Avaya Solution & Interoperability Test Lab

Application Notes for Telstra Enterprise SIP Trunking Service with Avaya IP Office Release 10 and Avaya Session Border Controller for Enterprise Release 7.1 - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya IP Office Release 10 with SIP Trunks to the Avaya Session Border Controller for Enterprise Release 7.1 (Avaya SBCE) when used to connect the Telstra Enterprise SIP Trunking service available from Telstra (Australia).

Telstra Enterprise SIP Trunking service provides PSTN access via a SIP trunk between the enterprise and the Telstra 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 any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Telstra 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 Telstra lab.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration for Avaya IP Office Release 10 with SIP Trunks to the Avaya Session Border Controller for Enterprise Release 7.1 (Avaya SBCE) when used to connect to the Telstra Enterprise SIP Trunking service available from Telstra (Australia).

The enterprise SIP Trunking service available from Telstra is one of many SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. The Telstra Enterprise SIP Trunking service allows enterprises in Australia to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

2. General Test Approach and Test Results

The general test approach was to make calls from/to the Avaya IP Office through the Avaya SBCE using Telstra Enterprise SIP Trunking service. The 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

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya IP Office, the Avaya SBCE, and the Telstra Enterprise SIP Trunking service.

The compliance testing was based on the standard Avaya DevConnect Generic SIP Trunk test plan and the Telstra SIP Connect Accreditation Test Plan. The testing covered functionality required for compliance as a solution supported on the Telstra Enterprise SIP Trunk network. Calls were made to and from the PSTN across the Telstra network. The following standard features were tested as part of this effort:

- Inbound PSTN calls to various phone types including H.323, SIP, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, SIP, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows.
- Inbound and outbound PSTN calls to/from Avaya Communicator for Web.
- Inbound and outbound IP Office calls from/to Telstra IP Telephony (TIPT phones).

- Inbound and outbound IP Office calls from/to Telstra Digital Office Technology (DOT phones).
- Dialing plans including local, long distance, international, outbound toll-free, calls etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.711A, G.711MU and G.729A.
- Incoming and outgoing fax using G.711 pass-through.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward with Diversion method.
- Mobile twinning.
- Response to OPTIONS heartbeat and Registration.
- Response to incomplete call attempts and trunk errors.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.
- Telstra Enterprise SIP Trunk failover.

2.2 Test Results

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

Please refer to the test case document for a complete list of solution issues found when tested.

- **Faxing** – Telstra Enterprise SIP Trunking service only supports FAX G.711 pass-through mode. G.711 fax pass-through was successfully tested during the compliance test.
- **Direct Media** – Direct Media must be turned off for SIP Line on IP Office to Telstra otherwise one way speech path may occur when changing media path mid call.

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com
- **Telstra:** Customers should contact their Telstra Business representative or follow the support links available on http://telstra.com.au

3. Reference Configuration

The reference configuration used in these Application Notes is shown in the diagram below and consists of several components.

- Avaya IP Office Application Server running on VMware ESXi 5.5.
- Avaya IP Office 500 V2.
- Avaya IP phones are represented with Avaya 9600 Series IP Telephones running H.323 software, Avaya 1600 Series IP Telephones running H.323 software, and Avaya 1100 Series IP Telephones running SIP software.
- Avaya Communicator for Windows 2.1.

- Avaya 1400 Series Digital Telephones.
- The Avaya SBCE 7.1 provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the Telstra Enterprise SIP Trunking service and the enterprise internal network.
- Telstra Enterprise SIP Trunking service provided two groups for SIP trunks. The solution as detailed in these application notes was a dual-trunk setup, with the single SBC configured up with two separate trunks, originating from two separate SBC's within the Telstra lab network ('sbc-cw.ipvs.net' and 'sbc-exh.ipvs.net'). Each trunk had different registration credentials, and was provisioned with a separate number range (Trunk Pilot numbers and DID's). DID range assigned by Telstra for this testing: 0353xxxxxx (10 digits).

The following is a summary of requirements for Telstra Enterprise SIP Trunk to process the incoming SIP INVITE to Telstra:

- The Enterprise Trunk Pilot number is required to be substituted into the P-Asserted-Identity Header.
- Calls originating from the customer equipment with the From Header as 'anonymous@anonymous.invalid' or 'anonymous@customer.sip.domain' (example) are no longer accepted. The From header always needs to be a valid DID number that is associated with the Enterprise SIP trunks.

Signaling Manipulation scripts are added on Avaya SBCE to satisfy above requirement.

All IP addresses shown in the diagram are private IP addresses:

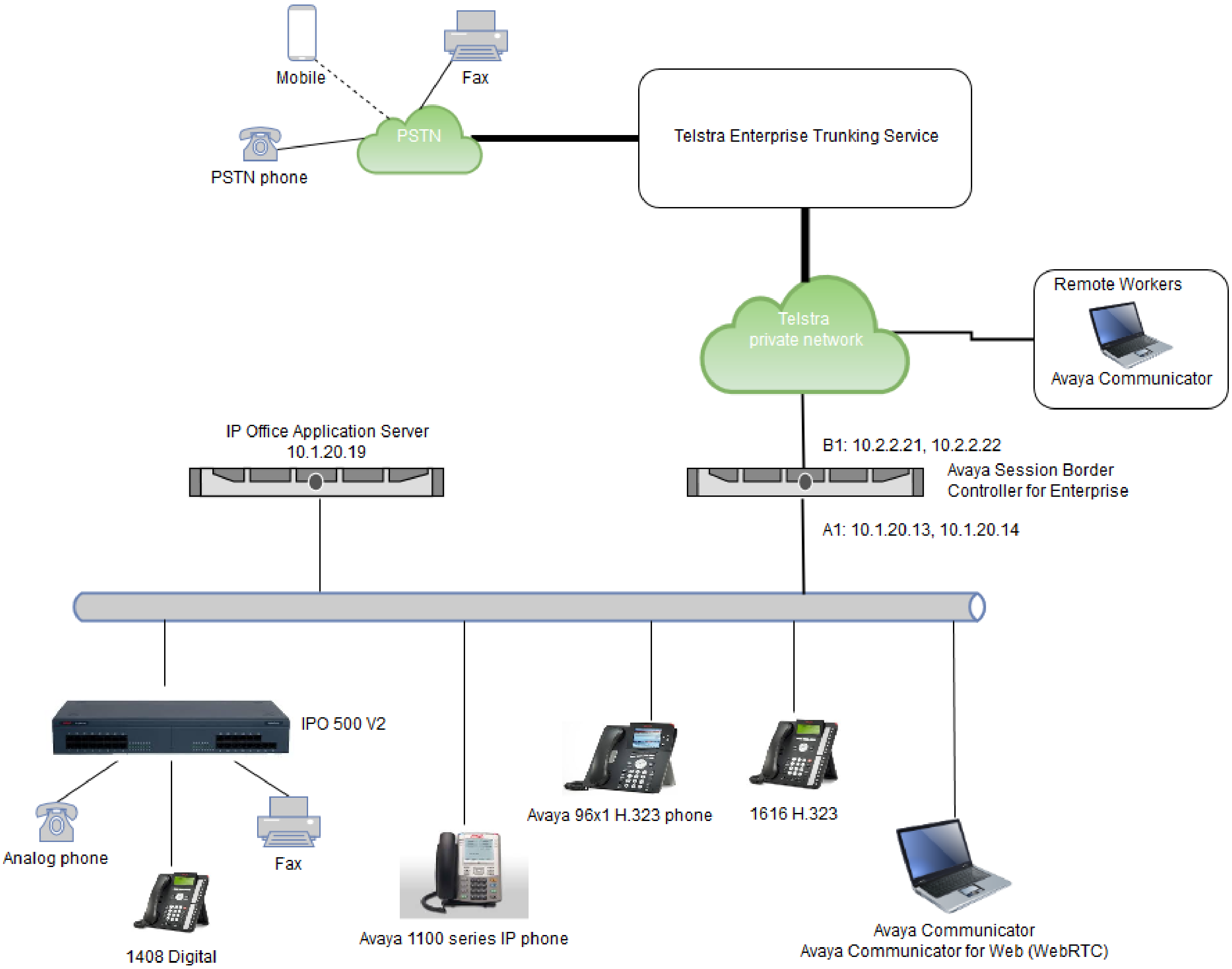


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

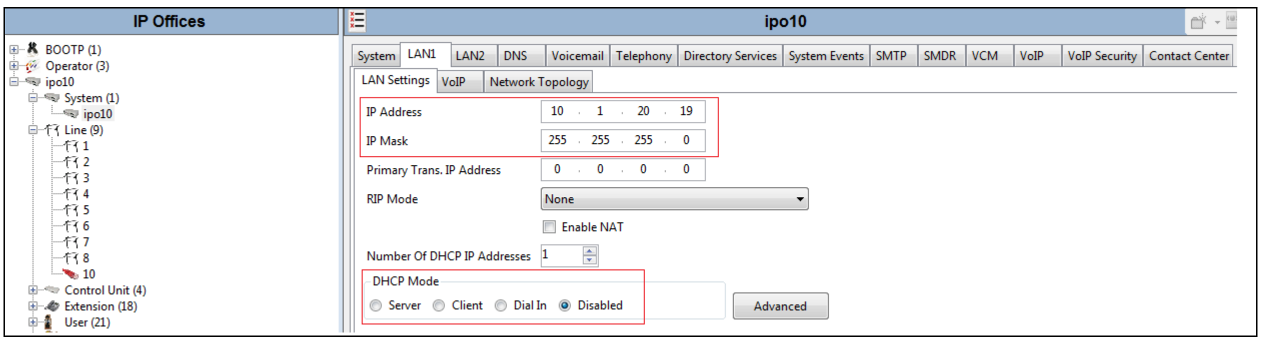
Component	Version
Avaya	
Avaya Session Border Controller for Enterprise	7.1.0.0-04-11122
Avaya IP Office	10.0.0.0.550
Avaya Communicator for Windows	2.1.3.237
Avaya 9600 series H.323 IP Deskphone	6.6.2.29
Avaya 1100 series SIP IP Deskphone	4.4.23
Avaya 1616 H.323 IP Deskphone	1.39A
Analog phone	N/A
Avaya 1408 Digital phone	Application R46 Boot 25
Service Provider	
BroadSoft	R19 SP1

5. Configure Avaya IP Office

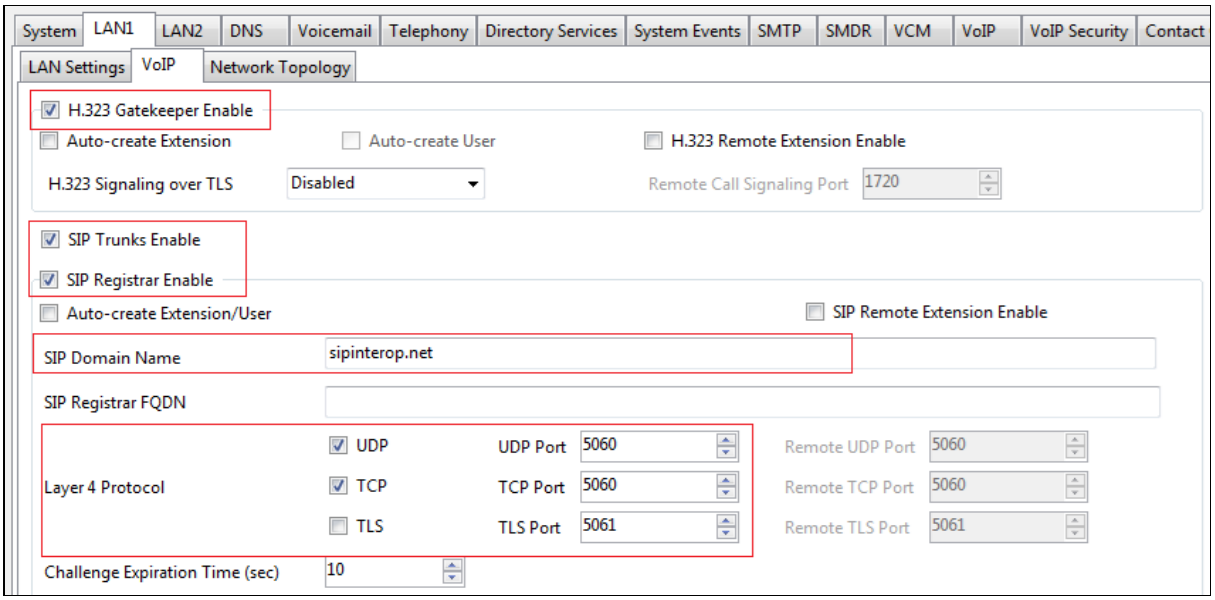
This section describes the Avaya IP Office configuration to support connectivity to Telstra Enterprise SIP Trunking service. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start > Programs > IP Office > 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 (not shown).

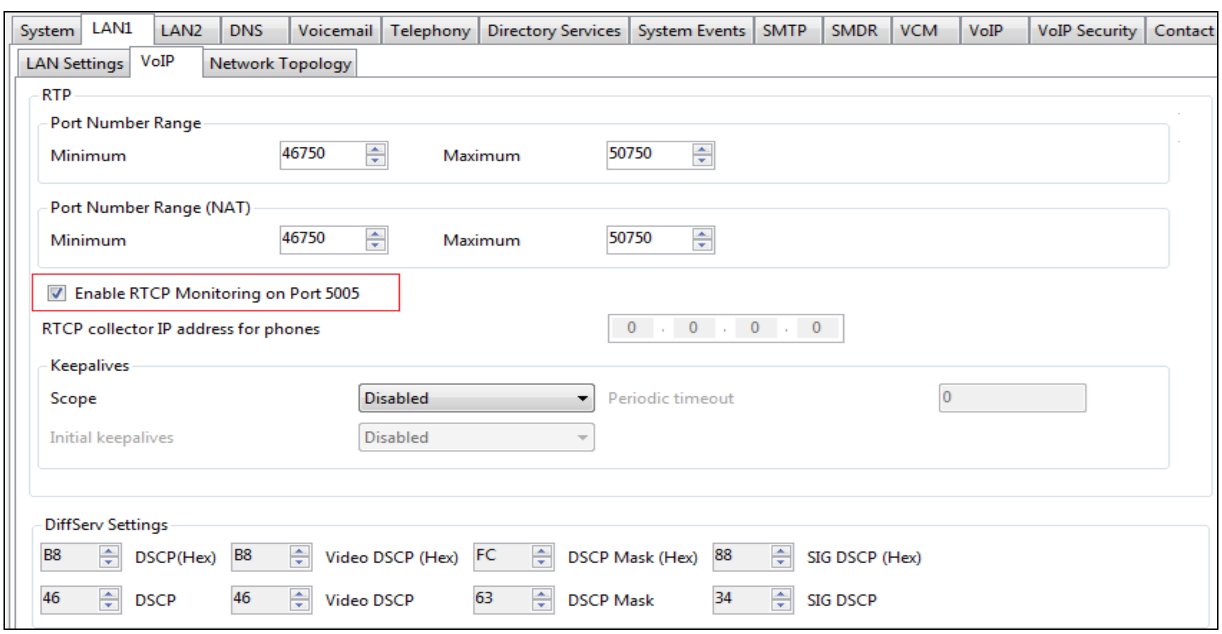
5.1 LAN1 Settings

In the sample configuration, IPO10 was used as the system name and the LAN1 port was used to connect to Telstra Enterprise SIP Trunking service. To access the LAN1 settings, first navigate to **System (1) > IPO10** in the **Navigation** and **Group** panes and then navigate to the **LAN1 > LAN Settings** tab in the **Details** pane. Set the **DHCP Mode** to **Disabled**, then set the **IP Address** field to the IP address assigned to the Avaya IP Office LAN port. Set the **IP Mask** field to the mask used on the network. Other parameters are set as default values.



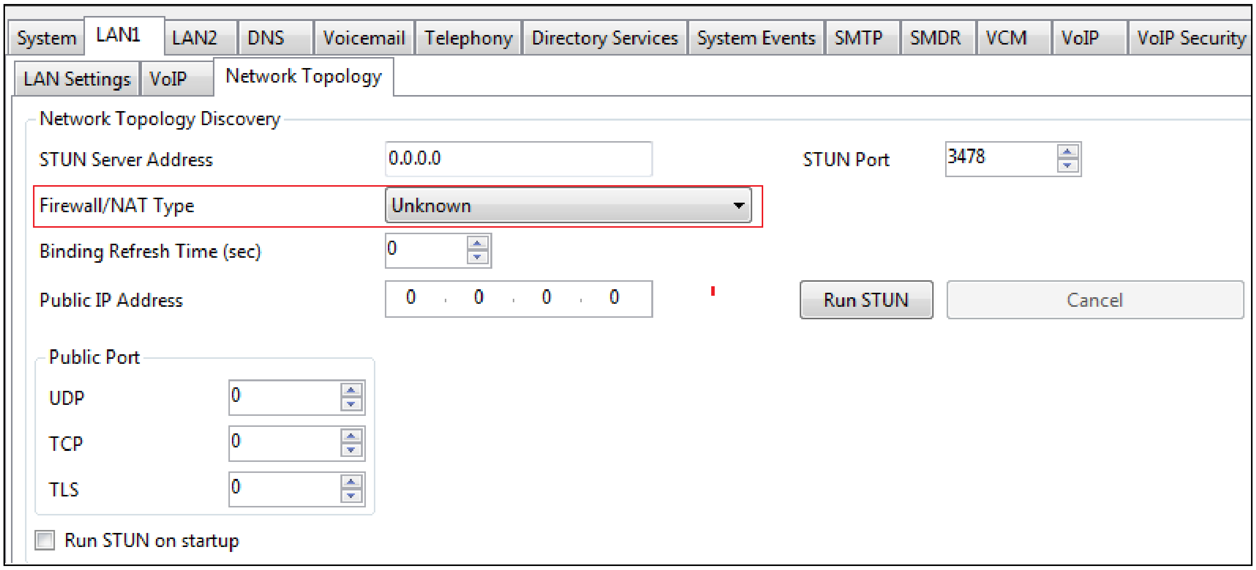
Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the 9600-Series IP Telephones used in the sample configuration. The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to Telstra. The **SIP Registrar Enable** box is checked to allow Avaya IP Office SIP phones usage. The **SIP Domain Name** is set to desired IP Office SIP domain. The **Layer 4 Protocol** use **UDP** with port **5060** and **TCP** with port **5060**. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. The **Enable RTCP Monitoring on Port 5005** is checked. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements.





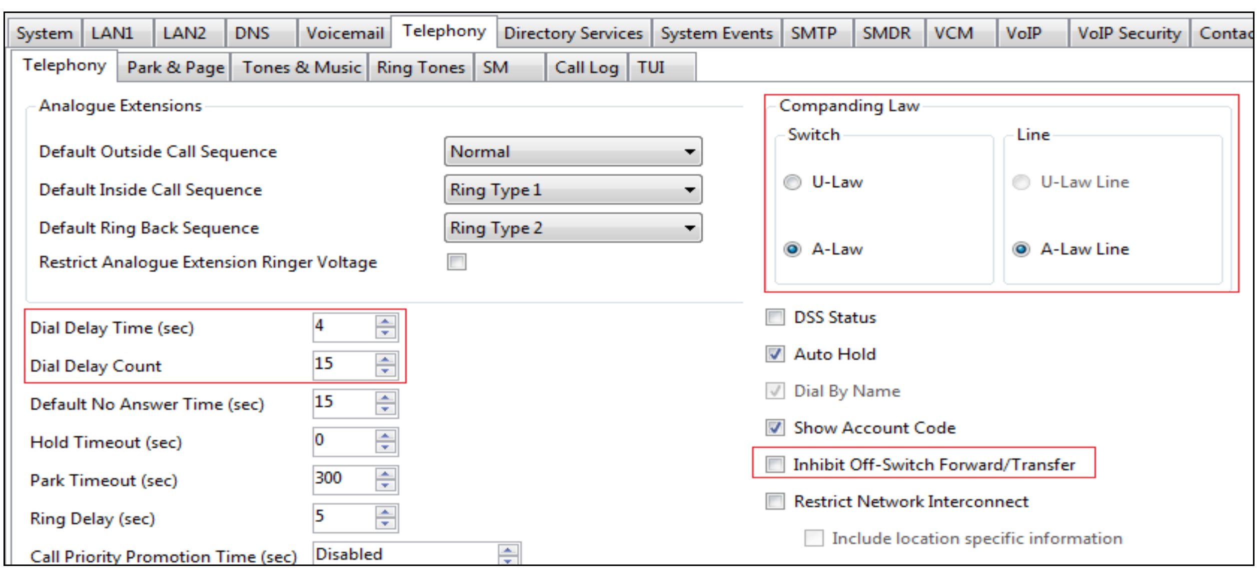
On the **Network Topology** tab in the **Details** Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. The parameter was set to **Unknown**. All other parameters should be set according to customer requirements.



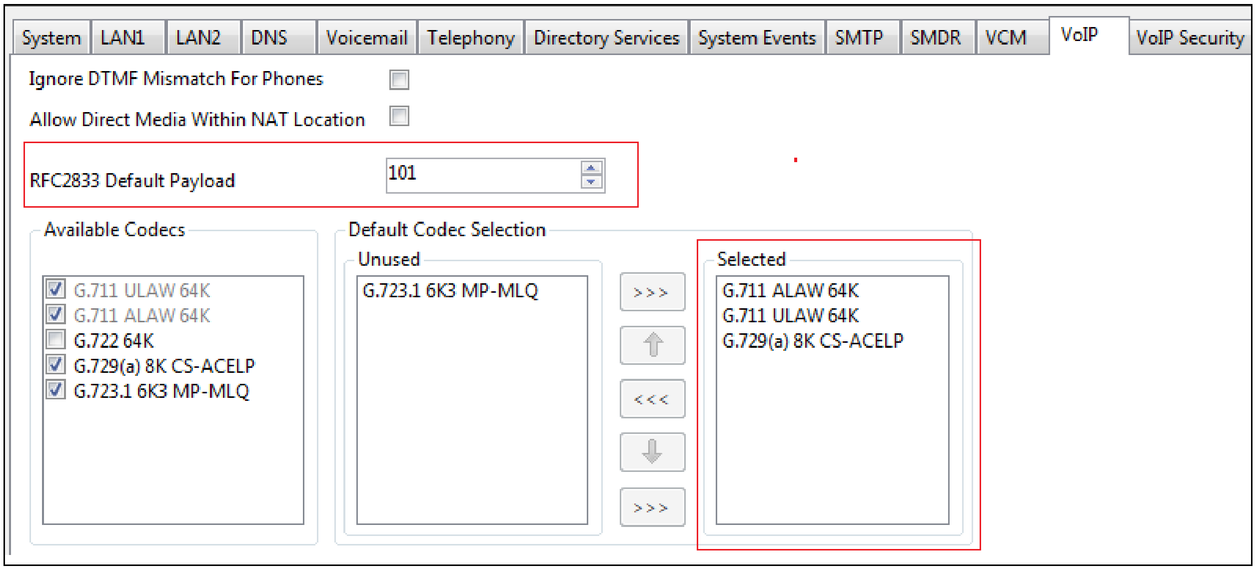
5.2 System Telephony Settings

Navigate to **System (1) > IPO10** in the **Navigation** and **Group** panes and then navigate to the **Telephony > Telephony** tab in the **Details** pane. Choose the **Companding Law** typical for the enterprise location. For Australia, **A-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 **Dial Delay Count** to **15** so IP Office will allow up to 15 digit dialing. Set **Dial Delay Time (sec)** to desired number.



5.3 System Codec Settings

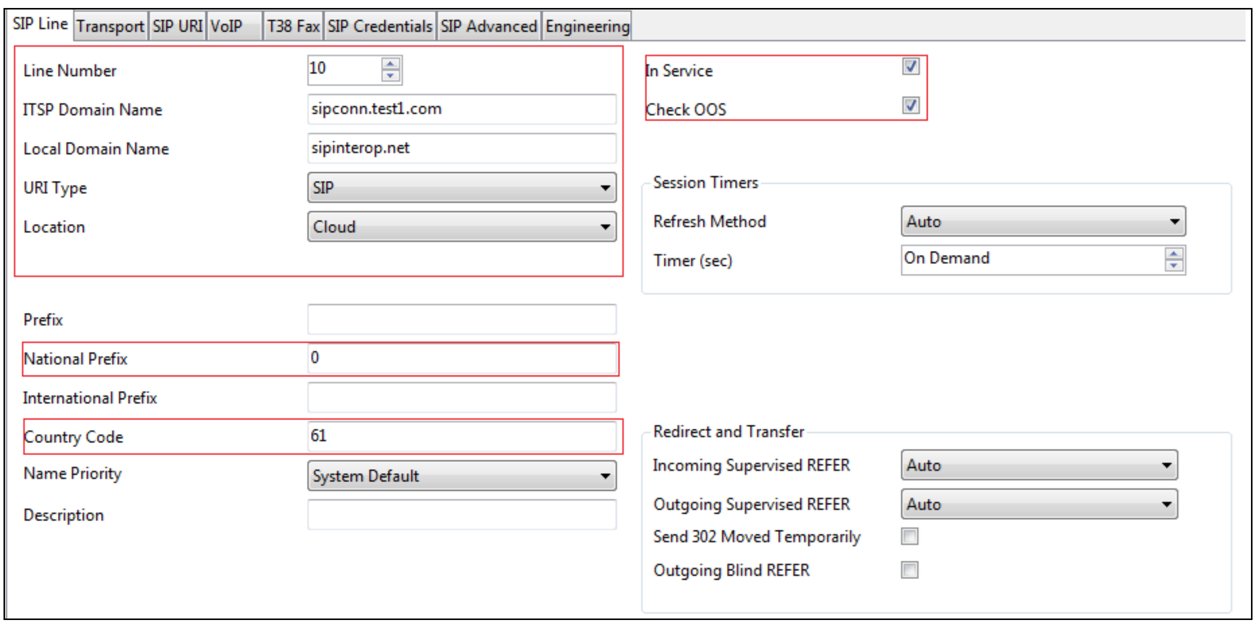
Navigate to **System (1)** > **IPO10** in the **Navigation** and **Group** panes and then navigate to the **Codecs** tab in the **Details** pane. Choose the **RFC2833 Default Payload** as IP Office default of **101**. Select codecs **G.711 ALAW 64K**, **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** that Telstra supports.



5.4 Administer SIP Line

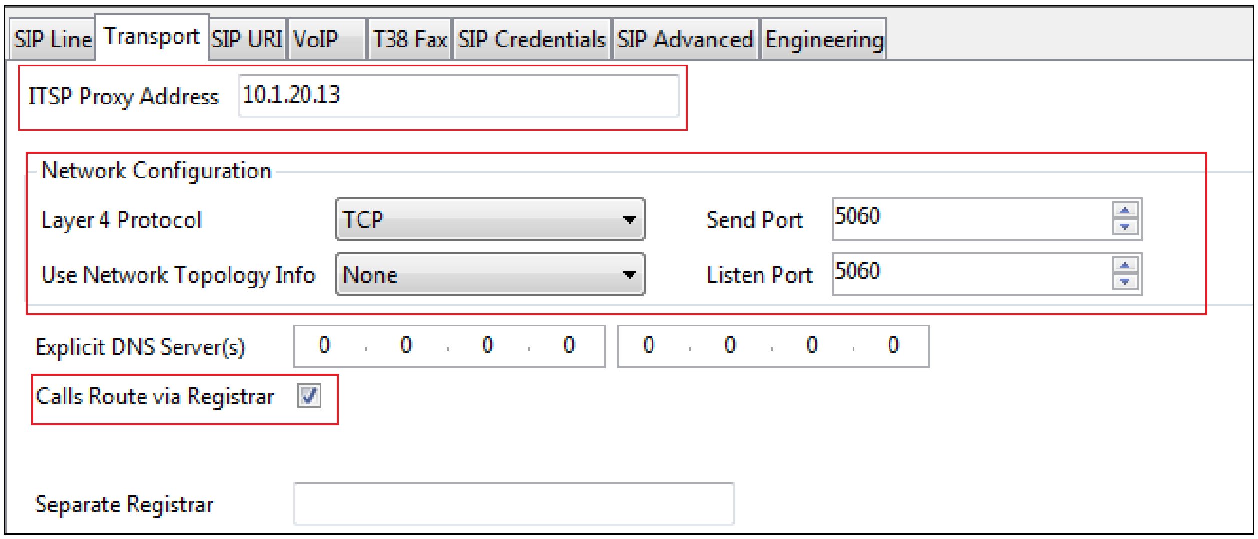
A SIP line is needed to establish the SIP connection between Avaya IP Office and Telstra Enterprise SIP Trunking service. To create a SIP line, begin by navigating to **Line** in the left **Navigation** pane, then right-click in the **Group** pane and select **New > SIP Line** (not shown) and enter the desired number for **Line number** (here 10 was chosen). 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 the SIP URI in SIP headers such as the From header.
- Set **Local Domain Name** to the same domain set in **LAN1**.
- Check the **In Service** box.
- Set **URI Type** to SIP.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Set **Location** to **Cloud**.
- Set **Country Code** to **61** (Country Code of Australia).
- Set **National Prefix** to **0**.
- Default values may be used for all other parameters.



Select the **Transport** tab:

- The **ITSP Proxy Address** is set to the IP address of Avaya SBCE A1 Interface which is used for SIP trunk with Telstra. As shown in **Figure 1**, this IP address is 10.1.20.13.
- In the **Network Configuration** area, **TCP** is selected as the Layer 4 Protocol, and the **Send Port** is set to the port number provided by Telstra, in this case the well-known SIP port of **5060** was used. The **Use Network Topology Info** parameter is set to **None**. Other parameters retain default values in the screen below.
- Check **Calls Route via Registrar**.

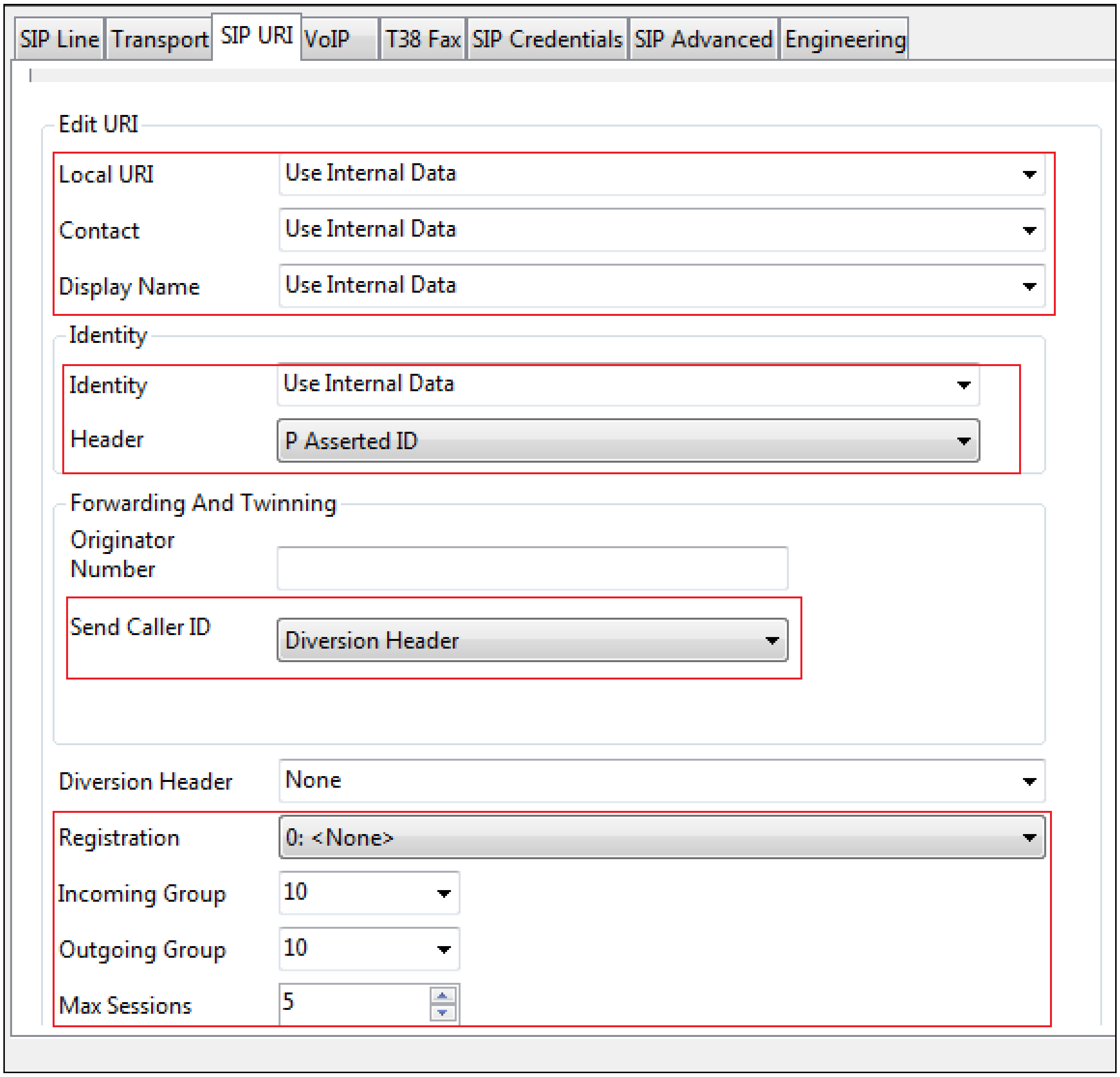


A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab then click the **Add** button and the **New Channel** area will appear at the bottom of the pane (not shown).

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:

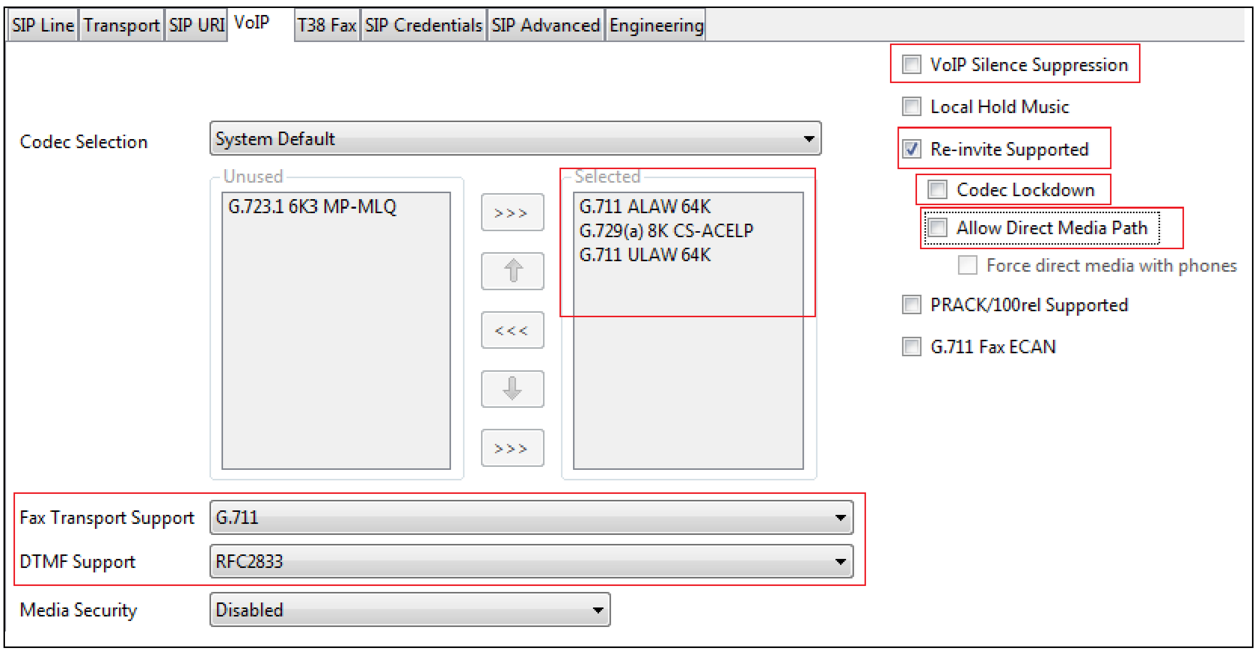
- Set **Local URI**, **Contact**, and **Display Name** to **Use Internal Data**. This setting allows calls on this line which SIP URI matches the number set in the SIP tab of any User as shown in **Section 5.7**.
- Under **Identity:** set **Identity** to **Use Internal Data** and set **Header** to **P Asserted ID**. 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 5.7**.
- Set **Registration** to **0: <None>**.
- Set **Send Caller ID** to **Diversion Header** for **Forwarding and Twinning**.
- 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 **10** was defined that only contains this line (line 10).

- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.



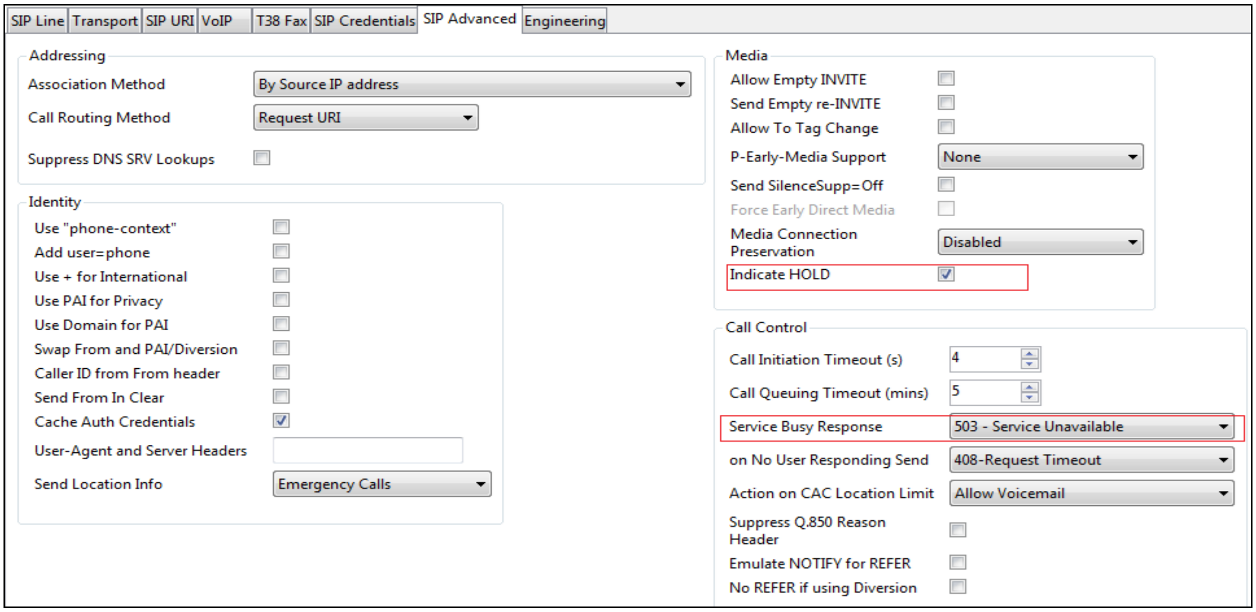
Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- The Codec Selection can be selected by choosing Custom from the pull-down menu, allowing an explicit ordered list of codecs to be specified. Selecting **G.711 ULAW 64K**, **G.729(a) 8K CS –ACELP** and **G.711 ULAW 64K** codecs causes Avaya IP Office to include these codecs, which are supported by Telstra Enterprise SIP Trunking service.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Uncheck **Codec Lockdown** box.
- Uncheck **Allow Direct Media Path** box.
- Set **Fax Transport Support** to **G.711** from the pull-down menu.
- Set the **DTMF Support** to **RFC2833** from the pull-down menu.
- Default values may be used for all other parameters.



Select **SIP Advanced** tab:

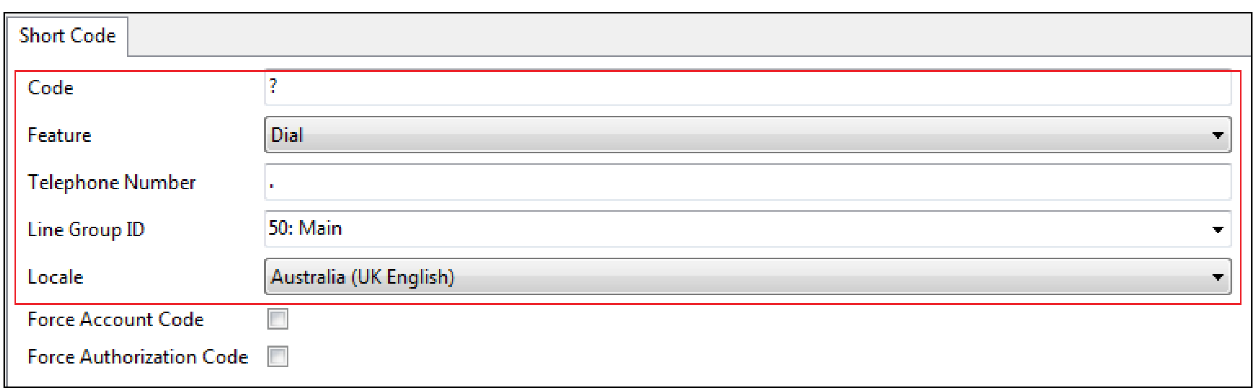
- Check **Indicate HOLD** box.
- Select **503-Service Unavailable** for **Service Busy Response** as requested by Telstra.



5.5 Short Codes

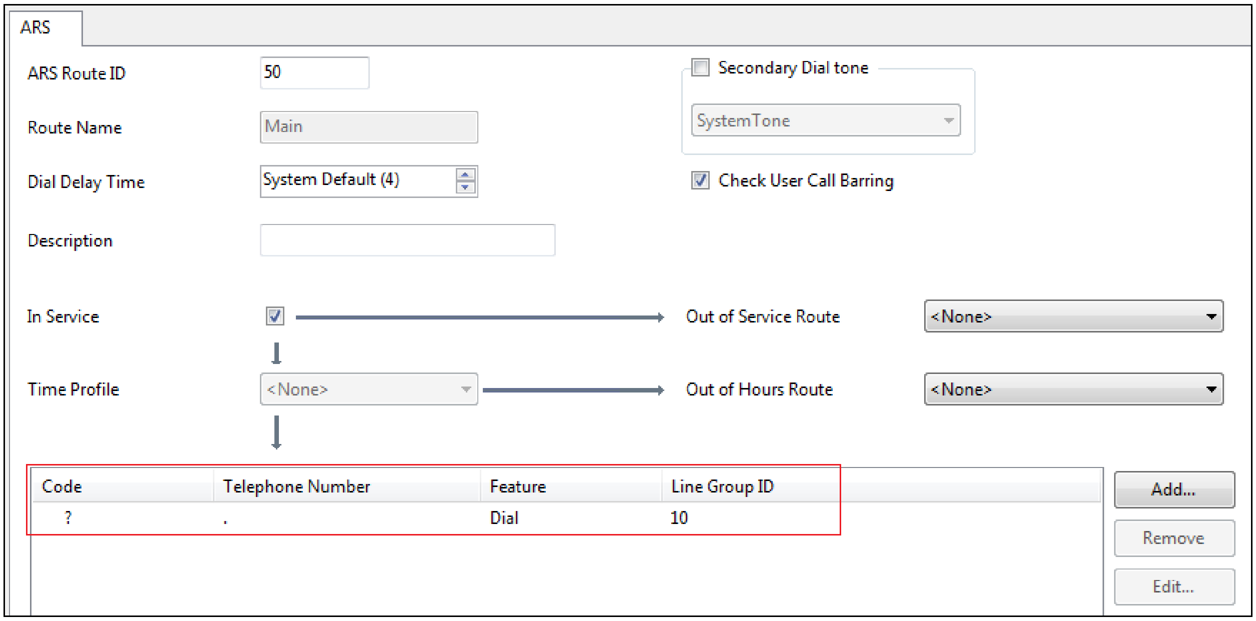
Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation pane and select **New** (not shown). On the **Short Code** tab in the **Details** pane, configure the parameters as shown below:

- In the **Code** field, enter the dial string which will trigger this short code. The example shows "**?**" which will be invoked when the user dials any digits.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to "**.**".
- Set the **Line Group Id** to **50:Main**.
- Set **Locale** to **Australia (UK English**).



5.6 ARS table

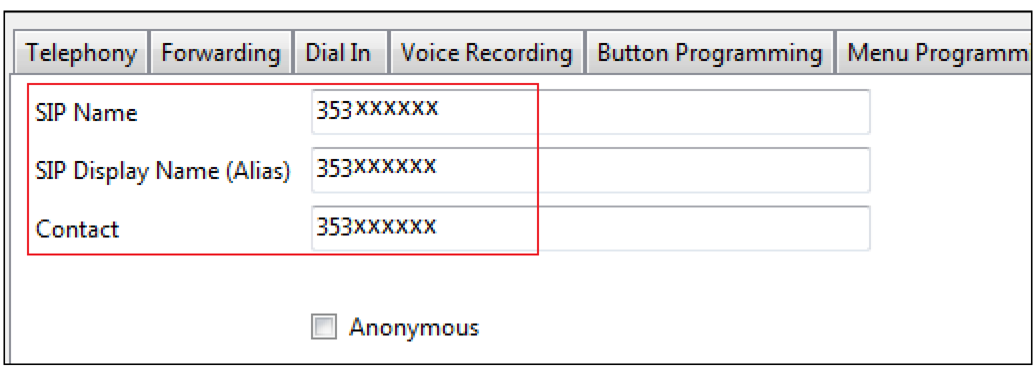
ARS Route ID 50 was selected to route outbound calls as defined in the Short Code in **Section 5.5**. That Short Code and the SIP Line created in **Section 5.4** must be added to this ARS Route ID as shown below.



5.7 User

Any user that is used to make outbound calls to Telstra must be configured with one of the DID numbers assigned by Telstra.

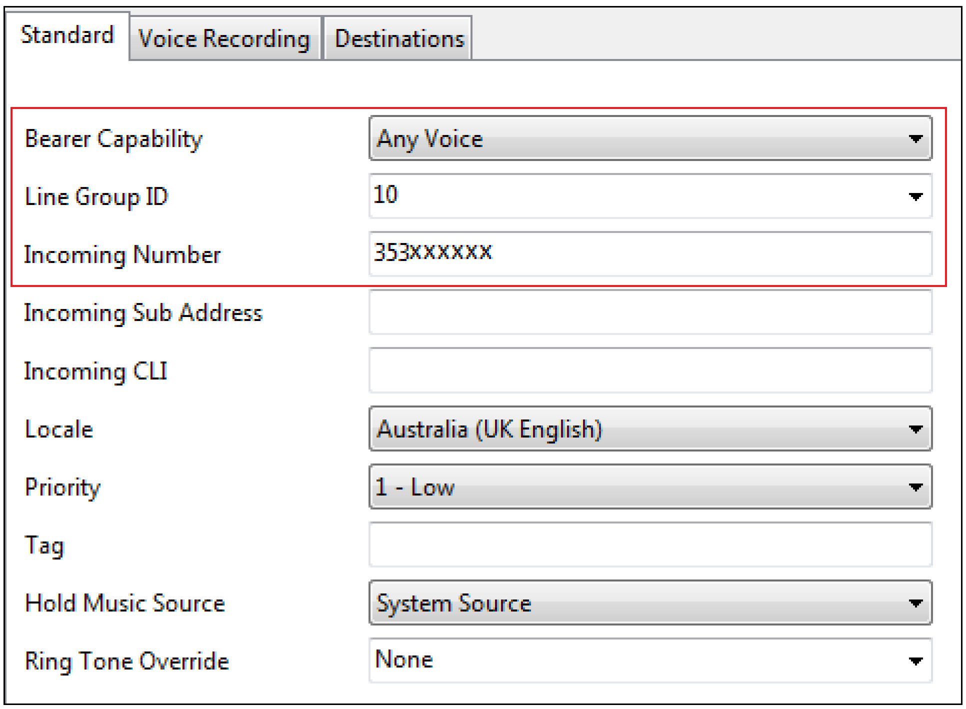
Select a user and navigate to **SIP** tab of that user, enter one of the DID numbers to **SIP Name**, **SIP Display Name (Alias)** and **Contact**.



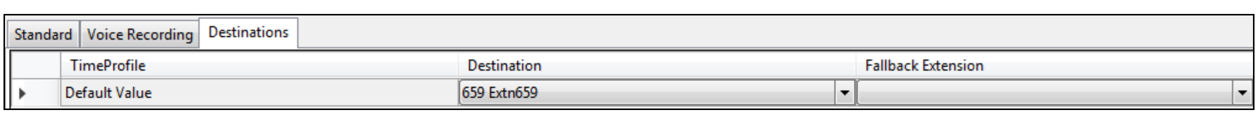
5.8 Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the **Navigation** pane and select **New** (not shown). On the **Standard** tab of the **Details** pane, enter the parameters as shown below:

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left. In this sample configuration, assigned DID numbers starting with 353 have been masked as 353xxxxxxx due to security reasons.
- Default values can be used for all other fields.

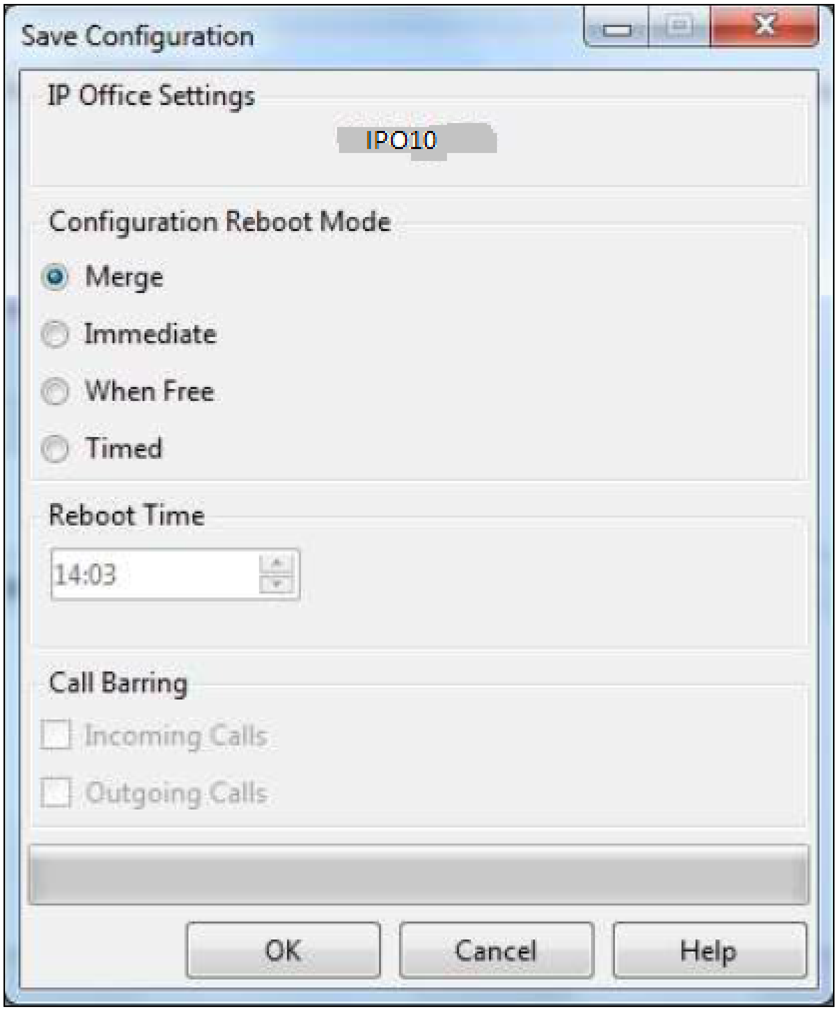


On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DID number **353xxxxxx** on line 10 are routed to extension 659.



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. A screen like the one shown below is displayed where the system configuration has been changed and needs to be saved on the system. **Merge**, **Immediate**, **When Free** or **Timed** is shown under the **Configuration Reboot Mode** column, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration.



6. Configure Avaya Session Border Controller for Enterprise

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

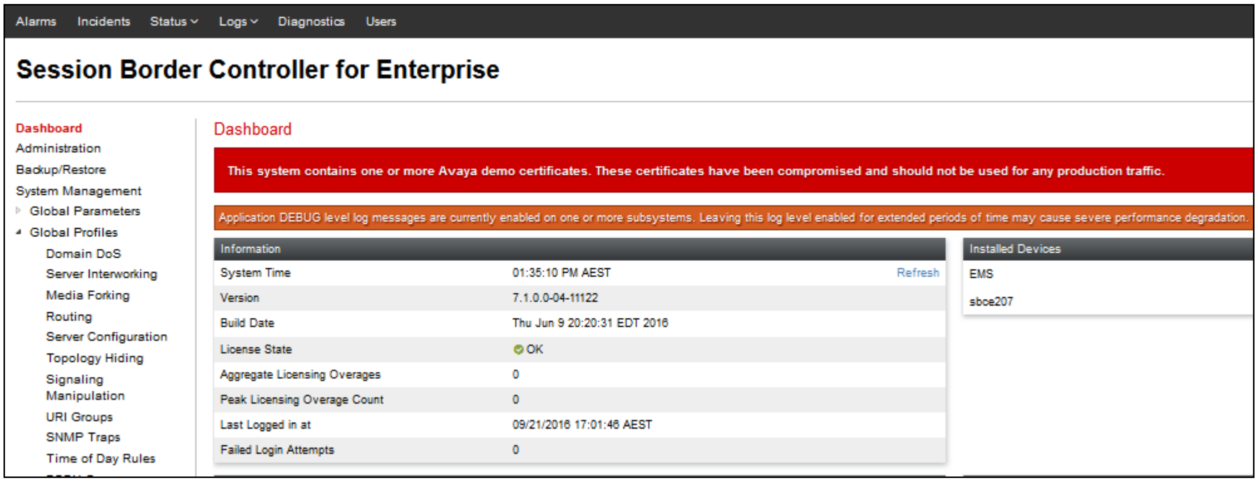
IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the enterprise site, (10.1.20.13), with access to the IP Office network. The connection to Telstra uses the Avaya SBCE public interface B1 (IP address 10.2.2.21). The follow provisioning is performed via the Avaya SBCE GUI interface, using the "M1" management LAN connection on the chassis.

1. Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the **Username** and click on **Continue**.

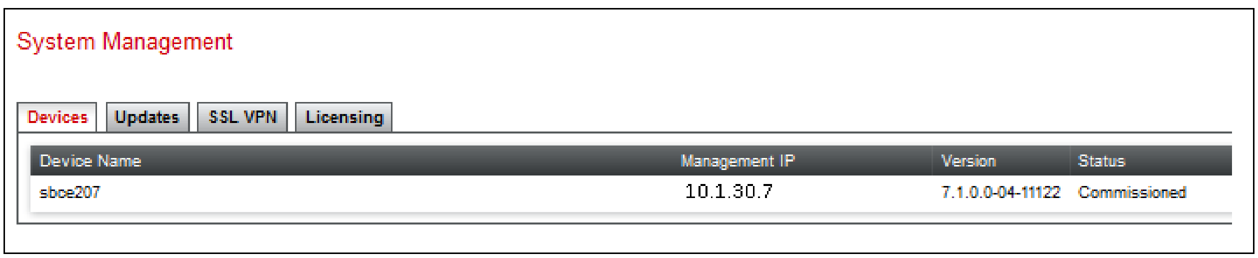
3. Enter the password and click on **Log In**.

The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

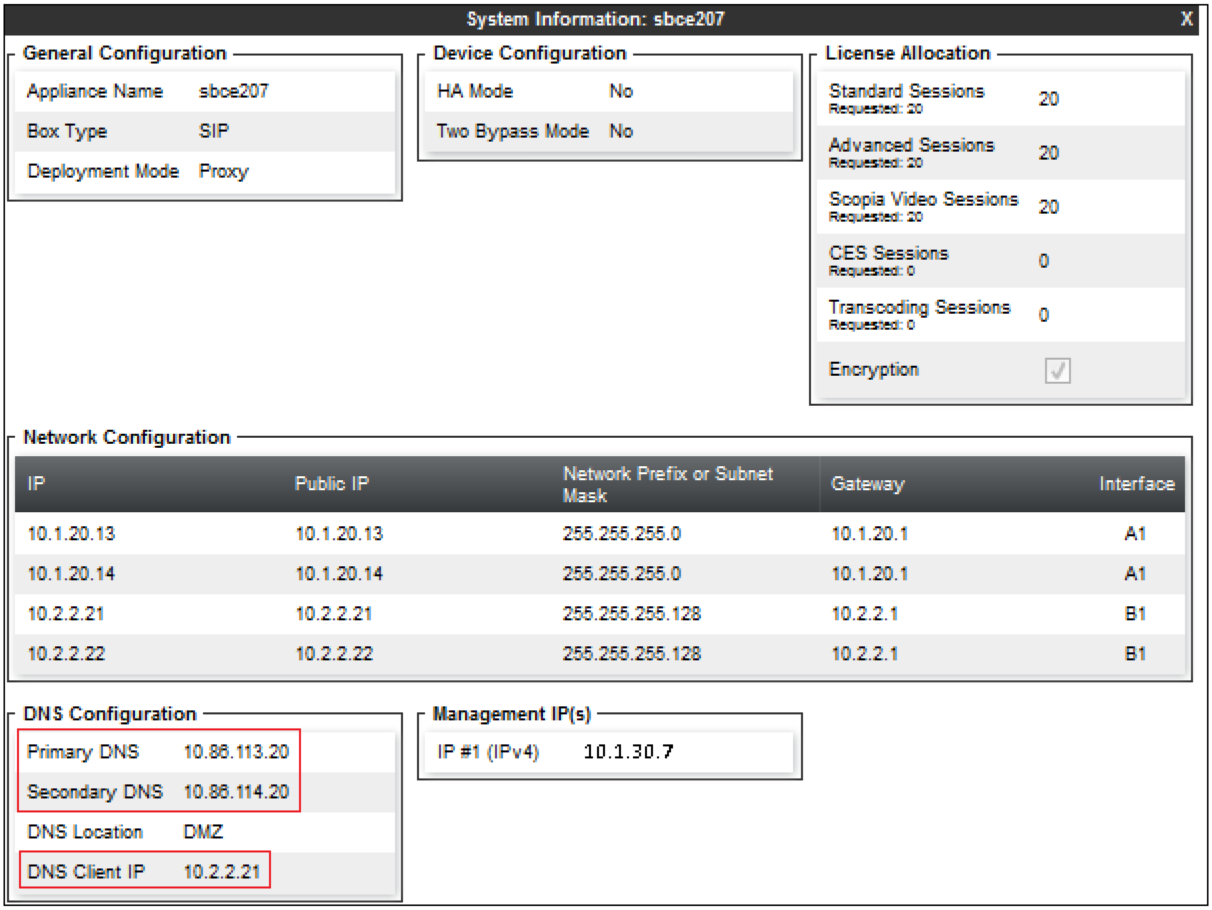


6.1 System Management – Status

1. Select **System Management** and verify that the **Status** column says **Commissioned**.



2. Click on **View** (not shown) to display the **System Information** screen. Note that DNS servers are Telstra DNS servers and DNS client must be B1 IP address that is used for SIP trunk with Telstra.



6.2 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

6.2.1 Uniform Resource Identifier (URI) Groups

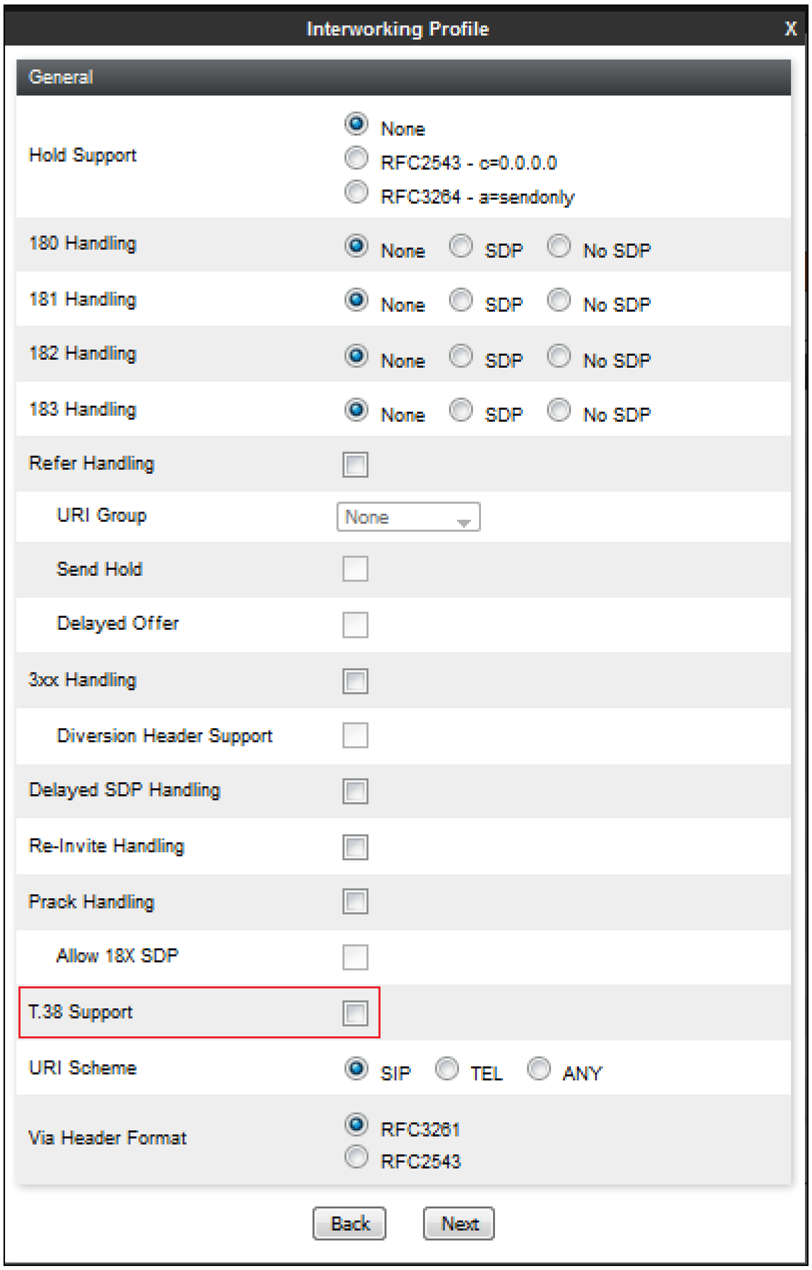
URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a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

For this configuration testing, “*” is used for all incoming and outgoing traffic.

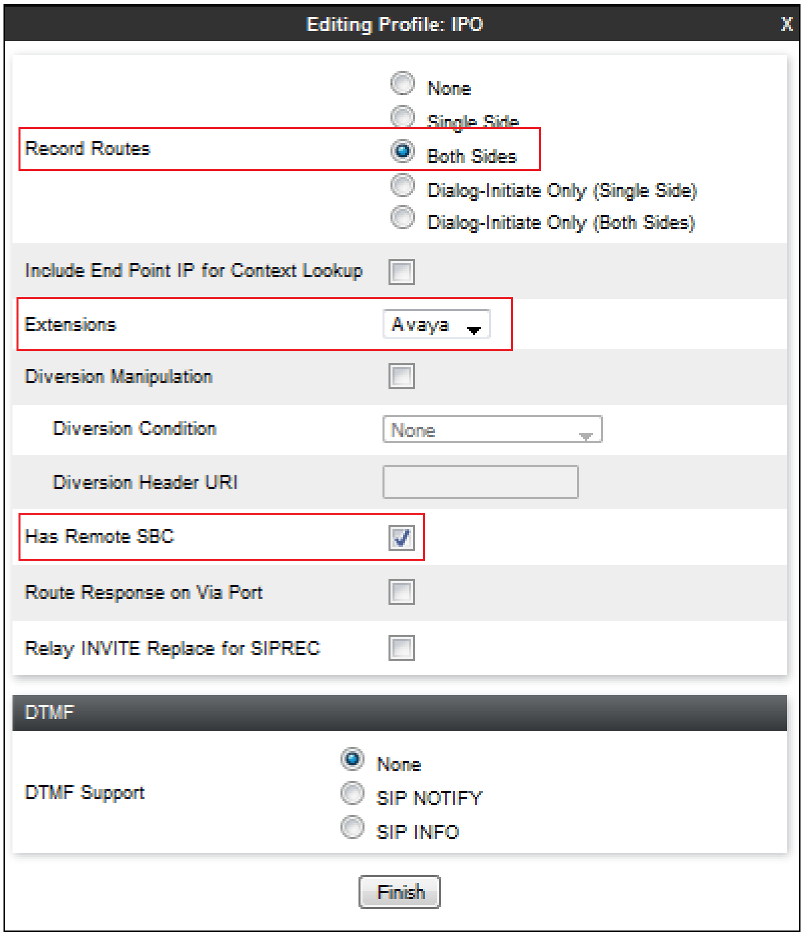
6.2.2 Server Interworking – IPO

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the profile for the connection to Avaya IP Office.

1. Select **Global Profiles** > **Server Interworking** from the left-hand menu.
2. Click **Add** and enter a name, e.g., **IPO** (not shown), then click **Next** (not shown).
3. The General screen will open.
   - Uncheck **T38 Support**.
   - All other options can be left with default values, and click **Next**.



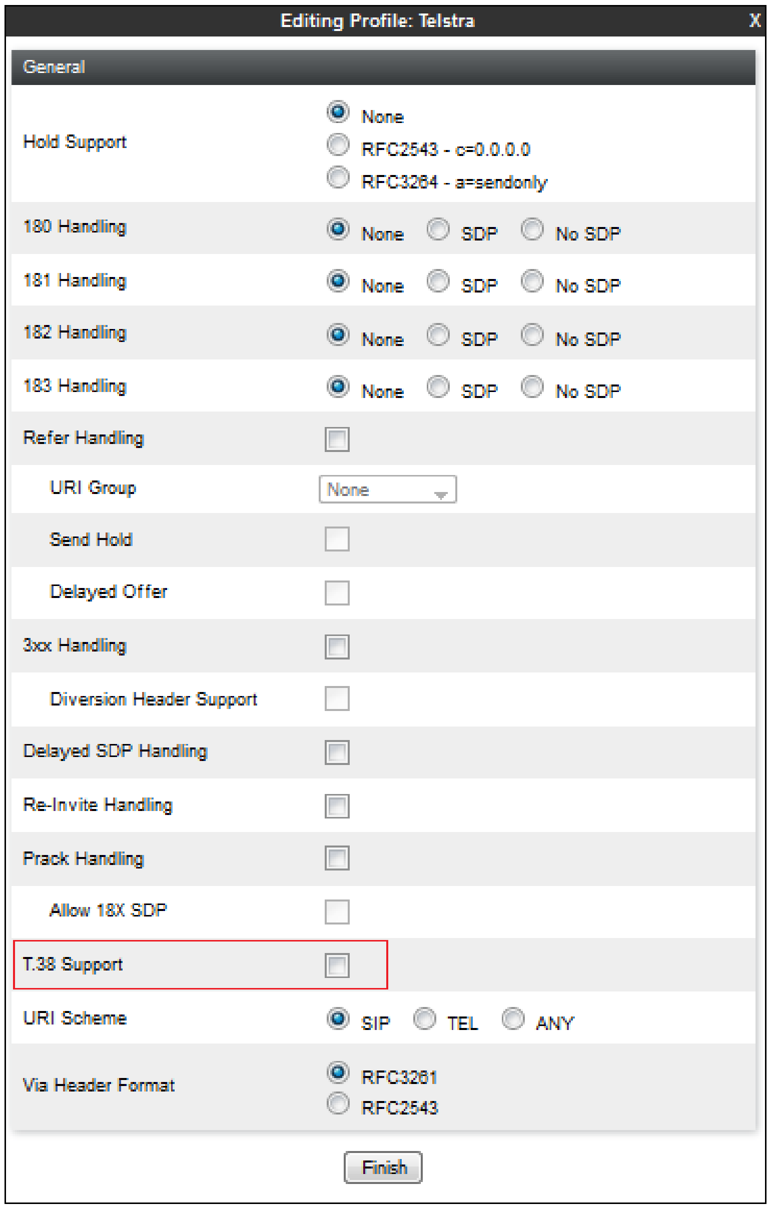
4. On the Timers and Privacy window, accept default values and click **Next** (not shown).
5. On the Advanced window:
   - **Record Routes**: Choose **Both Sides**.
   - **Extensions**: Choose **Avaya**.
   - Check **Has Remote SBC**



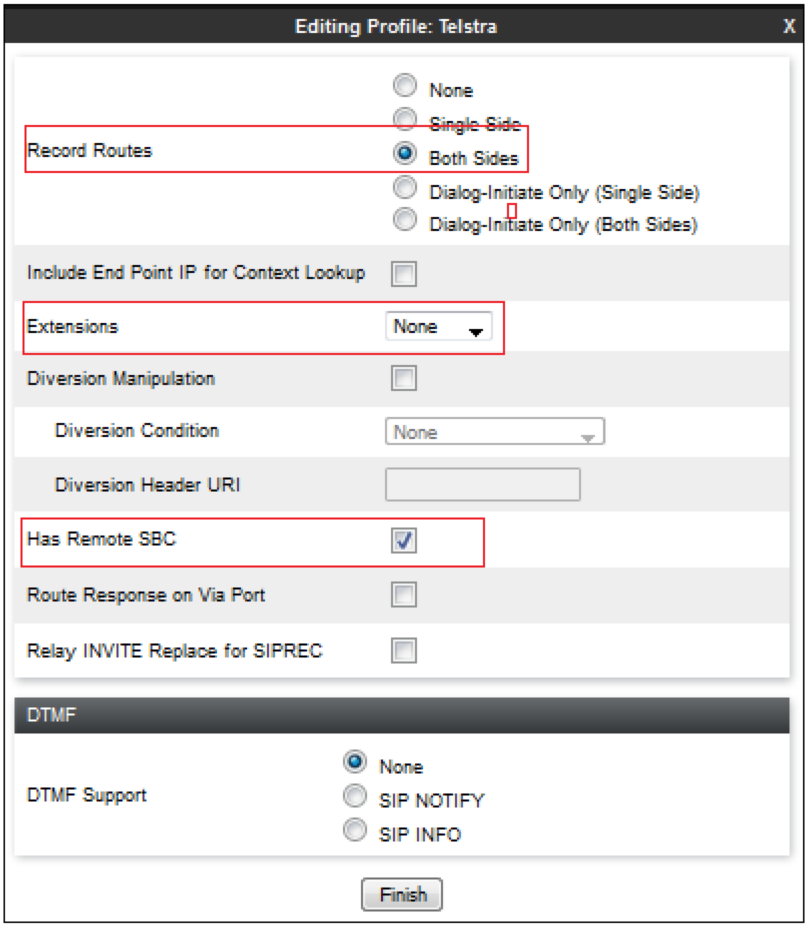
6.2.3 Server Interworking – Telstra

Repeat the steps shown in **Section 6.2.2** to add an Interworking Profile for the connection to Telstra via the public network, with the following changes:

1. Click **Add** to add a new profile, enter **Telstra** then click **Next** (not shown)
2. The **General** screen will open: Configure the same as shown in **Section 6.2.2**.
   - Click **Next** (not shown).
   - The **Privacy/DTMF**, **SIP Timers/Transport Timers** screens will open (not shown), accept default values for all the screens by clicking **Next**.



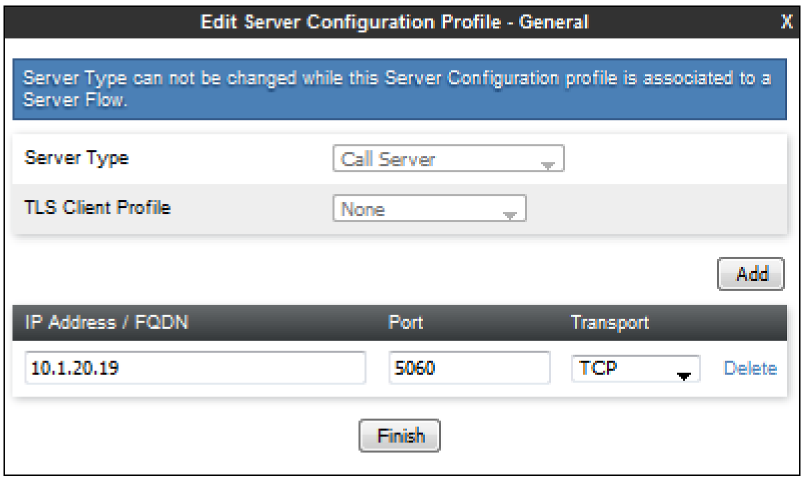
Advanced window is configured as below, click **Finish** to save the profile:



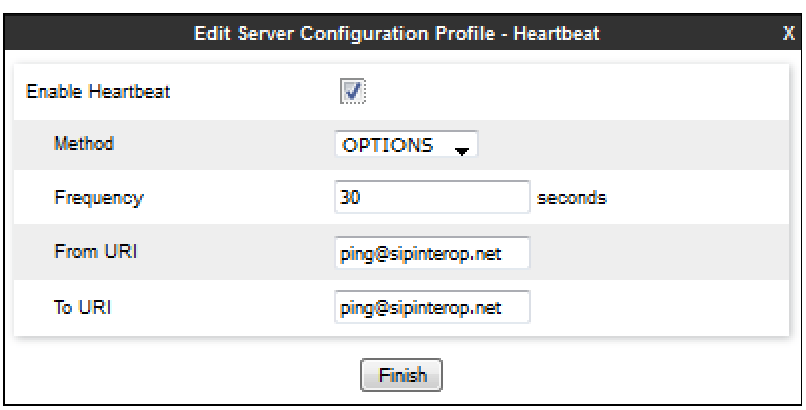
6.2.4 Server Configuration – IPO

This section defines the Server Configuration for the Avaya SBCE connection to IP Office.

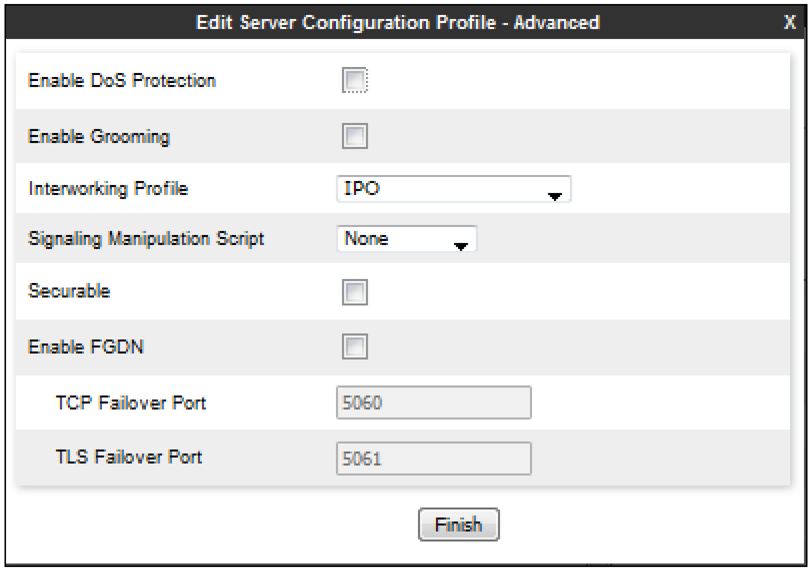
1. Select **Global Profiles > Server Configuration** from the left-hand menu.
2. Select **Add Profile** and the **Profile Name** window will open. Enter a Profile Name (e.g., **IPO**) and click **Next** (not shown).
3. The **Add Server Configuration Profile** window will open.
   - Select **Server Type**: **Call Server**.
   - **IP Address / FQDN**: **10.1.20.19** (IP Office LAN1 IP Address)
   - **Transport**: Select **TCP**.
   - **Port**: **5060**
   - Select **Next** (not shown).



4. The **Authentication** window will open (not shown).
   - Select **Next** to accept default values.
5. The **Heartbeat** window is configured as below and click **Next** (not shown).



6. The **Advanced** window will open.
   - For **Interworking Profile**, select the profile created for IP Office in **Section 6.2.2**.
   - Click **Finish**.



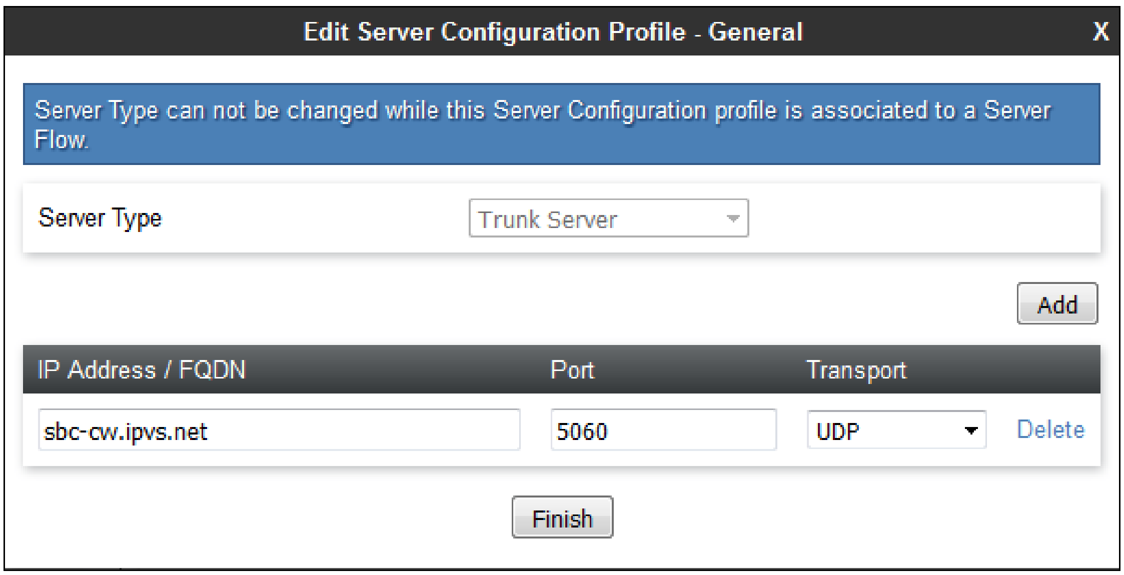
6.2.5 Server Configuration – Telstra

Telstra provided two trunk groups for Enterprise SIP Trunking service. These two trunk groups were connected to two outbound proxies. Telstra Enterprise SIP Trunking service requires authentication so Enterprise Trunk credentials must be provided by Telstra.

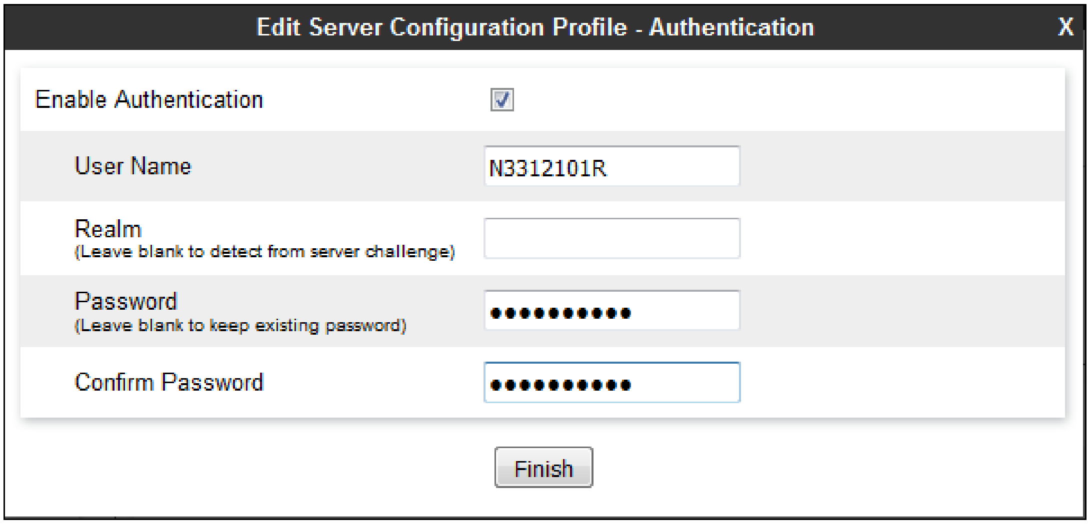
6.2.5.1 Telstra primary

Repeat the steps in **Section 6.2.4**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to Telstra Trunk Group 1.

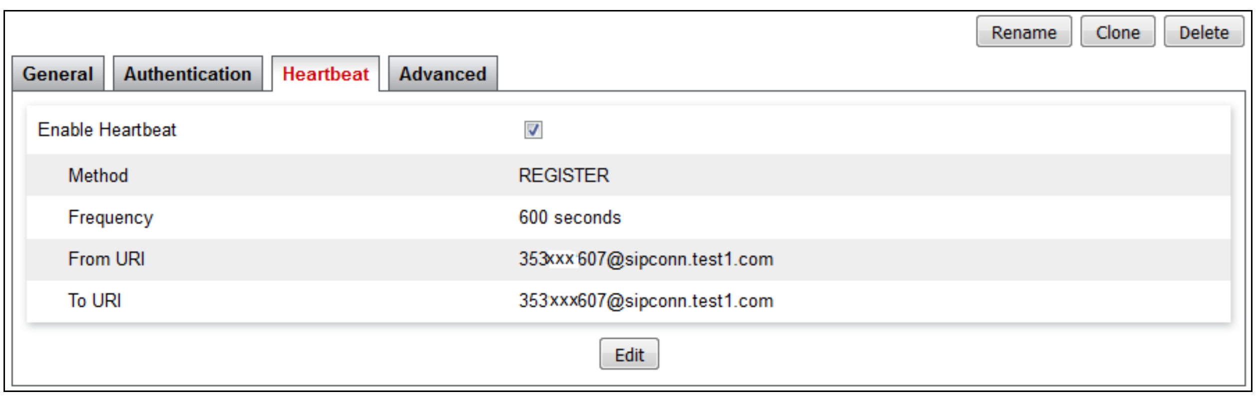
1. Select **Add Profile** and enter a Profile Name (e.g., **Telstra_pri**) and select **Next** (not shown).
2. On the **General** window, enter the following:
   - Select **Server Type**: **Trunk Server**.
   - **IP Address / FQDN: sbc-cw.ipvs.net** (outbound proxy 1 of Telstra)
   - **Transport**: Select **UDP**.
   - **Port: 5060**
   - Select **Next** (not shown).



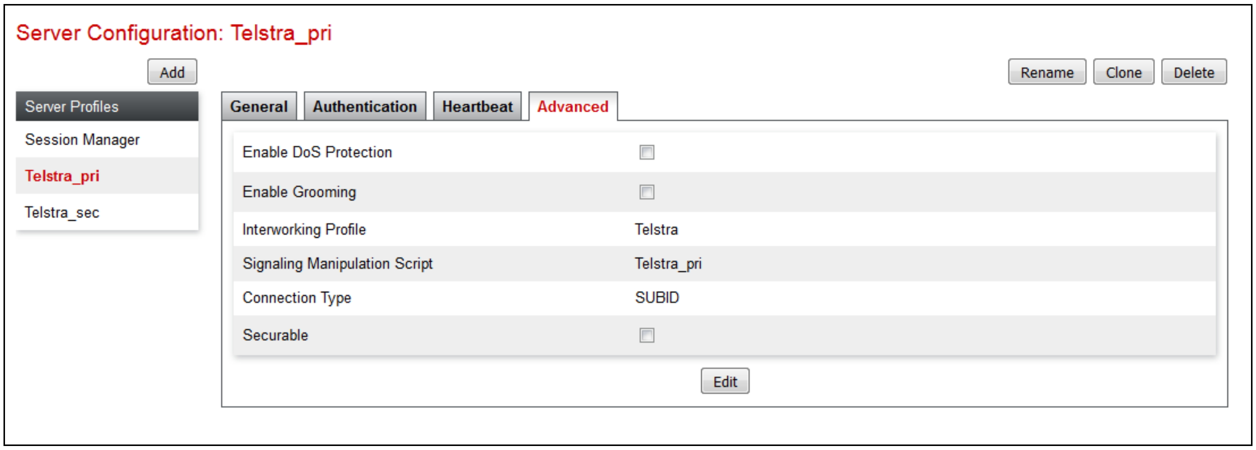
3. Under Authentication window:
   - Select **Enable Authentication**
   - **User Name**: Enter Authentication name for outbound proxy 1.
   - **Realm**: Leave blank.
   - **Password** and **Confirm Password**: Enter Password provided by Telstra.



4. Under Heartbeat window:
   - Select **Enable Heartbeat**.
   - **Method**: Choose **REGISTER**.
   - **Frequency**: Enter **600**.
   - **From URI** and **To URI**: Enter the Pilot number provided by Telstra.



5. Under Advanced window:
    - Select **Telstra** for Interworking Profile.
    - Select **Telstra_pri** for Signaling Manipulation Script (see **Notice 1**).



Notice 1:

Note that Signaling Manipulation Script **Telstra_pri** is required to:

- Add the primary Trunk Pilot number into the PAI Header on outgoing calls.
- If the FROM header is 'anonymous', then re-write the FROM with the primary Trunk Pilot number.

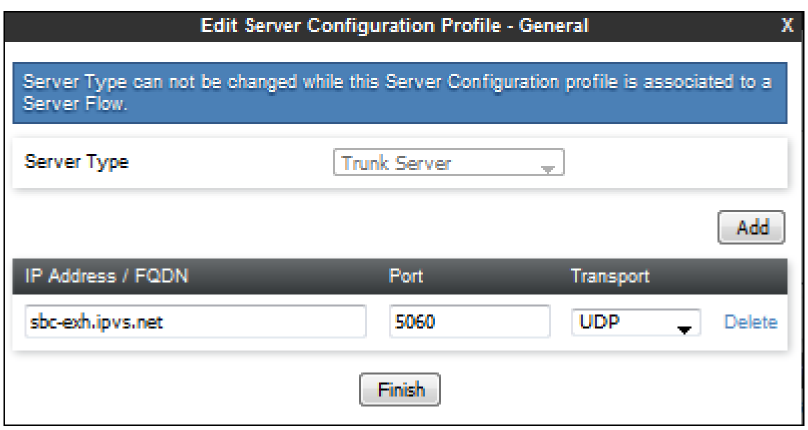
Navigate to **Global Profiles** > **Signaling Manipulation** to add **Telstra_pri** script:

```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%HEADERS["P-Asserted-Identity"][1].URI.USER = "353xxx607";
}
}
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
if(%HEADERS["FROM"][1].URI.USER = "anonymous")then
{
%HEADERS["FROM"][1].URI.USER = "353xxx607";
}
}
}
```

6.2.5.2 Telstra secondary

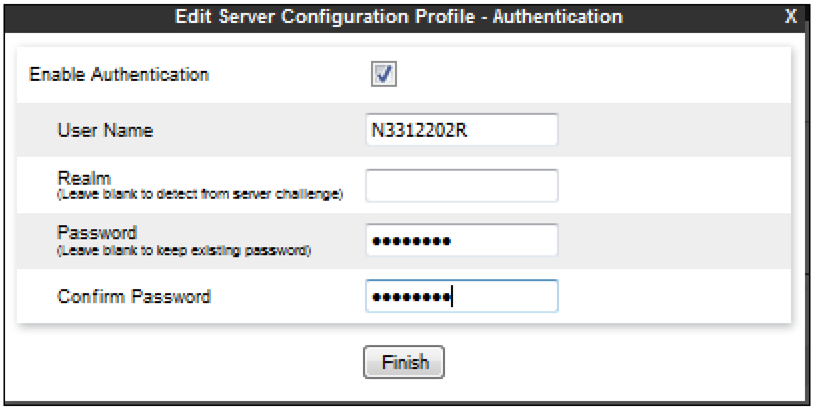
Repeat the steps in **Section 6.2.5.1**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to Telstra Trunk Group 2.

1. Select **Add Profile** and enter a Profile Name (e.g., **Telstra_sec**) and select **Next** (not shown).
2. On the **General** window, enter the following:
   - Select **Server Type**: **Trunk Server**.
   - **IP Address / FQDN: sbc-exh.ipvs.net** (outbound proxy 2 of Telstra)
   - **Transport**: Select **UDP**.
   - **Port: 5060**
   - Select **Next** (not shown).

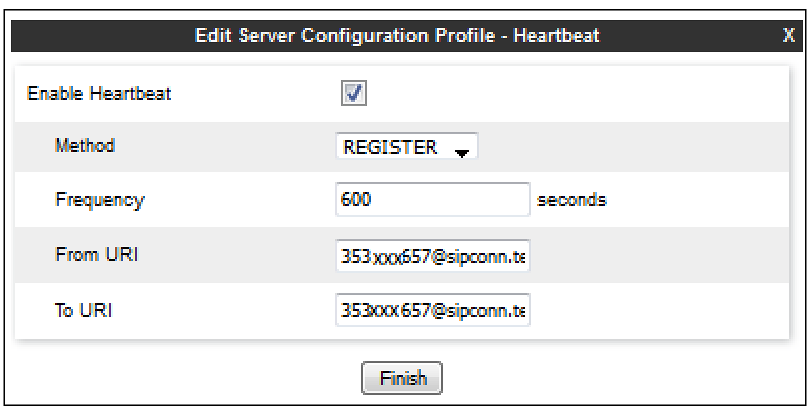


3. Under Authentication window:
   - Select **Enable Authentication**.
   - **User Name**: Enter Authentication name for outbound proxy 2.
   - **Realm**: Leave blank.

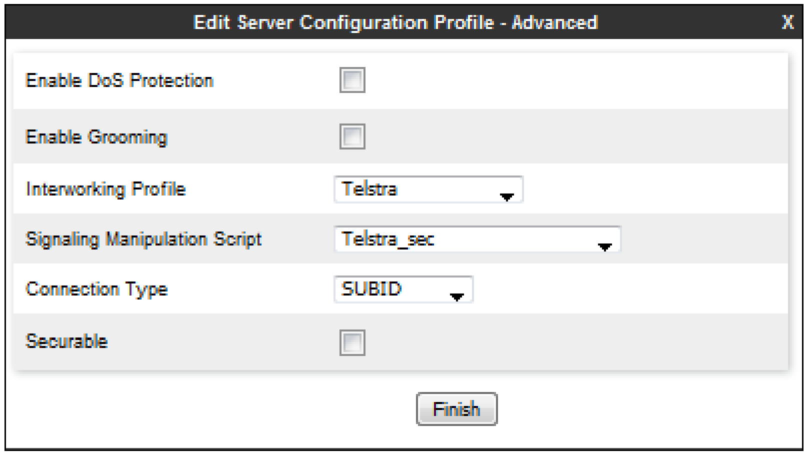
- Password and Confirm Password: enter Password provided by Telstra.



4. Under Heartbeat window:
   - Select **Enable Heartbeat**.
   - **Method**: Choose **REGISTER**.
   - **Frequency**: Enter **600**.
   - **From URI** and **To URI**: Enter the Pilot number provided by Telstra.



5. Under Advanced window:
    - Select **Telstra** for **Interworking Profile**.
    - Select **Telstra_sec** for **Signaling Manipulation Script** (see **Notice 2**).



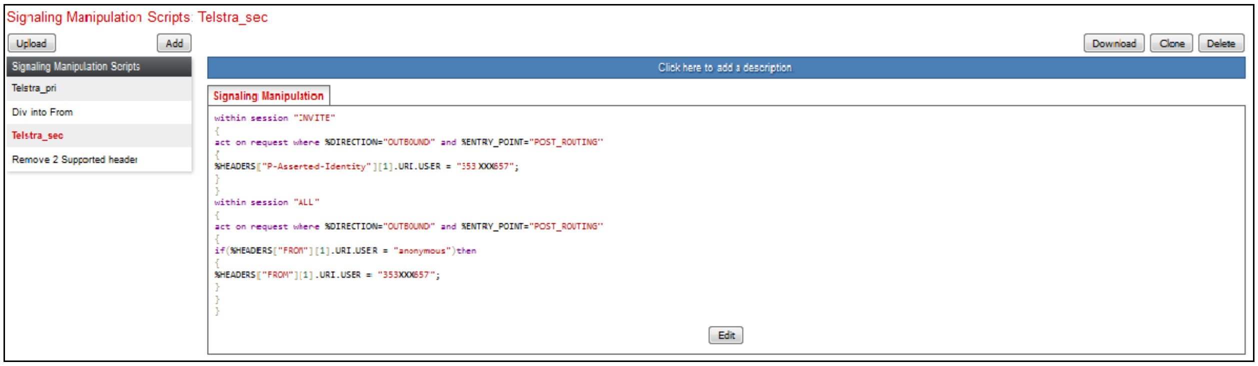
__**Notice 2:**__

Note that Signaling Manipulation Script **Telstra_sec** is required to:

- Add the second Trunk Pilot number into the PAI Header on outgoing calls.
- If the FROM header is ‘anonymous’, then re-write the FROM with the second Trunk Pilot number.

Repeat steps in **Notice 1** in **Section 6.2.5.1** to add **Telstra_sec** script:

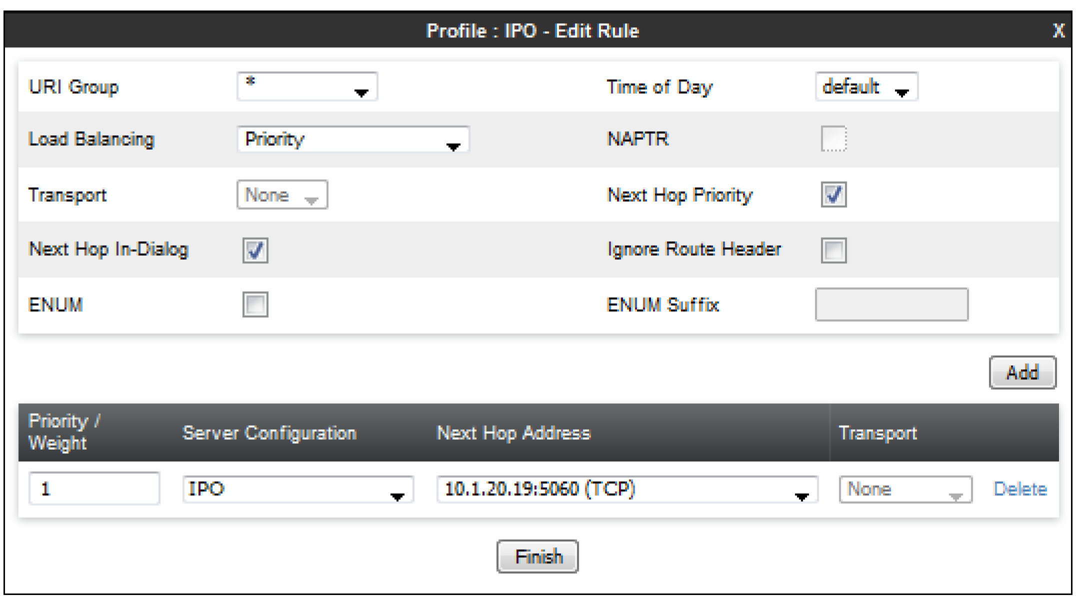
```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%HEADERS["P-Asserted-Identity"][1].URI.USER = "353xxx657";
}
}
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
if(%HEADERS["FROM"][1].URI.USER = "anonymous")then
{
%HEADERS["FROM"][1].URI.USER = "353xxx657";
}
}
}
```



6.2.6 Routing – To IP Office

This provisioning defines the Routing Profile for the connection to IP Office.

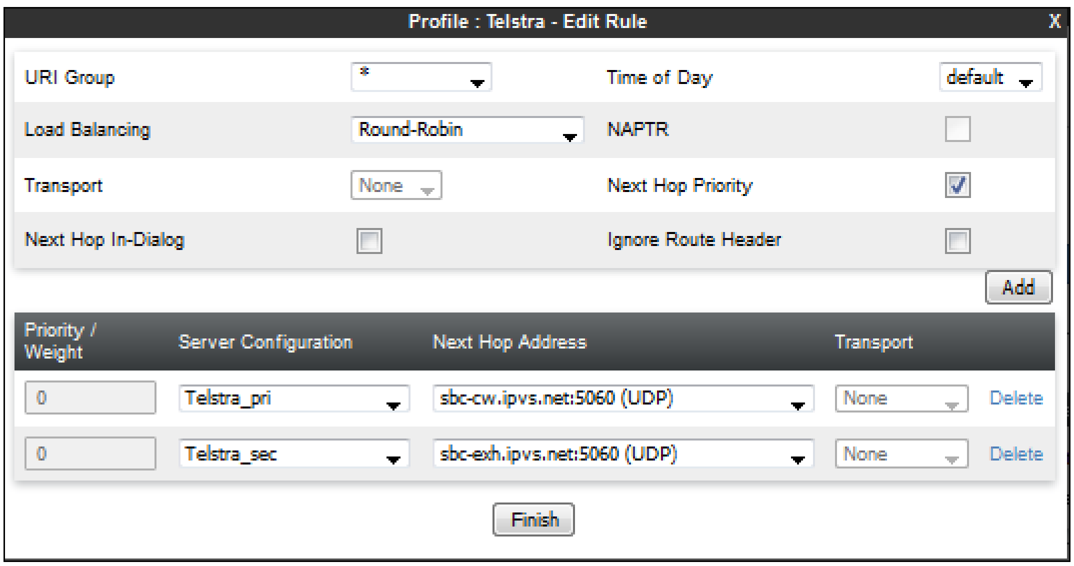
1. Select **Global Profiles → Routing** from the left-hand menu, and select **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **IPO**) and click **Next** (not shown).
3. The Routing Profile window will open. Check **Next Hop In-Dialog** box then click on **Add**.
4. The Next-Hop Address entry will be shown. Populate the following fields:
   - **Priority/Weight** = **1**
   - **Server Configuration** = **IPO**
   - **Next Hop Address:** Verify that the **10.1.20.19:5060 (TCP)** entry from the drop down menu is selected (IP Office LAN1 IP address). Also note that the **Transport** field is grayed out.
   - Click on **Finish**.



6.2.7 Routing – To Telstra

Repeat the steps in **Section 6.2.6**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Telstra.

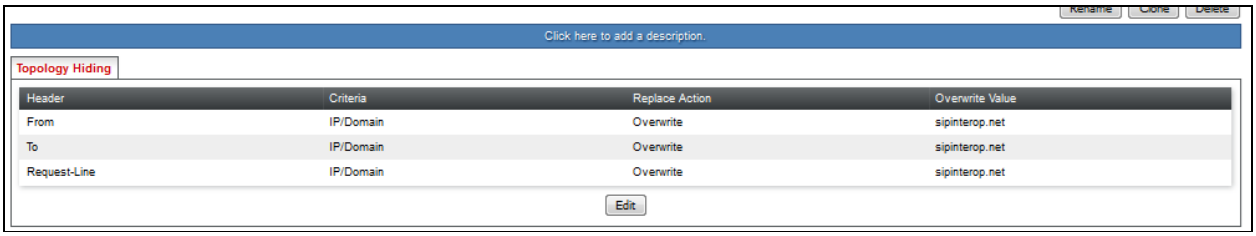
1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **Telstra**).
2. Load Balancing: select **Round-Robin**.
3. Uncheck **Next Hop In-Dialog** box.
4. On the **Next-Hop Address** entry, populate the following fields:
   - **Server Configuration: Telstra_pri**.
   - **Next Hop Address:** Verify that the **sbc-cw.ipvs.net:5060** entry from the drop down menu is selected.
   - Add another record for **Telstra_sec**
   - Use default values for the rest of the parameters.
5. Click **Finish**.



6.2.8 Topology Hiding – IP Office

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

1. Select **Global Profiles → Topology Hiding** from the left-hand side menu.
2. Select the **Add** button, enter **Profile Name** (e.g., **IPO**), and click **Next** (not shown).
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly until **To** header is added (not shown).
4. Populate the fields as shown below, and click **Finish**. Note that **sipinterop.net** is the domain used.

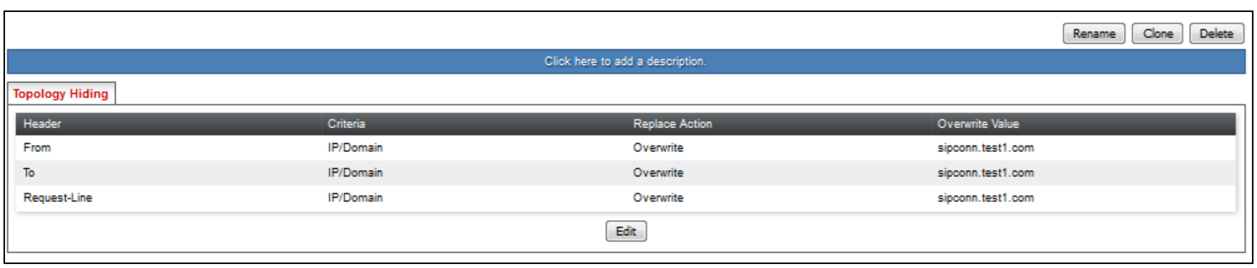


Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	sipinterop.net
To	IP/Domain	Overwrite	sipinterop.net
Request-Line	IP/Domain	Overwrite	sipinterop.net

6.2.9 Topology Hiding – Telstra

Repeat the steps in **Section 6.2.8**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Telstra.

1. Enter a **Profile Name**: (e.g., **Telstra**).
2. Click on the **Add Header** button repeatedly until **To** header is added (not shown).
3. Populate the fields as shown below, and click **Finish**. Note that **sipconn.test1.com** is the domain used.



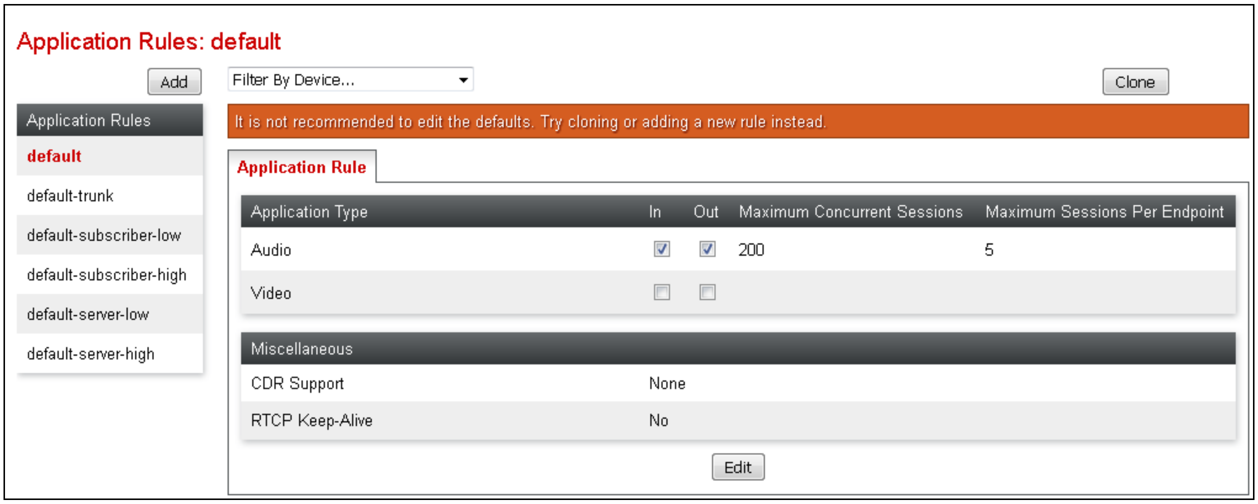
Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	sipconn.test1.com
To	IP/Domain	Overwrite	sipconn.test1.com
Request-Line	IP/Domain	Overwrite	sipconn.test1.com

6.3 Domain Policies

The Domain Policies feature allows users 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.

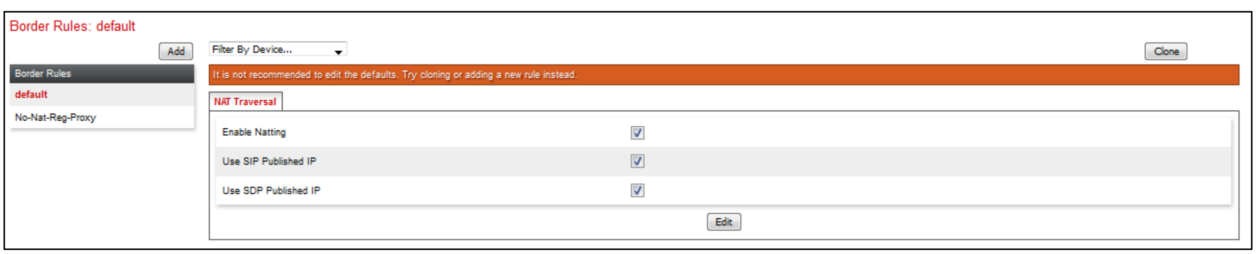
6.3.1 Application Rules

Ensure that the Application Rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the Avaya SBCE was licensed for 200 Voice sessions, and the default rule was amended accordingly. Other Application Rules could be utilized on an as needed basis.
Note: It is not recommended to edit default rules, new rules should be added or cloned from default rules.



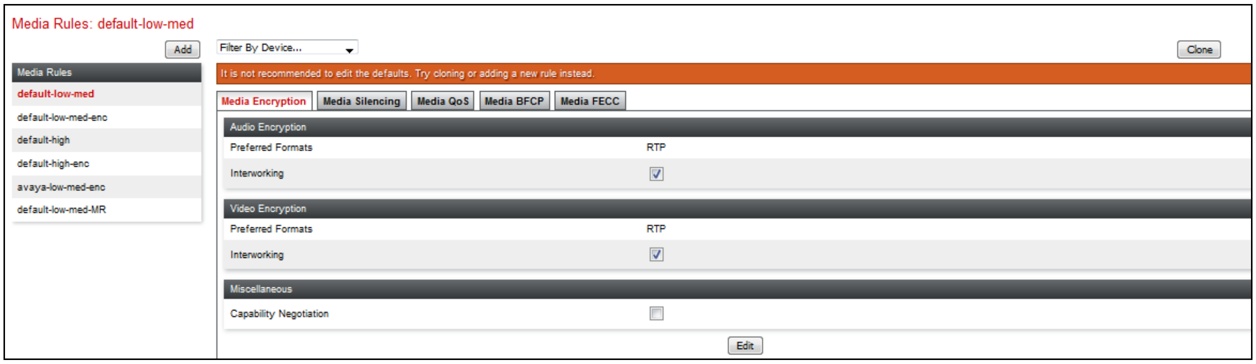
6.3.2 Border Rules

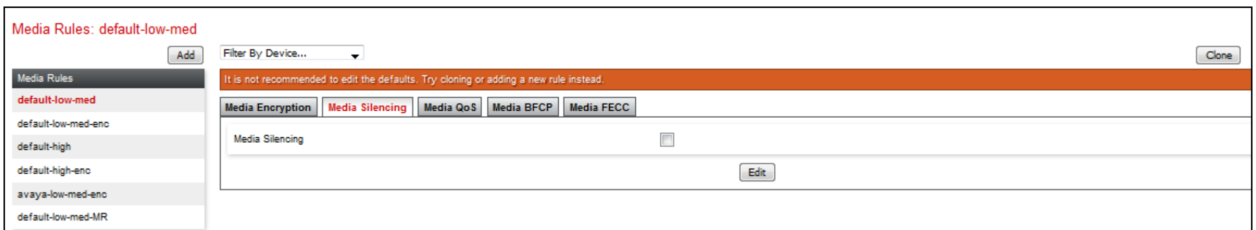
The Border Rule specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses.

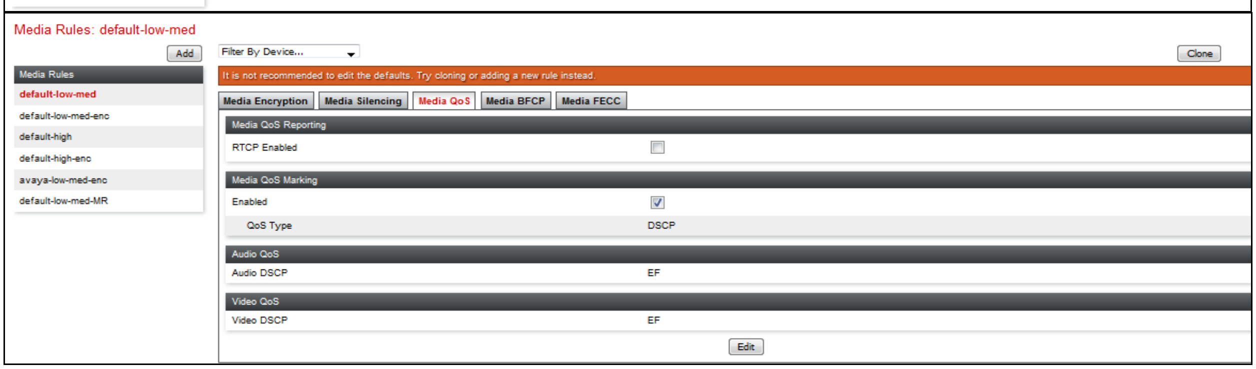


6.3.3 Media Rules

This Media Rule will be applied to both directions and therefore, only one rule is needed.
In the solution as tested, the **default-low-med** rule was utilized. No customization was required.

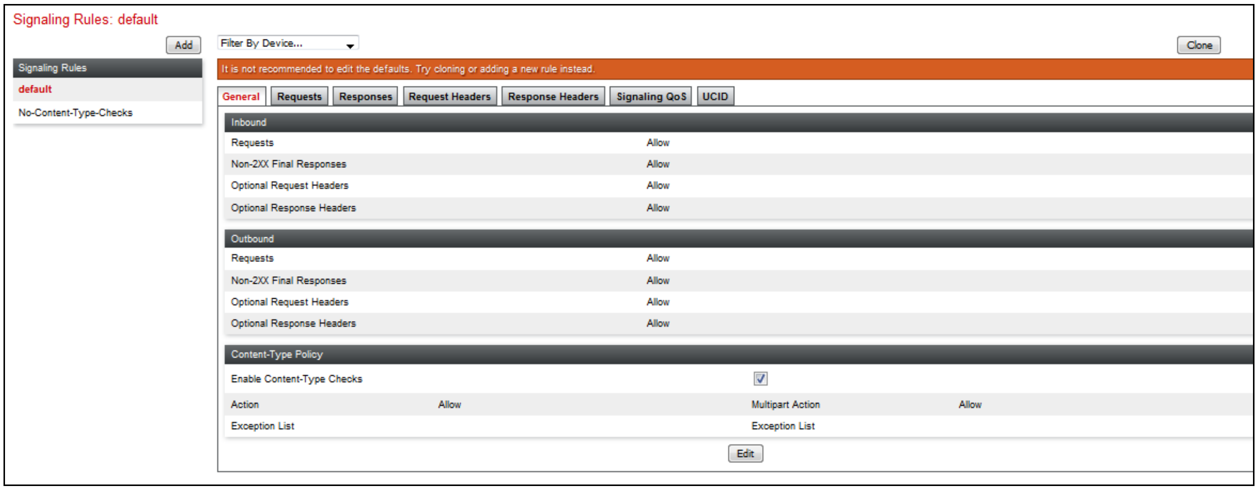






6.3.4 Signaling Rules

The default Signaling Rule was utilized. No customization was required.



6.3.5 Endpoint Policy Groups

In the solution as tested, the **default-low** rule was utilized. This rule incorporated the Media and Signaling Rules specified above, as well as other policies.

6.4 Device Specific Settings

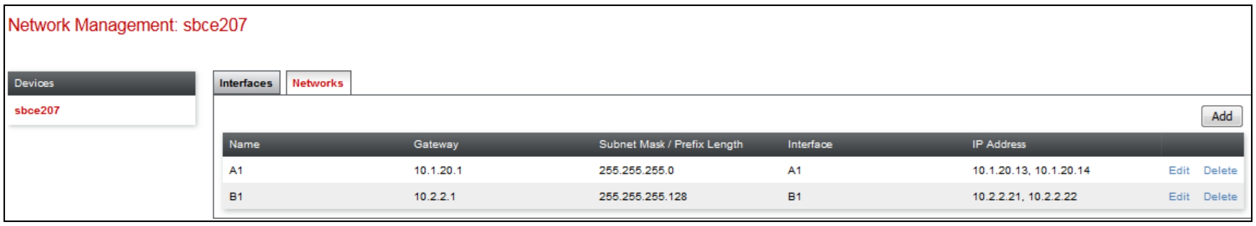
The **Device Specific Settings** feature for SIP provides aggregate system information, and manages various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, various device-specific protection features such as Message Sequence Analysis (MSA) functionality and end-point and session call flows can be defined and administered.

6.4.1 Network Management

1. Select **Device Specific Settings → Network Management** from the menu on the left-hand side (not shown).
2. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.

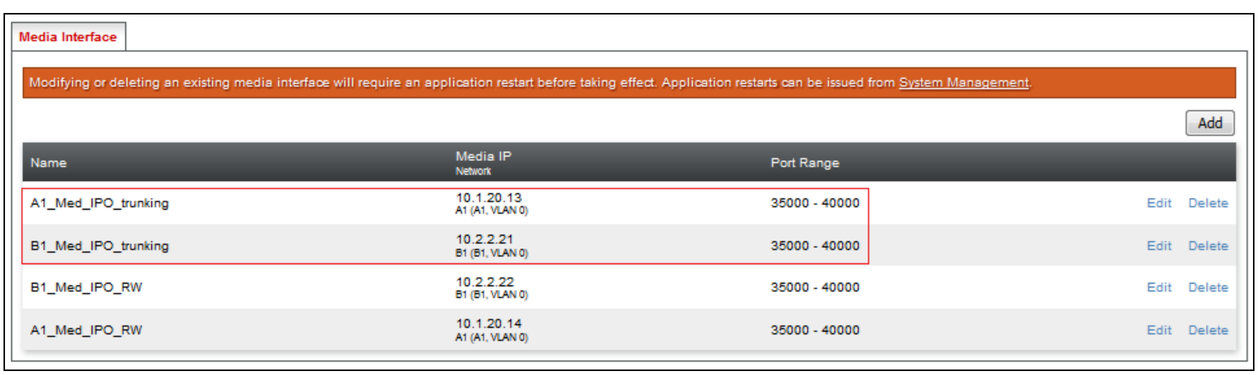
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

Note: B1 has two IP Addresses configured for each interface. One is used for SIP trunking, another one is used for Remote worker. Configuration for Remote worker is out of scope of this document.



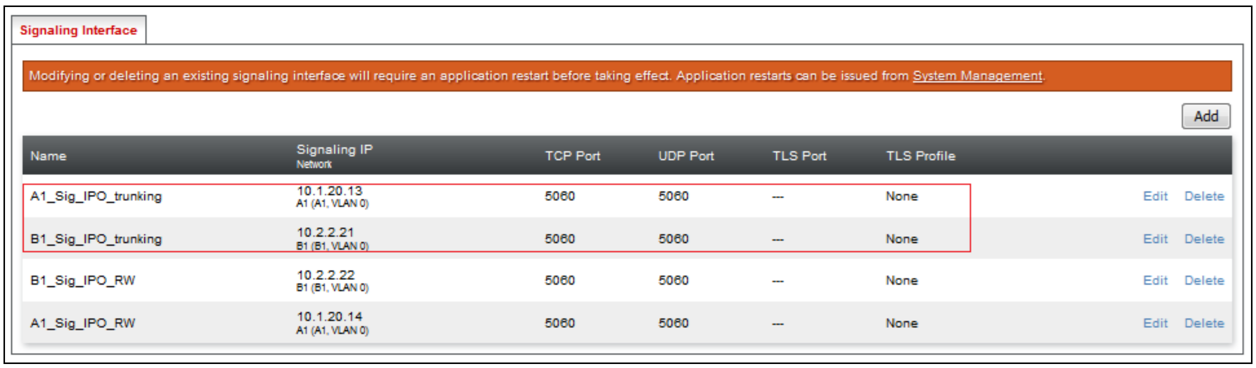
6.4.2 Media Interfaces

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
   - **Name**: **A1_Med_IPO_trunking**
   - **IP Address**: **10.1.20.13** (Avaya SBCE A1 address)
   - **Port Range**: **35000-40000**
4. Click **Finish** (not shown).
5. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
   - **Name**: **B1_Med_IPO_trunking**
   - **IP Address**: **10.2.2.21** (Avaya SBCE B1 address)
   - **Port Range**: **35000-40000**
6. Click **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.



6.4.3 Signaling Interface

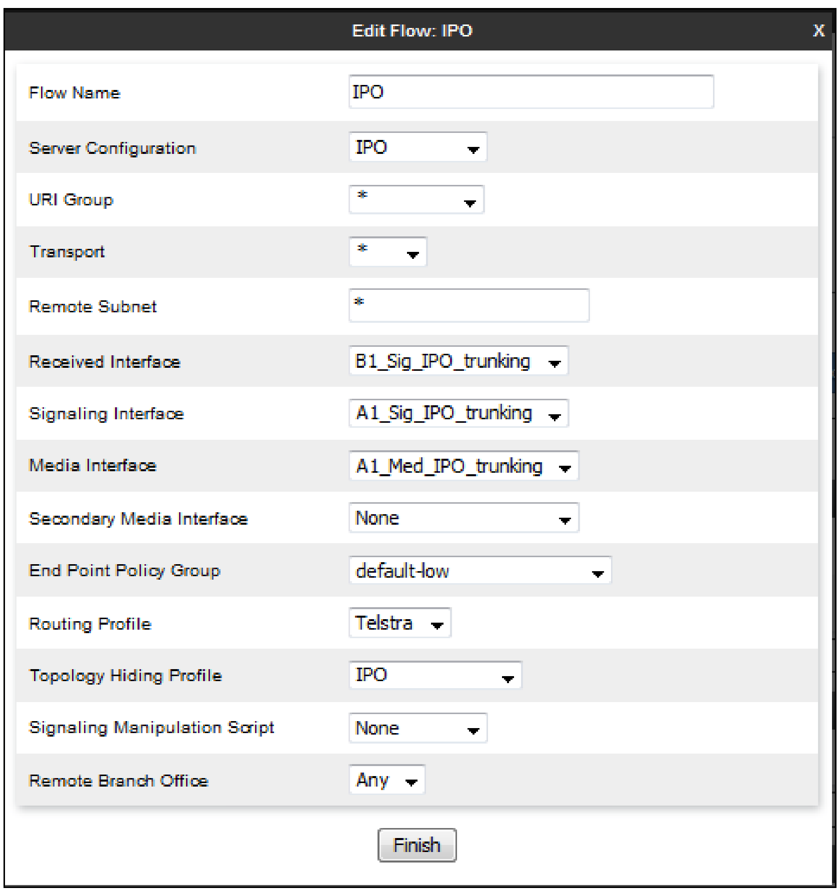
1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:
   - **Name**: **A1_Sig_IPO_trunking**
   - **IP Address**: **10.1.20.13** (Avaya SBCE A1 address)
   - **TCP Port**: **5060**
   - **UDP Port**: **5060**
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
   - **Name**: **B1_Sig_IPO_trunking**
   - **IP Address**: **10.2.2.21** (Avaya SBCE B1 address)
   - **TCP Port**: **5060**
   - **UDP Port**: **5060**
6. Click **Finish** (not shown). Note that changes to these values require an application restart.



Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
A1_Sig_IPO_trunking	10.1.20.13 A1 (A1, VLAN 0)	5060	5060	---	None	Edit	Delete
B1_Sig_IPO_trunking	10.2.2.21 B1 (B1, VLAN 0)	5060	5060	---	None	Edit	Delete
B1_Sig_IPO_RW	10.2.2.22 B1 (B1, VLAN 0)	5060	5060	---	None	Edit	Delete
A1_Sig_IPO_RW	10.1.20.14 A1 (A1, VLAN 0)	5060	5060	---	None	Edit	Delete

6.4.4 Endpoint Flows – For Session Manager

1. Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
   - **Name**: **IPO**
   - **Server Configuration**: **IPO**
   - **URI Group**: *****
   - **Transport**: *****
   - **Remote Subnet**: *****
   - **Received Interface**: **B1_Sig_IPO_trunking**
   - **Signaling Interface**: **A1_Sig_IPO_trunking**
   - **Media Interface**: **A1_Med_IPO_trunking**
   - **End Point Policy Group**: **default-low**
   - **Routing Profile**: **Telstra**
   - **Topology Hiding Profile**: **IPO**
   - Let other values default.
4. Click **Finish**.

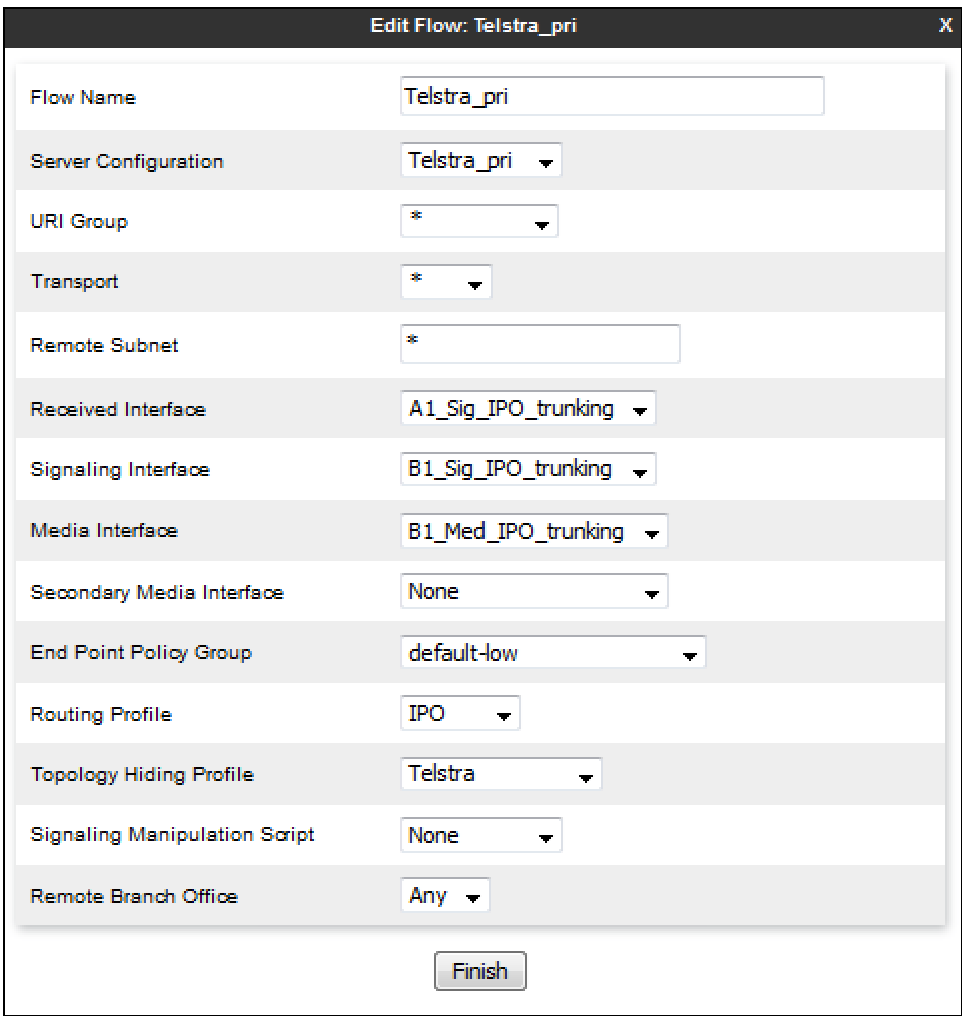


6.4.5 Endpoint Flows – For Telstra

6.4.5.1 Telstra primary

Repeat step **1** through **4** from **Section 6.3.4**, with the following changes:

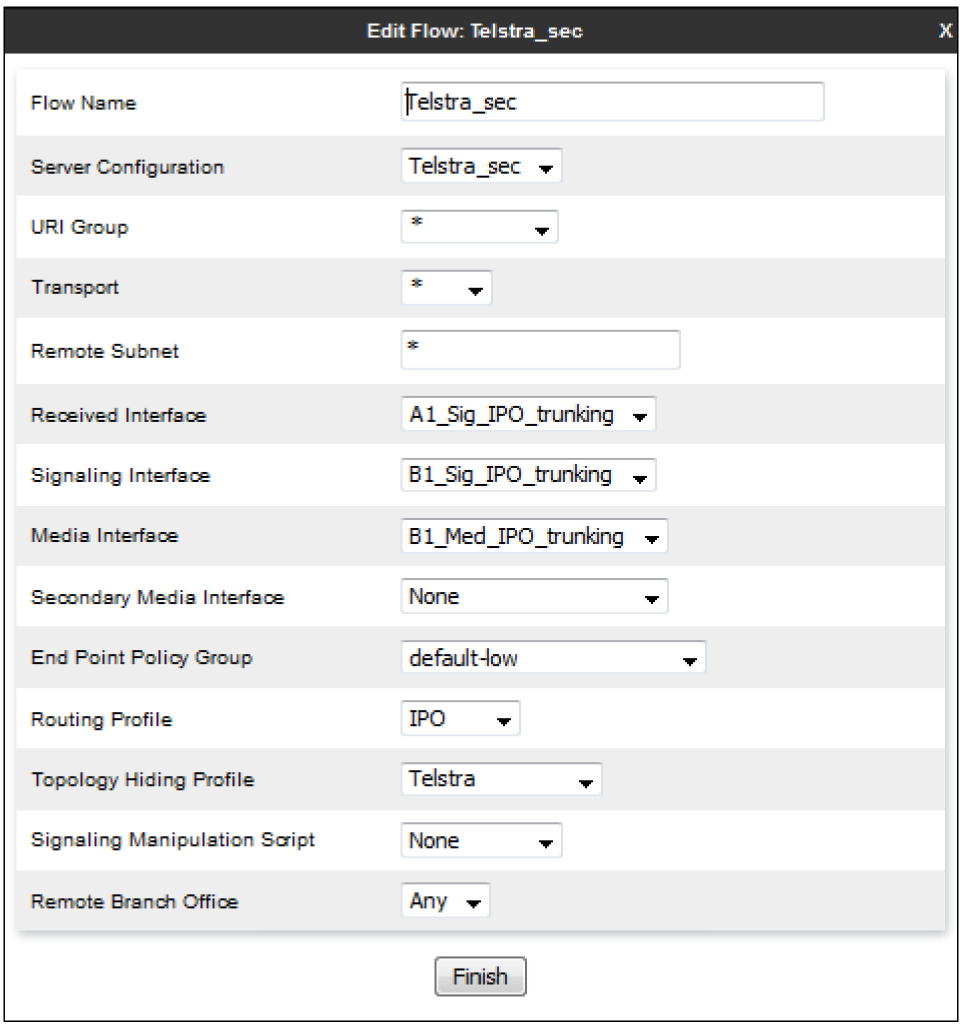
- **Name**: **Telstra_pri**
- **Server Configuration**: **Telstra_pri**
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **A1_Sig_IPO_trunking**
- **Signaling Interface**: **B1_Sig_IPO_trunking**
- **Media Interface**: **B1_Med_IPO_trunking**
- **End Point Policy Group**: **default_low**
- **Routing Profile**: **IPO**
- **Topology Hiding Profile**: **Telstra**



6.4.5.2 Telstra secondary

Repeat step **1** through **4** from **Section 6.3.4**, with the following changes:

- **Name**: **Telstra_sec**
- **Server Configuration**: **Telstra_sec**
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **A1_Sig_IPO_trunking**
- **Signaling Interface**: **B1_Sig_IPO_trunking**
- **Media Interface**: **B1_Med_IPO_trunking**
- **End Point Policy Group**: **default_low**
- **Routing Profile**: **IPO**
- **Topology Hiding Profile**: **Telstra**



7. Verification Steps

The following steps may be used to verify the configuration.

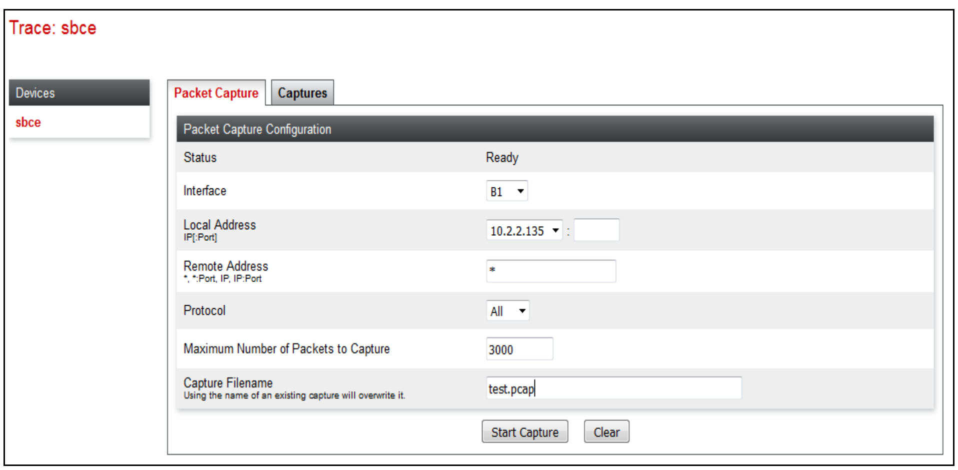
7.1 Avaya Session Border Controller for Enterprise

Log into the Avaya SBCE as shown in **Section 6**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.

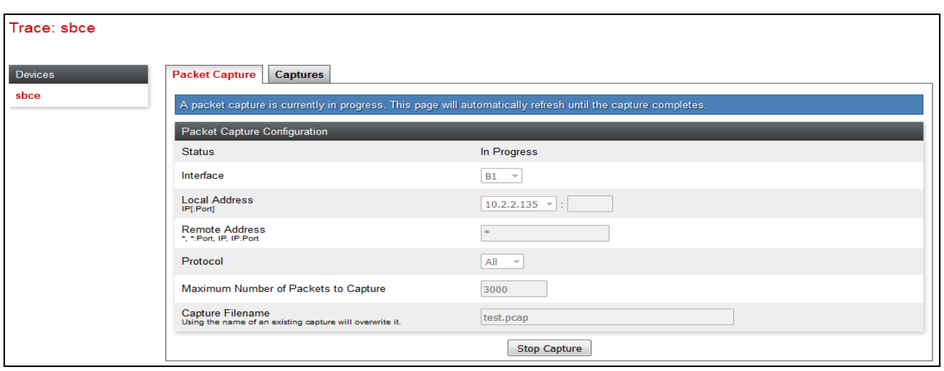
Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

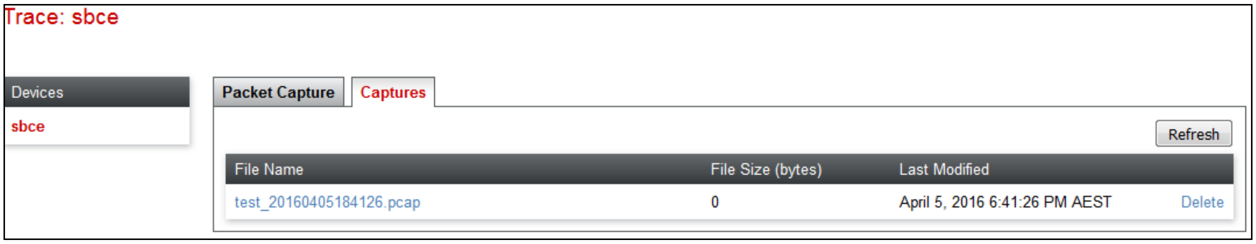
1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
   - Select the desired **Interface** from the drop down menu (e.g., **All**).
   - Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
   - Specify a **Capture Filename** (e.g., **TEST.pcap**).
   - Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
   - Click **Start Capture** to begin the trace.



The capture process will initialize and then display the following **In Progress** status window:

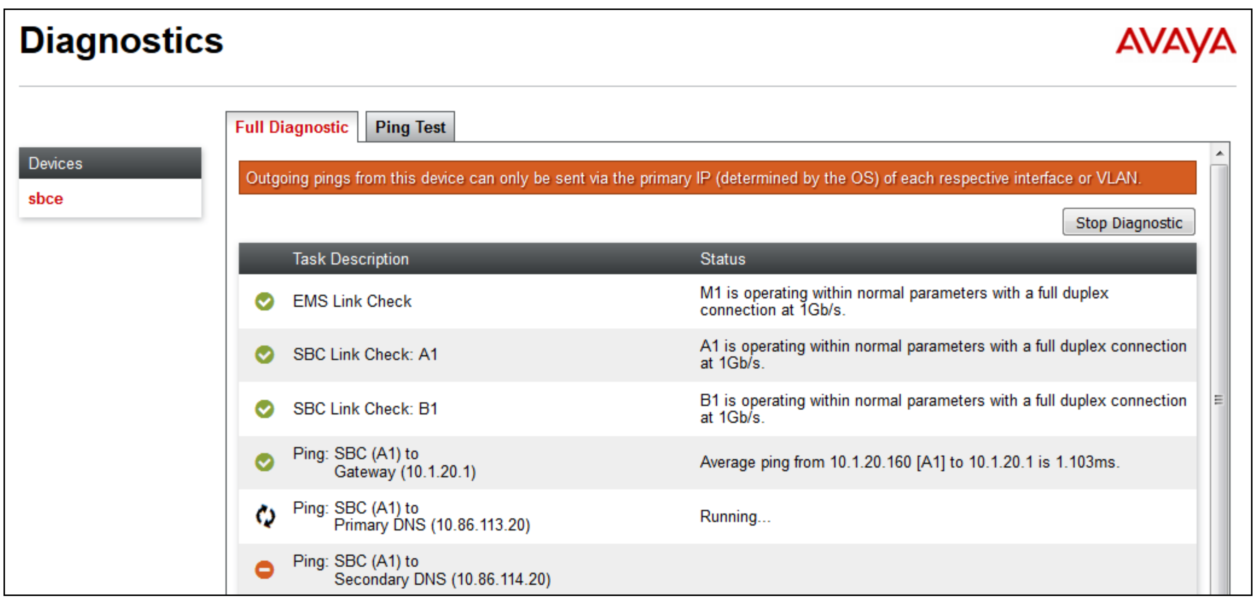


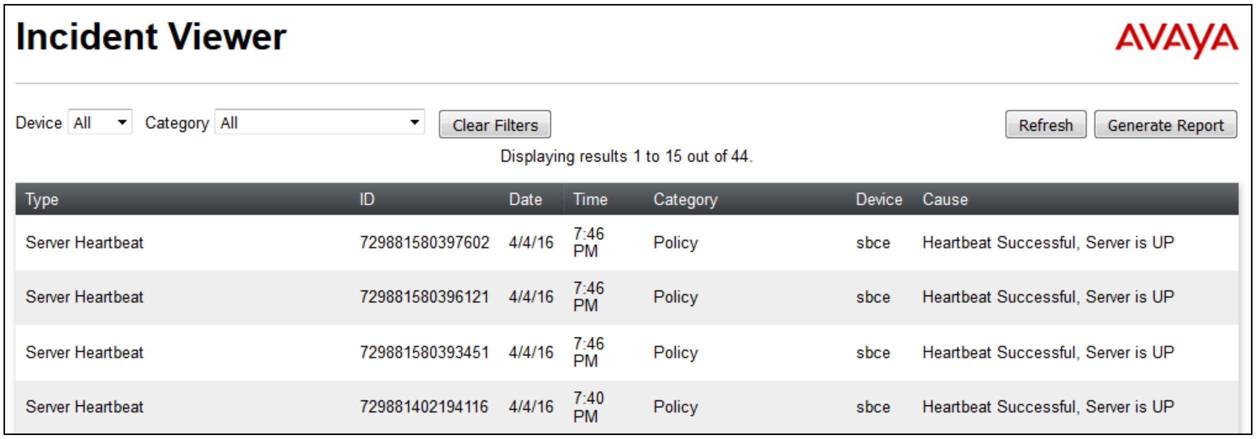
3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file and use Wireshark to open the trace.



The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the Telstra Enterprise SIP Trunk Service and the customer SIP PABX is the customer SBC.
On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

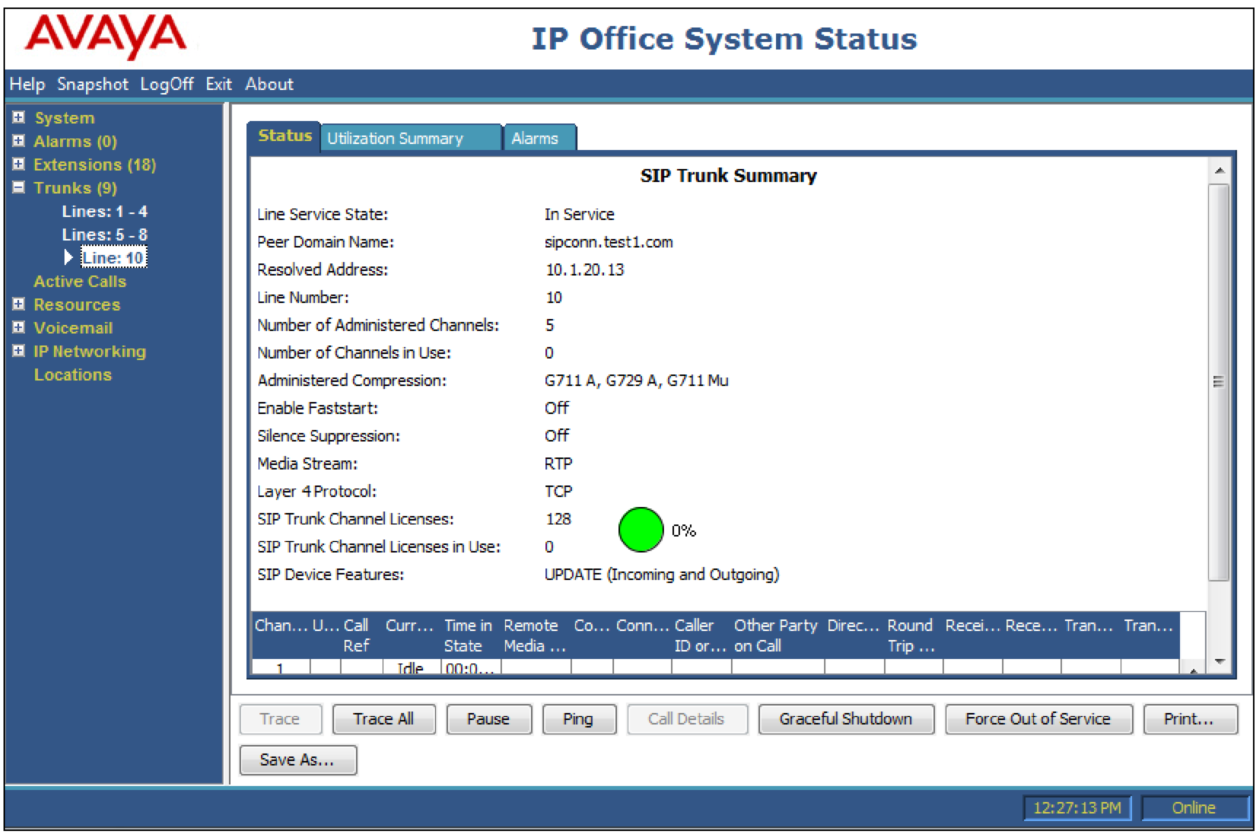
- Ping from the SBC to the Telstra network gateway.
- Ping from the SBC to the Session Manager.
- Ping from the Telstra network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.





7.2 Avaya IP Office

On the PC that has IP Office Manager installed, navigate to **Start** > **All Programs** > **IP Office** > **System Status**. A login window appears, login with proper credentials. Click on **Trunks** > **Line: 10** (the SIP line configured on IP Office for SIP trunking):



7.3 Telephony Services

1. Place inbound/outbound calls, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.

2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

8. Conclusion

As illustrated in these Application Notes, Avaya IP Office Release 10 and Avaya Session Border Control for Enterprise Release 7.1 can be configured to interoperate successfully with Telstra Enterprise SIP Trunking service. This solution allows enterprise users access to the PSTN using the Telstra Enterprise SIP Trunking service connection. Please refer to **Section 2.2** for exceptions.

9. Additional References

This section references the documentation relevant to these Application Notes. Avaya product documentation is available at http://support.avaya.com.

[1] *Avaya Session Border Controller for Enterprise Product Overview and Specification*, Release 7.1, 27 Jun 2016.
[2] *Deploying Avaya Session Border Controller*, Release 7.1, 27 Jun 2016.
[3] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.1, 27 Jun 2016.
[4] *Administering Avaya Session Border Controller*, Release 7.1, 27 Jun 2016.
[5] *Deploying IP Office Server Edition Solution*, Release 10, 29 August 2016.
[6] *Deploying IP Office IP500 V2*, Release 10, 03 August 2016.
[7] *Administering Avaya IP Office with Manager*, Release 10, 29 August 2016.
[8] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[9] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, http://www.ietf.org/
[10] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

Product documentation for Telstra Enterprise SIP Trunking Solution is available from Telstra.

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.