



Application Notes for Configuring Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise Release 6.2.1 to support Charter Communications SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise Release 6.2.1, to interoperate with Charter Communications SIP Trunking Service.

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

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

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

Charter Communications 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	4
2.2 Test Results.....	6
2.3 Support.....	6
3. Reference Configuration.....	7
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 Create a New SIP Trunk from Template	19
5.4.2 SIP Line - SIP Line Tab.....	22
5.4.3 SIP Line - Transport Tab	23
5.4.4 SIP Line - SIP URI Tab	24
5.4.5 SIP Line - VoIP Tab	25
5.5 Extension.....	26
5.6 Users	28
5.7 Incoming Call Route.....	33
5.8 Outbound Call Routing.....	35
5.8.1 Short Codes and Automatic Route Selection.....	35
5.9 Privacy/Anonymous Calls	37
5.10 Save Configuration	38
6. Configure the Avaya Session Border Controller for Enterprise.....	39
6.1 Log into the Avaya Session Border Controller for Enterprise.....	39
6.2 Global Profiles	42
6.2.1 Server Interworking profile - Avaya-IPO	42
6.2.2 Server Interworking profile – SP-General	45
6.2.3 Routing Profiles	48
6.2.4 Server Configuration.....	53
6.2.5 Topology Hiding.....	62
6.3 Domain Policies.....	66
6.3.1 Create Application Rules	66
6.3.2 End Point Policy Groups.....	68
6.4 Device Specific Settings	72
6.4.1 Network Management.....	72
6.4.2 Media Interface	74
6.4.3 Signaling Interface.....	76
6.4.4 End Point Flows.....	78
7. Charter Communications SIP Trunking Configuration	82

8. Verification and Troubleshooting	83
8.1 Verification Steps.....	83
8.2 Protocol Traces	83
8.3 IP Office System Status	84
8.4 IP Office Monitor.....	86
8.5 Avaya Session Border Controller for Enterprise	87
9. Conclusion	92
10. References.....	93

1. Introduction

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

In the sample configuration, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office (hereafter referred to as IP Office) 500v2 Release 9.0, Avaya Session Border Controller for Enterprise (hereafter referred to as Avaya SBCE) Release 6.2.1, Avaya IP Office Video Softphone, Avaya Flare® Experience for Windows and Avaya Deskphones, including SIP, H.323, digital, and analog. The Avaya SBCE provides security for the Avaya IP Office solution, as well as interoperability features for the SIP trunk.

Charter Communications SIP Trunking Service referenced within these Application Notes is designed for business customers. Customers using this service with the 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”, “Charter” or “Charter Communications” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using IP Office to connect to Charter’s network via the Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the feature and functionality tests listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

Testing was performed with IP Office 500v2 R9.0, but it also applies to IP Office Server Edition R9.0. Note that IP Office Server Edition requires an Expansion IP Office 500v2 R9.0 to support analog, digital endpoints or trunks.

2.1 Interoperability Compliance Testing

To verify Charter’s SIP Trunking interoperability, 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.
- Inbound and outbound calls to/from Remote Worker using Avaya Flare® Experience for Windows (SIP).
- Incoming and outgoing PSTN calls to/from IP Office Video Softphone.
- Incoming and outgoing PSTN calls to/from Avaya Flare® Experience for Windows.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the callee.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- Dialing plans including long distance, international, outbound toll-free, etc.
- Caller ID presentation and Caller ID blocking (Privacy).
- Codec G.711MU (Charter supported audio codec).
- No matching codecs.
- G.711 fax pass-through.
- Proper early media transmissions.
- Voicemail and DTMF tone transmissions per RFC 2833 (leaving and retrieving voice mail, 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.
- Mobile Twinning (Extension to Cellular call redirection).
- Simultaneous active calls.
- Long duration calls (over one hour).

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 discussed in these Application Notes, see **References Error! Reference source not found.**

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 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 “404 Not Found” instead of “488 Not Acceptable Here”, the user will hear re-order. This issue does not have any user impact, it is listed here simply as an observation.
- **Call Display on Transferred Calls to the PSTN:** Caller ID display is not updated on PSTN phones involved with call transfers from IP Office to the PSTN. After the call transfer is completed, the PSTN phone does not display the actual connected party but instead shows the number of the host extension that initiated the call transfer (transferor). The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/Charter solution. It is listed here simply as an observation.
- **Calls from the PSTN to busy DID numbers assigned to IP Office extensions (users):** Any time a DID number assigned to an IP Office extension (user) is busy (talking) with a PSTN user, Charter will send “INFO” instead of “INVITE” messages to IP Office when other PSTN users attempt to call the busy IP Office extension (user). Embedded within the “INFO” message body is the message: “Play tone CallwaitingTone1”. The PSTN user attempting to call the busy IP Office extension (user) will here ring-back tone for 2+ minutes, the IP Office extension (user) is never alerted of additional calls coming in from the PSTN (the IP Office phone does NOT ring). The IP Office extensions (users) were configured with multiple call appearances and are able to receive additional calls on any idle call appearance. IP Office expects to receive “INVITE” messages to complete additional calls to idle call appearances. This behavior is only seen when the IP Office extension (user) is busy talking with a PSTN user, if the IP Office extension (user) is busy talking with another IP Office extension (user) (internal within IP Office), this behavior does not occur. This issue was reported to Charter and is being investigated by Charter.
- **Outbound Calling Party Number (CPN) Blocking:** To support user privacy on outbound calls (calling party number blocking), when enabled by the IP Office user, IP Office sends “anonymous” as the calling number in the SIP “From” header and includes “Privacy: id” in the INVITE message. During the compliance test, Charter’s network responded with “404 Not Found” to outbound calls with privacy enabled on IP Office endpoints, resulting on the call failing to complete.

2.3 Support

For support on Charter Communications systems 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 below illustrates the test configuration used. It shows a simulated enterprise site connected to Charter's network through the public internet.

For confidentiality and privacy purposes, actual public IP addresses and PSTN routable phone numbers (DIDs) used during the compliance testing have been replaced with fictitious IP addresses and PSTN routable phone numbers throughout the Application Notes.

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

- Avaya IP Office 500v2.
- Avaya Session Border Controller for Enterprise.
- Avaya Voicemail Pro for IP Office.
- Avaya 96x0 Series H.323 IP Deskphones.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 11x0 Series SIP IP Deskphones.
- Avaya IP Office Video Softphone.
- Avaya Flare® Experience for Windows.
- Avaya 1408 Digital Deskphones.
- Avaya 9508 Digital Deskphones.

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

Also located at the enterprise site is Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codec's. The IP Office **LAN1** interface connects to the inside (A1) interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE (B1) connects to Charter's network via the public Internet.

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

For inbound calls, the calls flowed from Charter 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 for egress into Charter's network.

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's network (refer to **Section 5.8**). The short code 9 was stripped off by 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 calls between the NANP.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider 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

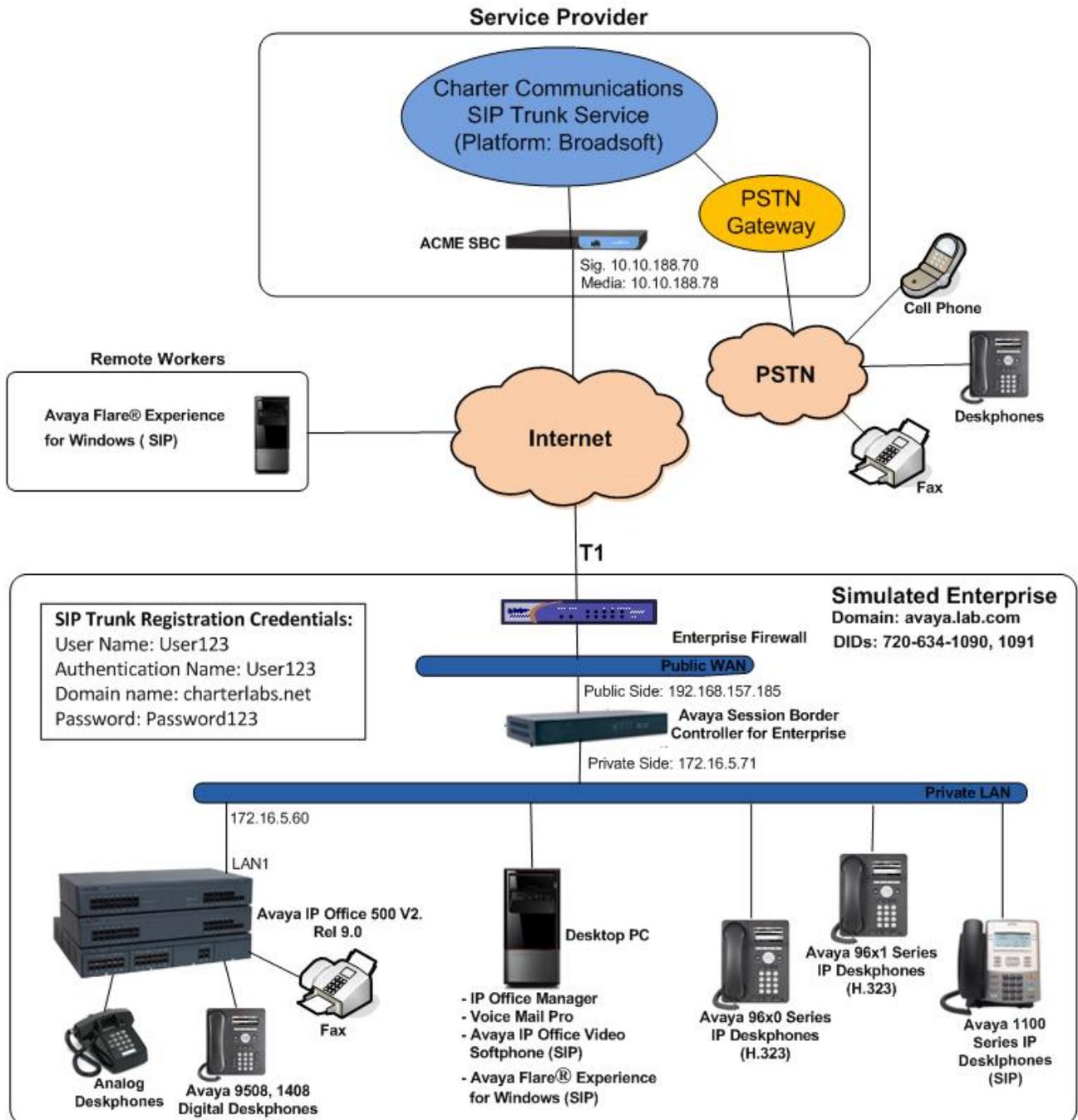


Figure 1: Avaya Interoperability Test Lab Configuration.

4. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration.

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	9.0.4.0 Build 965
Avaya IP Office DIG DCPx16 V2	9.0.4.0 Build 965
Avaya IP Office Manager	9.0.4.0 Build 965
Avaya Voicemail Pro Client	9.0.4.0 Build 18
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2.1.Q18
Avaya 96x0 IP Deskphones (H.323)	Avaya one-X® Deskphone Edition S3.220A
Avaya 96x1 Series IP Deskphones (H.323)	Avaya one-X® Deskphone H.323 Version 6.4014
Avaya 1120E IP Deskphones (SIP)	SIP1120e Ver. 04.04.14.00
Avaya IP Office Video Softphone	3.2.3.49 68975
Avaya Flare® Experience for Windows	1.1.4.23
Avaya Digital Deskphones 1408	38.0
Avaya Digital Deskphones 9508	0.55
Lucent Analog Phone	--
Charter Communications	
Broadworks Broadsoft Application Server	R17 SP4
ACME Packet 4500 Series SBC	nnSCX6.2.0mp

5. Configure IP Office

This section describes the IP Office configuration required to interwork with Charter. 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 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** in the Group pane. 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 containing various system components. The 'License (74)' item is selected. The main area shows the 'License Remote Server' configuration page. At the top, it indicates 'License Mode License Normal' and 'PLDS Host ID 111309813681'. Below this is a table listing various features and their license details.

Feature	License Key	Instances	Status	Expiry Date	Source
Proactive Reporting	ttDp8nbs9N@bd8JrHv9y8eEitvEwwzo5	255	Valid	Never	ADI Nodal
Report Viewer	Tvct73mdgdGtXkY6hS_FrhqFMzibPws1	255	Valid	Never	ADI Nodal
Mobility Features	0ICluRgHvKoiINxPi9o1LJpTOSo9pfjm	255	Obsolete	Never	ADI Nodal
Advanced Small Community Netw...	DaQI7Ve5vUULfzGvopYxp8hpk7GrikFe	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	T39BkqBxvtd6aLLRgllpq1nfnk9dMhLRsc	255	Valid	Never	ADI Nodal
IP500 Upgrade Standard to Profess...	QaHgn76v9j6CDtJGpS0HO6jYu_4UJ7J	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	JaHLHAVFXjDX2BwrUzkK6f61Kcu3Uq9J	4	Valid	Never	ADI Nodal
SIP Trunk Channels	B3CzqGBYDUsciExiBUz29J_McyEkr7@W	255	Valid	Never	ADI Nodal
VPN IP Extensions	@qm3fOoR55_R3RMfy7yB5ojUKrAPmSQ	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional cha...	2TXC@OoNQxtzOpABDlLkM6_9xbijkNz	255	Valid	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	hXIRxBVCEKNVD0wsYDeZ_XFZSoinv7zB	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Standar...	4AOGbV5D9DaLNCHRlHe2olG0g09csWde	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Professi...	dlyY_Dba5Uuq7seo3XXMTmN4rlJowPps9	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Stan...	dv956B89iXS_NKS8AAo_LcO_hnwdcU8EB	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Prof...	LHFZqB6XieQKvp3h@mgDjQelcvLeZm	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 IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.2.1 System - LAN1 Tab

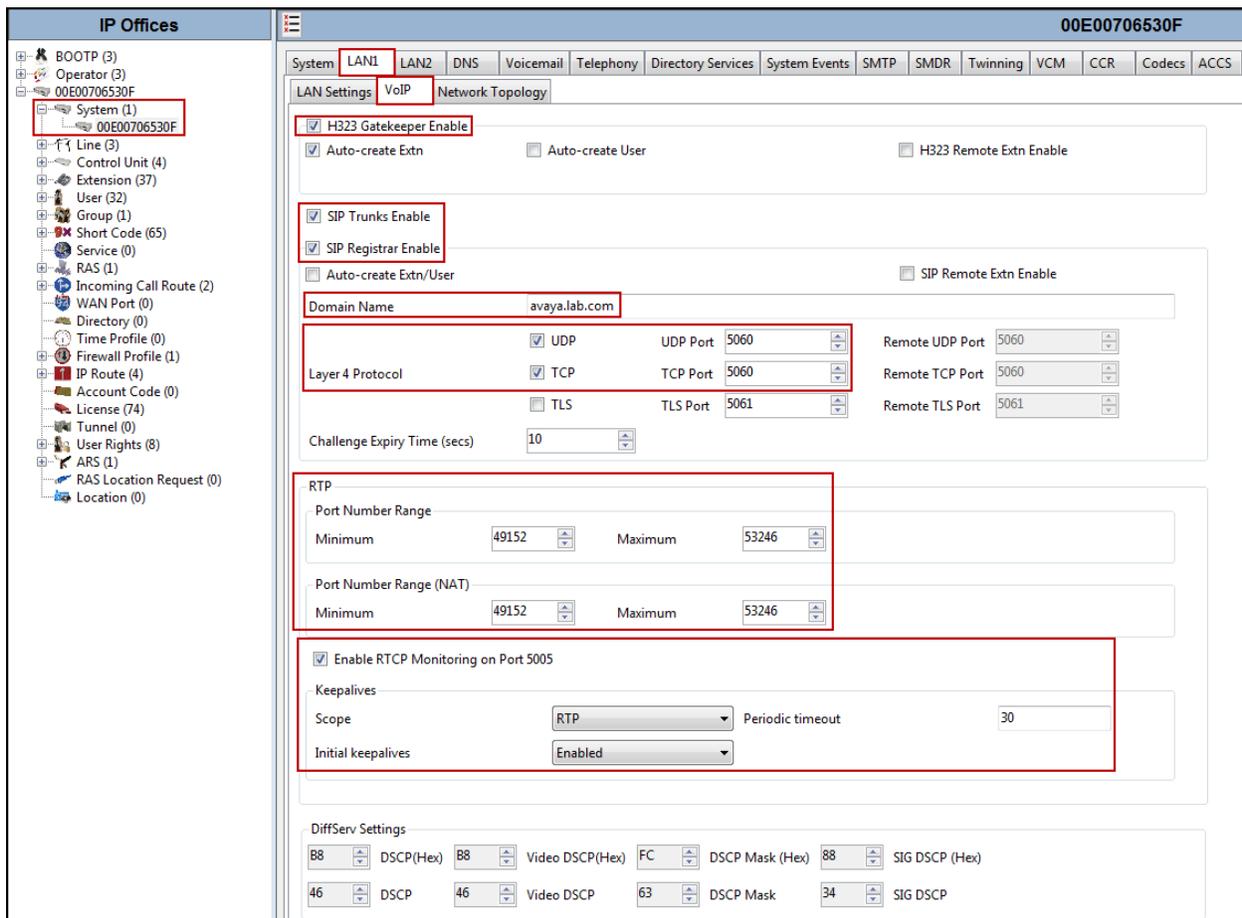
In the sample configuration, the MAC address **00E00706530F** was used as the system name and the **LAN** port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to Charter's network via the public internet. 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 configuration interface for an Avaya IP Office system. On the left, the 'IP Offices' navigation pane shows a tree structure with 'System (1) 00E00706530F' selected. The main pane shows the 'LAN1' tab with the 'LAN Settings' sub-tab active. The 'IP Address' field is set to '172.16.5.60' and the 'IP Mask' field is set to '255.255.255.0'. Other settings include 'Primary Trans. IP Address' (0.0.0.0), 'RIP Mode' (None), 'Enable NAT' (unchecked), and 'Number Of DHCP IP Addresses' (200). The 'DHCP Mode' is set to 'Disabled'.

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 that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even the default STUN settings are populated but 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 heartbeat to the service provider.
- Verify the **Public IP Address** is set to **0.0.0.0**.
- Set the **Public Port** to **5060** for **UDP**.
- All other parameters should be set according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface for the 'Network Topology' tab. The left sidebar shows a tree view of system components, with 'System (1)' and its associated IP Office instance '00E00706530F' highlighted. The main configuration area includes the following settings:

- STUN Server Address:** 69.90.168.13
- STUN Port:** 3478
- Firewall/NAT Type:** Open Internet
- Binding Refresh Time (seconds):** 300
- Public IP Address:** 0 . 0 . 0 . 0
- Public Port:** UDP 5060
- TCP:** 0
- TLS:** 0
- Run STUN on startup

Buttons for 'Run STUN' and 'Cancel' are visible at the bottom right of the configuration area.

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

5.2.2 System - Telephony Tab

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

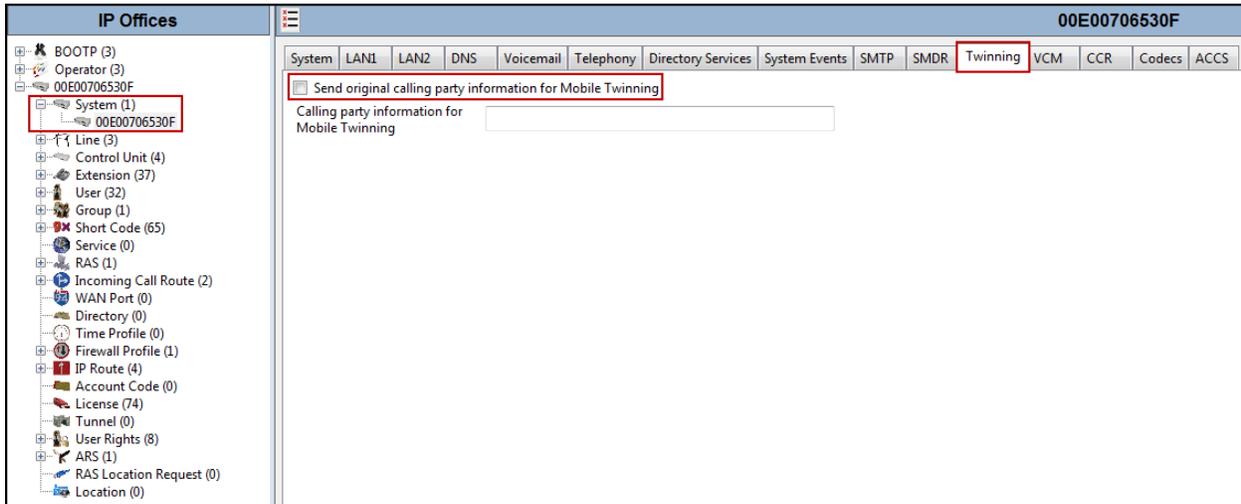
- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer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

The screenshot displays the configuration interface for the IP Office system 00E00706530F. The 'Telephony' tab is active, and the 'Companding Law' section is highlighted with a red box. In this section, the 'Switch' and 'Line' options are both set to 'U-Law'. The 'Inhibit Off-Switch Forward/Transfer' checkbox is also highlighted and is unchecked. Other parameters in the 'Analogue Extensions' section include: Default Outside Call Sequence (Normal), Default Inside Call Sequence (Ring Type 1), Default Ring Back Sequence (Ring Type 2), Restrict Analogue Extension Ringer Voltage (unchecked), Dial Delay Time (3), Dial Delay Count (0), Default No Answer Time (20), Hold Timeout (0), Park Timeout (300), Ring Delay (5), Call Priority Promotion Time (Disabled), Default Currency (USD), Default Name Priority (Favor Trunk), and Media Connection Preservation (Disabled). The 'DSS Status' checkbox is unchecked, while 'Auto Hold', 'Dial By Name', and 'Show Account Code' are checked. Other options like 'Restrict Network Interconnect', 'Drop External Only Impromptu Conference', 'Visually Differentiate External Call', 'Unsupervised Analog Trunk Disconnect Handling', 'High Quality Conferencing', 'Strict SIPs', and 'Digital/Analogue Auto Create User' are also checked.

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).

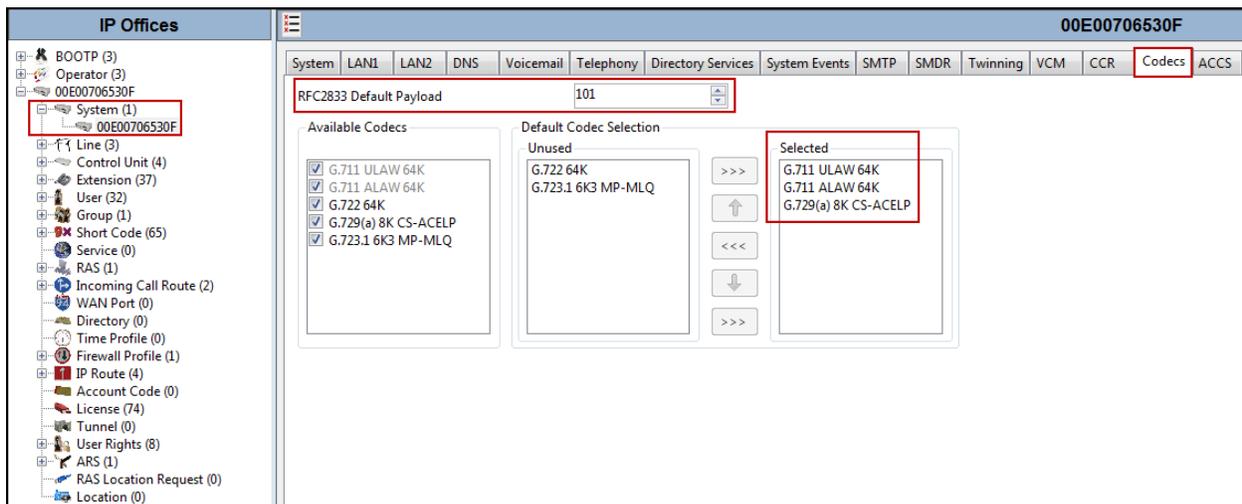


5.2.4 System - Codecs Tab

For Codec's 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 is new in IP Office release 9.0. It allows 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 phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific extension. The example below shows the codecs used for IP phones (SIP and H.323).
- Click OK to commit (not shown).

The Codec's settings are shown in the screenshot below with **G.711ULAW**, **G.711ALAW** and **G.729(a)** selected in prioritized order.



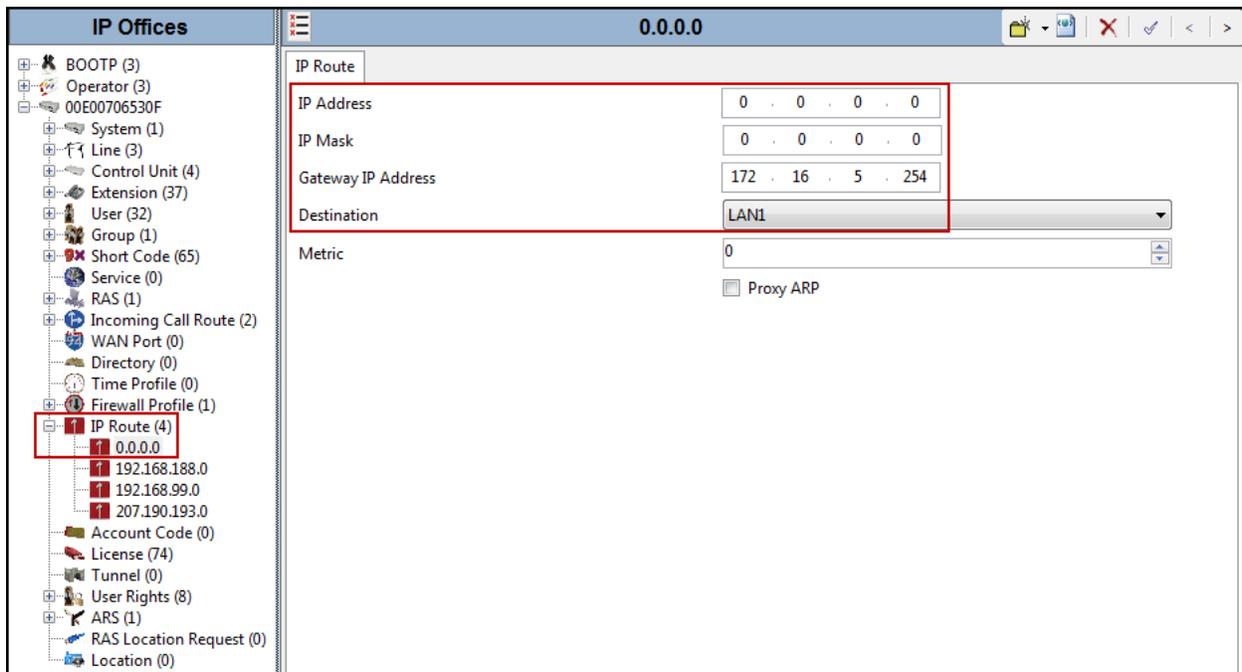
Note: The codec selections defined under this section (System – Codecs Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.5** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

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 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 IP subnets), on the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** of the IP 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 IP subnet.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).



5.4 SIP Line

A SIP line is needed to establish the SIP connection between IP Office and the Charter 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 IP Office Manager to create a SIP Line. Follow the steps in **Section 5.4.1** to create the SIP Line from the template.

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

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- ITSP Domain Name (should be left blank).
- Setting of the **Use Network Topology Info** field on the Transport tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 – 5.4.5**.

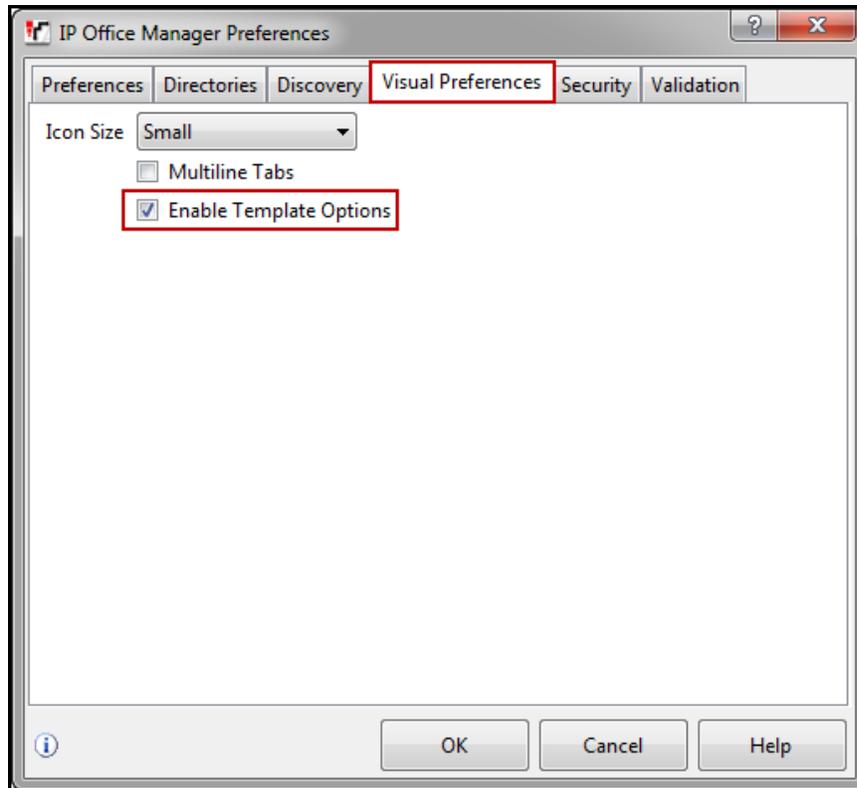
Also, the following SIP Line settings are not supported on Basic Edition:

- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

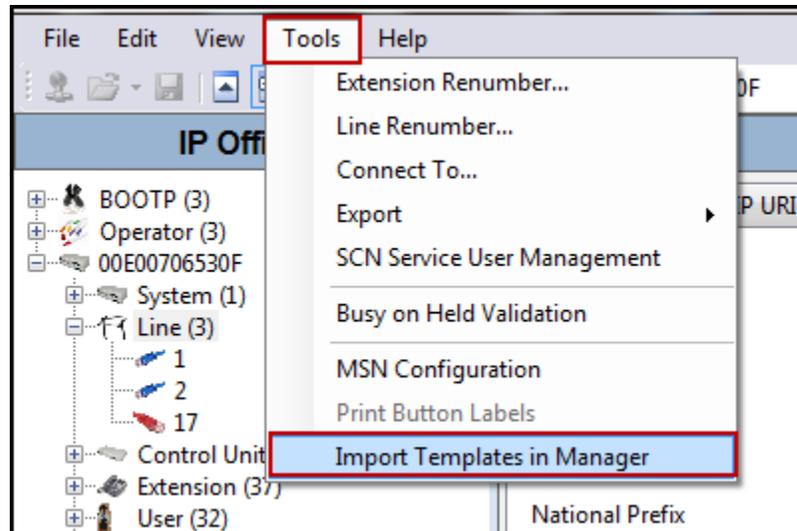
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2 – 5.4.5**.

5.4.1 Create a New SIP Trunk from Template

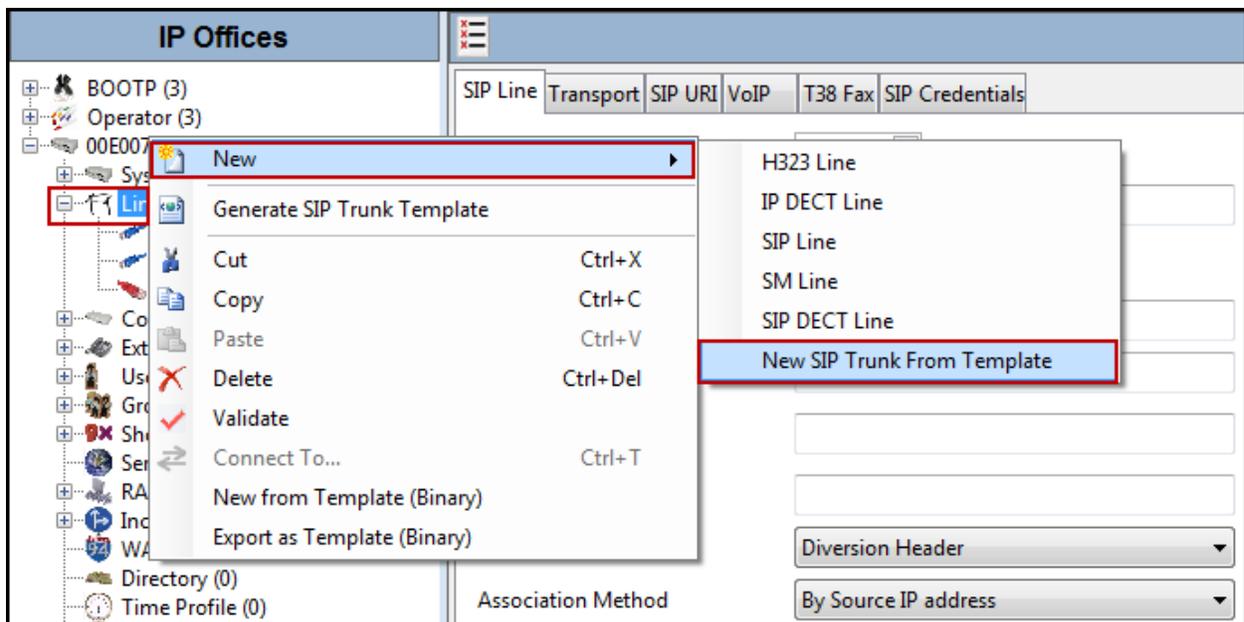
1. Copy the template file to the computer where IP Office Manager is installed. If needed rename the template file to **US_Charter_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.
2. Verify that template options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the **Visual Preferences** tab. Verify that the box is checked next to **Enable Template Options**. Click **OK**.



- Import the template into IP Office Manager. From IP Office Manager, select **Tools** → **Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template location is **C:\Program Files\Avaya\IP Office\Manager\Templates**.



- In the pop-up window (not shown) that appears select the directory where the template file was copied in **Step 1**. After the import is completed, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.
- To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New** → **New SIP Trunk From Template**.



6. In the subsequent Template Type Selection pop-up window, select **United States** from the **Country** pull-down menu and select **Charter** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**US_Charter_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2 – 5.4.5**.

Alternatively, a SIP Line can be created manually with the parameters shown below. To create a SIP line manually, begin by navigating to **Line** in the Navigation Pane. Right-click and select **New→ SIP Line**.

5.4.2 SIP Line - SIP Line Tab

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

- Leave the **ITSP Domain Name** blank.
- Verify that **In Service** box is checked.
- Verify that **Check OOS** box is checked. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Call Routing Method** is set to **Request URI**.
- Set **Send Caller ID** to **Diversion Header**.
- Uncheck the **REFER support** box. IP Office will not send REFER messages for calls that are transferred back to the PSTN (Refer to **Section 2.1**).
- Verify that **Method for Session Refresh** is set to **Auto**.
- Verify that **Session Timer (Seconds)** is set to **On Demand**.
- Verify that **Media Connection Preservation** is set to **Disabled**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

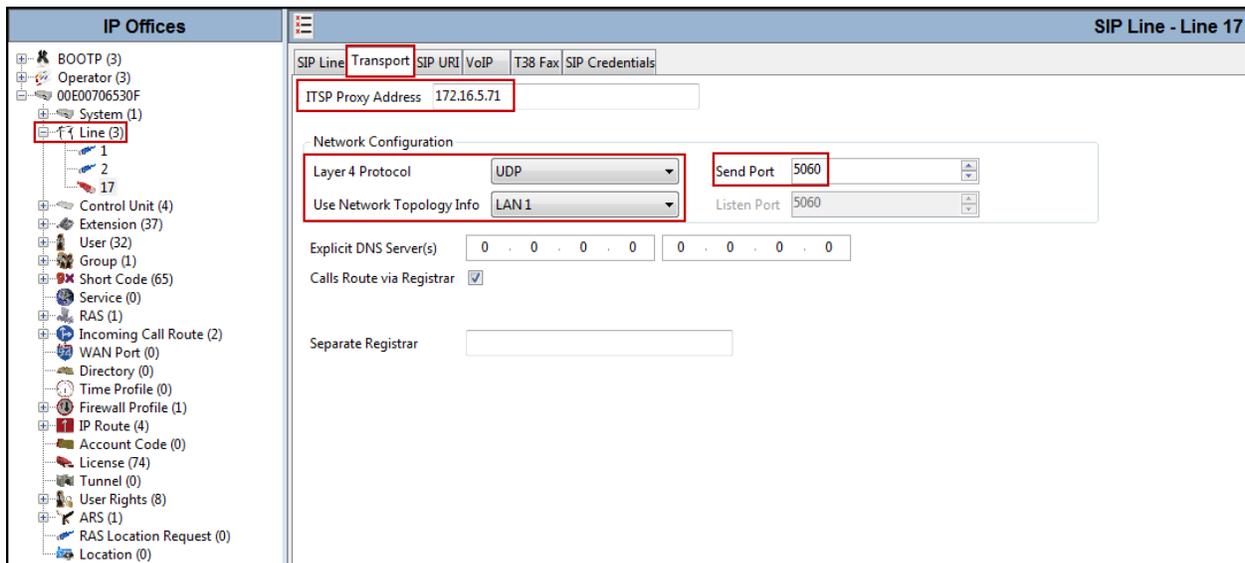
The screenshot displays the configuration page for a SIP Line (Line 17) in a software interface. The left sidebar shows a tree view of system components, with 'Line (3)' selected. The main area is titled 'SIP Line - Line 17' and contains the following configuration fields:

- Line Number:** 17
- ITSP Domain Name:** (Blank)
- In Service:**
- URI Type:** SIP
- Check OOS:**
- Call Routing Method:** Request URI
- Originator number for forwarded and twinning calls:** (Blank)
- Name Priority:** System Default
- Caller ID from From header:**
- Send From In Clear:**
- User-Agent and Server Headers:** (Blank)
- Service Busy Response:** 486 - Busy Here
- Action on CAC Location Limit:** Allow Voicemail
- Send Caller ID:** Diversion Header
- Association Method:** By Source IP address
- REFER Support:**
- Incoming:** Always
- Outgoing:** Always
- Method for Session Refresh:** Auto
- Session Timer (seconds):** On Demand
- Media Connection Preservation:** Disabled

5.4.3 SIP Line - Transport Tab

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

- Set the **ITSP Proxy Address**, this address was set to the inside IP Address of the Avaya SBCE or **172.16.5.71** as shown in **Figure 1**.
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



5.4.4 SIP Line - SIP URI Tab

A SIP URI entry needs to be created to match each incoming number that 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 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** to commit.
- Click **OK** to commit again (not shown).

The screenshot displays the IP Office configuration interface for a SIP Line. The left pane shows a tree view of IP Offices, with 'Line (3)' selected. The main pane shows the 'SIP Line - Line 17' configuration, with the 'SIP URI' tab active. A table lists the SIP URI entries, with the first entry selected. Below the table is the 'Edit Channel' dialog, which contains the following fields:

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

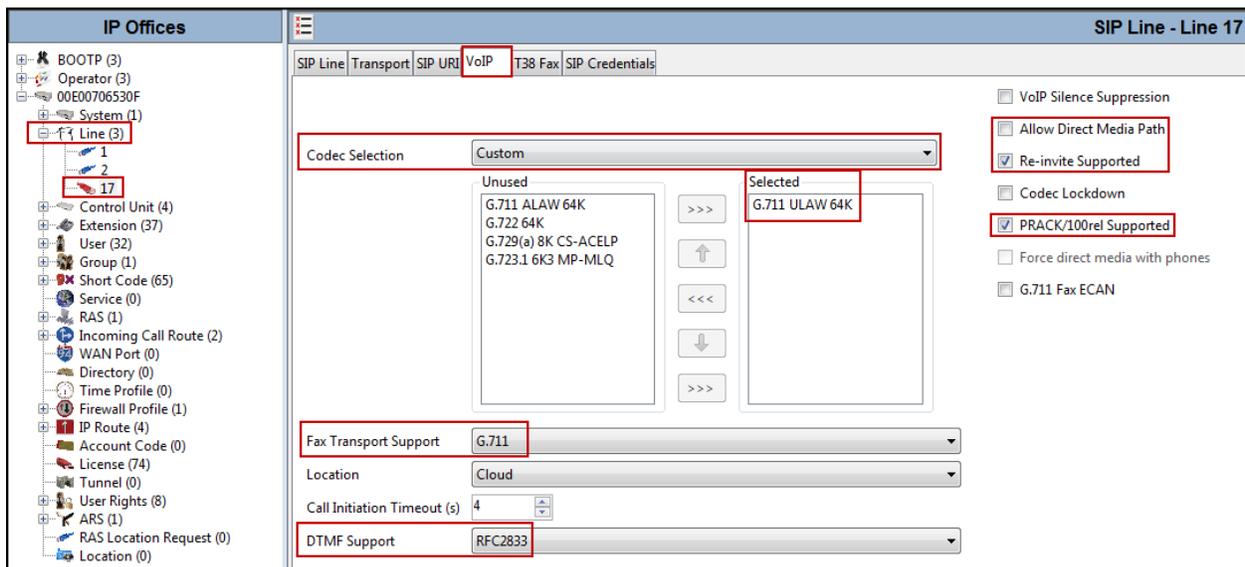
Via	172.16.5.60
Local URI	Use Internal Data
Contact	Use Internal Data
Display Name	Use Internal Data
PAI	None
Registration	0: <None>
Incoming Group	17
Outgoing Group	17
Max Calls per Channel	10

Additional SIP URIs may be required to allow inbound calls to numbers not associated with a user, such as a short code. These URIs are created in the same manner as shown above with the exception that the incoming DID number is entered directly in the **Local URI**, **Contact**, and **Display Name** fields.

5.4.5 SIP Line - VoIP Tab

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

- 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 IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Verify that **Allow Direct Media Path** is unchecked. Testing was done with Direct Media disabled.
- 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).

5.5 Extension

In this section, an example of an IP Office Extension will be illustrated. In the interests of brevity, not all users and extensions are 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 a H.323 Deskphone extension.

The screenshot displays the IP Office configuration interface. On the left, a tree view under 'IP Offices' shows a hierarchy: BOOTP (3), Operator (3), 00E00706530F, System (1), Line (3), Control Unit (4), and Extension (37). The 'Extension (37)' folder is selected, and a list of extensions is shown, with '8003 3040' highlighted. The main pane shows the configuration for this extension, with the 'Extn' tab selected. The configuration includes:

- Extension Id: 8003
- Base Extension: 3040
- Phone Password: (empty)
- Caller Display Type: On
- Reset Volume After Calls:
- Device Type: Unknown IP handset
- Location: Automatic
- Module: 0
- Port: 0
- Disable Speakerphone:

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

The screenshot displays the configuration page for H323 Extension 8003 3040. On the left, a tree view shows the hierarchy: IP Offices > BOOTP (3) > Operator (3) > 00E00706530F > System (1) > Line (3) > Control Unit (4) > Extension (37). The extension 8003 3040 is highlighted. The main configuration area is titled 'Ext: VoIP'. It includes fields for IP Address (0 . 0 . 0 . 0), MAC Address (00 00 00 00 00 00), and a Codec Selection dropdown set to 'System Default'. Below this are two lists: 'Unused' (G.722 64K, G.723.1 6K3 MP-MLQ) and 'Selected' (G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP). Navigation buttons (>>>, <<<, up, down) are between the lists. At the bottom, there are dropdown menus for Reserve License (None), TDM->IP Gain (Default), IP->TDM Gain (Default), and Supplementary Services (None). On the right side, there are checkboxes for VoIP Silence Suppression, Enable Faststart for non-Avaya IP phones, Out Of Band DTMF (checked), Local Tones, and Allow Direct Media Path (checked).

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**, which corresponds to a H.323 Deskphone extension.

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure under '00E00706530F'. The 'User (32)' folder is expanded, and the user '3040 Ext3040 H323' is selected and highlighted with a red box. The main configuration area on the right is titled 'Ext3040 H323: 3040' and shows the configuration for this user. The 'User' tab is active, and the configuration fields are as follows:

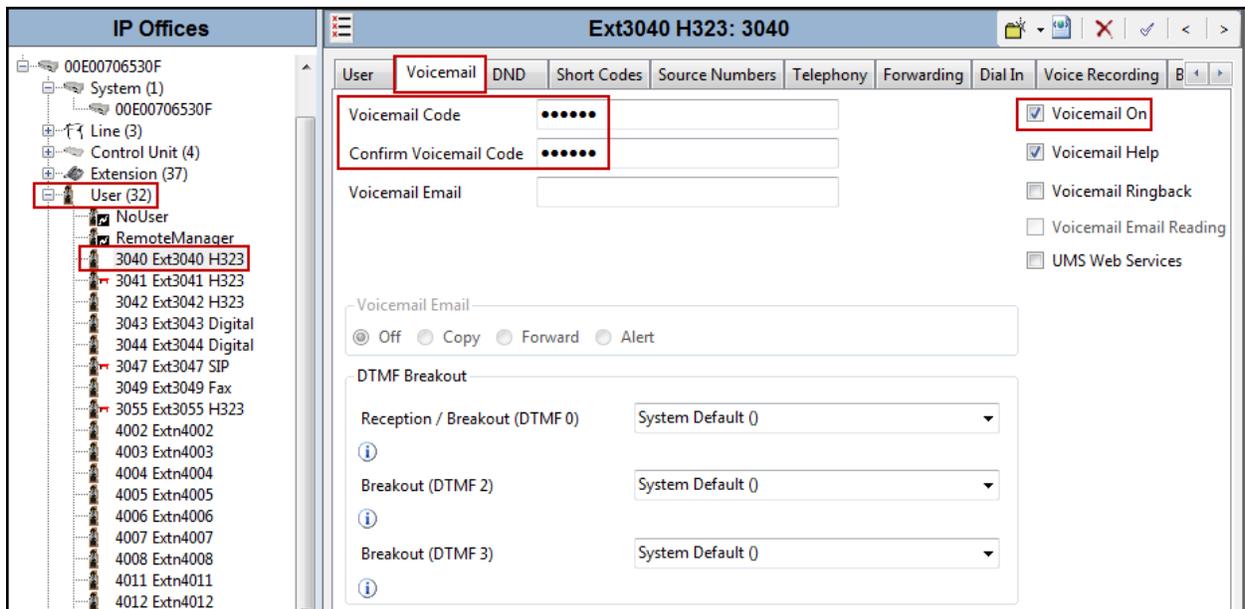
Field	Value
Name	Ext3040 H323
Password	••••
Confirm Password	••••
Account Status	Enabled
Full Name	Ext3040 H323
Extension	3040
Email Address	
Locale	
Priority	5
System Phone Rights	None
ACCS Agent Type	None
Profile	Basic User
Receptionist	<input type="checkbox"/>
Enable Softphone	<input type="checkbox"/>
Enable one-X Portal Services	<input checked="" type="checkbox"/>
Enable one-X TeleCommuter	<input type="checkbox"/>
Enable Remote Worker	<input checked="" type="checkbox"/>
Enable Flare	<input type="checkbox"/>
Enable Mobile VoIP Client	<input type="checkbox"/>
Send Mobility Email	<input type="checkbox"/>
Ex Directory	<input checked="" type="checkbox"/>
Device Type	Unknown IP handset
User Rights view	User data
Working hours time profile	<None>
Working hours User Rights	

In the example below, the name of the user is “Ext3047 SIP”. This is an IP Office Softphone user, set the Profile to **Power User** and check **Enable Softphone**.

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows a hierarchy: System (1) -> Line (3) -> Control Unit (4) -> Extension (37) -> User (32). The user '3047 Ext3047 SIP' is selected and highlighted with a red box. The main configuration pane on the right is titled 'Ext3047 SIP: 3047' and has tabs for 'User', 'Voicemail', 'DND', 'Short Codes', 'Source Numbers', 'Telephony', 'Forwarding', 'Dial In', and 'Voice Recording'. The 'User' tab is active. The configuration fields are as follows:

- 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
- Profile: Power User
- Receptionist:
- Enable Softphone: (highlighted with a red box)
- Enable one-X Portal Services:
- Enable one-X TeleCommuter:
- Enable Remote Worker:
- Enable Flare:
- Enable Mobile VoIP Client:
- Send Mobility Email:
- Ex Directory:
- Device Type: Unknown SIP device (with a phone icon)
- User Rights: User data
- Working hours time profile: <None>
- Working hours User Rights: [Dropdown]

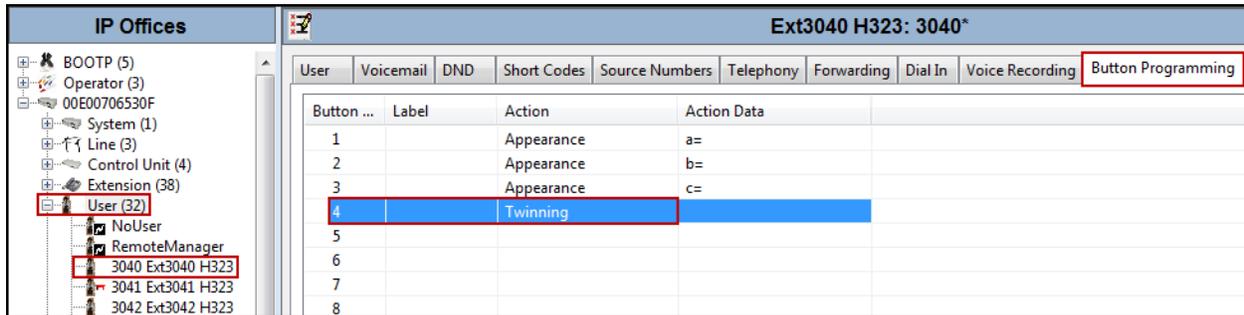
Select the **Voice Mail** tab. The following screen shows the **Voicemail** tab for the user with extension 3040. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application 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.

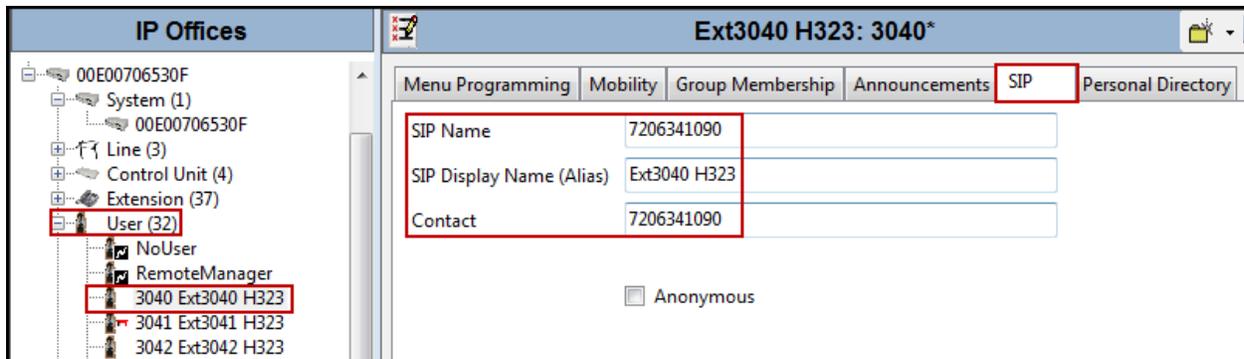
The screenshot displays the Avaya user configuration interface for User 3040. The left pane shows a tree view of the system hierarchy, with 'User (32)' expanded to show 'RemoteManager' and '3040 Ext3040 H323' selected. The right pane shows the 'Mobility' configuration tab for 'Ext3040 H323: 3040*'. The 'Internal Twinning' section is expanded, showing 'Twinned Handset' set to '<None>' and 'Maximum Number of Calls' set to '1'. The 'Mobility Features' and 'Mobile Twinning' checkboxes are checked. The 'Twinned Mobile Number (including dial access code)' field contains the value '917863311234'. Other settings include 'Twinning Time Profile' set to '<None>', 'Mobile Dial Delay (secs)' set to '2', and 'Mobile Answer Guard (secs)' set to '0'. The 'Hunt group calls eligible for mobile twinning', 'Forwarded calls eligible for mobile twinning', and 'Twin When Logged Out' checkboxes are unchecked. The 'one-X Mobile Client' checkbox is unchecked, 'Mobile Call Control' is checked, and 'Mobile Callback' is unchecked.

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 on 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 **7206341090** 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.



Note: Activating privacy by checking “Anonymous” (above) is not recommended with this solution since calls from IP Office to the PSTN will fail to complete, refer to **Section 2.2**.

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 5.4.4)** 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**.

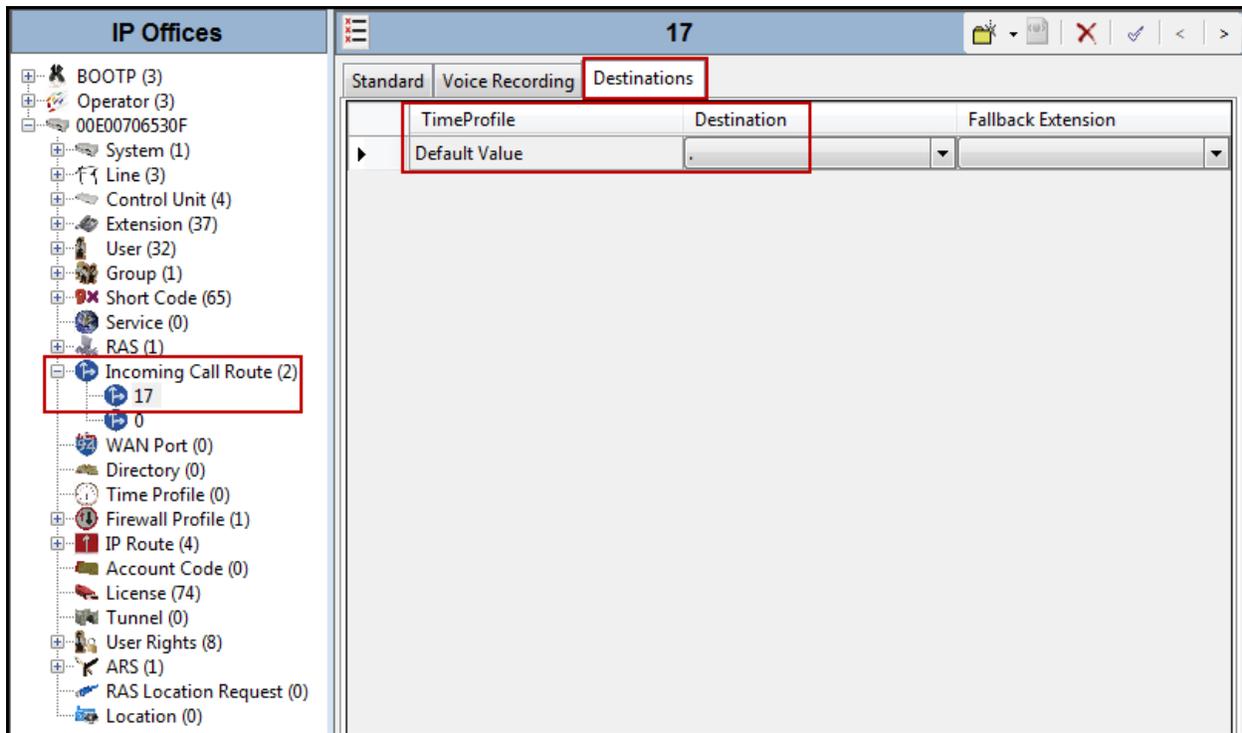
On the Details Pane (not shown), under the **Standard** tab, set the parameters as show bellow:

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

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'Incoming Call Route (2)' selected and highlighted with a red box. The right pane shows the configuration for line 17, with the 'Standard' tab selected. The 'Bearer Capacity' is set to 'Any Voice' and the 'Line Group ID' is set to '17', both highlighted with red boxes. Other parameters shown include Incoming Number, Incoming Sub Address, Incoming CLI, Locale, Priority (1 - Low), Tag, Hold Music Source (System Source), and Ring Tone Override (None).

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

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



5.8 Outbound Call Routing

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

5.8.1 Short Codes and Automatic Route Selection

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

The screenshot displays the 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 '9N: Dial' are shown. A red box highlights the following fields:

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

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **Xs** used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first digit on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office. The first example highlighted below shows that for calls to area codes in the North American Numbering Plan, the user dialed 9, followed by 11 digits, starting with a 1. The second example highlighted shows a seven digit number (for dialing seven digit local calls) starting with a 6, the user dialed 9, followed by the local number (e.g., 96341234).

The screenshot displays the configuration for the ARS route 'Main'. The 'ARS Route Id' is 50, and the 'Route Name' is 'Main'. The 'ARS' table contains the following entries:

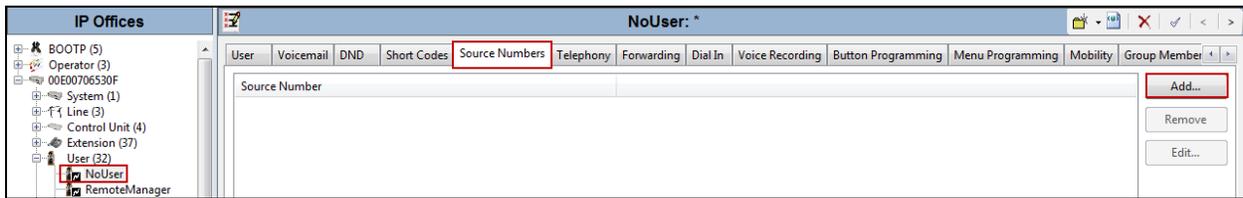
Code	Telephone Number	Feature	Line Group ID
001XXXXXXXXXX	001N	Dial	17
8XXXXXXXXXX	8N	Dial	17
1XXXXXXXXXX	1N	Dial	17
6XXXXXX	6N	Dial	17
3XXXXXXXXXX	3N	Dial	17
28XXXXXX	28N	Dial	17
55XXXXXXXXXX	55N	Dial	17

Additional settings shown include 'Secondary Dial tone' set to 'SystemTone', 'Check User Call Barring' checked, 'In Service' checked, and 'Alternate Route Priority Level' set to 3.

5.9 Privacy/Anonymous Calls

For outbound calls with privacy (anonymous) enabled, IP Office will replace the calling party number in the “From” and “Contact” headers of the SIP INVITE message with “restricted” and “anonymous” respectively. 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. By default, IP Office will use PPI for privacy. For the compliance test, PAI was used for the purposes of privacy.

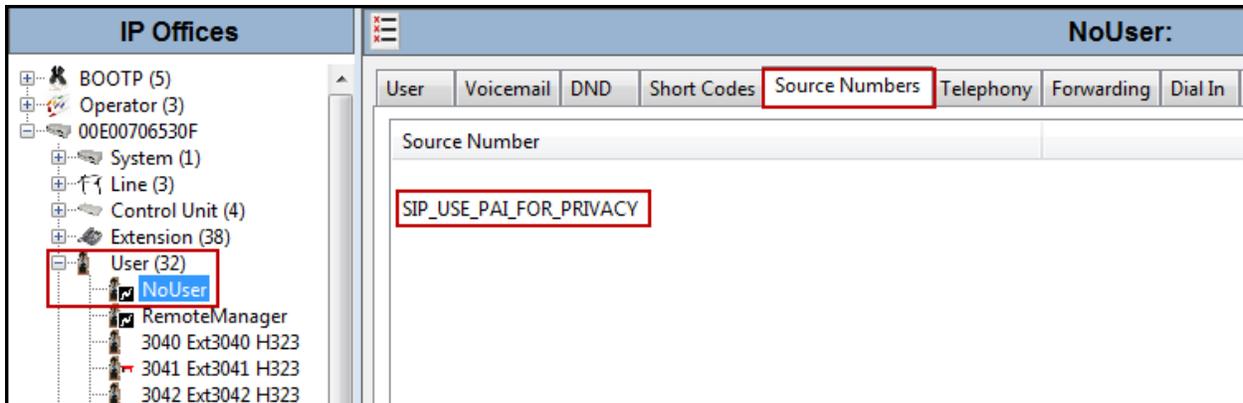
To configure IP Office to use PAI for privacy calls, navigate to **User → NoUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP_USE_PA1_FOR_PRIVACY**. Click **OK** (not shown).



The **SIP_USE_PA1_FOR_PRIVACY** parameter will appear in the list of Source Numbers as shown below.

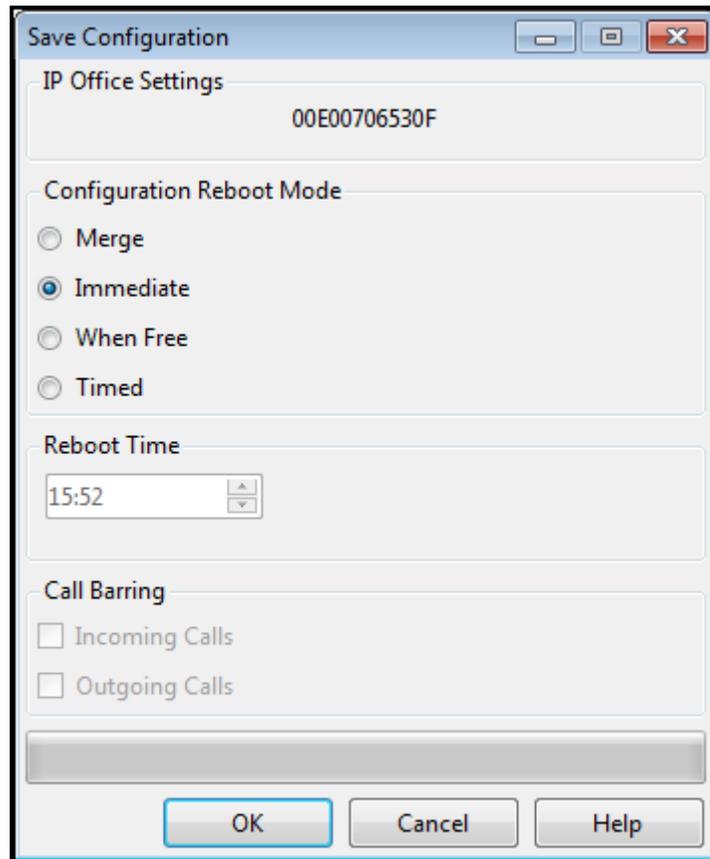


5.10 Save Configuration

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

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

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



The image shows a 'Save Configuration' dialog box with the following sections and controls:

- IP Office Settings:** A text field containing the value '00E00706530F'.
- Configuration Reboot Mode:** A group box containing four radio buttons: 'Merge', 'Immediate' (which is selected), 'When Free', and 'Timed'.
- Reboot Time:** A time selection control showing '15:52'.
- Call Barring:** A group box containing two checkboxes: 'Incoming Calls' and 'Outgoing Calls', both of which are currently unchecked.
- Buttons:** At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'.

6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For additional information on these configuration tasks, see **References Error! Reference source not found., Error! Reference source not found.** and Error! Reference source not found. in **Section 10**.

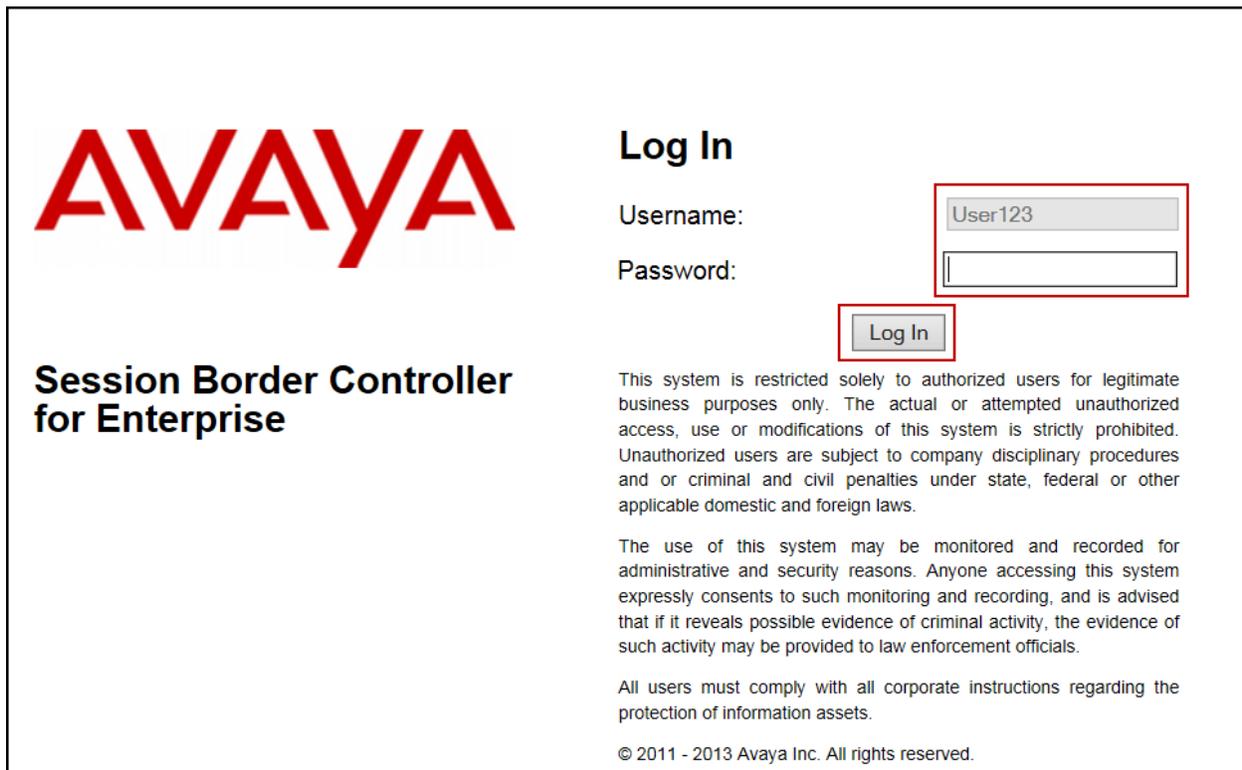
The configuration of the Avaya SBCE covers two major components, the Trunk Server for the service provider and Call Server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration was defined using the Avaya SBCE web user interface as described in the following sections.

Note: During the next pages and for brevity in these Application Notes not every provisioning step will have a screenshot associated with it.

6.1 Log into the Avaya Session Border Controller for Enterprise

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 management IP address.

Enter the appropriate credentials then 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 - 2013 Avaya Inc. All rights reserved.

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

The screenshot shows the Avaya Session Border Controller for Enterprise Dashboard. The navigation menu on the left includes Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Dashboard' and contains several sections: 'Information' with system time, version, and build date; 'Installed Devices' showing 'Avaya SBCE'; 'Alarms (past 24 hours)' with 'None found'; 'Incidents (past 24 hours)' with five entries of 'Avaya SBCE: No Server Flow Matched for Incoming Message'; and 'Notes' with 'No notes found'.

To view the system information that has been 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 the **View** as shown in the screenshot below.

The screenshot shows the Avaya Session Border Controller for Enterprise System Management page. The navigation menu on the left is the same as in the previous screenshot, but 'System Management' is highlighted. The main content area is titled 'System Management' and has tabs for 'Devices', 'Updates', 'SSL VPN', and 'Licensing'. The 'Devices' tab is active, showing a table with one device:

Device Name (Serial Number)	Management IP	Version	Status	
Avaya SBCE (IPCS31030132)	172.16.5.70	6.2.1.Q18	Commissioned	Reboot Shutdown Restart Application View Edit Delete

The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponded to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

IMPORTANT! – During the Avaya SBCE installation, the Management interface, (labeled “M1”), of the Avaya SBCE must be provisioned on a different IP subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to have this resolved.

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

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

General Configuration		Device Configuration	
Appliance Name	Avaya SBCE	HA Mode	No
Box Type	SIP	Two Bypass Mode	No
Deployment Mode	Proxy		

Network Configuration				
IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
192.168.157.185	192.168.157.185	255.255.255.192	192.168.157.129	B1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	B1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	B1
[Blurred]	[Blurred]	[Blurred]	[Blurred]	A1

DNS Configuration		Management IP(s)	
Primary DNS	172.16.5.102	IP	[Blurred]
Secondary DNS			
DNS Location	DMZ		
DNS Client IP	172.16.5.71		

On the screenshot shown above, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces of the Avaya SBCE respectively. The **A1** and **B1** interfaces and IP addresses shown are the ones relevant to the configuration of the SIP trunk to Charter. Other IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document, these IPs have been blurred out. The Management IP(s) was also blurred out for security reasons.

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 profile - Avaya-IPO

The Server Interworking function of the Global Profiles feature allows setting certain parameters to make the SBCE security device function in an enterprise VoIP network using different implementation of the SIP protocol.

Several profiles have already been 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 modifying a default profile is generally not recommended. For the Avaya-IPO interworking profile the default **avaya-ru** profile was duplicated, or “cloned”.

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

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



The screenshot shows a 'Clone Profile' dialog box. The title bar is 'Clone Profile' with a close button 'X'. The dialog contains two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'Avaya-IPO'. A red box highlights the 'Clone Name' field. Below the fields is a 'Finish' button.

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, and SIP Cluster. Under "System Management", "Global Profiles" is selected, and "Server Interworking" is highlighted. The main content area is titled "Interworking Profiles: Avaya-IPO" and features a list of profiles on the left, with "Avaya-IPO" selected. The right pane shows the configuration for the selected profile, with the "General" tab active. The configuration is organized into sections: General, Privacy, and DTMF. The "General" section includes settings for hold support, 180-183 handling, refer handling, URI group, 3xx handling, diversion header support, delayed SDP handling, re-invite handling, T.38 support, URI scheme, and via header format. The "Privacy" section includes privacy enabled, user name, P-Asserted-Identity, P-Preferred-Identity, and privacy header. The "DTMF" section includes DTMF support.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	
DTMF	
DTMF Support	None

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

The screenshot displays the configuration page for the **Avaya-IPO** Server Interworking Profile. The interface includes a navigation menu on the left, a list of interworking profiles in the center, and a configuration table on the right.

Navigation Menu:

- Dashboard
- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - Server Interworking
 - Domain DoS
 - Fingerprint
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration
 - Topology Hiding
 - Signaling Manipulation
 - URI Groups
- SIP Cluster
- Domain Policies
- TLS Management
- Device Specific Settings

Interworking Profiles:

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

Configuration Table (Advanced Tab):

General	Timers	URI Manipulation	Header Manipulation	Advanced
Record Routes				Both
Topology Hiding: Change Call-ID				No
Call-Info NAT				No
Change Max Forwards				Yes
Include End Point IP for Context Lookup				Yes
OCS Extensions				No
AVAYA Extensions				Yes
NORTEL Extensions				No
Diversion Manipulation				No
Metaswitch Extensions				No
Reset on Talk Spurt				No
Reset SRTP Context on Session Refresh				No
Has Remote SBC				Yes
Route Response on Via Port				No
Cisco Extensions				No

6.2.2 Server Interworking profile – SP-General

A second Server Interworking profile named **SP-General** was created for the service provider. Note that the **Add** button was used to add this profile.

On the left navigation pane, select **Global Profiles** → **Server Interworking**. From the **Interworking Profiles** list, select **Add** (not shown).

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.

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

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

The screenshot displays the configuration page for the **SP-General** Server Interworking Profile. The interface includes a navigation menu on the left, a list of interworking profiles in the center, and a detailed configuration table on the right.

Navigation Menu:

- Dashboard
- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles**
 - Domain DoS
 - Fingerprint
 - Server Interworking**
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration
 - Topology Hiding
 - Signaling Manipulation
 - URI Groups
 - SIP Cluster
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Interworking Profiles: SP-General

Interworking Profiles List:

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

Configuration Table:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	
DTMF	
DTMF Support	None

The following screen capture shows the **Advanced** tab of the newly created **SP-General** 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". On the left is a navigation menu with categories like Administration, System Management, and Global Profiles. The "Global Profiles" section is expanded, and "Server Interworking" is selected. The main content area shows "Interworking Profiles: SP-General" with a list of profiles including "SP-General" (highlighted). An "Add" button is present above the list. To the right, the configuration for the selected profile is shown, with tabs for General, Timers, URI Manipulation, Header Manipulation, and Advanced (selected). The Advanced tab contains a table of settings.

General	Timers	URI Manipulation	Header Manipulation	Advanced
Record Routes				Both
Topology Hiding: Change Call-ID				Yes
Call-Info NAT				No
Change Max Forwards				Yes
Include End Point IP for Context Lookup				No
OCS Extensions				No
AVAYA Extensions				No
NORTEL Extensions				No
Diversion Manipulation				No
Metaswitch Extensions				No
Reset on Talk Spurt				No
Reset SRTP Context on Session Refresh				No
Has Remote SBC				Yes
Route Response on Via Port				No
Cisco Extensions				No

6.2.3 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 in the test configuration, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to the service provider SIP trunk.

To create the inbound route with IP Office as the destination, from the **Global Profiles** menu on the left-hand side:

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



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route_to_IPO". Below the input field is a "Next" button.

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.60** (IP Office IP address).
- Check **Routing Priority Based on Next Hop Server**.
- Check **Outgoing Transport: UDP**.
- Click **Finish**.

Routing Profile

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group * ▾

Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port 172.16.5.60

Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port

Routing Priority based on
Next Hop Server

Use Next Hop
for In Dialog Messages

Ignore Route Header
for Messages Outside Dialog

NAPTR

SRV

Outgoing Transport TLS TCP UDP

Back Finish

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with categories: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing (highlighted), Server Configuration, Topology Hiding, Signaling Manipulation, URI Groups, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled 'Routing Profiles: Route_to_IPO'. It features an 'Add' button and a list of routing profiles: 'default', 'Route_to_SM', 'Route_to_SP', 'Route_to_CM', 'Route_to_CS1000', 'Route_to_IPO' (highlighted), and 'To SM from Rem W'. Above the list are 'Rename', 'Clone', and 'Delete' buttons.

The configuration details for the selected 'Route_to_IPO' profile are shown in a form. It includes a description field with the text 'Click here to add a description.' Below this is a table with the following structure:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	172.16.5.60	---	View Edit

An 'Add' button is located to the right of the table.

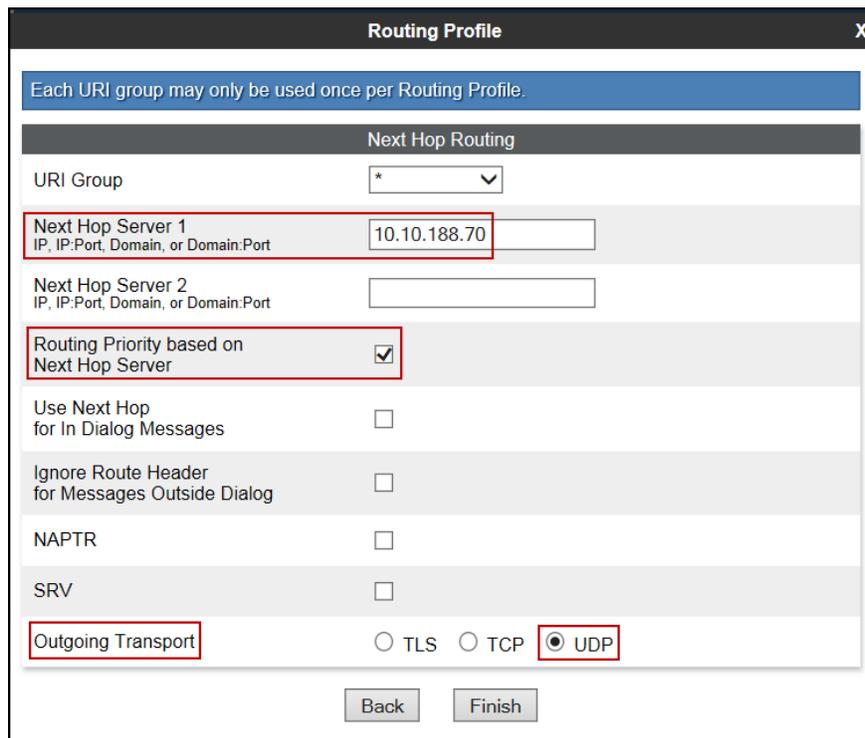
Similarly, to create the outbound route with the service provider as the destination, from the **Global Profiles** menu on the left-hand side:

- Select **Add** (not shown).
- Enter Profile Name: **Route_to_SP**.
- Click **Next**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Below the title bar, there is a text input field labeled "Profile Name" containing the text "Route_to_SP". A red rectangular box highlights this field. Below the input field, there is a "Next" button.

- **Next Hop Server 1: 10.10.188.70** (service provider's SIP proxy IP address).
- Check **Routing Priority Based on Next Hop Server**.
- Check **Outgoing Transport: UDP**.
- Click **Finish**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Below the title bar, there is a blue banner with the text "Each URI group may only be used once per Routing Profile." Below this banner, there is a section titled "Next Hop Routing". Under this section, there is a "URI Group" dropdown menu with a "*" symbol and a downward arrow. Below the dropdown menu, there are two "Next Hop Server" fields. The first field is labeled "Next Hop Server 1" and contains the IP address "10.10.188.70". The second field is labeled "Next Hop Server 2" and is empty. Below the "Next Hop Server 1" field, there is a checkbox labeled "Routing Priority based on Next Hop Server" which is checked. Below the "Routing Priority based on Next Hop Server" checkbox, there are three checkboxes: "Use Next Hop for In Dialog Messages", "Ignore Route Header for Messages Outside Dialog", and "NAPTR", all of which are unchecked. Below the "Ignore Route Header for Messages Outside Dialog" checkbox, there is a checkbox labeled "SRV" which is unchecked. Below the "SRV" checkbox, there is a section labeled "Outgoing Transport" with three radio buttons: "TLS", "TCP", and "UDP". The "UDP" radio button is selected. Below the "Outgoing Transport" section, there are two buttons: "Back" and "Finish".

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', '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 'Global Profiles' and 'Routing' highlighted. The main content area is titled 'Routing Profiles: Route_to_SP' and features an 'Add' button. Below this, a list of routing profiles is shown, with 'Route_to_SP' selected. A detailed view of the 'Route_to_SP' profile is displayed, showing a table with columns for 'Priority', 'URI Group', 'Next Hop Server 1', and 'Next Hop Server 2'. The table contains one entry with a priority of 1 and a next hop server of 10.10.188.70. An 'Add' button is visible in the top right corner of the table area.

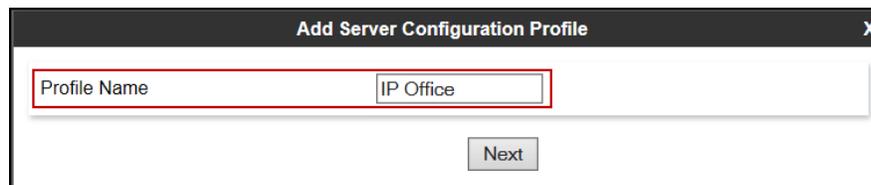
Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	10.10.188.70	---

6.2.4 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:

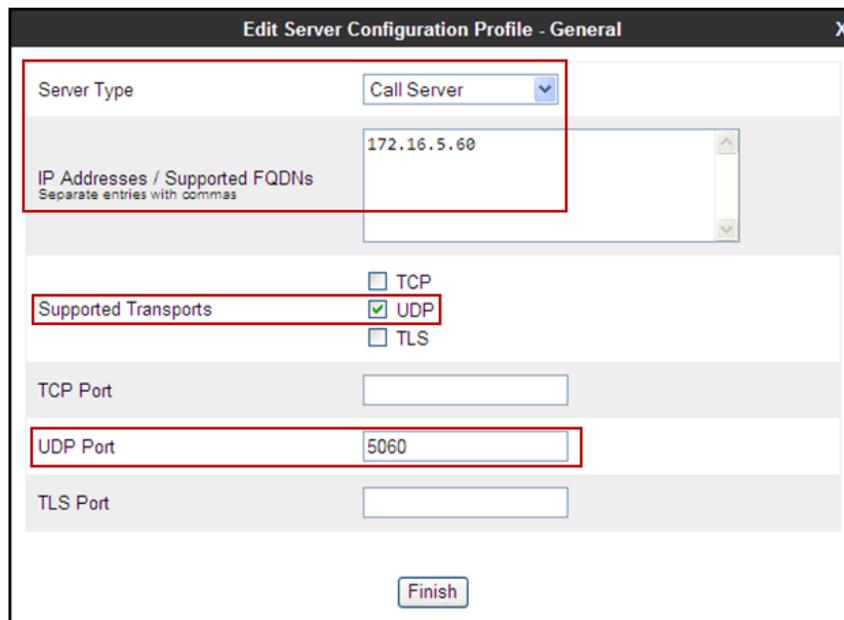
- Select **Server Configuration** (not shown).
- Click **Add** (not shown).
- Enter the profile name: **IP Office**,
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. The "Profile Name" field is highlighted with a red box and contains the text "IP Office". Below the field is a "Next" button.

On the **Add Server Configuration Profile** Tab:

- Select Server Type: **Call Server**.
- **IP Address: 172.16.5.60** (IP Address of IP Office).
- **Supported Transports: Check UDP.**
- **UDP Port: 5060.**
- Click **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. The "Server Type" dropdown is set to "Call Server". The "IP Addresses / Supported FQDNs" field contains "172.16.5.60". The "Supported Transports" section has "UDP" checked. The "UDP Port" field contains "5060". A "Finish" button is at the bottom.

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

- Click **Next** on the **Authentication** tab (not shown).
- Click **Next** on the **Heartbeat** tab (not shown).
- On the **Advanced** tab, select **Avaya-IPO** from the **Interworking Profile** drop down menu. Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection

Enable Grooming

Interworking Profile: Avaya-IPO

Signaling Manipulation Script: None

UDP Connection Type: SUBID PORTID MAPPING

Back Finish

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

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise AVAYA

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles Domain DoS Fingerprint Server Interworking Phone Interworking Media Forking Routing Server Configuration Topology Hiding Signaling Manipulation URI Groups SIP Cluster Domain Policies TLS Management Device Specific Settings

Server Configuration: IP Office Add Rename Clone Delete

Server Profiles: Session Manager, Service Provider, Com Manager, CS1000, **IP Office**

General Authentication Heartbeat Advanced

Server Type	Call Server
IP Addresses / FQDNs	172.16.5.60
Supported Transports	UDP
UDP Port	5060

Edit

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

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main title is 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A left sidebar lists various configuration categories, with 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: IP Office' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced', with 'Advanced' selected. A table lists configuration parameters:

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

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

Similarly, to add the profile for the Trunk Server, from the **Server Configuration** screen:

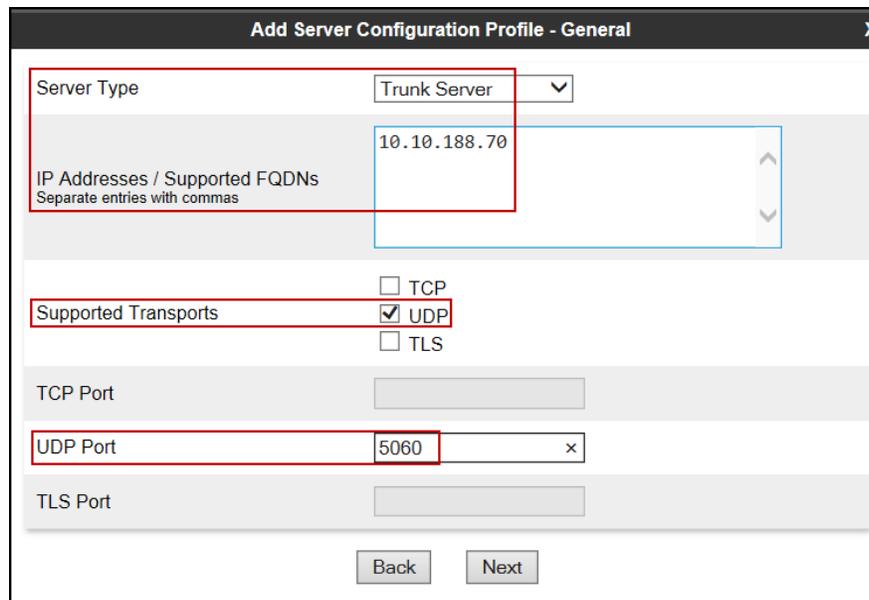
- Click **Add** (not shown).
- Enter the profile name: **Service Provider**.
- Click **Next**.



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

On the **Add Server Configuration Profile** Tab:

- Select Server Type: **Trunk Server**.
- **IP Address: 10.10.188.70** (service provider's SIP proxy IP address).
- **Supported Transports: Check UDP.**
- **UDP Port: 5060.**
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - General". It contains several fields and checkboxes:

- Server Type:** A dropdown menu set to "Trunk Server".
- IP Addresses / Supported FQDNs:** A text area containing "10.10.188.70". Below the text area is the instruction "Separate entries with commas".
- Supported Transports:** Three checkboxes: "TCP" (unchecked), "UDP" (checked), and "TLS" (unchecked).
- TCP Port:** An empty text input field.
- UDP Port:** A text input field containing "5060".
- TLS Port:** An empty text input field.

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

On the **Authentication** tab:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Leave **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

The screenshot shows a dialog box titled "Add Server Configuration Profile - Authentication". The dialog contains the following fields and controls:

- Enable Authentication:** A checkbox that is checked.
- User Name:** A text input field containing "User123".
- Realm:** A text input field that is empty, with the instruction "(Leave blank to detect from server challenge)" below it.
- Password:** A text input field with masked characters (dots).
- Confirm Password:** A text input field with masked characters (dots) and a small icon to the right.
- Buttons:** "Back" and "Next" buttons are located at the bottom of the dialog.

On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the service provider proxy server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider, **60** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI**: Use the **User Name** entered above under the **Authentication** screen (**User123**) and the service provider's domain name (**charterlabs.net**), as shown on the screen below.
Note: The **User Name** and **domain name** should be provided by the service provider.
 - **To URI**: Use the **User Name** entered above under the **Authentication** screen (**User123**) and the service provider proxy provider's domain name (**charterlabs.net**), as shown on the screen below.
Note: The **User Name** and **domain name** should be provided by the service provider.
 - Click **Next**.

Add Server Configuration Profile - Heartbeat

Enable Heartbeat

Method REGISTER

Frequency 60 seconds

From URI User123@charterlabs.r

To URI User123@charterlabs.r

Back Next

On the **Advanced** tab:

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

Add Server Configuration Profile - Advanced

Enable DoS Protection

Enable Grooming

Interworking Profile SP-General

Signaling Manipulation Script None

UDP Connection Type SUBID PORTID MAPPING

Back Finish

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

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'. The main title is 'Session Border Controller for Enterprise'. On the left is a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', and 'Server Configuration'. The 'Server Configuration' section is expanded to show 'Global Profiles', with 'Service Provider' selected. The main content area is titled 'Server Configuration: Service Provider' and features an 'Add' button and four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a table of configuration parameters:

Parameter	Value
Server Type	Trunk Server
IP Addresses / FQDNs	10.10.188.70
Supported Transports	UDP
UDP Port	5060

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

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. At the top, there is a navigation bar with links for 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'. Below this, the main title 'Session Border Controller for Enterprise' is shown. On the left side, a sidebar menu lists various configuration categories, with 'Global Profiles' and 'Server Configuration' highlighted in red. The main content area is titled 'Server Configuration: Service Provider 1' and features an 'Add' button. Below the title, there is a 'Server Profiles' list containing 'Session Manager', 'Com Manager', 'CS1000', and 'IP Office', with 'Service Provider' highlighted in red. To the right of the list are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced', with 'Authentication' selected. The 'Authentication' tab contains a form with the following fields: 'Enable Authentication' (checked), 'User Name' (user123), and 'Realm' (---). An 'Edit' button is located at the bottom right of the form.

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

The screenshot displays the 'Session Border Controller for Enterprise' management console. The left sidebar shows a navigation menu with 'Global Profiles' and 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: Service Provider 1' and features a 'Server Profiles' list on the left and a configuration table on the right. The 'Heartbeat' tab is selected, showing the following settings:

General	Authentication	Heartbeat	Advanced
Enable Heartbeat			<input checked="" type="checkbox"/>
Method		REGISTER	
Frequency		60 seconds	
From URI		User123@charterlabs.net	
To URI		User123@charterlabs.net	

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

The screenshot displays the 'Session Border Controller for Enterprise' management console, showing the 'Advanced' configuration for a 'Service Provider'. The 'Advanced' tab is selected in the configuration table, showing the following settings:

General	Authentication	Heartbeat	Advanced
Enable DoS Protection			<input type="checkbox"/>
Enable Grooming			<input type="checkbox"/>
Interworking Profile		SP-General	
Signaling Manipulation Script		None	
UDP Connection Type		SUBID	

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 the 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:

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



Field	Value
Profile Name	default
Clone Name	IP Office

Finish

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows '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', 'Global Parameters', 'Global Profiles', 'Domain DoS', 'Fingerprint', 'Server Interworking', 'Phone Interworking', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Global Profiles' and 'Topology Hiding' items are highlighted with red boxes.

The main content area is titled 'Topology Hiding Profiles: IP Office'. It features an 'Add' button and a list of profiles: 'default', 'cisco_th_profile', 'Session_Manager', 'Service_Provider', 'Com Manager', 'CS1000', and 'IP Office'. The 'IP Office' profile is selected and highlighted with a red box.

Below the profile list, there is a table for the 'Topology Hiding' configuration. The table has four columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table contains the following data:

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

Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible at the top and bottom of the configuration area.

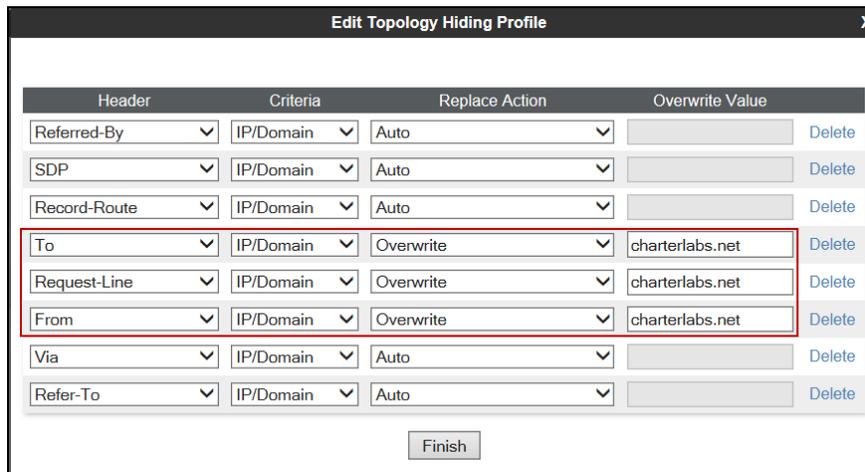
To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

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



The screenshot shows a dialog box titled "Clone Profile". It has two input fields: "Profile Name" with the value "default" and "Clone Name" with the value "Service_Provider". The "Clone Name" field is highlighted with a red border. A "Finish" button is located at the bottom center of the dialog.

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



The screenshot shows a dialog box titled "Edit Topology Hiding Profile". It contains a table with the following columns: Header, Criteria, Replace Action, and Overwrite Value. The table has 8 rows. The 'To', 'Request-Line', and 'From' rows are highlighted with a red border. Each of these rows has 'Overwrite' selected in the 'Replace Action' column and 'charterlabs.net' entered in the 'Overwrite Value' column. A 'Finish' button is at the bottom center.

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

The following screen capture shows the newly created **Service_Provider** Topology Hiding Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The main heading is "Session Border Controller for Enterprise" with the Avaya logo on the right. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and SIP Cluster. The "Global Profiles" section is expanded, and "Topology Hiding" is selected. The main content area is titled "Topology Hiding Profiles: Service_Provider" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a list of "Topology Hiding Profiles" with "Service_Provider" highlighted. The "Service_Provider" profile is expanded to show a table of header rules.

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

6.3 Domain Policies

Domain Policies allow the configuration of 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. Domain Policies include rules for Application, Media, Signaling, Security, etc.

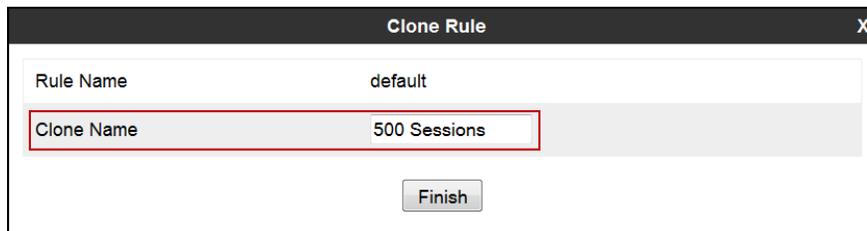
In the reference configuration, a new Application Rule was defined. All other rules under Domain Policies, linked together on End Point Policy Groups, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

6.3.1 Create Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device 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.

To add a new Application Rule, from the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Select **default trunk** Rule (not shown).
- Select **Clone Rule** button (not shown).
- Enter the **Application Rule Name: 500 Sessions**.
- Click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	500 Sessions
<input type="button" value="Finish"/>	

- Click **Edit** on the newly created **500 Sessions** Application Rule.
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** per license values specific to the enterprise, the value of **500** for **Audio** and **100** for Video was used in the sample configuration.
- Click **Finish**.

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

Miscellaneous

CDR Support: None, CDR w/ RTP, CDR w/o RTP

RTCP Keep-Alive:

Finish

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

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles SIP Cluster **Domain Policies** Application Rules Border Rules Media Rules Security Rules Signaling Rules Time of Day Rules End Point Policy Groups Session Policies TLS Management Device Specific Settings

Application Rules: 500 Sessions

Add Filter By Device... Rename Clone Delete

Click here to add a description.

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

Miscellaneous

CDR Support: None

RTCP Keep-Alive: No

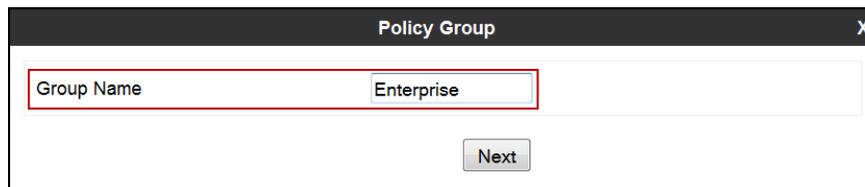
Edit

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.

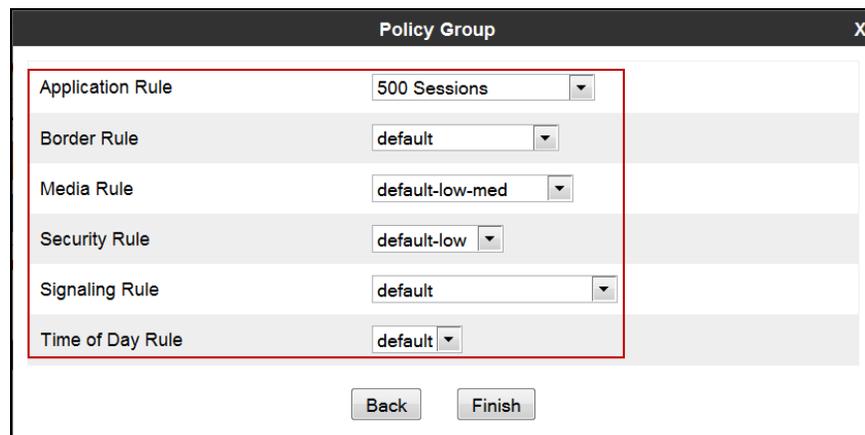
To create an End Point Policy Group for the enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add** (not shown).

- **Group Name: Enterprise.**
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" containing the text "Enterprise". 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.**
- **Time of Day: default.**
- Click **Finish**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. The dialog contains a list of rule settings, each with a dropdown menu. A red box highlights the first six rows. At the bottom, there are "Back" and "Finish" buttons.

Application Rule	500 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default
Time of Day Rule	default

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

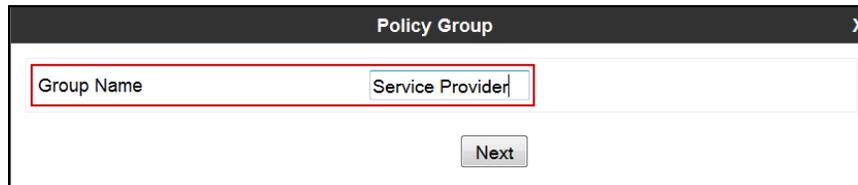
The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'SIP Cluster', 'Domain Policies', 'Application Rules', 'Border Rules', 'Media Rules', 'Security Rules', 'Signaling Rules', 'Time of Day Rules', 'End Point Policy Groups', 'Session Policies', 'TLS Management', and 'Device Specific Settings'. The 'End Point Policy Groups' item is highlighted with a red box.

The main content area is titled 'Policy Groups: Enterprise'. It features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are two blue bars with the text 'Click here to add a description'. A 'Policy Group' form is visible, containing a 'Summary' and 'Add' button. At the bottom, a table lists the policy groups:

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	500 Sessions	default	default-low-med	default-low	default	default	Edit Clone

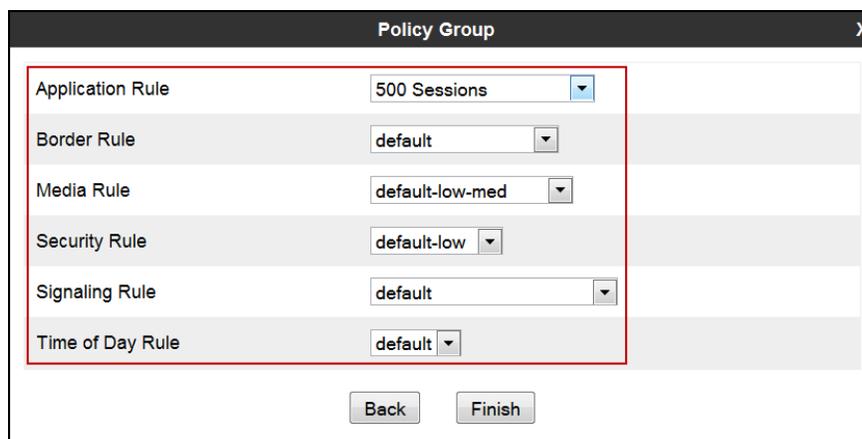
Similarly, to create an End Point Policy Group for the service provider SIP Trunk, select **Add** (not shown).

- **Group Name: Service Provider.**
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "Service Provider". A red rectangular box highlights this field. Below the input field, there is a "Next" button.

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



The screenshot shows the "Policy Group" dialog box with several dropdown menus. A red rectangular box highlights the following configurations:

Rule Type	Value
Application Rule	500 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default
Time of Day Rule	default

At the bottom of the dialog, there 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 Statistics Logs Diagnostics Users Settings Help Log Out

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Time of Day 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

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- avaya-def-high-subscriber
- avaya-def-high-server
- Enterprise
- Service Provider**
- Rem Workers Inside

Click here to add a description.

Hover over a row to see its description.

Policy Group Summary Add

Order	Application	Border	Media	Security	Signaling	Time of Day
1	500 Sessions	default	default-low-med	default-low	default	default

Edit Clone

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** menu 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 could be entered here.

For IP address assignments refer to **Figure 1**.

The screenshot displays the Avaya SBCE Network Management interface. The left sidebar shows the navigation menu with 'Device Specific Settings' expanded to 'Network Management'. The main content area is titled 'Network Management: Avaya SBCE' and has two tabs: 'Network Configuration' (selected) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.192), and 'B2 Netmask'. An 'Add' button and 'Save'/'Clear' buttons are also present. A table lists the configured IP addresses and their associated interfaces:

IP Address	Public IP	Gateway	Interface	Action
172.16.5.71		172.16.5.254	A1	Delete
192.168.157.185		192.168.157.129	B1	Delete
192.168.157.186		192.168.157.129	B1	Delete
192.168.157.187		192.168.157.129	B1	Delete
172.16.5.72		172.16.5.254	A1	Delete

On the previous screenshot, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces of the Avaya SBCE respectively. The **A1** and **B1** interfaces and IP addresses shown are the ones relevant to the configuration of the SIP trunk to Charter. Other IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document, these IPs have been blurred out.

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

The screenshot shows the Avaya SBCE web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', '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', 'Global Parameters', 'Global Profiles', 'SIP Cluster', 'Domain Policies', 'TLS Management', 'Device Specific Settings', and 'Network Management'. The 'Network Management' section is expanded, showing 'Avaya SBCE' and 'Interface Configuration' tabs. The 'Interface Configuration' tab is active, displaying a table with the following data:

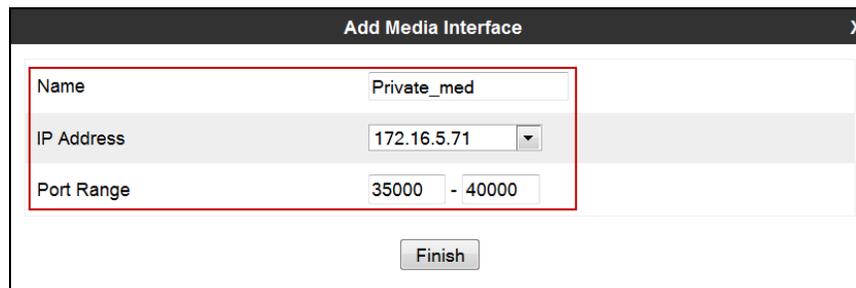
Name	Administrative Status	Toggle
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

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 ports range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**. Below is the configuration of the inside or private Media Interface of the Avaya SBCE.

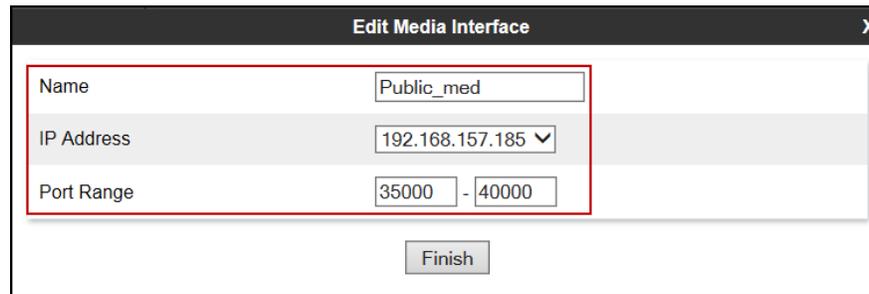
- Select **Add** in the **Media Interface** area (not shown).
- **Name: Private_med.**
- **IP Address: 172.16.5.71** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office).
- **Port Range: 35000-40000.**
- Click **Finish**.



Add Media Interface	
Name	Private_med
IP Address	172.16.5.71
Port Range	35000 - 40000
<input type="button" value="Finish"/>	

Below is the configuration of the outside or public Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area.
- **Name: Public_med.**
- **IP Address: 192.168.157.185** (Outside or B1 IP Address of the Avaya SBCE, toward the service provider).
- **Port Range: 35000-40000.**
- Click **Finish**.



Edit Media Interface X

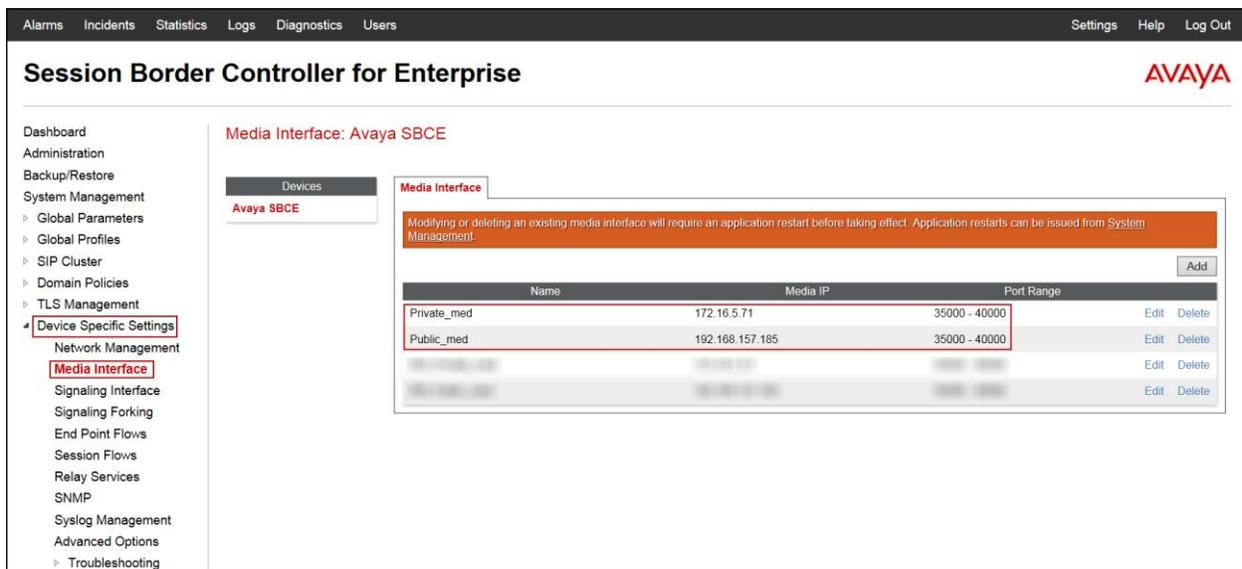
Name: Public_med

IP Address: 192.168.157.185

Port Range: 35000 - 40000

Finish

The following screen capture shows the newly created Media Interfaces.



Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
 Global Parameters
 Global Profiles
 SIP Cluster
 Domain Policies
 TLS Management
 Device Specific Settings
 Network Management
 Media Interface
 Signaling Interface
 Signaling Forking
 End Point Flows
 Session Flows
 Relay Services
 SNMP
 Syslog Management
 Advanced Options
 Troubleshooting

Media Interface: Avaya SBCE

Devices
Avaya SBCE

Media Interface

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

Add

Name	Media IP	Port Range	Edit	Delete
Private_med	172.16.5.71	35000 - 40000	Edit	Delete
Public_med	192.168.157.185	35000 - 40000	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**.
- **IP Address: 172.16.5.71** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port: 5060**.
- Click **Finish**.

Name	Private_sig
IP Address	172.16.5.71
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	5060
Enable Stun	<input type="checkbox"/>
TLS Port <small>Leave blank to disable</small>	
TLS Profile	AvayaSBCServer
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

Below is the configuration of the outside or public signaling Interface of the Avaya SBCE.

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: Public_sig**.
- **IP Address: 192.168.157.185** (Outside or B1 IP Address of the Avaya SBCE, toward the service provider).
- **UDP Port: 5060**.
- Click **Finish**.

Add Signaling Interface

Name: Pubic_sig

IP Address: 192.168.157.185

TCP Port: Leave blank to disable

UDP Port: 5060

Enable Stun:

TLS Port: Leave blank to disable

TLS Profile: AvayaSBCServer

Enable Shared Control:

Shared Control Port:

Finish

The following screen capture shows the newly Created Signaling Interfaces.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options
Troubleshooting

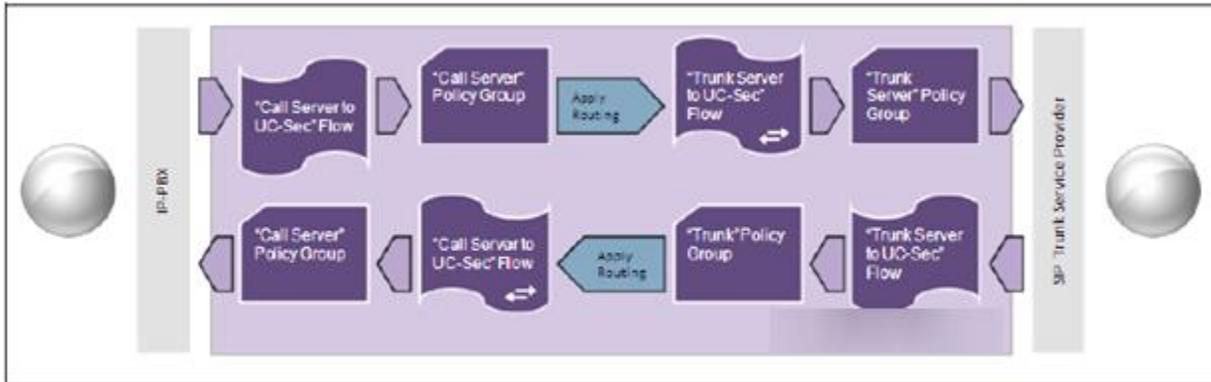
Signaling Interface: Avaya SBCE

Devices: Avaya SBCE

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Private_sig	172.16.5.71	---	5060	---	None	Edit	Delete
Public_sig	192.168.157.185	---	5060	---	None	Edit	Delete
						Edit	Delete
						Edit	Delete

6.4.4 End Point Flows

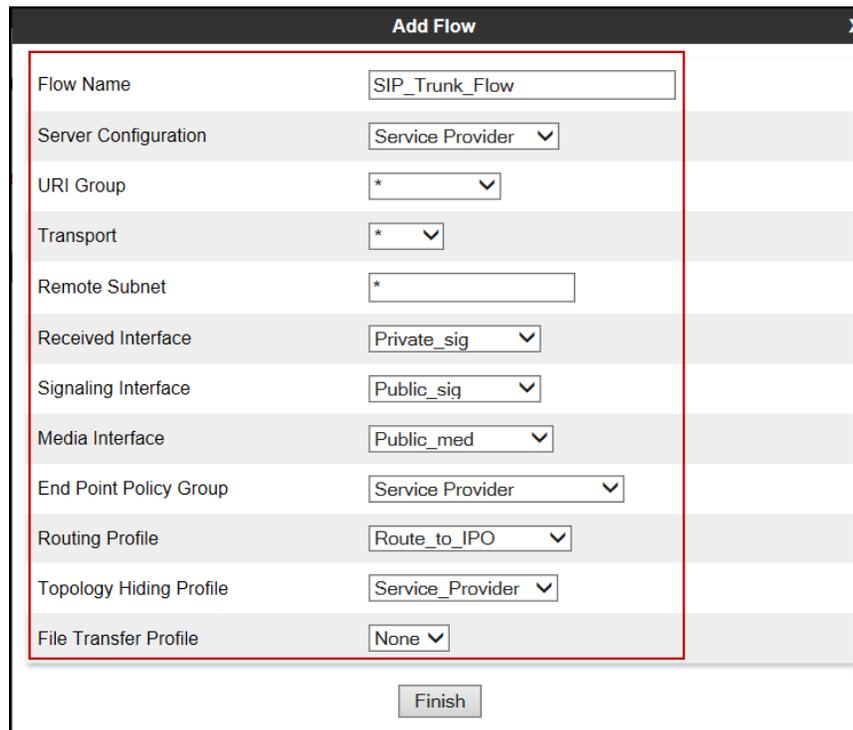
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing 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** defines 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 the service provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, tab **Server Flows**. Click **Add Flow** (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.
- **File Transfer Profile:** None.
- Click **Finish**.



The screenshot shows a window titled "Add Flow" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a corresponding input field or dropdown menu. A red rectangular box highlights the entire configuration area. At the bottom of the window, there is a "Finish" button.

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
File Transfer Profile	None

Finish

To create the call flow toward IP Office, click **Add 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** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: IP Office.**
- **File Transfer Profile: None.**
- Click **Finish**.

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
File Transfer Profile	None

Finish

The following screen capture shows the newly created Server Flows.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar menu lists various configuration areas, with 'End Point Flows' highlighted in red. The main content area is titled 'End Point Flows: Avaya SBCE' and features a 'Server Flows' tab. Below this, there are three tables representing server configurations for 'IP Office', 'Service Provider', and 'Session Manager'. Each table has columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile, along with 'View', 'Clone', 'Edit', and 'Delete' actions. The 'IP Office' table contains one row with 'IP_Office_Flow' as the flow name. The 'Service Provider' table contains one row with 'SIP_Trunk_Flow' as the flow name. The 'Session Manager' table is partially visible and contains one row.

End Point Flows: Avaya SBCE

Subscriber Flows Server Flows

Avaya SBCE

Click here to add a row description

Server Configuration: IP Office

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

Server Configuration: Service Provider

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

Server Configuration: Session Manager

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
							View Clone Edit Delete

7. Charter Communications SIP Trunking Configuration

To use Charter Communications 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.

Charter is responsible for the configuration of the SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya Session Border Controller for Enterprise at the customer's enterprise site. Charter Communications will provide the customer the necessary information to configure the SIP trunk connection, including:

- IP address of Charter's SIP Proxy server.
- SIP Trunk registration credentials.
- Supported codec's and order of preference.
- DID numbers.
- Etc.

8. Verification and Troubleshooting

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

8.1 Verification Steps

The following steps may be used to verify the configuration:

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

8.2 Protocol Traces

The following SIP message headers are inspected using 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.

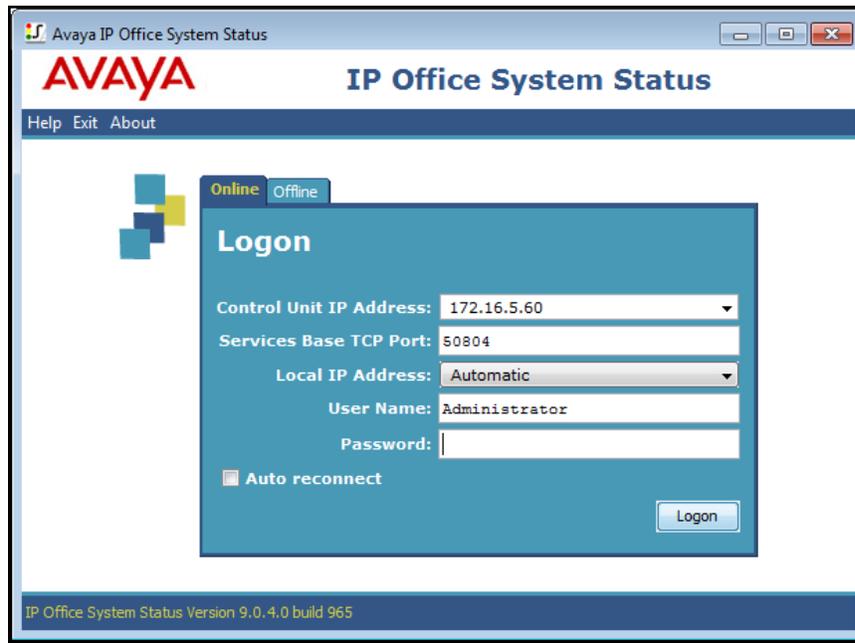
The following attributes in SIP message body are inspected using sniffer trace analysis tool:

- 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 event and fax attributes.

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 the SIP connection. 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).

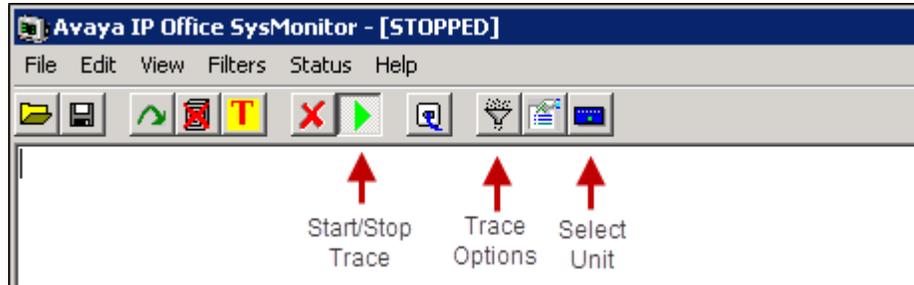
Channel Number	URI Group	Call Ref	Current State	Time In State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Cal
1			Idle	1 day 12:16:04					
2			Idle	1 day 12:16:04					
3			Idle	1 day 12:16:04					
4			Idle	1 day 12:16:04					
5			Idle	1 day 12:16:04					
6			Idle	1 day 12:16:04					
7			Idle	1 day 12:16:04					
8			Idle	1 day 12:16:04					
9			Idle	1 day 12:16:04					
10			Idle	1 day 12:16:04					

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

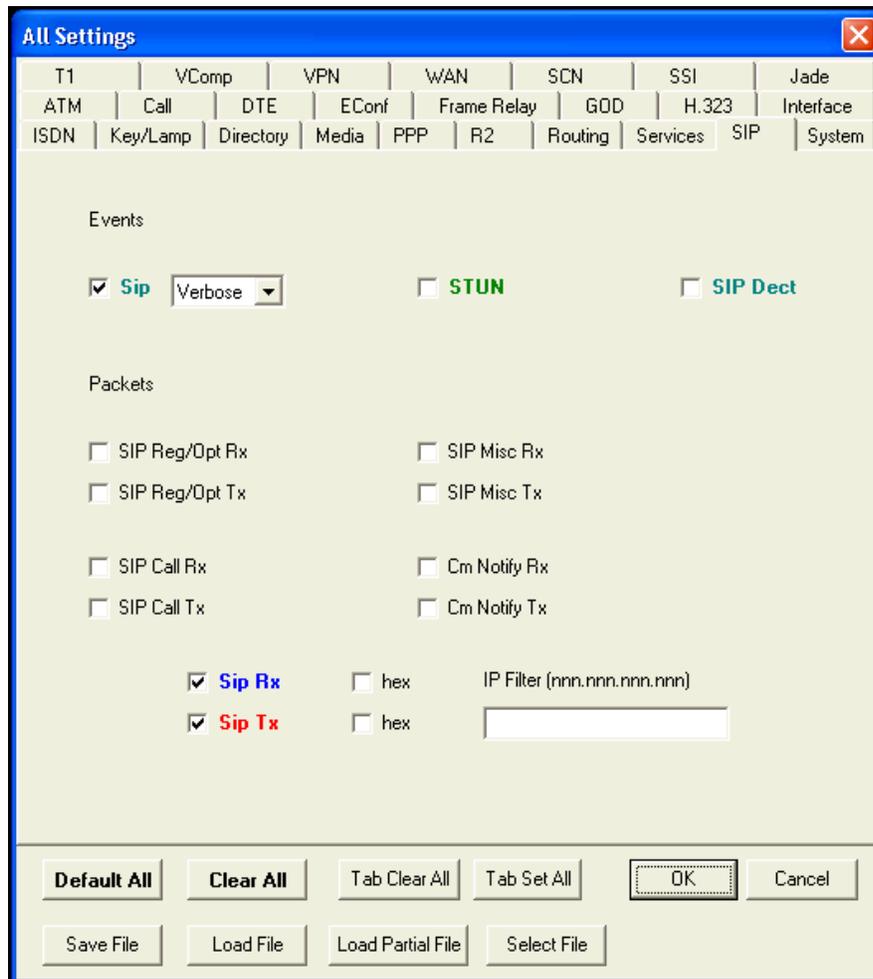
The screenshot shows the Avaya IP Office System Status web interface. The top left features the Avaya logo and a navigation menu with options: System, Alarms (9), Extensions (24), Trunks (3), Line: 1, Line: 2, Line: 17, Active Calls, Resources, Voicemail, IP Networking, and Locations. The top right displays 'IP Office System Status'. Below the navigation menu, there are tabs for 'Status', 'Utilization Summary', and 'Alarms'. The 'Alarms' tab is active, showing a header 'Alarms for Line: 17 SIP sip://172.16.5.71'. Below this header is a table with columns for 'Last Date Of Error', 'Occurrences', and 'Error Description'. The table is currently empty, indicating no active alarms.

8.4 IP Office Monitor

The 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 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

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

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

The screenshot shows the Avaya Session Border Controller for Enterprise dashboard. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the AVAYA logo. A left sidebar lists various management sections like Administration, System Management, and Device Specific Settings. The main content area is titled "Dashboard" and contains several panels: "Information" with system details, "Installed Devices" showing "Avaya SBCE", "Alarms (past 24 hours)" with "None found.", "Incidents (past 24 hours)" with five entries of "Avaya SBCE: No Server Flow Matched for Incoming Message", and "Notes" with "No notes found."

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

The screenshot shows the Avaya Alarm Viewer page. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Alarm Viewer" and the AVAYA logo. A left sidebar lists "Devices" with "EMS" and "Avaya SBCE". The main content area is titled "Alarms" and contains a table with columns for ID, Details, State, Time, and Device. The table is empty, showing "No alarms found for this device." Below the table are "Clear Selected" and "Clear All" buttons.

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

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Dashboard

Information

System Time	02:23:30 PM GMT	Refresh
Version	6.2.1.Q18	
Build Date	Mon Jul 14 14:53:03 UTC 2014	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message

Add

Notes

No notes found.

Navigation Menu:

- Dashboard
- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - SIP Cluster
 - Domain Policies
 - TLS Management
 - Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - Signaling Forking
 - End Point Flows
 - Session Flows
 - Relay Services
 - SNMP
 - Syslog Management
 - Advanced Options
 - Troubleshooting

The following screen shows the Incident Viewer page.

Incident Viewer AVAYA

Device: Category:

Displaying results 0 to 0 out of 0.

Type	ID	Date	Time	Category	Device	Cause
No incidents found.						

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

The following screen shows the Diagnostics page.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', '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 and troubleshooting options, with 'Device Specific Settings' and 'Trace' highlighted. The main content area is titled 'Trace: Avaya SBCE' and features three tabs: 'Call Trace', 'Packet Capture', and 'Captures'. The 'Packet Capture' tab is active, showing a 'Packet Capture Configuration' form with the following fields:

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address <small>[IP, Port]</small>	All
Remote Address <small>*, * Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	Inc_to_IPO.pcap
<input type="button" value="Start Capture"/> <input type="button" value="Clear"/>	

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', 'Statistics', '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 'Troubleshooting' highlighted. The main content area is titled 'Trace: Avaya SBCE' and features three tabs: 'Call Trace', 'Packet Capture', and 'Captures'. The 'Captures' tab is active, showing a table with one entry: 'No_180_20140721045220.pcap', which is 622,592 bytes and was last modified on July 21, 2014 at 4:52:38 AM GMT. A 'Delete' link is provided for this entry. A 'Refresh' button is also present in the top right of the table area.

File Name	File Size (bytes)	Last Modified
No_180_20140721045220.pcap	622,592	July 21, 2014 4:52:38 AM GMT

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 9.0, Avaya Session Border Controller for Enterprise Rel. 6.2.1 and Charter Communications SIP Trunking Service, as shown in **Figure 1**.

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

10. References

- [1] *IP Office 9.0 Installing IP500/IP500 V2*, Document Number 15-601042.
<https://downloads.avaya.com/css/P8/documents/100174004>
- [2] *IP Office Manager Release 9.0*, Document Number 15-601011.
<https://downloads.avaya.com/css/P8/documents/100174478>
- [3] *Administering Avaya Flare® Experience for iPad devices and Windows*.
<https://downloads.avaya.com/css/P8/documents/100175132>
- [4] *IP Office System Status Application*, Document Number 15-601758.
<https://downloads.avaya.com/css/P8/documents/100150298>
- [5] *Avaya IP Office Knowledgebase*.
<http://marketingtools.avaya.com/knowledgebase>
- [6] *Installing Avaya Session Border Controller for Enterprise*.
<https://downloads.avaya.com/css/P8/documents/100168983>
- [7] *Administering Avaya Session Border Controller for Enterprise*.
<https://downloads.avaya.com/css/P8/documents/100168982>
- [8] *Avaya Session Border Controller for Enterprise Release Notes*.
<https://downloads.avaya.com/css/P8/documents/100170131>
- [9] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*.
<https://downloads.avaya.com/css/P8/documents/100177106>

Documentation for Avaya products may be found at <http://support.avaya.com>.

Product documentation for Charter Communications SIP Trunking Service is available from Charter Communications.

©2014 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.