



Avaya Solution & Interoperability Test Lab

Application Notes for SIP Trunking between OneAccess-Telstra Business SIP and Avaya IP Office Release 10.1 and Avaya Session Border Controller for Enterprise Release 7.2.1 - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya IP Office Release 10.1 with SIP Trunks to the Avaya Session Border Controller for Enterprise Release 7.2.1 (Avaya SBCE) when used to connect the OneAccess-Telstra Business SIP (Australia).

OneAccess-Telstra Business SIP provides PSTN access via a SIP trunk between the enterprise and the OneAccess-Telstra Business SIP 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.

OneAccess-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 OneAccess test 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	7
5.	Configure Avaya IP Office	8
5.1	LAN1 Settings.....	8
5.2	System Telephony Settings	11
5.3	System Codec Settings	12
5.4	Administer SIP Line.....	13
5.5	Short Codes	19
5.6	ARS table	20
5.7	User	21
5.8	Incoming Call Route	22
5.9	Save Configuration.....	23
6.	Configure Avaya Session Border Controller for Enterprise	24
6.1	System Management – Status	26
6.2	Global Profiles.....	26
6.2.1	Uniform Resource Identifier (URI) Groups.....	26
6.3	Server Interworking – Avaya	27
6.3.1	Server Interworking – OneAccess	29
6.3.2	Signaling Manipulation – OneAccess.....	31
6.3.3	Server Configuration – Avaya	32
6.3.4	Server Configuration – OneAccess.....	34
6.3.5	Routing – To Avaya.....	38
6.3.6	Routing – To OneAccess	39
6.3.7	Topology Hiding – Avaya	40
6.3.8	Topology Hiding – OneAccess	41
6.4	Domain Policies	41
6.4.1	Application Rules.....	41
6.4.2	Border Rules	41
6.4.3	Media Rules	42
6.4.4	Signaling Rules	42
6.4.5	Endpoint Policy Groups	42
6.5	Device Specific Settings.....	43
6.5.1	Network Management.....	43
6.5.2	Media Interfaces.....	44
6.5.3	Signaling Interface	45
6.5.4	Endpoint Flows – For Avaya	46
6.5.5	Endpoint Flows – For OneAccess.....	48

7.	Verification Steps.....	50
7.1	Avaya Session Border Controller for Enterprise.....	50
7.2	Avaya IP Office.....	53
8.	Telephony Services	54
9.	Conclusion	54
10.	Additional References.....	54

1. Introduction

These Application Notes illustrate a sample configuration for Avaya IP Office Release 10.1 with SIP Trunks to the Avaya Session Border Controller for Enterprise Release 7.2.1 (Avaya SBCE) when used to connect to the OneAccess-Telstra Business SIP (Australia).

The enterprise SIP Trunking service available from OneAccess-Telstra Business SIP is one of many SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. The OneAccess-Telstra Business SIP 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 OneAccess-Telstra Business SIP. 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.

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

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

2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya IP Office, the Avaya SBCE, and the OneAccess-Telstra Business SIP.

The compliance testing was based on the standard Avaya DevConnect Generic SIP Trunk test plan and the Telstra Business SIP Accreditation test plan. The testing covered functionality required for compliance as a solution supported on the OneAccess-Telstra Business SIP. Calls were made to and from the PSTN across the OneAccess-Telstra Business SIP. 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.
- Dialing plans including local, long distance, international, outbound toll-free, calls etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.729A, G.711A and G.711MU.
- Fax using pass-through mode.
- 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.

2.2 Test Results

Interoperability testing of OneAccess-Telstra Business SIP 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.

- **User-Agent header** - As OneAccess SIP NTU requires User-Agent header in the SIP messages sent to it, a Sigma script must be used on Avaya SBCE to insert User-Agent header into SIP messages before Avaya SBCE sends those messages to OneAccess SIP NTU.

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>
- **OneAccess-Telstra Business SIP:** Customers should contact their OneAccess-Telstra representative or follow the support links available on <https://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 2400 Series Digital Telephones.
- The Avaya SBCE 7.2.1 provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the OneAccess-Telstra Business SIP and the enterprise network.
- OneAccess-Telstra Business SIP provided one trunk group and DID range for this testing is 0285xxx4xx (10 digits). Enterprise network is connected to Telstra network via OneAccess SIP Network Termination Unit (NTU).

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

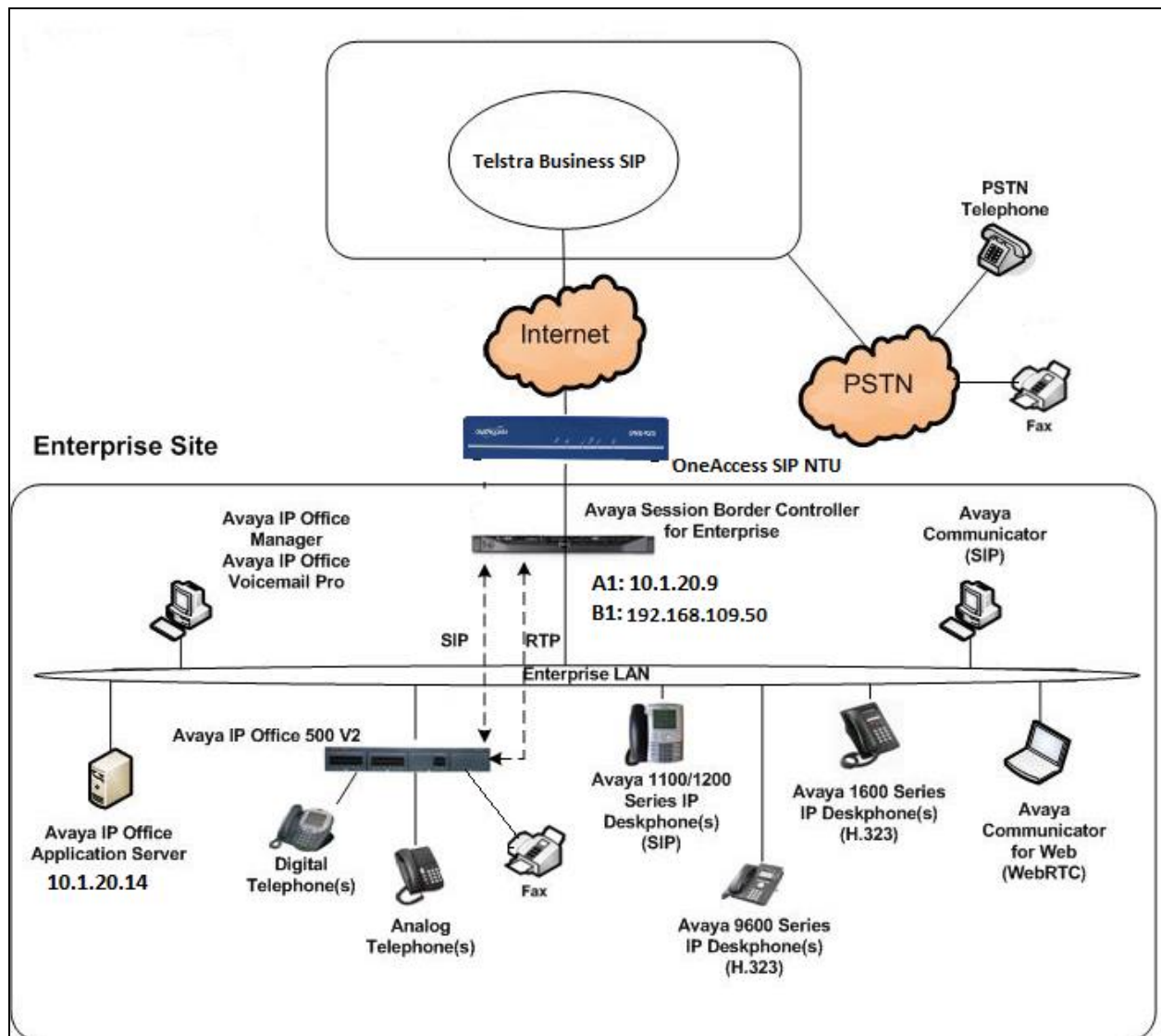


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya IP Office	10.1.0.1.0_3
Avaya SBCE	7.2.1.0-05-14222
Avaya 9600 Series IP Deskphones – H323	96x1-IPT-H323-R6_6_5_06-080917
Avaya 2400 Series Digital phones	R6
Avaya 1600 Series IP Deskphones, H.323	16xx-IPT-H323-R1_3_11-022417
Avaya 1100 Series IP Deskphones, SIP	4.4.8
Avaya Communicator for Windows	2.1.4.0
Analog Telephones	N/A
Service Provider	
OneAccess-Telstra Business SIP	Broadworks Version R19 SP1 SIP NTU: V5.2R2C3_KE3

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to Avaya SBCE. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start > Programs > IP Office > Manager** to launch the application. Navigate to **File > Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials (not shown).

5.1 LAN1 Settings

In the sample configuration, the LAN1 port was used to connect to Avaya SBCE. To access the LAN1 settings, first navigate to **System (1) > 000C292B2458** 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 configuration window. On the left is a tree view under the 'Configuration' header, showing a hierarchy from 'Solution' down to 'Line (2)'. The 'System (1)' node is expanded, showing '000C292B2458'. The main pane on the right is titled '000C292B2458' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', 'System Events', and 'SMTP'. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The 'IP Address' field is set to '10 . 1 . 20 . 14' and the 'IP Mask' field is set to '255 . 255 . 255 . 0'. Below these, the 'Number Of DHCP IP Addresses' is set to '200'. The 'DHCP Mode' section has three radio buttons: 'Server', 'Client', and 'Disabled'. The 'Disabled' option is selected and highlighted with a red box. An 'Advanced' button is located to the right of the DHCP Mode options.

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 Avaya SBCE. 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/TCP** with port **5060** and **TLS** with port **5061**. 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.

Configuration

- BOOTP (3)
- Operator (3)
- Solution
 - User(4)
 - Group(0)
 - Short Code(44)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(0)
- 000C292B2485
 - System (1)
 - 000C292B2485
 - Line (2)
 - Control Unit (11)
 - Extension (2)
 - User (3)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (4)
 - IP Route (1)
 - License (39)

000C292B2485

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | VoIP | VoIP Security

LAN Settings | VoIP | Network Topology

☒ H.323 Gatekeeper Enable

☐ Auto-create Extension ☐ Auto-create User ☐ H.323 Remote Extension Enable

H.323 Signaling over TLS: Disabled Remote Call Signaling Port: 1720

☒ SIP Trunks Enable

☒ SIP Registrar Enable

☐ Auto-create Extension/User ☐ SIP Remote Extension Enable

SIP Domain Name: sipinterop.net

SIP Registrar FQDN:

Layer 4 Protocol:

- ☒ UDP UDP Port: 5060 Remote UDP Port: 5060
- ☒ TCP TCP Port: 5060 Remote TCP Port: 5060
- ☒ TLS TLS Port: 5061 Remote TLS Port: 5061

Configuration

- BOOTP (3)
- Operator (3)
- Solution
 - User(4)
 - Group(0)
 - Short Code(44)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(0)
- 000C292B2485
 - System (1)
 - 000C292B2485
 - Line (2)
 - Control Unit (11)
 - Extension (2)
 - User (3)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (4)
 - IP Route (1)

000C292B2485

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR

LAN Settings | VoIP | Network Topology

RTP

Port Number Range

Minimum: 40750 Maximum: 50750

Port Number Range (NAT)

Minimum: 40750 Maximum: 50750

☒ Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones: 0 . 0 . 0 . 0

Keepalives

Scope: Disabled Periodic timeout

Initial keepalives: Enabled

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 a software configuration window with a tabbed interface. The tabs at the top are: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VCM, VoIP, and VoIP Security. The 'Network Topology' tab is selected. Below the tabs, there are sub-tabs: LAN Settings, VoIP, and Network Topology. The 'Network Topology' sub-tab is active, showing a 'Network Topology Discovery' section. This section contains the following fields and controls:

- STUN Server Address:** A text box containing '0.0.0.0'.
- STUN Port:** A spin box set to '3478'.
- Firewall/NAT Type:** A dropdown menu currently showing 'Unknown'. This field is highlighted with a red rectangular border.
- Binding Refresh Time (sec):** A spin box set to '0'.
- Public IP Address:** A text box showing '0 . 0 . 0 . 0' with a red cursor at the end.
- Public Port:** A group box containing three spin boxes: 'UDP' (0), 'TCP' (0), and 'TLS' (0).
- Run STUN on startup:** A checkbox that is currently unchecked.
- Buttons:** 'Run STUN' and 'Cancel' buttons are located at the bottom right of the configuration area.

5.2 System Telephony Settings

Navigate to **System (1) > 000C292B2458** 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 displays the 'System Telephony Settings' configuration page for the system 000C292B2458. The page is divided into several sections:

- Analogue Extensions:** Includes settings for Default Outside Call Sequence (Normal), Default Inside Call Sequence (Ring Type 1), Default Ring Back Sequence (Ring Type 2), and Restrict Analogue Extension Ringer Voltage (unchecked).
- Dial Delay Settings:** Includes Dial Delay Time (sec) set to 4, Dial Delay Count set to 15, Default No Answer Time (sec) set to 15, Hold Timeout (sec) set to 0, Park Timeout (sec) set to 300, Ring Delay (sec) set to 5, and Call Priority Promotion Time (sec) set to Disabled.
- Companding Law:** A section with two columns: Switch and Line. Under Switch, U-Law is unchecked and A-Law is selected. Under Line, U-Law Line is unchecked and A-Law Line is selected.
- Other Settings:** Includes DSS Status (unchecked), Auto Hold (checked), Dial By Name (checked), Show Account Code (checked), Inhibit Off-Switch Forward/Transfer (unchecked), Restrict Network Interconnect (unchecked), and Include location specific information (unchecked).

Red boxes highlight the following areas:

- The 'Dial Delay Time (sec)' and 'Dial Delay Count' fields.
- The 'Companding Law' section.
- The 'Inhibit Off-Switch Forward/Transfer' checkbox.

5.3 System Codec Settings

Navigate to **System (1) > 000C292B2458** 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**.

The screenshot displays the configuration interface for the system 000C292B2458. The top navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and VoIP Security. The VoIP tab is active, showing the Codecs configuration. The RFC2833 Default Payload is set to 101. The Available Codecs list includes G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-ACELP. The Default Codec Selection section shows an Unused list and a Selected list containing G.711 ALAW 64K, G.711 ULAW 64K, and G.729(a) 8K CS-ACELP.

Available Codecs	Default Codec Selection
<input checked="" type="checkbox"/> G.711 ULAW 64K <input checked="" type="checkbox"/> G.711 ALAW 64K <input type="checkbox"/> G.722 64K <input checked="" type="checkbox"/> G.729(a) 8K CS-ACELP	<div>Unused</div> <div>Selected</div> <div>G.711 ALAW 64K G.711 ULAW 64K G.729(a) 8K CS-ACELP</div>

5.4 Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and OneAccess-Telstra Business SIP. 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 **2** 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**.
- Under **Session Timers**:
 - **Refresh Method**: Select **Update**.
 - **Timer (sec)**: Enter **90**.
- Set **Country Code** to **61** (Country Code of Australia).
- Set **National Prefix** to **0**.
- Set **Incoming Supervised REFER** to **Never**.
- Set **Outgoing Supervised REFER** to **Never**.

SIP Line - Line 2	
SIP Line Transport SIP URI VoIP SIP Credentials SIP Advanced Engineering	
Line Number	2
ITSP Domain Name	192.168.109.1
Local Domain Name	sipinterop.net
URI Type	SIP
Location	Cloud
Prefix	
National Prefix	0
International Prefix	
Country Code	61
Name Priority	System Default
Description	
In Service	<input checked="" type="checkbox"/>
Check OOS	<input checked="" type="checkbox"/>
Session Timers	
Refresh Method	Update
Timer (sec)	90
Redirect and Transfer	
Incoming Supervised REFER	Never
Outgoing Supervised REFER	Never
Send 302 Moved Temporarily	<input type="checkbox"/>
Outgoing Blind REFER	<input type="checkbox"/>

Select the **Transport** tab:

- The **ITSP Proxy Address** is set to the IP address of Avaya SBCE A1 Interface. As shown in **Figure 1**, this IP address is **10.1.20.9**.
- In the **Network Configuration** area, **TLS** is selected as the Layer 4 Protocol, and the **Send Port** is set to **5061**. The **Use Network Topology Info** parameter is set to **None**. Other parameters retain default values in the screen below.
- Check **Calls Route via Registrar**.

SIP Line	Transport	SIP URI	VoIP	SIP Credentials	SIP Advanced	Engineering
ITSP Proxy Address 10.1.20.9						
Network Configuration						
Layer 4 Protocol		TLS		Send Port		5061
Use Network Topology Info		None		Listen Port		5061
Explicit DNS Server(s)		0 . 0 . 0 . 0		0 . 0 . 0 . 0		
Calls Route via Registrar		<input checked="" type="checkbox"/>				
Separate 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 **2** was defined that only contains this line (line 2).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

SIP Line	Transport	SIP URI	VoIP	SIP Credentials	SIP Advanced	Engineering
Edit URI						
Local URI	Use Internal Data ▼					
Contact	Use Internal Data ▼					
Display Name	Use Internal Data ▼					
Identity						
Identity	Use Internal Data ▼					
Header	P Asserted ID ▼					
Forwarding And Twinning						
Originator Number	<input type="text"/>					
Send Caller ID	Diversion Header ▼					
Diversion Header	None ▼					
Registration	0: <None> ▼					
Incoming Group	2 ▼					
Outgoing Group	2 ▼					
Max Sessions	10 ▲▼					

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 ALAW 64K**, **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** codecs causes Avaya IP Office to include these codecs.
- 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/RFC4733** from the pull-down menu.
- Default values may be used for all other parameters.

SIP Line - Line 2*

SIP Line | Transport | SIP URI | **VoIP** | SIP Credentials | SIP Advanced | Engineering

Codec Selection: Custom

Unused

Selected

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

Local Hold Music

☒ Re-invite Supported

☐ Codec Lockdown

☐ Allow Direct Media Path

☐ Force direct media with phones

☐ PRACK/100rel Supported

Fax Transport Support: G.711

DTMF Support: RFC2833/RFC4733

Media Security: Disabled

Select **SIP Advanced** tab:

- Check **Indicate HOLD** box.

The screenshot shows the 'SIP Line - Line 2' configuration window with the 'SIP Advanced' tab selected. The window is divided into several sections: Addressing, Identity, Media, and Call Control. In the 'Media' section, the 'Indicate HOLD' checkbox is checked and highlighted with a red rectangle. Other settings include 'Association Method' set to 'By Source IP address', 'Call Routing Method' set to 'Request URI', and 'Suppress DNS SRV Lookups' unchecked. The 'Identity' section has 'Cache Auth Credentials' checked. The 'Call Control' section has 'Call Initiation Timeout (s)' set to 4, 'Call Queuing Timeout (mins)' set to 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', and 'Action on CAC Location Limit' set to 'Allow Voicemail'.

Section	Setting	Value
Addressing	Association Method	By Source IP address
	Call Routing Method	Request URI
	Suppress DNS SRV Lookups	<input type="checkbox"/>
Identity	Use "phone-context"	<input type="checkbox"/>
	Add user=phone	<input type="checkbox"/>
	Use + for International	<input type="checkbox"/>
	Use PAI for Privacy	<input type="checkbox"/>
	Use Domain for PAI	<input type="checkbox"/>
	Swap From and PAI/Diversion	<input type="checkbox"/>
	Caller ID from From header	<input type="checkbox"/>
	Send From In Clear	<input type="checkbox"/>
	Cache Auth Credentials	<input checked="" type="checkbox"/>
	User-Agent and Server Headers	
Send Location Info	Never	
Add UUI header	<input type="checkbox"/>	
Add UUI header to redirected calls	<input type="checkbox"/>	
Media	Allow Empty INVITE	<input type="checkbox"/>
	Send Empty re-INVITE	<input type="checkbox"/>
	Allow To Tag Change	<input type="checkbox"/>
	P-Early-Media Support	None
	Send SilenceSup=Off	<input type="checkbox"/>
	Force Early Direct Media	<input type="checkbox"/>
Media Connection Preservation	Disabled	
Indicate HOLD	<input checked="" type="checkbox"/>	
Call Control	Call Initiation Timeout (s)	4
	Call Queuing Timeout (mins)	5
	Service Busy Response	486 - Busy Here
	on No User Responding Send	408-Request Timeout
	Action on CAC Location Limit	Allow Voicemail
	Suppress Q.850 Reason Header	<input type="checkbox"/>
	Emulate NOTIFY for REFER	<input type="checkbox"/>
	No REFER if using Diversion	<input type="checkbox"/>

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)**.

Short Code	
Code	?
Feature	Dial
Telephone Number	.
Line Group ID	50: Main
Locale	Australia (UK English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

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.

ARS

ARS Route ID

50

Route Name

Main

Dial Delay Time

10

Description

In Service

☒

Out of Service Route

<None>

Time Profile

<None>

Out of Hours Route

<None>

Secondary Dial tone

SystemTone

☒ Check User Call Barring

Code	Telephone Number	Feature	Line Group ID
?	.	Dial	2

Add...

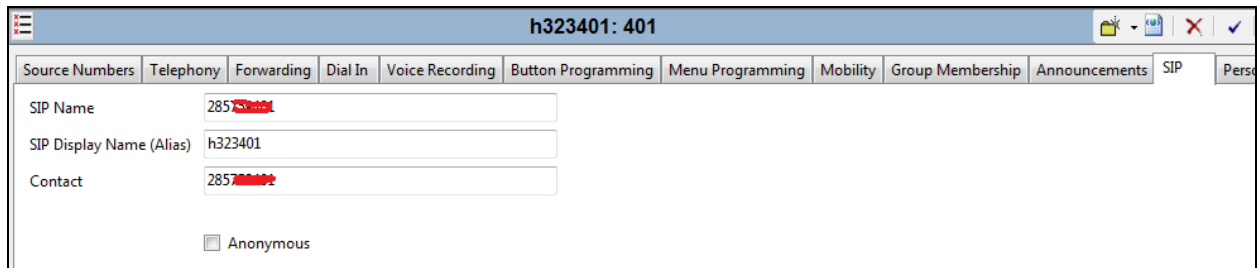
Remove

Edit...

5.7 User

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

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 a web-based configuration interface for a user identified as 'h323401: 401'. The interface has a top navigation bar with various tabs: Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, Button Programming, Menu Programming, Mobility, Group Membership, Announcements, SIP (selected), and Personal. Below the tabs, there are three input fields: 'SIP Name' with the value '2857XXXX', 'SIP Display Name (Alias)' with the value 'h323401', and 'Contact' with the value '2857XXXX'. At the bottom, there is a checkbox labeled 'Anonymous' which is currently unchecked.

Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership	Announcements	SIP	Personal
h323401: 401											
SIP Name: 2857XXXX											
SIP Display Name (Alias): h323401											
Contact: 2857XXXX											
<input type="checkbox"/> Anonymous											

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 028 have been masked as 285xxx4xx due to security reasons.


Standard	Voice Recording	Destinations
Bearer Capacity	Any Voice	
Line Group ID	2	
Incoming Number	285xxx4xx	
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 **0285xxx4xx** on line 2 are routed to extension 3xx.

Standard	Voice Recording	Destinations
	TimeProfile	Destination
▶	Default Value	4xx

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.

Select	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
▶	<input checked="" type="checkbox"/> 000C292B2485	Merge	9:34 AM	<input type="checkbox"/>	<input type="checkbox"/>		0%

OK Cancel 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.

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the enterprise site, (10.1.20.9), with access to the IP Office network. The connection to OneAccess-Telstra Business SIP uses the Avaya SBCE public interface B1 (192.168.109.50). 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**.



The screenshot shows the Avaya Session Border Controller for Enterprise login page. The Avaya logo is in the top left. The title "Session Border Controller for Enterprise" is on the left. On the right, under "Log In", there is a "Username:" label and an input field. Below the input field is a "Continue" button. To the right of the input field, there is a block of legal disclaimer text. At the bottom right, there is a copyright notice: "© 2011 - 2013 Avaya Inc. All rights reserved."

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



The screenshot shows the Avaya Session Border Controller for Enterprise login page, similar to the previous one, but with an additional "Password:" label and an input field below the "Username" field. Below the password input field is a "Log In" button. The rest of the page, including the Avaya logo, title, disclaimer text, and copyright notice, remains the same.

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.

[Alarms](#) [Incidents](#) [Status ▾](#) [Logs ▾](#) [Diagnostics](#) [Users](#)

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- Device Specific Settings

Dashboard

Information		
System Time	06:59:11 PM AEDT	Refresh
Version	7.2.1.0-05-14222	
Build Date	Tue Oct 31 00:06:46 UTC 2017	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	12/11/2017 21:37:33 AEDT	
Failed Login Attempts	1	

Installed Devices

EMS
sbce

6.1 System Management – Status

1. Select **System Management** and verify that the **Status** column says **Commissioned** (not shown).
2. Click on **View** (not shown) to display the **System Information** screen.

System Information: sbce

General Configuration

Appliance Name

sbce

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 100

100

Advanced Sessions

Requested: 100

100

Scopia Video Sessions

Requested: 100

100

CES Sessions

Requested: 100

100

Transcoding Sessions

Requested: 100

100

Encryption

☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.1.20.9	10.1.20.9	255.255.255.0	10.1.20.1	A1
10.239.192.234	10.239.192.234	255.255.255.248	10.239.192.233	B1

DNS Configuration

Primary DNS

10.1.20.3

Secondary DNS

DNS Location

DMZ

DNS Client IP

10.1.20.9

Management IP(s)

IP #1 (IPv4)

10.1.20.8

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 – Avaya

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., **Avaya** (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 'T38 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 RFC3284 - a=sendonly.
- 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 RFC3281 (selected) and RFC2543.

Buttons at the bottom: Back, 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**

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 – OneAccess

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

1. Click **Add** to add a new profile, enter **OneAccess** then click **Next** (not shown)
2. The **General** screen will open: Configure the same as shown in **Section 6.2.2**.
 - Click **Next**.
 - 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 the 'Interworking Profile' configuration window with the 'General' tab selected. The settings are as follows:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input checked="" type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

At the bottom, there are 'Back' and 'Next' buttons. The 'Next' button is highlighted with a red box.

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

Interworking Profile X

Record Routes

- ☒ None
- ☐ Single Side
- ☐ Both Sides
- ☐ Dialog-Initiate Only (Single Side)
- ☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☐

Extensions None ▾

Diversion Manipulation ☐

Diversion Condition None ▾

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

DTMF

DTMF Support

- ☒ None
- ☐ SIP Notify
- ☐ SIP Info
- ☐ Inband

Back **Finish**

6.2.4 Signaling Manipulation – OneAccess

As OneAccess SIP NTU requires User-Agent header in the SIP messages sent to it, a Sigma script must be used on Avaya SBCE to insert User-Agent header into SIP messages before Avaya SBCE sends those messages to OneAccess SIP NTU.

1. Navigate to **Global Profiles > Signaling Manipulation** from the left-hand menu.
2. Click on **Add** button to add a Sigma script as shown below.

Signaling Manipulation Scripts: OneAccess

Upload Add

Signaling Manipulation Scripts

OneAccess

Click here to add a description

Signaling Manipulation

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["User-Agent"][1] = "Avaya-SBC-v7.2.1";
  }
}
```

Edit

Text version of the script:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["User-Agent"][1] = "Avaya-SBC-v7.2.1";
  }
}
```

6.2.5 Server Configuration – Avaya

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., **Avaya**) and click **Next** (not shown).
3. The **Add Server Configuration Profile** window will open.
 - Select **Server Type: Call Server**.
 - **SIP Domain:** Leave blank.
 - **IP Address / FQDN: 10.1.20.14** (IP Office LAN1 IP Address)
 - **Transport:** Select **TLS**.
 - **Port: 5061**
 - **TLS Client Profile:** Select **ClientA1**. Certificates and TLS profiles configuration is out of scope of this Application Notes.
 - Select **Next** (not shown).

Edit Server Configuration Profile - General X

Server Type: Call Server

SIP Domain:

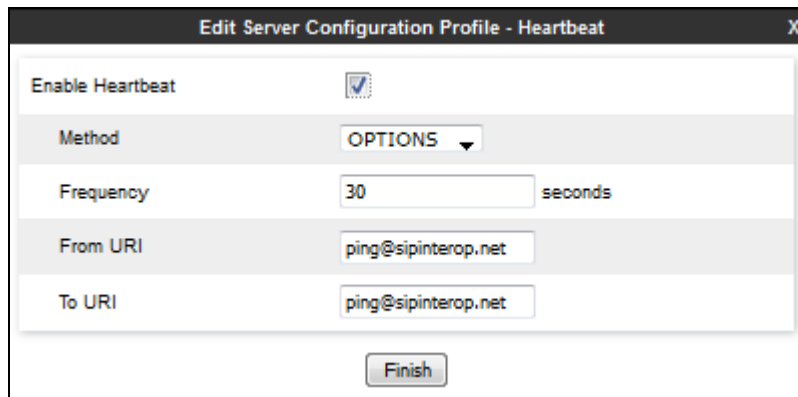
TLS Client Profile: ClientA1

Add

IP Address / FQDN	Port	Transport	
10.1.20.14	5061	TLS	Delete

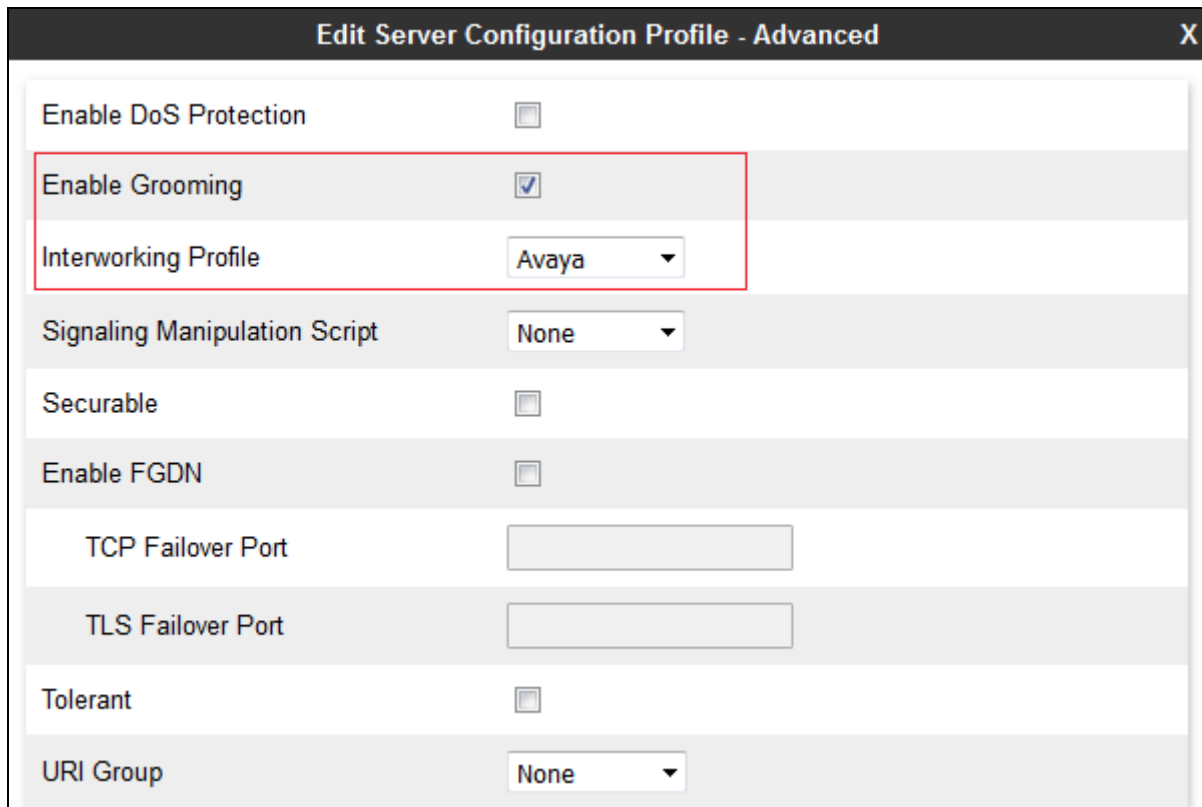
Back Next

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
<button>Finish</button>	

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



Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None

6.2.6 Server Configuration – OneAccess

Repeat the steps in **Section 6.2.5**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to OneAccess-Telstra Business SIP network.

1. Select **Add Profile** and enter a Profile Name (e.g., **OneAccess**) and click on **Next** (not shown).
2. On the **Edit Server Configuration Profile - General** window, enter the following.
 - Select **Server Type: Trunk Server**.
 - **SIP Domain:** Leave blank.
 - **IP Address / FQDN: 192.168.109.1** (OneAccess SIP NTU IP address).
 - **Transport:** Select **UDP**.
 - **Port: 5062**.
 - Click on **Next**.

Edit Server Configuration Profile - General X

Server Type: Trunk Server

SIP Domain:

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport	
192.168.109.1	5062	UDP	Delete

Back Next

3. On the **Edit Server Configuration Profile – Authentication** window, enter the following.
 - Select **Enable Authentication**.
 - Enter trunk Pilot number into **User Name**.
 - Enter assigned password into **Password** and **Confirm Password**.

Edit Server Configuration Profile - Authentication X

Enable Authentication ☒

User Name 2857 [redacted]

Realm
(Leave blank to detect from server challenge)

Password
(Leave blank to keep existing password)

Confirm Password

Finish

4. On the **Edit Server Configuration Profile – Heartbeat** window, enter the following.
- Select **Enable Heartbeat**.
 - **Method**: Select **REGISTER**.
 - **Frequency**: Enter desired number. In the compliance test, 600 was used.
 - **From URI** and **To URI**: Enter trunk pilot number provided, such as 285xxx4xx@192.168.109.50.

Edit Server Configuration Profile - Heartbeat X

Enable Heartbeat ☒

Method REGISTER ▾

Frequency 600 seconds

From URI 28571400@192.168.109.50

To URI 28571400@192.168.109.50

Finish

5. On the **Edit Server Configuration Profile – Advanced** window, enter the following.
- **Interworking Profile:** Select **OneAccess** created in **Section 6.2.3**.
 - **Signaling Manipulation Script:** Select **OneAccess** created in **Section 6.2.4**.

Add Server Configuration Profile - Advanced X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	OneAccess ▼
Signaling Manipulation Script	OneAccess ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None ▼

6.2.7 Routing – To Avaya

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., **Avaya**) 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 = Avaya**
 - **Next Hop Address**: Verify that the **10.1.20.14:5061 (TLS)** 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**.

The screenshot shows the 'Profile : Avaya - Edit Rule' window. The top section contains configuration options: URI Group (set to *), Time of Day (set to default), Load Balancing (set to Priority), Transport (set to None), Next Hop In-Dialog (checked), Ignore Route Header (unchecked), ENUM (unchecked), and ENUM Suffix (empty). An 'Add' button is located at the bottom right of this section. Below this is a table with four columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport. The first row contains the values: 1, Avaya, 10.1.20.14:5061 (TLS), and None. A 'Delete' button is next to the Transport field. At the bottom of the window is a 'Finish' button.

URI Group	Time of Day	Load Balancing	Transport	Next Hop In-Dialog	Ignore Route Header	ENUM	ENUM Suffix
*	default	Priority	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Avaya	10.1.20.14:5061 (TLS)	None	Delete

Finish

6.2.8 Routing – To OneAccess

Repeat the steps in **Section 6.2.7**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to OneAccess-Telstra Business SIP.

1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **OneAccess**).
2. On the **Routing Profile** window, populate the following fields:
 - **Server Configuration: OneAccess.**
 - **Next Hop Address:** Verify that the **192.168.109.1:5062 (UDP)** entry from the drop down menu is selected.
3. Click on **Finish**.

The screenshot shows the 'Profile : OneAccess - Edit Rule' window. It contains several configuration fields and a table at the bottom.

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
ENUM	<input type="checkbox"/>	ENUM Suffix	

Buttons: Add, Finish

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	OneAccess	192.168.109.1:5062 (UDP)	None	Delete

6.2.9 Topology Hiding – Avaya

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. Navigate to **Global Profiles > Topology Hiding** from the left-hand side menu.
2. Click on **Add** button (not shown), enter **Profile Name:** (e.g., **Avaya**), and click **Next** (not shown).
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button (not shown) repeatedly to add headers. Note that the **Overwrite Value** is **sipinterop.net**.
4. Populate the fields as shown below, and click on **Finish** (not shown).

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Overwrite	sipinterop.net
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	sipinterop.net
Request-Line	IP/Domain	Overwrite	sipinterop.net
From	IP/Domain	Overwrite	sipinterop.net
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

Edit

6.2.10 Topology Hiding – OneAccess

Repeat the steps in **Section 6.2.10**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to OneAccess-Telstra Business SIP.

1. Enter a **Profile Name**: (e.g., **OneAccess**).
2. Click on the **Add Header** button (not shown) repeatedly to add headers.
3. Populate the fields as shown below, and click on **Finish** (not shown). Note that the **Overwrite Value** is **192.168.109.1**.

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	192.168.109.1
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	192.168.109.1
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	192.168.109.1
Record-Route	IP/Domain	Auto	---
<div>Edit</div>			

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 default rule was used.

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 rules specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses. In the solution as tested, the **default** rule was utilized. No customization was required.

6.3.3 Media Rules

The Media rules will be applied to both directions. In the solution as tested, the **default-low-med** rule was utilized. No customization was required.

6.3.4 Signaling Rules

Signaling rules are a mechanism on the Avaya SBCE to manipulate the signaling beyond simple header manipulation. Signaling rules allow action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. In the solution as tested, the **default** rule was used.

6.3.5 Endpoint Policy Groups

In the solution as tested, the **default-low** rule was used. This rule incorporated the 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.
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.

Network Management: sbce

Devices
sbce

Interfaces

Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1	10.1.20.1	255.255.255.0	A1	10.1.20.9	Edit Delete
B1	192.168.109.1	255.255.255.0	B1	192.168.109.50	Edit Delete

6.4.2 Media Interfaces

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name:** Med_A1.
 - **IP Address:** 10.1.20.9 (Avaya SBCE A1 address).
 - **Port Range:** 35000-40000.
4. Click on **Finish** (not shown).
5. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name:** Med_B1.
 - **IP Address:** 192.168.109.50 (Avaya SBCE B1 address).
 - **Port Range:** 35000-40000.
6. Click on **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.

Media Interface: sbce

Devices
sbce

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](#).

Add

Name	Media IP Network	Port Range	
Med_A1	10.1.20.9 A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Med_B1	192.168.109.50 B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

6.4.3 Signaling Interface

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Click on **Add** (not shown) and enter the following:
 - **Name: Sig_A1.**
 - **IP Address: 10.1.20.9** (Avaya SBCE A1 address).
 - **TCP/UDP Port: 5060.**
 - **TLS Port: 5061.**
 - **TLS Profile: ServerA1.** Certificates and TLS profiles configuration are out of scope of this Application Notes.
4. Click on **Finish** (not shown).
5. Click on **Add** again, and enter the following:
 - **Name: Sig_B1.**
 - **IP Address: 192.168.109.50** (Avaya SBCE B1 address).
 - **UDP Port: 5060.**
6. Click on **Finish** (not shown). Note that changes to these values require an application restart.

Signaling Interface: sbce

Devices
sbce

Signaling Interface

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

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_B1	192.168.109.50 B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete
Sig_A1	10.1.20.9 A1 (A1, VLAN 0)	5060	5060	5061	ServerA1	Edit Delete

6.4.4 Endpoint Flows – For Avaya

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:
 - **Flow Name: Avaya.**
 - **Server Configuration: Avaya.**
 - **URI Group: *.**
 - **Transport: *.**
 - **Remote Subnet: *.**
 - **Received Interface: Sig_B1.**
 - **Signaling Interface: Sig_A1.**
 - **Media Interface: Med_A1.**
 - **End Point Policy Group: default-low.**
 - **Routing Profile: OneAccess.**
 - **Topology Hiding Profile: Avaya.**
 - Let other values default.
4. Click **Finish**.

Edit Flow: Avaya

X

Flow Name	Avaya
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_B1
Signaling Interface	Sig_A1
Media Interface	Med_A1
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	OneAccess
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

6.4.5 Endpoint Flows – For OneAccess

Repeat step **1** through **4** from **Section 7.3.4**, with the following changes:

- **Flow Name:** OneAccess.
- **Server Configuration:** OneAccess.
- **Received Interface:** Sig_A1.
- **Signaling Interface:** Sig_B1.
- **Media Interface:** Med_B1.
- **Endpoint Policy Groups:** default-low.
- **Routing Profile:** Avaya.
- **Topology Hiding Profile:** OneAccess.

Edit Flow: OneAccessX

Flow Name	OneAccess
Server Configuration	OneAccess
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_A1
Signaling Interface	Sig_B1
Media Interface	Med_B1
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	OneAccess
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., **B1**).
 - Specify the **Maximum Number of Packets to Capture** (e.g., **3000**).
 - 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.

Trace: sbce

Devices
sbce

Packet Capture

Captures

Packet Capture Configuration

StatusReady

InterfaceB1

Local Address
IP:Port192.168.109.90

Remote Address
*, *.Port, IP, IP:Port*

ProtocolAll

Maximum Number of Packets to Capture3000

Capture Filename
Using the name of an existing capture will overwrite it.test.pcap

Start Capture

Clear

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

Trace: sbce

Devices
sbce

Packet Capture

Captures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

Status	In Progress
Interface	B1
Local Address <small>(IP, Port)</small>	10.2.2.135 : <input type="text"/>
Remote Address <small>(IP, Port)</small>	<input type="text"/>
Protocol	All
Maximum Number of Packets to Capture	3000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	test.pcap

Stop Capture

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	
test_20160405184126.pcap	0	April 5, 2016 6:41:26 PM AEST	Delete

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 OneAccess-Telstra Business SIP 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 OneAccess-Telstra Business SIP network gateway.
- Ping from the SBC to the IPO.
- Ping from the OneAccess-Telstra Business SIP network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.

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)	Error: Unable to reach 10.1.20.1 from 10.1.20.9 [A1].
✓ Ping: SBC (A1) to Primary DNS (10.1.20.3)	Average ping from 10.1.20.9 [A1] to 10.1.20.3 is 0.492ms.
✓ Ping: SBC (B1) to Gateway (192.168.109.1)	Average ping from 192.168.109.50 [B1] to 192.168.109.1 is 1.385ms.
🔄 Ping: SBC (B1) to Primary DNS (10.1.20.3)	Running...

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: 2** (the SIP line configured on IP Office for SIP trunking):

The screenshot displays the Avaya IP Office System Status web application. The title bar indicates the system is at 10.1.20.14. The main header shows the Avaya logo and the title "IP Office System Status". A navigation menu on the left includes System, Alarms (5), Extensions (0), Trunks (2), and a sub-menu for Line: 2, which is currently selected. The main content area shows the "SIP Trunk Summary" for Line 2, with tabs for Status, Utilization Summary, and Alarms. The summary includes the following details:

- Line Service State: In Service
- Peer Domain Name: 192.168.109.1
- Resolved Address: 10.1.20.9
- Line Number: 2
- Number of Administered Channels: 10
- Number of Channels in Use: 0
- Administered Compression: G711 A, G711 Mu, G729 A
- Enable Faststart: Off
- Silence Suppression: Off
- Media Stream: RTP
- Layer 4 Protocol: TLS
- SIP Trunk Channel Licenses: 10
- SIP Trunk Channel Licenses in Use: 0
- SIP Device Features: UPDATE (Incoming and Outgoing)

A green circular progress indicator shows 0% utilization. Below the summary is a table with columns for Channel, U., Call, Curr..., Time, Remote C..., Con..., Caller, Other, Dire..., Rou..., Rec..., Rec..., Tra..., and Tra... The first row shows a channel in an "Idle" state with a "Round Trip Delay". At the bottom of the interface, there are buttons for Trace, Trace All, Pause, Ping, Call Details, Graceful Shutdown, Force Out of Service, Print..., and Save As... The status bar at the bottom right shows the time as 1:08:33 AM and the system as "Online".

8. 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.

9. Conclusion

As illustrated in these Application Notes, Avaya IP Office Release 10.1 and Avaya Session Border Control for Enterprise Release 7.2.1 can be configured to interoperate successfully with OneAccess-Telstra Business SIP. This solution allows enterprise users access to the PSTN using the OneAccess-Telstra Business SIP. Please refer to **Section 2.2** for exceptions.

10. 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 7.2.1.
- [2] *Deploying Avaya Session Border Controller*, Release 7.2.1.
- [3] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.2.1.
- [4] *Administering Avaya Session Border Controller*, Release 7.2.1.
- [5] *Deploying IP Office Server Edition Solution*, Release 10.1.
- [6] *Deploying IP Office IP500 V2*, Release 10.1.
- [7] *Administering Avaya IP Office with Manager*, Release 10.1.
- [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 OneAccess-Telstra Business SIP is available from Telstra.

©2018 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.