



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 Charter 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 Charter 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.

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

Charter 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 – SIP Advanced Tab	28
5.5 Extension.....	29
5.6 Users	31
5.7 Incoming Call Route	35
5.8 Outbound Call Routing.....	37
5.8.1 Short Codes and Automatic Route Selection.....	37
5.9 Save Configuration	39
6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).....	40
6.1 Log in Avaya SBCE.....	40
6.2 Global Profiles	43
6.2.1 Server Interworking – Avaya-IPO	43
6.2.2 Server Interworking - SP-General.....	46
6.2.3 Server Configuration.....	49
6.2.4 Routing Profiles	55
6.2.5 Topology Hiding.....	58
6.3 Domain Policies	61
6.3.1 Application Rules.....	61
6.3.2 End Point Policy Groups.....	62
6.4 Device Specific Settings	66
6.4.1 Network Management.....	66
6.4.2 Media Interface	68
6.4.3 Signaling Interface	70
6.4.4 End Point Flows	73
7. Charter Business SIP Trunk Service Configuration	77

8. Verification and Troubleshooting.....	78
8.1 Verification Steps.....	78
8.2 Protocol Traces	78
8.3 IP Office System Status	79
8.4 IP Office Monitor.....	82
8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)	83
9. Conclusion	88
10. References.....	89

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Charter 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.

As a required component of the Charter Business SIP Trunking service offering, Charter will install a Modular Access Router at the customer premises (enterprise site). Charter will perform the initial configuration and maintenance as required. The Modular Access Router will be considered Customer Premises Equipment (CPE).

The Charter 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 “Charter” 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 Charter 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 Charter 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 networks.
- 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 networks.
- 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 (Charter supported audio codec).
- Proper response to no matching codecs.
- 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:

- The use of the SIP REFER method for network call redirection is not currently supported by Charter.
- Inbound toll-free calls and 911 emergency calls are supported but were not tested as part of the compliance test.
- T.38 fax is not supported by Charter; therefore T.38 fax was not tested, G.711 Fax Pass-through was tested successfully and it is recommended instead.

2.2 Test Results

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

- **No matching codec on outbound calls:** If an unsupported audio codec is received by Charter on the SIP Trunk (e.g., 722), Charter will respond with “480 Temporarily Unavailable” instead of “488 Not Acceptable Here”, the user will hear re-order. 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.
- **Inbound calls to an unassigned enterprise extension:** IP Office sends a “404 Not Found” message to Charter when it receives calls to an unassigned extension, the user hears re-order instead of the common announcement informing the user that he/she has reached a non-working number, to please check the number and to try again. This issue is considered non service affecting and it’s being investigated by Charter, in order to apply the correct announcement to the user.

2.3 Support

For support on Charter Business SIP Trunking service visit the corporate Web page at: <https://www.charterbusiness.com/> or call 800-314-7195

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 Charter 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.

In the reference configuration, a Modular Access Router was required at the simulated enterprise site, acting as a SIP interface between the Avaya simulated enterprise and Charter’s network. Charter will install the Modular Access Router at the customer premises (enterprise site). Charter will

perform the initial configuration and maintenance as required. The Modular Access Router will be considered Customer Premises Equipment (CPE).

Located at the enterprise site is the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **A1** and **B1**. Interface **B1** was used to connect to the public network, and was only used for Remote Worker functionality. Access to the enterprise site by Remote Worker users was done via interface **B1**. Interface **A1** was used to connect to the enterprise private network (LAN). All SIP Trunk related traffic, entering or leaving the enterprise site, from Charter's network, across the public network, first flowed through Charter's Modular Access Router, to the Avaya SBCE (interface **A1**), then to IP Office (**LAN1** port). Remote Workers also used interface **A1** for connectivity to the enterprise private network (LAN), Remote Worker configuration is not discussed in this Application Notes.

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 codecs. The IP Office **LAN1** port was connected to the enterprise private network (LAN).

For inbound calls, the calls flowed from the PSTN to Charter's network, across the public Internet, to Charter's Modular Access Router, 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, to Charter's Modular Access Router, across the public Internet, to Charter's network.

The transport protocol between IP Office and the Avaya SBCE, across the enterprise private network (LAN), is SIP over UDP. The transport protocol between the Avaya SBCE and Charter's Modular Access router, across the enterprise private network (LAN), 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 Charter (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 Charter 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 Charter 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.

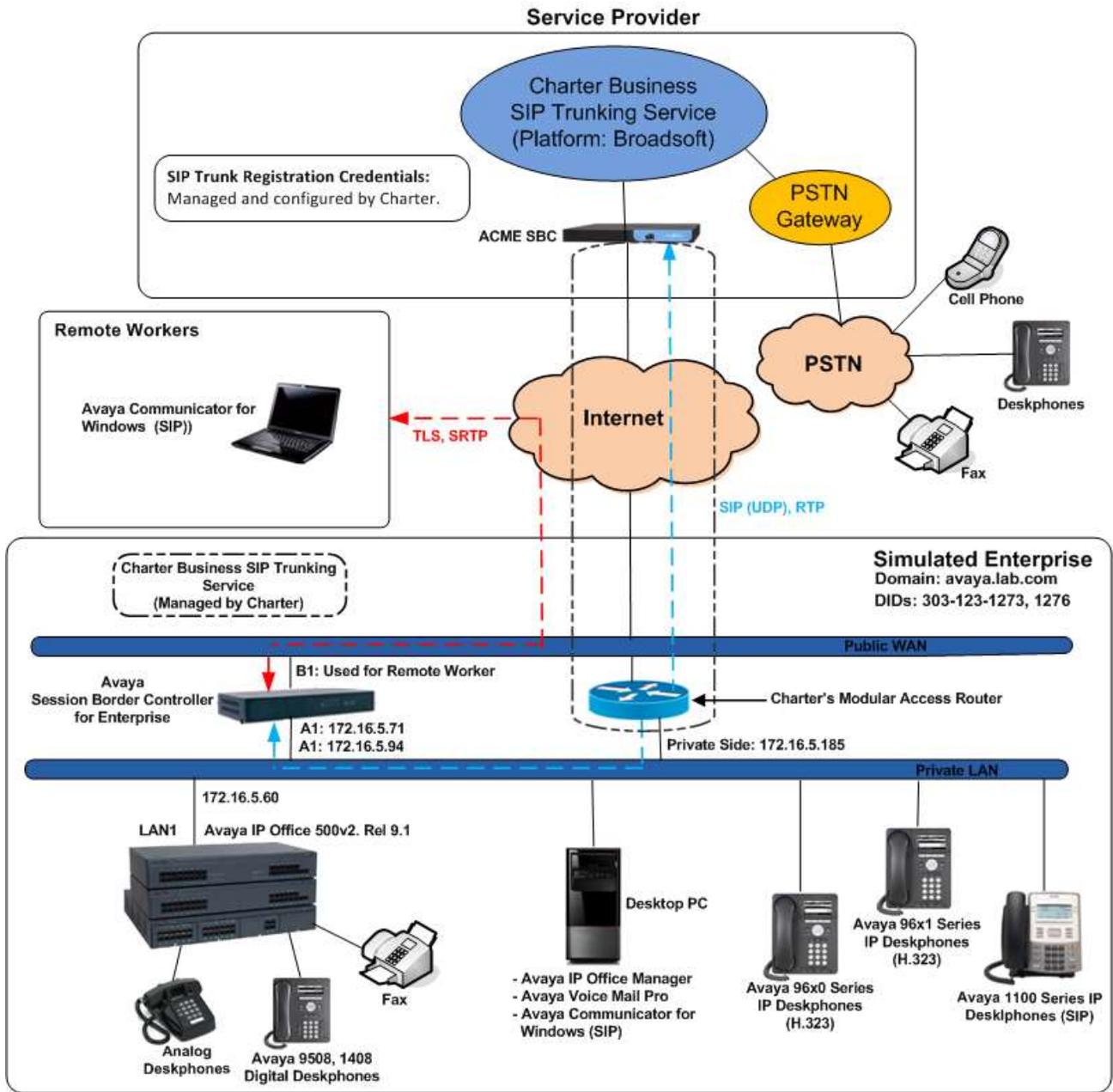


Figure 1: Avaya Interoperability Test Lab Configuration.

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	9.1.4.0 Build 137
Avaya IP Office DIG DCPx16 V2	9.1.4.0 Build 137
Avaya IP Office Manager	9.1.4.0 Build 137
Avaya Voicemail Pro Client	9.1.4.0 Build 7
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.0.0-21-6602
Avaya 96x0 IP Deskphones (H.323)	Avaya one-X® Deskphone Edition S3.230A
Avaya 96x1 Series IP Deskphones (H.323)	Avaya one-X® Deskphone H.323 Version 6.6029
Avaya 1120E IP Deskphones (SIP)	SIP1120e Ver. 04.04.18.00
Avaya Communicator for Windows	2.0.3.33
Avaya Digital Deskphones 1408	40.0
Avaya Digital Deskphones 9508	0.55
Lucent Analog Phone	--
Charter	
Broadworks Broadsoft Application Server	AS_Rel_17.sp4_1.197
Acme Packet 4500 Series SBC	SCX6.2.0 MR-9 GA (Build 1014)
Adtran NetVanta 3430 Modular Access Router	R10.3.0.V

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 Charter 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** in the Navigation pane and **SIP Trunk Channels**. Confirm that there is a valid license with sufficient “Instances” (trunk channels) in the Details pane. Note that the full License Keys in the screen below is not shown for security purposes.

The screenshot displays the Avaya IP Office Manager interface. On the left is the 'IP Offices' navigation pane with a tree view including categories like BOOTP, Operator, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WAN Port, Directory, Time Profile, Firewall Profile, IP Route, Account Code, License (74), Tunnel, User Rights, ARS, RAS Location Request, and Location. The 'License (74)' item is selected and highlighted in blue. The main area shows the 'License' configuration for 'SIP Trunk Channels'. At the top, there are tabs for 'License' and 'Remote Server'. Below the tabs, the 'License Mode' is set to 'License Normal' and the 'PLDS Host ID' is '111309813681'. A table lists various features and their license details:

Feature	License Key	Instances	Status	Expiry Date	Source
Report Viewer	Tvct73mdgdG...	255	Valid	Never	ADI Nodal
Mobility Features	0ICluRgHvKOx...	255	Obsolete	Never	ADI Nodal
Advanced Small Community Netw...	DaQJl7Ve5vUU...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	T39BkqBXvd6...	255	Valid	Never	ADI Nodal
IP500 Upgrade Standard to Profess...	QaHgn76v9j6...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	JaHLHAVFXjD...	4	Valid	Never	ADI Nodal
SIP Trunk Channels	IBCQzGBYDU...	255	Valid	Never	ADI Nodal
VPN IP Extensions	@qm3fOoR5S...	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional cha...	2TXC@OoNQ...	255	Valid	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	hXIRxBVCEKN...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Standar...	4AOGBV5D9D...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Professi...	dlyY_Dba5Uq7...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Stan...	dv956B9iXS_N...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Prof...	LlHFzqB6XleQ...	255	Valid	Never	ADI Nodal
UMS Web Services	pGcSuPdLASj...	255	Valid	Never	ADI Nodal
Customer Service Agent	jD0xhEoAADH0...	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

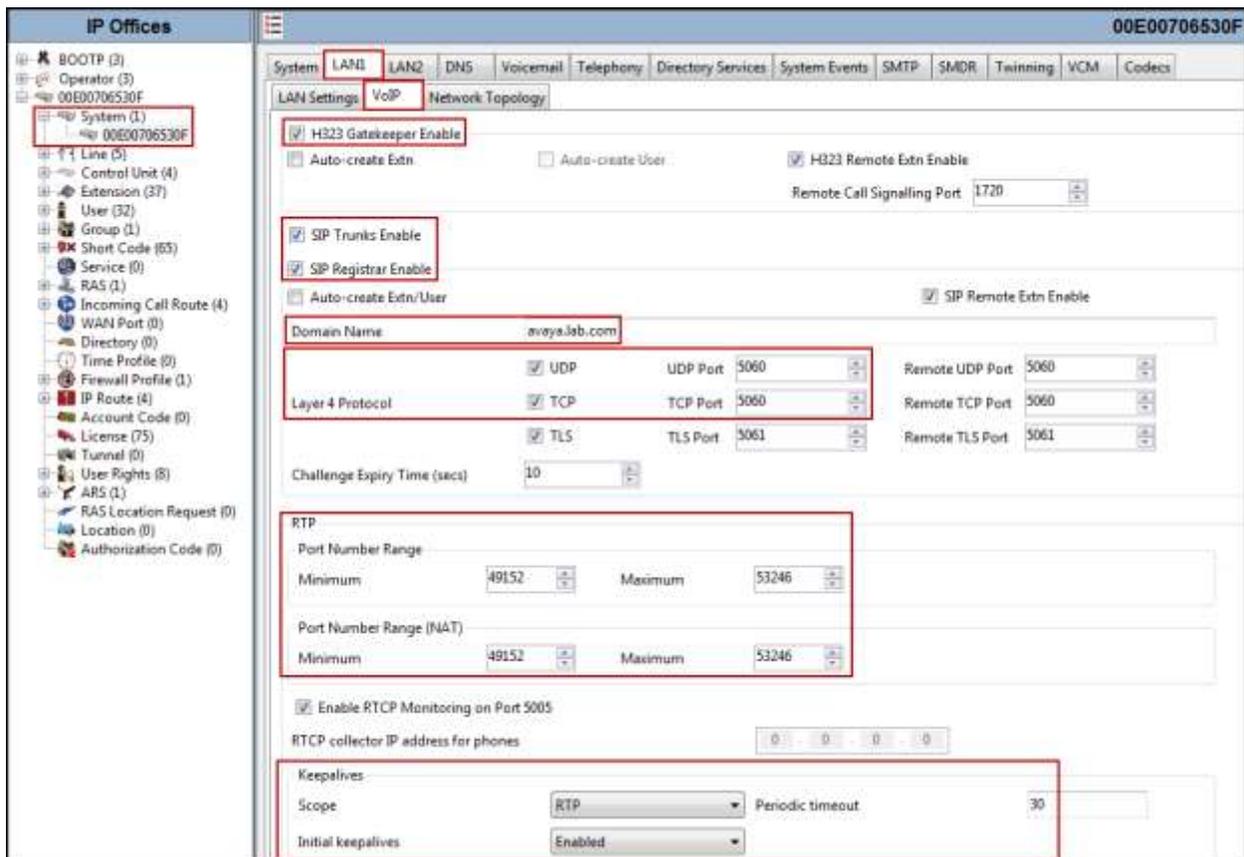
In the sample configuration, the MAC address **00E00706530F** was used as the system name. The **LAN** port connects to the Avaya SBCE across the enterprise LAN (private) network. The **LAN1** settings correspond to the **LAN** port in IP Office. To access the **LAN1** settings, navigate to **System (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 public 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 of system components. The 'System (1)' folder is expanded, and the specific system '00E00706530F' is selected and highlighted with a red box. On the right is the configuration details pane for this system. The 'LAN1' tab is active, and the 'LAN Settings' sub-tab is selected. 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 highlighted with a red box. Other visible settings include 'Primary Trans. IP Address' set to '0 . 0 . 0 . 0', 'RIP Mode' set to 'None', 'Enable NAT' checked, 'Number Of DHCP IP Addresses' set to '200', and 'DHCP Mode' set to 'Disabled'. An 'Advanced' button is visible at the bottom right of the settings pane.

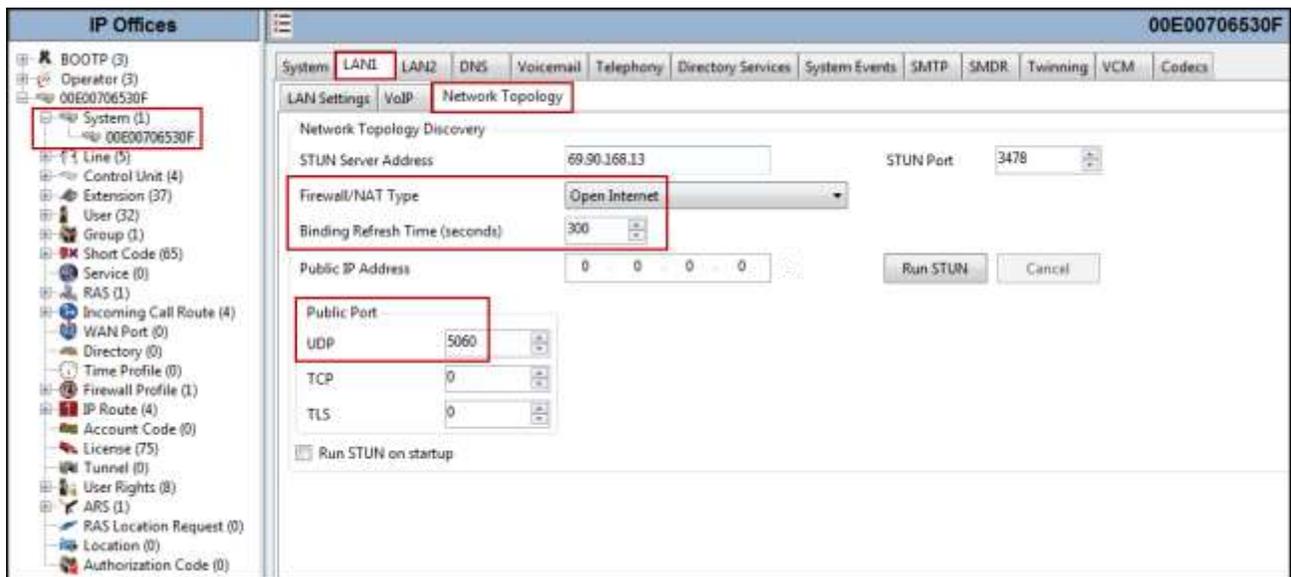
The **VoIP** tab as shown in the screenshot below was configured with following settings:

- 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 Charter.
- 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).



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

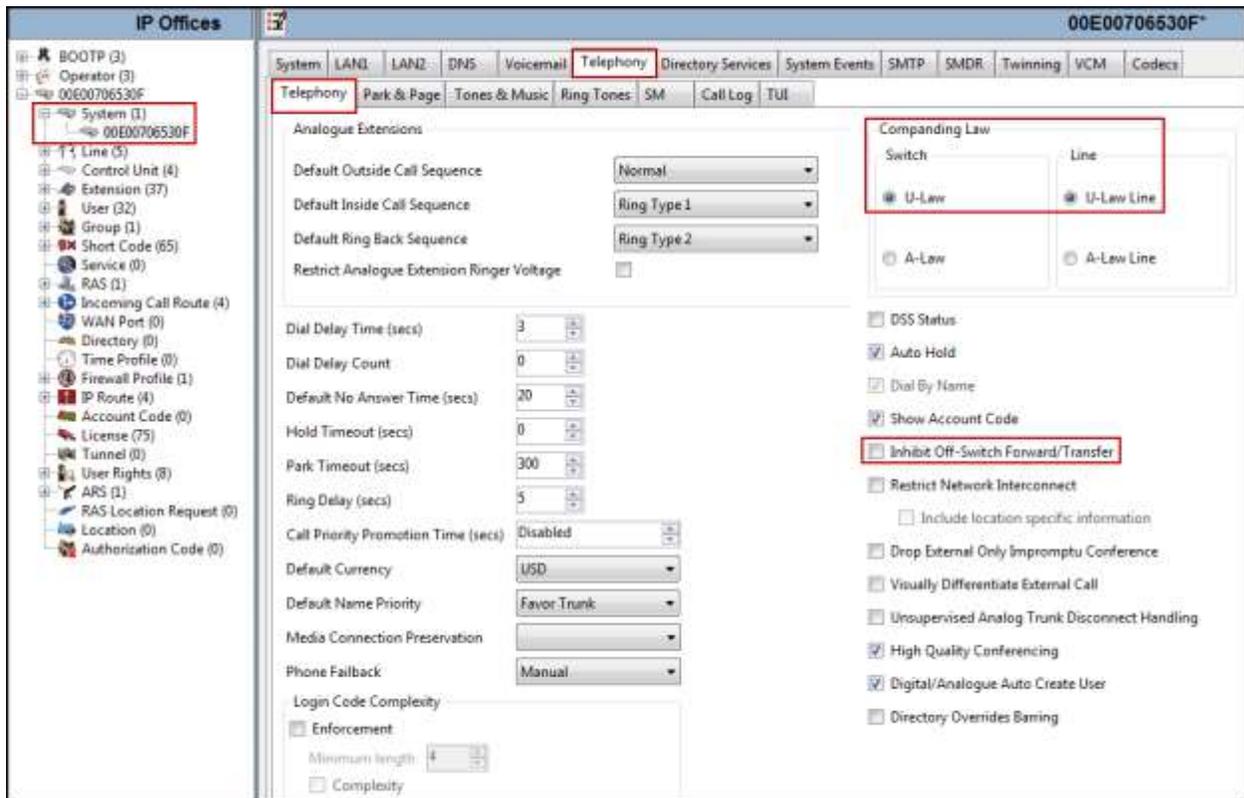
- Select the **Firewall/NAT Type** from the pull-down menu to the option that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even though the default STUN settings are populated, they will not be used.
- Set the **Binding Refresh 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).



5.2.2 System - Telephony Tab

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

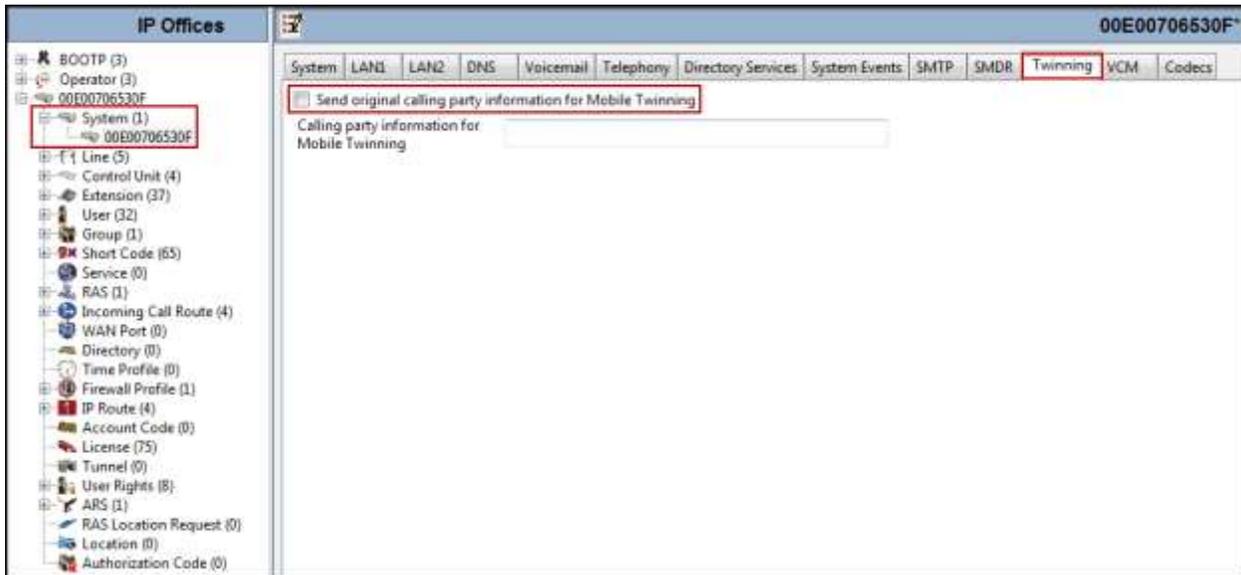
- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer 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:

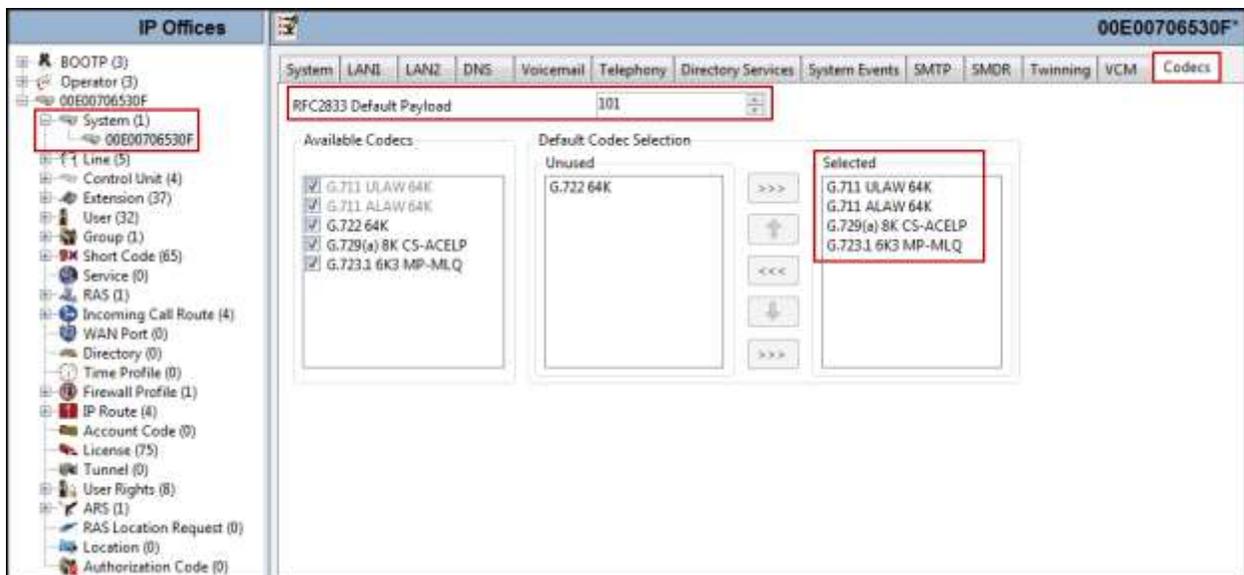
- Uncheck the **Send original calling party information for Mobile Twinning** box. This will allow the Caller ID for Twinning to be controlled by the setting on the SIP Line (**Section 5.4**). This setting also impacts the Caller ID for call forwarding.
- Click **OK** to commit (not shown).



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 shows the IP Office configuration interface. On the left is a tree view of configuration objects. The 'IP Route (4)' folder is expanded, and the '0.0.0.0' entry is selected and highlighted with a red box. On the right, the configuration details for the selected IP Route are shown. 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' is set to '0'. There is a checkbox for 'Proxy ARP' which is currently unchecked.

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 Charter 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 **5.4.7**.

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 **5.4.7**.

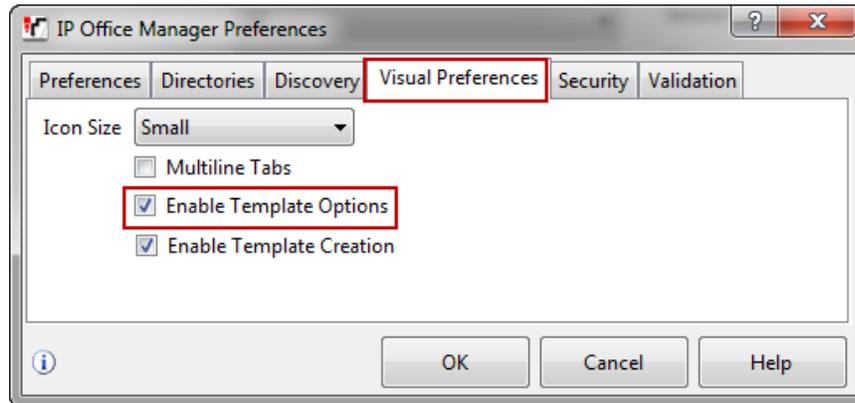
5.4.1 Importing a SIP Line Template

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.

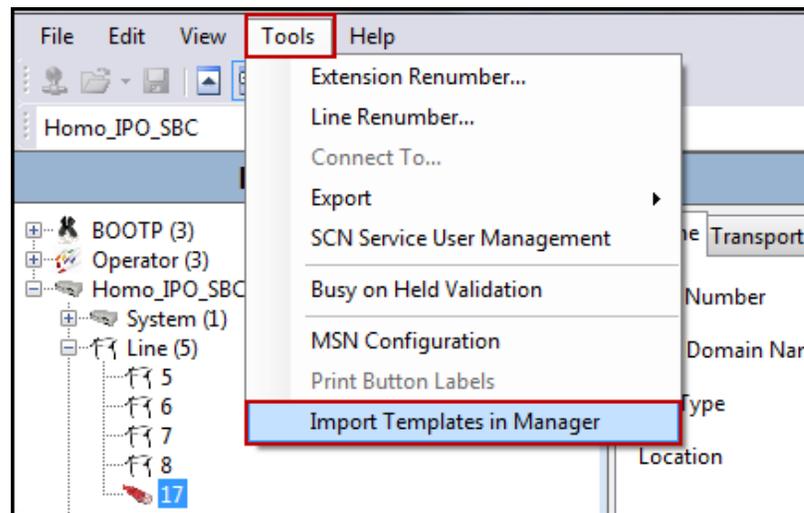
1. Copy a previously created template file to a location (e.g., C:\Temp) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **AF_<user supplied text>_SIPTrunk.xml**, where the **<user supplied text>** portion is entered during template file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

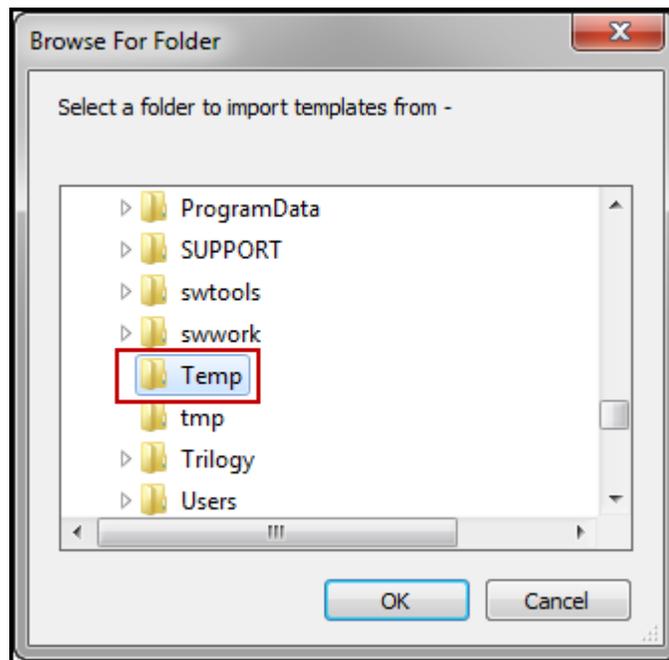
2. Verify that Template Options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the **Visual Preferences** tab. Check the box next to **Enable Template Options**. Click **OK**.



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

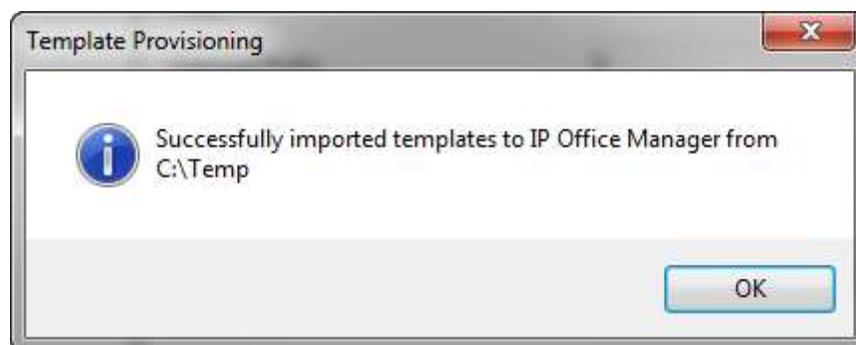


4. A folder browser will open. Select the directory used in **step 1** to store the template(s) (e.g., *C:\Temp*).

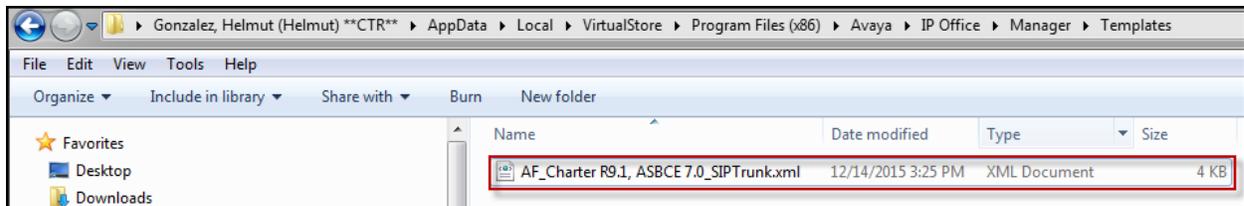
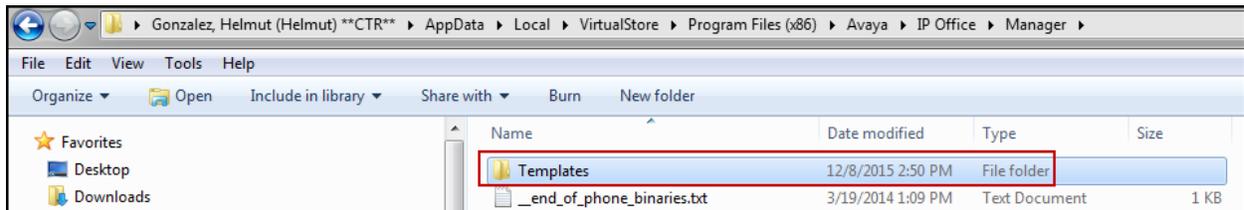
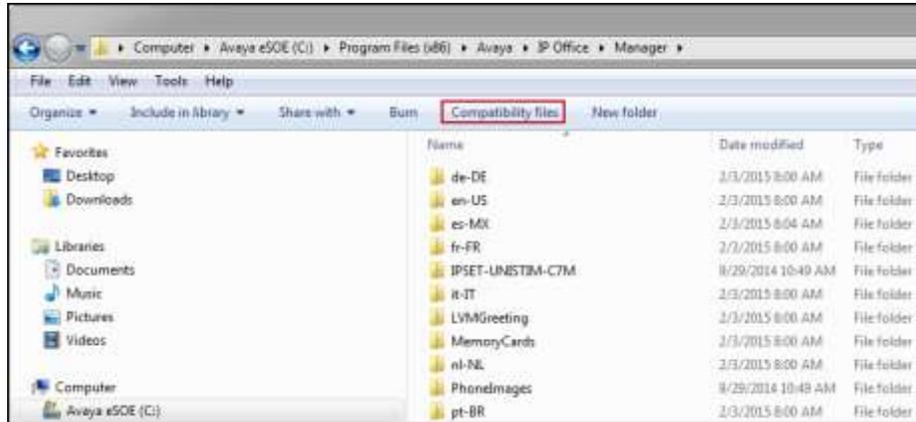


In the reference configuration, template files **AF_Charter R9.1**, **ASBCE 7.0_SIPTrunk.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

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

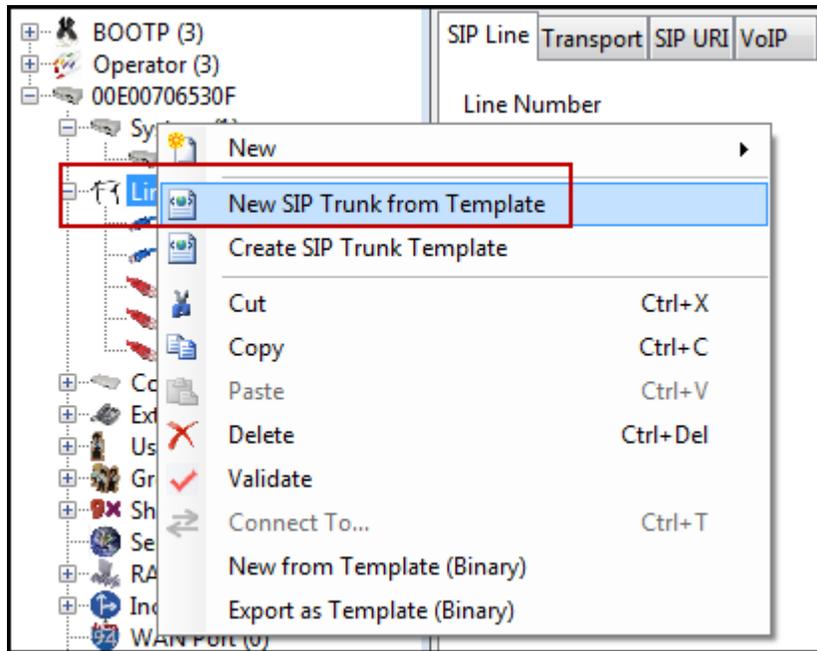


Note: Windows 7 (and later) locks the Avaya IP Office 9.1 **\Templates** directory, and it cannot be viewed. To enable browsing of the **\Templates** directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or **C:\Program Files (x86)\Avaya\IP Office\Manager\Templates**),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



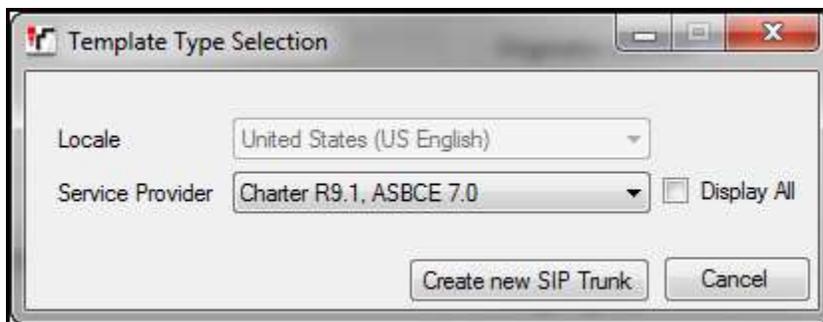
5.4.2 Creating a SIP Trunk from an XML Template

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

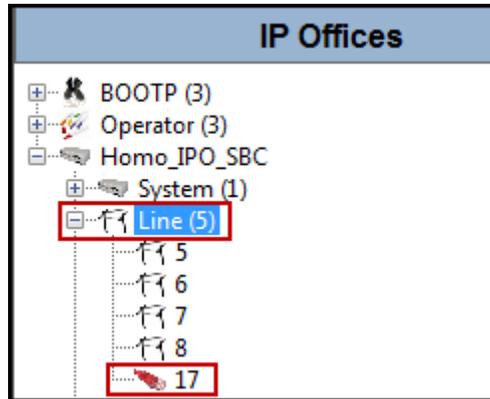


2. In the subsequent **Template Type Selection** pop-up window, from the **Service Provider** pull-down menu, select the XML template name from **Section 5.4.1**. Click **Create new SIP Trunk**.

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).

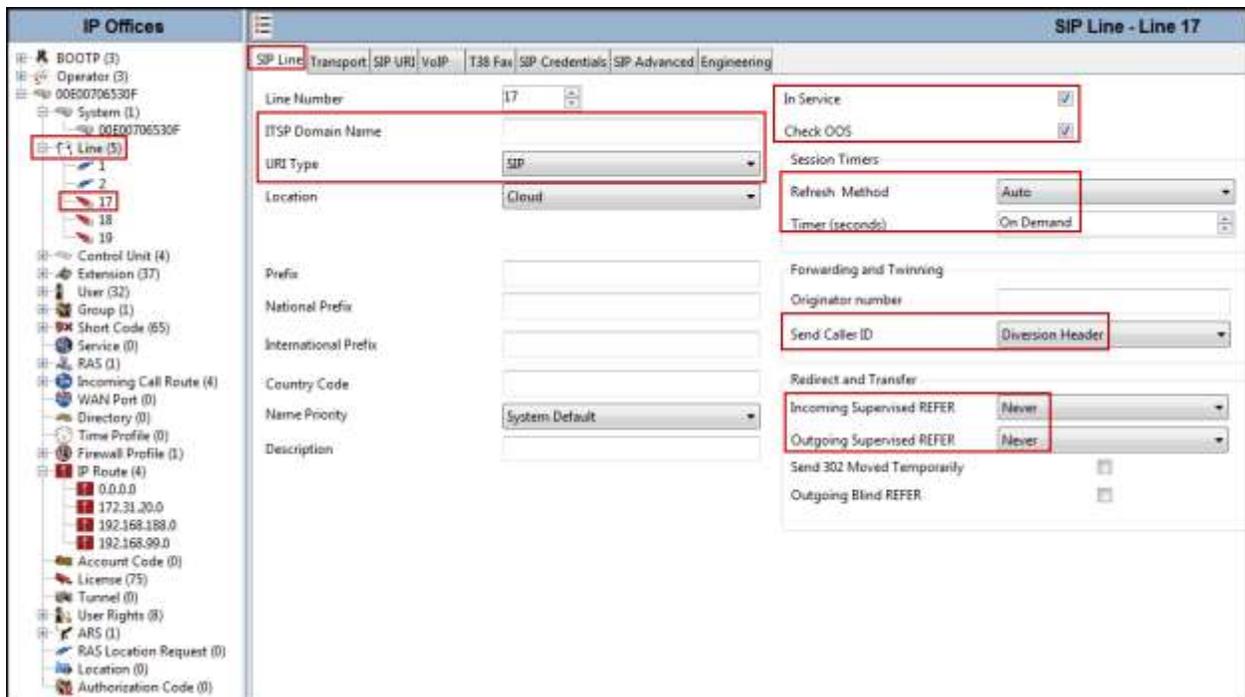


It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.3 to 5.4.7**.

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 **Never** (see **Section 2.1**).
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).



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, IP address **172.16.5.94** was used to connect to Charter's Modular Access Router, 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, a tree view under 'IP Offices' shows a hierarchy including 'Line (5)', with 'Line 17' selected and highlighted with a red box. The main configuration area on the right is titled 'SIP Line - Line 17' and has several tabs: 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'Transport' tab is active 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, the 'Network Configuration' section is highlighted with a red box and contains the following settings: 'Layer 4 Protocol' is set to 'UDP', 'Send Port' is set to '5060', and 'Use Network Topology Info' is set to 'LAN1'. The 'Listen Port' is also set to '5060'. Other fields include 'Explicit DNS Server(s)' set to '0 . 0 . 0 . 0', 'Calls Route via Registrar' checked, and 'Separate Registrar' set to an empty field.

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 displays the Avaya IP Office configuration interface. On the left, a tree view shows the hierarchy of IP Offices, with 'Line (5)' selected and '17' highlighted. The main pane shows the 'SIP URI' tab for a SIP Line. A table lists the channels, with channel 1 selected. The 'Edit Channel' form is open, showing the following fields:

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	17 17	1...				N...	0: <Non...	10

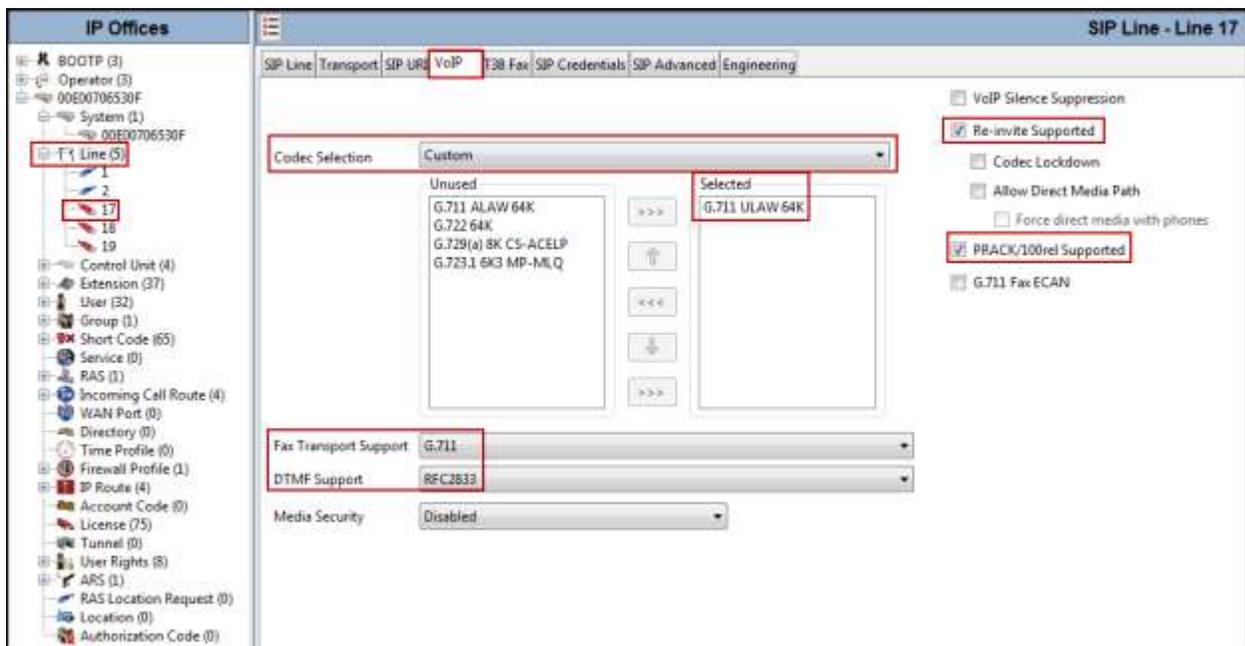
The 'Edit Channel' form fields are:

- 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
- Max Calls per Channel: 10

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. Charter only supports codec G.711ULAW for audio.
- Select **G.711** 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 Charter.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

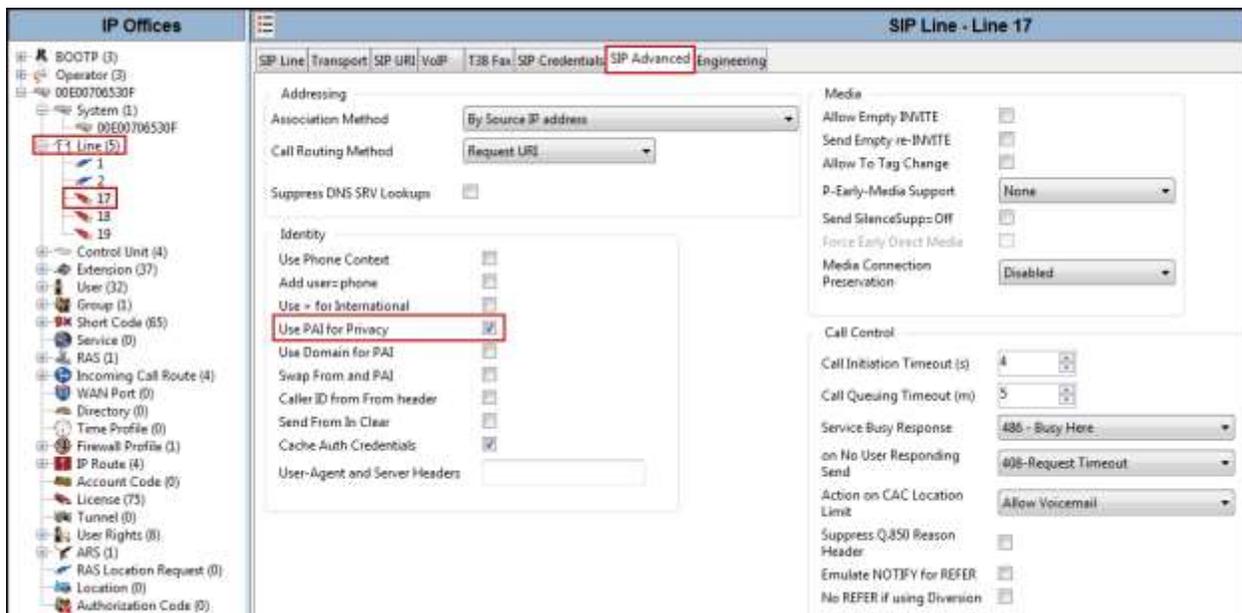


Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.4** (System – Codecs tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

5.4.7 SIP Line – 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**.
- 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**.

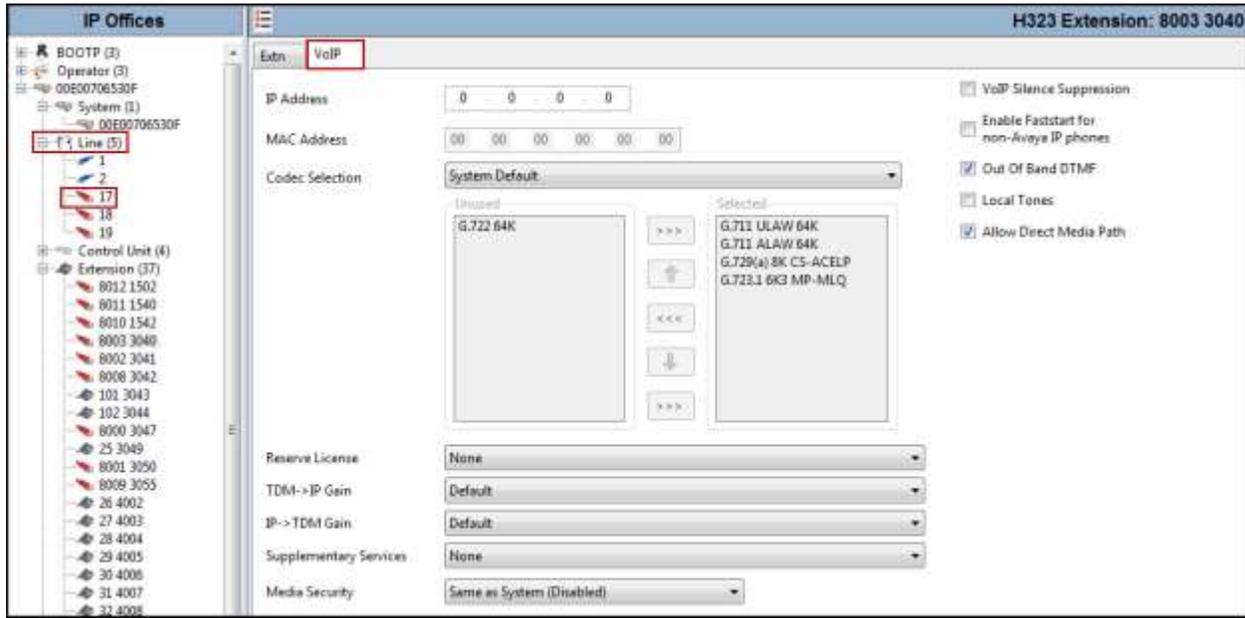
Select the **Extn** tab. Following is an example of extension 3040; this extension corresponds to an H.323 extension.

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows a hierarchy: BOOTP (5), Operator (3), System (1) 00E00706530F, Line (3) 1, 2, 17, and Control Unit (4). Under 'Control Unit (4)', there is an 'Extension (38)' folder, which is expanded to show a list of extensions: 8012 1502, 8011 1540, 8010 1542, 8003 3040 (highlighted with a red box), 8002 3041, 8008 3042, 101 3043, 102 3044, 8000 3047, 25 3049, and 8001 3050. The main configuration pane on the right is titled 'H323 Extension: 8003 3040' and has two tabs: 'Extn' (selected and highlighted with a red box) and 'VoIP'. The configuration fields are as follows:

Field	Value
Extension Id	8003
Base Extension	3040
Phone Password	
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Avaya 9620
Location	Automatic
Module	0
Port	0
Disable Speakerphone	<input type="checkbox"/>

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

By default, all IP phones (SIP and H.323) will use the system default codec selection configured under the System 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 **Ext3040 H323**.

The screenshot displays the Avaya user configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'User (32)' expanded, and '3040 Ext3040 H323' selected. The main panel is titled 'Ext3040 H323: 3040' 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: Ext3040 H323
- Password: [Redacted]
- Confirm Password: [Redacted]
- Account Status: Enabled
- Full Name: Ext3040 H323
- Extension: 3040
- Email Address: [Empty]
- Locale: [Dropdown]
- Priority: 5
- System Phone Rights: None
- ACCS Agent Type: None
- Profile: Basic User

Below the profile dropdown, there are several checkboxes for additional services:

- Receptionist
- Enable Softphone
- Enable one-X Portal Services
- Enable one-X TeleCommuter
- Enable Remote Worker
- Enable Flare
- Enable Mobile VoIP Client
- Send Mobility Email
- Ex Directory

The 'Device Type' is set to 'Avaya 9620'. At the bottom, the 'User Rights' section includes:

- User Rights view: User data
- Working hours time profile: <None>
- Working hours User Rights: [Dropdown]

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**.

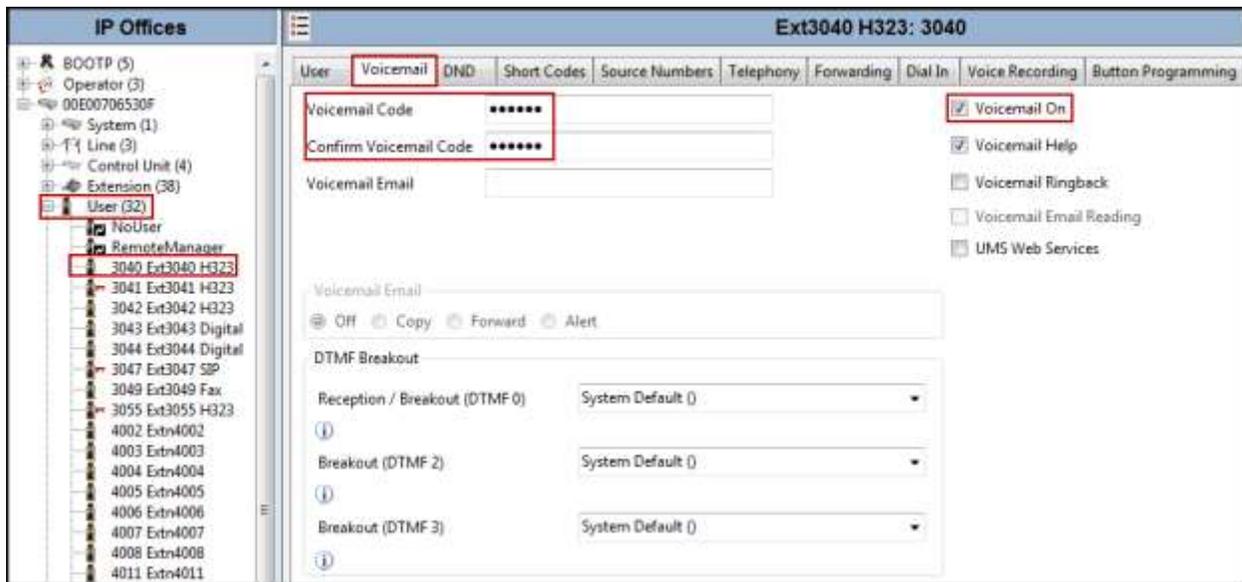
The screenshot displays the Avaya user configuration interface for a user named "Ext3047 SIP: 3047". The interface is divided into two main sections: a left-hand navigation tree and a right-hand configuration panel.

Left Panel (IP Offices): A tree view showing the organizational structure. Under "User (32)", the user "3047 Ext3047 SIP" is selected and highlighted with a red box.

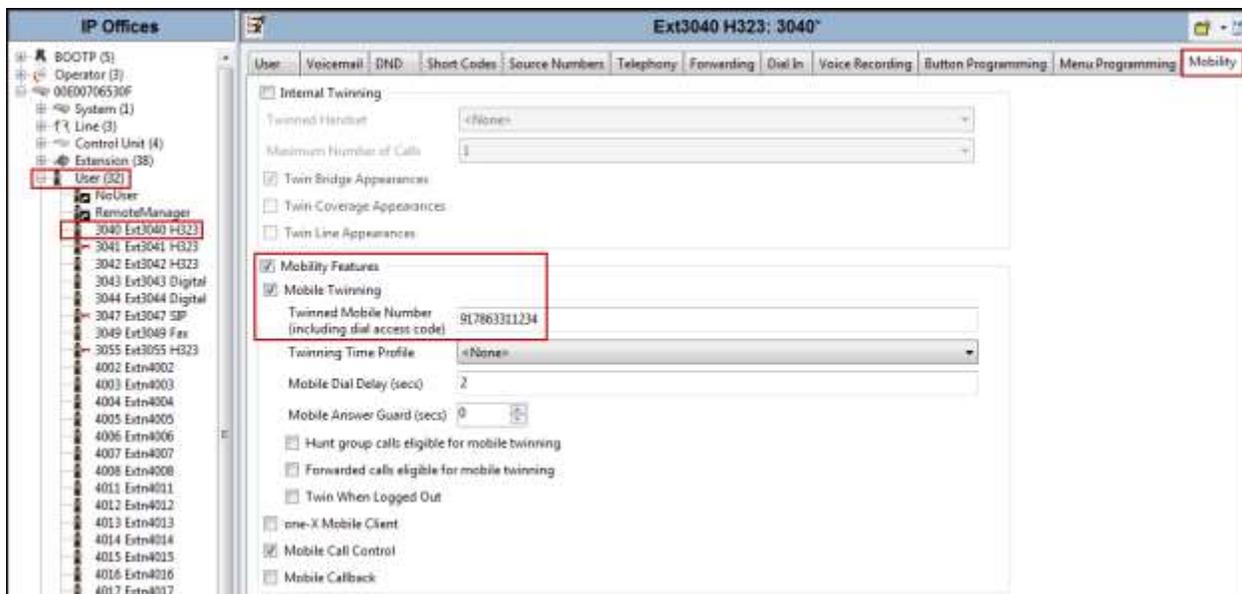
Right Panel (Ext3047 SIP: 3047): Configuration fields for the selected user. The "User" tab is active. The "Profile" dropdown menu is set to "Power User" and is highlighted with a red box. The "Enable Softphone" checkbox is checked and highlighted with a red box. Other configuration fields include:

- Name: Ext3047 SIP
- Password: [Redacted]
- Confirm Password: [Redacted]
- Account Status: Enabled
- Full Name: Softclient 3047
- Extension: 3047
- Email Address: [Empty]
- Locale: [Dropdown]
- Priority: 5
- System Phone Rights: None
- ACCS Agent Type: None
- Device Type: Unknown SIP device
- User Rights view: User data
- Working hours time profile: <None>

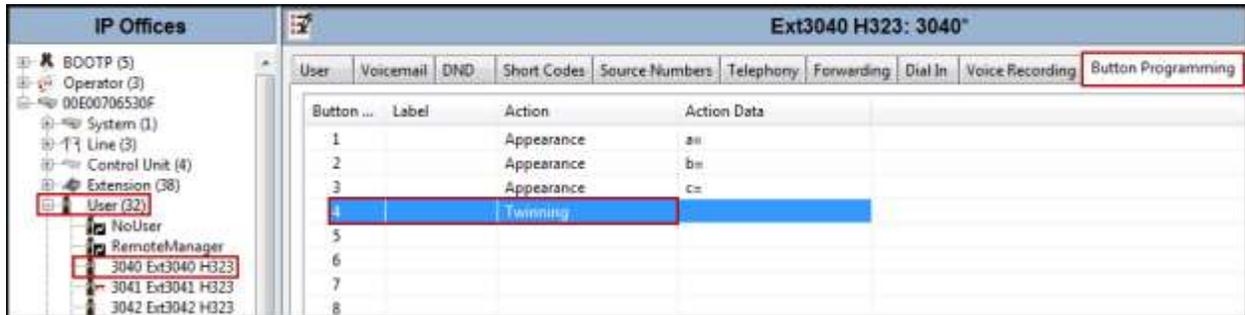
Select the **Voicemail** tab. The following screen shows the **Voicemail** tab for the user with extension 3040. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application Notes, incoming calls from Charter 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 3040 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for user 3040. 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 **917863311234**. Other options can be set according to customer requirements.

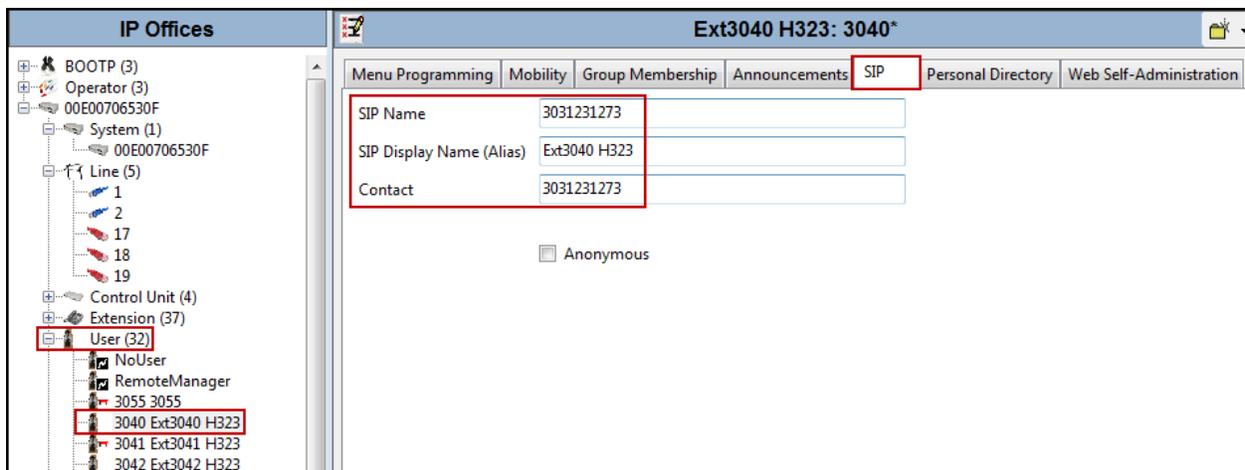


To program a key on the telephone to turn Mobile Twinning on and off, select the **Button Programming** tab on the user, then select the button to program to turn Mobile Twinning on and off, click on **Edit → Emulation → Twinning** (not shown). In the sample below, button **4** was programmed to turn Mobile Twinning on and off for user 3040.



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 Charter. In the example, DID number **3031231273** 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.



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 Charter DID numbers (**Section 5.6**).

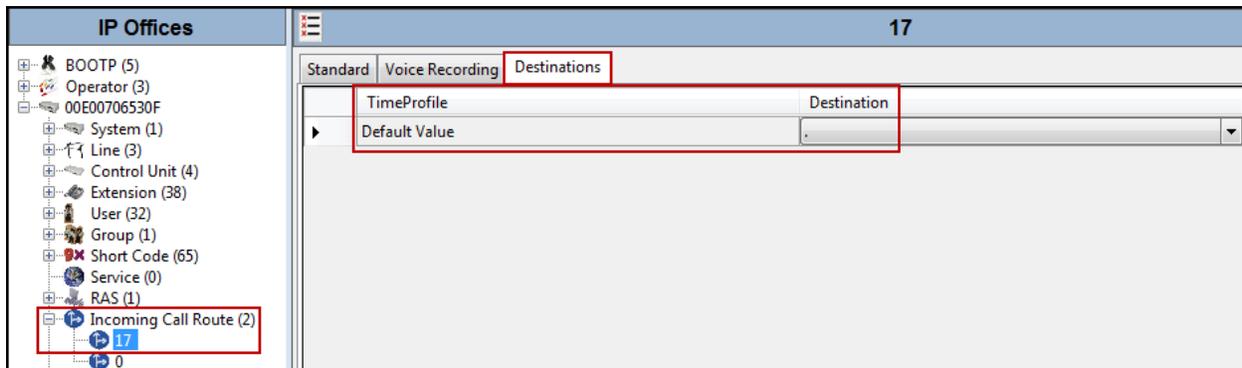
From the left Navigation Pane, right-click on **Incoming Call Route** and select **New**.

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 is the 'IP Offices' navigation pane, which is a tree view containing various system components. The 'Incoming Call Route (2)' item is highlighted with a red box. On the right is the configuration details pane for the selected item, showing the 'Standard' tab. The 'Standard' tab is also highlighted with a red box. Within this tab, the 'Bearer Capacity' dropdown is set to 'Any Voice' and the 'Line Group ID' dropdown is set to '17'. Both of these dropdowns are also highlighted with red boxes. Other configuration fields include 'Incoming Number', 'Incoming Sub Address', 'Incoming CLI', 'Locale', 'Priority' (set to '1 - Low'), 'Tag', 'Hold Music Source' (set to 'System Source'), and 'Ring Tone Override' (set to '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, a list of short codes is shown under the heading 'IP Offices'. The short code '9N' is highlighted with a red box. On the right, the configuration details for the short code '9N' are shown under the heading '9N: Dial'. The configuration includes:

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.

The screenshot displays the ARS configuration for the 'Main' route. The left sidebar shows the 'IP Offices' tree with 'ARS (1)' selected, and 'AS: Main' highlighted. The main configuration area includes fields for ARS Route ID (50), Route Name (Main), and various options like 'Secondary Dial tone' and 'Check User Call Barring'. A table lists dialing codes and their corresponding features and line group IDs. The first row is highlighted.

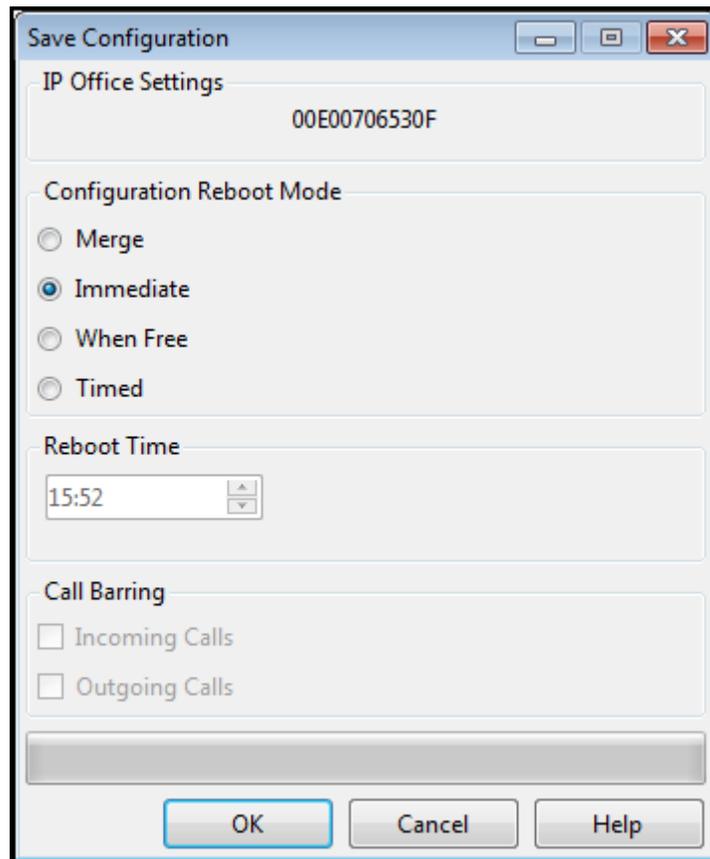
Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
001XXXXXXXXX	001N	Dial	17
8XXXXXXXXX	8N	Dial	17
1XXXXXXXXX	1N	Dial	17
6XXXXXX	6N	Dial	17
3XXXXXXXXX	3N	Dial	17

5.9 Save Configuration

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

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

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



The screenshot shows a 'Save Configuration' dialog box with the following fields and options:

- IP Office Settings:** 00E00706530F
- Configuration Reboot Mode:** Radio buttons for Merge, Immediate (selected), When Free, and Timed.
- Reboot Time:** A time selection field showing 15:52.
- Call Barring:** Checkboxes for Incoming Calls and Outgoing Calls, both of which are unchecked.
- Buttons:** OK, Cancel, and Help.

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

This section describes the required configuration of the Avaya SBCE to connect to Charter 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>/sbc` in the address field of the web browser, where `<ip-addr>` is the Avaya SBCE management IP address.

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



AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

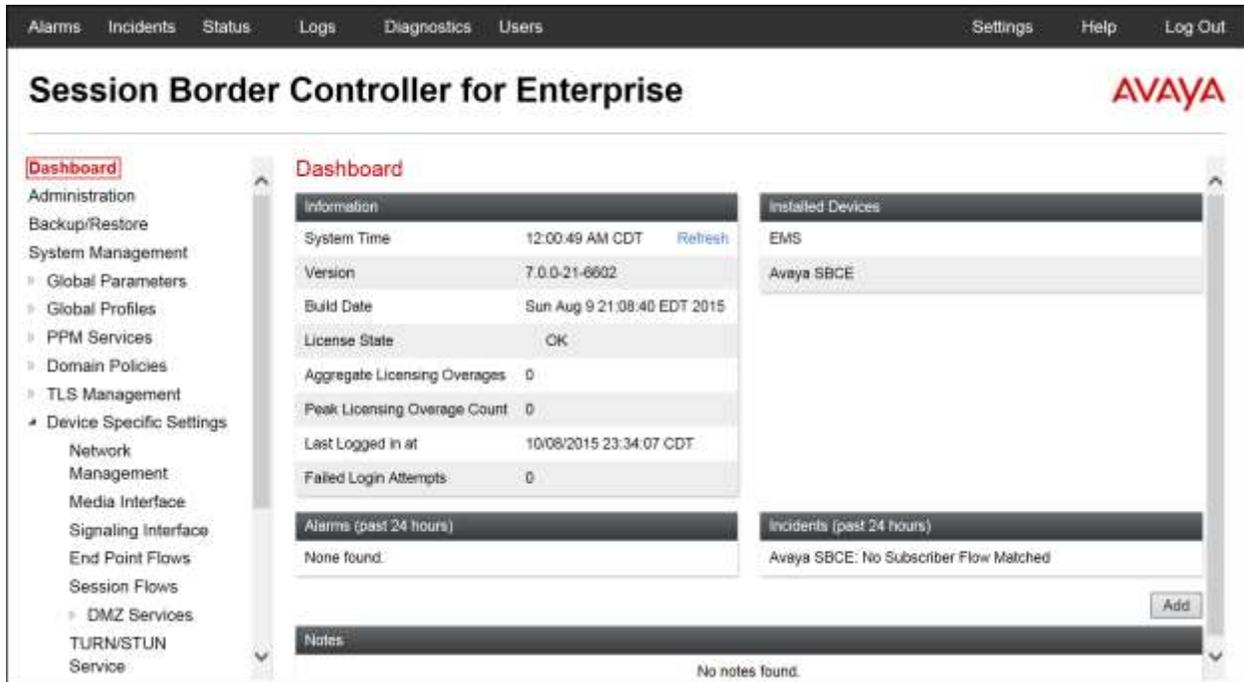
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under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



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.



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**.

The screenshot displays the 'System Information: Avaya SBCE' window with the following sections:

- General Configuration:**
 - Appliance Name: Avaya SBCE
 - Box Type: SIP
 - Deployment Mode: Proxy
- Device Configuration:**
 - HA Mode: No
 - Two Bypass Mode: No
- License Allocation:**
 - Standard Sessions: 2000 (Requested: 2000)
 - Advanced Sessions: 2000 (Requested: 2000)
 - Scopia Video Sessions: 500 (Requested: 500)
 - CES Sessions: 0 (Requested: 0)
 - Encryption:
- 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
[Blurred]	[Blurred]	[Blurred]	[Blurred]	A1
172.16.5.94	172.16.5.94	255.255.255.0	172.16.5.254	A1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	B1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	B1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	B1
- DNS Configuration:**
 - Primary DNS: [Blurred]
 - Secondary DNS: [Blurred]
 - DNS Location: DMZ
 - DNS Client IP: 192.168.157.189
- Management IP(s):**
 - IP: [Blurred]

On the previous screen, note that **A1** corresponds to the inside interface (Private Network side) and **B1** (with IP addresses blurred out) corresponds to the outside interface (Public Network side) of the Avaya SBCE. The **A1** interface was used to access IP Office (IP address: 172.16.5.71) and Charter’s Modular Access Router (IP address: 172.16.5.94) across the enterprise private network (LAN). In this solution, the **B1** interface was used for remote worker. The configuration required for Remote Worker is beyond the scope of these Application Notes and is not discussed here, thus IP addresses assigned to interface **B1** were blurred out. The management IP address was also blurred out for security reasons. (Use **Figure 1** as reference for IP address assignments).

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 Charter, 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 dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains 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 border. A "Finish" button is located at the bottom center of the dialog.

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

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The main title is "Session Border Controller for Enterprise". The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Server Interworking (highlighted), Media Forking, Routing, Server Configuration, Topology Hiding, Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, PPM Services, Domain Policies, TLS Management, and Device Specific Settings.

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

The configuration for the selected "Avaya-IPO" profile is shown in the "General" tab. The "General" tab is active, with other tabs including Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. A link "Click here to add a description" is visible at the top right of the configuration area.

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	No
URI Scheme	SIP
Via Header Format	RFC3261

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 main title is "Session Border Controller for Enterprise". The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Media Forking, Routing, Server Configuration, Topology Hiding, Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The "Global Profiles" section is expanded, showing "Server Interworking" selected. The main content area is titled "Interworking Profiles: Avaya-IPO" and includes an "Add" button. A list of interworking profiles is shown, with "Avaya-IPO" highlighted. The configuration details for the "Avaya-IPO" profile are displayed in a table with tabs for General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The "Advanced" tab is active, showing settings for Record Routes (Both Sides), Include End Point IP for Context Lookup (Yes), Extensions (Avaya), Diversion Manipulation (No), Has Remote SBC (Yes), and Route Response on Via Port (No). A "DTMF" section shows "DTMF Support" set to "None". An "Edit" button is located at the bottom right of the configuration area.

Profile Name	Record Routes	Include End Point IP for Context Lookup	Extensions	Diversion Manipulation	Has Remote SBC	Route Response on Via Port
cs2100						
avaya-ru						
OCS-Edge-Server						
cisco-ccm						
cups						
Sipera-Hala						
OCS-FrontEnd-Server						
Avaya-SM						
SP-General						
Avaya-CS1000						
Avaya-IPO	Both Sides	Yes	Avaya	No	Yes	No
Avaya-CM						

Setting	Value
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 Support	Value
DTMF Support	None

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.

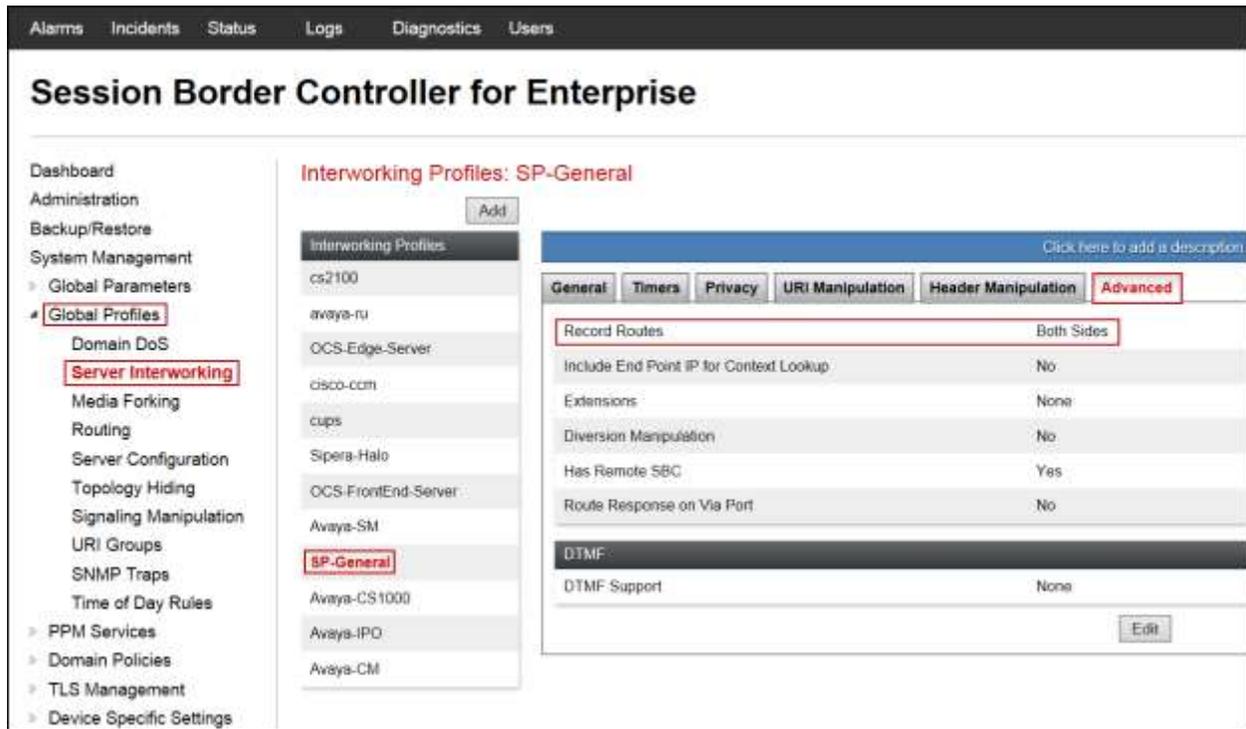
- Leave other fields with their default values.
- Click **Next** until the Advanced window is reached, check **Both Sides** then click **Finish** on the Advanced window.

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 title is 'Session Border Controller for Enterprise'. On the left, a navigation menu lists various sections, with 'Global Profiles' expanded to show 'Server Interworking'. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button. Below this is a list of interworking profiles, with 'SP-General' selected and highlighted. The configuration for 'SP-General' is shown in the 'General' tab, which includes a table of settings.

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	No
URI Scheme	SIP
Via Header Format	RFC3261

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

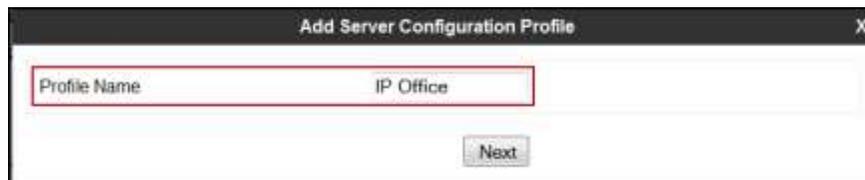


6.2.3 Server Configuration

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.

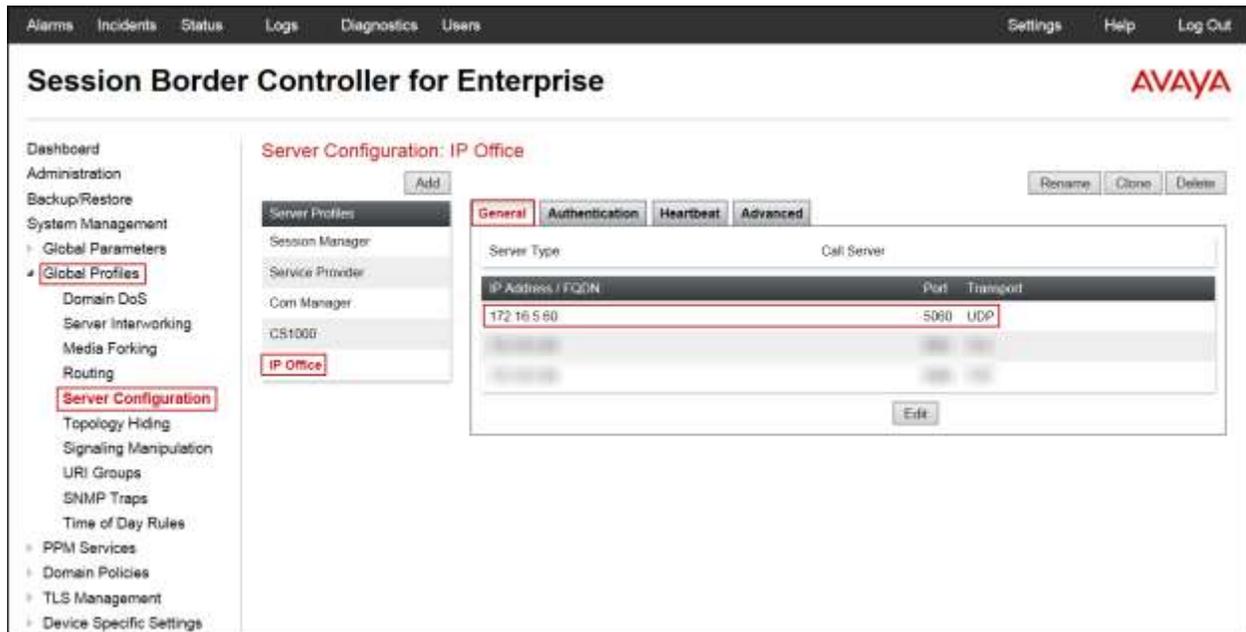
- Click **Next** on the **Authentication** window (not shown).
- Click **Next** on the **Heartbeat** window (not shown).

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

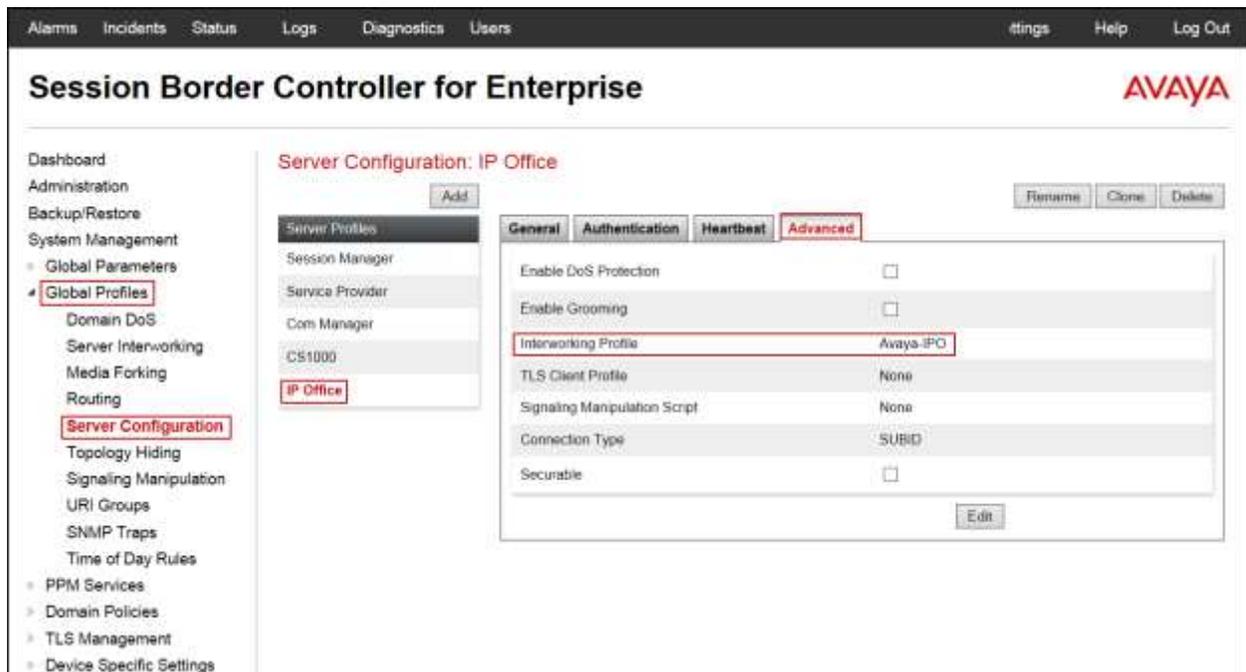
- Select **Avaya-IPO** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

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 dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. The main area contains a text input field labeled "Profile Name" with the text "Service Provider" entered. Below the input field is a "Next" button.

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

- **Server Type:** Select **Trunk Server**.
- **IP Address / FQDN:** **172.16.5.185** (Private IP Address of Charter’s Modular Access Router).
- **Port:** **5060**.
- **Transports:** Select **UDP**.
- Click **Next**.



The screenshot shows a window titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. The "Server Type" dropdown menu is set to "Trunk Server". Below this is an "Add" button. A table below contains the following information:

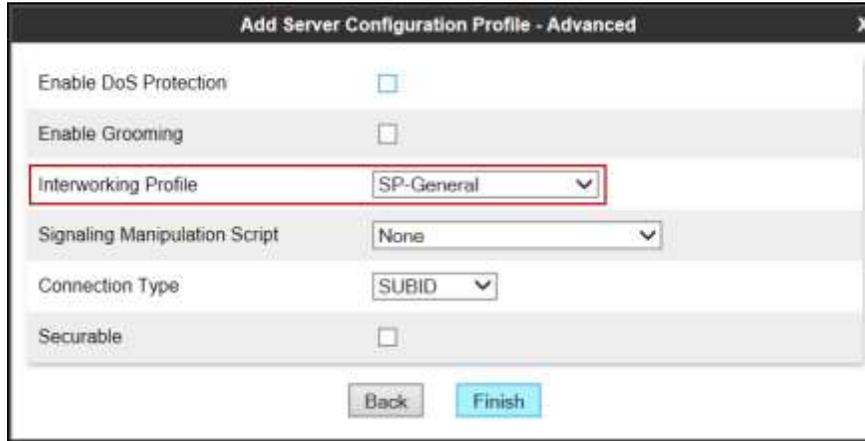
IP Address / FQDN	Port	Transport	
172.16.5.185	5060	UDP	Delete

At the bottom of the window are "Back" and "Next" buttons.

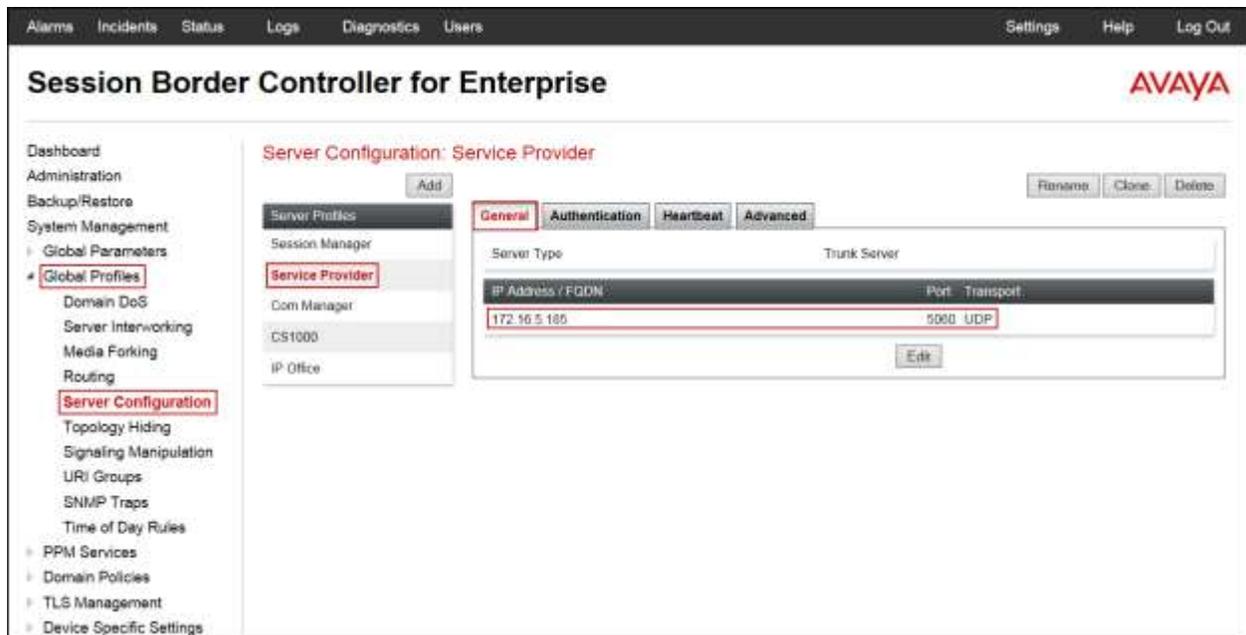
- Click **Next** in the **Add Server Configuration Profile - Authentication** window (not shown).
- Click **Next** in the **Add Server Configuration Profile - Heartbeat** window (not shown).

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

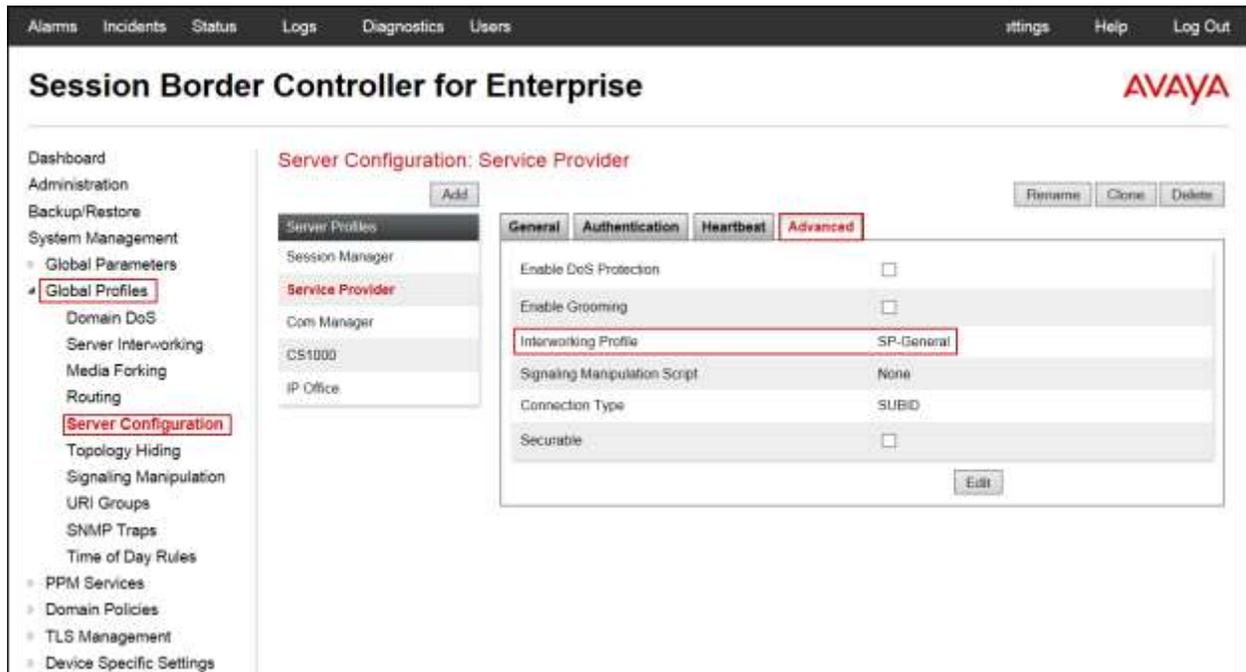
- Select **SP-General** from the **Interworking Profile**.
- Click **Finish**.



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



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 Charter'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 window titled "Routing Profile" with a close button (X) in the top right corner. Below the title bar is a form with a "Profile Name" label and a text input field containing "Route_to_IPO". A red rectangular box highlights the input field. Below the input field is a "Next" button.

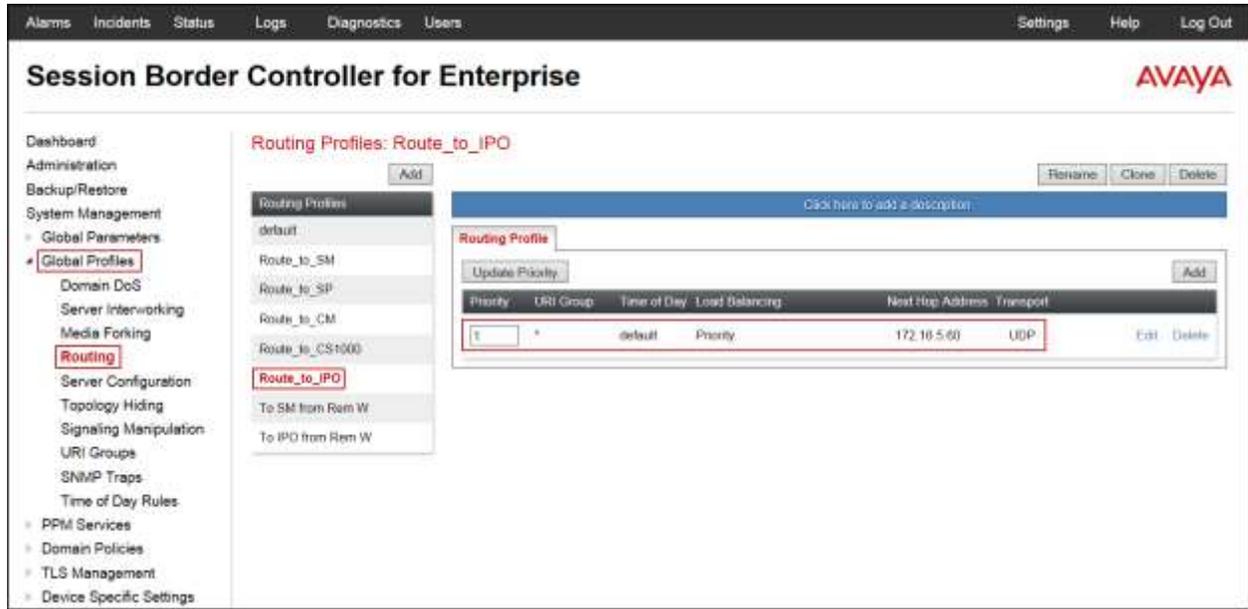
On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **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 a window titled "Routing Profile" with a close button (X) in the top right corner. The window contains several configuration options: "URI Group" (dropdown), "Time of Day" (dropdown set to "default"), "Load Balancing" (dropdown set to "Priority"), "NAPTR" (checkbox), "Transport" (dropdown set to "None"), "Next Hop Priority" (checkbox checked), "Next Hop In-Dialog" (checkbox), and "Ignore Route Header" (checkbox). Below these options is an "Add" button. Underneath is a table with the following columns: "Priority / Weight", "Server Configuration", "Next Hop Address", and "Transport". The table contains one row with the following values: "1", "IP Office", "172.16.5.60:5060 (UDP)", and "None". A red rectangular box highlights the "Priority / Weight", "Server Configuration", and "Next Hop Address" columns of this row. Below the table 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 **172.16.5.185:5060 (UDP)** (Private IP Address of Charter's Modular Access Router).
- Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	172.16.5.185:5060 (UDP)	None

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

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	172.16.5.185	UDP	Edit Delete

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.

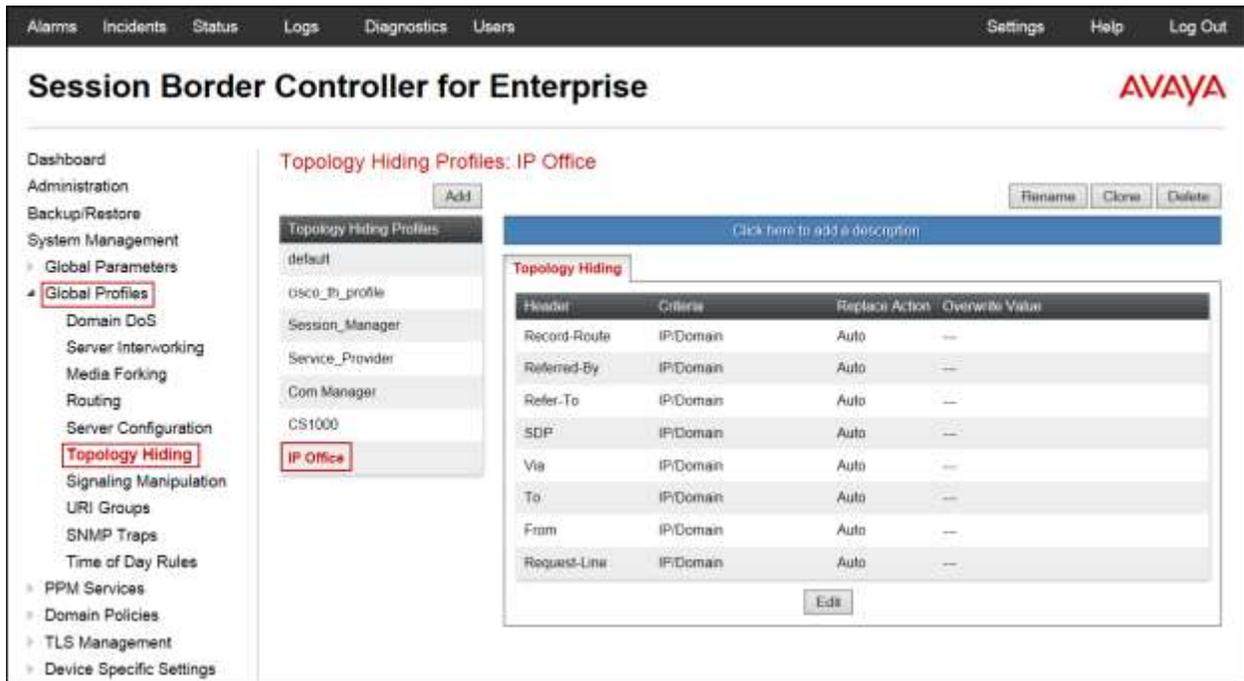
To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side (not shown):

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



The screenshot shows a dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains 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. A "Finish" button is located at the bottom center of the dialog.

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**.



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

The screenshot displays the Avaya Session Border Controller for Enterprise configuration page. The main title is "Session Border Controller for Enterprise" with the AVAYA logo on the right. The navigation menu on the left includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (selected), Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, PPM Services, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled "Topology Hiding Profiles: Service_Provider" and includes an "Add" button. Below this is a list of profiles: default, cisco_th_profile, Session_Manager, **Service_Provider** (highlighted), Com Manager, CS1000, and IP Office. To the right of the list are buttons for "Rename", "Clone", and "Delete".

The "Service_Provider" profile configuration is shown in a modal window. It has a blue header bar with the text "Click here to add a description." Below this is a table titled "Topology Hiding" with the following columns: Header, Criteria, Replace Action, and Overwrite Value.

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

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

6.3 Domain Policies

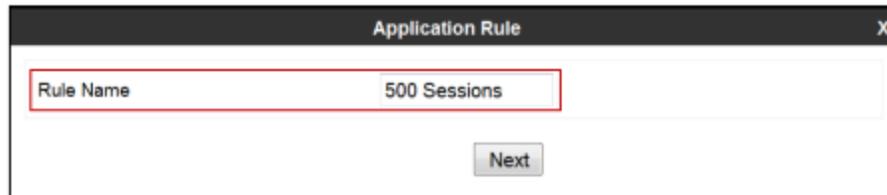
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

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.

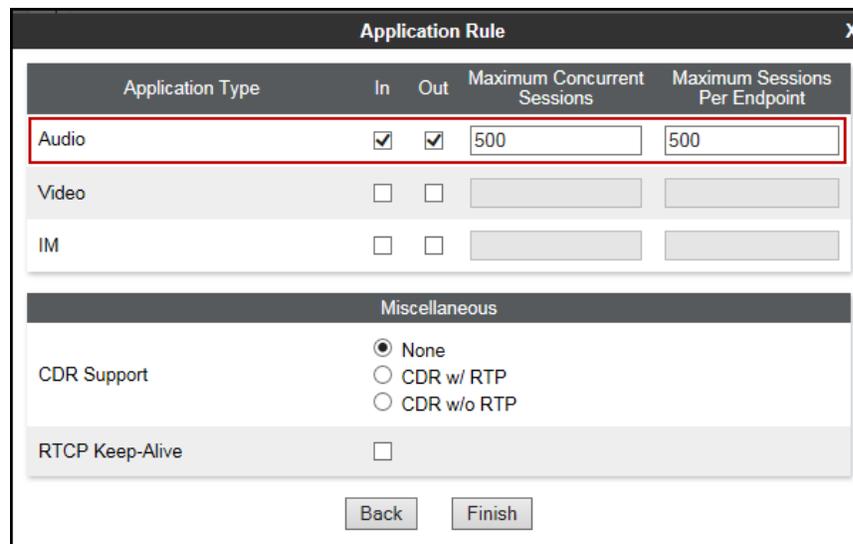
From the menu on the left-hand side, select **Domain Policies** → **Application Rules** (not shown).

- 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**.



The screenshot shows a window titled "Application Rule" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Rule Name" containing the text "500 Sessions". Below the input field is a "Next" button.

- 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**.



The screenshot shows a window titled "Application Rule" with a close button (X) in the top right corner. The window contains a table for configuring application types and a "Miscellaneous" section.

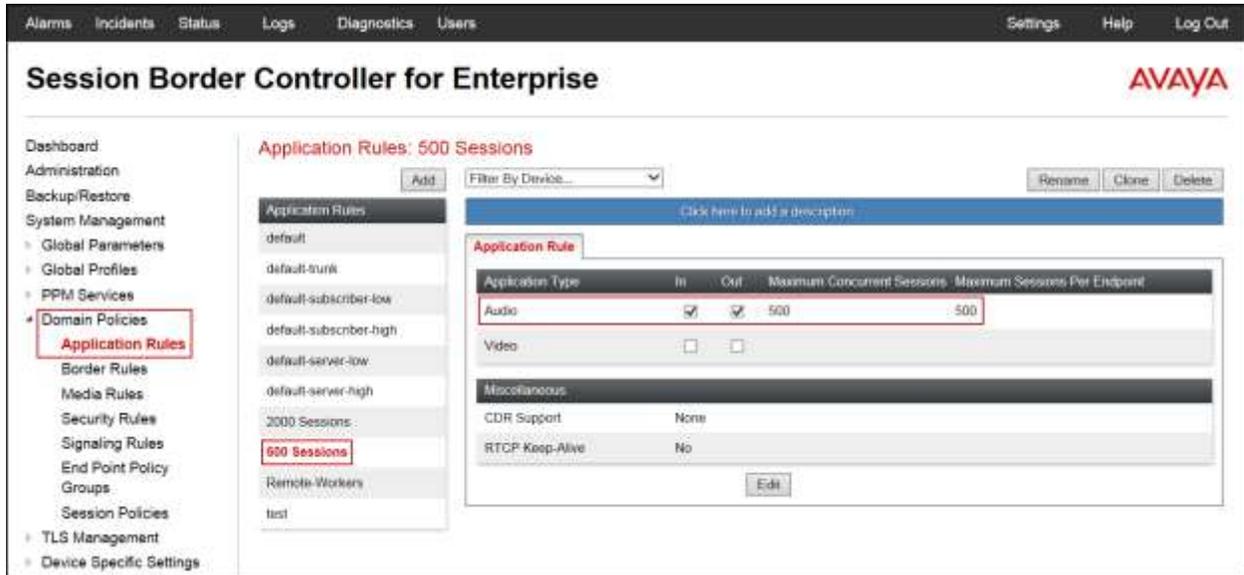
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	500	500
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Below the table is a "Miscellaneous" section with the following options:

- CDR Support: None, CDR w/ RTP, CDR w/o RTP
- RTCP Keep-Alive:

At the bottom of the window are "Back" and "Finish" buttons.

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**.

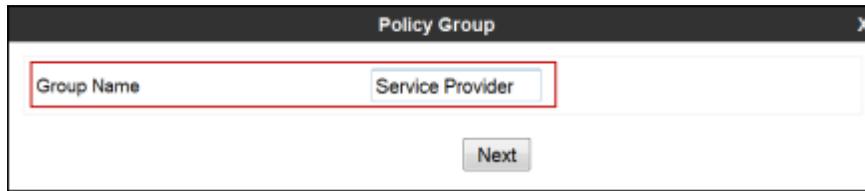


- **Application Rule: 500 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Click Finish.**

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

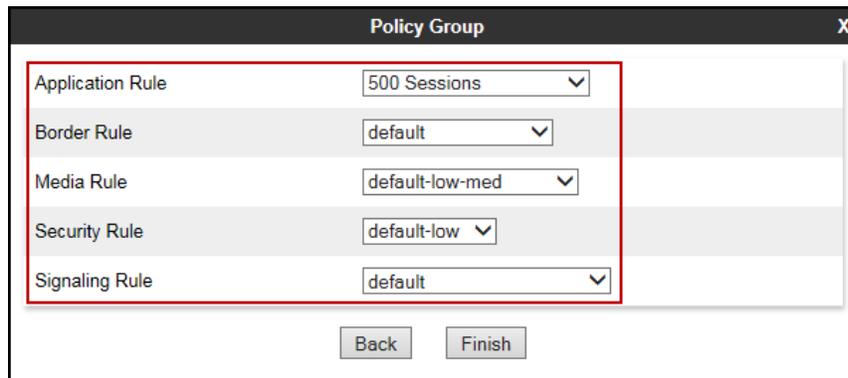
Similarly, to create an End Point Policy Group toward the Service Provider.

- 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". It has a text input field labeled "Group Name" which contains the text "Service Provider". A red rectangular box highlights the "Group Name" field and the "Service Provider" text. Below the input field is a "Next" button.

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



The screenshot shows a dialog box titled "Policy Group". It contains five rows of settings, each with a label and a dropdown menu. A red rectangular box highlights the entire area containing these five rows. The settings are: Application Rule (500 Sessions), Border Rule (default), Media Rule (default-low-med), Security Rule (default-low), and Signaling Rule (default). Below the settings are "Back" and "Finish" buttons.

The following screen capture shows the newly created **Service Provider** 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: Service Provider

Add Filter By Device... Rename Clone Delete

Policy Groups
Click here to add a description.
Click here to add a row description.

Policy Group Summary

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

Service Provi...

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 entity 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.

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
SNMP
Syslog Management
Advanced Options
‣ Troubleshooting

Network Management: Avaya SBCE

Devices: Avaya SBCE

Interfaces: **Networks**

Name	Gateway	Subnet Mask	Interface	IP Address	Edit	Delete
Network_A1	172.16.5.254	255.255.255.0	A1	172.16.5.71 172.16.5.94	Edit	Delete
					Edit	Delete

On the Interface Configuration tab, click the **Status** for interface **A1** 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.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the AVAYA logo. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. The 'Device Specific Settings' category is expanded, and 'Network Management' is highlighted with a red box. The main content area is titled 'Network Management: Avaya SBCE' and features three tabs: Devices, Interfaces, and Networks. The 'Interfaces' tab is active, showing a table with the following data:

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

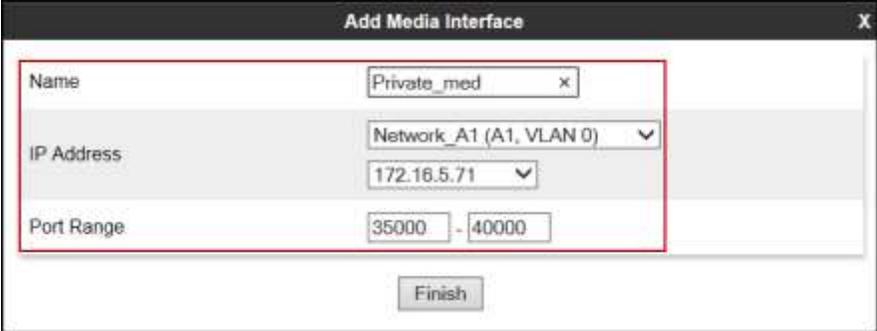
An 'Add VLAN' button is located in the top right corner of the interface table.

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 configuration window titled "Add Media Interface" with a close button (X) in the top right corner. The window contains three main input fields, each with a red border:

- Name:** A text input field containing "Private_med" and a small "x" icon to its right.
- IP Address:** A dropdown menu showing "Network_A1 (A1, VLAN 0)" with a downward arrow, and a secondary dropdown showing the IP address "172.16.5.71" with a downward arrow.
- Port Range:** Two text input fields, the first containing "35000" and the second containing "40000", separated by a hyphen.

Below these fields is a "Finish" button.

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** **Public_med**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**
Select **IP Address:** **172.16.5.94** (Inside or A1 IP Address of the Avaya SBCE, toward Charter's Modular Access Router).
- **Port Range:** **35000-40000**.
- Click **Finish**.

The following screen capture shows the newly created Media Interfaces.

Name	Media IP Network	Port Range	Edit	Delete
Private_med	172.16.5.71 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Public_med	172.16.5.94 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
...	Edit	Delete
...	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". The fields are as follows:

Name	Private_sig
IP Address	Network_A1 (A1, VLAN 0) 172.16.5.71
TCP Port	Leave blank to disable
UDP Port	5060 Leave blank to disable
TLS Port	Leave blank to disable
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: Public_sig.**
- Under **IP Address** select: **Network_A1 (A1, VLAN 0).**
- Select **IP Address: 172.16.5.94** (Inside or A1 IP Address of the Avaya SBCE, toward Charter's Modular Access Router).
- **UDP Port: 5060.**
- Click **Finish.**

Add Signaling Interface X

Name: Public_sig

IP Address: Network_A1 (A1, VLAN 0) (172.16.5.94)

TCP Port: Leave blank to disable

UDP Port: 5060 (Leave blank to disable)

TLS Port: Leave blank to disable

TLS Profile: None

Enable Shared Control:

Shared Control Port:

Finish

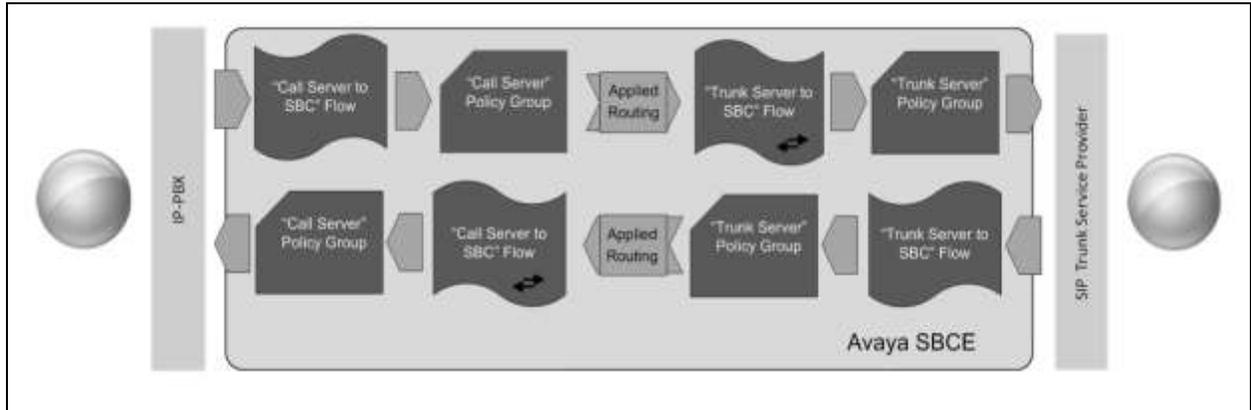
The following screen capture shows the newly created Signaling Interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Device Specific Settings' and 'Signaling Interface' highlighted. The main content area is titled 'Signaling Interface: Avaya SBCE' and features a 'Signaling Interface' tab. 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.' Below this is an 'Add' button and a table of signaling interfaces.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.5.71 Network_A1 (A1, VLAN 87)	---	5080	---	None	Edit Delete
Public_sig	172.16.5.94 Network_A1 (A1, VLAN 87)	---	5080	---	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 Charter's Modular Access Router, 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 Brach Office: Any.**
- Click **Finish.**

Field	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

Finish

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

- **Name: IP_Office_Flow.**
- **Server Configuration: IP Office.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Public_sig.**
- **Signaling Interface: Private_sig.**
- **Media Interface: Private_med.**
- **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 configuration window titled "Edit Flow: IP_Office_Flow". The window contains the following fields and 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 center of the window.

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 main title is "Session Border Controller for Enterprise" with the AVAYA logo on the right. The top navigation bar includes "Alarms", "Incidents", "Status", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out".

The left sidebar contains a navigation menu with the following items: 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, SNMP), Syslog Management, Advanced Options, and Troubleshooting.

The main content area is titled "End Point Flows: Avaya SBCE". It features two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of configurations. A blue bar at the top of the table area says "Click here to add a new description" with an "Add" button.

There are two sections of configuration tables:

- Server Configuration: IP Office**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	IP_Office_Flow	*	Public_sg	Private_sg	Enterprise	Route_to_SP	View	Clone	Edit	Delete
- Server Configuration: Service Provider**

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

7. Charter Business SIP Trunk Service Configuration

To use the Charter Business SIP Trunking service offering, a customer must request the service from Charter using the established sales processes. The process can be started by contacting Charter via the corporate web site at: <https://www.charterbusiness.com/> or by calling 800-314-7195.

During the signup process, Charter and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Charter's network. Charter 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 configuration discussed in the previous sections.

As previously noted, as a required component of the Charter Business SIP Trunking service offering, Charter will install a Modular Access Router at the customer premises (enterprise site). Charter will perform the initial configuration and maintenance as required. The Modular Access Router will be considered Customer Premises Equipment (CPE).

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.

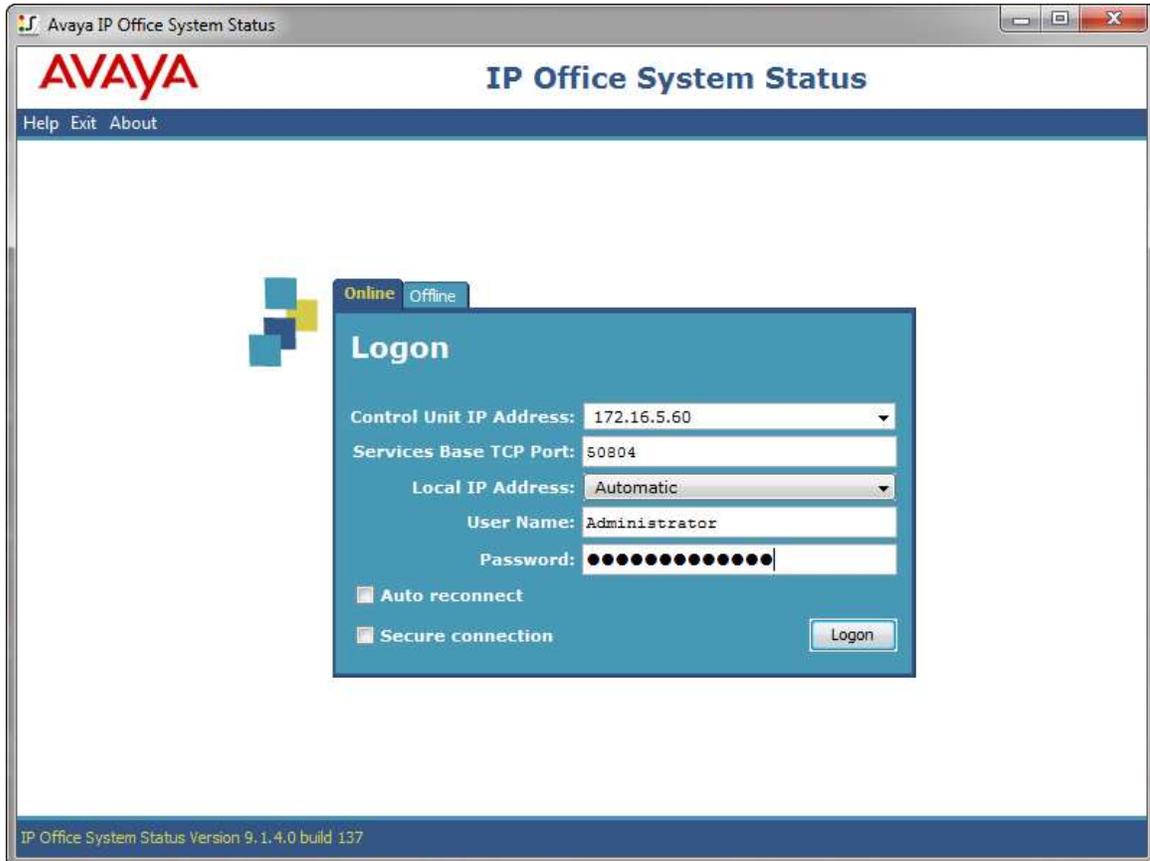
The following attributes in SIP message body are inspected using a sniffer trace analysis tool:

- 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 reads "Avaya IP Office System Status - 00E00706530F (172.16.5.60) - IP500 V2 9.1.4.0 build 137". The main window has a menu bar with "Help", "Snapshot", "LogOff", "Exit", and "About". A left-hand navigation pane contains a tree view with categories like "System", "Alarms (8)", "Extensions (24)", "Trunks (5)", "Active Calls", "Resources", "Voicemail", "IP Networking", and "Locations". Under "Trunks (5)", "Line:17" is selected.

The main content area is titled "IP Office System Status" and has three tabs: "Status" (selected), "Utilization Summary", and "Alarms". The "Status" tab displays a "SIP Trunk Summary" section with the following details:

- 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
- 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:

Below the summary is a table with columns: "Cha...", "U...", "Call Ref", "Curr... State", "Time in Remote Media...", "C...", "Con...", "Caller ID o...", "Other Party on...", "Dire...", "Round Trip ...", "Rec...", "Rec...", "Tran...", "Tran...". The table contains 10 rows, all with "Idle" in the "Curr... State" column and "4 da..." in the "Time in Remote Media..." column.

At the bottom of the window, there are several control buttons: "Trace", "Trace All", "Pause", "Ping", "Call Details", "Graceful Shutdown", "Force Out of Service", "Print...", and "Save As...". The status bar at the very bottom shows the time "9:30:21 AM" and the status "Online".

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

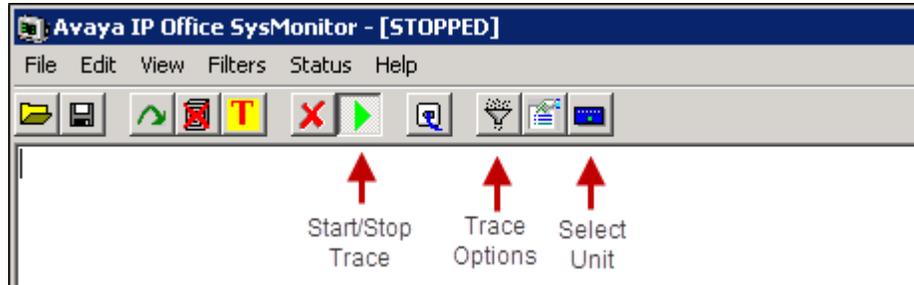
The screenshot displays the Avaya IP Office System Status web interface. The top navigation bar includes 'Help', 'Snapshot', 'LogOff', 'Exit', and 'About'. The left sidebar contains a tree view with categories: System, Alarms (8), Extensions (24), Trunks (5), Line:1, Line:2, Line:17 (selected), Line:18, Line:19, Active Calls, Resources, Voicemail, IP Networking, and Locations. The main content area has three tabs: 'Status', 'Utilization Summary', and 'Alarms'. The 'Alarms' tab is active and shows the title 'Alarms for Line: 17 SIP sip://172.16.5.71'. Below the title is a table with the following structure:

Last Date Of Error	Occurrences	Error Description
--------------------	-------------	-------------------

At the bottom of the interface, there are several control buttons: 'Ping', 'Clear', 'Clear All', 'Graceful Shutdown', 'Force Out of Service', 'Print...', and 'Save As...'. The bottom right corner shows the time '9:32:14 AM' and the status 'Online'.

8.4 IP Office Monitor

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



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



8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)

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

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

The screenshot shows the Avaya SBCE dashboard. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. A left sidebar contains a 'Dashboard' section with various administrative and management options. The main content area is divided into several panels: 'Information' (System Time: 12:30:50 AM CDT, Version: 7.0.0-21-6602, Build Date: Sun Aug 9 21:08:40 EDT 2015, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 10/08/2015 23:34:07 CDT, Failed Login Attempts: 0), 'Installed Devices' (listing EMS and Avaya SBCE), 'Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (None found), and 'Notes' (No notes found). An 'Add' button is visible at the bottom right of the dashboard area.

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

The screenshot shows the Avaya Alarm Viewer page. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Alarm Viewer' and the Avaya logo. A left sidebar contains a 'Devices' section with options for EMS and Avaya SBCE. The main content area is divided into several sections: 'Alarms' (No alarms found for this device), 'Clear Selected', and 'Clear All'.

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

The screenshot shows the Avaya Session Border Controller for Enterprise dashboard. The navigation menu at the top includes Alarms, Incidents (highlighted with a red arrow), Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled 'Dashboard' and contains several sections:

- Information:** System Time (12:30:50 AM CDT), Version (7.0.0-21-0002), Build Date (Sun Aug 9 21:08:40 EDT 2015), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (10/08/2015 23:34:07 CDT), and Failed Login Attempts (0).
- Installed Devices:** Lists EMS and Avaya SBCE.
- Alarms (past 24 hours):** None found.
- Incidents (past 24 hours):** None found.
- Notes:** No notes found.

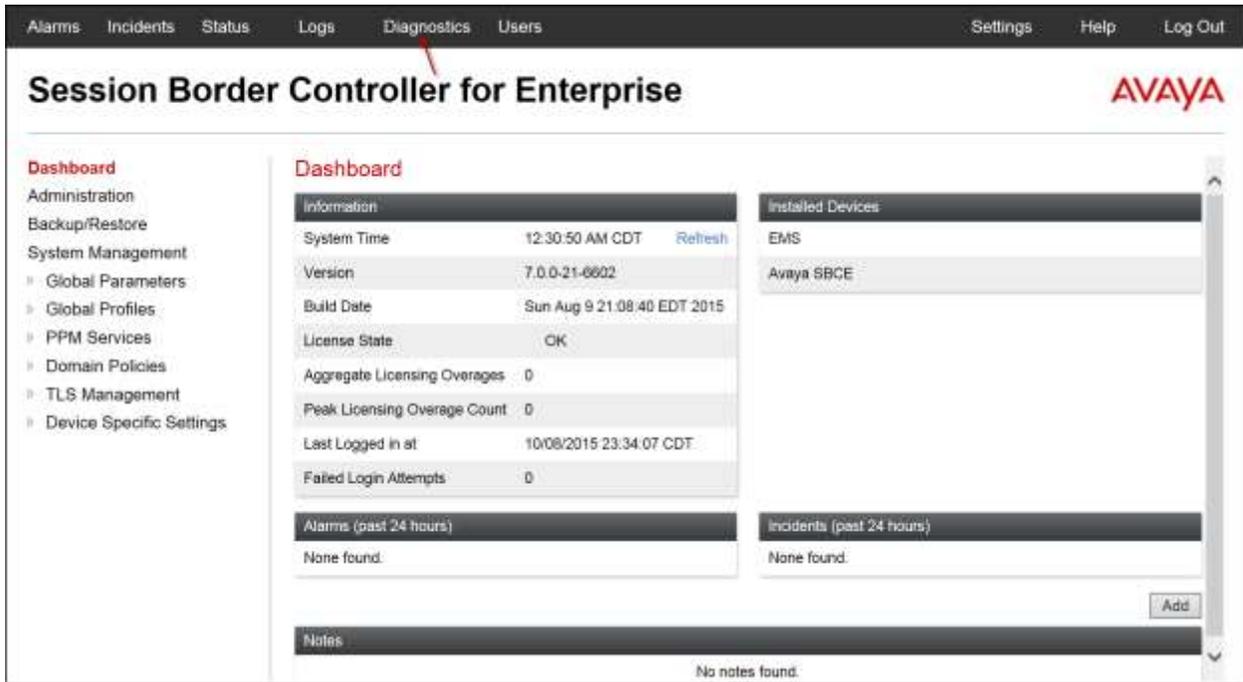
The following screen shows the Incident Viewer page.

The Incident Viewer page displays a table of incidents. At the top, there are filters for Device (Avaya SBCE) and Category (Policy), along with 'Clear Filters', 'Refresh', and 'Generate Report' buttons. The table shows the following data:

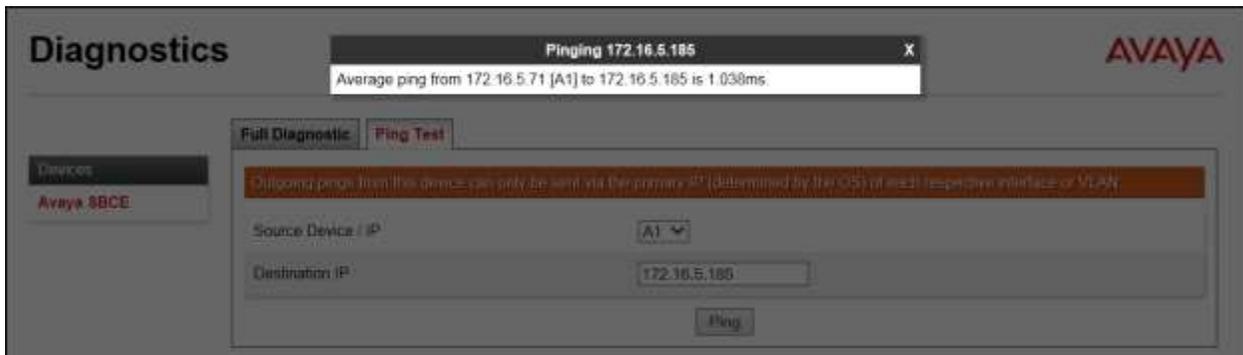
Type	ID	Date	Time	Category	Device	Cause
Message Dropped	722182809923738	10/8/15	11:40 PM	Policy	Avaya SBCE	No Subscriber Flow Matched
Server Heartbeat	721578665868258	9/24/15	10:55 PM	Policy	Avaya SBCE	Heartbeat Failed. Server is Down
Server Heartbeat	720627871533350	9/2/15	11:49 PM	Policy	Avaya SBCE	Heartbeat Failed. Server is Down
Server Heartbeat	720627092366599	9/2/15	11:23 PM	Policy	Avaya SBCE	Heartbeat Failed. Server is Down
Server Heartbeat	720581909185100	9/1/15	10:16 PM	Policy	Avaya SBCE	Heartbeat Failed. Server is Down

Navigation controls at the bottom of the table include '<<', '<', '1', '>', and '>>' buttons.

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**.



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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes '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 navigation menu is expanded to 'Troubleshooting', with 'Trace' selected. The main content area is titled 'Trace: Avaya SBCE' and features a 'Devices' dropdown menu showing 'Avaya SBCE'. Below this, there are two tabs: 'Packet Capture' and 'Captures', with 'Captures' being the active tab. A table lists the captured files, with one entry highlighted:

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

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 Charter 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 30u, November 06, 2015.
- [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 10j, November 06, 2015.
- [4] *Using IP Office System Monitor*, Document Number 15-601019, Issue 06e, May 19, 2015.

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.