



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring Avaya IP Office Release 10.1 and Avaya Session Border Controller for Enterprise Release 7.2 to support Frontier Communications SIP Trunking Service - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 10.1 and Avaya Session Border Controller for Enterprise Release 7.2 to support Frontier Communications SIP Trunking Service.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

Frontier Communications SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Frontier Communications network as an alternative to legacy analog or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

## Table of Contents

1. Introduction.....	4
2. General Test Approach and Test Results.....	4
2.1 Interoperability Compliance Testing .....	5
2.2 Test Results .....	6
2.3 Support.....	6
3. Reference Configuration .....	7
4. Equipment and Software Validated .....	10
5. Configure IP Office .....	11
5.1 Licensing.....	12
5.2 System.....	12
5.2.1 System - LAN1 Tab .....	12
5.2.2 System - Telephony Tab .....	16
5.2.3 System - VoIP Tab .....	17
5.2.4 System – VoIP Security Tab.....	18
5.3 IP Route .....	19
5.4 SIP Line .....	20
5.4.1 Creating a SIP Trunk from an XML Template .....	20
5.4.2 SIP Line - SIP Line Tab .....	23
5.4.3 SIP Line - Transport Tab .....	24
5.4.4 SIP Line - SIP URI Tab .....	25
5.4.5 SIP Line - VoIP Tab .....	26
5.4.6 SIP Line – T38 Fax Tab .....	27
5.4.7 SIP Line – SIP Advanced Tab .....	28
5.4.8 SIP Line – SIP Engineering Tab .....	29
5.5 Extension.....	30
5.6 Users .....	32
5.7 Incoming Call Route .....	37
5.7.1 Incoming Call Route – Standard Tab.....	37
5.7.2 Incoming Call Route – Destinations Tab .....	38
5.8 Outbound Call Routing .....	39
5.8.1 Short Codes and Automatic Route Selection.....	39
5.9 Save Configuration .....	42
6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).....	43
6.1 Log in Avaya SBCE.....	43
6.2 TLS Management.....	46
6.3 Global Profiles .....	46
6.3.1 Server Interworking – Avaya-IPO .....	46
6.3.2 Server Interworking - SP-General.....	50
6.3.3 Server Configuration.....	54
6.3.4 Routing Profiles .....	61
6.3.5 Topology Hiding.....	64
6.4 Domain Policies .....	67
6.4.1 Application Rules.....	67
6.4.2 Media Rules .....	69

6.4.3 End Point Policy Groups.....	72
6.5 Device Specific Settings .....	76
6.5.1 Network Management.....	76
6.5.2 Media Interface .....	77
6.5.3 Signaling Interface .....	79
6.5.4 End Point Flows .....	82
7. Frontier Communications SIP Trunking Service Configuration .....	86
8. Verification and Troubleshooting .....	87
8.1 Verification Steps.....	87
8.2 Protocol Traces .....	87
8.3 IP Office System Status .....	88
8.4 IP Office Monitor.....	91
8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE) .....	92
9. Conclusion .....	97
10. References.....	98

# 1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Frontier Communications and an Avaya SIP-enabled enterprise solution.

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500 V2 Release 10.1 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 7.2 (hereafter referred to as Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Frontier Communications SIP Trunking service referenced within these Application Notes is designed for business customers. Customers using this service with the Avaya IP Office solution are able to place and receive PSTN calls via a broadband WAN connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

The terms “service provider”, “Frontier Communications” or “Frontier” will be used interchangeably throughout these Application Notes.

## 2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by connecting IP Office and the Avaya SBCE to the Frontier Communications SIP Trunking service via the public Internet, as depicted in **Figure 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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). 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

To verify the Frontier Communications SIP Trunking service offering with Avaya IP Office and the Avaya SBCE, the following features and functionalities were exercised during the compliance testing:

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, digital, and analog endpoints at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP, H.323, digital, and analog endpoints at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya Communicator for Windows.
- Incoming and outgoing PSTN calls to/from Avaya Communicator for Web.
- Dialing plans including local calls, outbound toll-free, etc.
- Caller ID presentation.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two way speech-path. Testing was performed with codecs: G.711MU and G.729A, Frontier's preferred codec order.
- Proper response to no matching codecs.
- T.38 and G711 pass-through fax.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.

**Note:** Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

Items not supported or not tested included the following:

- The SIP REFER method for call redirection is not fully supported by Frontier, therefore it was not tested.

- Inbound toll free calls was not tested.
- 0, 0+10 digits, 411 Directory Assistance, 911 Emergency and international calls are supported by Frontier but were not tested.

## 2.2 Test Results

Interoperability testing of Frontier Communications SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **T.38 Fax:** Frontier does not support the method in which IP Office negotiates the use of T.38 for fax, which consist of IP Office sending a re-INVITE message with two media lines in the SDP, with the first media line set for audio, with the port set to 0, and the second media line set for T.38, with a valid port number, thus de-activating audio transmission for the call. To solve this issue, a SIP Line Custom String (SLIC) was added to the IP Office configuration used during the testing, as shown in **Section 5.4.8**. With the configuration shown in **Section 5.4.8**, IP Office will reverse the order of media line entries in the SDP, so that the active T.38 media line entry appears first, followed by the inactive audio media line entry, with the port set to 0. Although the re-INVITE message to use T.38 for fax was recognize by Frontier after this change was made, at the time of the testing, Frontier responded to the re-INVITE message sent by Avaya IP Office with "488 Not Acceptable Here", this resulted in the fax defaulting to G.711 pass-through. IP Office was configured to use T.38 on the first attempt, and G.711 pass-through if T.38 failed (refer to **Section 5.4.5**). Outbound G.711 pass-through fax was successfully tested, inbound G.711 pass-through fax failed. G.711 pass-through fax is supported by frontier, but due to the unpredictability of pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay, G.711 fax pass-through is delivered on a "best effort" basis; its success is not guaranteed, and it should be used at the customer's discretion.
- **Incorrect Call Display on call transfers to the PSTN Phone:** Call display was not properly updated on PSTN phone involved in a call transfer. After the call transfer was completed to the PSTN, the PSTN phone did not display the actual connected party, instead the DID number assigned to the IP Office station that initiated the transfer was displayed.
- **Outbound call from an enterprise extension to a busy PSTN number:** Frontier Communications did not send a "486 Busy Here" message on an outbound call to a PSTN number that was busy, as expected. There was no direct impact to the user, who heard busy tone.

## 2.3 Support

For support on Frontier Communications SIP Trunking service visit the corporate Web page at: <https://frontier.com/enterprise>

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

### 3. Reference Configuration

**Figure 1** illustrates the test configuration used. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Frontier Communications SIP Trunking service through the public Internet.

The Avaya components used to create the simulated enterprise customer site includes:

- Avaya IP Office 500v2.
- Avaya IP Office Application Server running Avaya Voicemail Pro, Avaya one-X® Portal for IP Office and Avaya WebRTC Gateway.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 1100 Series SIP IP Deskphones.
- Avaya 9508 Digital Deskphones.
- Analog Deskphones.
- Avaya Communicator for Windows softphone.
- Avaya Communicator for Web softphone.

Located at the edge of the enterprise is the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **B1** is used to connect to the public network, interface **A1** is used to connect to the private network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. The Avaya SBCE provides network address translation at both the IP and SIP layers.

Also located at the enterprise site is Avaya IP Office 500 V2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codec's. The IP Office **LAN1** interface connects to the inside (A1) interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE (B1) connects to Frontier Communications network via the public Internet.

For inbound calls, the calls flowed from the PSTN to Frontier Communications network to the Avaya SBCE, then to IP Office.

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk; the call was routed to the Avaya SBCE, across the public Internet, to Frontier Communications network.

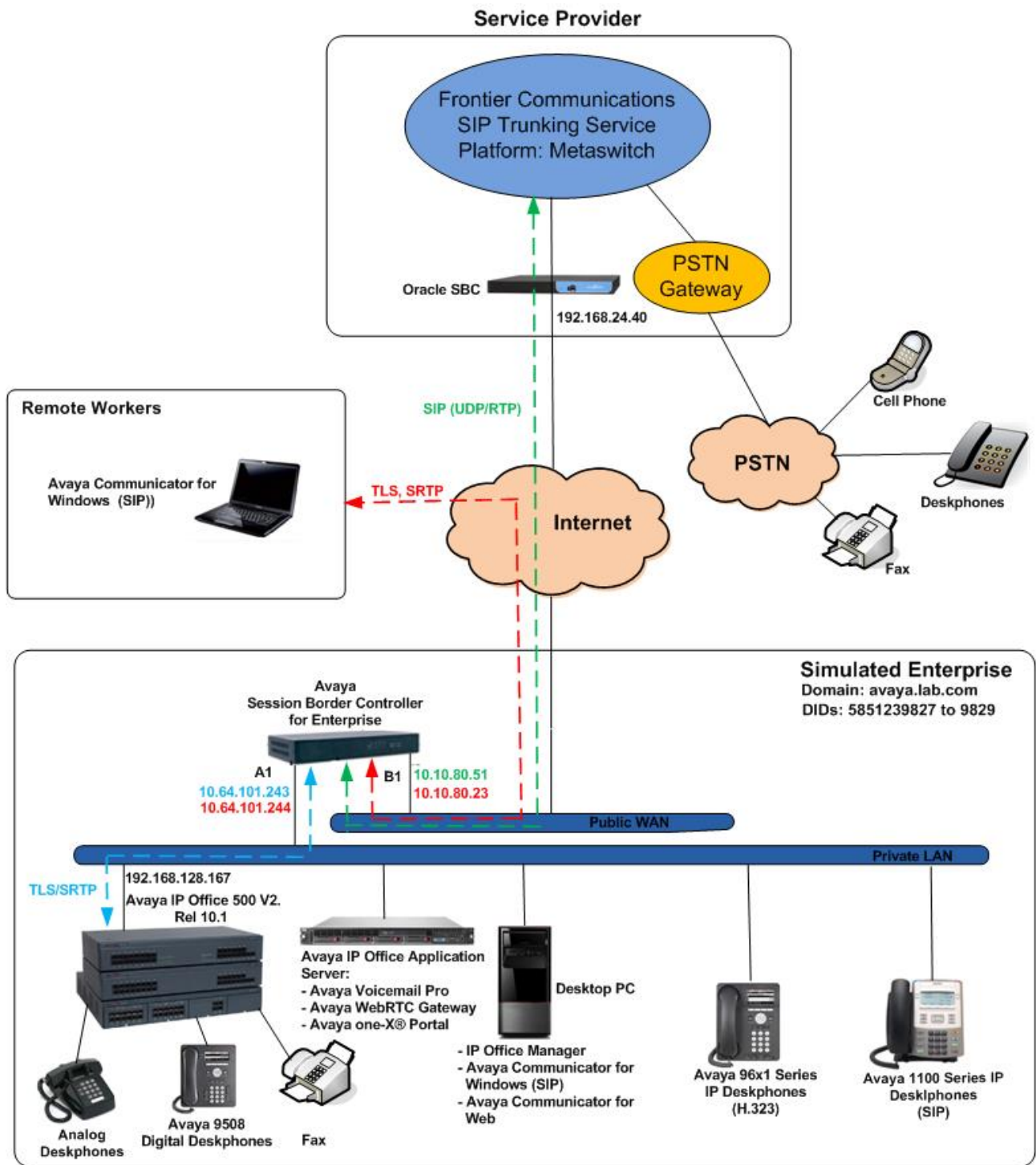
The transport protocol between the Avaya SBCE and Frontier Communications, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network (LAN), is SIP over TLS.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Frontier Communications. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network.

In an actual customer configuration, the enterprise site may also include additional network components between Frontier Communications and the enterprise. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and the enterprise must be allowed to pass through these devices.

For confidentiality and privacy purposes, actual public IP addresses and DID numbers used during the compliance test have been replaced with fictitious IP addresses and DID numbers throughout these Application Notes.





**Figure 1: Avaya Interoperability Test Lab Configuration.**

## 4. Equipment and Software Validated

The following equipment and software/firmware were used for the compliance testing.

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya IP Office 500v2	10.1.0.1.0 Build 3
Avaya IP Office DIG DCPx16 V2	10.1.0.1.0 Build 3
Avaya IP Office Manager	10.1.0.1.0 Build 3
Avaya IP Office Application Server	10.1.0.1.0 Build 3
▪ Voicemail Pro	10.1.0.1.0 build 6
▪ Avaya WebRTC Gateway	10.1.0.1.0 build 3
▪ Avaya one-X® Portal for IP Office	10.1.0.1.0 build 3
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.2.1.0-05-14222
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6506
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya Communicator for Windows	2.1.4.274
Avaya Communicator for Web	1.0.18.1124
Avaya Digital Deskphones 9508	R60
Lucent Analog Phone	--
<b>Frontier Communications</b>	
Metaswitch cCFS (Clustered Call Feature Server)	9.3.20
Oracle 3820 Session Border Controller	6.4

**Note:** Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500v2 and also when deployed with all configurations of IP Office Server Edition.

## 5. Configure IP Office

This section describes the IP Office configuration required to interwork with Frontier Communications SIP Trunking service. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. Navigate to **File → Open Configuration**, select the proper IP Office from the pop-up window, and log in with the appropriate credentials. A management window will appear as shown in the next sections. The appearance of IP Office Manager can be customized using the **View** menu (not shown). In the screenshots presented in this section, the **View** menu was configured to show the **Navigation Pane** on the left side and the **Details Pane** on the right side. These panes will be referenced throughout these Application Notes.

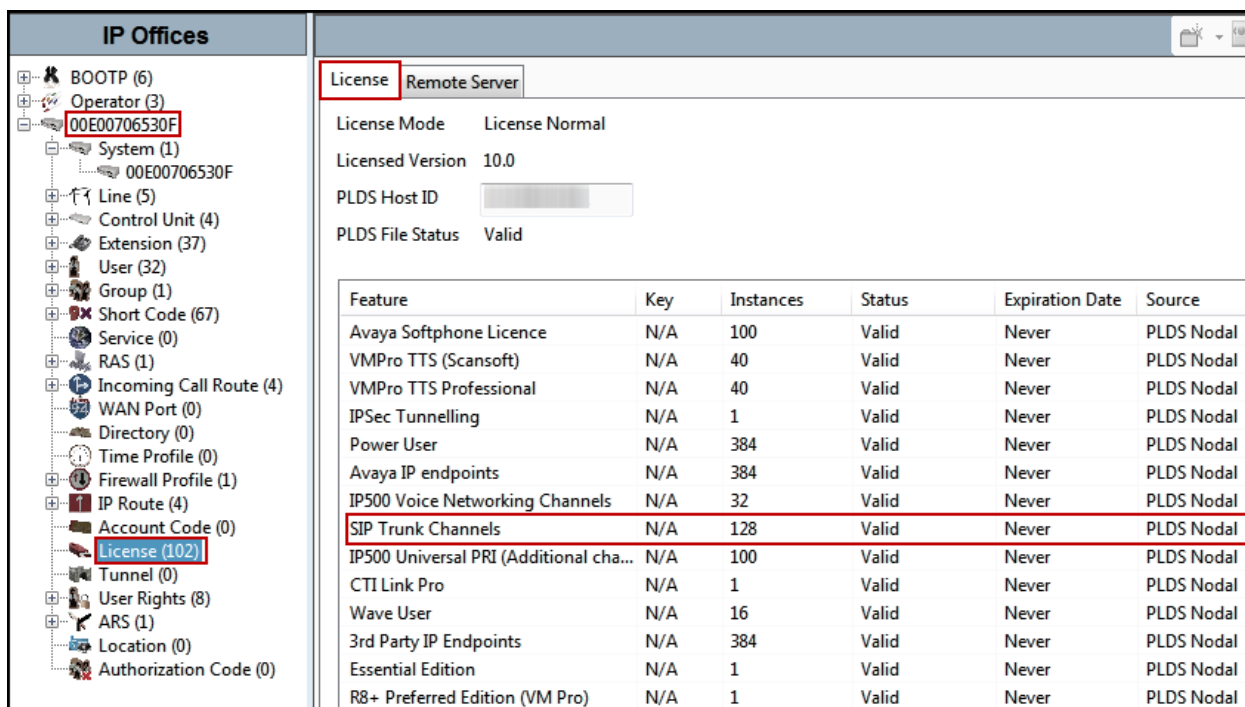
These Application Notes assume the basic installation and configuration of IP Office have already been completed and are not discussed here. For further information on IP Office, please consult

References in **Section 10**.

## 5.1 Licensing

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

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License**, then from the license tab, locate **SIP Trunk Channels**. Confirm that there is a valid license with sufficient “Instances” (trunk channels) in the Details pane. Note that the full License Keys in the screen below is not shown for security purposes.



The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree view shows a hierarchy starting with 'BOOTP (6)', followed by 'Operator (3)', 'System (1)', and '00E00706530F'. Under 'System (1)', 'License (102)' is selected. The right pane shows the 'License' tab with a table of installed licenses.

Feature	Key	Instances	Status	Expiration Date	Source
Avaya Softphone Licence	N/A	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	N/A	40	Valid	Never	PLDS Nodal
VMPro TTS Professional	N/A	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	N/A	1	Valid	Never	PLDS Nodal
Power User	N/A	384	Valid	Never	PLDS Nodal
Avaya IP endpoints	N/A	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	N/A	32	Valid	Never	PLDS Nodal
<b>SIP Trunk Channels</b>	N/A	<b>128</b>	<b>Valid</b>	<b>Never</b>	<b>PLDS Nodal</b>
IP500 Universal PRI (Additional cha...	N/A	100	Valid	Never	PLDS Nodal
CTI Link Pro	N/A	1	Valid	Never	PLDS Nodal
Wave User	N/A	16	Valid	Never	PLDS Nodal
3rd Party IP Endpoints	N/A	384	Valid	Never	PLDS Nodal
Essential Edition	N/A	1	Valid	Never	PLDS Nodal
R8+ Preferred Edition (VM Pro)	N/A	1	Valid	Never	PLDS Nodal

## 5.2 System

Configure the necessary system settings. In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to connect Avaya IP Office to the enterprise private network (LAN), **LAN2** was not used.

### 5.2.1 System - LAN1 Tab

In the sample configuration, the MAC address **00E00706530F** was used as the system name. The **LAN** port connects to the Avaya SBCE across the enterprise LAN (private) network. The **LAN1** settings correspond to the **LAN** port in IP Office. To access the **LAN1** settings, navigate to **System (1) → 00E00706530F** in the Navigation Pane, then in the Details Pane, navigate to the **LAN1 → LAN Settings** tab. The **LAN1** settings for the compliance testing were configured with following parameters:

- Set the **IP Address** field to the LAN IP address, e.g., **192.168.128.167**.
- Set the **IP Mask** field to the subnet mask of the private network, e.g., **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows the hierarchy for system 00E00706530F, with 'System (1)' selected. The main panel on the right shows the configuration for 'LAN1'. The 'LAN Settings' tab is active, and the 'IP Address' field is set to 192.168.128.167 and the 'IP Mask' field is set to 255.255.255.0. Other settings include 'Primary Trans. IP Address' (0.0.0.0), 'RIP Mode' (None), 'Enable NAT' (unchecked), 'Number Of DHCP IP Addresses' (200), and 'DHCP Mode' (Disabled). An 'Advanced' button is visible at the bottom right of the configuration area.

System: 00E00706530F	
System	LAN1
LAN Settings	
IP Address	192 . 168 . 128 . 167
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
<input type="checkbox"/> Enable NAT	
Number Of DHCP IP Addresses	200
DHCP Mode	
<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dial In <input checked="" type="radio"/> Disabled	
<button>Advanced</button>	

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

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Under **H.323 Signaling over TLS** select **Preferred**.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Frontier Communications.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- The **Domain Name** field was set with the Domain Name of the enterprise.
- Verify the **UDP Port**, **TCP Port** numbers under **Layer 4 Protocol** are set to **5060** and **TLS** port is set to **5061**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP-RTCP**, **Periodic Timeout** to **30**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP traffic is present.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

**IP Offices**

- BOOTP (6)
- Operator (3)
- 00E00706530F
  - System (1)
    - 00E00706530F
      - Line (5)
        - Control Unit (4)
        - Extension (37)
          - User (32)
          - Group (1)
          - Short Code (67)
          - Service (0)
          - RAS (1)
          - Incoming Call Route (4)
          - WAN Port (0)
          - Directory (0)
          - Time Profile (0)
          - Firewall Profile (1)
          - IP Route (4)
          - Account Code (0)
          - License (102)
          - Tunnel (0)
          - User Rights (8)
          - ARS (1)
          - Location (0)
          - Authorization Code (0)

**00E00706530F**

System **LAN1** LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR VCM 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 Preferred Remote Call Signaling Port 1720

☒ SIP Trunks Enable

☒ SIP Registrar Enable

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

SIP Domain Name avaya.lab.com

SIP Registrar FQDN avaya.lab.com

Layer 4 Protocol	<input checked="" type="checkbox"/> UDP	UDP Port	5060	Remote UDP Port	5060
	<input checked="" type="checkbox"/> TCP	TCP Port	5060	Remote TCP Port	5060
	<input checked="" type="checkbox"/> TLS	TLS Port	5061	Remote TLS Port	5061

Challenge Expiration Time (sec) 10

**RTP**

Port Number Range

Minimum 49152 Maximum 53246

Port Number Range (NAT)

Minimum 49152 Maximum 53246

☒ Enable RTCP Monitoring on Port 5005

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

**Keepalives**

Scope RTP-RTCP Periodic timeout 30

Initial keepalives Enabled

**Note:** In the compliance test, the LAN1 interface of was used to connect IP Office to the enterprise private network (LAN). The LAN2 interface was not used.

## 5.2.2 System - Telephony Tab

Navigate to the **Telephony** → **Telephony** Tab in the Details Pane, configure the following parameters:

- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya System Manager interface for system 00E00706530F. The left-hand pane shows a tree view of system components, with 'System (1)' selected. The main pane is the 'Telephony' configuration tab, which includes several sections:

- Analog Extensions:** Contains dropdowns for Default Outside Call Sequence (Normal), Default Inside Call Sequence (Ring Type 1), and Default Ring Back Sequence (Ring Type 2). It also has a checkbox for Restrict Analogue Extension Ringer Voltage.
- Dial Delay Time (sec):** Set to 3.
- Dial Delay Count:** Set to 0.
- Default No Answer Time (sec):** Set to 20.
- Hold Timeout (sec):** Set to 0.
- Park Timeout (sec):** Set to 300.
- Ring Delay (sec):** Set to 5.
- Call Priority Promotion Time (sec):** Set to Disabled.
- Default Currency:** Set to USD.
- Default Name Priority:** Set to Favor Trunk.
- Media Connection Preservation:** Set to Disabled.
- Phone Failback:** Set to Manual.
- Login Code Complexity:** Includes checkboxes for Enforcement (checked) and Complexity (checked), with a Minimum length of 6.
- RTCP Collector Configuration:** Includes a checkbox for Send RTCP to an RTCP Collector (unchecked), a Server Address field (0.0.0.0), a UDP Port Number field (5005), and an RTCP reporting interval (sec) field (5).
- Companding Law:** A section with two columns: Switch and Line. Under Switch, 'U-Law' is selected. Under Line, 'U-Law Line' is selected. There are also options for A-Law and A-Law Line.
- Other Settings:** Includes checkboxes for DSS Status, Auto Hold, Dial By Name, Show Account Code, Inhibit Off-Switch Forward/Transfer (unchecked), Restrict Network Interconnect, Include location specific information, Drop External Only Impromptu Conference, Visually Differentiate External Call, Unsupervised Analog Trunk Disconnect Handling, High Quality Conferencing, Digital/Analogue Auto Create User, Directory Overrides Barring, Advertise Callee State To Internal Callers, and Internal Ring on Transfer.



## 5.2.3 System - VoIP Tab

For **Codecs** settings, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **VoIP** tab and configure the following parameters:

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For **Codec Selection**, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order was used.
- Click **OK** to commit (not shown).

The screenshot displays the IP Office configuration interface for the **System (1) 00E00706530F**. The **VoIP** tab is selected, showing the following configuration:

- Ignore DTMF Mismatch For Phones:** ☐
- Allow Direct Media Within NAT Location:** ☐
- RFC2833 Default Payload:** 101

The **Default Codec Selection** area shows the following codecs:

- Unused:** G.722 64K
- Selected:** G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP, G.723.1 6K3 MP-MLQ

**Note:** The codec selections defined under this section (System – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.5** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

## 5.2.4 System – VoIP Security Tab

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

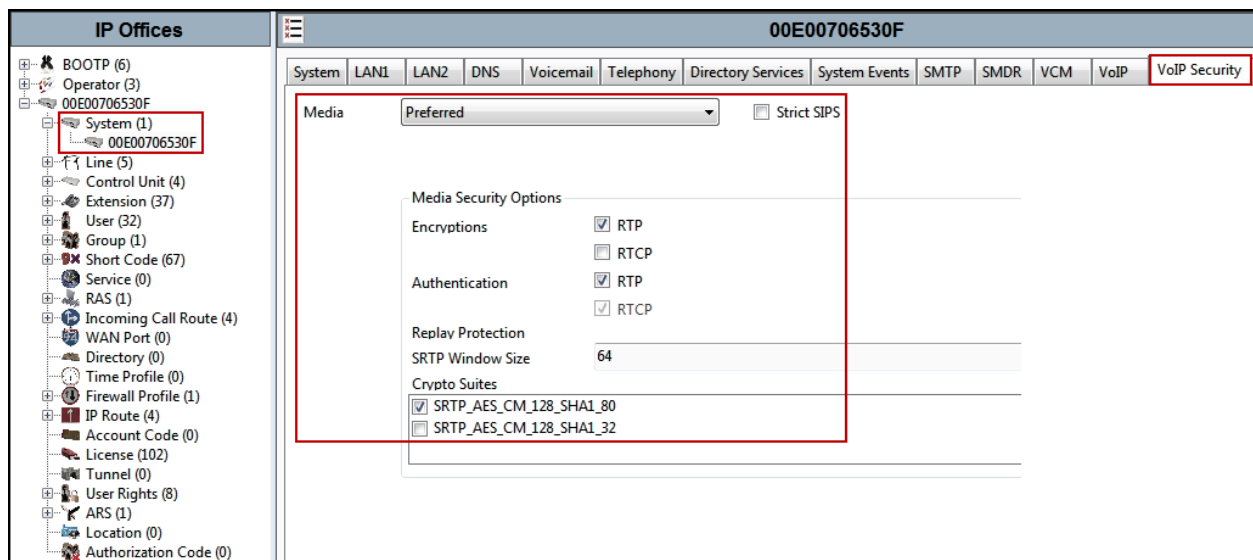
Configuring the use of SRTP at the system level is done on the **System VoIP Security** tab using the Media Security setting. The options are:

- Disabled (default).
- Preferred.
- Enforced.

When enabling SRTP on the system, the recommended setting is **Preferred**. In this scenario, IP Office uses SRTP if supported by the far-end, otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the far-end, the call is not established.

To configure the use of SRTP, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **VoIP Security** tab and configure the following parameters:

- Under **Media** select **Preferred** from the pull down menu.
- Verify that Strict **SIPS** is not checked.
- Under **Media Security Options** ensure that **RTP** is checked under **Encryptions** and **Authentication**.
- Under **Crypto Suites** ensure that **SRTP\_AES\_CM\_128\_SHA1\_80** is checked.
- Click **OK** to commit (not shown).



## 5.3 IP Route

In the reference configuration, the IP Office LAN1 interface and the private interface of the Avaya SBCE resided on different IP subnet, so an IP route was necessary. In an actual customer configuration, these two interfaces may be in different IP subnets, and in that case an IP route would have to be created to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides.

To create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the IP subnet where the Avaya SBCE resides (if located in different subnets), on the left **Navigation** pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** to **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the gateway/router used to route calls to the public network, e.g., **192.168.128.200**.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'Navigation' pane with a tree structure of configuration objects. The 'IP Route (4)' folder is expanded, showing a list of routes. The first route is highlighted with a red box, showing an IP Address of 0.0.0.0 and a Gateway IP Address of 192.168.99.0. On the right is the configuration window for the selected route, titled 'IP Route' with a subtitle '0.0.0.0'. The window contains the following fields:

IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	192 . 168 . 128 . 200
Destination	LAN1
Metric	0
<input type="checkbox"/> Proxy ARP	

## 5.4 SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Frontier Communications. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.4.1** to create the SIP Line from the template.

Some items relevant to a specific customer environment are not included in the template or may need to be updated after the SIP Line is created. Examples include the following:

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- Setting of the Use Network Topology Info field on the Transport tab

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 to 5.4.8**.

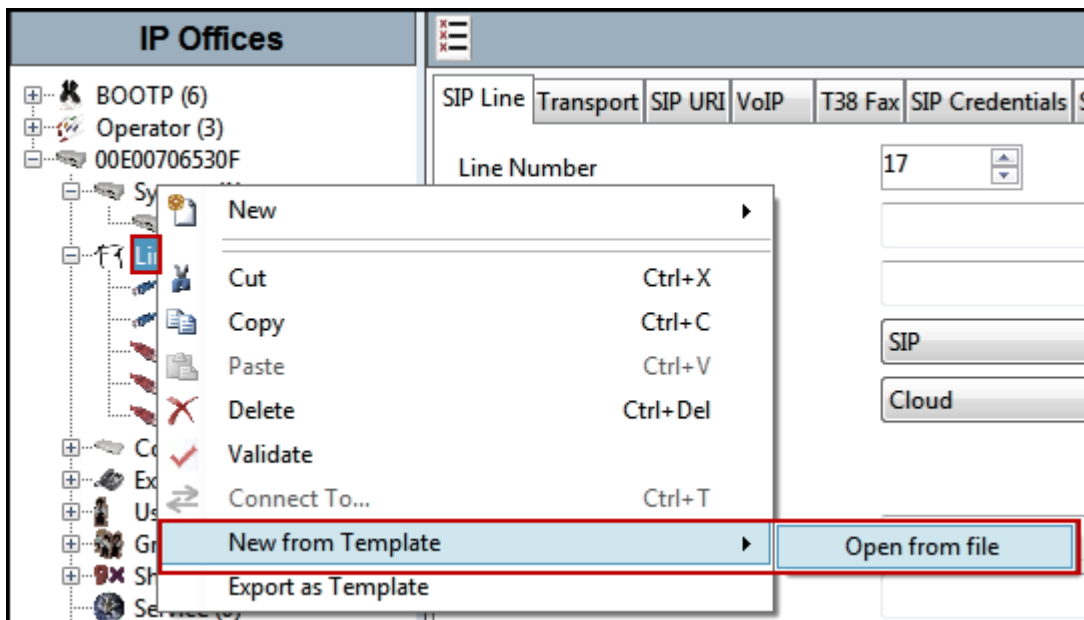
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2 to 5.4.8**.

### 5.4.1 Creating a SIP Trunk from an XML Template

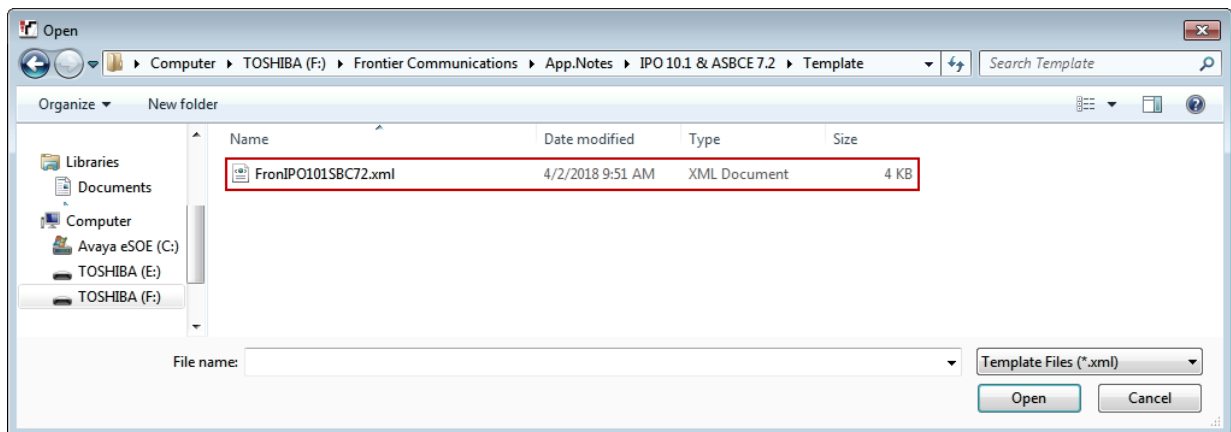
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., *\temp*) on the same computer where IP Office Manager is installed.

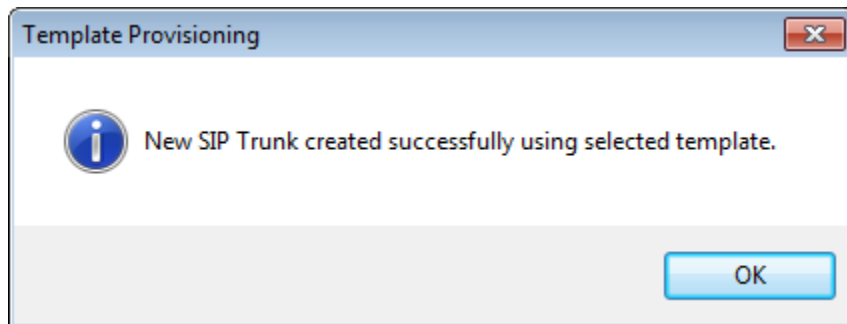
To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New from Template**→**Open from file**.



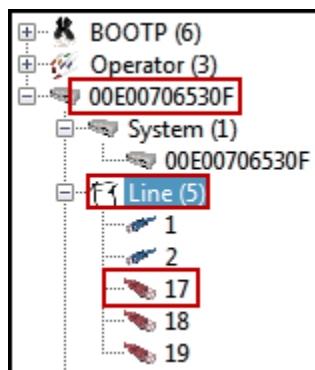
Navigate to the directory on the local machine where the template was copied and select the template.



After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**



The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line 17).



It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 to 5.4.8**.

## 5.4.2 SIP Line - SIP Line Tab

On the **SIP Line** tab in the Details Pane, configure or verify the parameters as shown below:

- Leave the **ITSP Domain Name** blank. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- Verify that **URI Type** is set to **SIP**.
- Verify that **In Service** box is checked, which is the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (seconds)** is set to **On Demand**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never** (Refer to Section 2.1).
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the 'SIP Line - Line 17' configuration window. The left pane shows a tree view of IP Office components, with 'SIP Line (5)' expanded and 'Line 17' selected. The main pane shows the 'SIP Line' tab with the following settings:

- Line Number:** 17
- ITSP Domain Name:** (blank)
- Local Domain Name:** (blank)
- URI Type:** SIP
- Location:** Cloud
- Prefix:** (blank)
- National Prefix:** (blank)
- International Prefix:** (blank)
- Country Code:** (blank)
- Name Priority:** System Default
- Description:** (blank)
- In Service:** ☒
- Check OOS:** ☒
- Session Timers:**
  - Refresh Method:** Auto
  - Timer (sec):** On Demand
- Redirect and Transfer:**
  - Incoming Supervised REFER:** Never
  - Outgoing Supervised REFER:** Never
  - Send 302 Moved Temporarily:** ☐
  - Outgoing Blind REFER:** ☐

### 5.4.3 SIP Line - Transport Tab

Select the **Transport** tab; configure the parameters as shown below:

- Set the **ITSP Proxy Address** to the IP address of the inside interface (or private side) assigned to the Avaya SBCE, as shown on **Figure 1**.
- Set the **Layer 4 Protocol** to **TLS**.
- Set **Use Network Topology Info** to **None** (see note below).
- Set the **Send Port** to **5061**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot shows the 'SIP Line - Line 17\*' configuration window. The 'Transport' tab is selected. The 'ITSP Proxy Address' is set to '10.64.101.243'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TLS', 'Send Port' is '5061', 'Use Network Topology Info' is set to 'None', and 'Listen Port' is '5061'. 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. 'Separate Registrar' is an empty field.

**Note** – For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was used in the test configuration. In addition, it was not necessary to configure the **System → LAN1 → Network Topology** tab for the purposes of SIP trunking. If a NAT is used between Avaya IP Office and the other end of the trunk, then the **Use Network Topology Info** field should be set to the LAN interface (LAN1) used by the trunk and the **System → LAN1 → Network Topology** tab needs to be configured with the details of the NAT device.



## 5.4.4 SIP Line - SIP URI Tab

Two SIP URI entries must be created to match each outgoing number that Avaya IP Office will send on this line and incoming numbers that Avaya IP Office will accept on this line.

To set the SIP URI for outgoing numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**
- Set **Identity** under **Identity** to **None**.
- Set **Header** under **Identity** to **P Asserted ID**.
- Set **Send Caller ID** under **Forwarding and Twinning** to **Diversion Header**.
- Set **Diversion Header** to **Auto**.
- Under **Registration**, select **0: <None>** from the pull-down menu.
- Set **Incoming Group** and **Outgoing Group** to **17** (SIP Line number being used).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit (not shown).
- Click **OK** to commit again (not shown).

## 5.4.5 SIP Line - VoIP Tab

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** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. Frontier Communications supports codec G.711 ULAW and G.729(a) for audio, with G.711 ULAW being the preferred codec.
- Select **T38 Fallback** for **Fax Transport Support** (Refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set the **Media Security** field to **Same as System (Preferred)**.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot shows the Avaya IP Office configuration interface for SIP Line - Line 17, specifically the VoIP tab. The left sidebar shows a tree view of the system configuration, with 'Line 17' selected. The main configuration area is divided into several sections:

- Codec Selection:** A dropdown menu is set to 'Custom'. Below it, two lists are shown: 'Unused' (G.711 ALAW 64K, G.722 64K, G.723.1 6K3 MP-MLQ) and 'Selected' (G.711 ULAW 64K, G.729(a) 8K CS-ACELP). Arrows between the lists allow for reordering.
- Fax Transport Support:** A dropdown menu is set to 'T38 Fallback'.
- DTMF Support:** A dropdown menu is set to 'RFC2833'.
- Media Security:** A dropdown menu is set to 'Same as System (Preferred)'. Below this, the 'Advanced Media Security Options' section is expanded, showing checkboxes for 'Encryptions' (RTP checked), 'Authentication' (RTP checked, RTCP checked), 'Replay Protection' (SRTP Window Size set to 64), and 'Crypto Suites' (SRTP\_AES\_CM\_128\_SHA1\_80 checked, SRTP\_AES\_CM\_128\_SHA1\_32 unchecked).
- Other Options:** On the right side, several checkboxes are visible: 'VoIP Silence Suppression' (unchecked), 'Local Hold Music' (unchecked), 'Re-invite Supported' (checked), 'Codec Lockdown' (unchecked), 'Allow Direct Media Path' (unchecked), 'Force direct media with phones' (unchecked), 'PRACK/100rel Supported' (checked), and 'G.711 Fax ECAN' (unchecked).

**Note:** The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.3** (System – VoIP tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

### 5.4.6 SIP Line – T38 Fax Tab

Select the **T38 Fax** tab, to set the Fax over Internet Protocol parameters of the SIP Line. Set or verify the parameters as shown below:

- Uncheck the **Use Default Values** at the bottom of the screen.
- Verify the **T.38 Fax Version** is set to **0**.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'T38 Fax' tab selected. The left sidebar shows a tree view of the system configuration, with 'Line 5' and '17' highlighted. The main configuration area contains the following settings:

Parameter	Value
T38 Fax Version	0
Transport	UDPTL
Redundancy	Low Speed: 0, High Speed: 0
TCF Method	Trans TCF
Max Bit Rate (bps)	14400
EFlag Start Timer (ms)	2600
EFlag Stop Timer (ms)	2300
Tx Network Timeout (sec)	150

On the right side, there are several checkboxes and input fields:

- ☒ Scan Line Fix-up
- ☒ TFOP Enhancement
- ☐ Disable T30 ECM
- ☐ Disable EFlags For First DIS
- ☐ Disable T30 MR Compression
- ☐ NSF Override
- Country Code: 0
- Vendor Code: 0

At the bottom left, the 'Use Default Values' checkbox is unchecked and highlighted with a red box.

## 5.4.7 SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab.

In the **Addressing** area:

- Select **To Header** for **Call Routing Method**.

In the **Identity** area, the **Use PAI for Privacy** parameter is checked to include the caller's DID number in the P-Asserted-Identity (PAI) SIP header for a privacy requested call:

- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'SIP Advanced' tab selected. The left sidebar shows a tree view of the configuration hierarchy, with 'Line (5)' selected. The main area is divided into three sections: Addressing, Identity, and Media.

**Addressing:**

- Association Method: By Source IP address
- Call Routing Method: To Header
- Suppress DNS SRV Lookups: ☐

**Identity:**

- Use "phone-context": ☐
- Add user=phone: ☐
- Use + for International: ☐
- Use PAI for Privacy: ☒
- Use Domain for PAI: ☐
- Swap From and PAI/Diversion: ☐
- Caller ID from From header: ☐
- Send From In Clear: ☐
- Cache Auth Credentials: ☒
- User-Agent and Server Headers:
- Send Location Info: Never
- Add UUI header: ☐
- Add UUI header to redirected calls: ☐

**Media:**

- Allow Empty INVITE: ☐
- Send Empty re-INVITE: ☐
- Allow To Tag Change: ☐
- P-Early-Media Support: None
- Send SilenceSupp=Off: ☐
- Force Early Direct Media: ☐
- Media Connection Preservation: Disabled
- Indicate HOLD: ☐

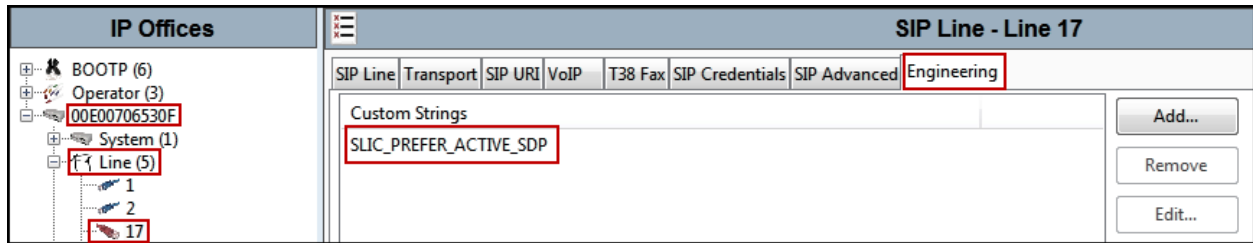
**Call Control:**

- 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: ☐
- Emulate NOTIFY for REFER: ☐
- No REFER if using Diversion: ☐

## 5.4.8 SIP Line – SIP Engineering Tab

A SIP Line Custom String (SLIC) is required for proper operation of T.38 fax calls (refer to **Section 2.2**). With this entry, IP Office will reverse the order of the media line entries in the SDP in the re-INVITE message it sends, with the active T.38 media line entry listed first followed by the inactive media line entry for audio (port set to 0).

To configure a custom string, select the **Engineering** tab and click **Add**. The New Custom String section will appear. In the **Custom String** field, enter **SLIC\_PREFER\_ACTIVE\_SDP**. Click **OK** to commit (not shown).



## 5.5 Extension

In this section, an example of an Avaya IP Office extension will be illustrated. In the interests of brevity, not all users and extensions will be presented, since the configuration can be easily extrapolated to other users and extensions. To add an extension, right click on **Extension** then select **New → Select H323 or SIP**.

Select the **Extn** tab. Following is an example of extension 3042; this extension corresponds to an H.323 extension.

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy: BOOTP (6), Operator (3), System (1), Line (5), Control Unit (4), and Extension (37). The 'Extension (37)' folder is expanded, and the extension '8008 3042' is selected. The main panel on the right is titled 'H.323 Extension: 8008 3042' and contains the following configuration fields:

Field	Value
Extension ID	8008
Base Extension	3042
Phone Password	
Confirm Phone Password	
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Avaya 9641
Location	Automatic
Fallback As Remote Worker	Auto
Module	0
Port	0
Disable Speakerphone	<input type="checkbox"/>

Select the **VOIP** tab. Use default values on VoIP tab. Following is an example for extension 3040; this extension corresponds to an H.323 extension.

By default, all IP phones (SIP and H.323) will use the system default codec selection configured under the System VoIP tab (**Section 5.2.3**), unless configured otherwise for a specific extension by selecting **Custom** under **Codec Selection** on the screenshot shown below. The example below shows the codecs used for IP phones (SIP and H.323).

By default, all IP phones (SIP and H.323) will use the system default Media Security selection configured under the System **VoIP Security** tab (**Section 5.2.4**), unless configured otherwise for a specific extension by selecting **Media Security** under **VoIP** tab on the screenshot shown below. The **Media Security** field was set to **Same as System (Preferred)**. The example below shows the Media Security used for IP phones (SIP and H.323).

The screenshot displays the configuration interface for an H.323 extension, specifically extension 8008 3042. The left sidebar shows a tree view of the system configuration, with 'Extension (37)' selected. The main panel is titled 'H.323 Extension: 8008 3042' and contains the following settings:

- Extension:** VoIP
- IP Address:** 0 . 0 . 0 . 0
- MAC Address:** 00 00 00 00 00 00
- Codec Selection:** System Default
- Reserve License:** None
- TDM->IP Gain:** Default
- IP->TDM Gain:** Default
- Supplementary Services:** None
- Media Security:** Same as System (Preferred)

The 'Media Security' section is expanded, showing 'Advanced Media Security Options' with the following settings:

- Encryptions:** ☒ RTP, ☐ RTCP
- Authentication:** ☒ RTP, ☒ RTCP
- Replay Protection:** ☐ SRTP Window Size: 64
- Crypto Suites:** ☒ SRTP\_AES\_CM\_128\_SHA1\_80, ☐ SRTP\_AES\_CM\_128\_SHA1\_32


Additional options on the right side of the page include:

- ☐ VoIP Silence Suppression
- ☐ Enable Faststart for non-Avaya IP phones
- ☒ Out Of Band DTMF
- ☐ Local Tones
- ☒ Allow Direct Media Path

## 5.6 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first navigate to **User** in the left Navigation Pane, and then select the name of the user to be modified. In the example below, the name of the user is **Ext3042 H323**.

The screenshot displays the Avaya SIP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'User (32)' selected and highlighted. The main panel is titled 'Ext3042 H323: 3042' and contains several tabs: 'User', 'Voicemail', 'DND', 'Short Codes', 'Source Numbers', 'Telephony', 'Forwarding', 'Dial In', 'Voice Recording', and 'Button Programming'. The 'User' tab is active, showing the following configuration fields:

- Name: Ext3042 H323
- Password: ••••
- Confirm Password: ••••
- Unique Identity:
- Conference PIN:
- Confirm Audio Conference PIN:
- Account Status: Enabled (dropdown)
- Full Name: Ext3042 H323
- Extension: 3042
- Email Address:
- Locale: (dropdown)
- Priority: 5 (dropdown)
- System Phone Rights: None (dropdown)
- Profile: Basic User (dropdown)
  - ☐ Receptionist
  - ☐ Enable Softphone
  - ☐ Enable one-X Portal Services
  - ☐ Enable one-X TeleCommuter
  - ☒ Enable Remote Worker
  - ☒ Enable Communicator
  - ☐ Enable Mobile VoIP Client
  - ☐ Send Mobility Email
  - ☐ Web Collaboration
- ☐ Exclude From Directory
- Device Type:  Avaya 9641
- User Rights:



In the example below, the name of the user is **Ext3047 SIP**. This is a Softphone user, set the **Profile** to **Power User** and check **Enable Softphone**.

**IP Offices**

- BOOTP (3)
- Operator (3)
- 00E00706530F
- System (1)
- 00E00706530F
- Line (5)
- Control Unit (4)
- Extension (37)
- User (32)**
  - NoUser
  - RemoteManager
  - 3055 3055
  - 3040 Ext3040 H323
  - 3041 Ext3041 H323
  - 3042 Ext3042 H323
  - 3043 Ext3043 Digita
  - 3044 Ext3044 Digita
  - 3047 Ext3047 SIP**
  - 3049 Ext3049 Fax
  - 4002 Extn4002
  - 4003 Extn4003
  - 4004 Extn4004
  - 4005 Extn4005
  - 4006 Extn4006
  - 4007 Extn4007
  - 4008 Extn4008
  - 4011 Extn4011
  - 4012 Extn4012
  - 4013 Extn4013
  - 4014 Extn4014
  - 4015 Extn4015
  - 4016 Extn4016
  - 4017 Extn4017
  - 4018 Extn4018
  - 4019 Extn4019
  - 4020 Extn4020
  - 4021 Extn4021
  - 4022 Extn4022
  - 4023 Extn4023
  - 4024 Extn4024
  - 3050 sip3050
- Group (1)
- Short Code (65)
- Service (0)
- RAS (1)
- Incoming Call Route (4)

**Ext3047 SIP: 3047**

**User** | Voicemail | DND | Short Codes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Programming

Name: Ext3047 SIP

Password: .....

Confirm Password: .....

Conference PIN:

Confirm Conference PIN:

Account Status: Enabled

Full Name: Softclient 3047

Extension: 3047

Email Address:

Locale:

Priority: 5

System Phone Rights: None

**Profile: Power User**

- ☐ Receptionist
- ☒ **Enable Softphone**
- ☒ Enable one-X Portal Services
- ☒ Enable one-X TeleCommuter
- ☐ Enable Remote Worker
- ☒ Enable Communicator
- ☒ Enable Mobile VoIP Client
- ☐ Send Mobility Email
- ☐ Ex Directory
- ☐ Web Collaboration

Device Type: Unknown SIP device

Select the **Voicemail** tab. The following screen shows the **Voicemail** tab for the user with extension 3042. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application Notes, incoming calls from Frontier Communications to this user were redirected to Voicemail Pro after no answer. Voicemail messages were recorded and retrieved successfully. Voice mail navigation and retrieval were performed locally and from PSTN telephones to test DTMF using RFC 2833.

The screenshot displays the Avaya IP Office configuration interface for extension 3042. The left-hand tree view shows the hierarchy: IP Offices > BOOTP (6) > Operator (3) > 00E00706530F > System (1) > Line (5) > Control Unit (4) > Extension (37) > User (32). The 'User (32)' node is selected, and the 'Voicemail' tab is active. The main configuration area shows the following settings:

- Voicemail Code:** [Redacted]
- Confirm Voicemail Code:** [Redacted]
- Voicemail Email:** [Empty field]
- Voicemail On:** ☒
- Voicemail Help:** ☒
- Voicemail Ringback:** ☐
- Voicemail Email Reading:** ☐
- UMS Web Services:** ☐
- Voicemail Email:**
  - ☒ Off
  - ☐ Copy
  - ☐ Forward
  - ☐ Alert
- DTMF Breakout:**
  - Reception/Breakout (DTMF 0):** System Default ()
  - Breakout (DTMF 2):** System Default ()
  - Breakout (DTMF 3):** System Default ()

Select the **Mobility** tab. In the sample configuration user 3042 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for user 3042. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned telephone, including the dial access code “9”, in this case **917864571234**. Other options can be set according to customer requirements.

The screenshot shows the Avaya User Configuration interface for user 3042. The left sidebar displays a tree view of the system hierarchy, with 'User (32)' selected. The main panel shows the 'Mobility' tab, which is highlighted in red. The 'Internal Twinning' section is disabled. The 'Mobility Features' section is checked, and the 'Mobile Twinning' checkbox is also checked. The 'Twinned Mobile Number' field is set to '917864571234'. Other settings like 'Twinning Time Profile', 'Mobile Dial Delay', and 'Mobile Answer Guard' are also visible.

To program a key on the telephone to turn Mobile Twinning on and off, select the **Button Programming** tab on the user, then select the button to program to turn Mobile Twinning on and off, click on **Edit → Action → Emulation**, select **Twinning** (not shown). In the sample below, button 4 was programmed to turn Mobile Twinning on and off for user 3042.

The screenshot shows the Avaya User Configuration interface for user 3042. The left sidebar displays a tree view of the system hierarchy, with 'User (32)' selected. The main panel shows the 'Button Programming' tab, which is highlighted in red. The table below shows the configuration for buttons 1 through 11. Button 4 is highlighted, showing its action as 'Twinning'.

Button ...	Label	Action	Action Data
1		Appearance	a=
2		Appearance	b=
3		Appearance	c=
4		Twinning	
5			
6			
7			
8			
9			
10			
11			

Select the **SIP** tab. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the “From” and “Contact” headers for outgoing SIP trunk calls. In addition, these settings are used to match against the SIP URI of incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.4**). The example below shows the settings for user “Ext3042 H323”. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Frontier Communications. In the example, DID number **5851239827** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

If all calls involving this user should be considered private, then the **Anonymous** box may be checked to withhold the Caller ID information from the network.

Ext3042 H323: 3042*	
Dial In	Voice Recording
Button Programming	Menu Programming
Mobility	Group Membership
Announcements	SIP
SIP Name	5851239827
SIP Display Name (Alias)	Ext3042 H323
Contact	5851239827
<input type="checkbox"/> Anonymous	

## 5.7 Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system. In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** (Section 5.4.7) and **SIP URI** (Section 5.4.4) and the users **SIP Name** and **Contact**, already populated with the assigned Frontier Communications DID numbers (Section 5.6).

### 5.7.1 Incoming Call Route – Standard Tab

To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**.

On the **Standard** tab of the Details Pane, enter the parameters as shown below.

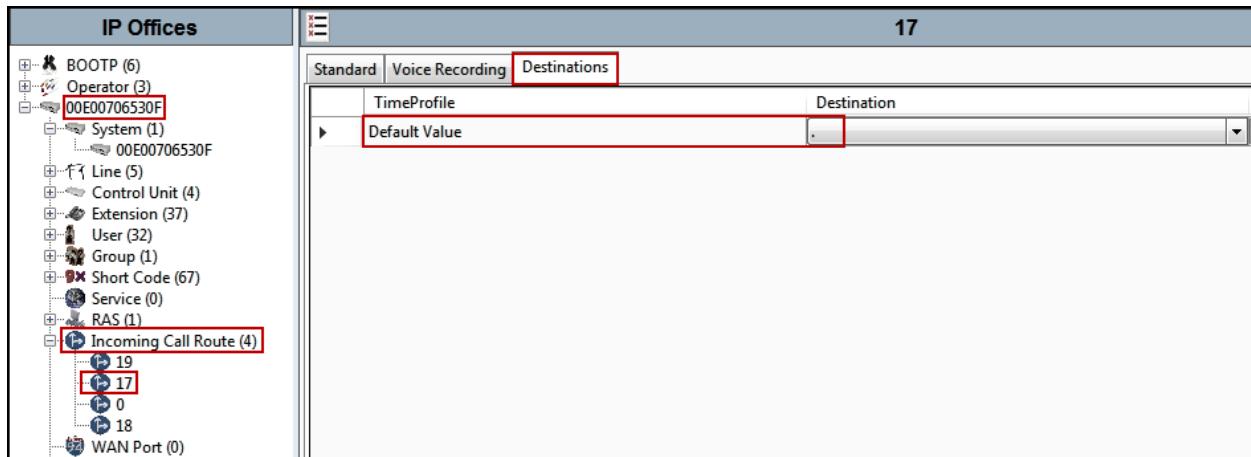
- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in Section 5.4.
- Default values can be used for all other fields.

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'Incoming Call Route (4)' selected and highlighted with a red box. Below it, the '17' route is also highlighted with a red box. On the right, the 'Details Pane' shows the 'Standard' tab selected, with 'Voice Recording' and 'Destinations' tabs also visible. The 'Standard' tab contains the following configuration fields:

Field	Value
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

## 5.7.2 Incoming Call Route – Destinations Tab

- Under the **Destinations** tab, enter “.” for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User**, which matches the number present on the user part of the incoming Request URI.
- Click **OK** to commit (not shown).



## 5.8 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used.

### 5.8.1 Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** on the Navigation Pane and select **New**. The screen below shows the short code **9N** created (Note that the semi-colon is not used here). In this case, when the Avaya IP Office user dials 9 plus any number **N**, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS. Configure the following parameters:

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **9N** was used (Note that the semi-colon is not used here).
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group Id** to **50: Main** to be directed to **Line Group 50: Main**, this is configurable via ARS.
- Click the **OK** to commit (not shown).

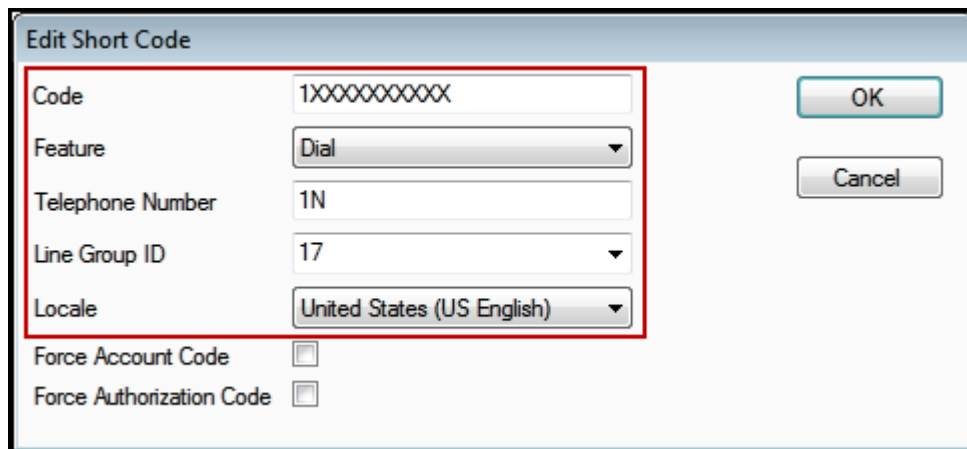
The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' navigation pane lists various system objects, with '9N' highlighted in blue. The main configuration area on the right is titled '9N: Dial' and contains the following fields:

Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **Xs** used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

To create a short code to be used for ARS, select **ARS → 50: Main** on the Navigation Pane and click **Add**. Configure the following parameters:

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **1** followed by **10 Xs** to represent the exact number of digits.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **1N**. The value **N** represents the additional number of digits dialed by the user after dialing **1** (The **9** will be stripped off).
- Set the **Line Group Id** to the Line Group number being used for the SIP Line, in this case **Line Group ID 17** was used.
- Click **OK** to commit.



Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.



The example highlighted below shows that for calls in the North American numbering plan, the user dialed **9**, followed by **1** and **10** digits (represented by **10 X's**). The **9** is stripped off, the remaining digits, including the **1** shown in the examples below, are included in the SIP INVITE message IP Office sends to Frontier Communications.

**IP Offices**

- BOOTP (6)
- Operator (3)
- 00E00706530F
- System (1)
- Line (5)
- Control Unit (4)
- Extension (37)
- User (32)
- Group (1)
- Short Code (67)
- Service (0)
- RAS (1)
- Incoming Call Route (4)
- WAN Port (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)
- IP Route (4)
- Account Code (0)
- License (102)
- Tunnel (0)
- User Rights (8)
- ARS (1)
  - 50: Main
- Location (0)
- Authorization Code (0)

**Main**

ARS

ARS Route ID: 50

Route Name: Main

Dial Delay Time: System Default (3)

Description:

In Service: ☒ Out of Service Route: <None>

Time Profile: <None> Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
1XXXXXXXXX	1N	Dial	17
6XXXXXX	6N	Dial	17
3XXXXXXXXX	3N	Dial	17
28XXXXXX	28N	Dial	17
55XXXXXXXXX	55N	Dial	17
01XXXXXXXXXXXX	01N	Dial	17
04X	04N	Dial	17

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

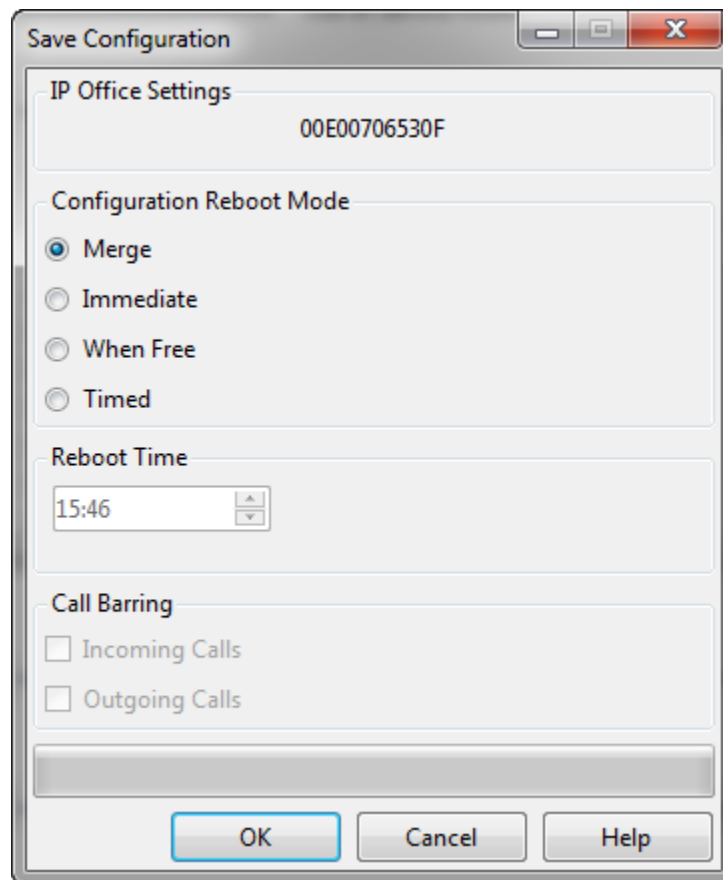
Alternate Route: <None>

## 5.9 Save Configuration

When desired, send the configuration changes made in Avaya IP Office Manager to the Avaya IP Office server in order for the changes to take effect.

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

Once the configuration is validated, a screen similar to the following will appear, with either the **Merge** or the **Immediate** radio button chosen based on the nature of the configuration changes made since the last save. Note that clicking OK may cause a service disruption due to system reboot. Click **OK** if desired.



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 '00E00706530F'. The second section, 'Configuration Reboot Mode', contains four radio buttons: 'Merge' (selected), 'Immediate', 'When Free', and 'Timed'. The third section, 'Reboot Time', contains a time selection field showing '15:46'. The fourth section, 'Call Barring', contains two checkboxes: 'Incoming Calls' and 'Outgoing Calls', both of which are unchecked. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

## 6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE)

This section describes the required configuration of the Avaya SBCE to connect to Frontier Communications SIP Trunking Service.

It is assumed that the Avaya SBCE was provisioned and is ready to be used. The configuration shown here is accomplished using the Avaya SBCE web interface.

**Note:** In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

### 6.1 Log in Avaya SBCE

Use a Web browser to access the Avaya SBCE Web interface. Enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the Avaya SBCE management IP address.

Enter the appropriate credentials and click **Log In**.



**AVAYA**

**Session Border Controller  
for Enterprise**

**Log In**

Username:

Password:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2017 Avaya Inc. All rights reserved.

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

**Session Border Controller for Enterprise** AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

**Dashboard**

Administration  
Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ Domain Policies  
‣ TLS Management  
‣ Device Specific Settings

**Dashboard**

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

The following certificates will expire within the next 60 days:  
• Clearcom\_Cert.crt (Certificate)

Information		
System Time	11:07:07 AM EDT	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	04/02/2018 16:18:53 EDT	
Failed Login Attempts	0	

**Installed Devices**

EMS  
Avaya\_SBCE

**Active Alarms (past 24 hours)**  
None found.

**Incidents (past 24 hours)**  
Avaya\_SBCE : No Subscriber Flow Matched  
Avaya\_SBCE : No Subscriber Flow Matched  
Avaya\_SBCE : No Subscriber Flow Matched  
Avaya\_SBCE : No Subscriber Flow Matched  
Avaya\_SBCE : No Subscriber Flow Matched

**Notes**  
No notes found.

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

**Session Border Controller for Enterprise** AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

**System Management**

Dashboard  
Administration  
Backup/Restore  
**System Management**  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ Domain Policies  
‣ TLS Management  
‣ Device Specific Settings

**Devices** Updates SSL VPN Licensing Key Bundles

Device Name	Management IP	Version	Status	
Avaya_SBCE		7.2.1.0-05-14222	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The **System Information** screen is displayed showing the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.

System Information: Avaya\_SBCE

**General Configuration**

Appliance NameAvaya\_SBCE

Box TypeSIP

Deployment ModeProxy

**Device Configuration**

HA ModeNo

Two Bypass ModeNo

**License Allocation**

Standard Sessions  
Requested: 20002000

Advanced Sessions  
Requested: 20002000

Scopia Video Sessions  
Requested: 500500

CES Sessions  
Requested: 00

Transcoding Sessions  
Requested: 00

Encryption☒

**Network Configuration**

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.101.243	10.64.101.243	255.255.255.0	10.64.101.1	A1
				A1
				A1
				B1
				B1
10.10.80.51	10.10.80.51	255.255.255.128	10.10.80.1	B1

**DNS Configuration**

Primary DNS8.8.8.8

Secondary DNS7.7.7.7

DNS LocationDMZ

DNS Client IP10.10.80.51

**Management IP(s)**

IP #1 (IPv4)

On the previous screen, note that **A1** corresponds to the inside interface (Private Network side) and **B1** corresponds to the outside interface (Public Network side) of the Avaya SBCE. (Use **Figure 1** as reference for IP addresses assignments). The configuration required for Remote Worker is beyond the scope of these Application Notes and is not discussed in these Application Notes, thus IP addresses used for Remote Worker assigned to interfaces **A1** and **B1** were blurred out. The management IP address was also blurred out for security reasons.

**IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled “M1”) 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).**

## 6.2 TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

For the compliance testing, the transport protocol that was used between IP Office and the Avaya SBCE, across the enterprise private IP network (LAN), was SIP over TLS. SIP over UDP was used between the Avaya SBCE and Frontier Communications, across the public Internet.

It is assumed that generation and installation of certificates and the creation of TLS Profiles on the Avaya SBCE have been previously completed, as it's not discussed in this document. Refer to item [8] in **Section 10**.

## 6.3 Global Profiles

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

### 6.3.1 Server Interworking – Avaya-IPO

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunking service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or “cloned”. Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or “cloned”. If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution. For Frontier Communications, this profile was left with the **avaya-ru** default values.

On the left navigation pane, select **Global Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone** on top right of the screen (not shown).

Enter the new profile name in the **Clone Name** field; the name of **Avaya-IPO** was chosen in this example. Click **Finish**.



Clone Profile	
Profile Name	avaya-ru
Clone Name	Avaya-IPO
<button>Finish</button>	

Click **Edit** on the newly cloned **Avaya-IPO** interworking profile:

- On the **General** tab, check **T.38 Support**.
- Leave remaining fields with default values.
- Click **Finish**.

The following screen capture shows the **General** tab of the newly created **Avaya-IPO** Server Interworking Profile.

The screenshot shows a window titled "Editing Profile: Avaya-IPO" with a close button (X) in the top right corner. The "General" tab is selected. The following settings are visible:

Field	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 (dropdown)
Send Hold	<input type="checkbox"/>
Delayed Offer	<input 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"/>
<b>T.38 Support</b>	<input checked="" 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 of the window is a "Finish" button.

The following screen capture shows the **General** tab of the newly created **Avaya-IPO** Server Interworking Profile

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

## Session Border Controller for Enterprise

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▾ Global Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Server Configuration

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

RADIUS

▸ PPM Services

▸ Domain Policies

▸ TLS Management

▸ Device Specific Settings

Interworking Profiles: Avaya-IPO

Add

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

Avaya-SM

SP-General

Avaya-IPO

Avaya-CS1000

Avaya-CM

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

General

Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Edit

HG; Reviewed:  
SPOC 5/18/2018

Solution & Interoperability Test Lab Application Notes  
©2018 Avaya Inc. All Rights Reserved.

48 of 99  
FronIPO101SBC72



The following screen capture shows the **Advanced** tab of the newly created **Avaya-IPO** Server Interworking Profile.

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a tree view with categories like 'Dashboard', 'Administration', 'System Management', 'Global Parameters', 'Global Profiles', 'Domain DoS', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'RADIUS', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Global Profiles' section is expanded, showing 'Server Interworking' as the selected profile. The main content area is titled 'Interworking Profiles: Avaya-IPO' and features an 'Add' button. Below this is a list of profiles: 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General', 'Avaya-IPO' (highlighted), 'Avaya-CS1000', and 'Avaya-CM'. The 'Avaya-IPO' profile is selected, and its configuration is shown in the 'Advanced' tab. The configuration includes a table for 'Record Routes' and 'Include End Point IP for Context Lookup', a section for 'DTMF' support, and an 'Edit' button.

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Click here to add a description.					
Record Routes		Both Sides			
Include End Point IP for Context Lookup		Yes			
Extensions		Avaya			
Diversion Manipulation		No			
Has Remote SBC		Yes			
Route Response on Via Port		No			
Relay INVITE Replace for SIPREC		No			
MOBX Re-INVITE Handling		No			
<b>DTMF</b>					
DTMF Support		None			
<a href="#">Edit</a>					

### 6.3.2 Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the service provider.

On the left navigation pane, select **Global Profiles → Server Interworking** (not shown). From the **Interworking Profiles** list, select **Add** (not shown) (note that **Add** is being used to create the SP-General profile instead of cloning the avaya-ru profile).

Enter the new profile name; the name of **SP-General** was chosen in this example.

- Click **Next**.



The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "SP-General". A red rectangular box highlights the "Profile Name" label and the input field. Below the input field, there is a "Next" button.

On the **General** tab, check **T.38 Support**. Click **Next**, and then click **Finish** on the last tab leaving remaining fields with default values (not shown).

**Interworking Profile** [X]

**General**

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"/>
<b>T.38 Support</b>	<input checked="" 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

Back Next

The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a tree view with categories like 'Dashboard', 'Administration', 'System Management', 'Global Parameters', 'Global Profiles', 'Domain DoS', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'RADIUS', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Global Profiles' section is expanded, showing 'Server Interworking' as the selected profile. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button. Below this is a list of interworking profiles: 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (highlighted), 'Avaya-IPO', 'Avaya-CS1000', and 'Avaya-CM'. The 'General' tab is selected, showing a table of settings. The 'T.38 Support' setting is highlighted with a red box and set to 'Yes'. Other settings include 'Hold Support' (NONE), '180 Handling' (None), '181 Handling' (None), '182 Handling' (None), '183 Handling' (None), 'Refer Handling' (No), 'URI Group' (None), 'Send Hold' (No), 'Delayed Offer' (No), '3xx Handling' (No), 'Diversion Header Support' (No), 'Delayed SDP Handling' (No), 'Re-Invite Handling' (No), 'Prack Handling' (No), 'Allow 18X SDP' (No), 'URI Scheme' (SIP), and 'Via Header Format' (RFC3261). An 'Edit' button is located at the bottom right of the settings table.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', and 'Settings'. The left sidebar contains a tree view with categories like 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'Domain DoS', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'RADIUS', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Global Profiles' section is expanded, showing a list of profiles: 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-...', 'Avaya-SM', 'SP-General' (highlighted), 'Avaya-IPO', 'Avaya-CS1000', and 'Avaya-CM'. The 'SP-General' profile is selected, and its 'Advanced' tab is active. The 'Advanced' tab shows settings for 'Record Routes' (Both Sides), 'Include End Point IP for Context Lookup' (No), 'Extensions' (None), 'Diversion Manipulation' (No), 'Has Remote SBC' (Yes), 'Route Response on Via Port' (No), 'Relay INVITE Replace for SIPREC' (No), 'MOBX Re-INVITE Handling' (No), and 'DTMF Support' (None). An 'Edit' button is visible at the bottom right of the settings area.

**Session Border Controller for Enterprise**

Alarms 2 Incidents Status Logs Diagnostics Users Settings

Dashboard  
Administration  
Backup/Restore  
System Management  
▸ Global Parameters  
▾ Global Profiles  
    Domain DoS  
    Media Forking  
    Routing  
    Server Configuration  
    Topology Hiding  
    Signaling Manipulation  
    URI Groups  
    SNMP Traps  
    Time of Day Rules  
    FGDN Groups  
    Reverse Proxy Policy  
    RADIUS  
▸ PPM Services  
▸ Domain Policies  
▸ TLS Management  
▸ Device Specific Settings

**Interworking Profiles: SP-General**

Add Rename

Interworking Profiles

cs2100  
avaya-ru  
OCS-Edge-Server  
cisco-ccm  
cups  
OCS-FrontEnd-...  
Avaya-SM  
**SP-General**  
Avaya-IPO  
Avaya-CS1000  
Avaya-CM

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation **Advanced**

Record Routes Both Sides

Include End Point IP for Context Lookup No

Extensions None

Diversion Manipulation No

Has Remote SBC Yes

Route Response on Via Port No

Relay INVITE Replace for SIPREC No

MOBX Re-INVITE Handling No

**DTMF**

DTMF Support None

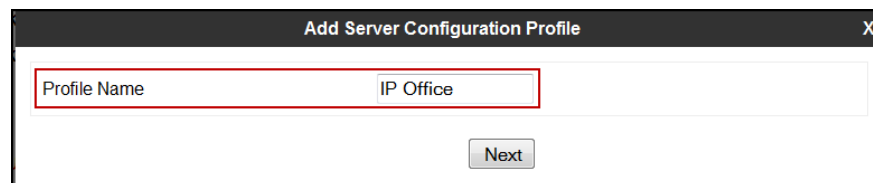
Edit

### 6.3.3 Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (IP Office) and the Trunk Server or SIP Proxy at the service provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** (not shown). Click **Add Profile** (not shown) and enter the profile name: **IP Office**.

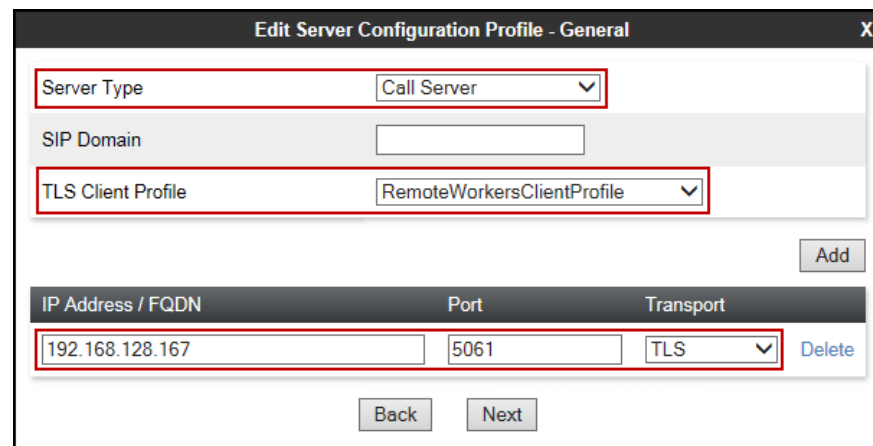
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "IP Office". Below this field is a "Next" button.

On the **Edit Server Configuration Profile – General** window:

- **Server Type:** Select **Call Server**.
- **TLS Client Profile:** Select the appropriate **TLS Client Profile**.
- **IP Address / FQDN:** **192.168.128.167** (IP Address of IP Office).
- **Port:** **5061** (This port must match the port number defined in **Section 5.4.3**).
- **Transports:** Select **TLS**.
- Click **Next**



The screenshot shows a window titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. The window contains several fields: "Server Type" is a dropdown menu set to "Call Server"; "SIP Domain" is an empty text field; "TLS Client Profile" is a dropdown menu set to "RemoteWorkersClientProfile"; "IP Address / FQDN" is a text field containing "192.168.128.167"; "Port" is a text field containing "5061"; and "Transport" is a dropdown menu set to "TLS". There is an "Add" button to the right of the "TLS Client Profile" field. At the bottom, there are "Back" and "Next" buttons.

- Click **Next** on the **Add Server Configuration Profile - Authentication** window (not shown).
- Click **Next** on the **Add Server Configuration Profile - Heartbeat** window (not shown).
- Click **Next** on the **Add Server Configuration Profile - Ping** window (not shown).

On the **Add Server Configuration Profile - Advanced** window:

- Select **Avaya-IPO** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

**Add Server Configuration Profile - Advanced** X

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

Back Finish

The following screen capture shows the **General** tab of the newly created **IP Office** Server Configuration Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the Avaya logo. The left sidebar contains a menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration (highlighted), Topology Hiding, Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, Reverse Proxy Policy, RADIUS, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Server Configuration: IP Office' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a tabbed interface with 'General', 'Authentication', 'Heartbeat', 'Ping', and 'Advanced' tabs. The 'General' tab is active, showing 'Server Type' as 'Call Server' and 'TLS Client Profile' as 'RemoteWorkersClientProfile'. A table lists server configurations with columns 'IP Address / FQDN', 'Port', and 'Transport'. The first entry is '192.168.128.167' on port '5061' using 'TLS' transport. An 'Edit' button is located at the bottom right of the table.

IP Address / FQDN	Port	Transport
192.168.128.167	5061	TLS



The following screen capture shows the **Advanced** tab of the newly created **IP Office** Server Configuration Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms (2), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand navigation menu lists various system management options, with "Server Configuration" highlighted. The main content area is titled "Server Configuration: IP Office" and features an "Add" button. Below this, a list of server profiles is shown, with "IP Office" selected. The "Advanced" tab is active, displaying configuration options such as "Enable DoS Protection", "Enable Grooming", "Interworking Profile" (set to "Avaya-IPO"), "Signaling Manipulation Script", "Securable", "Enable FGDN", "Tolerant", and "URI Group". An "Edit" button is located at the bottom right of the configuration area.

To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** (not shown) section and enter the profile name: **Service Provider UDP**.

- Click **Next**.

The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "e Provider UDP" followed by a small 'x' icon. Below the input field is a "Next" button.

On the **Edit Server Configuration Profile – General** window:

- **Server Type:** Select **Trunk Server**.
- **IP Address / FQDN:** **192.168.24.40** (Public IP address of Frontier Communications SIP proxy server).
- **Port:** **5060**.
- **Transports:** Select **UDP**.
- Click **Next**.

**Edit Server Configuration Profile - General**

Server Type: Trunk Server

SIP Domain:

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport	
192.168.24.40	5060	UDP	Delete

Back Next

- Click **Next** until the **Add Server Configuration Profile - Advanced** window is reached.
- Select **SP-General** from the **Interworking Profile**.
- Click **Finish**.

**Add Server Configuration Profile - Advanced**

Enable DoS Protection: ☐

Enable Grooming: ☐

Interworking Profile: SP-General

Signaling Manipulation Script: None

Securable: ☐

Enable FGDN: ☐

TCP Failover Port: 5060

TLS Failover Port: 5061

Tolerant: ☐

URI Group: None

Back Finish

The following screen capture shows the **General** tab of the newly created **Service Provider UDP** Server Configuration Profile.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', and 'Settings'. The left sidebar lists various configuration categories, with 'Global Profiles' expanded to show 'Server Configuration' and 'Service Provider U...'. The main content area is titled 'Server Configuration: Service Provider UDP' and features tabs for 'General', 'Authentication', 'Heartbeat', 'Ping', and 'Advanced'. The 'General' tab is active, showing a table with the following data:

IP Address / FQDN	Port	Transport
192.168.24.40	5060	UDP

The table is titled 'Trunk Server' and includes an 'Edit' button. The 'General' tab is highlighted with a red box, and the 'Service Provider U...' link in the sidebar is also highlighted with a red box.

The following screen capture shows the **Advanced** tab of the newly created **Service Provider UDP** Server Configuration Profile.

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main title is "Session Border Controller for Enterprise".

On the left, a sidebar menu lists various configuration categories: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration (highlighted), Topology Hiding, Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, and FGDN Groups.

The main content area is titled "Server Configuration: Service Provider UDP". It features a list of server profiles: CS1000, Com Manager, Session Manager, Service Provider TLS, IP Office, and Service Provider U... (highlighted). An "Add" button is located above this list.

The configuration for the selected profile is shown in a tabbed interface with tabs for General, Authentication, Heartbeat, Ping, and Advanced (highlighted). The Advanced tab contains the following settings:

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None

An "Edit" button is located at the bottom right of the configuration table.

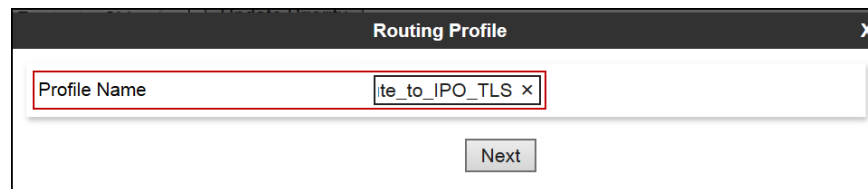
### 6.3.4 Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created; one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to Frontier Communications.

To create the inbound route, from the **Global Profiles** menu on the left-hand side (not shown):

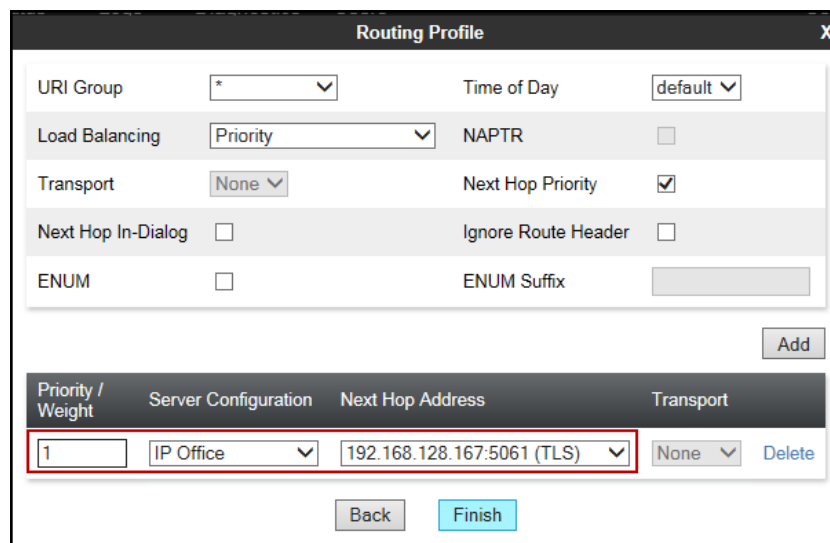
- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route\_to\_IPO\_TLS**.
- Click **Next**.



The screenshot shows a 'Routing Profile' dialog box. The 'Profile Name' field is highlighted with a red box and contains the text 'te\_to\_IPO\_TLS'. Below the field is a 'Next' button.

On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **IP Office**.
- The **Next Hop Address** is populated automatically with **192.168.128.167:5061 (TLS)** (IP Office IP address, Port and Transport).
- Click **Finish**.



The screenshot shows the 'Routing Profile' configuration screen. It includes several settings: URI Group (\*), Time of Day (default), Load Balancing (Priority), NAPTR (unchecked), Transport (None), Next Hop Priority (checked), Next Hop In-Dialog (unchecked), Ignore Route Header (unchecked), ENUM (unchecked), and ENUM Suffix. Below these settings is an 'Add' button. At the bottom, there is a table with columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport. The table contains one entry: Priority / Weight: 1, Server Configuration: IP Office, Next Hop Address: 192.168.128.167:5061 (TLS), and Transport: None. The 'Add' button is highlighted with a red box. Below the table are 'Back' and 'Finish' buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IP Office	192.168.128.167:5061 (TLS)	None

The following screen shows the newly created **Route\_to\_IPO\_TLS** Routing Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Routing' highlighted under 'Global Profiles'. The main content area is titled 'Routing Profiles: Route\_to\_IPO\_TLS'. It features a list of routing profiles on the left, including 'default', 'Route\_to\_SM', 'Route\_to\_CM', 'Route\_to\_IPO...', 'To SM from R...', 'To IPO from R...', 'Route\_to\_IPO...', 'Route\_to\_SP...', 'Route\_to\_CS1...', and 'Route\_to\_SP...'. The 'Route\_to\_IPO...' profile is selected. On the right, the configuration details for the selected profile are shown. A table lists the routing profile's parameters: Priority (1), URI Group (\*), Time of Day (default), Load Balancing (Priority), Next Hop Address (192.168.128.167), and Transport (TLS). The 'Add' button is visible in the top right corner of the configuration area.

Similarly, for the outbound route:

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route\_to\_SP\_UDP**.
- Click **Next**.

The screenshot shows a 'Routing Profile' configuration dialog box. It has a title bar with 'Routing Profile' and a close button (X). The main area contains a 'Profile Name' label and a text input field. The text 'ite\_to\_SP\_UDP x' is entered in the field. Below the input field is a 'Next' button.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **Service Provider UDP**.
- The **Next Hop Address** is populated automatically with **192.168.24.40 (UDP)** (Frontier Communications SIP Proxy public IP address, port and transport).
- Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window. It has a top section with various settings: URI Group (dropdown with '\*'), Time of Day (dropdown with 'default'), Load Balancing (dropdown with 'Priority'), NAPTR (checkbox), Transport (dropdown with 'None'), Next Hop Priority (checkbox checked), Next Hop In-Dialog (checkbox), Ignore Route Header (checkbox), ENUM (checkbox), and ENUM Suffix (text field). Below this is an 'Add' button. The bottom section is a table with columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport. The first row has values: 1, Service Provider, 192.168.24.40:5060 (UDP), and None. There are 'Back' and 'Finish' buttons at the bottom.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	192.168.24.40:5060 (UDP)	None

The following screen capture shows the newly created **Route\_to\_SP\_UDP** Routing Profile.

The screenshot shows the 'Session Border Controller for Enterprise' interface. The left sidebar has a menu with 'Global Profiles' expanded, and 'Routing' selected. The main area shows 'Routing Profiles: Route\_to\_SP\_UDP'. There is a list of routing profiles on the left, with 'Route\_to\_SP\_UDP' highlighted. The main content area shows the configuration for 'Route\_to\_SP\_UDP'. It has a table with columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The first row has values: 1, \*, default, Priority, 192.168.24.40, and UDP. There are 'Edit' and 'Delete' buttons for this row.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	192.168.24.40	UDP

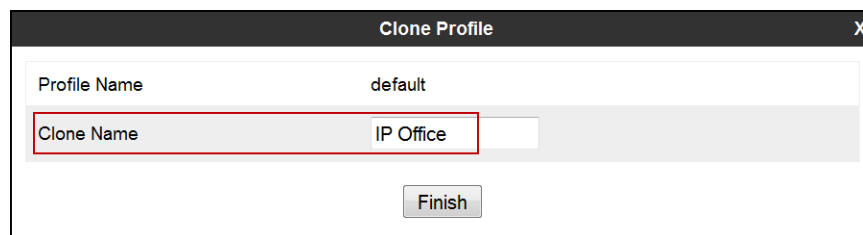
### 6.3.5 Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by IP Office and the SIP trunking service provider, allowing the call to be accepted in each case.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Clone Name**: **IP Office**.
- Click **Finish**.



The screenshot shows a 'Clone Profile' dialog box. It has a title bar with 'Clone Profile' and a close button 'X'. Inside, there are two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'IP Office'. The 'Clone Name' field is highlighted with a red border. At the bottom right, there is a 'Finish' button.



The following screen capture shows the newly added **IP Office** Topology Hiding Profile. Note that for IP Office no values were overwritten (left with default values).

**Session Border Controller for Enterprise** AVAYA

Alarms 1 Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Dashboard  
Administration  
Backup/Restore  
System Management  
▸ Global Parameters  
▾ **Global Profiles**  
    Domain DoS  
    Server Interworking  
    Media Forking  
    Routing  
    Server Configuration  
    **Topology Hiding**  
    Signaling Manipulation  
    URI Groups  
    SNMP Traps  
    Time of Day Rules  
    FGDN Groups  
    Reverse Proxy Policy  
▸ PPM Services

**Topology Hiding Profiles: IP Office**

Add Rename Clone Delete

Topology Hiding Profiles  
default  
cisco\_th\_profile  
Session\_Manager  
Service\_Provider  
Com Manager  
CS1000  
**IP Office**

Click here to add a description.

**Topology Hiding**

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

Edit

To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

- Click on **default** profile and select **Clone Profile** (not shown).
- Enter the **Clone Name: Service\_Provider**.
- Click **Finish**.

**Clone Profile** X

---

Profile Name default

Clone Name Service\_Provider

Finish

The following screen capture shows the newly added **Service\_Provider** Topology Hiding Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' expanded to show 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: Service\_Provider' and features an 'Add' button, a description field, and action buttons (Rename, Clone, Delete). A table titled 'Topology Hiding' lists the configured rules.

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

## 6.4 Domain Policies

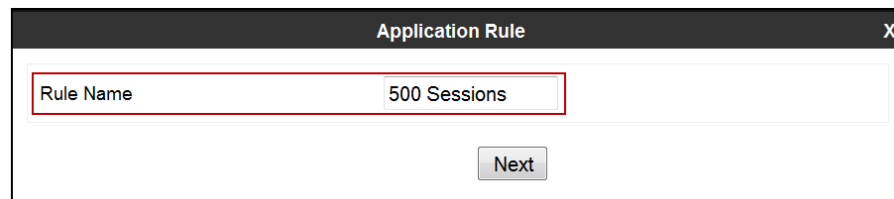
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

### 6.4.1 Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

From the menu on the left-hand side, select **Domain Policies → Application Rules** (not shown).

- Click on the **Add** button to add a new rule (not shown).
- **Rule Name:** enter the name of the profile, e.g., **500 Sessions**.
- Click **Next**.



The screenshot shows a web-based configuration window titled "Application Rule". It features a text input field with the label "Rule Name" and the value "500 Sessions". A "Next" button is positioned below the input field. The entire window is enclosed in a dark border with a close button in the top right corner.

- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of **500** was used in the sample configuration.
- Under **Video** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of **100** was used in the sample configuration.
- Click **Finish**.

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	500	500
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100

Miscellaneous

CDR Support

☒ Off  
☐ RADIUS  
☐ CDR Adjunct

RADIUS Profile

None

Media Statistics Support

☐

Call Duration

☒ Setup  
☐ Connect

RTCP Keep-Alive

☐

Back

Finish

The following screen capture shows the newly created **500 Sessions** Application Rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Domain Policies', where 'Application Rules' is highlighted. The main content area shows the configuration for the '500 Sessions' Application Rule. The rule is listed in a table with columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The '500 Sessions' rule is highlighted with a red box. Below the table, the 'Miscellaneous' section shows 'CDR Support' set to 'Off' and 'RTCP Keep-Alive' set to 'No'. The 'Edit' button is visible at the bottom right of the rule configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	500	500
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100

## 6.4.2 Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward IP Office and one toward the Service Provider.

To add a media rule in the IP Office direction, from the menu on the left-hand side, select **Domain Policies** → **Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **IPO\_SRTP**.
- Click Next.

The screenshot shows the 'Media Rule' configuration dialog box. The 'Rule Name' field is highlighted with a red box and contains the text 'IPO\_SRTP'. The 'Next' button is visible at the bottom right of the dialog box.

- Under Audio Encryption, **Preferred Format #1**, select **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous check **Capability Negotiation**.
- Click **Next**.

Media Rule
X

Audio Encryption

Preferred Format #1

SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

Leave blank to match any value.

2^

Interworking

☒

Video Encryption

Preferred Format #1

SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

Leave blank to match any value.

2^

Interworking

☒

Miscellaneous

Capability Negotiation

☒

Back

Next

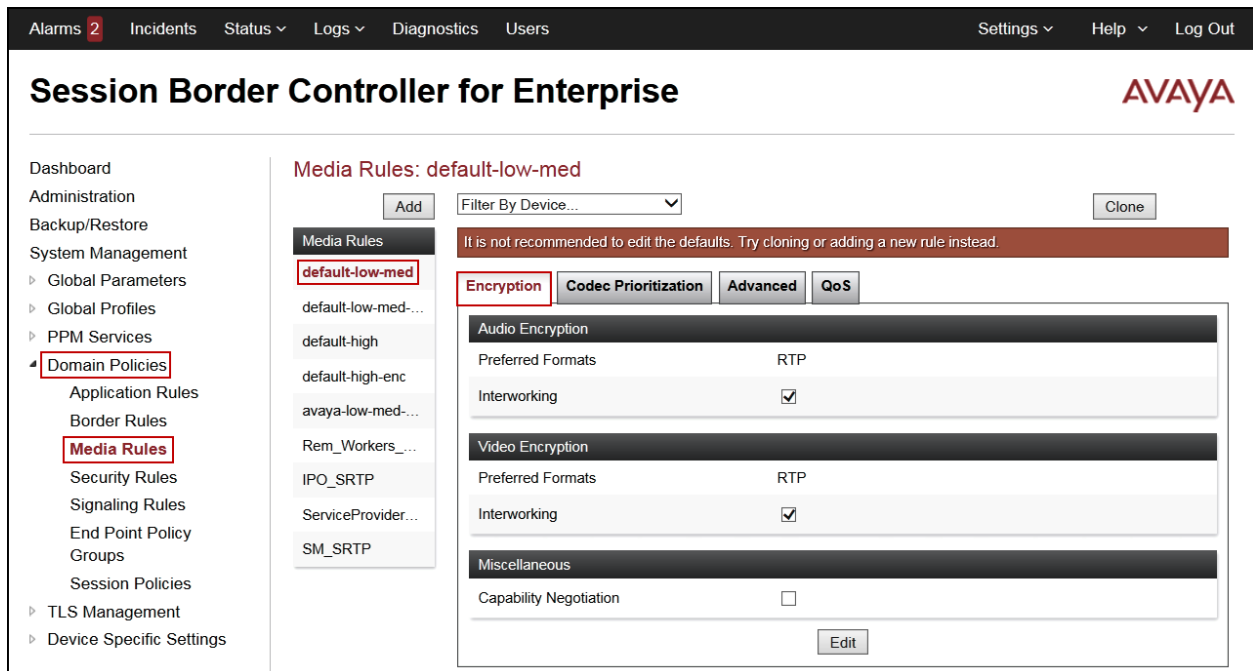
- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

The following screen capture shows the newly created **IPO\_SRTP** Media Rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' expanded and 'Media Rules' selected. The main content area is titled 'Media Rules: IPO\_SRTP' and includes an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. The 'Media Rules' list on the left includes 'default-low-med', 'default-low-med-...', 'default-high', 'default-high-enc', 'avaya-low-med-...', 'Rem\_Workers\_...', 'IPO\_SRTP' (highlighted), 'ServiceProvider...', and 'SM\_SRTP'. The configuration for 'IPO\_SRTP' is shown with tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing 'Audio Encryption' and 'Video Encryption' sections. Both sections have 'Preferred Formats' set to 'SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80 RTP', 'Encrypted RTCP' unchecked, 'MKI' unchecked, 'Lifetime' set to 'Any', and 'Interworking' checked. The 'Miscellaneous' section at the bottom has 'Capability Negotiation' checked. An 'Edit' button is located at the bottom right of the configuration area.

In the Service Provider direction, the existing **default-low-med** Media Rule was used.

The following screen capture shows the existing **default-low-med** Media Rule.



### 6.4.3 End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups** (not shown).

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name: IPO SRTP.**
- Click **Next**.





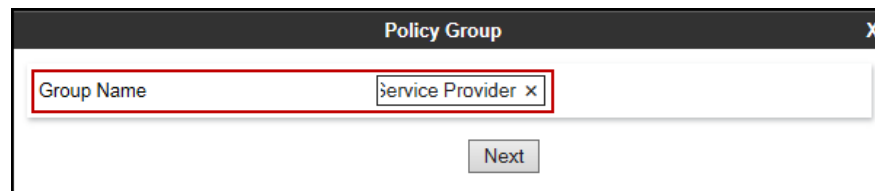
- **Application Rule: 500 Sessions.**
- **Border Rule: default.**
- **Media Rule: IPO\_SRTP.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Click Finish.**

The following screen capture shows the newly created **IPO\_SRTP** End Point Policy Group.

Order	Application	Border	Media	Security	Signaling	RTCP Mon Gen	
1	500 Sessions	default	IPO_SRTP	default-low	default	<input type="checkbox"/>	Edit

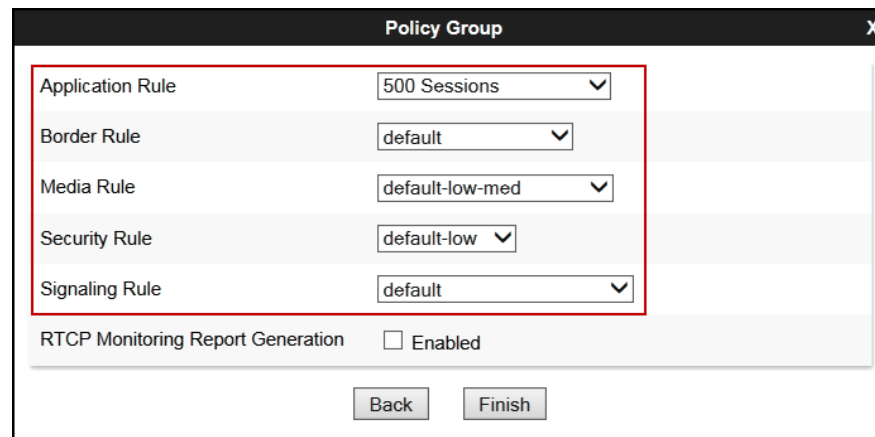
Similarly, to create an End Point Policy Group toward the Service Provider.

- Click on the **Add** button to add a new policy group (not shown).
- **Group Name: Service Provider.**
- Click **Next**.



The screenshot shows a 'Policy Group' dialog box. The title bar is 'Policy Group' with a close button 'X'. Inside, there is a text input field labeled 'Group Name' which contains the text 'Service Provider x'. Below the input field is a 'Next' button.

- **Application Rule: 500 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- Click **Finish**.



The screenshot shows the 'Policy Group' dialog box with several dropdown menus. The 'Application Rule' is set to '500 Sessions', 'Border Rule' to 'default', 'Media Rule' to 'default-low-med', 'Security Rule' to 'default-low', and 'Signaling Rule' to 'default'. Below these is a checkbox for 'RTCP Monitoring Report Generation' which is unchecked. At the bottom are 'Back' and 'Finish' buttons.

The following screen capture shows the newly created **Service Provider** End Point Policy Group.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various configuration categories, with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: Service Provider' and features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-s...', 'avaya-def-high-s...', and 'Enterprise'. The 'Service Provider' group is selected. The right-hand pane shows the configuration for the 'Service Provider' group, including a table with columns for Order, Application, Border, Media, Security, Signaling, and RTCP Mon Gen. The table contains one row with the following values: Order 1, Application 500 Sessions, Border default, Media default-low-med, Security default-low, Signaling default, and RTCP Mon Gen (checkbox). The 'Edit' button is visible next to the row.

Session Border Controller for Enterprise

AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
‣ PPM Services  
‣ **Domain Policies**  
‣ Application Rules  
‣ Border Rules  
‣ Media Rules  
‣ Security Rules  
‣ Signaling Rules  
‣ **End Point Policy Groups**  
‣ Session Policies  
‣ TLS Management  
‣ Device Specific Settings

Policy Groups: Service Provider

Add Filter By Device... Rename Clone Delete

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	RTCP Mon Gen	
1	500 Sessions	default	default-low-med	default-low	default	<input type="checkbox"/>	Edit

Service Provider

## 6.5 Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc., are defined here.

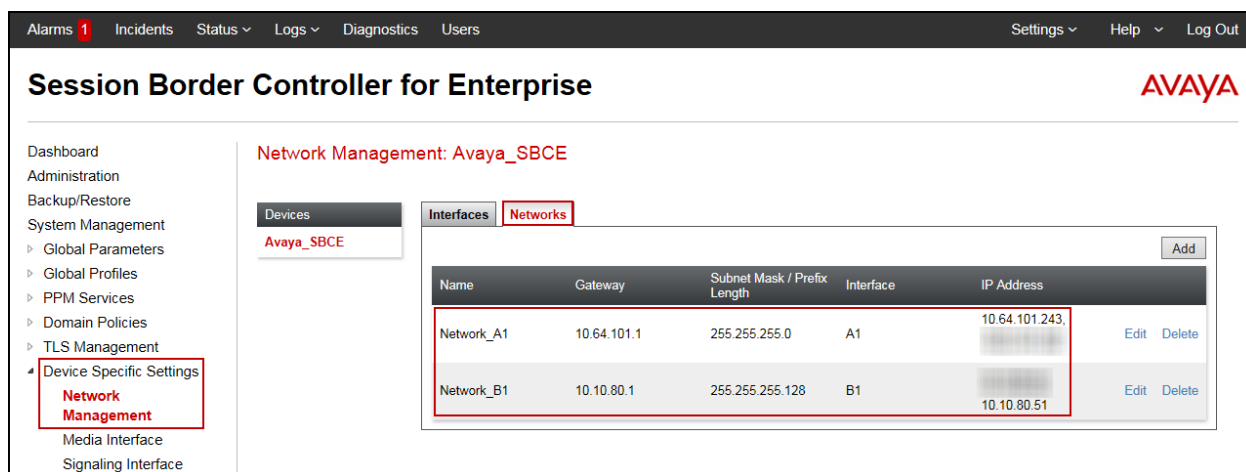
### 6.5.1 Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** under **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Networks** tab.

In the event that changes need to be made to the network configuration information, they can be entered here.

Use **Figure 1** as reference for IP address assignments.

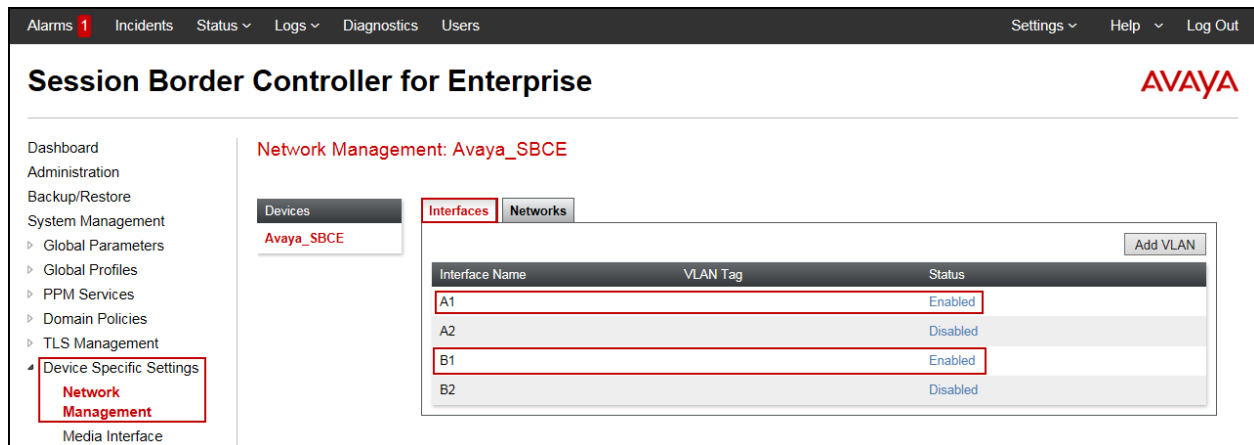
**Note:** Only the highlighted items were created for the compliance test, and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.



The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the AVAYA logo. The left sidebar lists various management options, with 'Device Specific Settings' and 'Network Management' highlighted. The main content area is titled 'Network Management: Avaya\_SBCE' and shows a table of network configurations. The table has columns for Name, Gateway, Subnet Mask / Prefix Length, Interface, and IP Address. Two networks are listed: Network\_A1 and Network\_B1. The IP addresses are highlighted with a red box.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Network_A1	10.64.101.1	255.255.255.0	A1	10.64.101.243	Edit Delete
Network_B1	10.10.80.1	255.255.255.128	B1	10.10.80.51	Edit Delete

On the **Interfaces** tab, click the **Status** for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **Disabled**, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.



## 6.5.2 Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving and arriving at the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface** (not shown).

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** **Private\_med**.
- Under **IP Address** select: **Network\_A1 (A1, VLAN 0)**.
- Select **IP Address:** **10.64.101.243** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office)
- **Port Range:** **35000-40000**.
- Click **Finish**.

Name	Private_med
IP Address	Network_A1 (A1, VLAN 0) 10.64.101.243
Port Range	35000 - 40000

Finish

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** **Public\_med**.
- Under **IP Address** select: **Network\_B1 (B1, VLAN 0)**.  
Select **IP Address: 10.10.80.51** (Outside public IP Address of the Avaya SBCE, toward Frontier Communications).
- **Port Range:** **35000-40000**.
- Click **Finish**.

The following screen capture shows the newly created Media Interfaces.

Name	Media IP Network	Port Range	Edit	Delete
Private_med	10.64.101.243 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Public_med	10.10.80.51 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

### 6.5.3 Signaling Interface

To create the Signaling Interface toward IP Office, from the **Device Specific** menu on the left hand side, select **Signaling Interface** (not shown).

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name:** **Private\_sig**.
- Under **IP Address** select: **Network\_A1 (A1, VLAN 0)**.
- Select **IP Address:** **10.64.101.243** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office).
- **TLS Port:** **5061**.
- Under **TLS Profile** select the appropriate TLS Profile.
- Click **Finish**.

**Add Signaling Interface** X

Name: Private\_sig

IP Address: Network\_A1 (A1, VLAN 0) ▼  
10.64.101.243 ▼

TCP Port:   
Leave blank to disable

UDP Port:   
Leave blank to disable

TLS Port: 5061  
Leave blank to disable

TLS Profile: NewRemoteWorkerServerProfile ▼

Enable Shared Control: ☐

Shared Control Port:

Finish

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name:** **Public\_sig**.
- Under **IP Address** select: **Network\_B1 (B1, VLAN 0)**.
- Select **IP Address:** **10.10.80.51** (Outside/public IP Address of the Avaya SBCE, toward Frontier Communications).
- **UDP Port:** **5060**.
- Click **Finish**.

**Add Signaling Interface** X

Name

IP Address

TCP Port  Leave blank to disable

UDP Port  Leave blank to disable

TLS Port  Leave blank to disable

TLS Profile

Enable Shared Control ☐

Shared Control Port

**Finish**



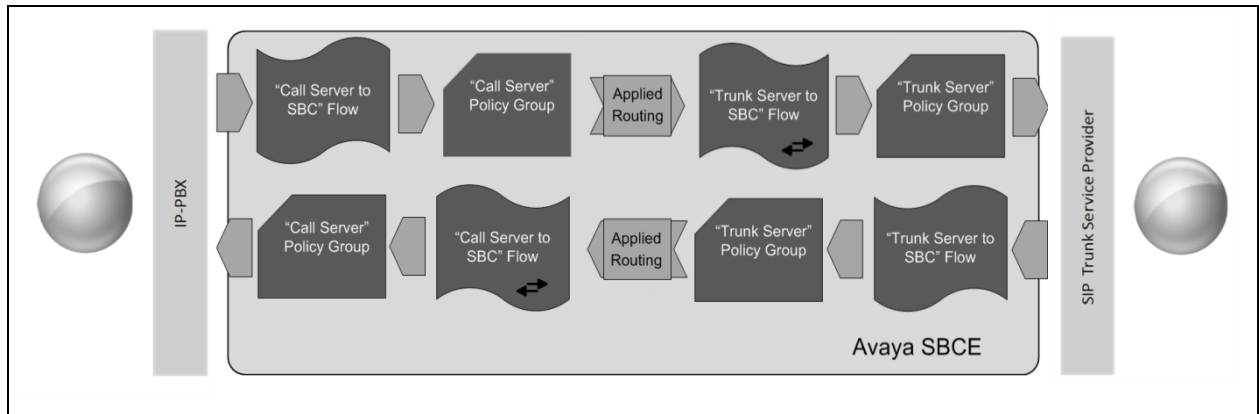
The following screen capture shows the newly created Signaling Interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Device Specific Settings' and its sub-item 'Signaling Interface' highlighted. The main content area is titled 'Signaling Interface: Avaya\_SBCE' and features a sub-tab 'Signaling Interface'. A warning message states that modifying or deleting an existing signaling interface requires an application restart. Below this is a table listing the configured signaling interfaces.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	10.64.101.243 Network_A1 (A1, VLAN 0)	---	---	5061	NewRemoteWorkerServerProfile	Edit Delete
Public_sig	10.10.80.51 Network_B1 (B1, VLAN 0)	---	---	5060	None	Edit Delete

## 6.5.4 End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward Frontier Communications, from the **Device Specific Settings** menu, select **End Point Flows** (not shown), then the **Server Flows** tab. Click **Add** (not shown).

- **Name:** SIP\_Trunk\_Flow\_UDP.
- **Server Configuration:** Service Provider UDP.
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** Private\_sig.
- **Signaling Interface:** Public\_sig.
- **Media Interface:** Public\_med.
- **Secondary Media Interface:** None.
- **End Point Policy Group:** Service Provider.
- **Routing Profile:** Route\_to\_IPO\_TLS (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** Service\_Provider.
- **Signaling Manipulation Script:** None.
- **Remote Branch Office:** Any.
- Click **Finish**.

Edit Flow: SIP_Trunk_Flow_UDP	
Flow Name	SIP_Trunk_Flow_UDP
Server Configuration	Service Provider UDP
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
Secondary Media Interface	None
End Point Policy Group	Service Provider
Routing Profile	Route_to_IPO_TLS
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

To create the call flow toward IP Office, click **Add** (not shown).

- **Name:** IP\_Office\_Flow.
- **Server Configuration:** IP Office.
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** Public\_sig.
- **Signaling Interface:** Private\_sig.
- **Media Interface:** Private\_med.
- **Secondary Media Interface:** None.
- **End Point Policy Group:** IPO SRTP.
- **Routing Profile:** Route\_to\_SP\_UDP (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** IP Office.
- **Signaling Manipulation Script:** None.
- **Remote Branch Office:** Any.
- Click **Finish**.

**Edit Flow: IP\_Office\_Flow**

Flow Name	IP_Office_Flow
Server Configuration	IP Office
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
Secondary Media Interface	None
End Point Policy Group	IPO SRTP
Routing Profile	Route_to_SP_UDP
Topology Hiding Profile	IP Office
Signaling Manipulation Script	None
Remote Branch Office	Any

**Finish**

The following screen capture shows the newly created **End Point Flows**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms (2), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo.

On the left sidebar, the "Device Specific Settings" menu is expanded, and "End Point Flows" is selected. The main content area is titled "End Point Flows: Avaya\_SBCE". It features two tabs: "Subscriber Flows" and "Server Flows", with "Server Flows" being the active tab.

Below the tabs, there is a section for "Server Configuration: IP Office". It includes an "Add" button and a table with the following columns: Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The table contains one row with the following values: Priority 1, Flow Name IP\_Office\_Flow, URI Group \*, Received Interface Public\_sig, Signaling Interface Private\_sig, End Point Policy Group IPO SRTTP, and Routing Profile Route\_to\_SP\_UDP. There are also "View", "Clone", "Edit", and "Delete" buttons for this row.

Below this, there is a section for "Server Configuration: Service Provider UDP". It also includes an "Add" button and a table with the same columns. The table contains one row with the following values: Priority 1, Flow Name SIP\_Trunk\_Flow\_UDP, URI Group \*, Received Interface Private\_sig, Signaling Interface Public\_sig, End Point Policy Group Service Provider, and Routing Profile Route\_to\_IPO\_TLS. There are also "View", "Clone", "Edit", and "Delete" buttons for this row.

## 7. Frontier Communications SIP Trunking Service Configuration

To use Frontier Communications SIP Trunking service, a customer must request the service from Frontier Communications using the established sales processes. The process can be started by contacting Frontier Communications via the corporate web site at: <https://frontier.com/enterprise> and requesting information.

During the signup process, Frontier Communications and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Frontier Communications network.

Frontier Communications is responsible for the configuration of Frontier Communications SIP Services. The customer will need to provide a public IP address to be used to reach the Avaya SBCE at the enterprise. In the case of the compliance test, this is the outside or public IP address of the Avaya SBCE (B1 interface).

Frontier Communications will provide the customer the necessary information to configure Avaya IP Office and the Avaya SBCE following the steps discussed in the previous sections, including:

- Public IP address of Frontier Communications SIP Proxy server.
- DID numbers, etc.

## 8. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting tips that can be used to troubleshoot the solution.

### 8.1 Verification Steps

The following steps may be used to verify the configuration:

- Verify that endpoints at the enterprise site can place calls to PSTN and that calls remain active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from PSTN and that calls can remain active for more than 35 seconds.
- Verify that the user on the PSTN side can end an active call by hanging up.
- Verify that an Avaya endpoint at the enterprise site can end an active call by hanging up.

### 8.2 Protocol Traces

The following SIP message headers are inspected using a sniffer trace analysis tool:

- Request-URI: Verify the request number and SIP domain.
- From: Verify the display name and display number.
- To: Verify the display name and display number.
- P-Asserted-Identity: Verify the display name and display number.
- Privacy: Verify privacy masking with “user, id”.
- Diversion: Verify the display name and display number.

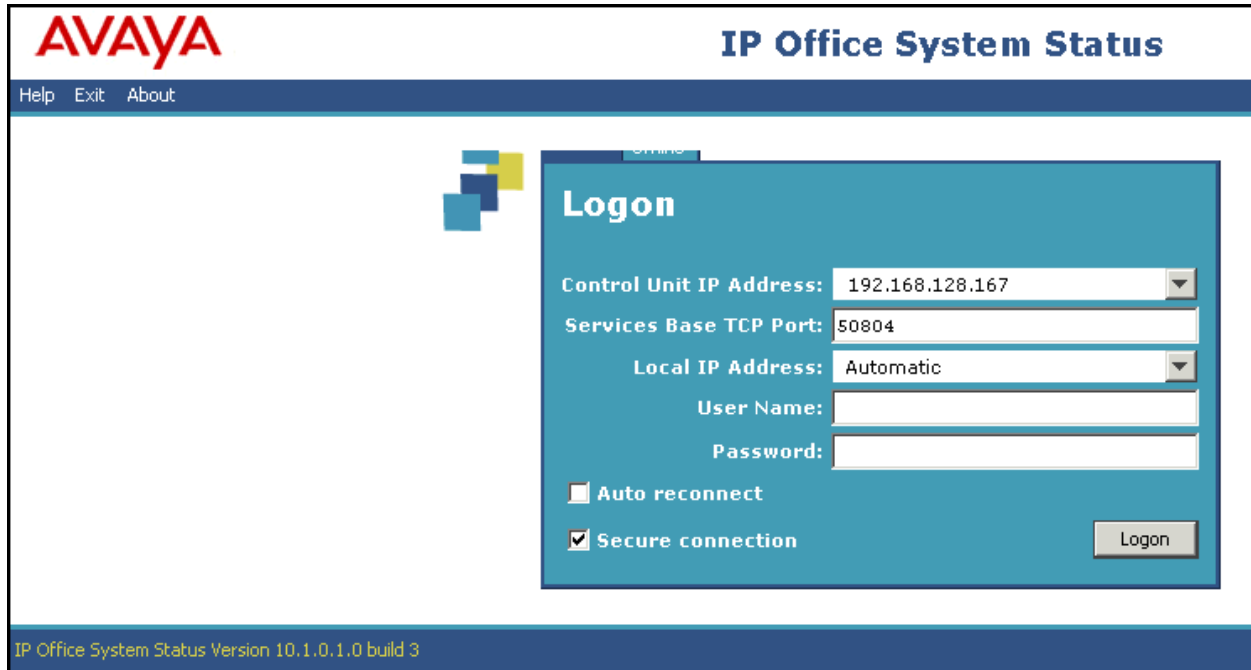
The following attributes in SIP message body are inspected using a sniffer trace analysis tool:

- Connection Information (c line): Verify IP addresses of near end and far end endpoints.
- Time Description (t line): Verify session timeout value of near end and far end endpoints.
- Media Description (m line): Verify audio port, codec, DTMF event description.
- Media Attribute (a line): Verify specific audio port, codec, ptime, send/ receive ability, DTMF events.

### 8.3 IP Office System Status

The following steps can also be used to verify the configuration.

Use the Avaya IP Office **System Status** application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed, log in with the proper credentials.



The screenshot shows the Avaya IP Office System Status application window. The title bar reads "IP Office System Status". The menu bar includes "Help", "Exit", and "About". The main window features a blue header with the "AVAYA" logo on the left and the title "IP Office System Status" on the right. Below the header, there is a large white area with a blue sidebar on the left containing a "Logon" button. The main content area is a blue box with the "Logon" title. It contains the following fields and controls:

- Control Unit IP Address: 192.168.128.167 (dropdown menu)
- Services Base TCP Port: 50804 (text field)
- Local IP Address: Automatic (dropdown menu)
- User Name: (text field)
- Password: (text field)
- ☐ Auto reconnect
- ☒ Secure connection
- Logon (button)

At the bottom of the window, the version information "IP Office System Status Version 10.1.0.1.0 build 3" is displayed.



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

Avaya IP Office System Status - 00E00706530F (192.168.128.167) - IP500 V2 10.1.0.1.0 build 3

# AVAYA

## IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (10)
- Extensions (25)
- Trunks (5)
  - Line: 1
  - Line: 2
  - Line: 17
  - Line: 18
  - Line: 19
- Active Calls
- Resources
- Voicemail
- IP Networking
- Locations

**Status** Utilization Summary Alarms

### SIP Trunk Summary

Line Service State: In Service

Peer Domain Name: sip://10.64.101.243

Resolved Address: 10.64.101.243

Line Number: 17

Number of Administered Channels: 10

Number of Channels in Use: 0

Administered Compression: G711 Mu, G729 A

Enable Faststart: Off

Silence Suppression: Off

Media Stream: Best Effort

Layer 4 Protocol: TLS

SIP Trunk Channel Licenses: 128

SIP Trunk Channel Licenses in Use: 0

SIP Device Features:

0%

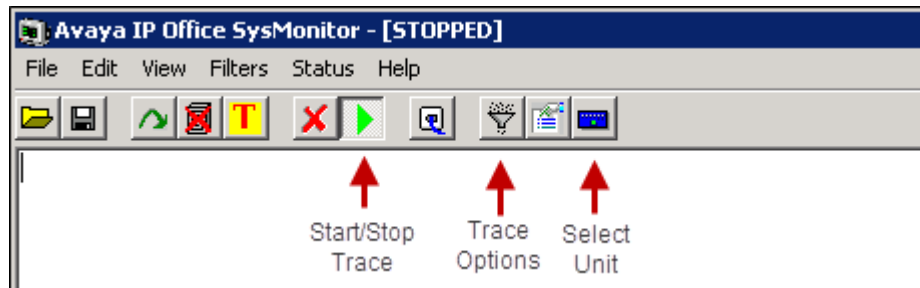
Channel Number	URI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call
1			Idle	00:02:17					
2			Idle	00:02:17					
3			Idle	00:02:17					
4			Idle	00:02:17					
5			Idle	00:02:17					
6			Idle	00:02:17					
7			Idle	00:02:17					
8			Idle	00:02:17					
9			Idle	00:02:17					
10			Idle	00:02:17					

2. Select the **Alarms** tab and verify that no alarms are active on the SIP Line.

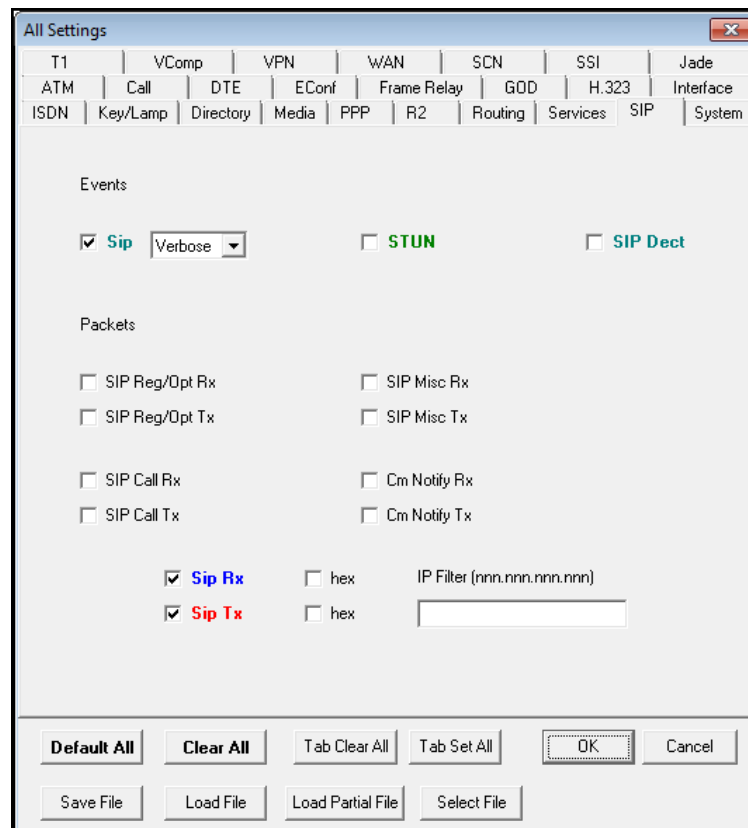
The screenshot displays the Avaya IP Office System Status web interface. The left-hand navigation pane shows a tree structure with 'System' expanded, containing 'Alarms (15)', 'Extensions (27)', and 'Trunks (5)'. Under 'Trunks (5)', 'Line: 17' is selected and highlighted with a red box. The main content area has three tabs: 'Status', 'Utilization Summary', and 'Alarms', with 'Alarms' being the active tab. The title of the active tab is 'Alarms for Line: 17 SIP sip://10.64.101.243'. Below the title is a table with three columns: 'Last Date Of Error', 'Occurrences', and 'Error Description'. The table is currently empty. At the bottom of the main content area, there are several buttons: 'Ping', 'Clear', 'Clear All', 'Graceful Shutdown', 'Force Out of Service', 'Print...', and 'Save As...'. The bottom status bar shows the time '4:00:08 PM' and the status 'Online'.

## 8.4 IP Office Monitor

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where Avaya IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and select the IP address of the IP Office system under verification.



Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting to the desired color.



## 8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)

There are several links and menus located on the taskbar at the top of the screen of the web interface that can be used for diagnostic and troubleshooting.

**Alarms:** Provides information about the health of the Avaya SBCE.

**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.

Information	
System Time	04:03:49 PM EST
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	02/19/2018 13:01:56 EST
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya_SBCE : Heartbeat Successful, Server is UP
Avaya_SBCE : Heartbeat Failed, Server is Down
Avaya_SBCE : Timeout while contacting DNS serversip.clearcom.mx
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : Timeout while contacting DNS serversip.clearcom.mx

Notes: No notes found.

The following screen shows the **Alarm Viewer** page.

**Alarm Viewer**

**Alarms**

ID	Details	State	Time	Device
No alarms found for this device.				

Clear Selected Clear All

**Incidents:** Provides detailed reports of anomalies, errors, policies violations, etc.

**Session Border Controller for Enterprise** AVAYA

**Dashboard**

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

**Information**

System Time	04:03:49 PM EST	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	02/19/2018 13:01:56 EST	
Failed Login Attempts	0	

**Installed Devices**

EMS
Avaya_SBCE

**Active Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

Avaya_SBCE : Heartbeat Successful, Server is UP
Avaya_SBCE : Heartbeat Failed, Server is Down
Avaya_SBCE : Timeout while contacting DNS serversip.clearcom.mx
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : Timeout while contacting DNS serversip.clearcom.mx

**Notes**

No notes found.

The following screen shows the Incident Viewer page.

**Incident Viewer** AVAYA

Device: All Category: All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 2001.

Type	ID	Date	Time	Category	Device	Cause
Message Dropped	759537161742432	2/19/18	4:05 PM	Policy	Avaya_SBCE	No Subscriber Flow Matched
Server Heartbeat	759536745834278	2/19/18	3:51 PM	Policy	Avaya_SBCE	Heartbeat Successful, Server is UP

<< < 1 2 3 4 5 > >>

**Diagnostics:** This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

The following screen shows the Diagnostics page with the results of a ping test.

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left sidebar contains a menu with 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'PPM Services', 'Domain Policies', 'TLS Management', 'Device Specific Settings' (highlighted), 'Network Management', 'Media Interface', 'Signaling Interface', 'End Point Flows', 'Session Flows', 'DMZ Services', 'TURN/STUN Service', 'SNMP', 'Syslog Management', 'Advanced Options', 'Troubleshooting' (highlighted), 'Debugging', 'Trace' (highlighted), and 'DoS Learning'. The main content area is titled 'Trace: Avaya\_SBCE' and features two tabs: 'Devices' and 'Avaya\_SBCE'. The 'Packet Capture' tab is active, showing a 'Packet Capture Configuration' dialog box. The dialog box has the following fields: 'Status' (Ready), 'Interface' (A1), 'Local Address' (All), 'Remote Address' (\*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (10000), and 'Capture Filename' (Wireshark\_Capture\_1.pcap). The 'Start Capture' and 'Clear' buttons are at the bottom of the dialog box.

Packet Capture Configuration	
Status	Ready
Interface	A1
Local Address <small>(IP[:Port])</small>	All
Remote Address <small>*, *:Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	Wireshark_Capture_1.pcap

Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand navigation menu lists various system management options, with "Device Specific Settings" and "Troubleshooting" highlighted. Under "Troubleshooting", the "Trace" option is selected. The main content area is titled "Trace: Avaya\_SBCE" and features two tabs: "Packet Capture" and "Captures". The "Captures" tab is active, showing a table of captured files. The table has columns for File Name, File Size (bytes), Last Modified, and a Delete button. Two files are listed, both captured on October 24, 2016, at 5:37 PM EDT.

File Name	File Size (bytes)	Last Modified	Delete
Wireshark_Capture_1_20161024173718.pcap	135,168	October 24, 2016 5:37:35 PM EDT	Delete
Wireshark_Capture_1_20161024173655.pcap	8,192	October 24, 2016 5:37:06 PM EDT	Delete



## 9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 10.1 and the Avaya Session Border Controller for Enterprise Release 7.2 to support Frontier Communications SIP Trunking Service, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

## 10. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya IP Office, including the following, is available at:

<http://support.avaya.com/>

- [1] *Avaya IP Office Platform Solution Description, Release 10.1, Issue 1.2, September 2017.*
- [2] *Avaya IP Office Platform Feature Description, Release 10.1, Issue 1a, September 2017.*
- [3] *Deploying Avaya IP Office Platform IP500 V2, Document Number 15-601042, Issue 32I, December 19, 2017.*
- [4] *Administering Avaya IP Office Platform with Manager, Release 10.1, Issue 14, July 2017*
- [5] *Using Avaya Communicator for Windows on IP Office, Release 10, August 2016.*
- [6] *Administering Avaya Communicator on IP Office, Release 10.0, Issue 01.01, August 2016.*
- [7] *Deploying Avaya Session Border Controller for Enterprise, Release 7.2.1, Issue 6, January 2018.*
- [8] *Administering Avaya Session Border Controller for Enterprise, Release 7.2.1, Issue 8, February 2018.*
- [9] *Troubleshooting and Maintaining Avaya session Border Controller for Enterprise, Release 7.2.1, Issue 2, November 2017.*
- [10] *Avaya IP Office Platform Security Guidelines, Release 10. Issue 01e, May 8, 2017.*
- [11] *IP Office Technical Bulletin number 175 (<http://www.ipofficeinfo.com/TechBulletins/tb175.pdf>)*

Additional Avaya IP Office documentation can be found at:

<http://marketingtools.avaya.com/knowledgebase/>

---

**©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](mailto:devconnect@avaya.com).