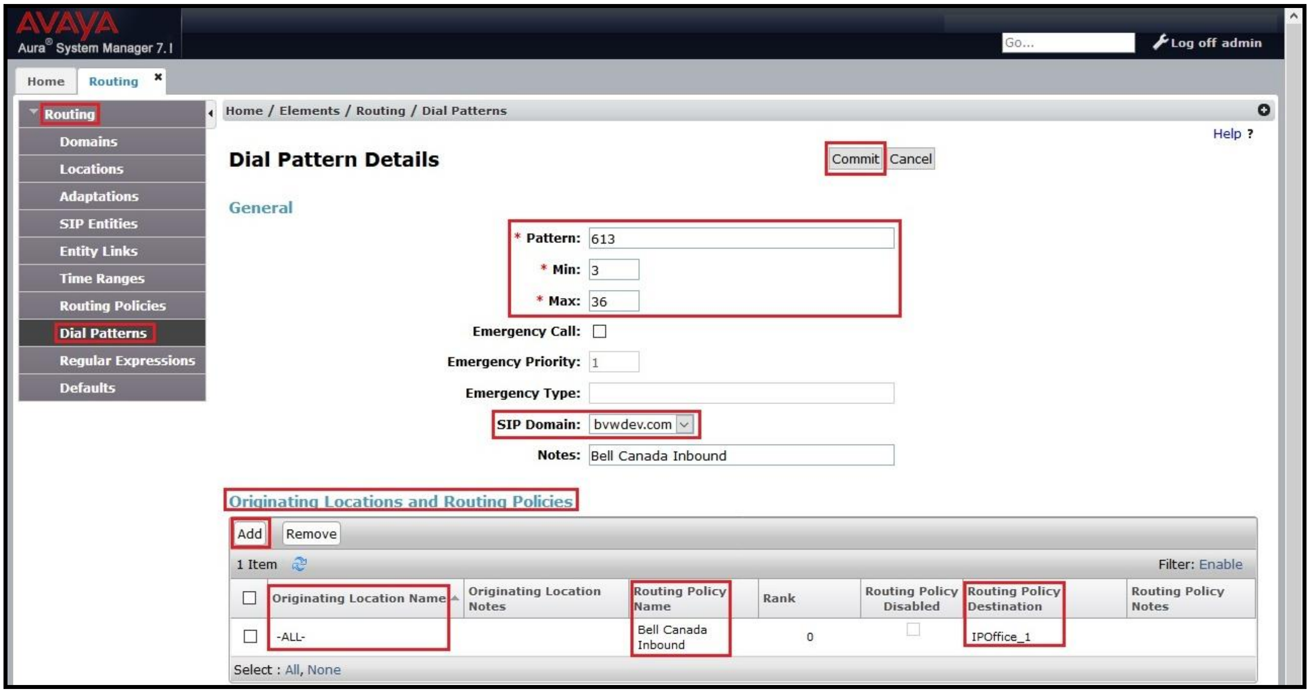

Figure 35: Dial Pattern_613

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

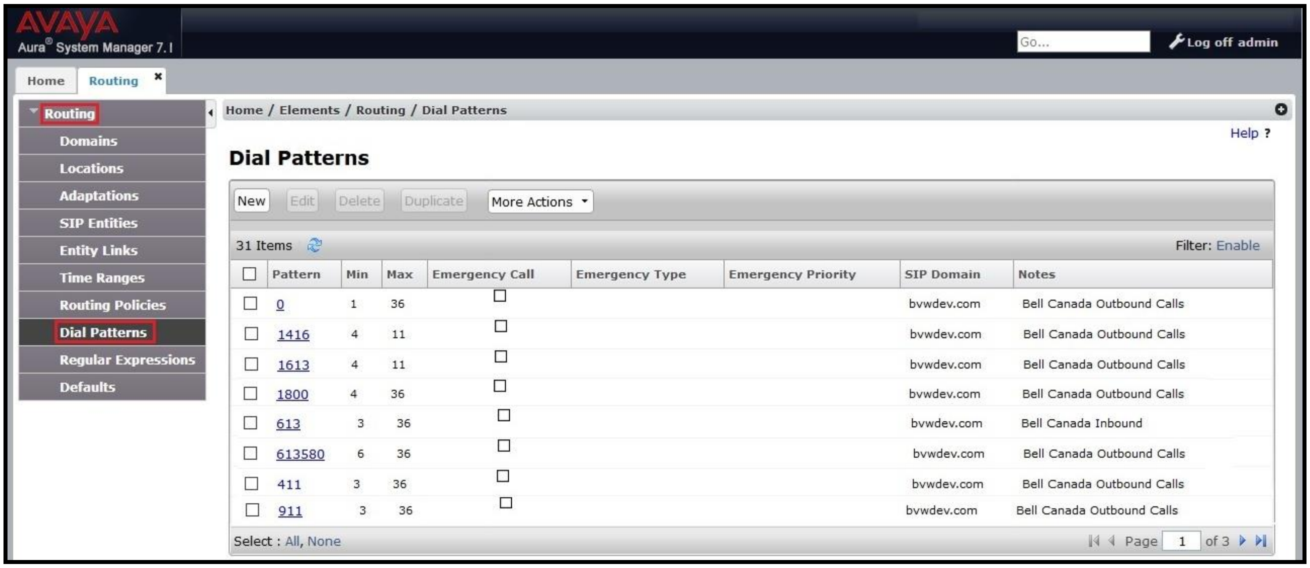

Figure 36: Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the Bell Canada system.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Bell Canada system resides on the Public side of the network.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, refer to the documentation listed in **Section 11** of these Application Notes.

7.1. Log in to Avaya Session Border Controller for Enterprise

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

Enter the **Username** and **Password** and click on **Log In** button.

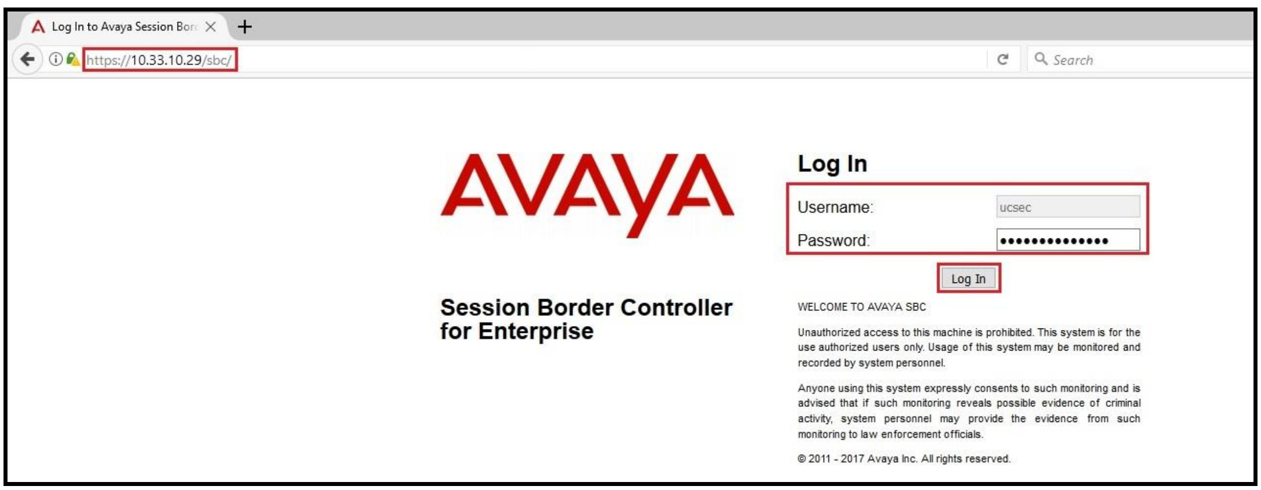

Figure 37: Avaya SBCE Login

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

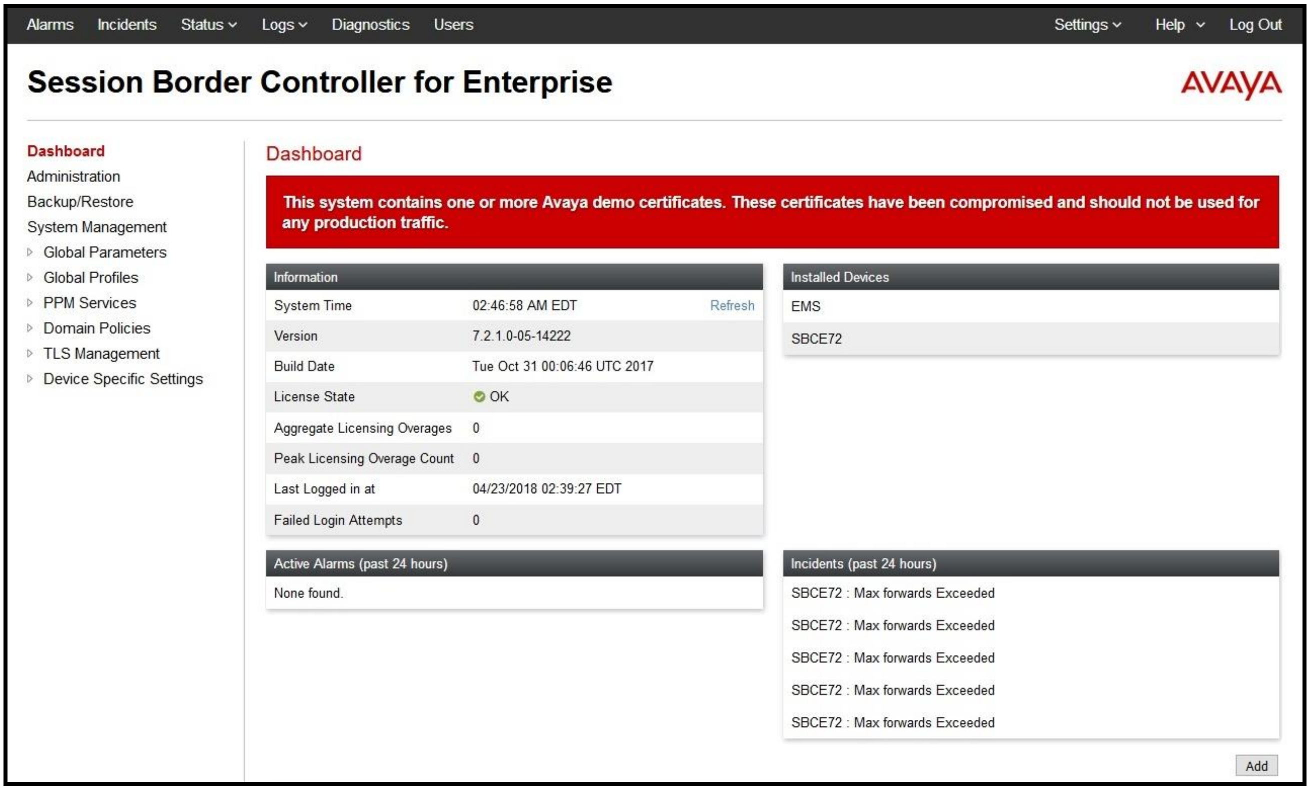

Figure 38: Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **SBCE72** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

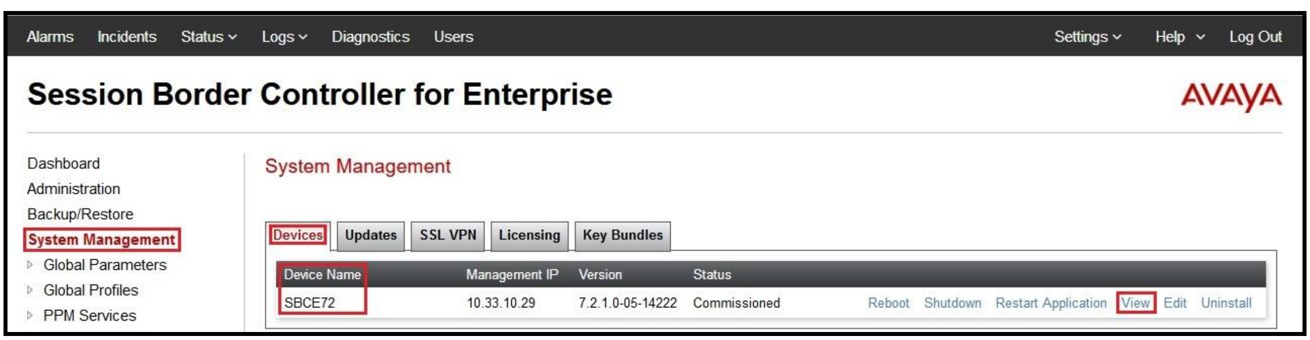

Figure 39: Avaya SBCE System Management

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.

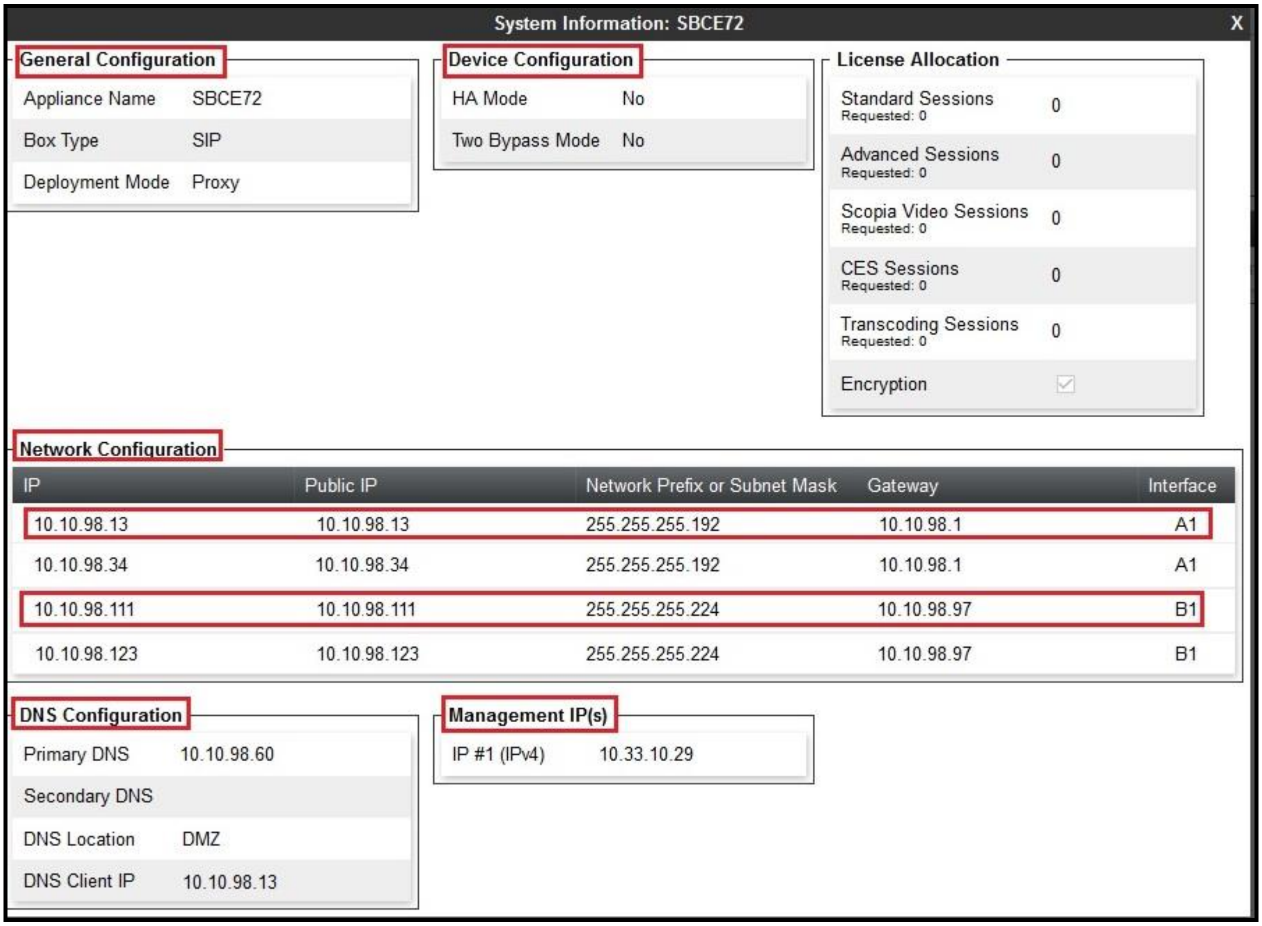

Figure 40: Avaya SBCE System Information

7.2. Global Profiles

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

7.2.1. Configure Server Interworking Profile - Avaya Site

Server Interworking profile allows administrator to configure and manage various SIP call server specific capabilities such as call hold, 180 handling, etc.

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

- Select **avaya-ru** in **Interworking Profiles**
- Click **Clone**
- Enter **Clone Name**: **SMVM** and click **Finish** (not shown)
- Select **SMVM** in **Interworking Profiles**
- Click **Edit** button
- Check **T.38 Support** option if customer supports Fax T.38 and click **Finish** (not shown)

The following screen shows that Session Manager server interworking profile (named: **SMVM**) was added.

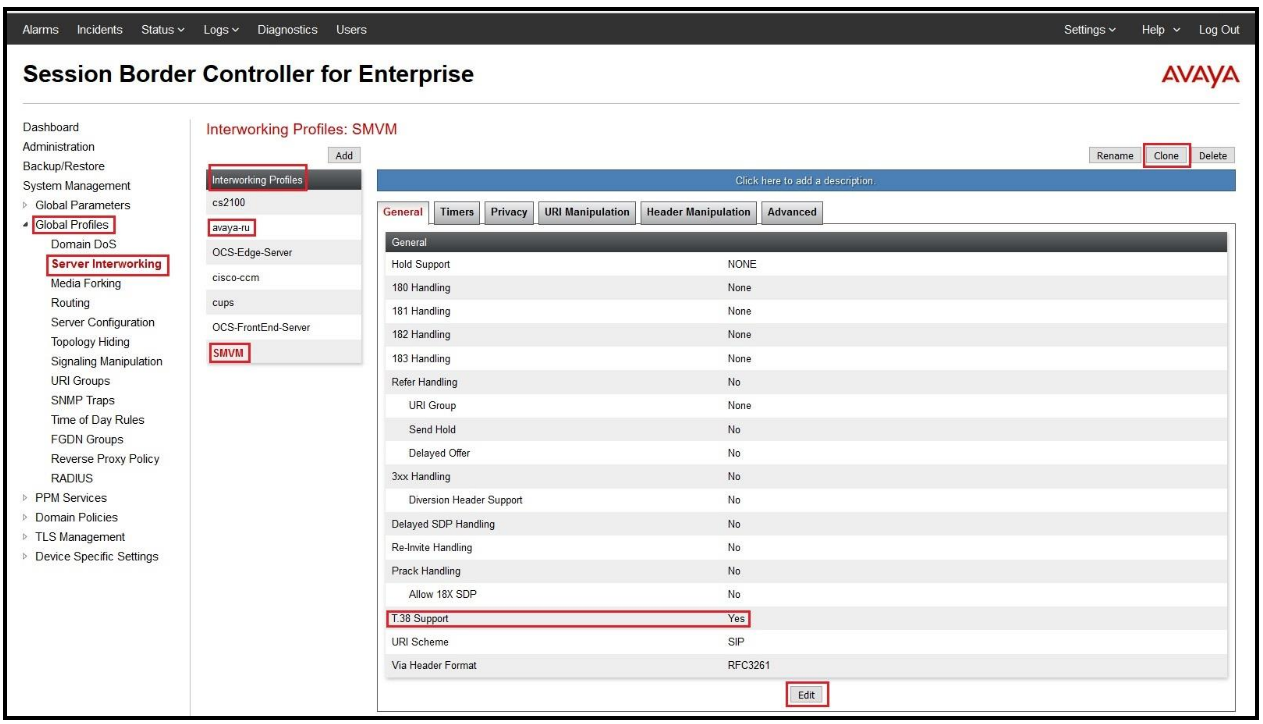

Figure 41: Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – Bell Canada SIP Trunk Site

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

- Enter **Profile Name**: **SP5_Bell** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)
- Select **SP5_Bell** in **Interworking Profiles**
- Click **Edit** button
- Check **T.38 Support** option if customer supports Fax T.38 and click **Finish** (not shown)

The following screen shows that Bell Canada server interworking profile (named: **SP5_Bell**) was added.

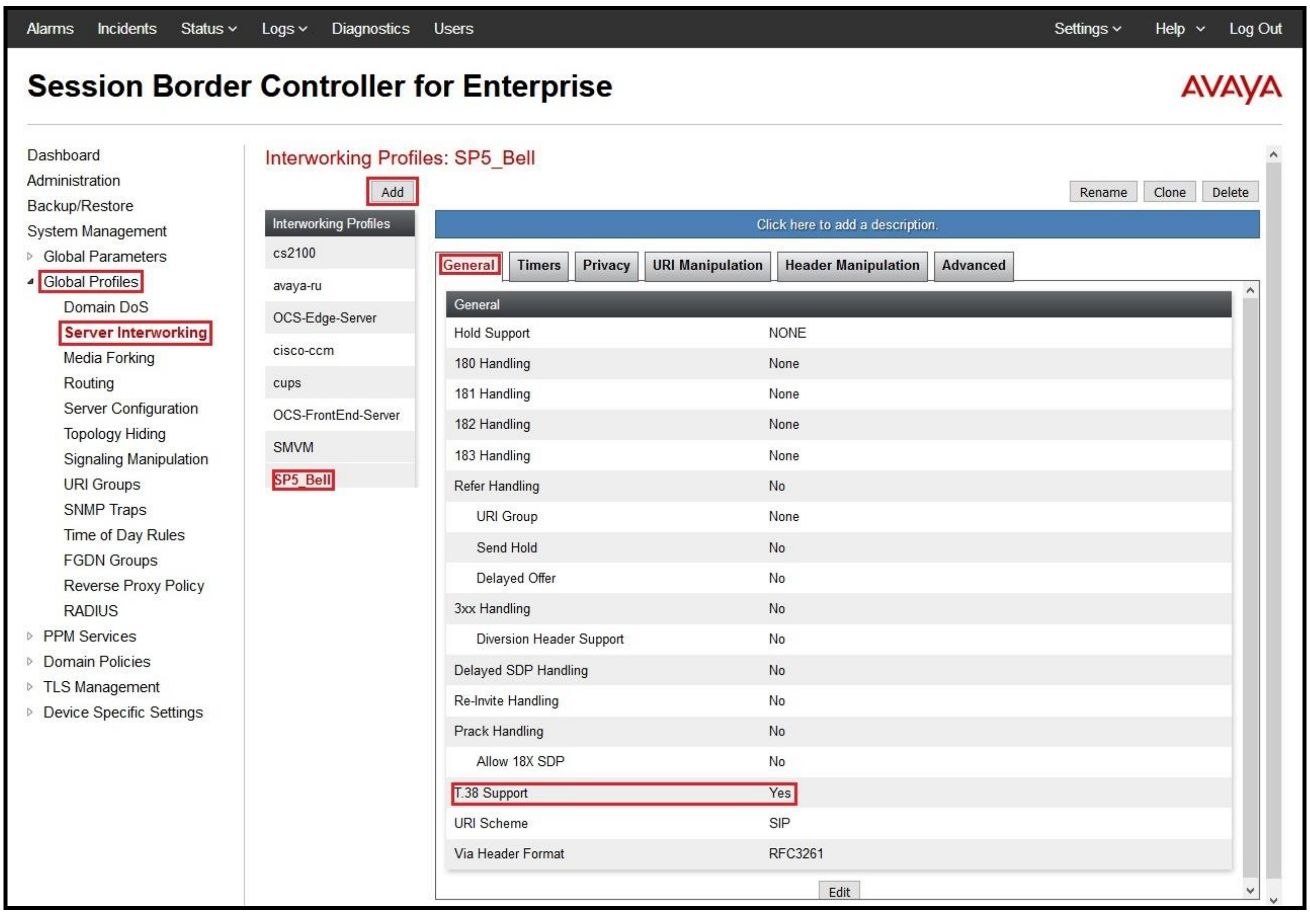

Figure 42: Server Interworking – General - Bell Canada SIP Trunk site

From the menu on the left-hand side, select **Global Profiles → Server Interworking**
Select **SP5_Bell** in **Interworking Profiles**

- Select **URI Manipulation** tab and click on **Add** button to create User Regex or Domain Regex

- Enter **User Regex** as **6506**. Enter **User Action** to **add prefix 613XXX**. This URI Manipulation is used to add a prefix on user URI of From, Contact and PAI headers for outbound calls.
- Enter **User Regex** as **6507**. Enter **User Action** to **add prefix 613XXX**. This URI Manipulation is used to add a prefix on user URI of From, Contact and PAI headers for outbound calls.
- Enter **User Regex** as **6508**. Enter **User Action** to **add prefix 613XXX**. This URI Manipulation is used to add a prefix on user URI of From, Contact and PAI headers for outbound calls.
- Enter **Domain Regex** as **192.168.237.209**. Enter **Domain Action** to **replace with siptrunking.bell.ca**. This URI Manipulation is used to replace the URI domain of Refer-to header in off-net forward/transfer calls.
- Click **Finish** (not shown)

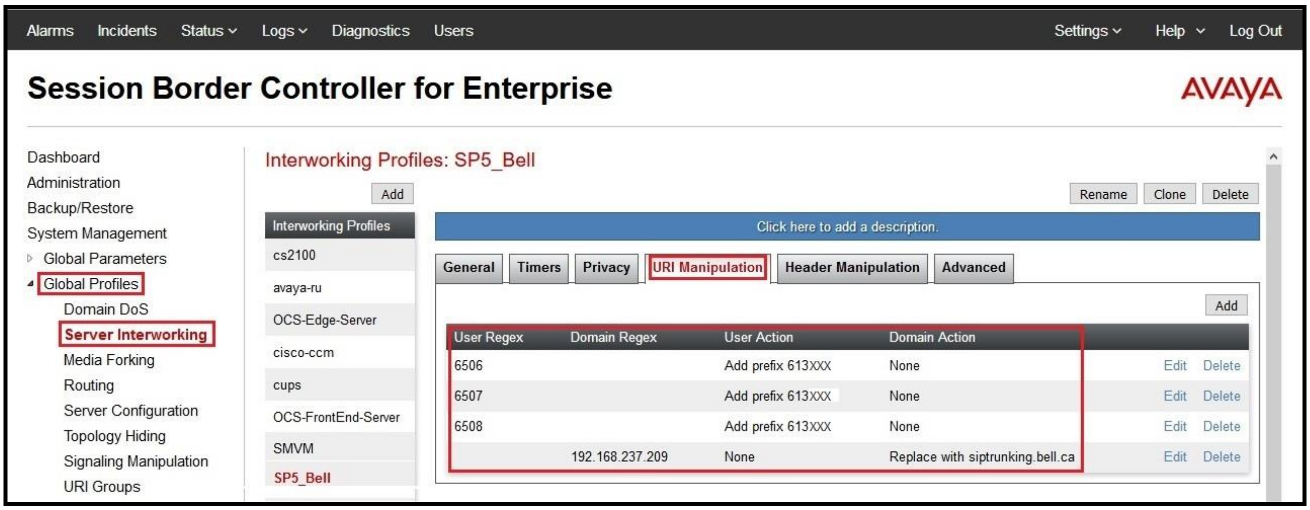

Figure 43: Server Interworking – URI Manipulation - Bell Canada SIP Trunk site

Bell's Static/Dynamic ONND (Outbound Calling Name and Number Display) and Trunk Group Selection features require header manipulation in Avaya SBCE. However, this Header Manipulation is NOT required under a normal configuration. This is provided as reference configuration for this specific testing. For more details, refer to *Bell Canada SIP Trunking Service Interface Specification, version 2.0.7*.

For Static ONND in this compliance testing, the From, PAI and Diversion headers should always be including parameter user=phone. And for Trunk Group Selection, it is optional that the PAI and Diversion headers include parameter otg=trunk-group-id**.** With the presence of a Trunk Group Selection the display will be as in the From header. The display will be as in the PAI with an implicit Trunk Group Selection (i.e. without a Trunk Group Selection). Even though, these ***user*** and ***otg*** parameters are not required in the From header, it is being included in here for completeness. When using a Trunk Group Selection, the otg tag must be present in the From, PAI and Diversion headers when applicable.

Note: For multi-trunk group and geographic redundant configuration refer to document: Application Notes for Bell Canada SIP Trunking Service using Least Cost Routing with Avaya Aura® Communication Manager R6.0.1, Geographic Redundant Avaya Aura® Session Managers R6.1 and Avaya Session Border Controllers for Enterprise R4.0.5 –Issue 1.0
https://www.devconnectprogram.com/fileMedia/download/f1603e7f-a6c4-4555-bea5-3b0a8deb61e0

Below is the sample of Header Manipulation used in this compliance test. Headers are added to include the parameter **otg=trunk-group-id** and **user=phone** to the **From**, **Diversion** and **P-Asserted-Identity** headers as Bell Canada required

- **Header**: This field is where **From** and **P-Asserted-Identity** is selected
- **Action**: **Add Parameter w/[value]** is selected
- **Parameter** = **user** and **Value** = **phone**
- **Parameter** = **otg** and **Value** = **VEND6_613XXX6506_01A**

Note: As designed, IP Office using SM Line does not add the Diversion header for responses, UPDATE and re-Invite's in off-net call forward. IP Office used SIP Refer method instead (See **Section 2.2** in details). Therefore, there is no Diversion header to be added in Header Manipulation to test with ONND. In order to make off-net call forward work, the SIP Refer has to be implemented and supported by customer.

The screenshots below illustrate the Server Interworking profile **SP5_Bell** with **Header Manipulation**.

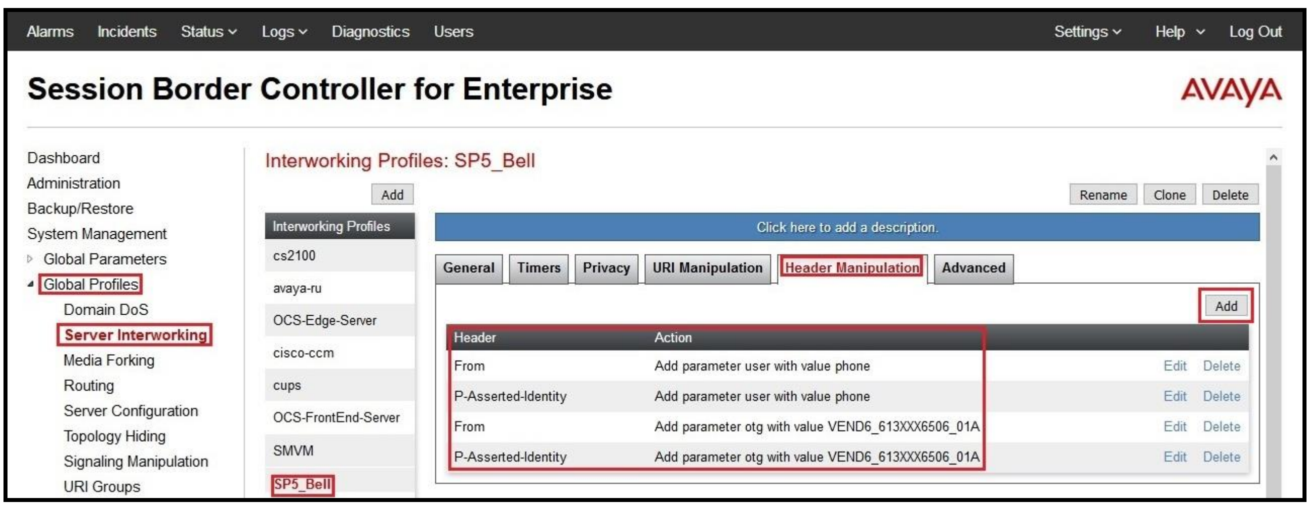

Figure 44: Server Interworking – Header Manipulation - Bell Canada SIP Trunk site

7.3. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

From the menu on the left-hand side, select **Global Profiles → Signaling Manipulation → Add**

- Enter script **Title**: **SP5-Bell**. In the script editing window, enter the text exactly as shown in the screenshot to perform the following:
  - Remove P-Asserted-Identity for the outbound calls (This is optional for ONND testing)
  - Replace the user URI of PPI header (This is for anonymous outbound call)
  - Replace user URI of PAI header with the valid number for off-net redirection calls
  - Click **Save** (not shown)

Note: See **Appendix A** in **Section 12** for the reference of this signaling manipulation (SigMa) script.

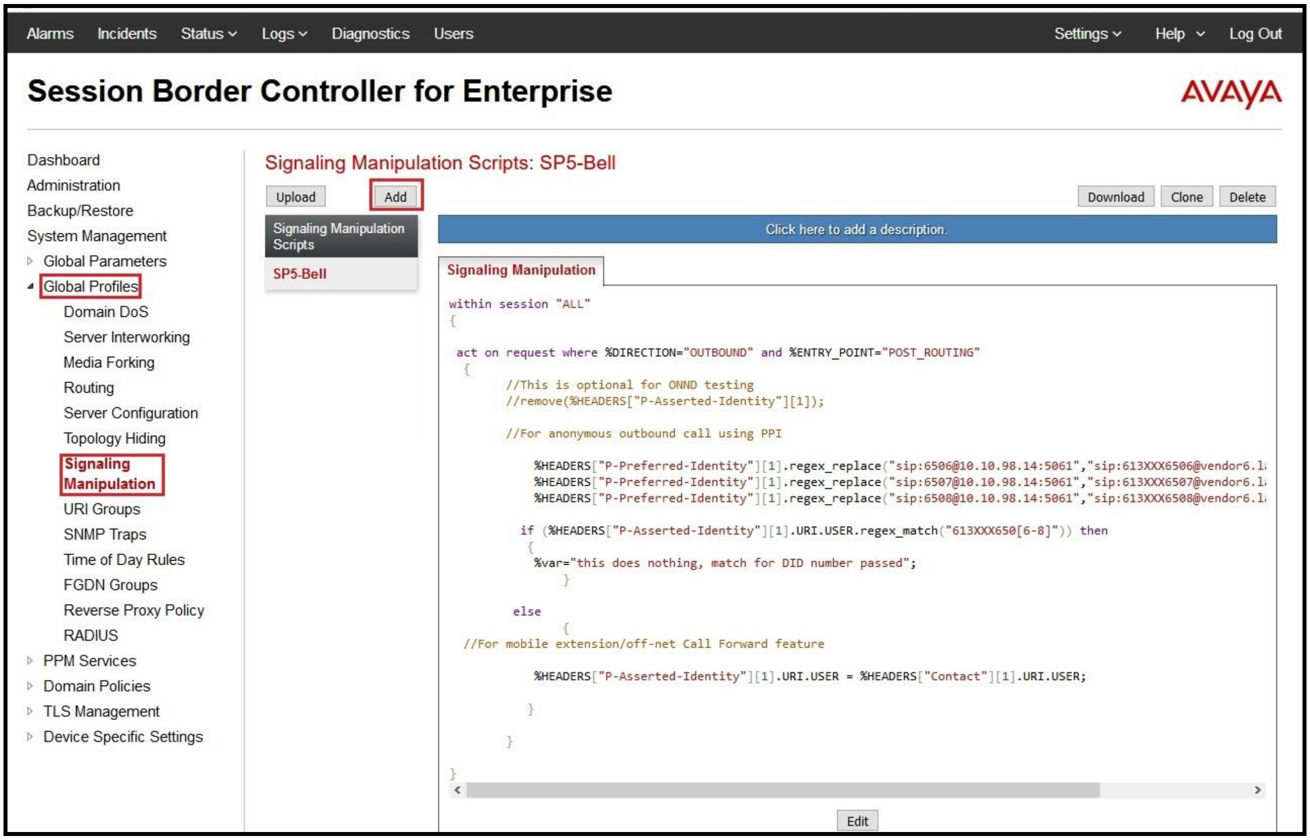

Figure 45: Signaling Manipulation

7.4. Configure Server – Avaya Site

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

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

Enter **Profile Name**: **SMVM**

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

- **Server Type**: Select **Call Server**
- **TLS Client Profile**: Select **AvayaSBCClient71**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
- **IP Address/FQDN**: **10.33.10.43** (Session Manager IP Address)
- **Port**: **5061**
- **Transport**: **TLS**
- Click **Finish** (not shown)

Figure 46: Server Configuration – General - Avaya site

On the **Advanced** tab:

- **Enable Grooming** box is checked
- Select **SMVM** for **Interworking Profile** (see **Section 7.2.1**)
- Click **Finish** (not shown)

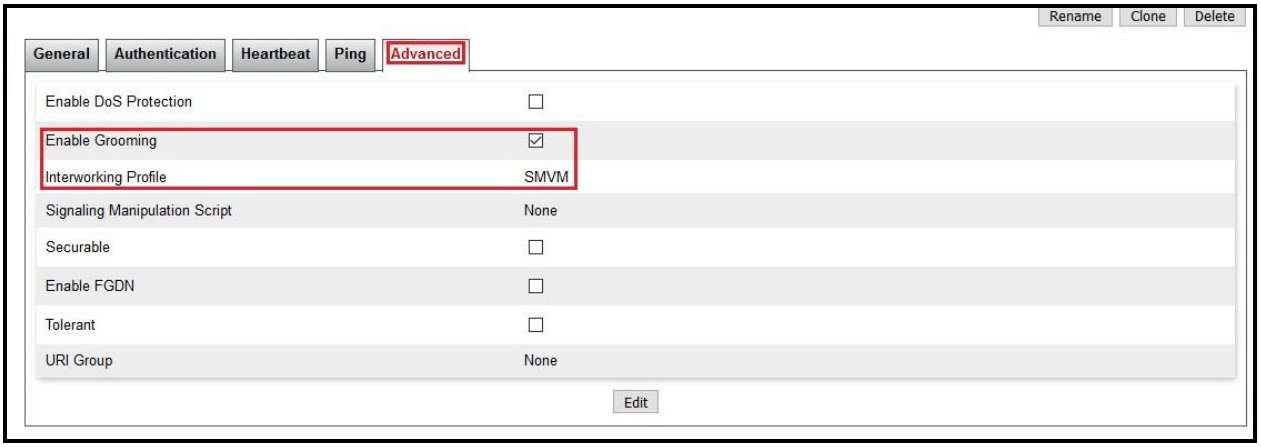

Figure 47: Server Configuration – Advanced - Avaya site

7.5. Configure Server – Bell Canada SIP Trunk

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**
Enter **Profile Name**: **SP5-Bell**

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

- **Server Type**: Select **Trunk Server**
- **IP Address/FQDN**: **192.168.237.209** (Bell Canada SIP Signaling Server IP Address)
- **Port**: **5060**
- **Transport**: **UDP**
- Click **Finish** (not shown)

Figure 48: Server Configuration – General – Bell Canada site

On **Heartbeat** tab, click **Edit** button to enter the following:

- Check **Enable Heartbeat**
- Select **Method**: **OPTIONS**
- **Frequency**: **60 seconds**
- **From URI**: **ping@vendor6.lab.internetvoice.ca**
- **To URI**: **ping@siptrunking.bell.ca**

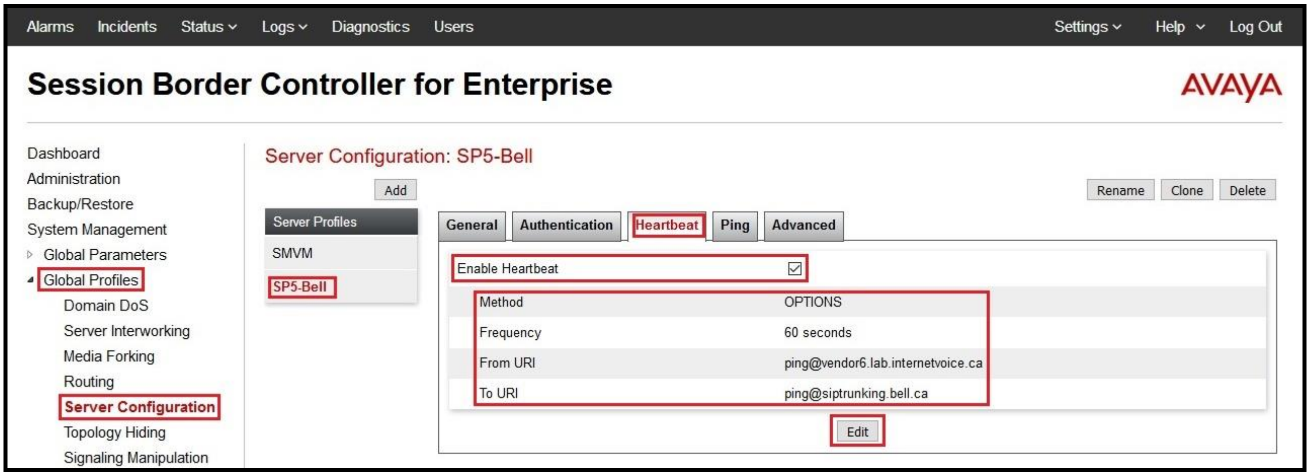

Figure 49: Server Configuration – Heartbeat – Bell Canada site

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

- Check **Enable Authentication**
- Enter **User** as **VEN6_613XXX6505_01A** (Bell Canada provides this information)
- Enter **Password** and **Confirm Password** (Bell Canada provides this information)
- Click **Finish** button to save the changes.

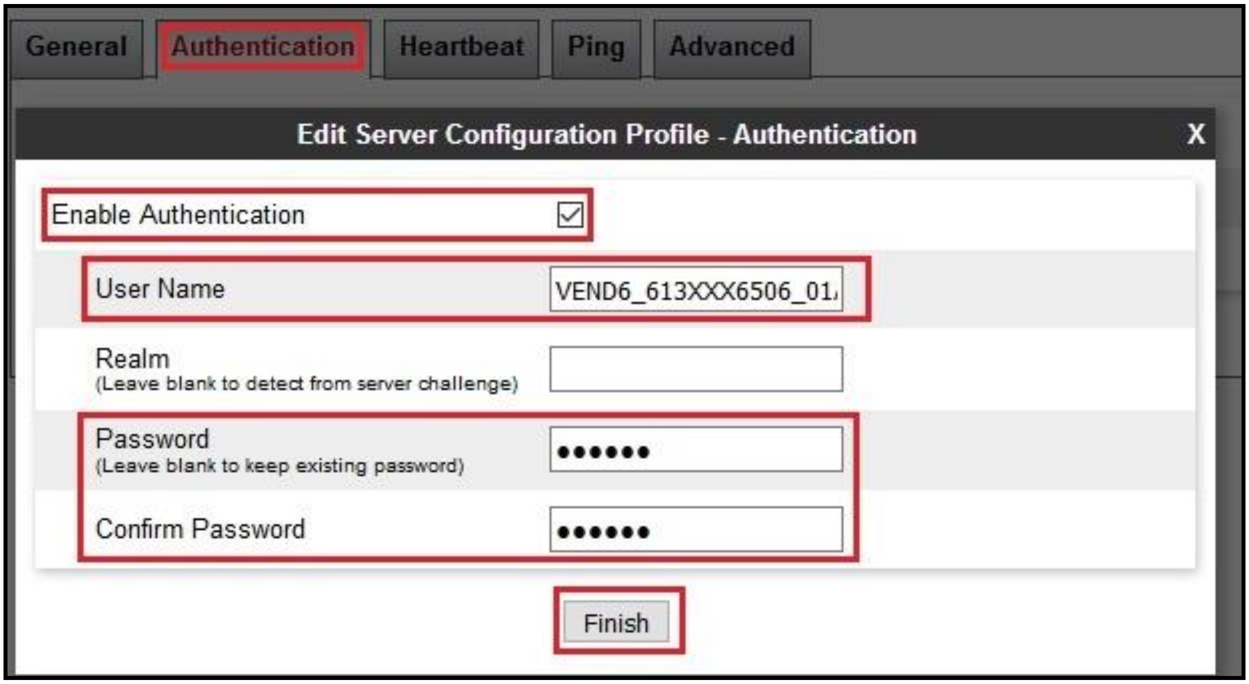

Figure 50: Server Configuration – Authentication – Bell Canada site

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

- **Interworking Profile**: **SP5_Bell** (see **Section 7.2.2**)
- **Signaling Manipulation Script**: **SP5-Bell** (see **Section 7.3**)
- Click **Finish** (not shown)

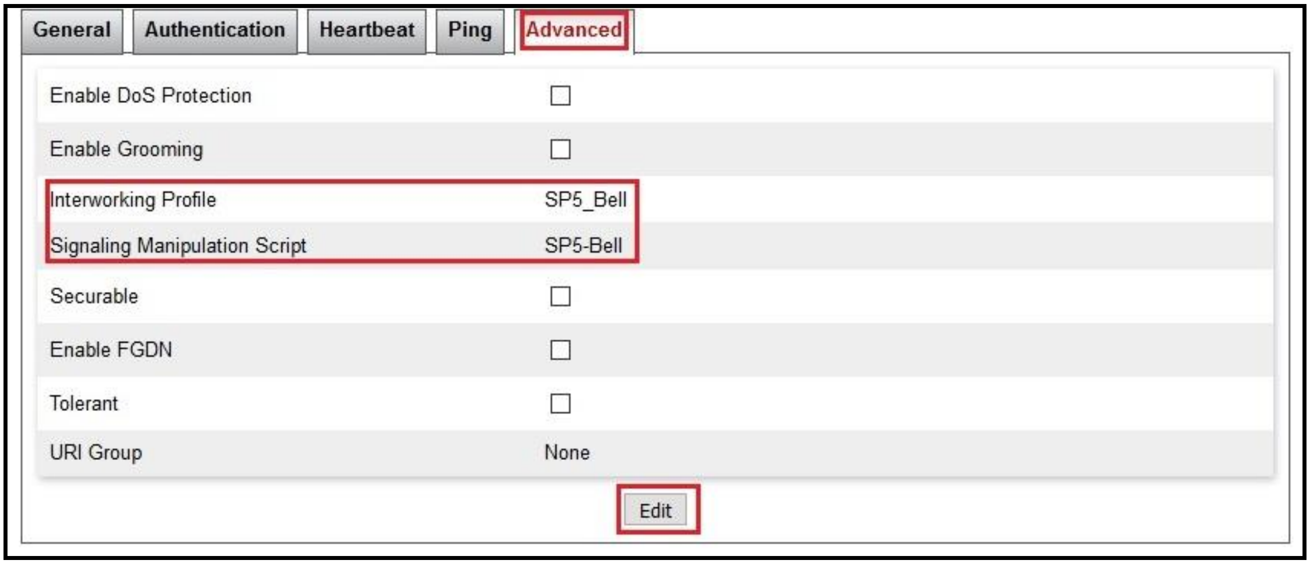

Figure 51: Server Configuration – Advanced – Bell Canada site

7.6. Configure Routing – Avaya Site

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

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

Enter **Profile Name**: **SP5_Bell_To_SMVM** and click **Next** button (Not Shown)

- Select **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **Server Configuration**: **SMVM** (see **Section 7.4**)
- **Next Hop Address**: **10.33.10.43:5061 (TLS)** (Session Manager IP Address)
- Click **Finish**

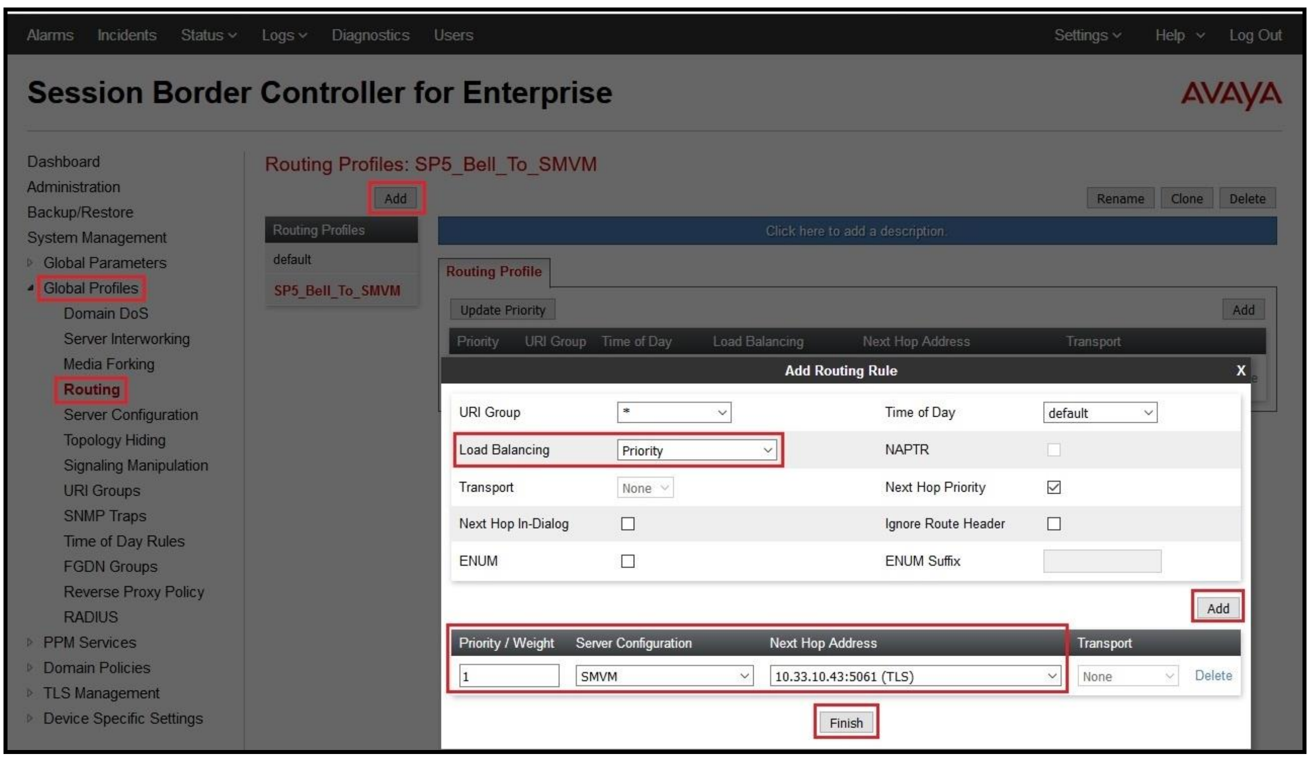

Figure 52: Routing to Session Manager

7.7. Configure Routing – Bell Canada SIP Trunk Site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

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

Enter **Profile Name**: **SMVM_To_SP5_Bell** and click **Next** button (not shown)

- **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **Server Configuration**: **SP5-Bell** (see **Section 7.5**)
- **Next Hop Address**: **192.168.237.209:5060 (UDP)** (Bell Canada Signaling Server IP Address)
- Click **Finish**

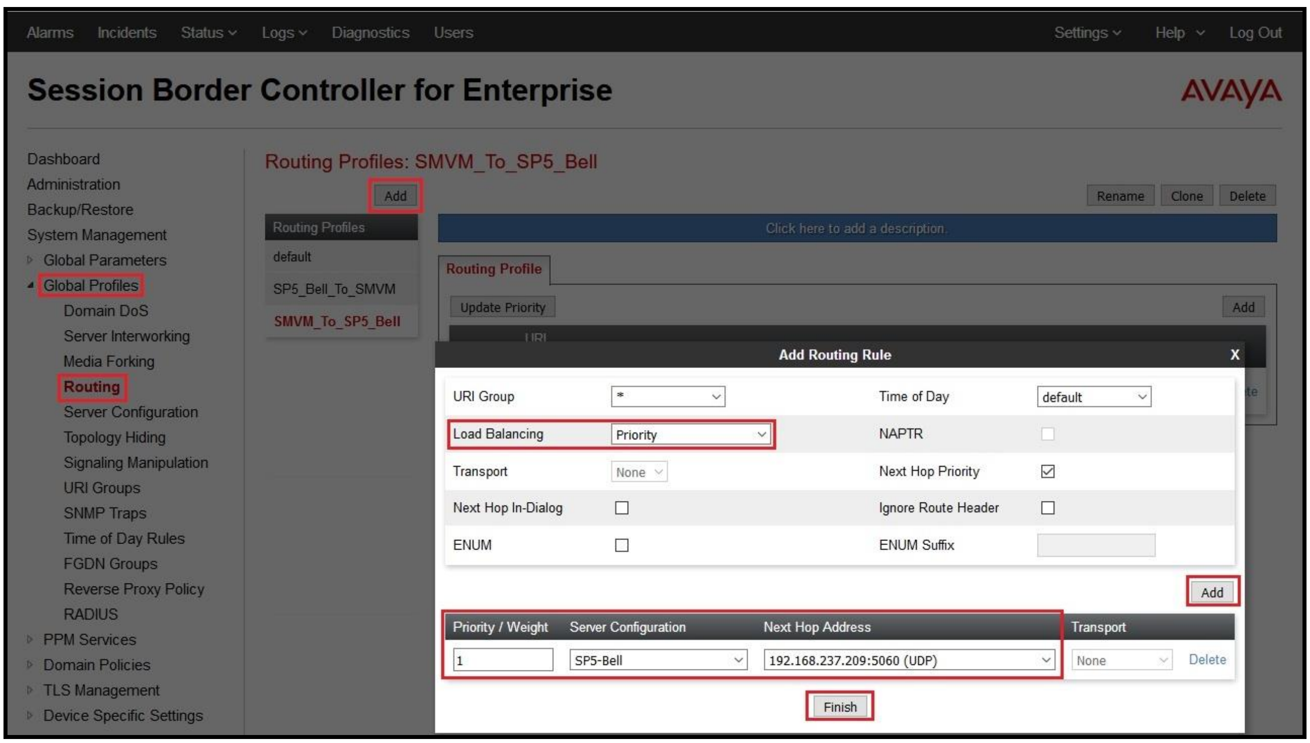

Figure 53: Routing to Bell Canada SIP Trunk

7.8. Configure Topology Hiding

The **Topology Hiding** screen allows an administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **SP5_Bell_To_SMVM** and click **Finish** (not shown)
- Select **SP5_Bell_To_SMVM** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**
- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
    In the **Overwrite Value** column: **bvwdev.com**

Click **Finish** (not shown)

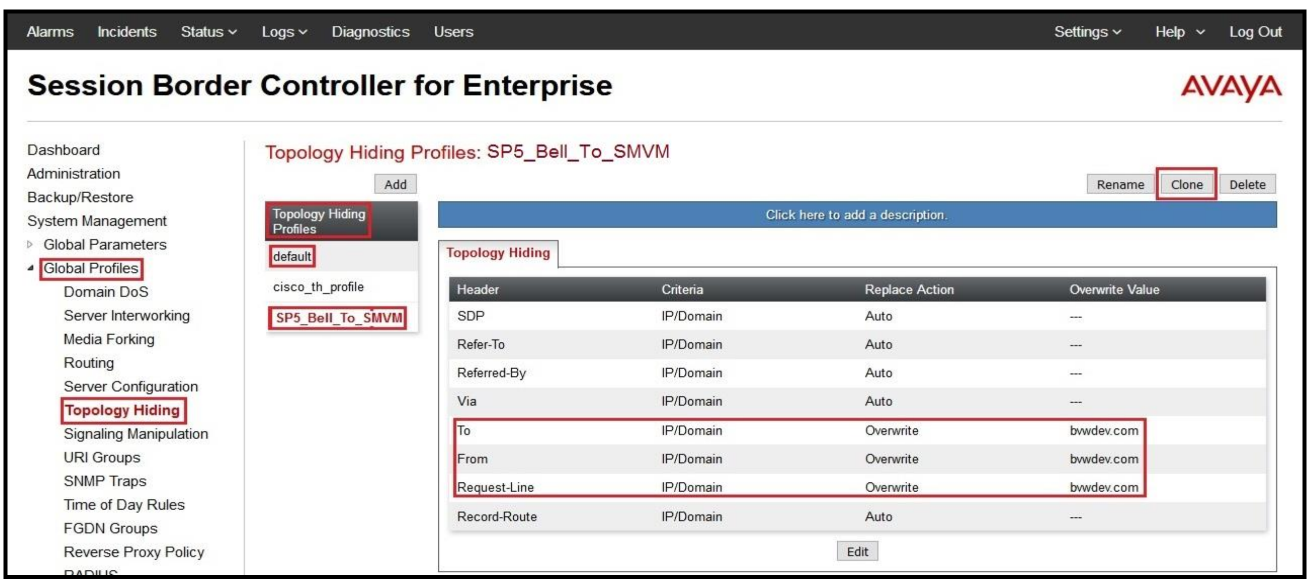

Figure 54: Topology Hiding To Session Manager

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **SMVM_To_SP5_Bell** and click **Finish** (not shown)
- Select **SMVM_To_SP5_Bell** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **siptrunking.bell.ca**
- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **siptrunking.bell.ca**
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **vendor6.lab.internetvoice.ca**
    Note: For ONND testing, the **Overwrite Value** is set to **lab.internetvoice.ca** for From header. This is optional configuration

Click **Finish** (not shown)

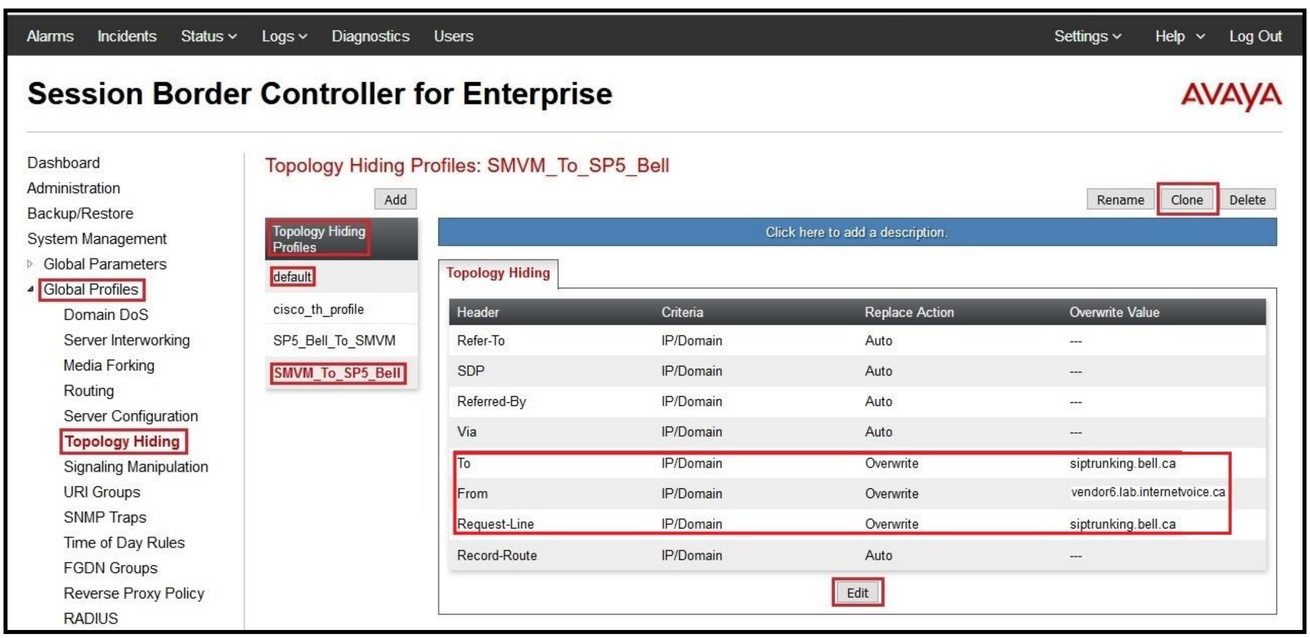

Figure 55: Topology Hiding To Bell Canada

7.9. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

7.9.1. Create Application Rules

Application Rules allow one to define which types of Avaya applications will be passed. The Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, one can determine the maximum number of concurrent voice and video sessions so that the network will process to prevent resource exhaustion. For the compliance test, the **SP5_IPO_14** application rule (shown below) was used for the End Point Policy Group defined in **Section 7.9.3**.

From the menu on the left-hand side, select **Domain Policies → Application Rules**

- Select the **default** rule and click on **Clone** button
- Enter **Clone Name**: **SP5_IPO_14** and click **Finish** button (not shown)
- Select the **SP5_IPO_14** rule from the list of **Application Rules** and click on **Edit** button
- Set **Maximum Concurrent Sessions** to **500** and **Maximum Sessions Per Endpoint** to **500**
- Click **Finish** button (not shown) to save the changes

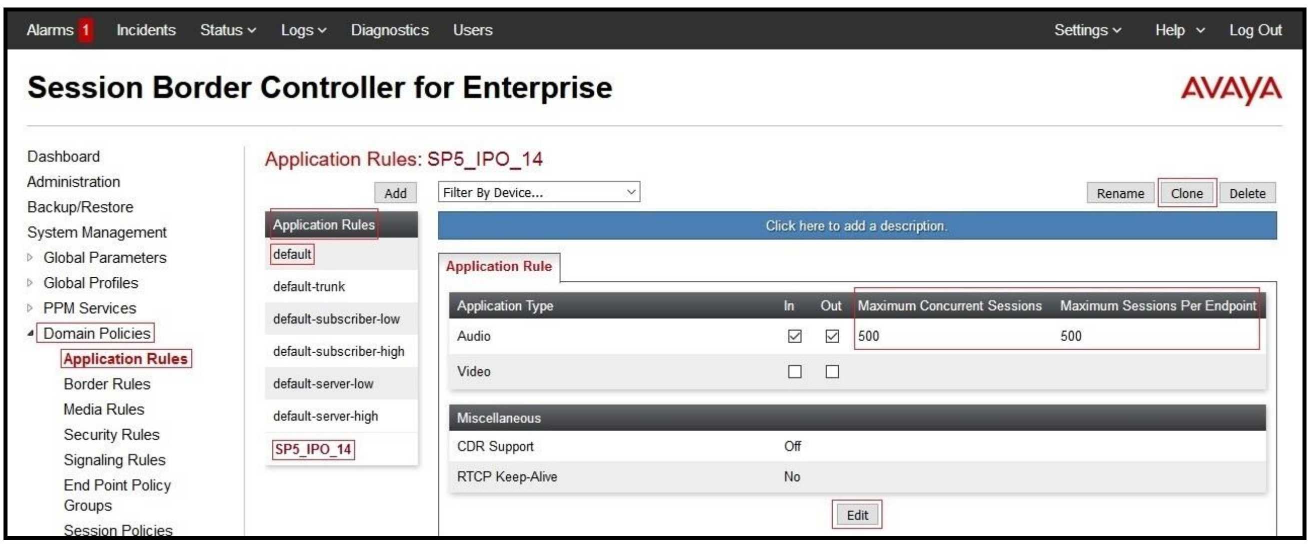

Figure 56 – Application Rule

7.9.2. Create Media Rules

Media Rules allow one to define 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 packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, the predefined **default-low-med-enc** media rule (shown below) was used to clone and edit.

From the menu on the left-hand side, select **Domain Policies → Media Rules**

- Select the **default-low-med-enc** rule, click **Clone**. Enter **Clone Name**: **SMVM_SP5_Bell** Click **Finish** (not shown)
- Select **SMVM_SP5_Bell** under **Media Rules** to **Edit**

The **Encryption** tab indicates that **RTP** and **SRTP_AES_CM_128_HMAC_SHA1_80** encryption were used as **Preferred Formats** for **Audio Encryption**.

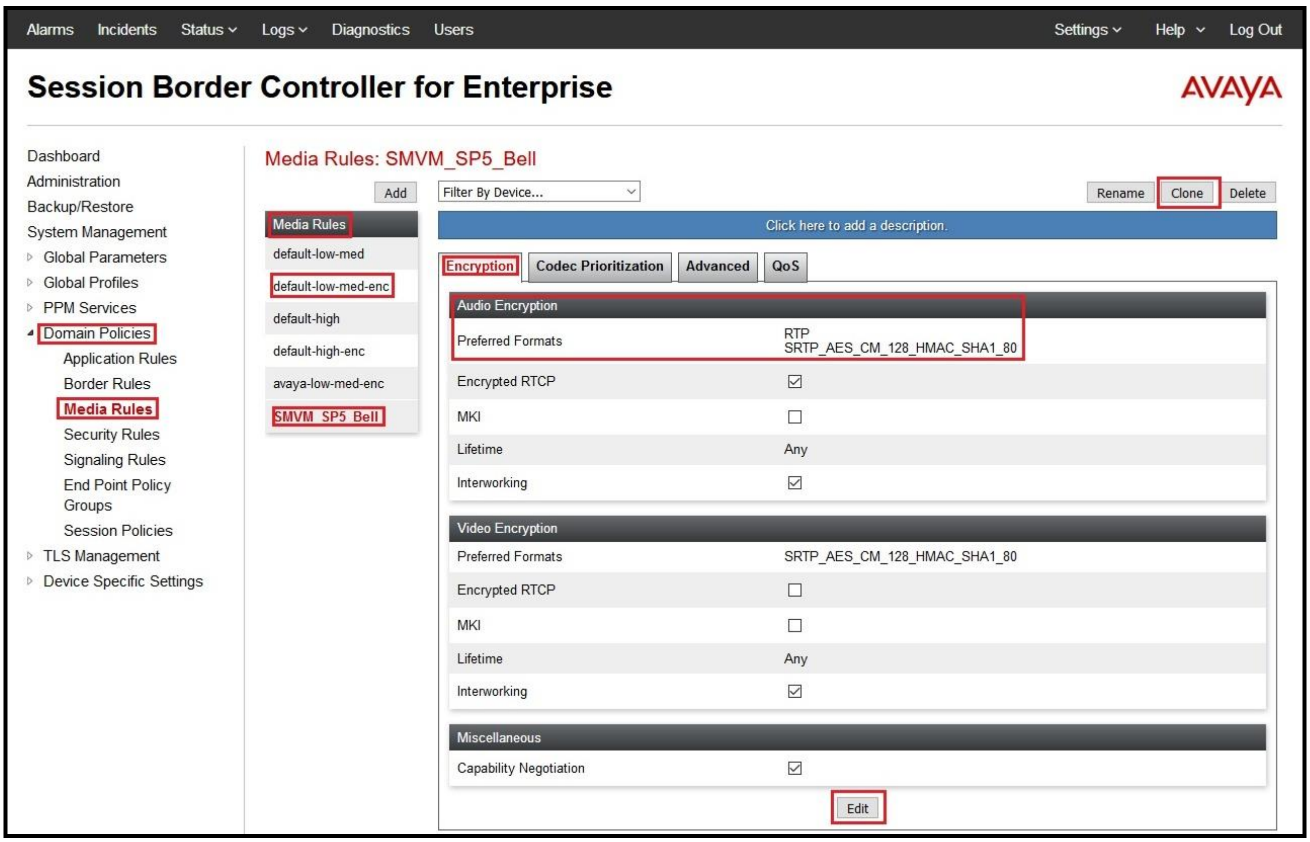

Figure 57: Media Rule

7.9.3. Create Endpoint Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD, each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

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

- Select **Add**
- Enter **Group Name**: **SMVM_SP5_Bell**
    - **Application Rule**: **SP5_IPO_14** (See in **Section 7.9.1**)
    - **Border Rule**: **default**
    - **Media Rule**: **SMVM_SP5_Bell** (See in **Section 7.9.2**)
    - **Security Rule**: **default-low**
    - **Signaling Rule**: **default**
- Select **Finish** (not shown)

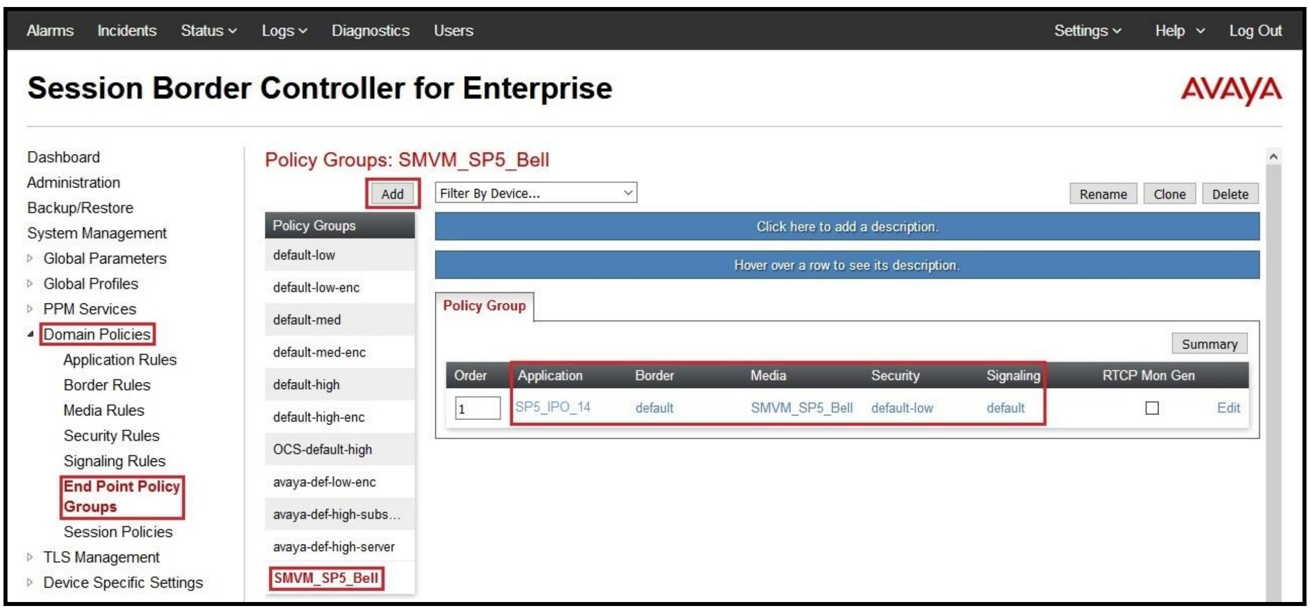

Figure 58: Endpoint Policy

7.10. Device Specific Settings

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

7.10.1. Manage Network Settings

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

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - **Name**: **Network_A1**
  - **Default Gateway**: **10.10.98.1**
  - **Subnet Mask**: **255.255.255.192**
  - **Interface**: **A1** (This is the Avaya SBCE inside interface)
  - Click the **Add** button to add the **IP Address** for inside interface: **10.10.98.13**
  - Click the **Finish** button to save the changes

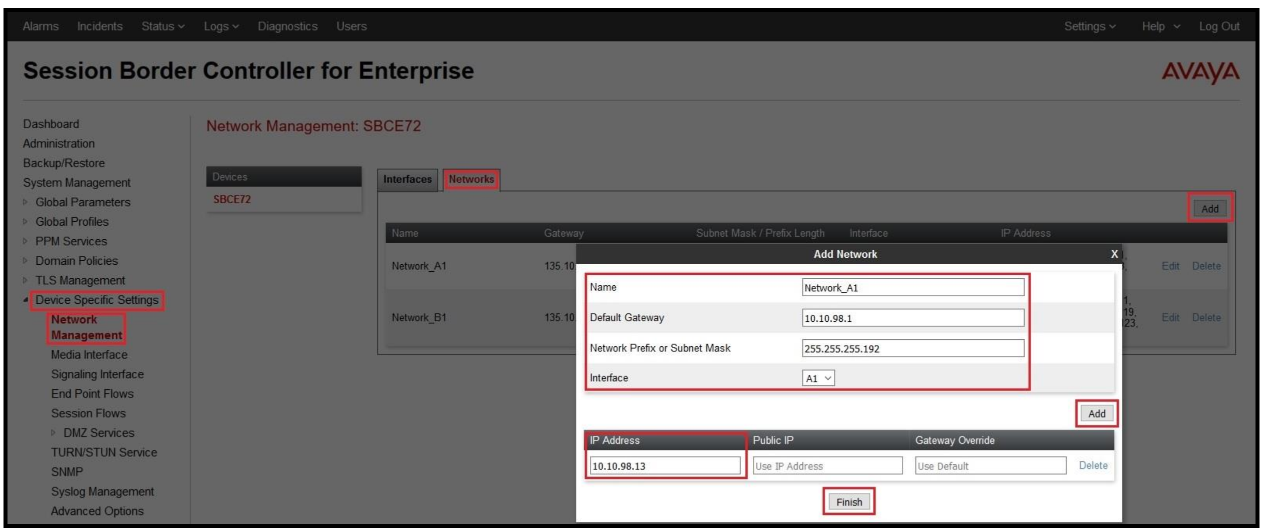

Figure 59: Network Management – Inside Interface

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

- Select **Networks** tab and click **Add** button to add a network for the outside interface as follows:
  - **Name**: **Network_B1**
  - **Default Gateway**: **10.10.98.97**
  - **Subnet Mask**: **255.255.255.224**
  - **Interface**: **B1** (This is the Avaya SBCE outside interface)
  - Click the **Add** button to add the **IP Address** for outside interface: **10.10.98.111**
  - Click the **Finish** button to save the changes

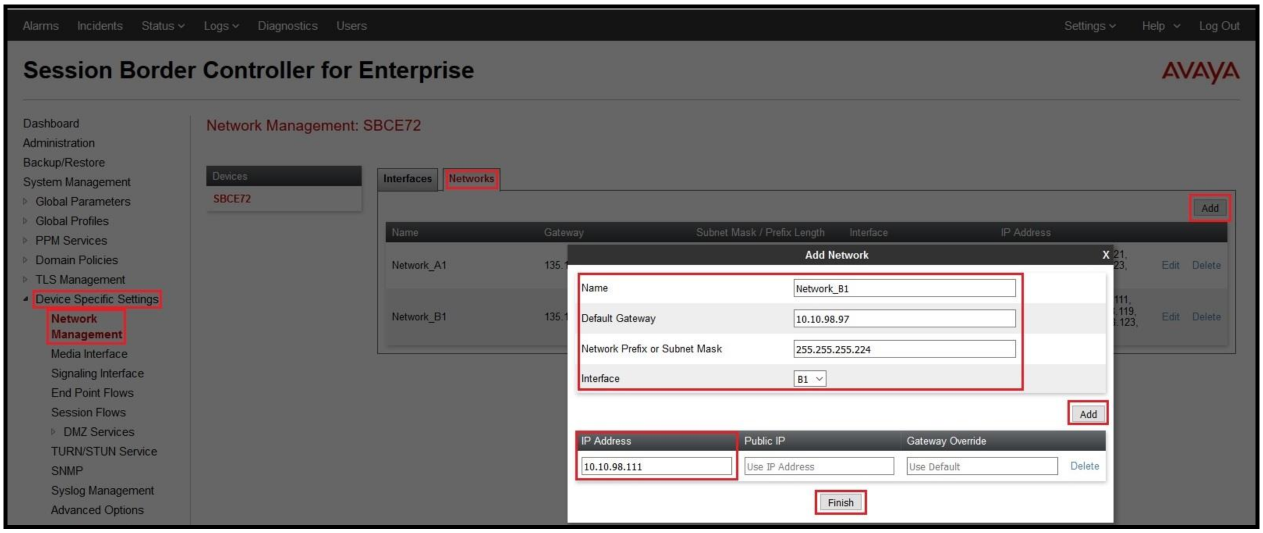

Figure 60: Network Management – Outside Interface

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

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

Figure 61: Network Management – Interface Status

7.10.2. Create Media Interfaces

Media Interfaces define the IP addresses and port ranges in which the Avaya SBCE will accept media streams on each interface. The default media port range on the Avaya SBCE can be used for inside port.

From the menu on the left-hand side, **Device Specific Settings → Media Interface**

- Select the **Add** button and enter the following:
  - **Name**: **InsideMedia1**
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Session Manager)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - **Name**: **OutsideMedia1**
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward Bell Canada)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)

Figure 62: Media Interface

7.10.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

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

- Select the **Add** button and enter the following:
  - **Name**: **OutsideUDP**
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward Bell Canada)
  - **UDP Port**: **5060**
  - Click **Finish** (not shown)

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

- Select the **Add** button and enter the following:
  - **Name**: **InsideTLS**
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Session Manager)
  - **TLS Port**: **5061**
  - **TLS Profile**: **AvayaSBCServer71**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
  - Click **Finish** (not shown)

Note: For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 the same as Bell Canada used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

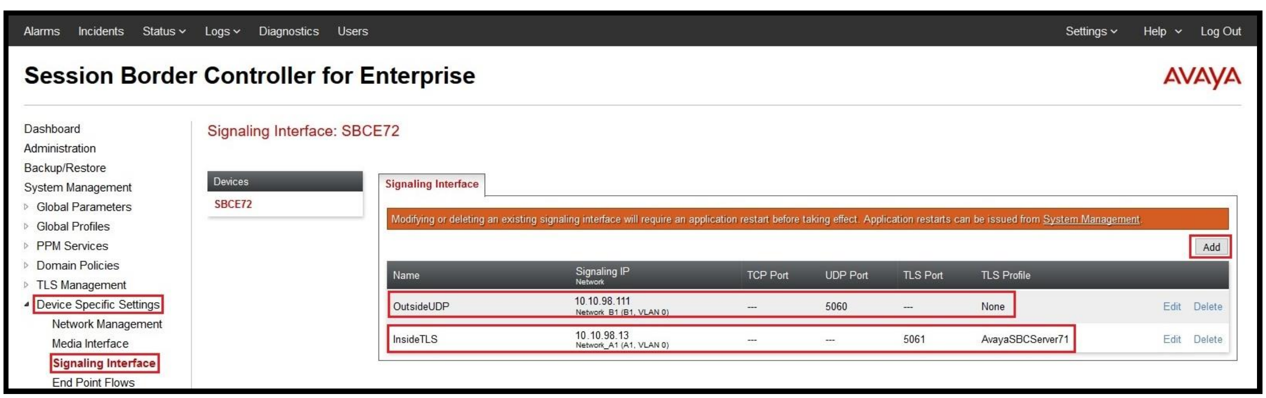

Figure 63: Signaling Interface

7.10.4. Configuration Server Flows

Server Flows allow an administrator to categorize trunk-side signaling and apply a policy.

7.10.4.1 Create End Point Flows – SMVM Flow

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

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name**: **SMVM Bell Flow**
    - **Server Configuration**: **SMVM** (see **Section 7.4**)
    - **URI Group**: *
    - **Transport: ***
    - **Remote Subnet: ***
    - **Received Interface**: **OutsideUDP** (see **Section 7.10.3**)
    - **Signaling Interface**: **InsideTLS** (see **Section 7.10.3**)
    - **Media Interface**: **InsideMedia1** (see **Section 7.10.2**)
    - **Secondary Media Interface**: **None**
    - **End Point Policy Group**: **SMVM_SP5_Bell** (see **Section 7.9.3**)
    - **Routing Profile**: **SMVM_To_SP5_Bell** (see **Section 7.7**)
    - **Topology Hiding Profile**: **SP5_Bell_To_SMVM** (see **Section 7.8**)
    - Leave other parameters as default
    - Click **Finish**

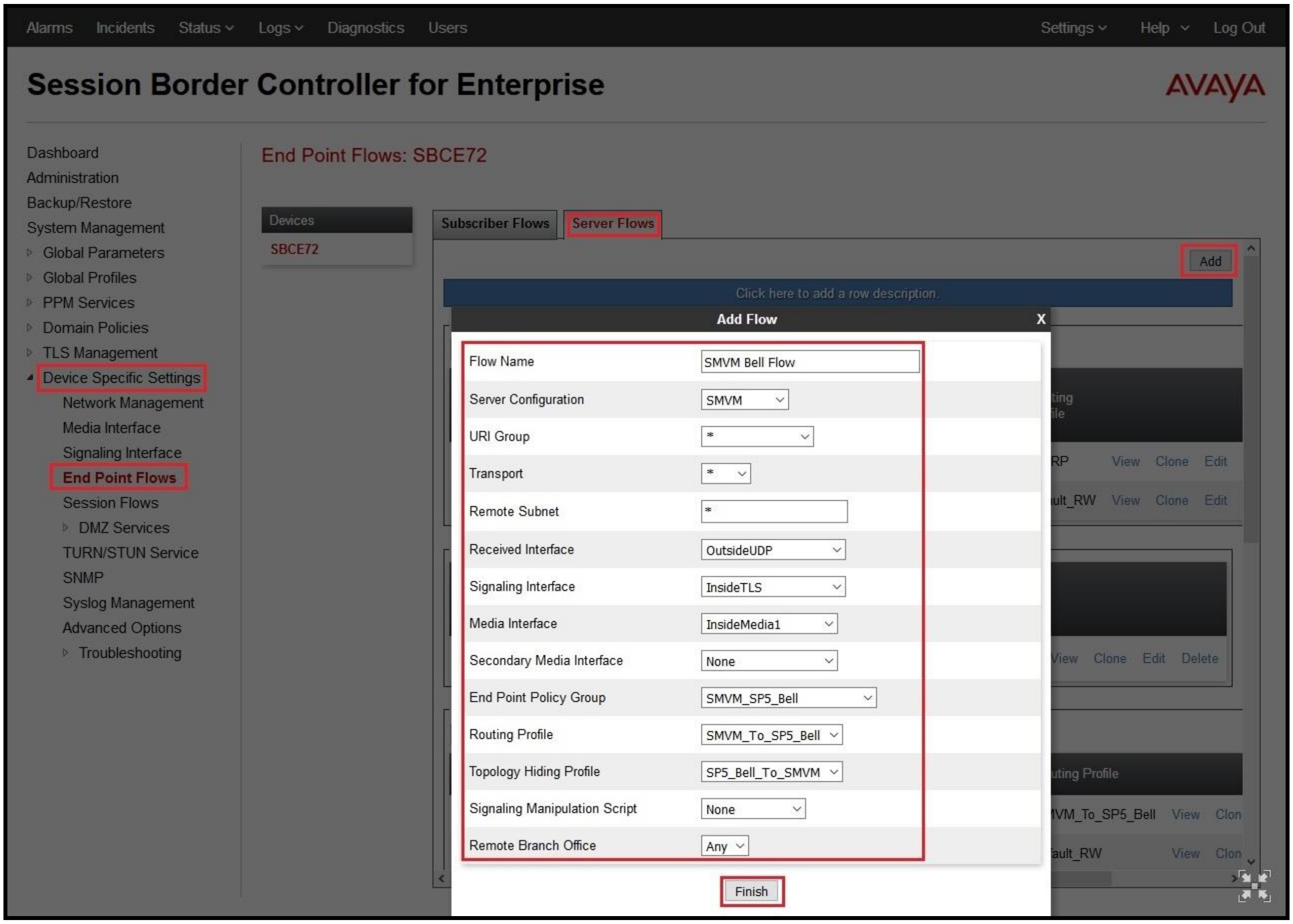

Figure 64: End Point Flow 1

7.10.4.2 Create End Point Flows – Bell Canada SIP Trunk Flow

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

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name**: **SP5 Bell Flow**
  - **Server Configuration**: **SP5-Bell** (see **Section 7.5**)
  - **URI Group**: *
  - **Transport: ***
  - **Remote Subnet: ***
  - **Received Interface**: **InsideTLS** (see **Section 7.10.3**)
  - **Signaling Interface**: **OutsideUDP** (see **Section 7.10.3**)
  - **Media Interface**: **OutsideMedia1** (see **Section 7.10.2**)
  - **Secondary Media Interface**: **None**
  - **End Point Policy Group**: **SMVM_SP5_Bell** (see **Section 7.9.3**)
  - **Routing Profile**: **SP5_Bell_To_SMVM** (see **Section 7.6**)
  - **Topology Hiding Profile**: **SMVM_To_SP5_Bell** (see **Section 7.8**)
  - Leave other parameters as default
  - Click **Finish**

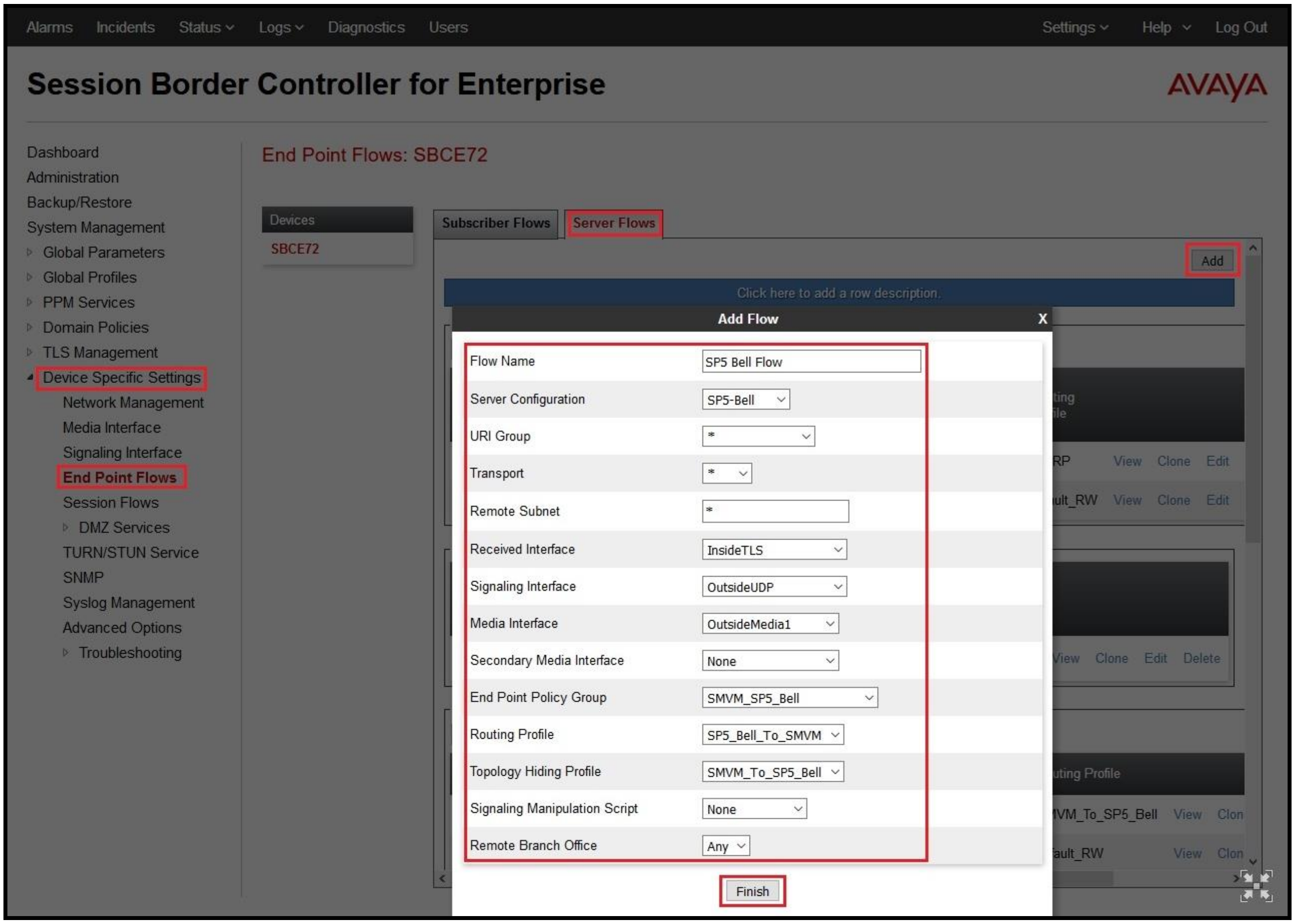

Figure 65: End Point Flow 2

8. Bell Canada SIP Trunk Configuration

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

- IP address and port number used for signaling or media servers through any security devices
- DID numbers
- Bell Canada SIP Trunk Specification (if applicable)

9. 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 SM Line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** for each channel. (The below screen shot showed 2 active calls at the time.)

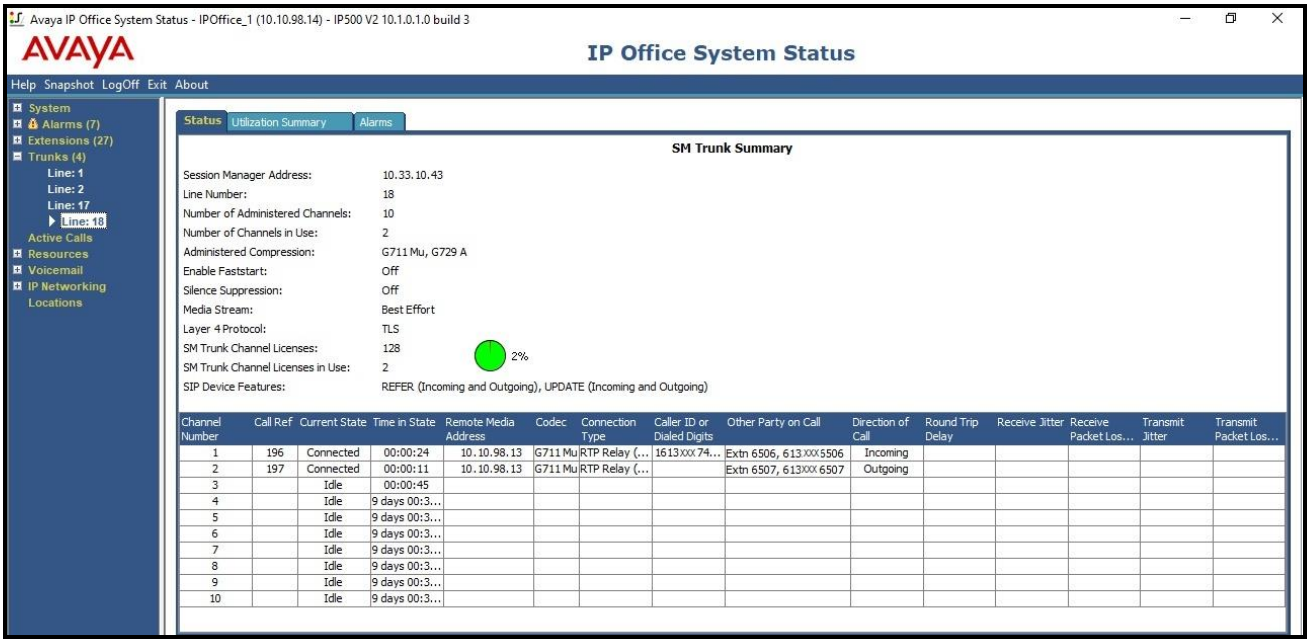

Figure 66 – SIP Trunk status

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

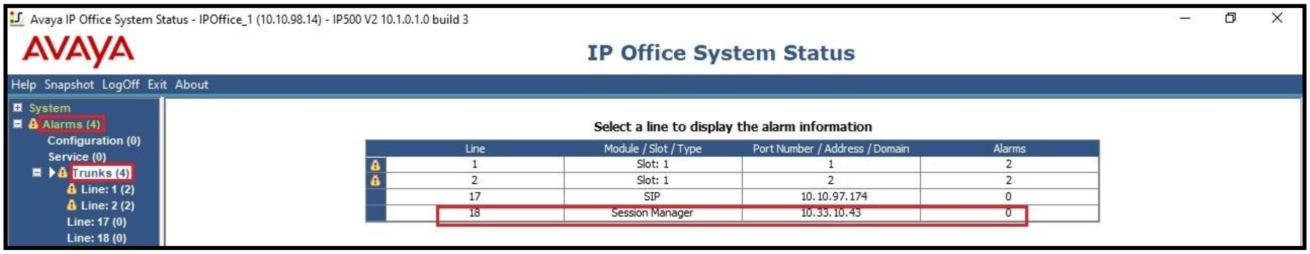

Figure 67 – SIP Trunk alarm

- Verify that a phone connected to the PSTN can successfully place a call to Avaya IP Office with two-way audio.
- Verify that a phone connected to Avaya IP Office can successfully place a call to the PSTN with two-way audio.
- Capture SIP call traces on Avaya SBCE by executing command via the Command Line Interface (CLI): Login Avaya SBCE with root user and enter the command: #traceSBC. The tool updates the database directly based on which trace mode is selected.

10. Conclusion

Bell Canada passed compliance testing with the limitation listed in **Section 2.2**. These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 10.1, Avaya Aura Session Manager 7.1 and the Avaya SBCE 7.2 to support Bell Canada SIP Trunking service, as shown in **Figure 1**.

11. Additional References

[1] Administering Avaya IP Office Platform with Manager, Release 10.1, 15-601011, Issue 14, July 2017.

[2] Deploying Avaya IP Office™ Platform IP500V2, Release 10.1, 15-601042, Issue 32d, May 2017.

[3] Avaya IP Office™ Platform Release 10.1 - Release Notes / Technical Bulletin General Availability

[4] Avaya Session Border Controller for Enterprise 7.2 Release Notes, Issue 1, June 2017

[5] Using Avaya Communicator for Web, Release 1, Issue 1.0.6, May 2016

[6] Administering Avaya Aura® Session Manager, Release 7.1.1, Issue 2, August 2017

[7] Administering Avaya Aura® System Manager, Release 7.1.1, Issue 7, October 2017

Product documentation for Avaya products may be found at: http://support.avaya.com. Additional IP Office documentation can be found at:
http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=manuals.xml&TEMPLATE=pdf_feed_template.html

Product documentation for Bell Canada SIP Trunking may be found at:
https://business.bell.ca/shop/enterprise/sip-trunking-service

12. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.3**:

```
within session "ALL"
{

 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
       //This is optional for ONND testing
       //remove(%HEADERS["P-Asserted-Identity"][1]);

       //For anonymous outbound call using PPI

          %HEADERS["P-Preferred-Identity"][1].regex_replace("sip:6506@10.10.98.14:5061","sip:613XXX6506@vendor6.lab.internetvoice.ca");
          %HEADERS["P-Preferred-Identity"][1].regex_replace("sip:6507@10.10.98.14:5061","sip:613XXX6507@vendor6.lab.internetvoice.ca");
          %HEADERS["P-Preferred-Identity"][1].regex_replace("sip:6508@10.10.98.14:5061","sip:613XXX6508@vendor6.lab.internetvoice.ca");

         if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("613XXX650[6-8]")) then
          {
          %var="this does nothing, match for DID number passed";
             }

        else
             {
  //For mobile extension/off-net Call Forward feature

          %HEADERS["P-Asserted-Identity"][1].URI.USER = %HEADERS["Contact"][1].URI.USER;

          }

       }

}
```

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.