



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise Release 7.0 to support Cincinnati Bell Business 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 9.1 and Avaya Session Border Controller for Enterprise Release 7.0 to support Cincinnati Bell Business 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.

Cincinnati Bell Business SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Cincinnati Bell's 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.

Cincinnati Bell is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction.....	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	6
4. Equipment and Software Validated	9
5. Configure IP Office	10
5.1 Licensing.....	10
5.2 System.....	11
5.2.1 System - LAN1 Tab	11
5.2.2 System - Telephony Tab	14
5.2.3 System - Twinning Tab.....	15
5.2.4 System - Codecs Tab.....	16
5.3 IP Route	17
5.4 SIP Line	18
5.4.1 Importing a SIP Line Template.....	18
5.4.2 Creating a SIP Trunk from an XML Template	22
5.4.3 SIP Line - SIP Line Tab.....	24
5.4.4 SIP Line - Transport Tab	25
5.4.5 SIP Line - SIP URI Tab	26
5.4.6 SIP Line - VoIP Tab	27
5.4.7 SIP Line – T.38 Fax Tab.....	28
5.4.8 SIP Line – SIP Advanced Tab	29
5.5 Extension.....	30
5.6 Users	32
5.7 Incoming Call Route	36
5.8 Outbound Call Routing	38
5.8.1 Short Codes and Automatic Route Selection.....	38
5.9 Save Configuration	40
6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).....	41
6.1 Log in Avaya SBCE.....	41
6.2 Global Profiles	44
6.2.1 Server Interworking – Avaya-IPO	44
6.2.2 Server Interworking - SP-General.....	48
6.2.3 Server Configuration.....	52
6.2.4 Routing Profiles	58
6.2.5 Topology Hiding.....	61
6.3 Domain Policies	65
6.3.1 Application Rules.....	65
6.3.2 End Point Policy Groups.....	66
6.4 Device Specific Settings	70
6.4.1 Network Management.....	70
6.4.2 Media Interface	72
6.4.3 Signaling Interface	74
6.4.4 End Point Flows	77

7. Cincinnati Bell Business SIP Trunking Service Configuration	81
8. Verification and Troubleshooting	82
8.1 Verification Steps.....	82
8.2 Protocol Traces	82
8.3 IP Office System Status	83
8.4 IP Office Monitor.....	86
8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)	87
9. Conclusion	92
10. References	93

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Cincinnati Bell 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 500v2 Release 9.1 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 7.0 (hereafter referred to as Avaya SBCE), Avaya Communicator for Windows and Avaya Deskphones, including SIP, H.323, digital, and analog.

The Cincinnati Bell Business 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” or “Cincinnati Bell” will be used interchangeable 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 Cincinnati Bell Business 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.

2.1 Interoperability Compliance Testing

To verify the Cincinnati Bell Business 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 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 telephone 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.
- Dialing plans including long distance, outbound toll-free, etc.
- Caller ID presentation and Caller ID restriction.
- 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.
- Codec G.711MU and G.729(a) (Cincinnati Bell supported audio codec).
- Proper response to no matching codecs.
- T.38 fax.
- G.711 fax pass-through.
- 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:

- Inbound toll-free calls and 911 emergency calls are supported but were not tested as part of the compliance test.
- Notification of intermediate call states (via NOTIFY messages) for a call that is redirected with a REFER message.

2.2 Test Results

Interoperability testing with Cincinnati Bell Business SIP Trunking service was successfully completed with the exception of observations/limitations described below:

- **No ring back tone on PSTN stations after Blind Transfers to the PSTN:** When a PSTN endpoint (P1) calls an IP Office H.323 station and that station blind transfers the call to another PSTN endpoint (P2), no ring back tone is heard by the calling party (P1) while P2 is ringing. This issue is only seen on IP Office H.323 endpoints, this issue is not seen on IP Office SIP endpoints. This issue is under investigation.
- **No matching codec on outbound calls:** If an unsupported audio codec is received by Cincinnati Bell on the SIP Trunk (e.g., G.711A), Cincinnati Bell will respond with “503 Service Unavailable” instead of “488 Not Acceptable Here”. The user will hear a series of tones. This issue does not have any user impact and should not be seen since the codecs will be matched during the installation. It is listed here simply as an observation.
- **Operator –assisted calls:** Operator-assisted calls (0 + 10 digits) are routed the same as direct dialed calls (1 + 10 digits).

2.3 Support

For support on Cincinnati Bell Business SIP Trunking service visit the corporate Web page at: https://www.cincinnati-bell.com/customer_support/

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 Cincinnati Bell Business 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 Voicemail Pro.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x0 Series H.323 IP Deskphones.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 1100 Series SIP IP Deskphones.
- Avaya Communicator for Windows.
- Avaya 1408 Digital Telephones.
- Avaya 9508 Digital Telephones.

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 500v2 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 Cincinnati Bell's network via the public Internet.

For inbound calls, the calls flowed from the PSTN to Cincinnati Bell's 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 Cincinnati Bell's network.

The transport protocol between the Avaya SBCE and Cincinnati Bell, across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and IP Office, across the enterprise private IP network, is also SIP over UDP.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Cincinnati Bell (refer to **Section 5.8**). The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network. Since Cincinnati Bell is a U.S. based company, a country member of the North American Numbering Plan (NANP), the users dialed 7 or 10 digits for local calls, and 11 (1 + 10) digits for other calls between the NANP.

In an actual customer configuration, the enterprise site may also include additional network components between Cincinnati Bell 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.

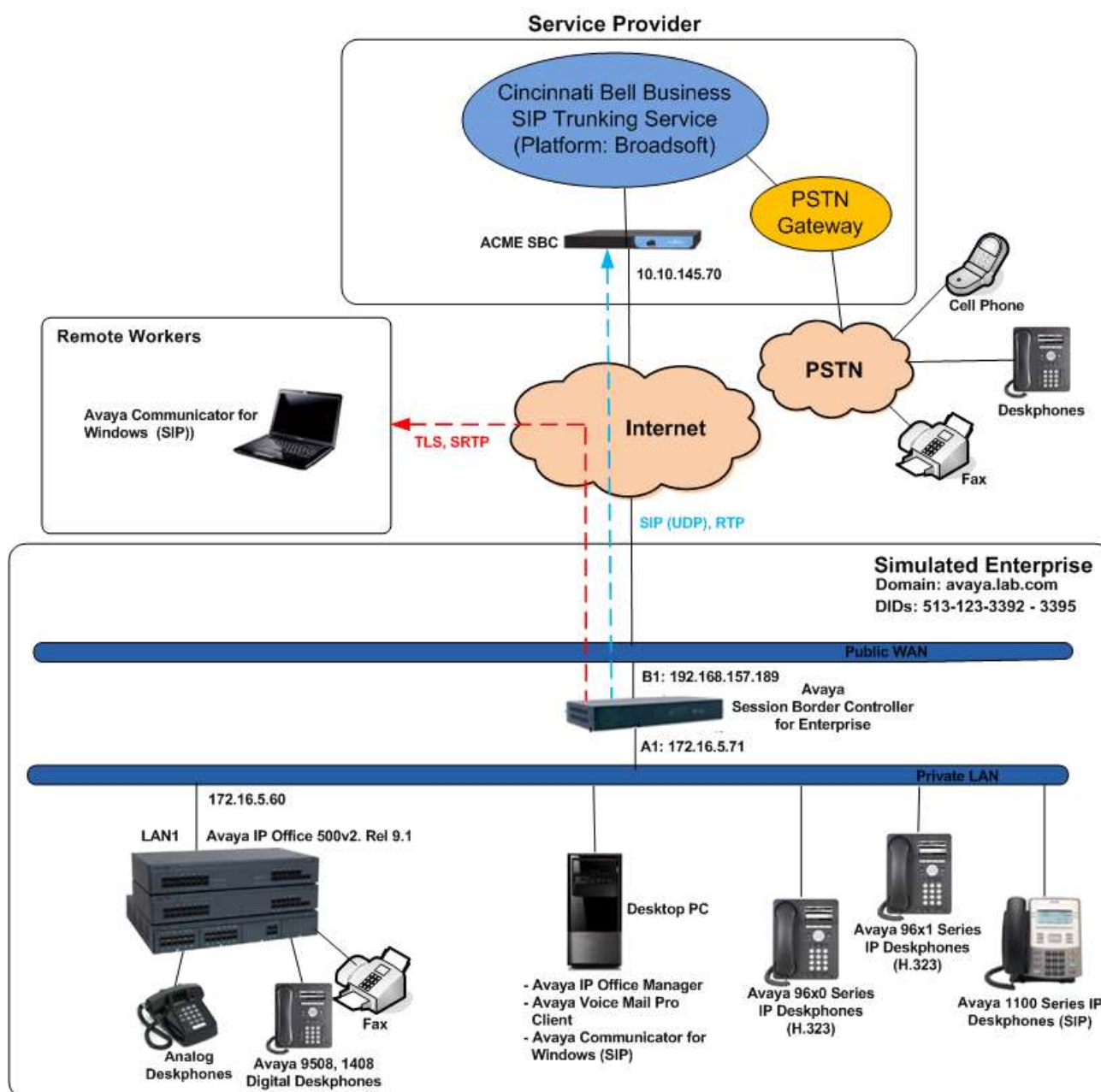


Figure 1: Avaya Interoperability Test Lab Configuration.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	9.1.6.0 Build 153
Avaya IP Office DIG DCPx16 V2	9.1.6.0 Build 153
Avaya IP Office Manager	9.1.6.0 Build 153
Avaya Voicemail Pro Client	9.1.6.0 Build 2
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.0.1-03-8739
Avaya 96x0 IP Deskphones (H.323)	Avaya one-X® Deskphone Edition S3.230A
Avaya 96x1 Series IP Deskphones (H.323)	6.6029
Avaya 1120E IP Deskphones (SIP)	SIP1120e Ver. 04.04.18.00
Avaya Communicator for Windows	2.0.3.40
Avaya Digital Deskphones 1408	40.0
Avaya Digital Deskphones 9508	0.55
Lucent Analog Phone	--
Cincinnati Bell	
Broadworks	R20
Acme Packet 6300 Series SBC	ScZ7.2.0

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 without T.38 Fax Service.

5. Configure IP Office

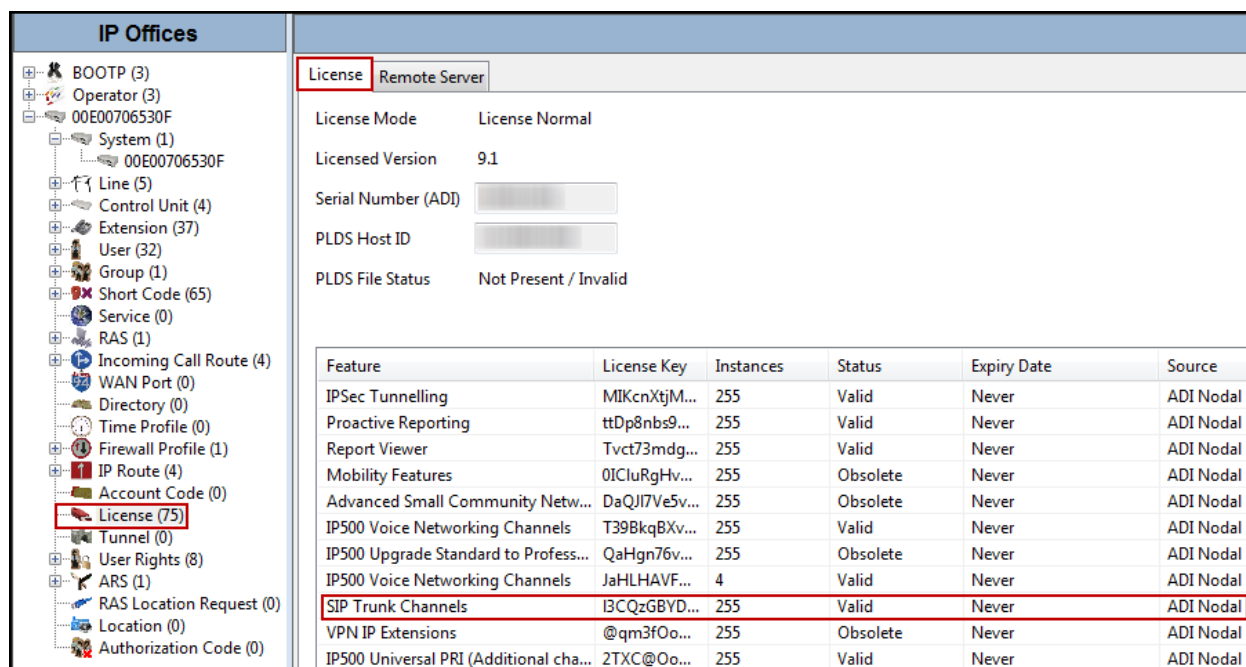
This section describes the IP Office configuration required to interwork with Cincinnati Bell Business SIP Trunking service. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP 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.



Feature	License Key	Instances	Status	Expiry Date	Source
IPSec Tunneling	MIKcnXtjM...	255	Valid	Never	ADI Nodal
Proactive Reporting	ttDp8nbs9...	255	Valid	Never	ADI Nodal
Report Viewer	Tvct73mdg...	255	Valid	Never	ADI Nodal
Mobility Features	0ICluRgHv...	255	Obsolete	Never	ADI Nodal
Advanced Small Community Netw...	DaQI7Ve5v...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	T39BkqBXv...	255	Valid	Never	ADI Nodal
IP500 Upgrade Standard to Profess...	QaHgn76v...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	JaHLHAVF...	4	Valid	Never	ADI Nodal
SIP Trunk Channels	l3CQzGBYD...	255	Valid	Never	ADI Nodal
VPN IP Extensions	@qm3fOo...	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional cha...	2TXC@Oo...	255	Valid	Never	ADI 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., **172.16.5.60**.
- 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 is the 'IP Offices' navigation pane, showing a tree structure with 'System (1)' selected, and its sub-item '00E00706530F' highlighted with a red box. The main area on the right shows the 'LAN1' tab selected, with 'LAN Settings' as the active sub-tab. The 'IP Address' field is set to '172 . 16 . 5 . 60' and the 'IP Mask' field is set to '255 . 255 . 255 . 0', both fields are enclosed in a red rectangular box. Other visible settings include 'Primary Trans. IP Address' set to '0 . 0 . 0 . 0', 'RIP Mode' set to 'None', 'Enable NAT' checkbox, 'Number Of DHCP IP Addresses' set to '200', and 'DHCP Mode' with 'Disabled' selected. An 'Advanced' button is located at the bottom right of the settings area.

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.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Cincinnati Bell.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **Domain Name**.
- Verify the **UDP Port** and **TCP Port** numbers under **Layer 4 Protocol** are set to **5060**.
- 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**, **Periodic Timeout to 30**, and **Initial keepalives to Enabled**. This will cause the IP Office to send RTP 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).

The screenshot displays the Avaya IP Office configuration interface for system 00E00706530F. The left-hand navigation tree shows various system components, with 'System (1)' selected. The main configuration area is divided into tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, and Codecs. The 'VoIP' tab is active, showing settings for H323 Gatekeeper, SIP Trunks, SIP Registrar, Layer 4 Protocol, RTP, and Keepalives. Red boxes highlight the specific settings mentioned in the text: H323 Gatekeeper Enable, SIP Trunks Enable, SIP Registrar Enable, Domain Name (avaya.lab.com), Layer 4 Protocol ports (UDP/TCP 5060), RTP Port Number Range (49152-53246), and Keepalives (Scope: RTP, Periodic timeout: 30, Initial keepalives: Enabled).

In the **Network Topology** tab, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu to the option that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even though the default STUN settings are populated, they will not be used.
- Set the **Binding Refresh Time (seconds)** to a desired value. The value of **300** (or every 5 minutes) was used during the compliance testing. This value is used to determine the **frequency** that IP Office will send OPTIONS heartbeats to the service provider.
- Verify the **Public IP Address** is set to **0.0.0.0**.
- Set the **Public Port** to **5060** for **UDP**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot shows the IP Office configuration interface. On the left, a tree view lists system components, with 'System (1)' and '00E00706530F' selected. The main window displays the 'Network Topology' tab for the selected system. The 'Network Topology Discovery' section includes the following settings:

- STUN Server Address: 69.90.168.13
- STUN Port: 3478
- Firewall/NAT Type: Open Internet
- Binding Refresh Time (seconds): 300
- Public IP Address: 0.0.0.0

Below these settings, the 'Public Port' section is configured as follows:

- UDP: 5060
- TCP: 0
- TLS: 0

A checkbox for 'Run STUN on startup' is located at the bottom left. 'Run STUN' and 'Cancel' buttons are on the right.

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).

5.2.3 System - Twinning Tab

Navigate to the **Twining** tab on the Details Pane, configure the following parameters:

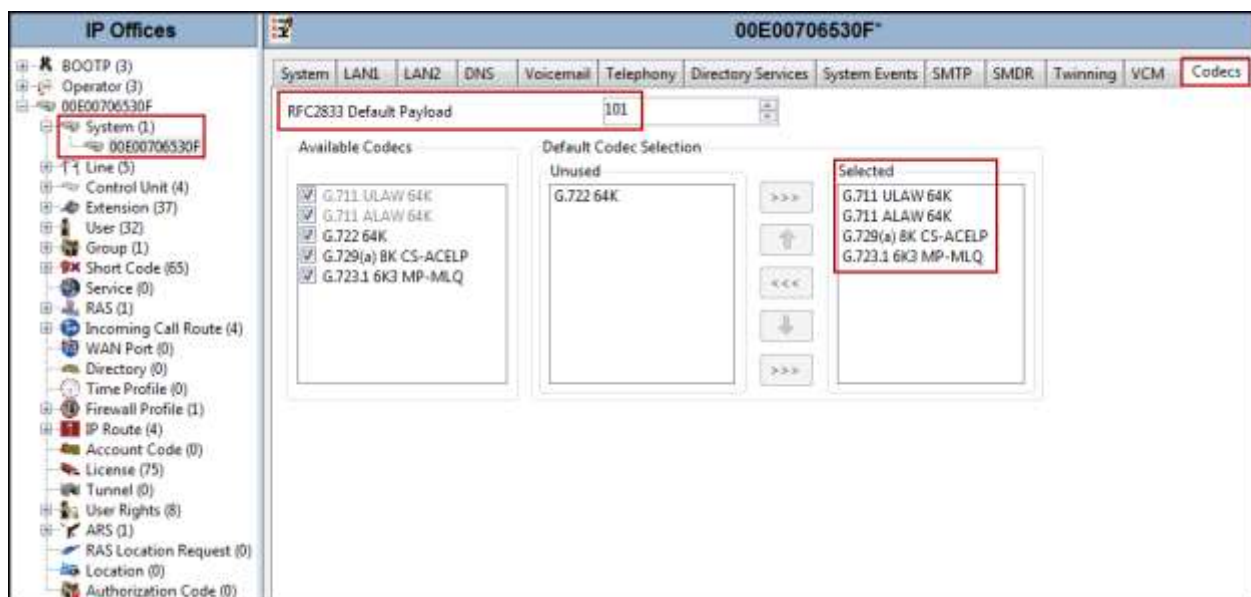
- Uncheck the **Send original calling party information for Mobile Twinning** box. This will allow the Caller ID for Twinning to be controlled by the setting on the SIP Line (**Section 5.4**). This setting also impacts the Caller ID for call forwarding.
- Click **OK** to commit (not shown).



5.2.4 System - Codecs Tab

For **Codecs** settings, navigate to the **System (1) → 00E00706530F** in the Navigation Pane, select the **Codecs** 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).



Note: The codec selections defined under this section (System – Codecs Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.6** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.3 IP Route

In the reference configuration, the IP Office LAN1 interface and the private interface of the Avaya SBCE resided on the same IP subnet, so an IP route was not 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** of the subnet of the private side of the Avaya SBCE, or enter **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).

The screenshot displays the IP Office configuration interface. On the left, a tree view under 'IP Offices' shows various configuration categories. The 'IP Route (4)' category is selected, and a sub-item '0.0.0.0' is highlighted with a red box. On the right, the 'IP Route' configuration window is open, showing fields for 'IP Address', 'IP Mask', 'Gateway IP Address', 'Destination', and 'Metric'. The 'IP Address' and 'IP Mask' fields are both set to '0 . 0 . 0 . 0'. The 'Gateway IP Address' field is set to '172 . 16 . 5 . 254'. The 'Destination' field is set to 'LAN1'. The 'Metric' field is set to '0'. A 'Proxy ARP' checkbox is present and unchecked. A red box highlights the 'IP Address', 'IP Mask', 'Gateway IP Address', and 'Destination' fields.

0.0.0.0	
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	172 . 16 . 5 . 254
Destination	LAN1
Metric	0
<input type="checkbox"/> Proxy ARP	

5.4 SIP Line

A SIP Line is needed to establish the SIP connection between IP Office and Cincinnati Bell Business SIP Trunking Service. 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 Avaya IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.4.1** and **5.4.2** 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 trunk Registration Credentials.
- 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 5.4.3** 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 5.4.3** to **5.4.8**.

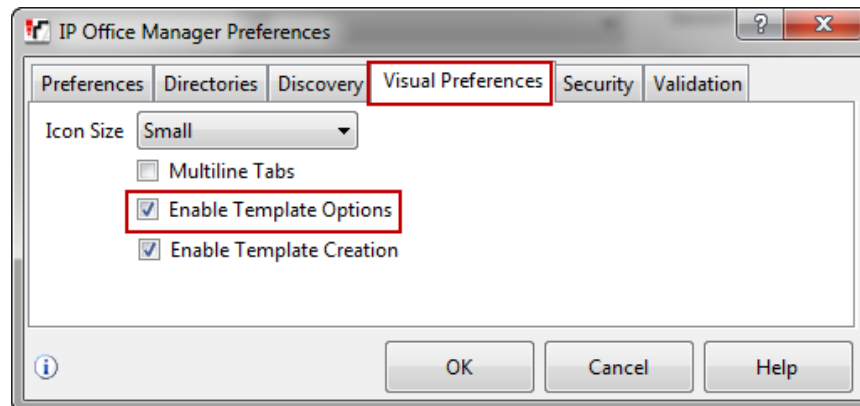
5.4.1 Importing a SIP Line Template

Note: 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 (500v2) 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.

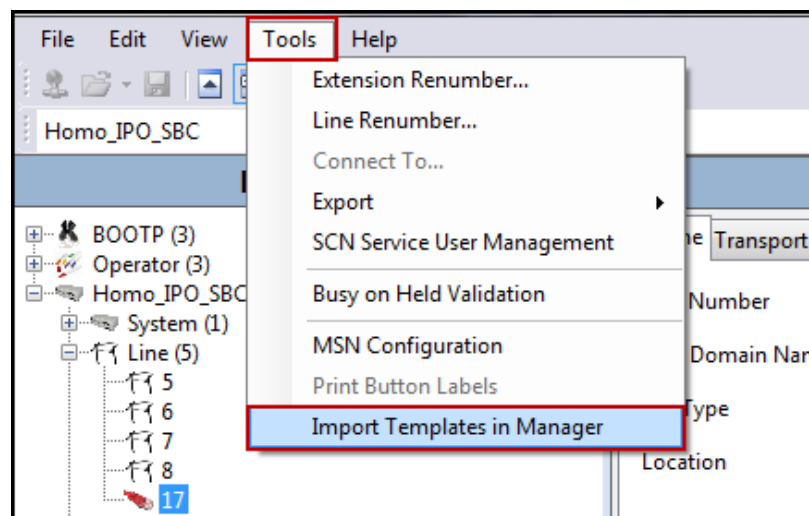
1. Copy a previously created template file to a location (e.g., C:\Temp) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **AF_<user supplied text>_SIPTrunk.xml**, where the **<user supplied text>** portion is entered during template file creation.

Note: If necessary, the **<user supplied text>** portion of the template file name may be modified, however the **AF_<user supplied text>_SIPTrunk.xml** format of the file name must be maintained. For example, an original template file **AF_TEST_SIPTrunk.xml** could be changed to **AF_Test1_SIPTrunk.xml**. The template file name is selected in **Section 5.4.2, step 2**, to create a new SIP Line.

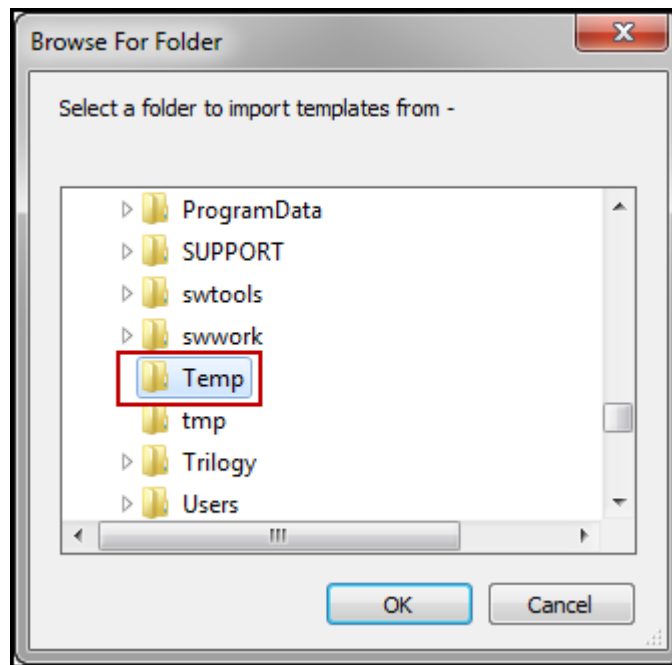
2. Verify that Template Options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the **Visual Preferences** tab. Check the box next to **Enable Template Options**. Click **OK**.



3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**.

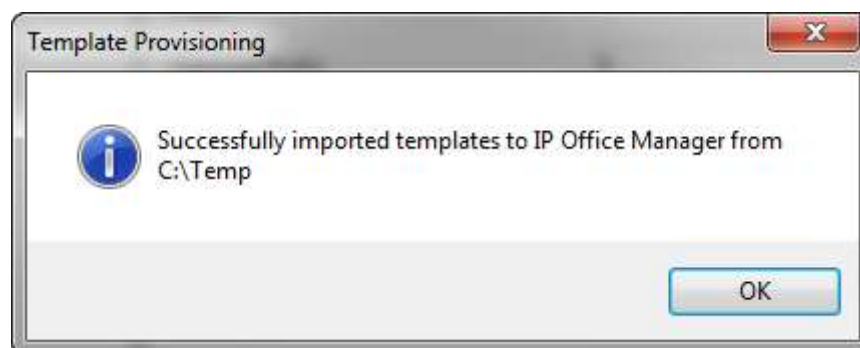


4. A folder browser will open. Select the directory used in **step 1** to store the template(s) (e.g., C:\Temp).

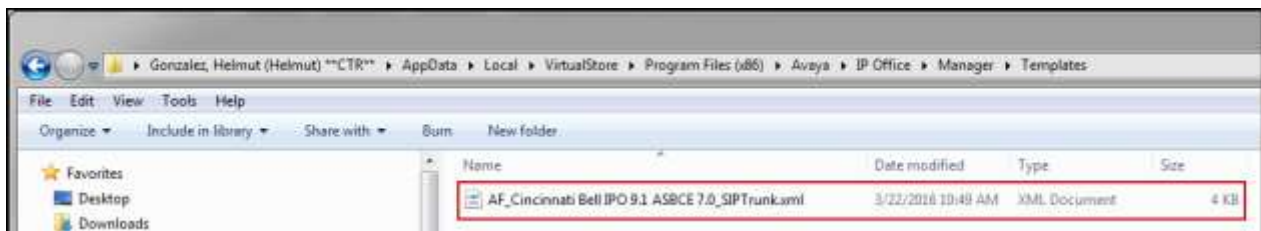
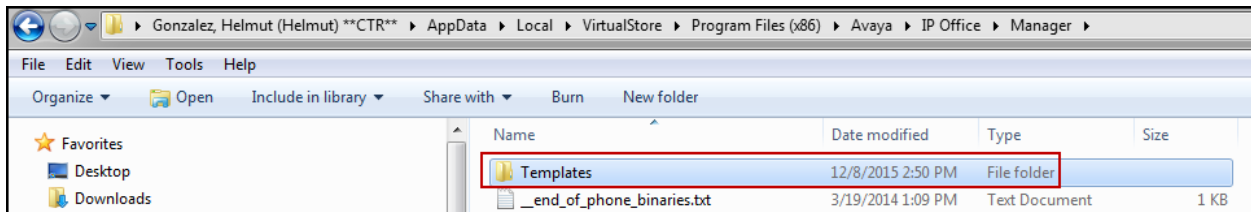
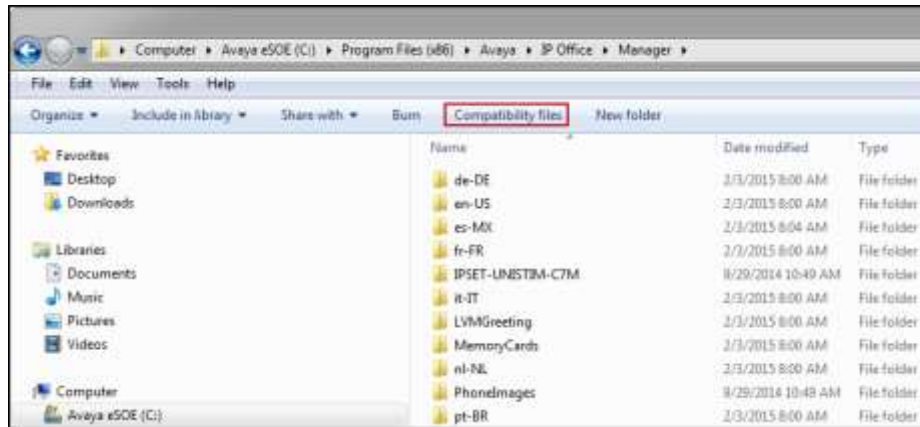


In the reference configuration, template files **AF_Cincinnati Bell IPO 9.1 ASBCE 7.0_SIPTrunk.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

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

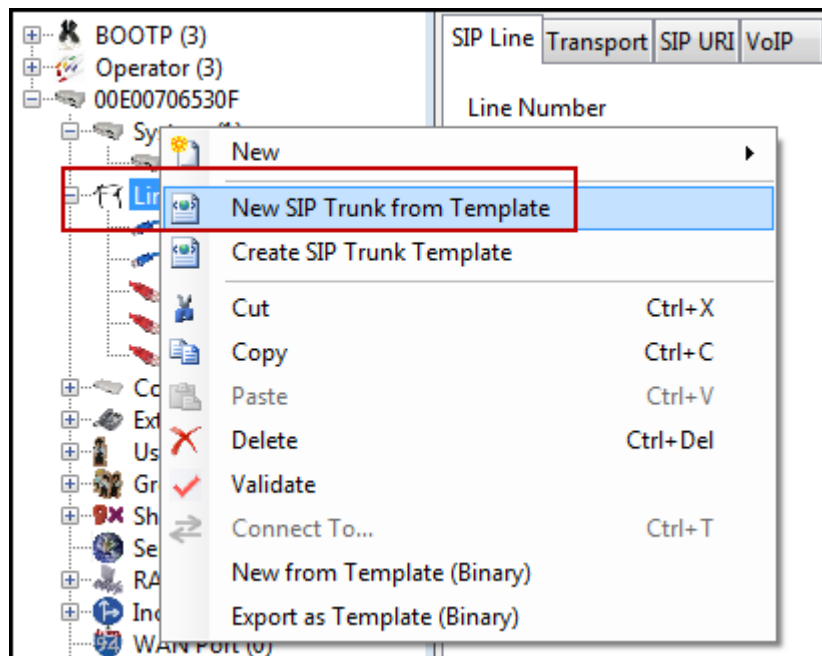


Note: Windows 7 (and later) locks the Avaya IP Office 9.1 \Templates directory, and it cannot be viewed. To enable browsing of the \Templates directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or C:\Program Files (x86)\Avaya\IP Office\Manager\Templates), and then click on the **Compatibility files** option shown below. The \Templates directory and its contents can then be viewed.



5.4.2 Creating a SIP Trunk from an XML Template

1. To create the SIP Trunk from a template, right-click on **Line** in the Navigation Pane, and select **New SIP Trunk from Template**.

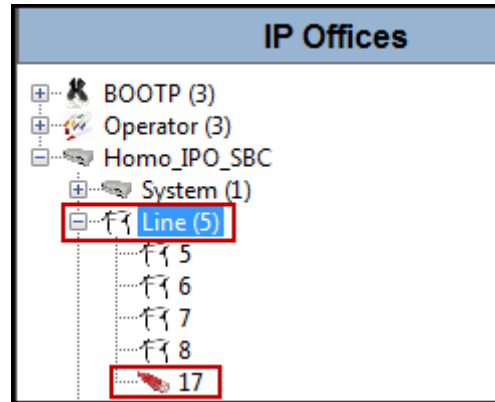


2. In the subsequent **Template Type Selection** pop-up window, from the **Service Provider** pull-down menu, select the XML template name from **Section 5.4.1**. Click **Create new SIP Trunk**.

Note: The drop down menu will display the *<user supplied text>* part of the template file name (see **Section 5.4.1**). If you check the **Display All** box, then the full template file name is displayed.



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 5.4.3 to 5.4.8**.

5.4.3 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. The time between SIP OPTIONS sent by IP Office will use the Binding Refresh Time for LAN1, as shown in **Section 5.2.1**.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (seconds)** is set to **On Demand**.
- Set **Send Caller ID** to **Diversion Header**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** Support and **Outgoing Supervised REFER** to **Always**.
- 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 'Line 17' selected. The main pane shows the 'SIP Line' tab with various configuration fields. Red boxes highlight the following settings:

- Line Number:** 17
- ITSP Domain Name:** (blank)
- URI Type:** SIP
- Location:** Cloud
- In Service:** ☒
- Check OOS:** ☒
- Refresh Method:** Auto
- Timer (seconds):** On Demand
- Send Caller ID:** Diversion Header
- Incoming Supervised REFER:** Always
- Outgoing Supervised REFER:** Always

5.4.4 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** (**Note:** On interface **A1** of the Avaya SBCE, IP address **172.16.5.71** was used to connect to IP Office, refer to **Sections 6.1** and **6.4**).
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2.1**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view under 'IP Offices' containing various system components like BOOTP, Operator, System, and Line (5). The 'Line (5)' is expanded, showing lines 1 through 19, with line 17 highlighted. The main panel is titled 'SIP Line - Line 17' and contains several tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The 'Transport' tab is selected and highlighted with a red box. Within this tab, the 'ITSP Proxy Address' field is set to '172.16.5.71' and is also highlighted with a red box. Below this, a 'Network Configuration' section is highlighted with a red box, containing the following settings: 'Layer 4 Protocol' is set to 'UDP', 'Send Port' is '5060', 'Use Network Topology Info' is set to 'LAN1', and 'Listen Port' is '5060'. Other visible fields include 'Explicit DNS Server(s)' (0.0.0.0), 'Calls Route via Registrar' (checked), and 'Separate Registrar' (empty).

5.4.5 SIP Line - SIP URI Tab

A SIP URI entry needs to be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, and 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. In the example screen below, a previously configured entry was edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact**, **Display Name** to **Use Internal Data**.
- Set **PAI** to **None**.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK**.
- Click **OK** again to commit (not shown).

The screenshot shows the Avaya IP Office configuration interface. On the left is a tree view of the system configuration, including IP Offices, Operators, Systems, Lines, Control Units, Extensions, Users, Groups, Short Codes, Services, RAS, Incoming Call Routes, WAN Ports, Directories, Time Profiles, Firewall Profiles, IP Routes, Account Codes, Licenses, Tunnels, User Rights, ARS, RAS Location Requests, Locations, and Authorization Codes. The 'Line 17' is selected in the tree.

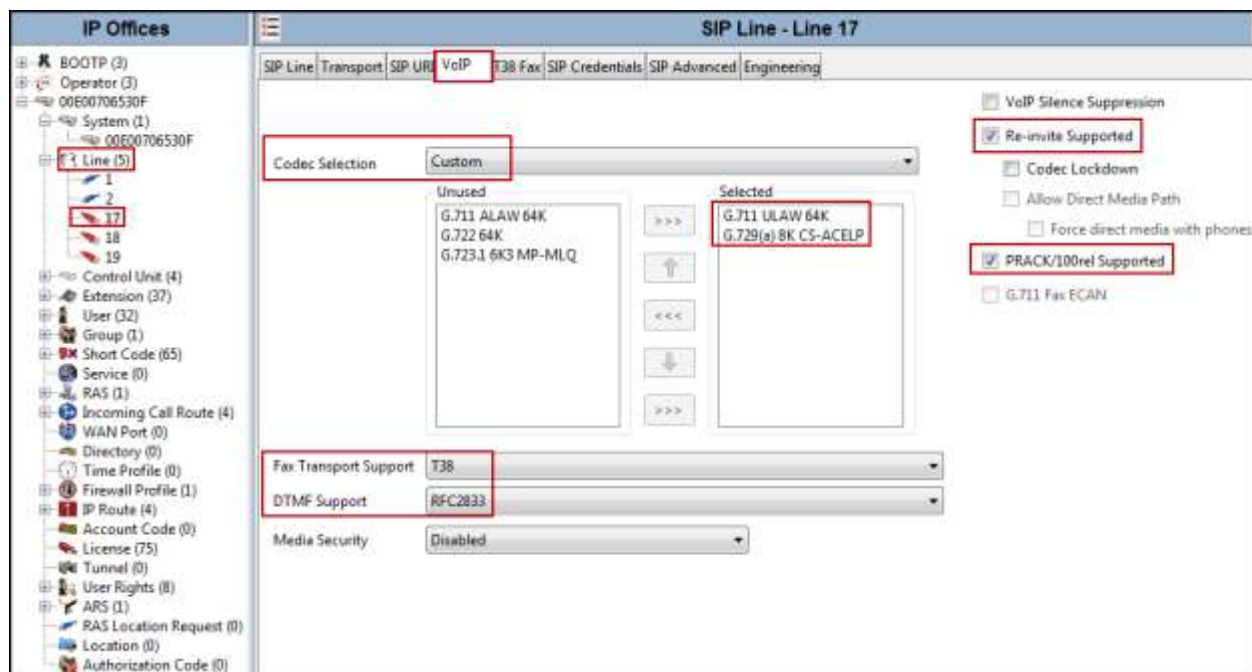
The main window is titled 'SIP Line - Line 17'. It has several tabs: SIP Line, Transport, SIP URI (selected), VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The 'SIP URI' tab displays a table with columns: Channel, Groups, Via, Local URI, Contact, Display Name, PAI, Credential, and Max Calls. The table contains one entry with Channel 1, Groups 17 17, Via 1..., Local URI N..., Contact 0: <Non..., and Max Calls 10.

Below the table is the 'Edit Channel' dialog. It has fields for: Via (172.16.5.60), Local URI (Use Internal Data), Contact (Use Internal Data), Display Name (Use Internal Data), PAI (None), Registration (0: <None>), Incoming Group (17), Outgoing Group (17), and Max Calls per Channel (10). Red boxes highlight the Local URI, Contact, Display Name, PAI, Incoming Group, Outgoing Group, and Max Calls per Channel fields. There are 'OK' and 'Cancel' buttons at the bottom right of the dialog.

5.4.6 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:

- In the sample configuration, 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. Cincinnati Bell supports codec G.711ULAW and G.729(a) for audio, with G.711ULAW being the preferred codec.
- Select **T.38** for **Fax Transport Support** (Refer to **Section 2.1**).
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- 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 the **PRACK/100rel Supported** box, to advertise the support for reliable provisional responses and Early Media to Cincinnati Bell.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



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 5.2.4** (System – Codecs tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

5.4.7 SIP Line – T.38 Fax Tab

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

- Uncheck **Use Default Values** at the bottom of the screen.
- Set **T38 Fax Version** to **0**. Cincinnati Bell Business SIP Trunking supports T.38 fax version 0.
- Set **Max Bit Rate (bps)** to **14400**, the highest fax bit rate that Avaya IP Office supports for T.38 faxing.
- Check the **Disable T30 ECM** option.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy including BOOTP, Operator, System, and Line 5. Line 5 is expanded, showing lines 1, 2, 17, 18, and 19. Line 17 is selected. The main panel is titled 'SIP Line - Line 17' and contains several tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, SIP Credentials, SIP Advanced, and Engineering. The 'T38 Fax' tab is active. The configuration parameters are as follows:

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 (msecs)	2600
EFlag Stop Timer (msecs)	2300
Tx Network Timeout (secs)	150
Use Default Values	<input type="checkbox"/>

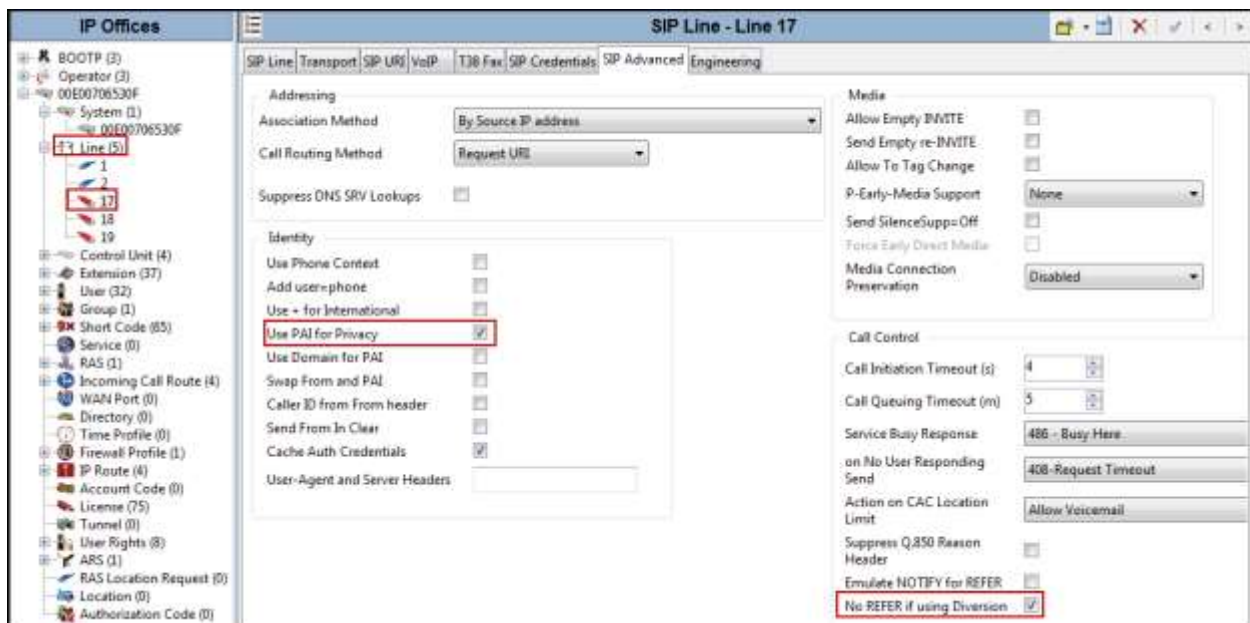
On the right side of the T38 Fax tab, there are several checkboxes and input fields:

- ☒ 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

5.4.8 SIP Line – SIP Advanced Tab

Select the **SIP Advanced** tab. For outbound calls with privacy enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with “anonymous”. IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity (PAI) header to pass the actual calling party information for authentication and billing purposes. By default, IP Office will use the PPI header for privacy. To configure IP Office to use the PAI header for privacy calls:

- Check the box for **Use PAI for Privacy**.
- Check **No REFER if using Diversion**. This directs IP Office not to send the REFER message with the Diversion message.
- Default values may be used for all other parameters.
- 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**.

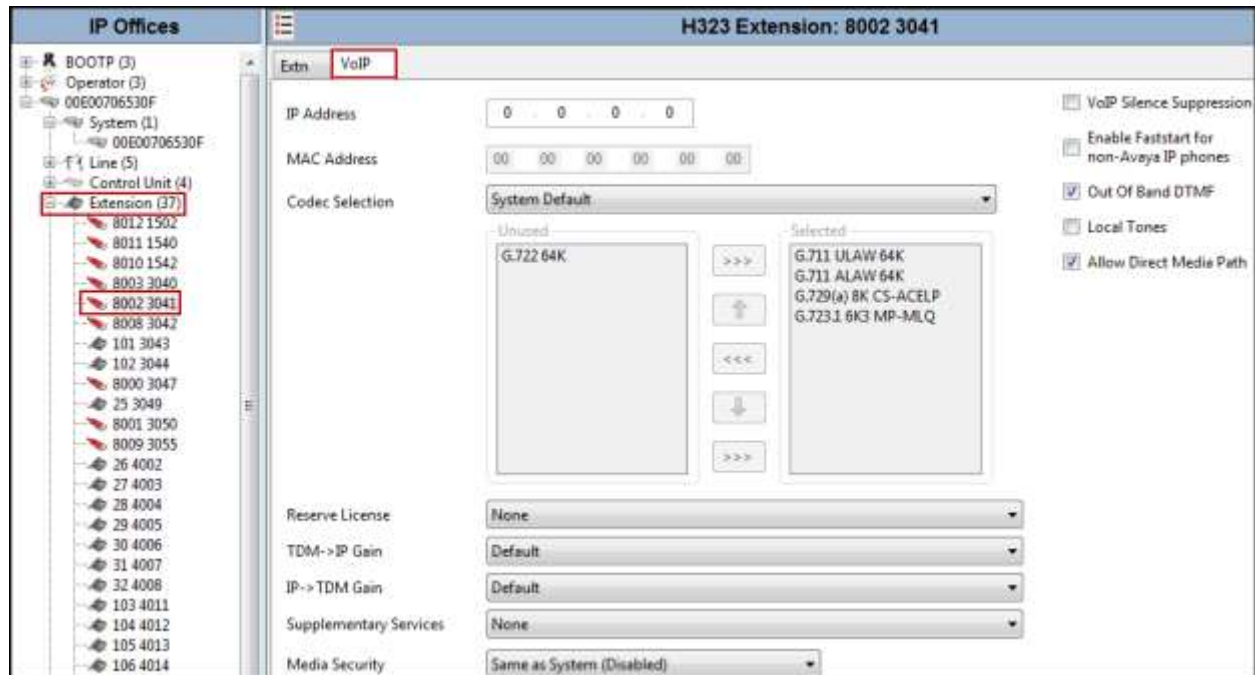
Select the **Extn** tab. Following is an example of extension 3041; this extension corresponds to an H.323 extension.

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows a hierarchy: BOOTP (3), Operator (3), 00E00706530F, System (1), 00E00706530F, Line (5), Control Unit (4), and Extension (37). The 'Extension (37)' folder is expanded, and the extension '8002 3041' is selected and highlighted with a red box. The main panel on the right is titled 'H323 Extension: 8002 3041' and contains configuration fields for the selected extension. The 'Extn' tab is active, and a red box highlights the 'Extn' tab label. The configuration fields are as follows:

Field	Value
Extension ID	8002
Base Extension	3041
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 3041; 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 Codecs tab (**Section 5.2.4**), 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).



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 **Ext3041 H323**.

The screenshot displays the Avaya SIP User Configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure. Under 'User (32)', the user '3041 Ext3041 H323' is selected. The main configuration area on the right is titled 'Ext3041 H323: 3041' 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: Ext3041 H323
- Password: [Redacted]
- Confirm Password: [Redacted]
- Conference PIN: [Redacted]
- Confirm Conference PIN: [Redacted]
- Account Status: Enabled
- Full Name: Ext3041 H323
- Extension: 3041
- Email Address: [Redacted]
- Locale: [Redacted]
- Priority: 5
- System Phone Rights: None
- Profile: Basic User

Below the profile section, there are several checkboxes for enabling various services:

- ☐ 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

At the bottom, the 'Device Type' is set to 'Avaya 9641'.

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 3041. 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 Cincinnati Bell 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.

Select the **Mobility** tab. In the sample configuration user 3041 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for user 3041. 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 **917861238616**. Other options can be set according to customer requirements.

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 3041.

Ext3041 H323: 3041									
User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
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 “Ext3040 H323”. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Cincinnati Bell. In the example, DID number **5131233393** 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.

Ext3041 H323: 3041							
Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership	Announcements	SIP	Personal Directory
SIP Name	5131233393						
SIP Display Name (Alias)	Ext3041 H323						
Contact	5131233393						
<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** and **SIP URI (Section 5.4.5)** and the users **SIP Name** and **Contact**, already populated with the assigned Cincinnati Bell DID numbers (**Section 5.6**).

From the left Navigation Pane, right-click on **Incoming Call Route** and select **New**.

On the Details Pane (not shown), under the **Standard** tab, set the parameters as show below:

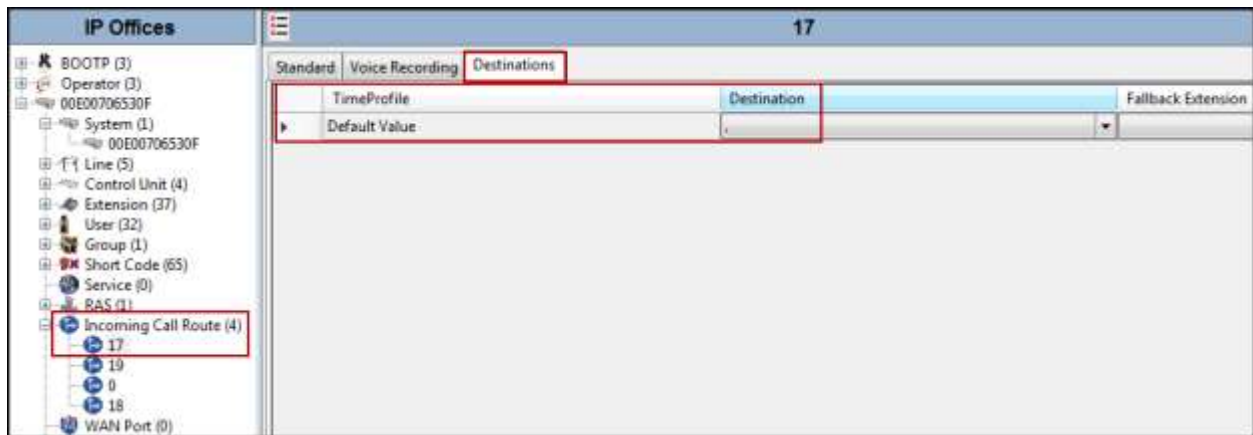
- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group ID** to the incoming line group of the SIP line defined in **Section 5.4**.
- Default values may be used for all other parameters.

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. The main pane shows the configuration for 'Incoming Call Route 17'. The 'Standard' tab is active, and the 'Line Group ID' is set to '17'. The 'Bearer Capacity' is set to 'Any Voice'. Other parameters like 'Incoming Number', 'Incoming Sub Address', 'Incoming CLI', 'Locale', 'Priority', 'Tag', 'Hold Music Source', and 'Ring Tone Override' are also visible.

IP Offices	
BOOTP (3)	
Operator (3)	
00E00706530F	
System (1)	
00E00706530F	
Line (5)	
Control Unit (4)	
Extension (37)	
User (32)	
Group (1)	
Short Code (65)	
Service (0)	
RAS (1)	
Incoming Call Route (4)	
17	
19	
0	
18	
WAN Port (0)	
Directory (0)	
Time Profile (0)	
Firewall Profile (1)	

Incoming Call Route 17	
Standard	Voice Recording
Standard	Destinations
Bearer Capacity	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

- 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. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance testing.

5.8.1 Short Codes and Automatic Route Selection

To create the short code used for ARS, right-click on **Short Code** in the Navigation Pane and select **New** (not shown). The screen below shows the creation of the short code **9N** used in the reference configuration. When the Avaya IP Office users dialed 9 plus any number N, calls were directed to **Line Group 50: Main**, configurable via ARS and defined next in this section.

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' navigation pane lists various short codes, 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"/>

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 digit on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office. The first example highlighted below shows that for calls to area codes in the North American Numbering Plan, the user dialed 9, followed by 11 digits, starting with a 1.

IP Offices

- BOCTP (3)
- Operator (3)
- 00600706530F
- System (1)
- 00E00706530F
- Line (3)
- Control Unit (4)
- Extension (37)
- User (32)
- Group (1)
- Short Code (65)
- 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 (75)
- Tunnel (0)
- User Rights (8)
- ARS (1)**
 - 50: Main**
- RAS Location Request (0)
- 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
11	911	Dial Emergency	0
911	911	Dial Emergency	0
001XXXXXXXXX	001N	Dial	17
8XXXXXXXXX	8N	Dial	17
1XXXXXXXXX	1N	Dial	17
6XXXXXX	6N	Dial	17
3XXXXXXXXX	3N	Dial	17

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

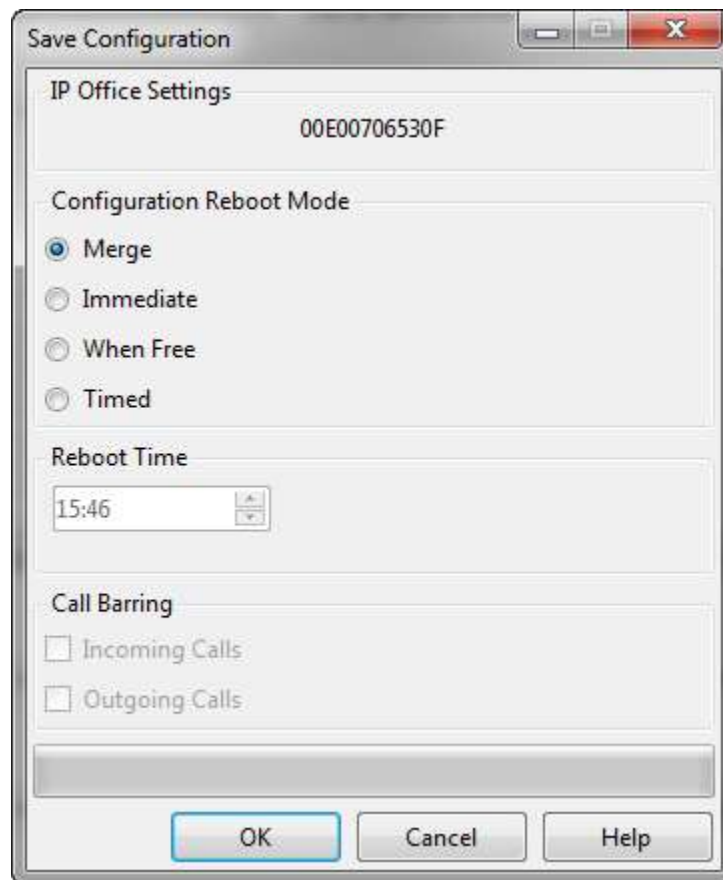
Alternate Route: <None>

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.



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

This section describes the required configuration of the Avaya SBCE to connect to Cincinnati Bell Business 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>/sbce` 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:

Log In

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

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

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

© 2011 - 2015 Avaya Inc. All rights reserved.

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

The screenshot shows the Avaya Session Border Controller for Enterprise Dashboard. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays the product name and the Avaya logo. On the left, a sidebar menu lists various management options, with 'Dashboard' highlighted. The main content area is divided into several sections: 'Information' (System Time, Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, Failed Login Attempts), 'Installed Devices' (listing EMS and Avaya SBCE), 'Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (Avaya SBCE: Max forward), and a 'Notes' section at the bottom.

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.

The screenshot shows the Avaya Session Border Controller for Enterprise System Management page. The top navigation bar is the same as the dashboard. The main header displays the product name and the Avaya logo. On the left, a sidebar menu lists various management options, with 'System Management' highlighted. The main content area is divided into several sections: 'System Management' (with tabs for Devices, Updates, SSL VPN, and Licensing), 'Device Name' (listing Avaya SBCE), 'Management IP' (192.168.1.1), 'Version' (7.0.1-03-8739), 'Status' (Commissioned), and a list of actions (Reboot, Shutdown, Restart Application, View, Edit, Uninstall). The 'View' button is highlighted with a red box.

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

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

System Information: Avaya SBCE

General Configuration		Device Configuration		License Allocation	
Appliance Name	Avaya SBCE	HA Mode	No	Standard Sessions	2000
Box Type	SIP	Two Bypass Mode	No	Advanced Sessions	2000
Deployment Mode	Proxy			Scopia Video Sessions	500
				CES Sessions	0
				Encryption	128

Network Configuration				
IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
192.168.157.189	192.168.157.189	255.255.255.192	192.168.157.129	B1

DNS Configuration		Management IP(s)	
Primary DNS	192.168.157.129	IP	172.16.5.71
Secondary DNS	192.168.157.129		
DNS Location	DMZ		
DNS Client IP	192.168.157.180		

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 and DNS addresses were 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 Global Profiles

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

6.2.1 Server Interworking – Avaya-IPO

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk 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 Cincinnati Bell, 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**.



The screenshot shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The dialog has two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'Avaya-IPO'. The 'Clone Name' field is highlighted with a red rectangular border. Below the fields is a 'Finish' button.

For the newly created **Avaya-IPO** profile, click **Edit** at the bottom of the **General** tab (not shown):

- Check **T.38 Support**.
- Click **Finish**.

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

- Hold Support:** ☒ None, ☐ RFC2543 - c=0 0 0 0, ☐ RFC3264 - a=sendonly
- 180 Handling:** ☒ None, ☐ SDP, ☐ No SDP
- 181 Handling:** ☒ None, ☐ SDP, ☐ No SDP
- 182 Handling:** ☒ None, ☐ SDP, ☐ No SDP
- 183 Handling:** ☒ None, ☐ SDP, ☐ No SDP
- Refer Handling:** ☐
- URI Group:** None (dropdown menu)
- Send Hold:** ☐
- Delayed Offer:** ☐
- 3xx Handling:** ☐
- Diversion Header Support:** ☐
- Delayed SDP Handling:** ☐
- Re-Invite Handling:** ☐
- Prack Handling:** ☐
- Allow 18X SDP:** ☐
- T.38 Support:** ☒ (highlighted with a red rectangle)
- URI Scheme:** ☒ SIP, ☐ TEL, ☐ ANY
- Via Header Format:** ☒ RFC3261, ☐ RFC2543

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

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, and System Management. Under 'System Management', 'Global Profiles' is selected, and 'Server Interworking' is highlighted. The main content area is titled 'Interworking Profiles: Avaya-IPO' and features a list of profiles on the left, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-com', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General', 'Avaya-CS1000', 'Avaya-IPO' (highlighted), and 'Avaya-CM'. An 'Add' button is located above the list. The right pane shows the configuration for the 'Avaya-IPO' profile, with the 'General' tab selected. This tab contains a table of settings for various SIP-related features.

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

An 'Edit' button is located at the bottom right of the configuration pane.

The following screen capture shows the **Advanced** tab of the newly created **Avaya-IPO Server Interworking** 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, Users, and Settings. The main title is "Session Border Controller for Enterprise".

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

The main content area is titled "Interworking Profiles: Avaya-IPO" and features an "Add" button. Below this is a list of interworking profiles: cs2100, avaya-ru, OCS-Edge-Server, cisco-cdm, cups, Sipera-Halo, OCS-FrontEnd-S..., Avaya-SM, SP-General, Avaya-CS1000, **Avaya-IPO** (highlighted), and Avaya-CM.

The configuration for the selected "Avaya-IPO" profile is shown in the "Advanced" tab. The tab is part of a set including General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The configuration details are as follows:

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
DTMF	
DTMF Support	None

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

6.2.2 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.

- Check **T.38 Support**.
- Click **Next**.

Interworking Profile

General

Hold Support: ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling: ☒ None ☐ SDP ☐ No SDP

181 Handling: ☒ None ☐ SDP ☐ No SDP

182 Handling: ☒ None ☐ SDP ☐ No SDP

183 Handling: ☒ None ☐ SDP ☐ No SDP

Refer Handling: ☐

URI Group: None

Send Hold: ☒

Delayed Offer: ☒

3xx Handling: ☐

Diversion Header Support: ☐

Delayed SDP Handling: ☐

Re-Invite Handling: ☐

Prack Handling: ☐

Allow 18X SDP: ☐

T.38 Support: ☒

URI Scheme: ☒ SIP ☐ TEL ☐ ANY

Via Header Format: ☒ RFC3261 ☐ RFC2543

Back Next

- Accept all other default values by clicking **Next** and then **Finish** (not shown)

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 main header is 'Session Border Controller for Enterprise'. On the left, a sidebar menu lists various configuration areas, with 'Global Profiles' and 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SP-General' and features a list of profiles on the left and a configuration table on the right. The 'General' tab is selected, showing a table of settings for the 'SP-General' profile.

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 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 areas, with 'Global Profiles' and 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SP-General' and features a list of profiles on the left, including 'SP-General' which is selected. The 'Advanced' tab is active, showing configuration options for Record Routes, Include End Point IP for Context Lookup, Extensions, Diversion Manipulation, Has Remote SBC, Route Response on Via Port, and DTMF Support. The 'DTMF Support' is set to 'None'. An 'Edit' button is visible at the bottom of the configuration area.

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					
DTMF					
DTMF Support: None					

6.2.3 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" 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 "IP Office". The input field is highlighted with a red border. Below the input field, there is a "Next" button.

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

- **Server Type:** Select **Call Server**.
- **IP Address / FQDN:** **172.16.5.60** (IP Address of IP Office).
- **Port:** **5060** (This port must match the port number defined in **Section 5.4.4**).
- **Transports:** Select **UDP**.
- Click **Next**.

IP Address / FQDN	Port	Transport
172.16.5.60	5060	UDP

Note: UDP transport protocol was used on the connection between the Avaya SBCE and IP Office. However, TCP can be used instead if necessary.

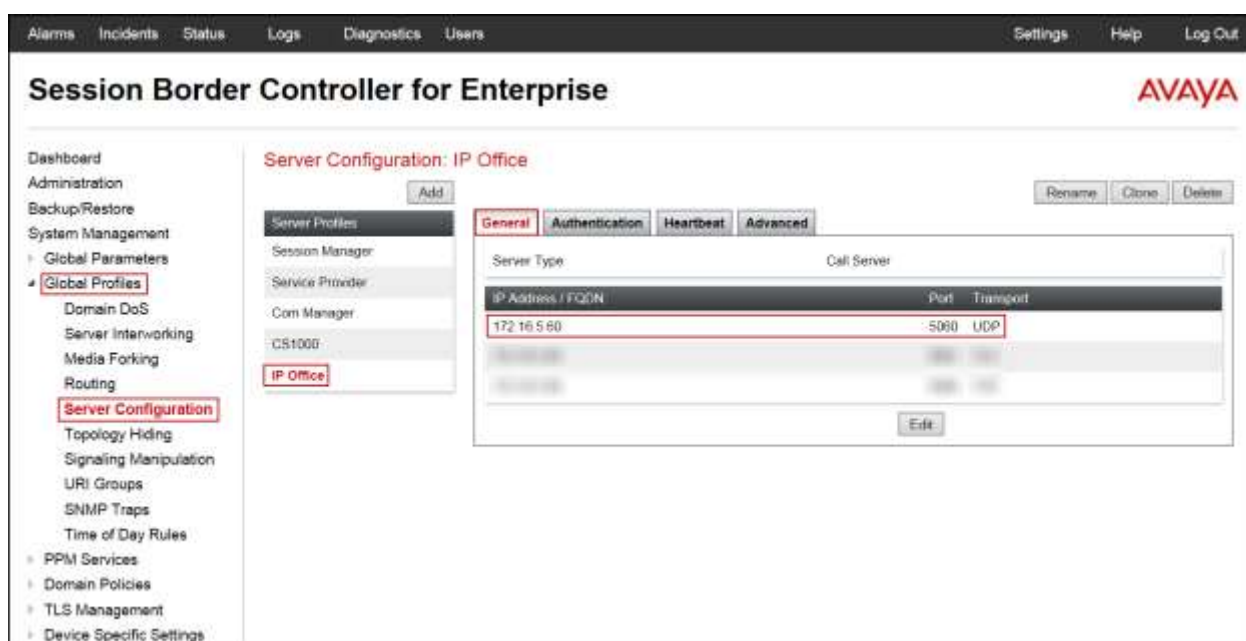
- Click **Next** on the **Authentication** window (not shown).
- Click **Next** on the **Heartbeat** window (not shown).

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

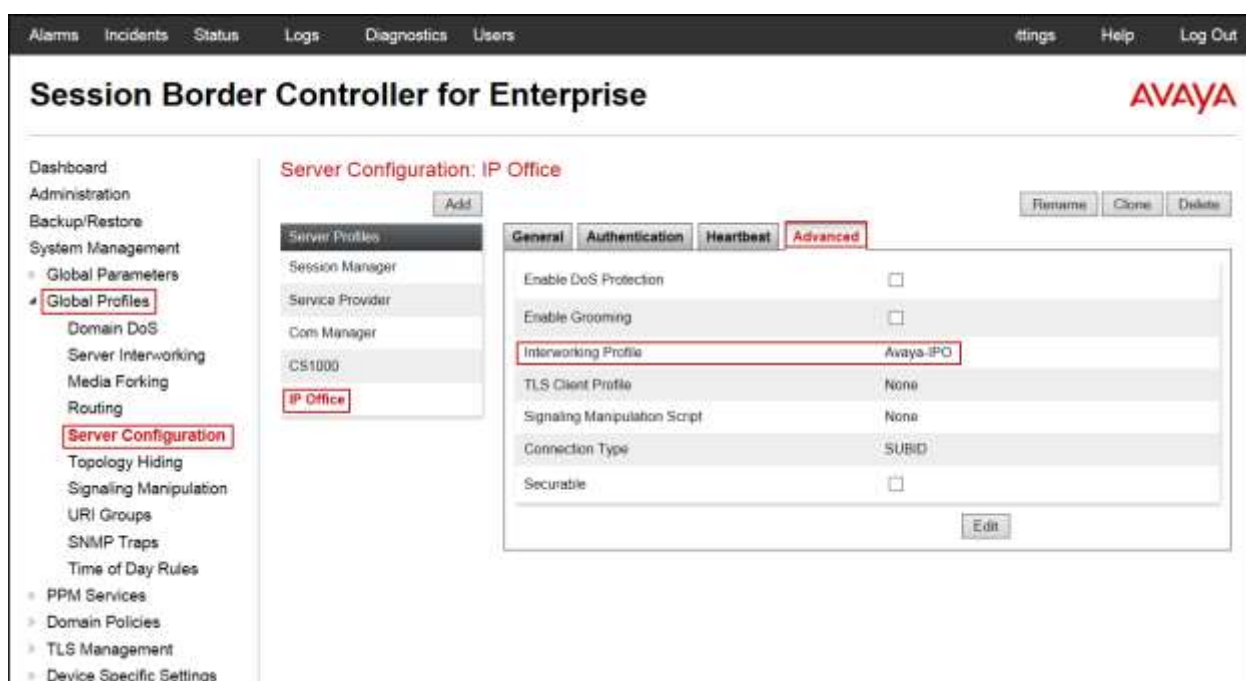
- Select **Avaya-IPO** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya-IPO
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	<input type="checkbox"/>

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

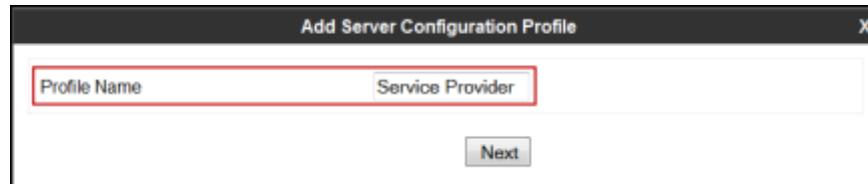


The following screen capture shows the **Advanced** tab of the newly created **IP Office** Server Configuration Profile.



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**.

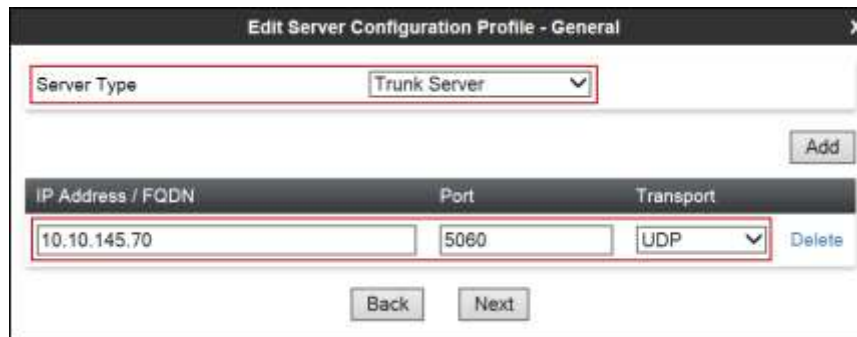
- Click **Next**.



The screenshot shows a window titled "Add Server Configuration Profile". It has a single text input field labeled "Profile Name" containing the text "Service Provider". Below the input field is a "Next" button.

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

- **Server Type:** Select **Trunk Server**.
- **IP Address / FQDN:** **10.10.145.70** (Cincinnati Bell's SIP Proxy address).
- **Port:** **5060**.
- **Transports:** Select **UDP**.
- Click **Next**.



The screenshot shows a window titled "Edit Server Configuration Profile - General". It contains a "Server Type" dropdown menu set to "Trunk Server". Below this is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "10.10.145.70", "5060", and "UDP". There are "Add", "Back", "Next", and "Delete" buttons.

IP Address / FQDN	Port	Transport
10.10.145.70	5060	UDP

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

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

- 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**

Connection Type **SUBID**

Securable ☐

Back **Finish**

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

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
Domain DoS
Server Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
PPM Services

Server Configuration: Service Provider

Add

Rename Clone Delete

Server Profiles
Session Manager
Service Provider
Com Manager
CS1000
IP Office

General Authentication Heartbeat Advanced

Server Type Trunk Server

IP Address / FQDN	Port	Transport
10.10.145.70	5050	UDP

Edit

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



6.2.4 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 Cincinnati Bell's Modular Access Router.

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

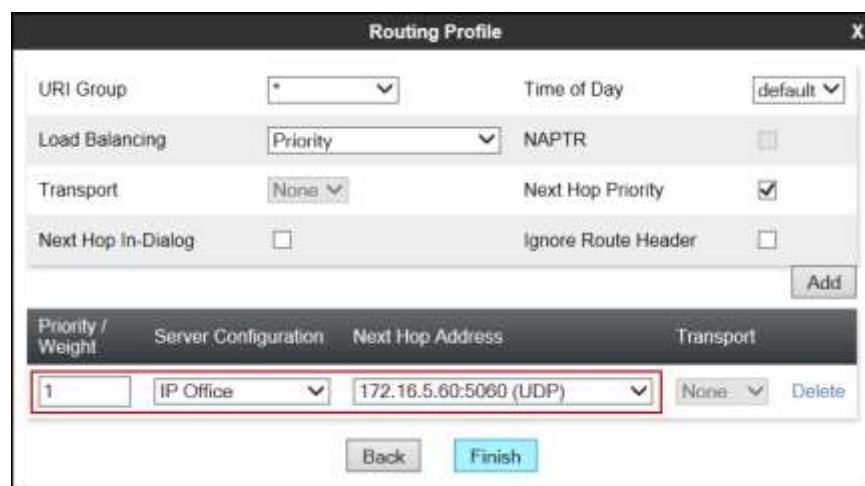
- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route_to_IPO**.
- Click **Next**.



The screenshot shows a 'Routing Profile' dialog box. The 'Profile Name' field is highlighted with a red box and contains the text 'Route_to_IPO'. 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 **172.16.5.60:5060 (UDP)** (IP Office IP address, Port and Transport).
- Click **Finish**.

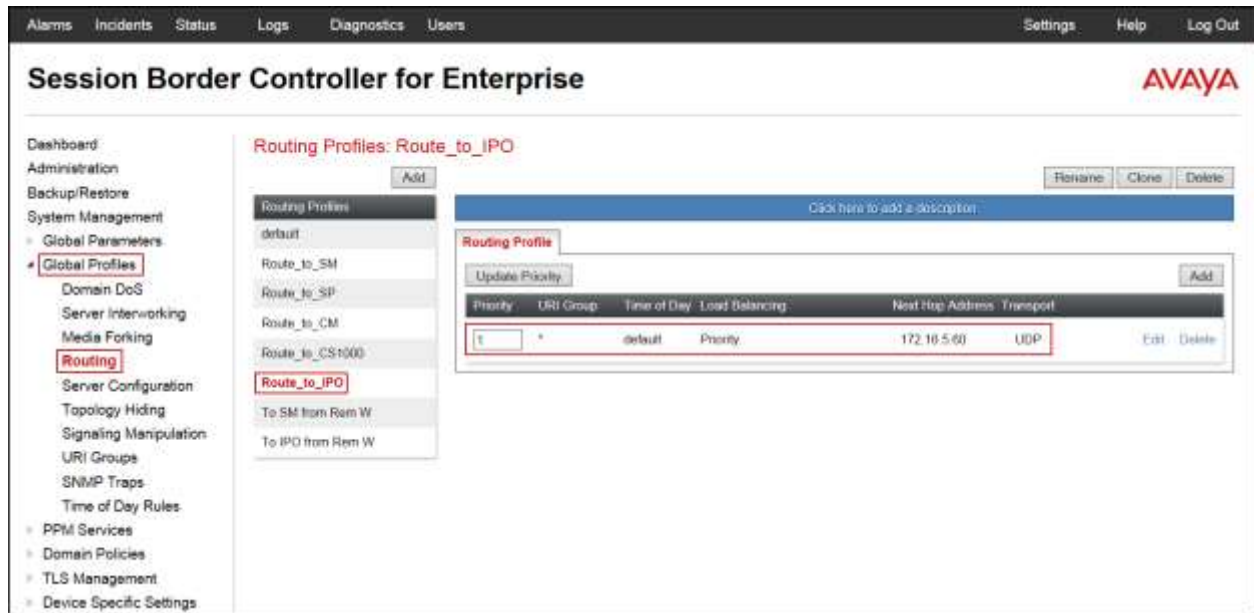


The screenshot shows the 'Routing Profile' dialog box with various configuration options. The 'URI Group' is set to '*', 'Time of Day' is 'default', 'Load Balancing' is 'Priority', 'NAPTR' is unchecked, 'Transport' is 'None', 'Next Hop Priority' is checked, and 'Ignore Route Header' is unchecked. Below these options is an 'Add' button. A table below the 'Add' button shows the configuration for the next hop:

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IP Office	172.16.5.60:5060 (UDP)	None

At the bottom of the dialog are 'Back' and 'Finish' buttons.

The following screen shows the newly created **Route_to_IPO** Routing Profile.



Similarly, for the outbound route:

- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route_to_SP**.
- Click **Next**.



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**.
- The **Next Hop Address** is populated automatically with **10.10.145.70:5060 (UDP)** (Cincinnati Bell's SIP Proxy IP address).
- Click **Finish**.

The screenshot shows the 'Add Routing Rule' dialog box. It contains several configuration fields: 'URI Group' (set to '*'), 'Time of Day' (set to 'default'), 'Load Balancing' (set to 'Priority'), 'NAPTR' (unchecked), 'Transport' (set to 'None'), 'Next Hop Priority' (checked), 'Next Hop In-Dialog' (unchecked), and 'Ignore Route Header' (unchecked). Below these fields is a table with columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'. The table contains one row with values: '1', 'Service Provider', '10.10.145.70:5060 (UDP)', and 'None'. There is a 'Delete' button next to the 'Transport' column. At the bottom of the dialog is a 'Finish' button.

The following screen capture shows the newly created **Route_to_SP** Routing Profile.

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left sidebar contains a navigation menu with items like 'Dashboard', 'Administration', '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', and 'PPM Services'. The 'Routing Profiles: Route_to_SP' section is highlighted. The main area shows the 'Route_to_SP' profile with a table of routing rules. The table has columns: 'Priority', 'URI Group', 'Time of Day', 'Load Balancing', 'Next Hop Address', and 'Transport'. The table contains one row with values: '1', '*', 'default', 'Priority', '10.10.145.70', and 'UDP'. There are 'Edit' and 'Delete' buttons next to the 'Transport' column. The 'Add' button is also visible.

6.2.5 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 trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

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 **Profile 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).



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 **Profile Name: Service_Provider**.
- Click **Finish**.



- Click **Edit** on the newly created **Service_Provider** Topology Hiding profile.
- On the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**as.voip.fuse.net**) under **Overwrite Value**
- On the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (**as.voip.fuse.net**) under **Overwrite Value**.
- On the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the service provider (**as.voip.fuse.net**) under **Overwrite Value**.
- Click **Finish**.

Edit Topology Hiding Profile
X

Header	Criteria	Replace Action	Overwrite Value	
From	IP/Domain	Overwrite	as.voip.fuse.net	Delete
Referred-By	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	as.voip.fuse.net	Delete
Request-Line	IP/Domain	Overwrite	as.voip.fuse.net	Delete
SDP	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete

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 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Global Profiles' expanded and 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: Service_Provider' and features an 'Add' button. Below this, a list of profiles is shown, with 'Service_Provider' highlighted. The 'Topology Hiding' tab is active, displaying a table with the following data:

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

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

6.3 Domain Policies

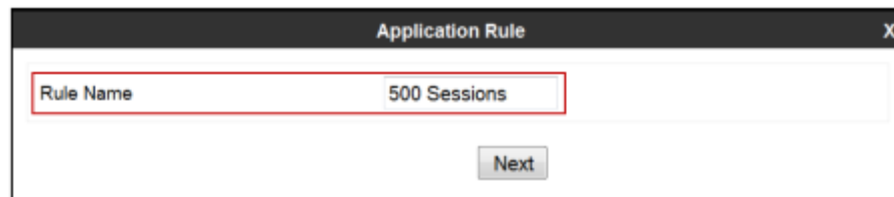
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.3.1 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**.

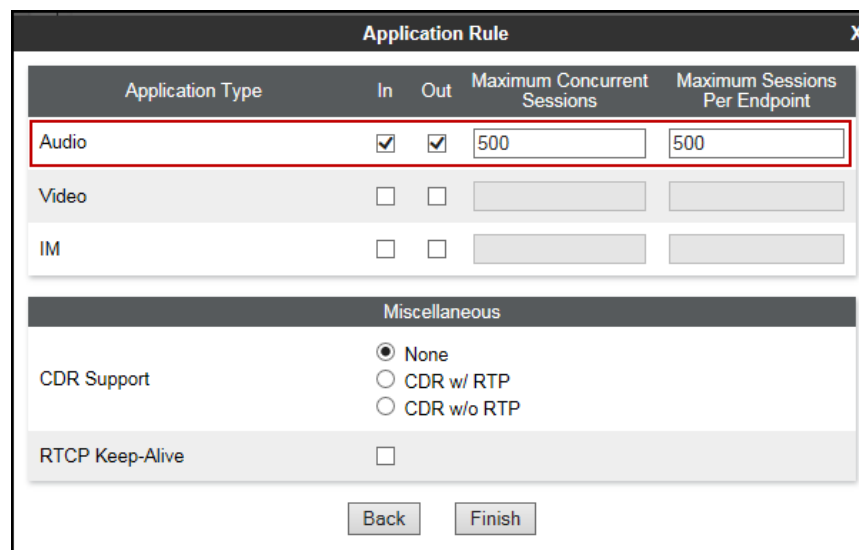


Application Rule

Rule Name 500 Sessions

Next

- 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.
- 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 type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

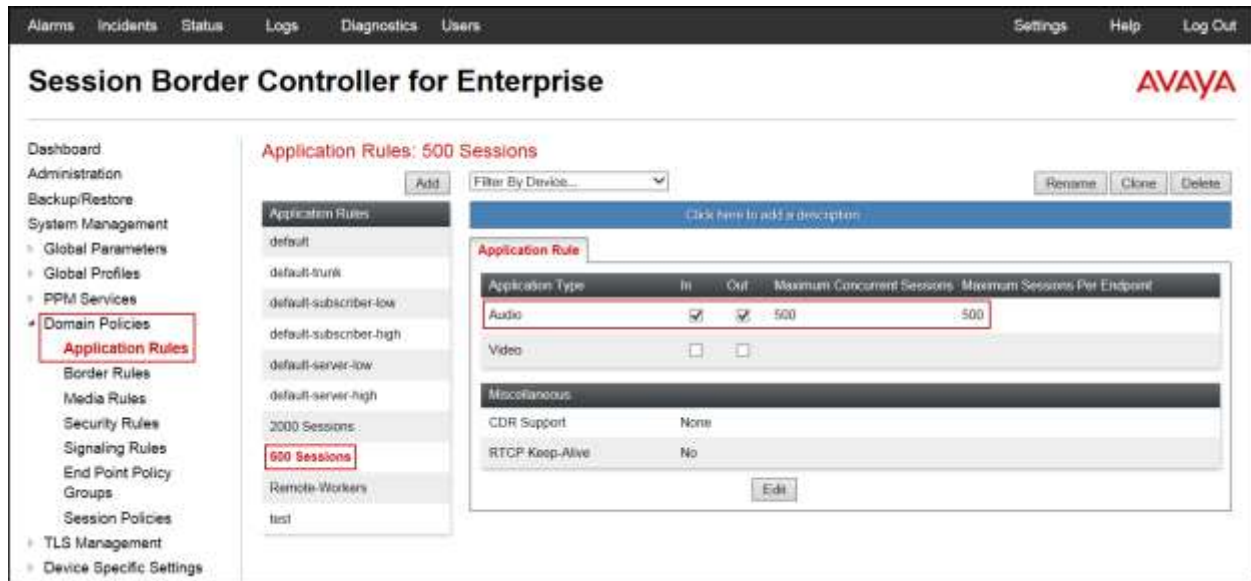
Miscellaneous

CDR Support ☒ None ☐ CDR w/ RTP ☐ CDR w/o RTP

RTCP Keep-Alive ☐

Back Finish

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

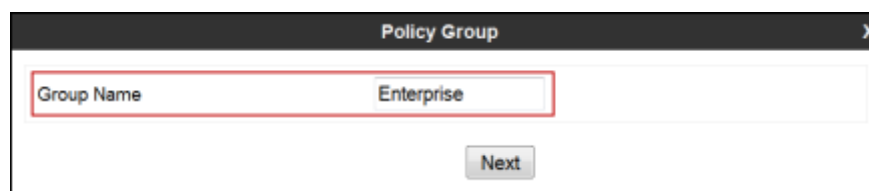


6.3.2 End Point Policy Groups

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: Enterprise.**
- Click **Next**.



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

Policy Group

Application Rule: 500 Sessions

Border Rule: default

Media Rule: default-low-med

Security Rule: default-low

Signaling Rule: default

Back Finish

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

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** Application Rules Border Rules Media Rules Security Rules Signaling Rules **End Point Policy Groups** Session Policies TLS Management Device Specific Settings

Policy Groups: Enterprise

Add Filter By Device... Rename Clone Delete

Policy Groups

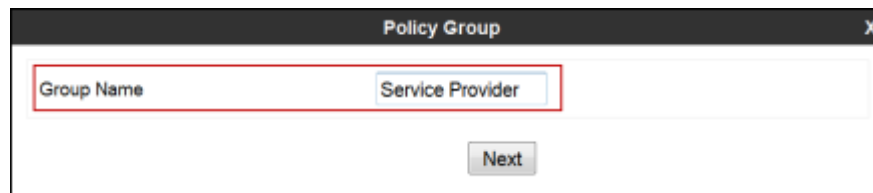
- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-h...
- avaya-def-low...
- avaya-def-hig...
- avaya-def-hig...
- Enterprise**
- Service Provider

Policy Group Summary

Order	Application	Border	Media	Security	Signaling	
1	500 Sessions	default	default-low-med	default-low	default	Edit

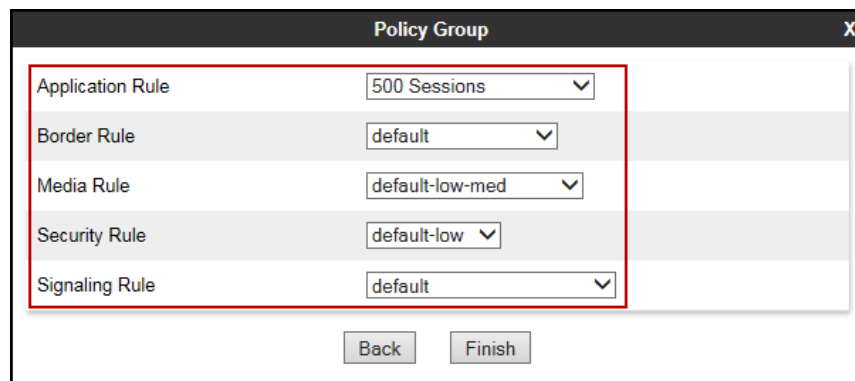
Similarly, to create an End Point Policy Group toward the Service Provider.

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



The screenshot shows a dialog box titled "Policy Group". Inside, there is a text input field labeled "Group Name" which contains the text "Service Provider". This field is highlighted with a red rectangular box. Below the input field, there is a button labeled "Next".

- **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 same "Policy Group" dialog box, but now with several dropdown menus. A red rectangular box highlights the area containing five rows of rule selections:

Rule Type	Selected Value
Application Rule	500 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default

Below this table, there are two buttons: "Back" and "Finish".

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 system management options, with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: Service Provider' and features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below these are two blue bars with text prompts to add descriptions. A 'Policy Group' table is shown with a 'Summary' button. The table has columns for Order, Application, Border, Media, Security, and Signaling. A single row is visible, representing the newly created 'Service Provider' policy group.

Order	Application	Border	Media	Security	Signaling	
1	500 Sessions	default	default-low-med	default-low	default	Edit

6.4 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.


6.4.1 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 **Network Configuration** 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 SBCE web interface. The top navigation bar includes 'Alarms', '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' expanded and 'Network Management' highlighted. The main content area is titled 'Network Management: Avaya SBCE' and has two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active, showing a table of network configurations. The table has columns for Name, Gateway, Subnet Mask, Interface, and IP Address. Two networks are listed: Network_A1 and Network_B1. Network_A1 has a Gateway of 172.16.5.254, Subnet Mask of 255.255.255.0, Interface of A1, and IP Address of 172.16.5.71. Network_B1 has a Gateway of 192.168.157.129, Subnet Mask of 255.255.255.192, Interface of B1, and IP Address of 192.168.157.189. Each row has 'Edit' and 'Delete' links. An 'Add' button is in the top right of the table area.

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	172.16.5.254	255.255.255.0	A1	172.16.5.71	Edit Delete
Network_B1	192.168.157.129	255.255.255.192	B1	192.168.157.189	Edit Delete

On the Interface Configuration 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.

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

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
 ▸ Global Parameters
 ▸ Global Profiles
 ▸ PPM Services
 ▸ Domain Policies
 ▸ TLS Management
▸ Device Specific Settings
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 ▸ DMZ Services
TURN/STUN Service

Network Management: Avaya SBCE

Devices
Avaya SBCE

Interfaces Networks

Add VLAN

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

6.4.2 Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving 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:** **172.16.5.71** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office)
- **Port Range:** **35000-40000**.
- Click **Finish**.

The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing "Private_med" and a clear button (x).
- IP Address:** A dropdown menu showing "Network_A1 (A1, VLAN 0)" with a downward arrow. Below it, a sub-dropdown shows "172.16.5.71" with a downward arrow.
- Port Range:** Two text input fields containing "35000" and "40000" separated by a hyphen.
- Finish:** A button at the bottom center of the dialog.

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** **Public_med**.
- Under **IP Address** select: **Network_B1 (B1, VLAN 0)**.
Select **IP Address:** **192.168.157.189** (Outside IP Address of the Avaya SBCE, toward Cincinnati Bell).
- **Port Range:** **35000-40000**.
- Click **Finish**.

Add Media Interface

Name:

IP Address:

Port Range: -

The following screen capture shows the newly created Media Interfaces.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Media Interface: Avaya SBCE

Media Interface

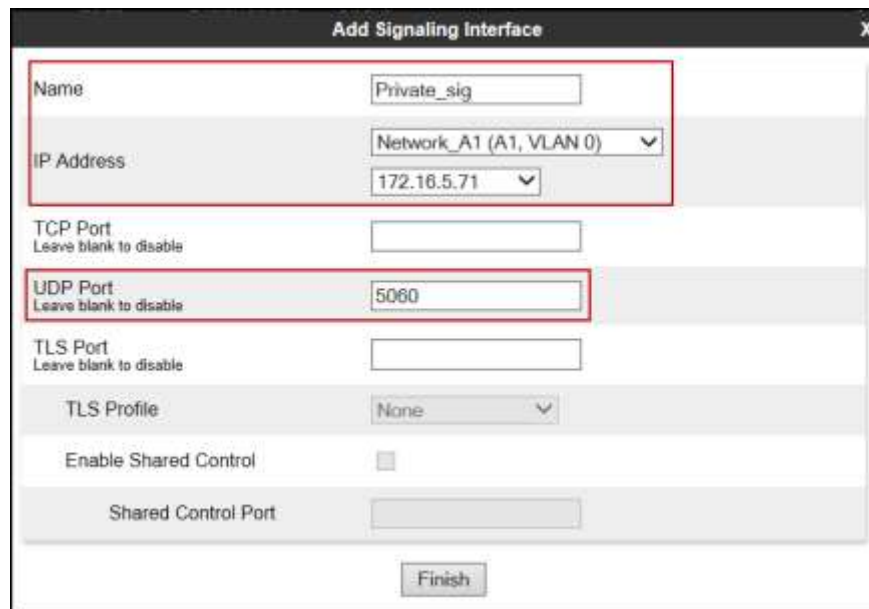
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Name	Media IP Network	Port Range		
Private_med	172.16.5.71 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Public_med	192.168.157.189 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

6.4.3 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:** **172.16.5.71** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port:** **5060**.
- Click **Finish**.



The screenshot shows a configuration window titled "Add Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a "Finish" button at the bottom. The fields are as follows:

Field	Value
Name	Private_sig
IP Address (Dropdown)	Network_A1 (A1, VLAN 0)
IP Address (Text)	172.16.5.71
TCP Port (Text)	
UDP Port (Text)	5060
TLS Port (Text)	
TLS Profile (Dropdown)	None
Enable Shared Control (Checkbox)	<input type="checkbox"/>
Shared Control Port (Text)	

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

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name:** **Public_sig**.
- Under **IP Address** select: **Network_B1 (B1, VLAN 0)**.
- Select **IP Address:** **192.168.157.189** (Outside or B1 IP Address of the Avaya SBCE, toward Cincinnati Bell).
- **UDP Port:** **5060**.
- Click **Finish**.

The screenshot shows a configuration window titled "Add Signaling Interface". The window contains several fields and a "Finish" button. The "Name" field is set to "Public_sig". The "IP Address" section has a dropdown menu set to "Network_B1 (B1, VLAN 0)" and a text field set to "192.168.157.189". The "UDP Port" field is set to "5060". The "TCP Port" field is empty. The "TLS Port" field is empty. The "TLS Profile" dropdown is set to "None". The "Enable Shared Control" checkbox is unchecked. The "Shared Control Port" field is empty. A red box highlights the "Name", "IP Address" dropdown, and "IP Address" text field. Another red box highlights the "UDP Port" field.

Name	Public_sig x
IP Address	Network_B1 (B1, VLAN 0) v
	192.168.157.189 v
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	
TLS Profile	None v
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	
Finish	

The following screen capture shows the newly created Signaling Interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) 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 title "Session Border Controller for Enterprise" and the Avaya logo.

On the left, a sidebar menu lists various administration options. The "Device Specific Settings" section is expanded, and the "Signaling Interface" option is highlighted.

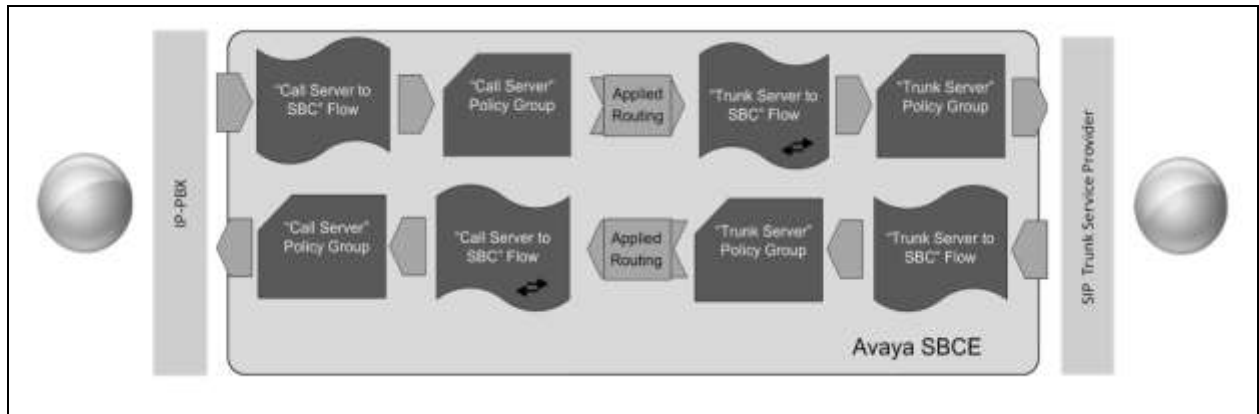
The main content area is titled "Signaling Interface: Avaya SBCE". Below this, there is a sub-tab labeled "Signaling Interface". A warning message states: "Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#)." An "Add" button is located to the right of the warning.

A table lists the configured signaling interfaces:

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Private_sig	172.16.5.71 Network_A1 (A1, VLAN 0)		5060	--	None	Edit	Delete
Public_sig	192.168.157.189 Network_B1 (B1, VLAN 0)	--	5060	--	None	Edit	Delete
...	Edit	Delete
...	Edit	Delete

6.4.4 End Point Flows

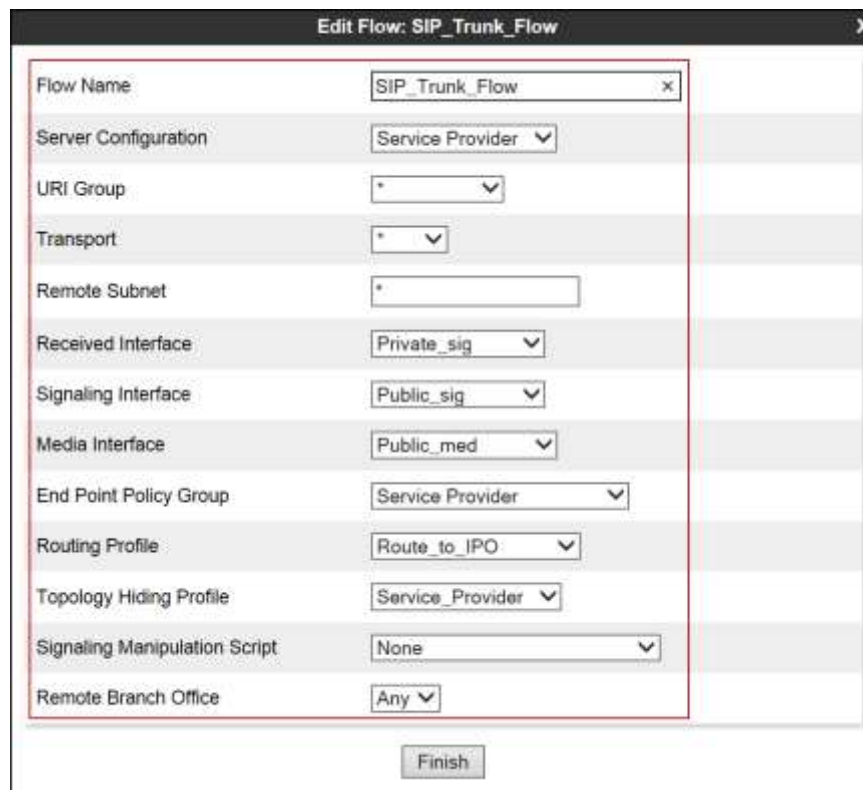
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing 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 Cincinnati Bell, 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.
- **Server Configuration:** Service Provider.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Private_sig.
- **Signaling Interface:** Public_sig.
- **Media Interface:** Public_med.
- **End Point Policy Group:** Service Provider.
- **Routing Profile:** Route_to_IPO (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**.



The screenshot shows a dialog box titled "Edit Flow: SIP_Trunk_Flow". It contains a list of configuration parameters, each with a label and a value field. The values are as follows:

Parameter	Value
Flow Name	SIP_Trunk_Flow
Server Configuration	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
End Point Policy Group	Service Provider
Routing Profile	Route_to_IPO
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom of the dialog box is a "Finish" button.

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.**
- **End Point Policy Group: Enterprise.**
- **Routing Profile: Route_to_SP** (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**.

The screenshot shows a dialog box titled "Edit Flow: IP_Office_Flow". It contains a list of configuration fields with their respective values:

Field	Value
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
End Point Policy Group	Enterprise
Routing Profile	Route to SP
Topology Hiding Profile	IP Office
Signaling Manipulation Script	None
Remote Branch Office	Any

A "Finish" button is located at the bottom of the dialog.

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, 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 its sub-item "End Point Flows" highlighted with red boxes. The main content area is titled "End Point Flows: Avaya SBCE" and features two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of configurations. Above the table is a blue bar with the text "Click here to add a row description" and an "Add" button. The table is divided into two sections: "Server Configuration: IP Office" and "Server Configuration: Service Provider". Each section has an "Update" button and a table with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. In the "IP Office" section, a row is visible with Priority 1, Flow Name "IP_Office_Flow", URI Group "*", Received Interface "Public_sig", Signaling Interface "Private_sig", End Point Policy Group "Enterprise", and Routing Profile "Route_to_SP". In the "Service Provider" section, a row is visible with Priority 1, Flow Name "SIP_Trunk_Flow", URI Group "*", Received Interface "Private_sig", Signaling Interface "Public_sig", End Point Policy Group "Service Provider", and Routing Profile "Route_to_IPO". Each row has "View", "Clone", "Edit", and "Delete" action links.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IP_Office_Flow	*	Public_sig	Private_sig	Enterprise	Route_to_SP	View Clone Edit Delete

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SIP_Trunk_Flow	*	Private_sig	Public_sig	Service Provider	Route_to_IPO	View Clone Edit Delete

7. Cincinnati Bell Business SIP Trunking Service Configuration

To use the Cincinnati Bell Business SIP Trunking service offering, a customer must request the service from Cincinnati Bell using the established sales processes. The process can be started by contacting Cincinnati Bell via the corporate web site at:

https://www.cincinnati-bell.com/customer_support/

During the signup process, Cincinnati Bell and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Cincinnati Bell's network. Cincinnati Bell will provide IP addresses, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the Avaya IP Office and Avaya SBCE configuration discussed in the previous sections.

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.

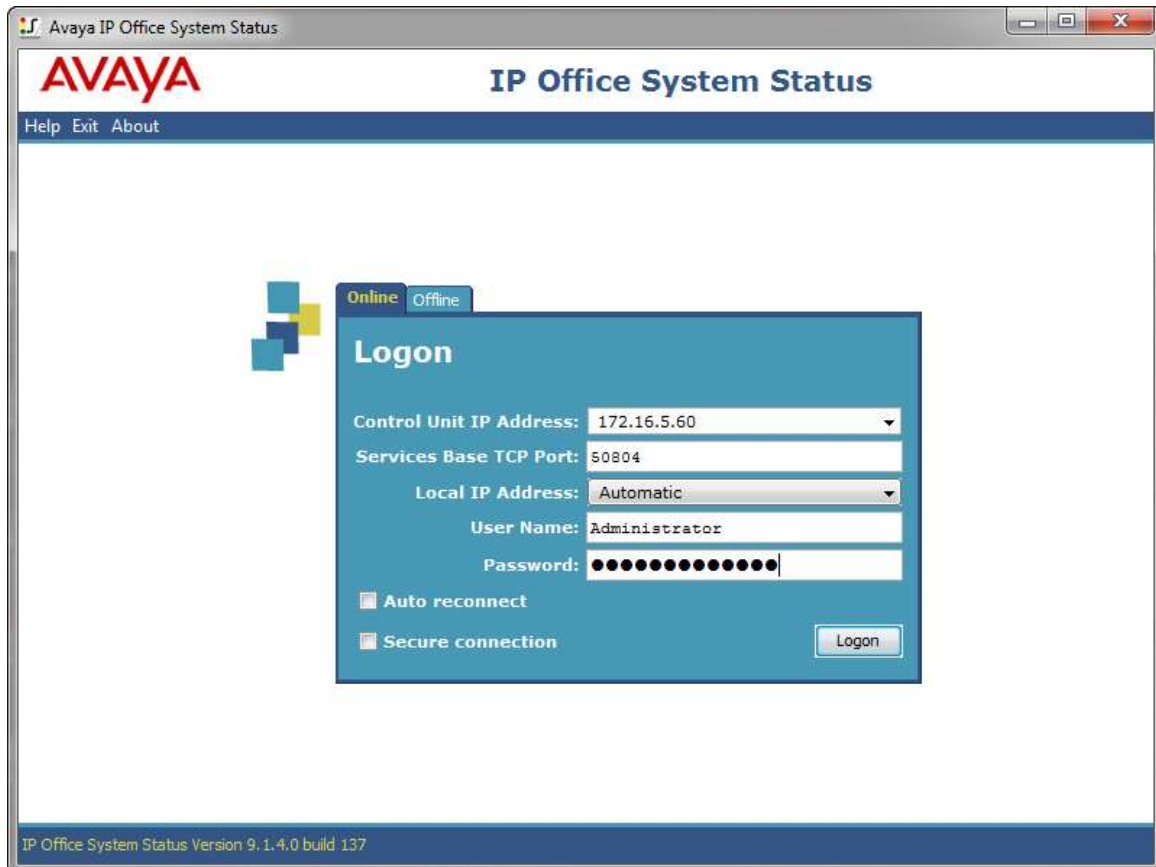
The following attributes in SIP message body are inspected using a sniffer trace analysis tool:

- 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.



- 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).

The screenshot shows the Avaya IP Office System Status application window. The title bar indicates the system is at 172.16.5.60, running IP500 V2 9.1.6.0 build 153. The left-hand navigation pane shows a tree structure with 'System' expanded, and 'Trunks (5)' selected. Under 'Trunks (5)', 'Line:17' is highlighted with a red box. The main right-hand pane has three tabs: 'Status' (selected), 'Utilization Summary', and 'Alarms'. The 'Status' tab displays the 'SIP Trunk Summary' for Line 17. The summary shows the line is 'In Service', with a peer domain of 'sip://172.16.5.71' and a resolved address of '172.16.5.71'. It lists 10 administered channels, all of which are currently 'Idle'. A green circular progress indicator shows 0% utilization. Below the summary is a table with 15 columns: Channel, U..., Call Ref, Curr..., Time in State, Remote Media..., C..., Con..., Caller ID o..., Other Party on..., Dire..., Round Trip ..., Rec..., Rec..., Tran..., and Tran... The first 10 rows of the table show channels 1 through 10, all with a 'Curr...' state of 'Idle' and a 'Time in State' of '00:0...'. At the bottom of the window, there is a row of buttons: 'Trace', 'Trace All', 'Pause', 'Ping', 'Call Details', 'Graceful Shutdown', and 'Force Out of Service'. Below these are 'Print...' and 'Save As...' buttons. The bottom status bar shows the time as 4:34:00 PM and the system is 'Online'.

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System

Alarms (15)

Extensions (26)

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://172.16.5.71

Resolved Address: 172.16.5.71

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: RTP

Layer 4 Protocol: UDP

SIP Trunk Channel Licenses: Unlimited

SIP Trunk Channel Licenses in Use: 0

SIP Device Features: REFER (Incoming and Outgoing)

0%

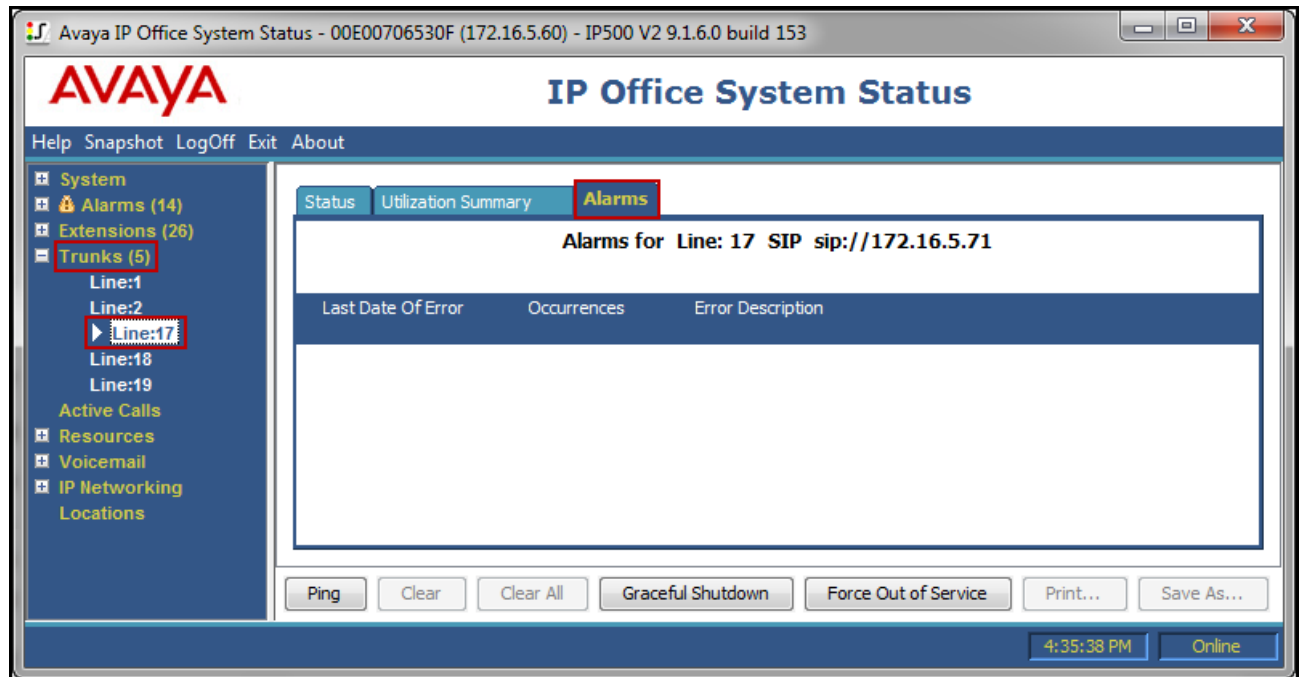
Cha...	U...	Call Ref	Curr...	Time in State	Remote Media...	C...	Con...	Caller ID o...	Other Party on...	Dire...	Round Trip ...	Rec...	Rec...	Tran...	Tran...
1			Idle	00:0...											
2			Idle	00:0...											
3			Idle	00:0...											
4			Idle	00:0...											
5			Idle	00:0...											
6			Idle	00:0...											
7			Idle	00:0...											
8			Idle	00:0...											
9			Idle	00:0...											
10			Idle	00:0...											

Trace Trace All Pause Ping Call Details Graceful Shutdown Force Out of Service

Print... Save As...

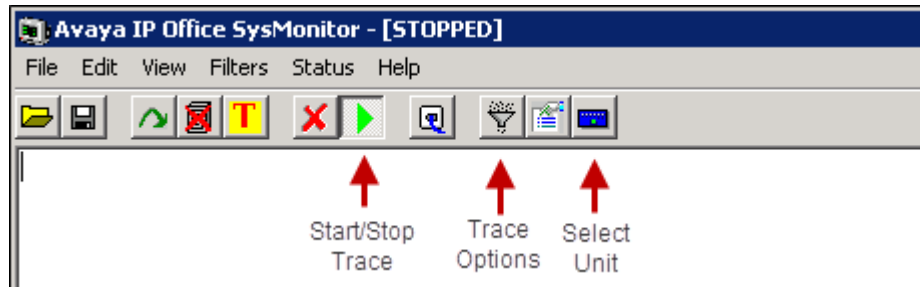
4:34:00 PM Online

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

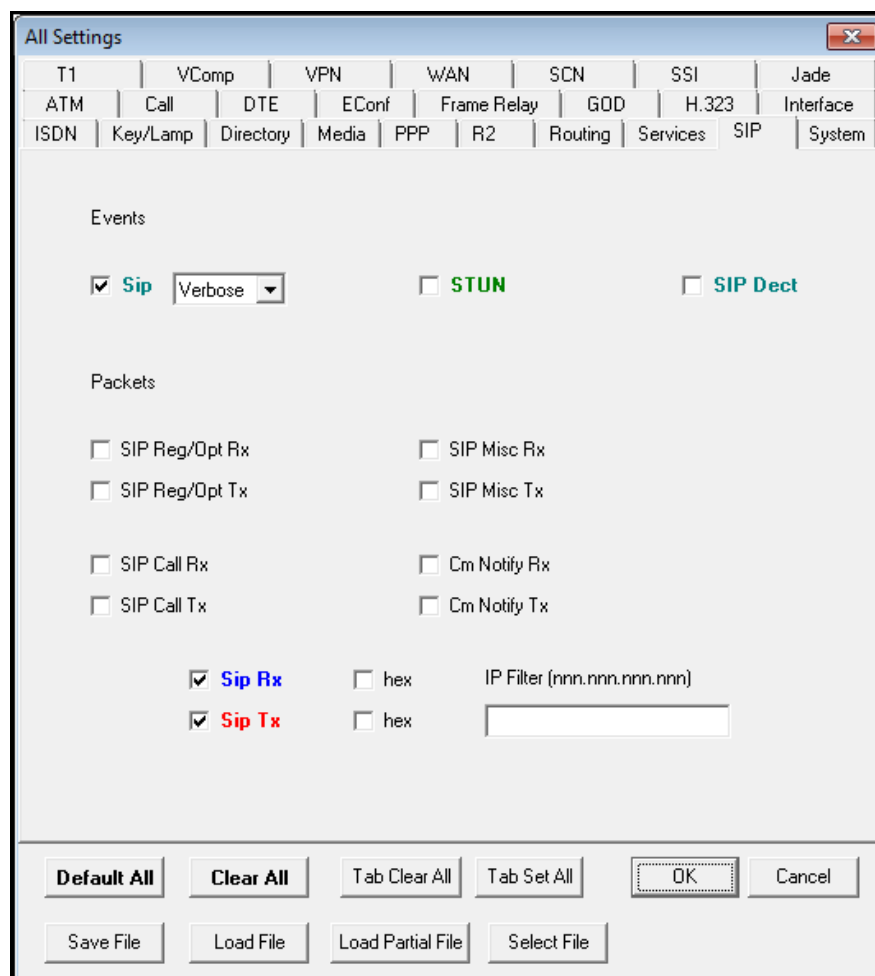


8.4 IP Office Monitor

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

Information

System Time	05:24:25 AM CDT	Refresh
Version	7.0.1-03-8739	
Build Date	Fri Jan 15 22:53:12 EST 2016	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	03/21/2016 01:49:31 CDT	
Failed Login Attempts	0	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

Notes

No notes found.

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

Alarm Viewer

Devices

EMS
Avaya SBCE

Alarms

<input checked="" type="checkbox"/>	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

Dashboard

Information

System Time	05:24:25 AM CDT	Refresh
Version	7.0.1-03-0739	
Build Date	Fri Jan 15 22:53:12 EST 2016	
License State	OK	
Aggregate Licensing Oversages	0	
Peak Licensing Overage Count	0	
Last Logged in at	03/21/2016 01:48:31 CDT	
Failed Login Attempts	0	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

Notes

No notes found.

The following screen shows the Incident Viewer page.

Incident Viewer

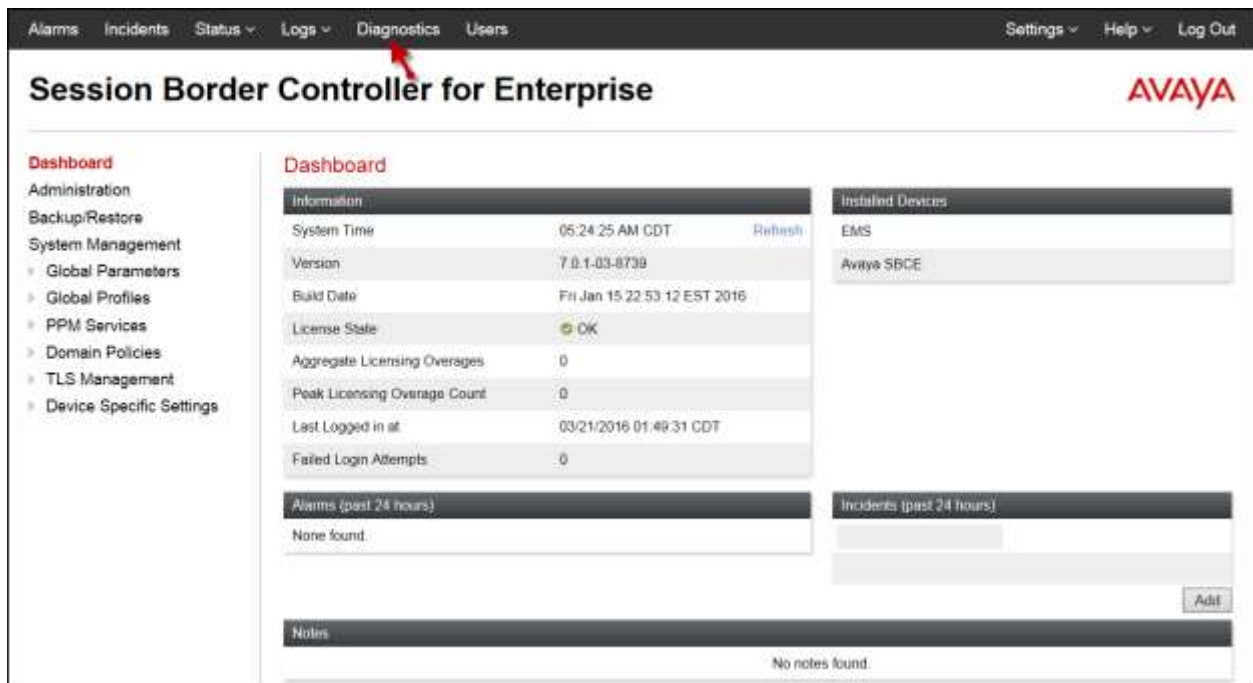
Device: All Category: All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 2002.

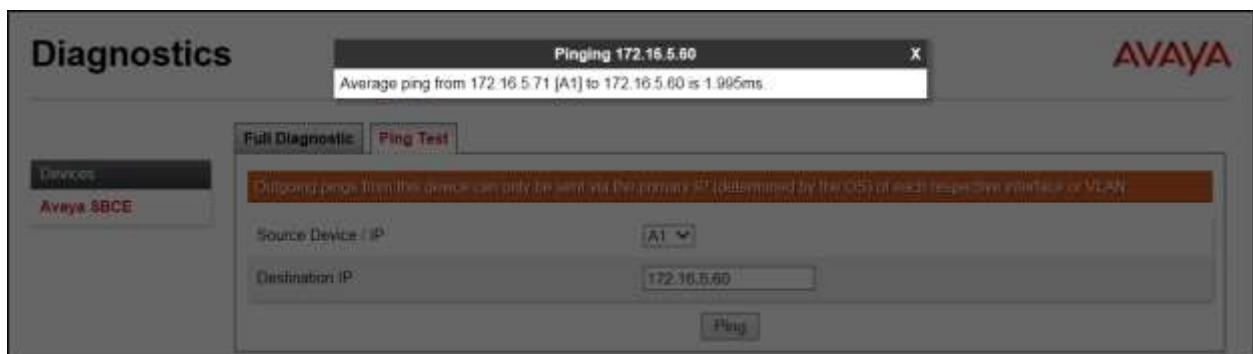
Type	ID	Date	Time	Category	Device	Cause
Routing Failure	729364126490041	3/23/16	5:17 AM	Policy	Avaya SBCE	Max forwards Exceeded
Routing Failure	729364096481672	3/23/16	5:16 AM	Policy	Avaya SBCE	Max forwards Exceeded

<< < 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 management 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. On the left sidebar, the "Device Specific Settings" menu is expanded, showing options like Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, and Advanced Options. Under "Advanced Options", the "Troubleshooting" section is selected, and the "Trace" option is highlighted. The main content area is titled "Trace: Avaya SBCE" and features two tabs: "Packet Capture" (active) and "Captures". The "Packet Capture Configuration" form includes the following fields: Status (Ready), Interface (A1), Local Address (IP:Port) (All), Remote Address (IP:Port) (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Test.pcap). A note below the filename field states: "Using the name of an existing capture will overwrite it." At the bottom of the form are "Start Capture" and "Clear" buttons.

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 (SBCE) 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. On the left, a sidebar menu lists various configuration and management options, including TLS Management, Device Specific Settings, Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, Troubleshooting, Debugging, Trace, DoS, and Learning. The "Trace: Avaya SBCE" section is active, showing a "Devices" dropdown menu with "Avaya SBCE" selected. Below this, there are two tabs: "Packet Capture" and "Captures", with the latter being selected. A "Refresh" button is located to the right of the table. The table lists captured files with columns for File Name, File Size (bytes), and Last Modified. One file is listed: "Test_20151012004900.pcap" with a size of 12,288 bytes and a last modified date of October 12, 2015 12:49:10 AM CDT. A "Delete" button is visible next to the file name.

File Name	File Size (bytes)	Last Modified
Test_20151012004900.pcap	12,288	October 12, 2015 12:49:10 AM CDT

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 9.1 and the Avaya Session Border Controller for Enterprise Release 7.0 to support Cincinnati Bell Business 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] *Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 30zc, March 21, 2016.
- [2] *Using Avaya IP Office Platform System Status*, Document Number 15-601758, Issue 10f, August 2015.
- [3] *Administering Avaya IP Office Platform Voicemail Pro*, Document Number 15-601063, Issue 10m, February 05, 2016.
- [4] *Using IP Office System Monitor*, Document Number 15-601019, Issue 06g, February 08, 2016.

Product documentation for the Avaya Session Border Controller for Enterprise, including the following, is available at: <http://support.avaya.com/>

- [5] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
- [6] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.

Additional Avaya IP Office documentation can be found at:

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

©2016 Avaya Inc. All Rights Reserved.

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

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