



## **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.....	4
2.	General Test Approach and Test Results.....	4
2.1	Interoperability Compliance Testing.....	4
2.2	Test Results .....	5
2.3	Support .....	5
3.	Reference Configuration .....	5
4.	Equipment and Software Validated .....	8
5.	Configure Avaya IP Office .....	9
5.1	LAN1 Settings.....	9
5.2	System Telephony Settings .....	11
5.3	System Codec Settings .....	12
5.4	Administer SIP Line.....	13
5.5	Short Codes .....	17
5.6	ARS table .....	18
5.7	User .....	18
5.8	Incoming Call Route .....	19
5.9	Save Configuration.....	20
6.	Configure Avaya Session Border Controller for Enterprise .....	21
6.1	System Management – Status .....	22
6.2	Global Profiles.....	23
6.2.1	Uniform Resource Identifier (URI) Groups.....	23
6.2.2	Server Interworking – IPO.....	24
6.2.3	Server Interworking – Telstra .....	26
6.2.4	Server Configuration – IPO .....	28
6.2.5	Server Configuration – Telstra.....	30
6.2.6	Routing – To IP Office .....	36
6.2.7	Routing – To Telstra .....	37
6.2.8	Topology Hiding – IP Office .....	38
6.2.9	Topology Hiding – Telstra.....	38
6.3	Domain Policies .....	38
6.3.1	Application Rules.....	39
6.3.2	Border Rules .....	39
6.3.3	Media Rules .....	40
6.3.4	Signaling Rules .....	41
6.3.5	Endpoint Policy Groups.....	41
6.4	Device Specific Settings.....	41
6.4.1	Network Management.....	41
6.4.2	Media Interfaces.....	42
6.4.3	Signaling Interface .....	43
6.4.4	Endpoint Flows – For Session Manager .....	44

6.4.5	Endpoint Flows – For Telstra .....	45
7.	Verification Steps.....	47
7.1	Avaya Session Border Controller for Enterprise.....	47
7.2	Avaya IP Office.....	49
7.3	Telephony Services .....	49
8.	Conclusion .....	50
9.	Additional References.....	50

# 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.

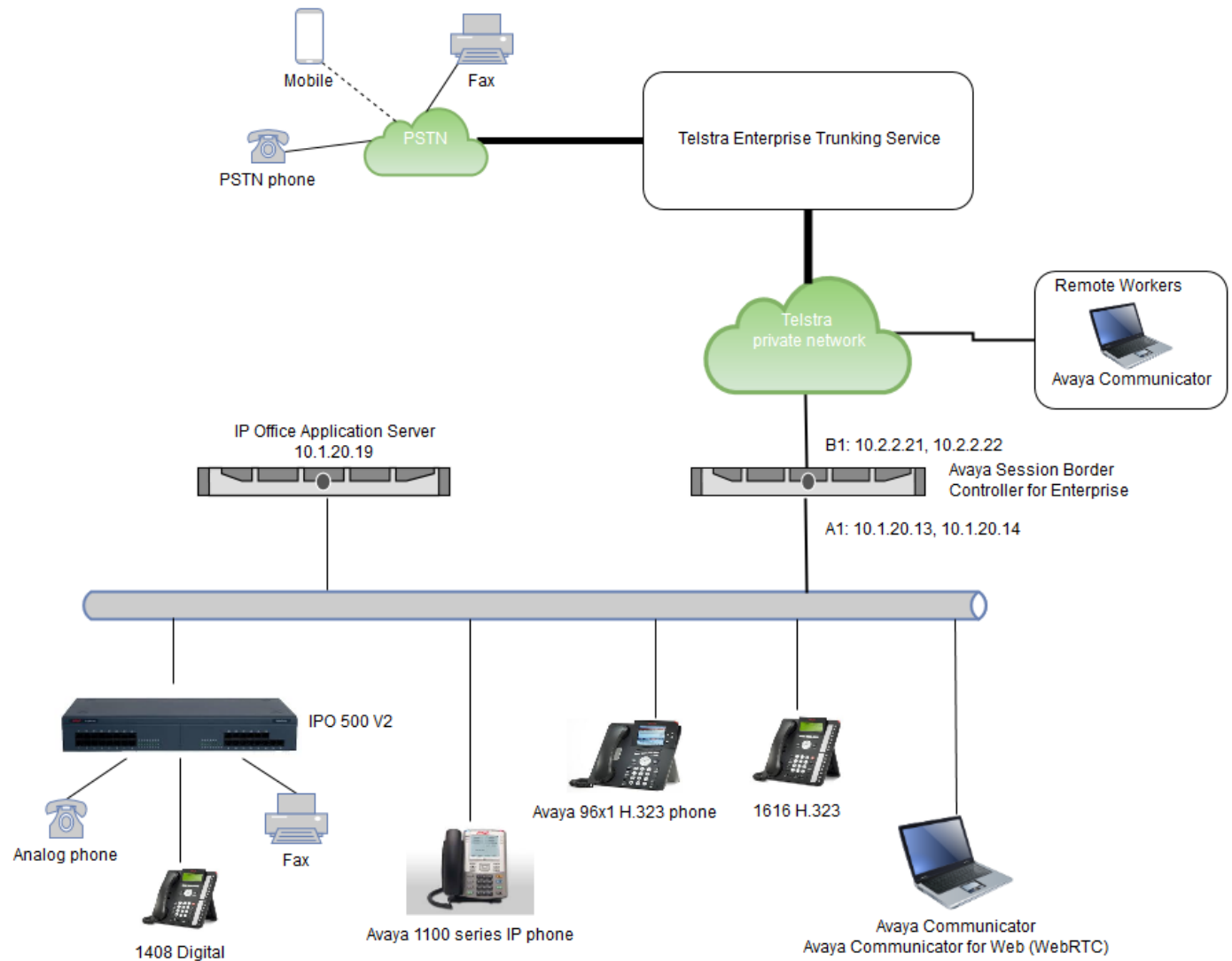
- Avaya 1400 Series Digital Telephones.
- The Avaya SBCE 7.1 provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the Telstra Enterprise SIP Trunking service and the enterprise internal network.
- Telstra Enterprise 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
<b>Avaya</b>	
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
<b>Service Provider</b>	
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.

The screenshot displays the Avaya IP Office Manager interface. On the left, the 'IP Offices' tree shows a hierarchy: BOOTP (1), Operator (3), ipo10, System (1), and Line (9). The main pane is titled 'ipo10' and contains several tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VCM, VoIP, VoIP Security, and Contact Center. The 'LAN1' tab is active, showing 'LAN Settings'. The 'IP Address' field is set to '10 . 1 . 20 . 19' and the 'IP Mask' field is set to '255 . 255 . 255 . 0'. The 'Primary Trans. IP Address' field is set to '0 . 0 . 0 . 0'. The 'RIP Mode' dropdown is set to 'None'. The 'Enable NAT' checkbox is unchecked. The 'Number Of DHCP IP Addresses' spinner is set to '1'. The 'DHCP Mode' section has four radio buttons: 'Server', 'Client', 'Dial In', and 'Disabled'. The 'Disabled' radio button is selected. An 'Advanced' button is located at the bottom right of the settings pane.

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.

The screenshot shows the 'VoIP' configuration page with the following settings:

- H323 Gatekeeper Enable**: ☒ (highlighted with a red box)
- Auto-create Extension**: ☐
- Auto-create User**: ☐
- H323 Remote Extension Enable**: ☐
- H323 Signaling over TLS**: Disabled
- Remote Call Signaling Port**: 1720
- SIP Trunks Enable**: ☒ (highlighted with a red box)
- SIP Registrar Enable**: ☒ (highlighted with a red box)
- Auto-create Extension/User**: ☐
- SIP Remote Extension Enable**: ☐
- SIP Domain Name**: sipinterop.net (highlighted with a red box)
- SIP Registrar FQDN**: (empty)
- Layer 4 Protocol**:
  - ☒ UDP, UDP Port: 5060
  - ☒ TCP, TCP Port: 5060
  - ☐ TLS, TLS Port: 5061
- Remote UDP Port**: 5060
- Remote TCP Port**: 5060
- Remote TLS Port**: 5061
- Challenge Expiration Time (sec)**: 10

The screenshot shows the 'RTP' configuration page with the following settings:

- Port Number Range**:
  - Minimum: 46750, Maximum: 50750
- Port Number Range (NAT)**:
  - Minimum: 46750, Maximum: 50750
- Enable RTCP Monitoring on Port 5005**: ☒ (highlighted with a red box)
- RTCP collector IP address for phones**: 0 . 0 . 0 . 0
- Keepalives**:
  - Scope**: Disabled
  - Periodic timeout**: 0
  - Initial keepalives**: Disabled
- DiffServ Settings**:
 

B8	DSCP (Hex)	B8	Video DSCP (Hex)	FC	DSCP Mask (Hex)	88	SIG DSCP (Hex)
46	DSCP	46	Video DSCP	63	DSCP Mask	34	SIG DSCP

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.

The screenshot shows the 'Network Topology' configuration page. The 'Firewall/NAT Type' dropdown menu is highlighted with a red box and is set to 'Unknown'. Other visible fields include 'STUN Server Address' (0.0.0.0), 'STUN Port' (3478), 'Binding Refresh Time (sec)' (0), 'Public IP Address' (0.0.0.0), and 'Public Port' (UDP, TCP, TLS all set to 0). A 'Run STUN' button is also visible.

## 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.

The screenshot shows the 'System Telephony Settings' page. The 'Companding Law' section is highlighted with a red box, showing 'A-Law' selected for both 'Switch' and 'Line'. The 'Dial Delay Time (sec)' is set to 4 and 'Dial Delay Count' is set to 15, both highlighted with red boxes. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked and highlighted with a red box.

## 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.

The screenshot displays the 'System Codec Settings' interface. At the top, there is a navigation bar with tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VCM, VoIP, and VoIP Security. The 'VoIP' tab is selected. Below the navigation bar, there are two checkboxes: 'Ignore DTMF Mismatch For Phones' and 'Allow Direct Media Within NAT Location', both of which are unchecked. The 'RFC2833 Default Payload' is set to '101'. Below this, there are three main sections: 'Available Codecs', 'Default Codec Selection', and 'Selected'. The 'Available Codecs' section lists five codecs with checkboxes: G.711 ULAW 64K (checked), G.711 ALAW 64K (checked), G.722 64K (unchecked), G.729(a) 8K CS-ACELP (checked), and G.723.1 6K3 MP-MLQ (checked). The 'Default Codec Selection' section has a sub-section 'Unused' containing 'G.723.1 6K3 MP-MLQ'. The 'Selected' section contains 'G.711 ALAW 64K', 'G.711 ULAW 64K', and 'G.729(a) 8K CS-ACELP'. Between the 'Unused' and 'Selected' sections are four buttons: '>>>', '<<<', '<<<', and '>>>'. The 'Selected' section is highlighted with a red border.

## 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.

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials	SIP Advanced	Engineering
<div><div><div>Line Number<input type="text" value="10"/></div><div>ITSP Domain Name<input type="text" value="sipconn.test1.com"/></div><div>Local Domain Name<input type="text" value="sipinterop.net"/></div><div>URI Type<input type="text" value="SIP"/></div><div>Location<input type="text" value="Cloud"/></div></div><div><div>Prefix<input type="text"/></div><div>National Prefix<input type="text" value="0"/></div><div>International Prefix<input type="text"/></div><div>Country Code<input type="text" value="61"/></div><div>Name Priority<input type="text" value="System Default"/></div><div>Description<input type="text"/></div></div></div> <div><div><div>In Service<input checked="" type="checkbox"/></div><div>Check OOS<input checked="" type="checkbox"/></div></div><div><div>Session Timers</div><div>Refresh Method<input type="text" value="Auto"/></div><div>Timer (sec)<input type="text" value="On Demand"/></div></div><div><div>Redirect and Transfer</div><div>Incoming Supervised REFER<input type="text" value="Auto"/></div><div>Outgoing Supervised REFER<input type="text" value="Auto"/></div><div>Send 302 Moved Temporarily<input type="checkbox"/></div><div>Outgoing Blind REFER<input type="checkbox"/></div></div></div>							

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**.

The screenshot shows the 'Transport' tab of the Avaya SIP Line configuration. The 'ITSP Proxy Address' is set to '10.1.20.13'. The 'Network Configuration' section shows 'Layer 4 Protocol' set to 'TCP', 'Send Port' set to '5060', and 'Use Network Topology Info' set to 'None'. The 'Listen Port' is also set to '5060'. The 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is checked. The 'Separate Registrar' field is empty.

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.

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials	SIP Advanced	Engineering
<b>Edit URI</b>							
Local URI	Use Internal Data ▼						
Contact	Use Internal Data ▼						
Display Name	Use Internal Data ▼						
<b>Identity</b>							
Identity	Use Internal Data ▼						
Header	P Asserted ID ▼						
<b>Forwarding And Twinning</b>							
Originator Number	<input type="text"/>						
Send Caller ID	Diversion Header ▼						
Diversion Header	None ▼						
Registration	0: <None> ▼						
Incoming Group	10 ▼						
Outgoing Group	10 ▼						
Max Sessions	5 ▲▼						

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.

The screenshot displays the Avaya IP Office configuration interface for the VoIP tab. The interface includes a top navigation bar with tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The VoIP tab is selected.

The main configuration area is divided into several sections:

- Codec Selection:** A pull-down menu is set to "System Default". Below it, there are two lists: "Unused" and "Selected". The "Selected" list contains the following codecs: G.711 ALAW 64K, G.729(a) 8K CS-ACELP, and G.711 ULAW 64K. Arrows between the lists allow for moving codecs between them.
- Checkboxes:** On the right side, there are several checkboxes:
  - ☐ VoIP Silence Suppression
  - ☐ Local Hold Music
  - ☒ Re-invite Supported
  - ☐ Codec Lockdown
  - ☐ Allow Direct Media Path
  - ☐ Force direct media with phones
  - ☐ PRACK/100rel Supported
  - ☐ G.711 Fax ECAN
- Fax Transport Support:** A pull-down menu set to "G.711".
- DTMF Support:** A pull-down menu set to "RFC2833".
- Media Security:** A pull-down menu set to "Disabled".



Select **SIP Advanced** tab:

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

The screenshot shows the 'SIP Advanced' configuration tab. On the left, the 'Addressing' section has 'Association Method' set to 'By Source IP address' and 'Call Routing Method' set to 'Request URI'. The 'Identity' section has several checkboxes, with 'Cache Auth Credentials' checked. On the right, the 'Media' section has 'Indicate HOLD' checked and highlighted with a red box. The 'Call Control' section has 'Service Busy Response' set to '503 - Service Unavailable' and highlighted with a red box. Other settings include 'Call Initiation Timeout (s)' at 4, 'Call Queuing Timeout (mins)' at 5, 'on No User Responding Send' set to '408-Request Timeout', and 'Action on CAC Location Limit' set to 'Allow Voicemail'.

## 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)**.

The screenshot shows the 'Short Code' configuration details pane. The 'Code' field is set to '?', 'Feature' is 'Dial', 'Telephone Number' is '.', 'Line Group ID' is '50: Main', and 'Locale' is 'Australia (UK English)'. These fields are highlighted with a red box. Below these fields, there are checkboxes for 'Force Account Code' and 'Force Authorization Code', both of which are unchecked.

## 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.

The screenshot shows the ARS configuration interface. The 'ARS Route ID' is set to 50. The 'Route Name' is 'Main'. The 'Dial Delay Time' is 'System Default (4)'. The 'Description' field is empty. The 'In Service' checkbox is checked. The 'Time Profile' is set to '<None>'. The 'Out of Service Route' and 'Out of Hours Route' are both set to '<None>'. A table at the bottom is used to add routes, with one entry highlighted in red:

Code	Telephone Number	Feature	Line Group ID
?	.	Dial	10

Buttons for 'Add...', 'Remove', and 'Edit...' are located to the right of the table.

## 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**.

The screenshot shows the SIP configuration interface. The 'SIP Name' field is set to '353XXXXXX'. The 'SIP Display Name (Alias)' field is set to '353XXXXXX'. The 'Contact' field is set to '353XXXXXX'. The 'Anonymous' checkbox is unchecked.

## 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 353xxxxxx due to security reasons.
- Default values can be used for all other fields.

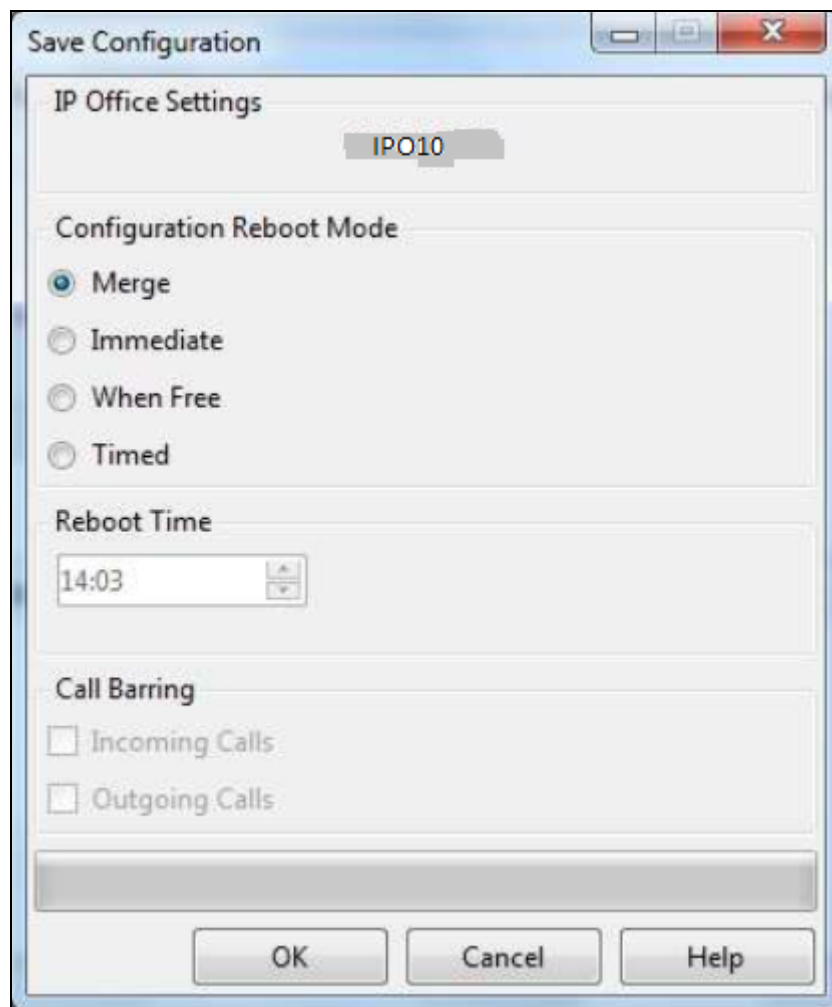
Standard	Voice Recording	Destinations
Bearer Capability	Any Voice	
Line Group ID	10	
Incoming Number	353xxxxxx	
Incoming Sub Address		
Incoming CLI		
Locale	Australia (UK English)	
Priority	1 - Low	
Tag		
Hold Music Source	System Source	
Ring Tone Override	None	

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. 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.

Standard	Voice Recording	Destinations	
	TimeProfile	Destination	Fallback Extension
►	Default Value	659 Extn659	

## 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.



The image shows a 'Save Configuration' dialog box with a title bar containing standard window controls. The dialog is divided into several sections. The first section, 'IP Office Settings', contains a text field with the value 'IPO10'. The second section, 'Configuration Reboot Mode', contains four radio button options: 'Merge' (which is selected), 'Immediate', 'When Free', and 'Timed'. The third section, 'Reboot Time', contains a time selection field showing '14:03'. The fourth section, 'Call Barring', contains two unchecked checkboxes: 'Incoming Calls' and 'Outgoing Calls'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

## 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**.

AVAYA

Session Border Controller for Enterprise

Log In

Username:

The system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modification of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

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

AVAYA

Session Border Controller for Enterprise

Log In

Username:

Password:

The system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modification of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

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.

**Session Border Controller for Enterprise**

**Dashboard**

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation.

Information	
System Time	01:35:10 PM AEST
Version	7.1.0.0-04-11122
Build Date	Thu Jun 9 20:20:31 EDT 2016
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	09/21/2016 17:01:46 AEST
Failed Login Attempts	0

**Installed Devices**

Device Name
sbce207

## 6.1 System Management – Status

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

**System Management**

**Devices** | Updates | SSL VPN | Licensing

Device Name	Management IP	Version	Status
sbce207	10.1.30.7	7.1.0.0-04-11122	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.

**System Information: sbce207**
X

**General Configuration**  
Appliance Name    sbce207  
Box Type            SIP  
Deployment Mode   Proxy

**Device Configuration**  
HA Mode            No  
Two Bypass Mode   No

**License Allocation**  
Standard Sessions    20  
Requested: 20  
Advanced Sessions    20  
Requested: 20  
Scoopia Video Sessions   20  
Requested: 20  
CES Sessions            0  
Requested: 0  
Transcoding Sessions   0  
Requested: 0  
Encryption            ☒

**Network Configuration**  

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.1.20.13	10.1.20.13	255.255.255.0	10.1.20.1	A1
10.1.20.14	10.1.20.14	255.255.255.0	10.1.20.1	A1
10.2.2.21	10.2.2.21	255.255.255.128	10.2.2.1	B1
10.2.2.22	10.2.2.22	255.255.255.128	10.2.2.1	B1

**DNS Configuration**  
Primary DNS    10.86.113.20  
Secondary DNS   10.86.114.20  
DNS Location    DMZ  
DNS Client IP   10.2.2.21

**Management IP(s)**  
IP #1 (IPv4)    10.1.30.7

## 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**.

The screenshot shows the 'Interworking Profile' configuration window with the 'General' tab selected. The 'T.38 Support' checkbox is highlighted with a red box and is currently unchecked. Other options include:

- Hold Support:** Radio buttons for None (selected), RFC2543 - c=0.0.0.0, and RFC3264 - a=sendsonly.
- 180 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 181 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 182 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 183 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- Refer Handling:** Check box (unchecked).
- URI Group:** Dropdown menu set to 'None'.
- Send Hold:** Check box (unchecked).
- Delayed Offer:** Check box (unchecked).
- 3xx Handling:** Check box (unchecked).
- Diversion Header Support:** Check box (unchecked).
- Delayed SDP Handling:** Check box (unchecked).
- Re-Invite Handling:** Check box (unchecked).
- Prack Handling:** Check box (unchecked).
- Allow 18X SDP:** Check box (unchecked).
- URI Scheme:** Radio buttons for SIP (selected), TEL, and ANY.
- Via Header Format:** Radio buttons for RFC3261 (selected) and RFC2543.

At the bottom are 'Back' and 'Next' buttons.



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**

The screenshot shows the 'Editing Profile: IPO' window with the following configuration options:

- Record Routes**: Radio buttons for None, Single Side, **Both Sides** (selected), Dialog-Initiate Only (Single Side), and Dialog-Initiate Only (Both Sides).
- Include End Point IP for Context Lookup**: Check box (unchecked).
- Extensions**: Dropdown menu set to **Avaya**.
- Diversion Manipulation**: Check box (unchecked).
- Diversion Condition**: Dropdown menu set to **None**.
- Diversion Header URI**: Text input field (empty).
- Has Remote SBC**: Check box (checked).
- Route Response on Via Port**: Check box (unchecked).
- Relay INVITE Replace for SIPREC**: Check box (unchecked).
- DTMF**: Section header.
- DTMF Support**: Radio buttons for **None** (selected), SIP NOTIFY, and SIP INFO.
- Finish**: Button at the bottom.

### 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**.

The screenshot shows a window titled "Editing Profile: Telstra" with a close button (X) in the top right corner. The window contains a "General" tab with the following settings:

- Hold Support:** Radio buttons for ☒ None, ☐ RFC2543 - c=0.0.0.0, and ☐ RFC3264 - a=sendonly.
- 180 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 181 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 182 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 183 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- Refer Handling:** ☐
- URI Group:** A dropdown menu showing "None".
- Send Hold:** ☐
- Delayed Offer:** ☐
- 3xx Handling:** ☐
- Diversion Header Support:** ☐
- Delayed SDP Handling:** ☐
- Re-Invite Handling:** ☐
- Prack Handling:** ☐
- Allow 18X SDP:** ☐
- T.38 Support:** ☐ (This row is highlighted with a red border in the original image).
- URI Scheme:** Radio buttons for ☒ SIP, ☐ TEL, and ☐ ANY.
- Via Header Format:** Radio buttons for ☒ RFC3261 and ☐ RFC2543.

At the bottom of the window is a "Finish" button.

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

The screenshot shows a window titled "Editing Profile: Telstra" with a close button (X) in the top right corner. The window contains several configuration sections:

- Record Routes:** A red box highlights the radio button options. "Both Sides" is selected.
- Include End Point IP for Context Lookup:** An unchecked checkbox.
- Extensions:** A red box highlights the dropdown menu, which is set to "None".
- Diversion Manipulation:** An unchecked checkbox.
- Diversion Condition:** A dropdown menu set to "None".
- Diversion Header URI:** An empty text input field.
- Has Remote SBC:** A red box highlights the checked checkbox.
- Route Response on Via Port:** An unchecked checkbox.
- Relay INVITE Replace for SIPREC:** An unchecked checkbox.
- DTMF:** A section header with a dark background.
- DTMF Support:** Radio button options: "None" (selected), "SIP NOTIFY", and "SIP INFO".

A "Finish" button is located at the bottom center of the window.

## 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).

IP Address / FQDN	Port	Transport
10.1.20.19	5060	TCP

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).

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	30 seconds
From URI	ping@sipinterop.net
To URI	ping@sipinterop.net

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

The screenshot shows a window titled "Edit Server Configuration Profile - Advanced". It contains the following settings:

Option	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	IPO
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061

A "Finish" button is located at the bottom right of the window.

## 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).

**Edit Server Configuration Profile - General** X

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server

Add

IP Address / FQDN	Port	Transport	
sbc-cw.ipvs.net	5060	UDP	Delete

Finish

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.

Enable Authentication ☒

User Name N3312101R

Realm  
(Leave blank to detect from server challenge)

Password  
(Leave blank to keep existing password)

Confirm Password

Finish

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.

Rename Clone Delete

General Authentication **Heartbeat** Advanced

Enable Heartbeat ☒

Method REGISTER

Frequency 600 seconds

From URI 353xxx607@sipconn.test1.com

To URI 353xxx607@sipconn.test1.com

Edit

5. Under Advanced window:

- Select **Telstra** for Interworking Profile.
- Select **Telstra\_pri** for Signaling Manipulation Script (see **Notice 1**).

Server Configuration: Telstra\_pri

Buttons: Add, Rename, Clone, Delete

Tabs: General, Authentication, Heartbeat, **Advanced**

Left Sidebar: Server Profiles, Session Manager, **Telstra\_pri**, Telstra\_sec

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Telstra
Signaling Manipulation Script	Telstra_pri
Connection Type	SUBID
Securable	<input type="checkbox"/>

Buttons: Edit

**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";
}
}
}
```

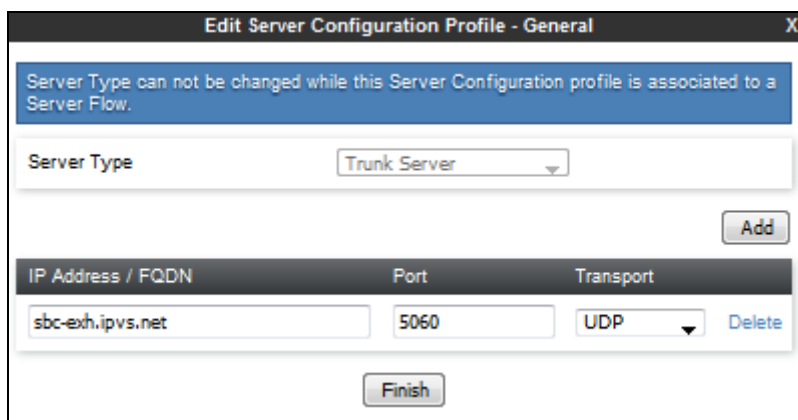




### 6.2.5.2 Telstra secondary

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.

**Edit Server Configuration Profile - Authentication**

Enable Authentication ☒

User Name

Realm   
(Leave blank to detect from server challenge)

Password   
(Leave blank to keep existing password)

Confirm Password

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.

**Edit Server Configuration Profile - Heartbeat**

Enable Heartbeat ☒

Method

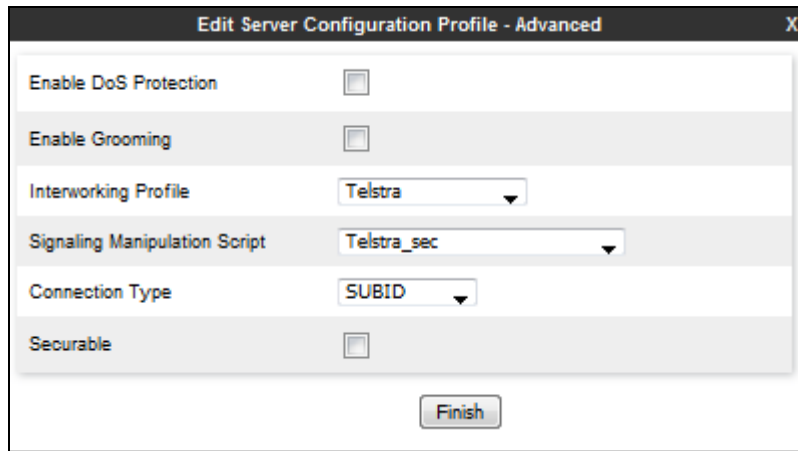
Frequency  seconds

From URI

To URI

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";
}
}
}
```

Signaling Manipulation Scripts Telstra\_sec

Upload Add Download Clone Delete

Click here to add a description

Signaling Manipulation

```

within session "INVITE"
{
  act on request where NDIRECTION="OUTBOUND" and XENTRY_POINT="POST_ROUTING"
  {
    $HEADERS["P-Asserted-Identity"][1].URI.USER = "353X00657";
  }
}

within session "ALL"
{
  act on request where NDIRECTION="OUTBOUND" and XENTRY_POINT="POST_ROUTING"
  {
    if ($HEADERS["FROM"][1].URI.USER = "anonymous") then
    {
      $HEADERS["FROM"][1].URI.USER = "353X00657";
    }
  }
}

```

Edit

## 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**.

Profile : IPO - Edit Rule

URI Group \* Time of Day default

Load Balancing Priority NAPTR

Transport None Next Hop Priority ☒

Next Hop In-Dialog ☒ Ignore Route Header ☐

ENUM ☐ ENUM Suffix

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IPO	10.1.20.19:5060 (TCP)	None	Delete

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**.

The screenshot shows the 'Profile : Telstra - Edit Rule' window. The top section contains configuration options: URI Group (set to '\*'), Time of Day (set to 'default'), Load Balancing (set to 'Round-Robin'), NAPTR (unchecked), Transport (set to 'None'), Next Hop Priority (checked), Next Hop In-Dialog (unchecked), and Ignore Route Header (unchecked). An 'Add' button is located to the right of these options. Below this is a table with two rows of server configurations. The first row has Priority/Weight 0, Server Configuration 'Telstra\_pri', Next Hop Address 'sbc-cw.ipvs.net:5060 (UDP)', and Transport 'None'. The second row has Priority/Weight 0, Server Configuration 'Telstra\_sec', Next Hop Address 'sbc-exh.ipvs.net:5060 (UDP)', and Transport 'None'. Each row has a 'Delete' button to its right. A 'Finish' button is at the bottom center.

Priority / Weight	Server Configuration	Next Hop Address	Transport	
0	Telstra_pri	sbc-cw.ipvs.net:5060 (UDP)	None	Delete
0	Telstra_sec	sbc-exh.ipvs.net:5060 (UDP)	None	Delete

### 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.

**Application Rules: default**

Buttons: Add, Filter By Device..., Clone

Application Rules:

- default
- default-trunk
- default-subscriber-low
- default-subscriber-high
- default-server-low
- default-server-high

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

**Application Rule**

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>		

**Miscellaneous**

CDR Support	None
RTCP Keep-Alive	No

Edit

### 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.

**Border Rules: default**

Buttons: Add, Filter By Device..., Clone

Border Rules:

- default
- No-Nat-Reg-Proxy

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

**NAT Traversal**

Enable Natting	<input checked="" type="checkbox"/>
Use SIP Published IP	<input checked="" type="checkbox"/>
Use SDP Published IP	<input checked="" type="checkbox"/>

Edit

### 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.

Media Rules: default-low-med

Add Filter By Device... Clone

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- default-low-med-MR

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Media Encryption Media Silencing Media QoS Media BFCP Media FECC

Audio Encryption

Preferred Formats RTP

Interworking ☒

Video Encryption

Preferred Formats RTP

Interworking ☒

Miscellaneous

Capability Negotiation ☐

Edit

Media Rules: default-low-med

Add Filter By Device... Clone

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- default-low-med-MR

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Media Encryption Media Silencing Media QoS Media BFCP Media FECC

Media Silencing ☐

Edit

Media Rules: default-low-med

Add Filter By Device... Clone

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- default-low-med-MR

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Media Encryption Media Silencing Media QoS Media BFCP Media FECC

Media QoS Reporting

RTCP Enabled ☐

Media QoS Marking

Enabled ☒

QoS Type DSCP

Audio QoS

Audio DSCP EF

Video QoS

Video DSCP EF

Edit



### 6.3.4 Signaling Rules

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

Signaling Rules: default

Signaling Rules

default

No-Content-Type-Checks

Filter By Device...

Clone

General

Requests

Responses

Request Headers

Response Headers

Signaling QoS

UCID

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Inbound

Requests

Non-2XX Final Responses

Optional Request Headers

Optional Response Headers

Outbound

Requests

Non-2XX Final Responses

Optional Request Headers

Optional Response Headers

Content-Type Policy

Enable Content-Type Checks

Action

Exception List

Multipart Action

Exception List

Edit

### 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.

Policy Groups: default-low

Policy Groups

default-low

default-low-enc

default-med

default-med-enc

default-high

default-high-enc

avaya-def-low-enc

avaya-def-high-subscriber

avaya-def-high-server

Filter By Device...

Clone

It is not recommended to edit the defaults. Try cloning or adding a new group instead.

Hover over a row to see its description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling
1	default	default	default-low-med	default-low	default

Edit

## 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.

Network Management: sbce207

Devices sbce207	Interfaces	Networks	
--------------------	------------	----------	--

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1	10.1.20.1	255.255.255.0	A1	10.1.20.13, 10.1.20.14	Edit Delete
B1	10.2.2.1	255.255.255.128	B1	10.2.2.21, 10.2.2.22	Edit Delete

## 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.

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Name	Media IP Network	Port Range	
A1_Med_IPO_trunking	10.1.20.13 A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
B1_Med_IPO_trunking	10.2.2.21 B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
B1_Med_IPO_RW	10.2.2.22 B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
A1_Med_IPO_RW	10.1.20.14 A1 (A1, VLAN 0)	35000 - 40000	Edit Delete

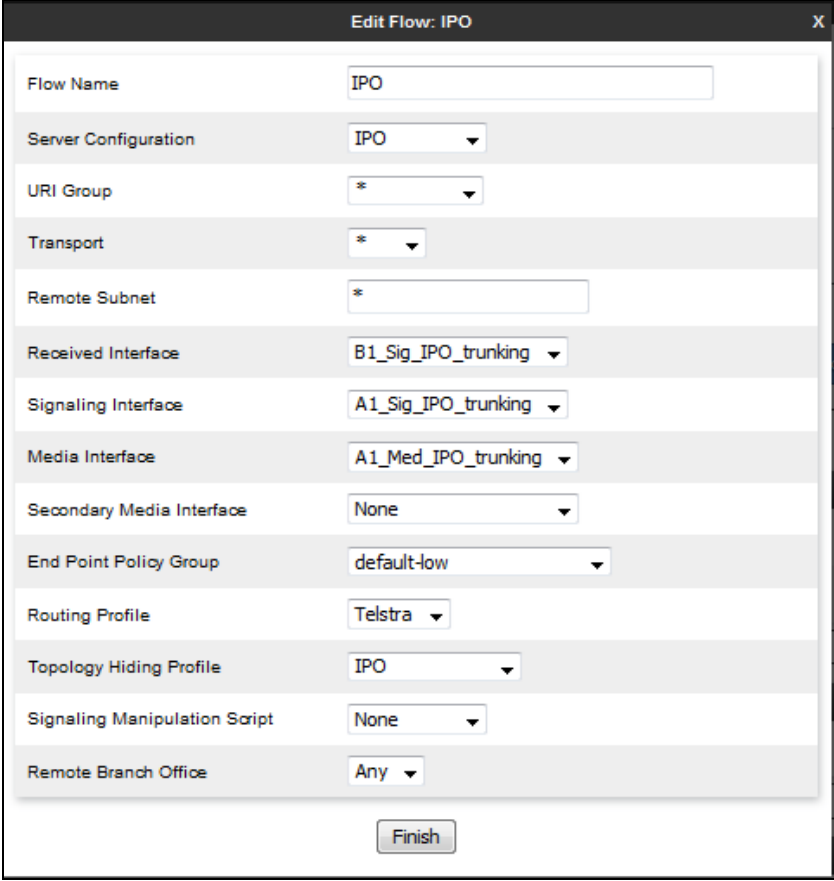
### 6.4.3 Signaling Interface

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.

Signaling Interface						
Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from <a href="#">System Management</a> .						
<a href="#">Add</a>						
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	<a href="#">Edit</a> <a href="#">Delete</a>
B1_Sig_IPO_trunking	10.2.2.21 B1 (B1, VLAN 0)	5060	5060	---	None	<a href="#">Edit</a> <a href="#">Delete</a>
B1_Sig_IPO_RW	10.2.2.22 B1 (B1, VLAN 0)	5060	5060	---	None	<a href="#">Edit</a> <a href="#">Delete</a>
A1_Sig_IPO_RW	10.1.20.14 A1 (A1, VLAN 0)	5060	5060	---	None	<a href="#">Edit</a> <a href="#">Delete</a>

#### 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**.



The screenshot shows a window titled "Edit Flow: IPO" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a value or dropdown menu. The fields are as follows:

Field Label	Value
Flow 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
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Telstra
Topology Hiding Profile	IPO
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom of the window, there is a "Finish" button.

## 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

The screenshot shows a configuration window titled "Edit Flow: Telstra\_pri". It contains the following fields and values:

Field	Value
Flow 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
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	IPO
Topology Hiding Profile	Telstra
Signaling Manipulation Script	None
Remote Branch Office	Any

A "Finish" button is located at the bottom center of the window.

### 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

Flow 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

Secondary Media Interface: None

End Point Policy Group: default-low

Routing Profile: IPO

Topology Hiding Profile: Telstra

Signaling Manipulation Script: None

Remote Branch Office: Any

Finish

## 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 screenshot shows the 'Trace: sbce' window with the 'Packet Capture' tab selected. The 'Captures' sub-tab is also visible. The 'Packet Capture Configuration' section shows the following settings: Status: Ready, Interface: B1, Local Address: 10.2.2.135, Remote Address: \*, Protocol: All, Maximum Number of Packets to Capture: 3000, and Capture Filename: test.pcap. The 'Start Capture' and 'Clear' buttons are at the bottom.

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

The screenshot shows the 'Trace: sbce' window with the 'Packet Capture' tab selected. The 'Captures' sub-tab is also visible. The 'Packet Capture Configuration' section shows the following settings: Status: In Progress, Interface: B1, Local Address: 10.2.2.135, Remote Address: \*, Protocol: All, Maximum Number of Packets to Capture: 3000, and Capture Filename: test.pcap. The 'Stop Capture' button is at the bottom. A message at the top states: 'A packet capture is currently in progress. This page will automatically refresh until the capture completes.'

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.

Trace: sbce

Devices  
sbce

Packet Capture Captures

Refresh

File Name	File Size (bytes)	Last Modified	
<a href="#">test_20160405184126.pcap</a>	0	April 5, 2016 6:41:26 PM AEST	<a href="#">Delete</a>

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.

**Diagnostics** AVAYA

Devices  
sbce

Full Diagnostic Ping Test

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Stop Diagnostic

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (10.1.20.1)	Average ping from 10.1.20.160 [A1] to 10.1.20.1 is 1.103ms.
⌛ Ping: SBC (A1) to Primary DNS (10.86.113.20)	Running...
✗ Ping: SBC (A1) to Secondary DNS (10.86.114.20)	



Incident Viewer

AVAYA

Device 

All

 Category 

All

Clear Filters

Refresh

Generate Report

Displaying results 1 to 15 out of 44.

Type	ID	Date	Time	Category	Device	Cause
Server Heartbeat	729881580397602	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580396121	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580393451	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881402194116	4/4/16	7:40 PM	Policy	sbce	Heartbeat Successful, Server is UP

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):

AVAYA

IP Office System Status

Help Snapshot LogOff Exit About

System

Alarms (0)

Extensions (18)

Trunks (9)

Lines: 1 - 4

Lines: 5 - 8

Line: 10

Active Calls

Resources

Voicemail

IP Networking

Locations

Status

Utilization Summary

Alarms

SIP Trunk Summary

Line Service State:

In Service

Peer Domain Name:

sipconn.test1.com

Resolved Address:

10.1.20.13

Line Number:

10

Number of Administered Channels:

5

Number of Channels in Use:

0

Administered Compression:

G711 A, G729 A, G711 Mu

Enable Faststart:

Off

Silence Suppression:

Off

Media Stream:

RTP

Layer 4 Protocol:

TCP

SIP Trunk Channel Licenses:

128

0%

SIP Trunk Channel Licenses in Use:

0

SIP Device Features:

UPDATE (Incoming and Outgoing)

Chan...

U...

Call

Curr...

Time in

Remote

Co...

Conn...

Caller

Other Party

Dirac...

Round

Recei...

Rece...

Tran...

Tran...

Ref

State

Media ...

ID or ...

on Call

Trip ...

1

Idle

00:0...

Trace

Trace All

Pause

Ping

Call Details

Graceful Shutdown

Force Out of Service

Print...

Save As...

12:27:13 PM

Online

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.

---

**©2016 Avaya Inc. All Rights Reserved.**

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

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