



Application Notes for Configuring Avaya IP Office Release 10.0 and Avaya Session Border Controller for Enterprise Release 7.1 to support Charter Spectrum Enterprise SIP Trunking Service on legacy Charter Communications Platform - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 10.0 and Avaya Session Border Controller for Enterprise Release 7.1 to support Charter Spectrum Enterprise SIP Trunking Service on legacy Charter Communications Platform.

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.

The Charter Spectrum Enterprise SIP Trunking Service on legacy Charter Communications Platform provides PSTN access via a SIP Trunk between the enterprise and the legacy 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.

Legacy 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	5
2.2 Test Results.....	6
2.3 Support.....	6
3. Reference Configuration.....	6
4. Equipment and Software Validated	8
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 - VoIP Tab	15
5.3 IP Route	16
5.4 SIP Line	17
5.4.1 Importing a SIP Line Template.....	17
5.4.2 Creating a SIP Trunk from an XML Template	20
5.4.3 SIP Line - SIP Line Tab.....	22
5.4.4 SIP Line - Transport Tab	23
5.4.5 SIP Line - SIP URI Tab	24
5.4.6 SIP Line - VoIP Tab	25
5.4.7 SIP Line – SIP Advanced Tab	25
5.5 Extension.....	27
5.6 Users	29
5.7 Incoming Call Route	33
5.8 Outbound Call Routing.....	35
5.8.1 Short Codes and Automatic Route Selection.....	35
5.9 Save Configuration	38
6. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).....	39
6.1 Log in Avaya SBCE.....	39
6.2 Global Profiles	42
6.2.1 Server Interworking – Avaya-IPO	42
6.2.2 Server Interworking - SP-General.....	45
6.2.3 Server Configuration.....	48
6.2.4 Routing Profiles	54
6.2.5 Topology Hiding.....	57
6.3 Domain Policies.....	60
6.3.1 Application Rules.....	60
6.3.2 End Point Policy Groups.....	61
6.4 Device Specific Settings	65
6.4.1 Network Management.....	65
6.4.2 Media Interface	66
6.4.3 Signaling Interface	68
6.4.4 End Point Flows	71
7. Charter Spectrum Enterprise SIP Trunking Service Configuration on legacy Charter Communications Platform.....	75

8. Verification and Troubleshooting	76
8.1 Verification Steps.....	76
8.2 Protocol Traces	76
8.3 IP Office System Status	77
8.4 IP Office Monitor.....	80
8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)	81
9. Conclusion	86
10. References	86

1. Introduction

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

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500v2 Release 10.0 (hereafter referred to as IP Office), Avaya Session Border Controller for Enterprise Release 7.1 (hereafter referred to as Avaya SBCE), Avaya Communicator for Windows, Avaya Communicator for Web and Avaya Deskphones, including SIP, H.323, digital and analog.

For brevity, from this point forward, the “Charter Spectrum Enterprise SIP Trunking Service on legacy Charter Communications Platform ” will be referred to as the “Charter SIP Trunking Service”. The terms “service provider”, “Charter” or “Charter Communications” will be used interchangeably throughout these Application Notes, referring to the “legacy Charter Communications” company.

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

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

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by connecting IP Office and the Avaya SBCE to the Charter SIP Trunking Service via the public Internet, as depicted in **Figure 1**.

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

2.1 Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, digital and analog at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP Trunk from the service provider networks.
- Outgoing PSTN calls from Avaya endpoints including SIP, H.323, digital and analog telephone at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider networks.
- Incoming and outgoing PSTN calls to/from Avaya Communicator for Windows.
- Incoming and outgoing PSTN calls to/from Avaya Communicator for Web.
- Dialing plans including long distance, outbound toll-free, etc.
- Caller ID presentation and Caller ID restriction.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codec G.711MU (Charter supported audio codec).
- Proper response to no matching codecs.
- G.711 Fax Pass-through.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.

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

Items not supported or not tested included the following:

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

2.2 Test Results

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

- **G.711 Fax Pass-Through:** G.711 fax pass-through calls failed intermittently. Inbound fax calls from the PSTN to IP Office and outbound fax calls from IP Office to the PSTN failed intermittently. This issue is believed to be network related, thus this issue is not necessarily indicative of a limitation of the combined Avaya/Charter solutions. It's listed here simply as an observation.
- **Call Display on Transferred Calls to 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 number of the actual connected party but instead shows the number assigned to extension in IP Office that initiated the call transfer. 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.
- **Inbound calls to an unassigned enterprise extension:** IP Office sends a "404 Not Found" message to the Charter network when it receives calls to an unassigned extension, the user hears re-order instead of the common announcement informing the user that he/she has reached a non-working number, to please check the number and to try again. This issue is considered non service affecting.

2.3 Support

For support on Charter Spectrum Enterprise SIP Trunking Service visit the corporate Web page at: <https://business.spectrum.com/content/sip-trunking> or call 888-692-8635.

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

3. Reference Configuration

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

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

- Avaya IP Office 500v2.
- Avaya IP Office Voicemail Pro.
- Avaya Session Border Controller for Enterprise.
- Avaya IP Office Application Server.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 1100 Series SIP IP Deskphones.
- Avaya Communicator for Windows.
- Avaya Communicator for Web.
- Avaya 1408 Digital Telephones.
- Avaya 9508 Digital Telephones.

In the reference configuration, a Modular Access Router was required at the simulated enterprise site, acting as a SIP interface between the Avaya simulated enterprise and the Charter's network. Charter will install the Modular Access Router at the customer premises (enterprise site). Charter will perform the initial configuration and maintenance as required. The Modular Access Router will be considered Customer Premises Equipment (CPE).

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

Also located at the enterprise site is Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codecs. The IP Office **LAN1** port was connected to the enterprise private network (LAN).

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

Outbound calls to the PSTN were first processed by IP Office. Once IP Office selected the proper SIP trunk; the call was routed to the Avaya SBCE, to the Charter Modular Access Router, across the public Internet, to Charter's network.

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

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

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

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

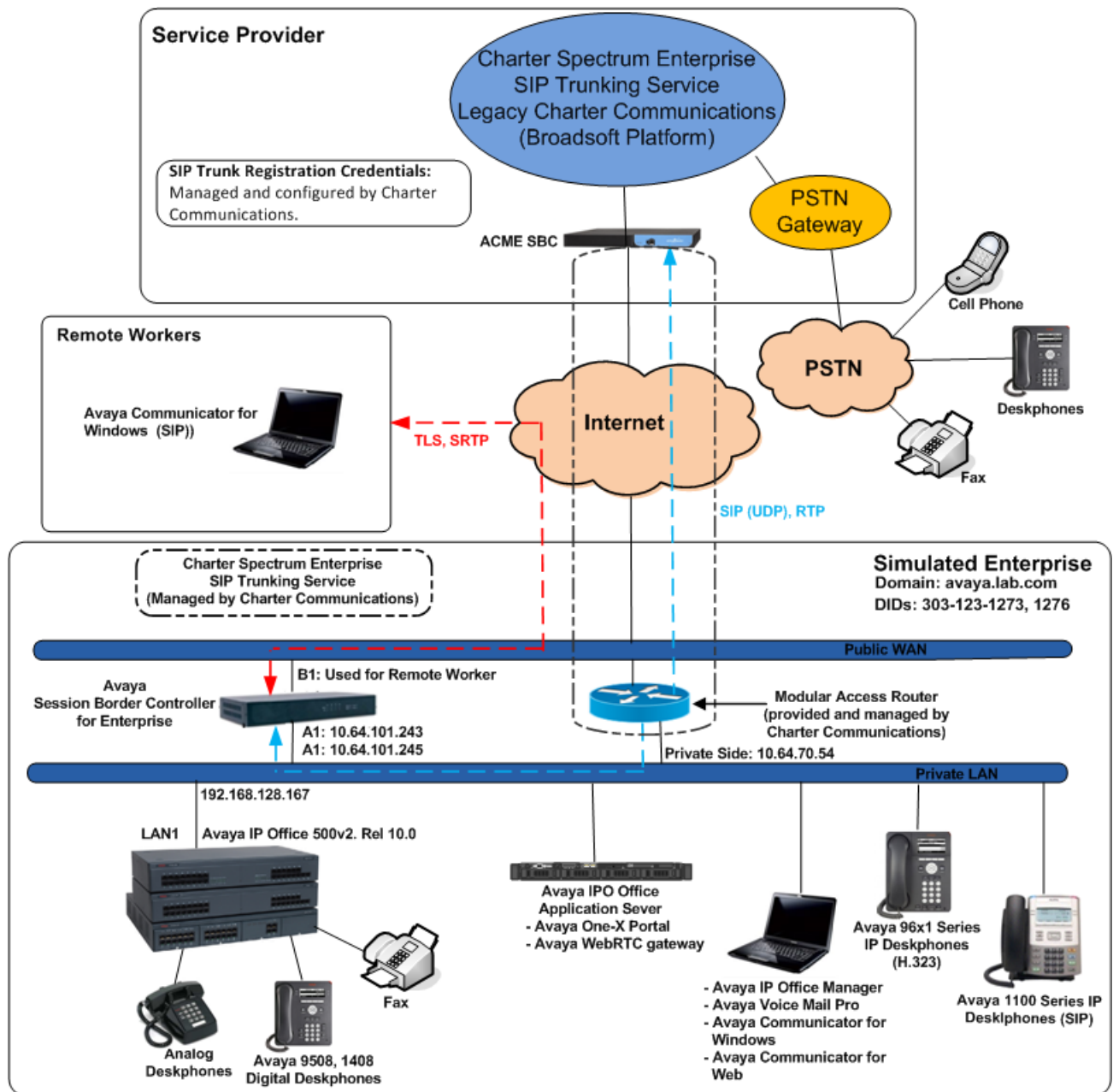


Figure 1: Avaya Interoperability Test Lab Configuration.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	10.0.0.2.0 Build 10
Avaya IP Office DIG DCPx16 V2	10.0.0.2.0 Build 10
Avaya IP Office Manager	10.0.0.2.0 Build 10
Avaya Voicemail Pro Client	10.0.0.2.0 Build 29
Avaya IP Office Application Server	10.0.0.1.0 Built 53
- Avaya WebRTC Gateway	10.0.0.1.0 Built 3
- Avaya one-X Portal for IP Office	10.0.0.1.0 Built 16
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.1.0.1-07-12368
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6302
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya Communicator for Windows	2.1.3.237
Avaya Communicator for Web	1.0.16.1718
Avaya Digital Deskphones 1408	R46
Avaya Digital Deskphones 9508	R59
Lucent Analog Phone	--
Charter Communications	
Broadworks Broadsoft Application Server	AS_Rel_17.sp4_1.197
Acme Net-Net 4500 Series SBC	SCX6.2.0 MR-9 GA (Build 1014)
Adtran NetVanta 3430 Modular Access Router	R11.4.6.V

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

5. Configure IP Office

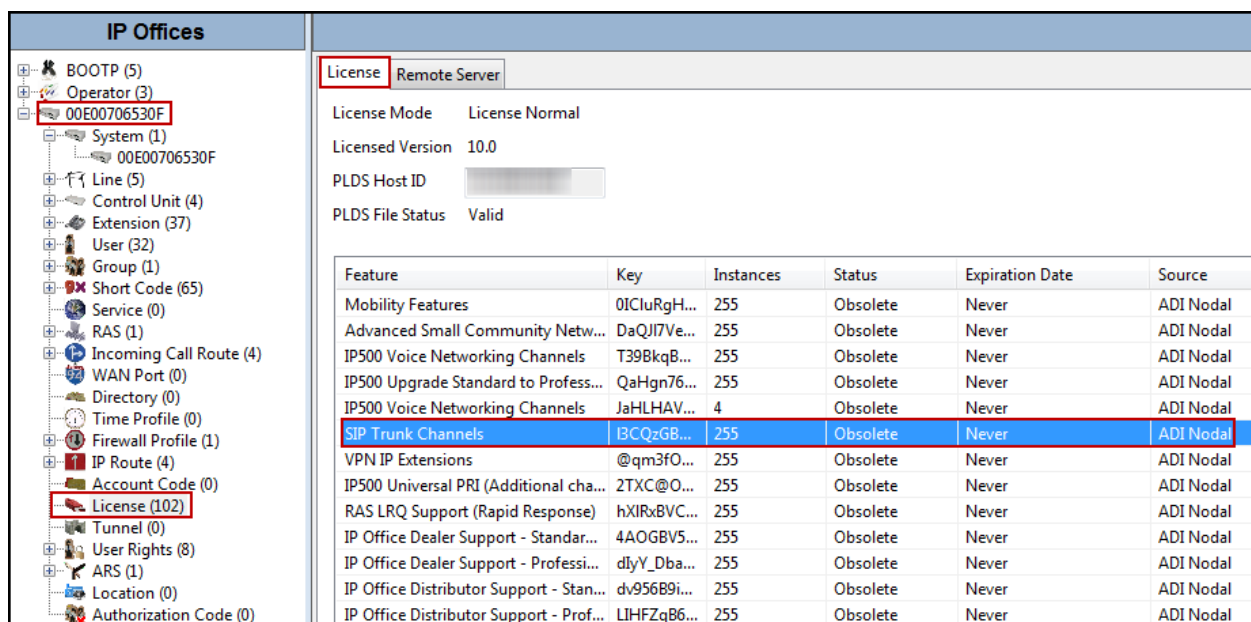
This section describes the IP Office configuration required to interwork with Charter SIP Trunking Service. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager.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

These Application Notes assume the basic installation and configuration of IP Office have already been completed and are not discussed here. For further information on IP Office, please consult References in **Section 10**.

5.1 Licensing

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

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



Feature	Key	Instances	Status	Expiration Date	Source
Mobility Features	0ICluRgH...	255	Obsolete	Never	ADI Nodal
Advanced Small Community Netw...	DaQJl7Ve...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	T39BkqB...	255	Obsolete	Never	ADI Nodal
IP500 Upgrade Standard to Profess...	QaHgn76...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	JaHLHAV...	4	Obsolete	Never	ADI Nodal
SIP Trunk Channels	BCQzGB...	255	Obsolete	Never	ADI Nodal
VPN IP Extensions	@qm3fO...	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional cha...	2TXC@O...	255	Obsolete	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	hXlRxBVC...	255	Obsolete	Never	ADI Nodal
IP Office Dealer Support - Standar...	4A0GBV5...	255	Obsolete	Never	ADI Nodal
IP Office Dealer Support - Professi...	dlyY_Dba...	255	Obsolete	Never	ADI Nodal
IP Office Distributor Support - Stan...	dv956B9i...	255	Obsolete	Never	ADI Nodal
IP Office Distributor Support - Prof...	LIHFZqB6...	255	Obsolete	Never	ADI Nodal

5.2 System

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

5.2.1 System - LAN1 Tab

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, showing a tree structure with 'System (1)' expanded to '00E00706530F'. On the right is the 'Details' pane for system '00E00706530F'. The 'LAN1' tab is selected, and within it, the 'LAN Settings' sub-tab is active. The 'IP Address' is set to '192 . 168 . 128 . 167' and the 'IP Mask' is set to '255 . 255 . 255 . 0'. Other settings include 'Primary Trans. IP Address' as '0 . 0 . 0 . 0', 'RIP Mode' as 'None', 'Enable NAT' as an unchecked checkbox, 'Number Of DHCP IP Addresses' as '200', and 'DHCP Mode' with 'Disabled' selected. An 'Advanced' button is located at the bottom right of the settings area.

00E00706530F							
System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events
LAN Settings		VoIP	Network Topology				
IP Address	192 . 168 . 128 . 167						
IP Mask	255 . 255 . 255 . 0						
Primary Trans. IP Address	0 . 0 . 0 . 0						
RIP Mode	None						
<input type="checkbox"/> Enable NAT							
Number Of DHCP IP Addresses	200						
DHCP Mode							
<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dial In <input checked="" type="radio"/> Disabled							
<button>Advanced</button>							

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

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- 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-RTCP**, **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).

IP Offices

- BOOTP (5)
- Operator (3)
- 00E00706530F
- System (1) **00E00706530F**
- Line (5)
- Control Unit (4)
- Extension (37)
- User (32)
- Group (1)
- Short Code (65)
- Service (0)
- RAS (1)
- Incoming Call Route (4)
- WAN Port (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)
- IP Route (4)
- Account Code (0)
- License (102)
- Tunnel (0)
- User Rights (8)
- ARS (1)
- Location (0)
- Authorization Code (0)

00E00706530F

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

LAN Settings **VoIP** Network Topology

☒ **H.323 Gatekeeper Enable**

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

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

☒ **SIP Trunks Enable**

☒ **SIP Registrar Enable**

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

SIP Domain Name **avaya.lab.com**

SIP Registrar FQDN

Layer 4 Protocol ☒ UDP UDP Port 5060 Remote UDP Port 5060

☒ TCP TCP Port 5060 Remote TCP Port 5060

☒ TLS TLS Port 5061 Remote TLS Port 5061

Challenge Expiration Time (sec) 10

RTP

Port Number Range

Minimum 49152 Maximum 53246

Port Number Range (NAT)

Minimum 49152 Maximum 53246

☒ Enable RTCP Monitoring on Port 5005

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

Keepalives

Scope RTP-RTCP Periodic timeout 30

Initial keepalives Enabled

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

- Select the **Firewall/NAT Type** from the pull-down menu to the option that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even though the default STUN settings are populated, they will not be used.
- Set the **Binding Refresh Time (seconds)** to a desired value. The value of **300 (or every 5 minutes)** was used during the compliance testing. This value is used to determine the **frequency** that IP Office will send OPTIONS heartbeats to the service provider.
- Set the **Public IP Address** to the IP address assigned under the LAN Settings tab, e.g., **192.168.128.167**
- 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. On the left is a tree view under 'IP Offices' with 'System (1)' selected. The main window shows the '00E00706530F' configuration for 'LAN1'. The 'Network Topology' tab is active, showing the following settings:

- STUN Server Address: 69.90.168.13
- STUN Port: 3478
- Firewall/NAT Type: Open Internet
- Binding Refresh Time (sec): 300
- Public IP Address: 192 . 168 . 128 . 167
- 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.

5.2.2 System - Telephony Tab

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

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

The screenshot displays the Avaya System Manager interface for configuring a system (00E00706530F). The left-hand pane shows a tree view of system components, with 'System (1)' selected. The main pane shows the 'Telephony' configuration tab, which is highlighted with a red box. The 'Telephony' tab contains several sub-sections: 'Analogue Extensions', 'Dial Delay Time', 'Dial Delay Count', 'Default No Answer Time', 'Hold Timeout', 'Park Timeout', 'Ring Delay', 'Call Priority Promotion Time', 'Default Currency', 'Default Name Priority', 'Media Connection Preservation', 'Phone Failback', 'Login Code Complexity', and 'Companding Law'. The 'Companding Law' section is highlighted with a red box, showing 'U-Law' selected for both 'Switch' and 'Line'. The 'Inhibit Off-Switch Forward/Transfer' checkbox is also highlighted with a red box and is unchecked. Other settings like 'DSS Status', 'Auto Hold', 'Dial By Name', 'Show Account Code', 'Restrict Network Interconnect', 'Drop External Only Impromptu Conference', 'Visually Differentiate External Call', 'Unsupervised Analog Trunk Disconnect Handling', 'High Quality Conferencing', 'Digital/Analogue Auto Create User', 'Directory Overrides Barring', and 'Advertise Callee State To Internal Callers' are also visible.

5.2.3 System - VoIP Tab

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

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

The screenshot displays the IP Office configuration interface for the **System (1) 00E00706530F**. The **VoIP** tab is selected in the top navigation bar. The left navigation pane shows a tree view of system components, with **System (1) 00E00706530F** highlighted. The main configuration area shows the following settings:

- Ignore DTMF Mismatch For Phones:** ☐
- Allow Direct Media Within NAT Location:** ☐
- RFC2833 Default Payload:** 101
- Default Codec Selection:**
 - Available Codecs:**
 - ☒ G.711 ULAW 64K
 - ☒ G.711 ALAW 64K
 - ☒ G.722 64K
 - ☒ G.729(a) 8K CS-ACELP
 - ☒ G.723.1 6K3 MP-MLQ
 - Unused:** G.722 64K
 - Selected:**
 - G.711 ULAW 64K
 - G.711 ALAW 64K
 - G.729(a) 8K CS-ACELP
 - G.723.1 6K3 MP-MLQ

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

5.3 IP Route

In the reference configuration, the IP Office LAN1 interface and the private interface of the Avaya SBCE resided on different IP subnet, so an IP route was necessary. In an actual customer configuration, these two interfaces may be in the same IP subnets, and in that is the case an IP route would not have to be created.

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, which lists various system components. The 'IP Route' component is highlighted with a red box, and its configuration is shown in the main pane on the right. The main pane has a title bar with '0.0.0.0'. The 'IP Route' configuration table is as follows:

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

5.4 SIP Line

A SIP Line is needed to establish the SIP connection between 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 Avaya IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.4.1** and **5.4.2** to create the SIP Line from the template.

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

- IP addresses.
- SIP trunk Registration Credentials.
- SIP URI entries.
- Setting of the Use Network Topology Info field on the Transport tab.

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

Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.3** to **5.4.7**.

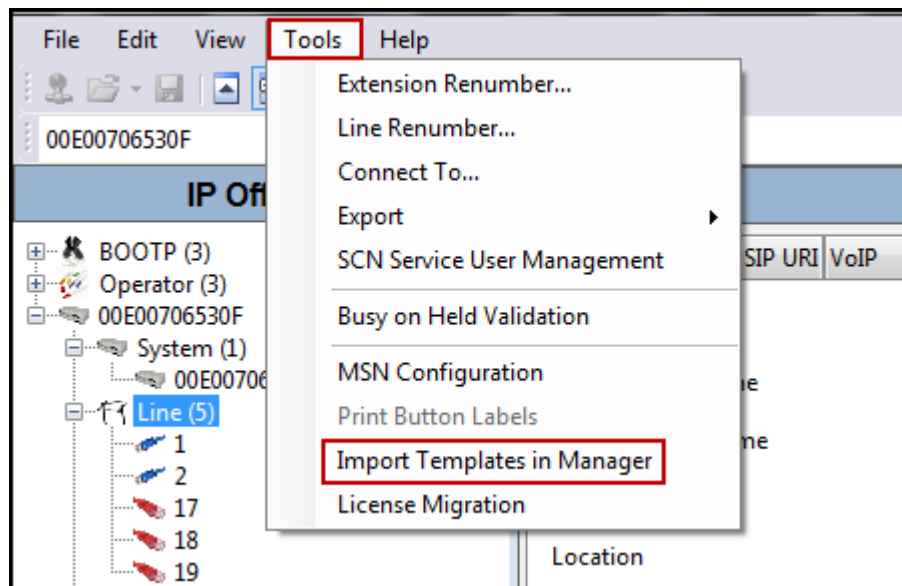
5.4.1 Importing a SIP Line Template

Note – DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500v2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

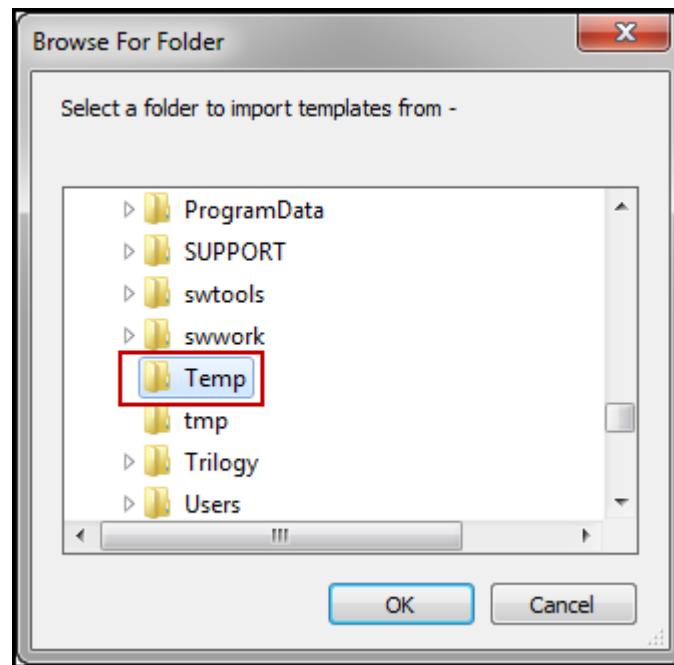
1. Copy a previously created template file to a location (e.g., C:\Temp) on the same computer where IP Office Manager is installed. By default, the template file name will have the format **<user supplied text>.xml**, where the **<user supplied text>** portion is entered during template file creation.

Note – If necessary, the **<user supplied text>** portion of the template file name may be modified, however the **<user supplied text>.xml** format of the file name must be maintained. For example, an original template file **Test.xml** could be changed to **Test1.xml**. The template file name is selected in **Section 5.4.2, step 1**, to create a new SIP Line.

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

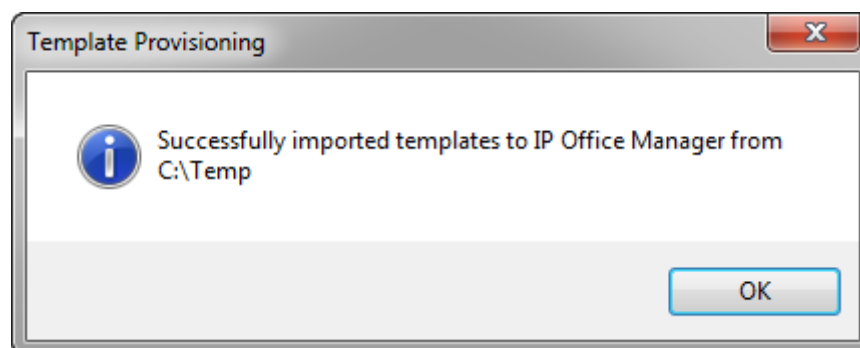


3. A folder browser will open. Select the directory used in **step 1** to store the template(s) (e.g., C:\Temp).



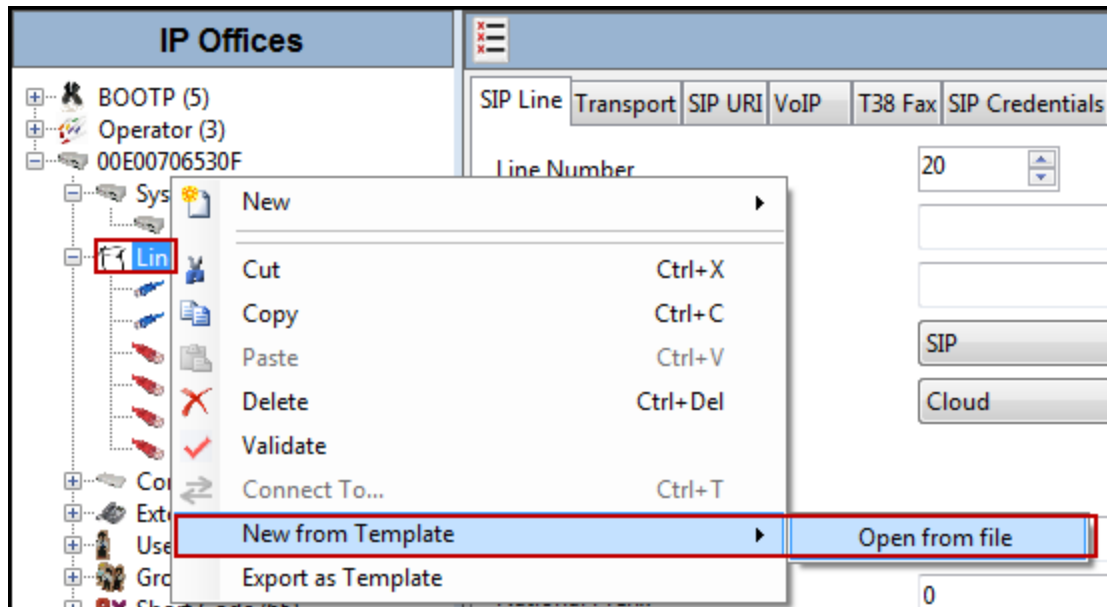
In the reference configuration, template files **CharterIPO10SBC.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.

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

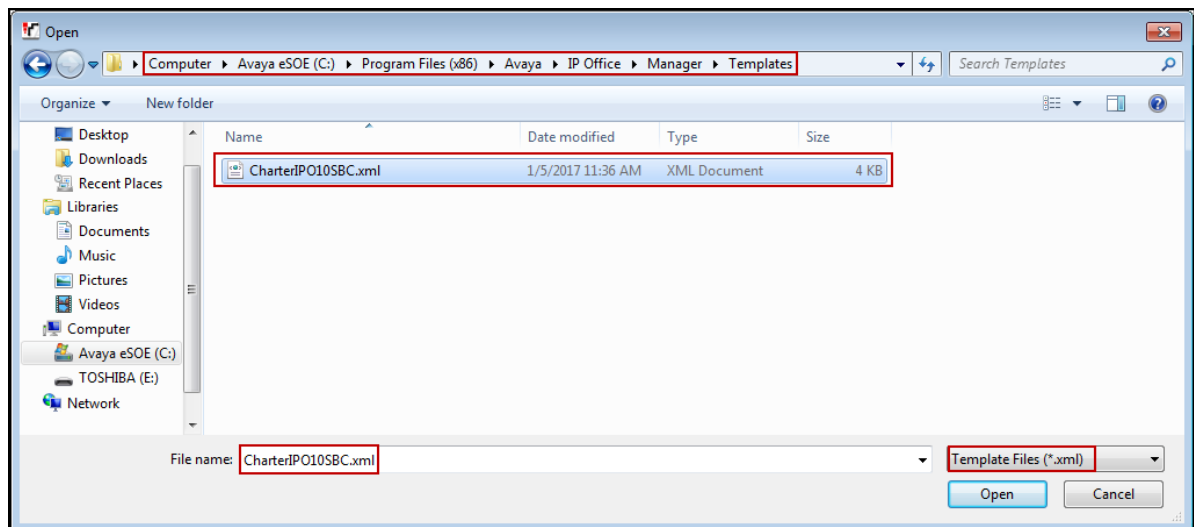


5.4.2 Creating a SIP Trunk from an XML Template

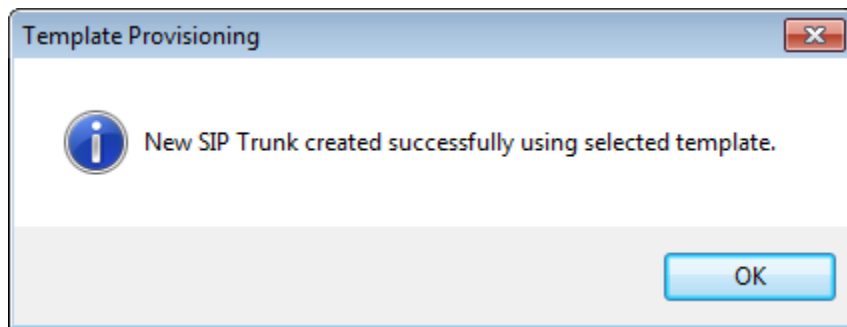
1. To create the SIP Trunk from a template, right-click on **Line** in the **Navigation** pane, and select **New from Template**→**Open from file**.



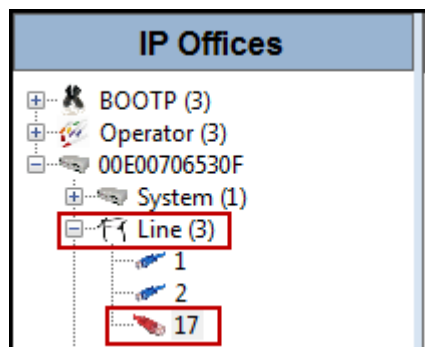
Navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates** (or **C:\Program Files (x86)\Avaya\IP Office\Manager\Templates**), on the bottom right hand side chose **Template Files (*.xml)** format and select the template, in this case **CharterIPO10SBC.xml** was selected.



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



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



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

5.4.3 SIP Line - SIP Line Tab

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

- Leave the **ITSP Domain Name** blank. Note that if this field is left blank, then IP Office inserts the ITSP Proxy Address from the Transport tab as the ITSP Domain in the SIP messaging.
- Verify that **URI Type** is set to **SIP**.
- Verify that **In Service** box is checked, which is the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by IP Office will use the Binding Refresh Time for LAN1, as shown in **Section 5.2.1**.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (seconds)** is set to **On Demand**.
- Under **Redirect and Transfer**, set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Never** (see **Section 2.1**).
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

The screenshot displays the 'SIP Line - Line 17' configuration window. The left pane shows the 'IP Offices' tree with 'Line 17' selected. The main pane has tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP Line' tab is active, showing fields for Line Number (17), ITSP Domain Name (blank), Local Domain Name, URI Type (SIP), Location (Cloud), Prefix, National Prefix, International Prefix, Country Code, Name Priority (System Default), and Description. On the right, there are checkboxes for 'In Service' and 'Check OOS', both checked. Below these are 'Session Timers' with 'Refresh Method' set to 'Auto' and 'Timer (sec)' set to 'On Demand'. At the bottom, the 'Redirect and Transfer' section shows 'Incoming Supervised REFER' and 'Outgoing Supervised REFER' both set to 'Never'.

5.4.4 SIP Line - Transport Tab

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

- Set the **ITSP Proxy Address** to the IP address of the inside interface (or private side) assigned to the Avaya SBCE, as shown on **Figure 1** (**Note:** On interface **A1** of the Avaya SBCE, IP address **10.64.101.243** was used to connect to IP Office, IP address **10.64.101.245** was used to connect to the Charter Modular Access Router, refer to **Section 6.4**).
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2.1**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy starting with 'BOOTP (5)', followed by 'Operator (3)', and then '00E00706530F'. Under this, 'System (1)' is listed, and within it, 'Line (5)' is selected, showing sub-items 1, 2, 17, 18, and 19. The main panel on the right is titled 'SIP Line - Line 17' and contains several tabs: 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'Transport' tab is active. It features a text field for 'ITSP Proxy Address' set to '10.64.101.243'. Below this is a 'Network Configuration' section with a dropdown for 'Layer 4 Protocol' set to 'UDP', a 'Send Port' field set to '5060', a dropdown for 'Use Network Topology Info' set to 'LAN1', and a 'Listen Port' field set to '5060'. Further down are fields for 'Explicit DNS Server(s)' (both set to '0 . 0 . 0 . 0') and a checked checkbox for 'Calls Route via Registrar'. At the bottom is a 'Separate Registrar' text field.

5.4.5 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 URI** 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 **Identity** under **Identity** to **Auto**.
- Set **Header** under **Identity** to **P Asserted ID**
- Set **Send Caller ID** under **Forwarding and Twinning** to **Diversion Header**.
- Set **Diversion Header** to **Auto**.
- 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 Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit (not shown).
- Click **OK** to commit again (not shown).

The screenshot displays the IP Office configuration interface for 'SIP Line - Line 17'. The left sidebar shows a tree view of system components, with 'Line 17' selected. The main window has tabs for 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'SIP URI' tab is active, showing a table of URI entries and a configuration form below.

URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID	Diversion Header	Credential	Max Calls
17 17		<Internal>	<Internal>	<Internal>	Auto	PAI		Diversion	Auto	0: <Non...	10

Edit URI

Local URI: Use Internal Data
Contact: Use Internal Data
Display Name: Use Internal Data

Identity

Identity: Auto
Header: P Asserted ID

Forwarding And Twinning

Originator Number:
Send Caller ID: Diversion Header

Diversion Header: Auto

Registration: 0: <None>

Incoming Group: 17
Outgoing Group: 17
Max Sessions: 10

5.4.6 SIP Line - VoIP Tab

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

- In the sample configuration, the **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown.
- Select **G.711** for **Fax Transport Support** (Refer to **Section 2.1** and **2.2**).
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- 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).

The screenshot displays the Avaya IP Office configuration window for 'SIP Line - Line 17'. The 'VoIP' tab is active, showing the following settings:

- Codec Selection:** Set to 'Custom'. The 'Unused' list contains G.711 ALAW 64K, G.722 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ. The 'Selected' list contains G.711 ULAW 64K.
- Fax Transport Support:** Set to 'G.711'.
- DTMF Support:** Set to 'RFC2833'.
- Media Security:** Set to 'Disabled'.
- Checkboxes:** 'Re-invite Supported' and 'PRACK/100rel Supported' are checked. Other options like 'VoIP Silence Suppression', 'Local Hold Music', 'Codec Lockdown', 'Allow Direct Media Path', 'Force direct media with phones', and 'G.711 Fax ECAN' are unchecked.

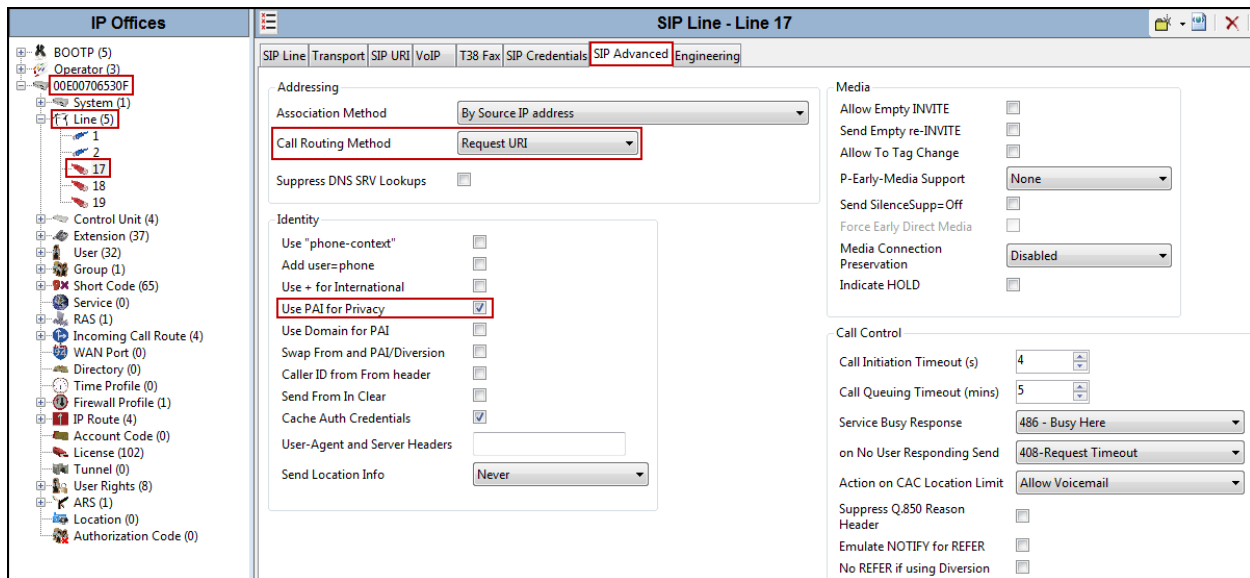
Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.3** (System – VoIP tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

5.4.7 SIP Line – SIP Advanced Tab

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

purposes. By default, IP Office will use the PPI header for privacy. To configure IP Office to use the PAI header for privacy calls:

- Verify the **Call Routing Method** is set to **Request URI**.
- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



5.5 Extension

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

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

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows a hierarchy: BOOTP (5), Operator (3), 00E00706530F, System (1), Line (5), Control Unit (4), and Extension (37). The 'Extension (37)' folder is expanded, showing a list of extensions. The extension '8003 3040' is highlighted with a red box. The main panel on the right is titled 'H.323 Extension: 8003 3040' and contains configuration fields for the selected extension. The 'Extension' tab is selected, and a red box highlights the 'Extension' label in the tab bar. The configuration fields include:

Field	Value
Extension ID	8003
Base Extension	3040
Phone Password	
Confirm Phone Password	
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Avaya 9641
Location	Automatic
Fallback As Remote Worker	Auto
Module	0
Port	0
Disable Speakerphone	<input type="checkbox"/>

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

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

IP Offices

- BOOTP (5)
- Operator (3)
- 00E00706530F
- System (1)
- Line (5)
- Control Unit (4)
- Extension (37)
 - 8012 1502
 - 8011 1540
 - 8010 1542
 - 8003 3040
 - 8002 3041
 - 8008 3042
 - 101 3043
 - 102 3044
 - 8000 3047
 - 25 3049
 - 8001 3050
 - 8009 3055
 - 26 4002
 - 27 4003
 - 28 4004
 - 29 4005
 - 30 4006
 - 31 4007
 - 32 4008
 - 103 4011
 - 104 4012
 - 105 4013
 - 106 4014
 - 107 4015
 - 108 4016

H.323 Extension: 8003 3040

Extension **VoIP**

IP Address: 0 . 0 . 0 . 0

MAC Address: 00 00 00 00 00 00

Codec Selection: System Default

Unused: G.722 64K

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

Reserve License: None

TDM->IP Gain: Default

IP->TDM Gain: Default

Supplementary Services: None

Media Security: Same as System (Disabled)

☐ VoIP Silence Suppression

☐ Enable Faststart for non-Avaya IP phones

☒ Out Of Band DTMF

☐ Local Tones

☒ Allow Direct Media Path

5.6 Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first navigate to **User** in the left **Navigation** pane, and then select the name of the user to be modified. In the example below, the name of the user is **Ext3040 H323**.

The screenshot displays the Avaya IP Office Manager application window. The title bar indicates the version is 10.0.0.2.0 build 10, running as Administrator. The interface is divided into a left navigation pane and a main configuration area.

Left Navigation Pane: Shows a tree structure of IP Offices. The 'User' folder is expanded, and the user '3040 Ext3040 H323' is selected and highlighted with a red box.

Main Configuration Area: The title is 'Ext3040 H323: 3040'. Below the title is a tabbed interface with the 'User' tab selected. The configuration fields are as follows:

- Name:** Ext3040 H323
- Password:** [Redacted]
- Confirm Password:** [Redacted]
- Unique Identity:** [Redacted]
- Conference PIN:** [Redacted]
- Confirm Audio Conference PIN:** [Redacted]
- Account Status:** Enabled (dropdown)
- Full Name:** Ext3040 H323
- Extension:** 3040
- Email Address:** [Redacted]
- Locale:** [Redacted]
- Priority:** 5 (dropdown)
- System Phone Rights:** None (dropdown)
- Profile:** Basic User (dropdown)
 - ☐ Receptionist
 - ☐ Enable Softphone
 - ☐ Enable one-X Portal Services
 - ☐ Enable one-X TeleCommuter
 - ☒ Enable Remote Worker
 - ☒ Enable Communicator
 - ☐ Enable Mobile VoIP Client
 - ☐ Send Mobility Email
 - ☐ Web Collaboration
- ☐ Exclude From Directory
- Device Type:** Avaya 9641 (with a phone icon)

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

The screenshot displays the Avaya User Management Interface. On the left, a tree view under 'IP Offices' shows the hierarchy: BOOTP (5), Operator (3), System (1), Line (5), Control Unit (4), Extension (37), and User (32). The 'User (32)' folder is expanded, and '3047 Ext3047 SIP' is selected. The main panel on the right is titled 'Ext3047 SIP: 3047' and contains several tabs: User, Voicemail, DND, Short Codes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, and Button Programming. The 'User' tab is active. It contains the following fields and options:

- Name: Ext3047 SIP
- Password: [Redacted]
- Confirm Password: [Redacted]
- Unique Identity: [Empty]
- Conference PIN: [Empty]
- Confirm Audio Conference PIN: [Empty]
- Account Status: Enabled (dropdown)
- Full Name: Softclient 3047
- Extension: 3047
- Email Address: [Empty]
- Locale: [Empty]
- Priority: 5 (dropdown)
- System Phone Rights: None (dropdown)
- Profile: Power User (dropdown)
- ☐ Receptionist
- ☒ Enable Softphone
- ☒ Enable one-X Portal Services
- ☒ Enable one-X TeleCommuter
- ☐ Enable Remote Worker
- ☒ Enable Communicator
- ☒ Enable Mobile VoIP Client
- ☐ Send Mobility Email
- ☐ Web Collaboration
- ☐ Exclude From Directory
- Device Type: [Icon of a phone] Unknown SIP device

Select the **Voicemail** tab. The following screen shows the **Voicemail** tab for the user with extension 3040. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application Notes, incoming calls from Charter to this user were redirected to Voicemail Pro after no answer. Voicemail messages were recorded and retrieved successfully. Voice mail navigation and retrieval were performed locally and from PSTN telephones to test DTMF using RFC 2833.

Select the **Mobility** tab. In the sample configuration user 3040 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for user 3040. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned telephone, including the dial access code “9”, in this case **917864571234**. Other options can be set according to customer requirements.

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

Button ...	Label	Action	Action Data
1		Appearance	a=
2		Appearance	b=
3		Appearance	c=
4		Twining	
5			
6			
7			
8			

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 5.4.5**). The example below shows the settings for user “Ext3040 H323”. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Charter. In the example, DID number **3031231273** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

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

Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership	Announcements	SIP
<div> <div>SIP Name</div> <div>3031231273</div> </div> <div> <div>SIP Display Name (Alias)</div> <div>Ext3040 H323</div> </div> <div> <div>Contact</div> <div>3031231273</div> </div> <div> <input type="checkbox"/> Anonymous </div>							

5.7 Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system.

In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** and **SIP URI** (Section 5.4.5) and the users **SIP Name** and **Contact**, already populated with the DID numbers assigned by Charter (Section 5.6).

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

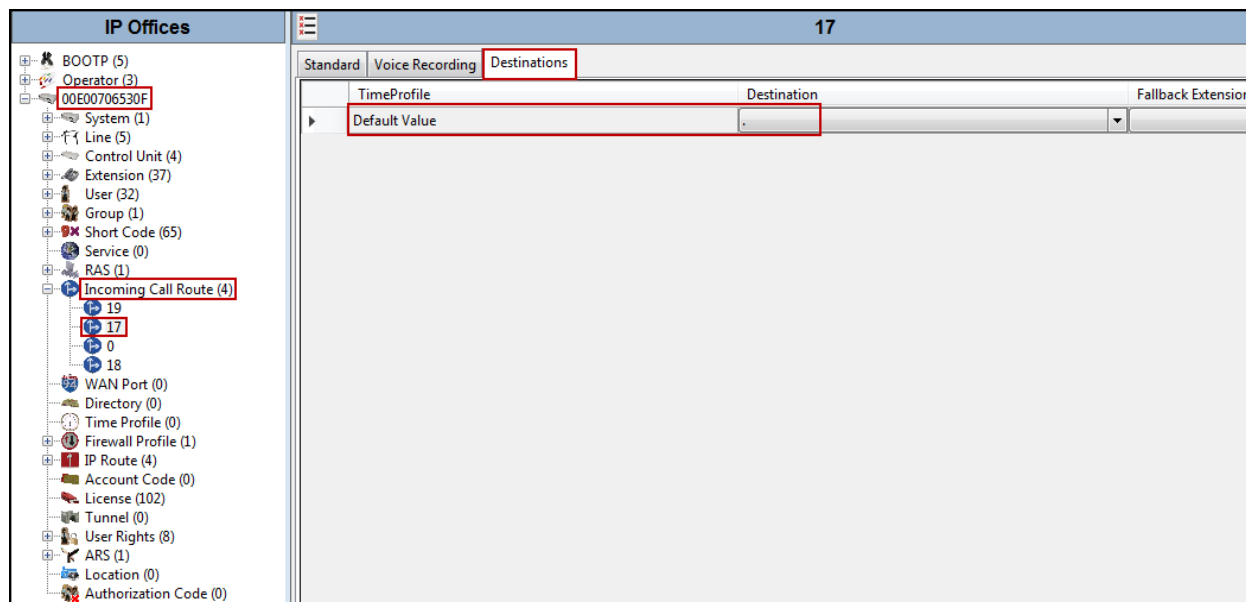
On the **Details** pane (not shown), under the **Standard** tab, set the parameters as show below:

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

The screenshot displays the IP Office configuration interface. On the left, the **Navigation** pane shows a tree structure under **IP Offices**. The **Incoming Call Route (4)** folder is expanded, and the route with ID **17** is selected. On the right, the **Details** pane is shown with the **Standard** tab active. The configuration parameters for route 17 are as follows:

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** (not shown). 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 17** which is configurable via ARS.

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **9N** was used (note that the semi-colon is not used here).
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group ID** to **50: Main** to be directed to **Line Group 17**, which is configurable via ARS.
- Click the **OK** to commit (not shown).

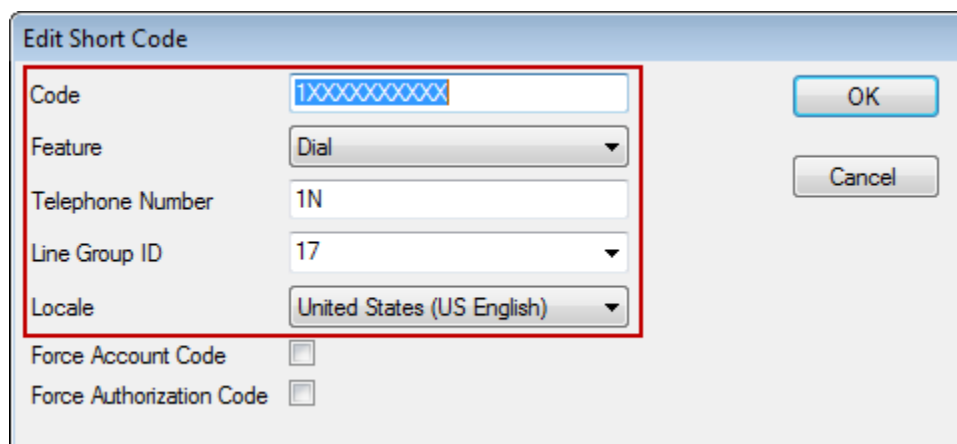
The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' navigation pane lists various short codes, with '9N' highlighted in blue. The main configuration area on the right is titled '9N: Dial' and contains a 'Short Code' section. This section includes the following fields:

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

The following screen shows a sample ARS configuration for the route **50: Main**. Note the sequence of **X**'s used in the **Code** field of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

To create a short code to be used for ARS, select **ARS → 50: Main** on the **Navigation** pane and click **Add** (not shown).

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



The screenshot shows the 'Edit Short Code' dialog box. The 'Code' field is highlighted with a red box and contains the text '1XXXXXXXXXX'. The 'Feature' dropdown is set to 'Dial'. The 'Telephone Number' field contains '1N'. The 'Line Group ID' dropdown is set to '17'. The 'Locale' dropdown is set to 'United States (US English)'. There are two checkboxes at the bottom: 'Force Account Code' and 'Force Authorization Code', both of which are unchecked. On the right side of the dialog, there are two buttons: 'OK' and 'Cancel'.

The following screenshot shows the ARS dial pattern entry after it was added.

IP Offices

- BOOTP (5)
- Operator (3)
- 00E00706530F
- System (1)
- Line (5)
- Control Unit (4)
- Extension (37)
- User (32)
- Group (1)
- Short Code (65)
- Service (0)
- RAS (1)
- Incoming Call Route (4)
- WAN Port (0)
- Directory (0)
- Time Profile (0)
- Firewall Profile (1)
- IP Route (4)
- Account Code (0)
- License (102)
- Tunnel (0)
- User Rights (8)
- ARS (1)
- 50: Main
- Location (0)
- Authorization Code (0)

Main

ARS

ARS Route ID: 50

Route Name: Main

Dial Delay Time: System Default (3)

Description:

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

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

Code	Telephone Number	Feature	Line Group ID
8XXXXXXXXX	8N	Dial	17
1XXXXXXXXX	1N	Dial	17
6XXXXXX	6N	Dial	17
3XXXXXXXXX	3N	Dial	17
28XXXXXX	28N	Dial	17
55XXXXXXXX	55N	Dial	17
01XXXXXXXXXXXX	01N	Dial	17

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

Alternate Route: <None>

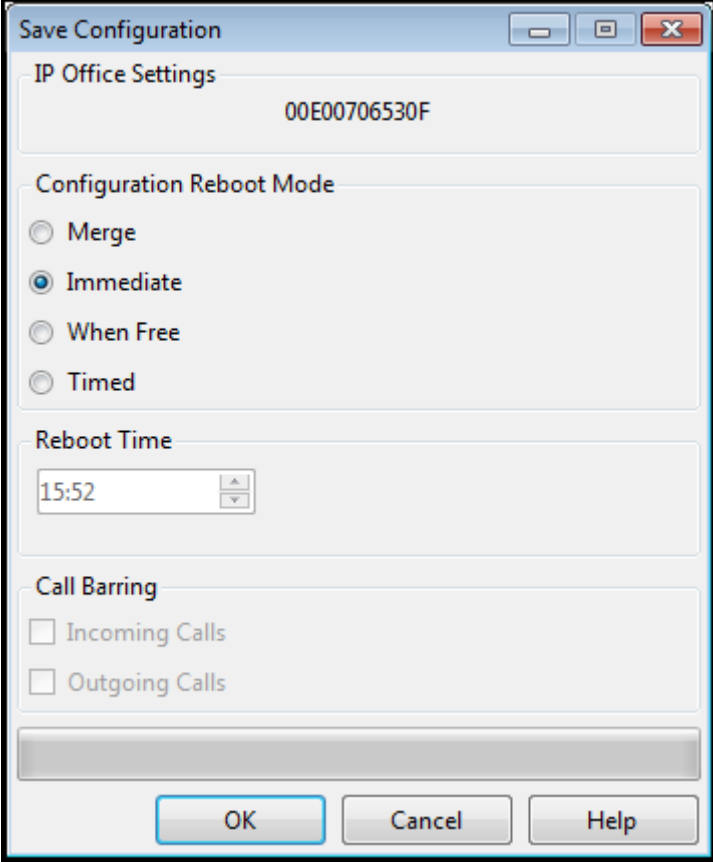
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

5.9 Save Configuration

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

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

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



The image shows a 'Save Configuration' dialog box with a title bar containing minimize, maximize, and close buttons. The dialog is divided into several sections: 'IP Office Settings' with a text field containing '00E00706530F'; 'Configuration Reboot Mode' with four radio buttons ('Merge', 'Immediate', 'When Free', 'Timed'), where 'Immediate' is selected; 'Reboot Time' with a time selection field showing '15:52'; and 'Call Barring' with two unchecked checkboxes ('Incoming Calls', 'Outgoing Calls'). At the bottom, there is a horizontal bar and three buttons: 'OK', 'Cancel', and 'Help'.

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

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


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

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

6.1 Log in Avaya SBCE

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

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



AVAYA

Log In

Username:

Password:

**Session Border Controller
for Enterprise**

WELCOME TO AVAYA SBC

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

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

© 2011 - 2016 Avaya Inc. All rights reserved.

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

Session Border Controller for Enterprise AVAYA

Alarms **2** Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Dashboard

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

Information

System Time	12:10:01 PM EST	Refresh
Version	7.1.0.1-07-12368	
Build Date	Fri Nov 11 09:21:54 EST 2016	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	01/06/2017 12:06:58 EST	
Failed Login Attempts	0	

Installed Devices

EMS
Avaya_SBCE 2

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched

[Add](#)

Notes

No notes found.

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

Session Border Controller for Enterprise AVAYA

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

System Management

Devices Updates SSL VPN Licensing Key Bundles

Device Name	Management IP	Version	Status						
Avaya_SBCE		7.1.0.1-07-12368	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

The **System Information** window is displayed as shown below.

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

General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 2000	2000
Advanced Sessions Requested: 2000	2000
Scopia Video Sessions Requested: 500	500
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
Encryption	<input checked="" type="checkbox"/>

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.101.243	10.64.101.243	255.255.255.0	10.64.101.1	A1
				A1
10.64.101.245	10.64.101.245	255.255.255.0	10.64.101.1	A1
				B1
				B1
				B1

DNS Configuration

Primary DNS	75.75.75.75
Secondary DNS	75.75.75.76
DNS Location	DMZ
DNS Client IP	50.207.80.51

Management IP(s)

IP #1 (IPv4)	
--------------	--

On the previous screen, note that **A1** corresponds to the inside interface (Private Network side) and **B1** (with IP addresses blurred out) corresponds to the outside interface (Public Network side) of the Avaya SBCE. The IP address 10.64.101.243 assigned to the **A1** interface was used to access IP Office (IP address: 192.168.128.167) across the enterprise private network (LAN). The IP address 10.64.101.245 assigned to the **A1** interface was used to access the Charter Modular Access Router (IP address: 10.64.70.54) across the enterprise private network (LAN). In this solution, the **B1** interface was used for remote worker. The configuration required for Remote Worker is beyond the scope of these Application Notes and is not discussed here, thus IP addresses assigned to interface **B1** were blurred out. The management IP address was also blurred out for security reasons. (Use **Figure 1** as reference for IP address assignments).

IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled “M1”) of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

6.2 Global Profiles

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

6.2.1 Server Interworking – Avaya-IPO

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

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

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

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



The screenshot shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The dialog has two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'Avaya-IPO'. The 'Clone Name' field is highlighted with a red border. At the bottom center 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 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a tree view with categories like 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'Domain DoS', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Global Profiles' section is expanded, showing 'Server Interworking' as the selected profile. The main content area is titled 'Interworking Profiles: Avaya-IPO' and features an 'Add' button. Below this is a list of interworking profiles: 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General', 'Avaya-IPO' (highlighted), 'Avaya-CS1000', and 'Avaya-CM'. The 'Avaya-IPO' profile is selected, and its configuration is shown in the 'General' tab. The configuration table lists various SIP-related settings and their values.

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

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar contains a tree view with categories like 'Dashboard', 'Administration', 'System Management', and 'Global Profiles'. Under 'Global Profiles', 'Server Interworking' is highlighted. The main content area is titled 'Interworking Profiles: Avaya-IPO' and features a list of profiles on the left, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General', 'Avaya-IPO' (highlighted), 'Avaya-CS1000', and 'Avaya-CM'. An 'Add' button is located above this list. To the right, the 'Advanced' tab is selected, showing a table of configuration parameters. The table has two columns: the parameter name and its value. The parameters include 'Record Routes' (Both Sides), 'Include End Point IP for Context Lookup' (Yes), 'Extensions' (Avaya), 'Diversion Manipulation' (No), 'Has Remote SBC' (Yes), 'Route Response on Via Port' (No), 'Relay INVITE Replace for SIPREC' (No), and 'DTMF Support' (None). An 'Edit' button is at the bottom right of the table.

Click here to add a description.	
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
DTMF	
DTMF Support	None

6.2.2 Server Interworking - SP-General

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

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

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

- Click **Next**.



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

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

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar shows a tree view with 'Global Profiles' expanded, and 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button. Below this is a list of interworking profiles, with 'SP-General' highlighted. To the right, the 'General' tab is active, showing a table of configuration parameters.

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

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

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The top navigation bar includes links for Alarms (2), Incidents, Status, Logs, Diagnostics, and Users. The main heading is "Session Border Controller for Enterprise".

On the left, a sidebar menu lists various configuration categories, with "Global Profiles" expanded and "Server Interworking" selected. The main content area is titled "Interworking Profiles: SP-General" and features an "Add" button. Below this, a list of interworking profiles is shown, with "SP-General" highlighted. The "Advanced" tab is selected, displaying a table of configuration parameters.

Click here to add a description.					
General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes		Both Sides			
Include End Point IP for Context Lookup		No			
Extensions		None			
Diversion Manipulation		No			
Has Remote SBC		Yes			
Route Response on Via Port		No			
Relay INVITE Replace for SIPREC		No			
DTMF					
DTMF Support		None			

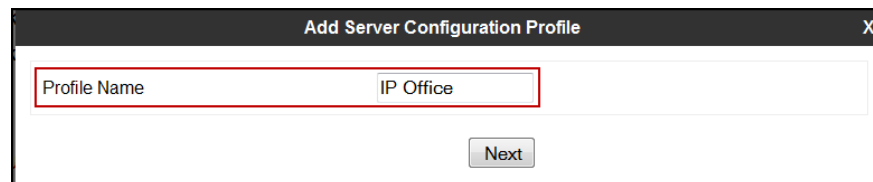
An "Edit" button is located at the bottom right of the configuration table.

6.2.3 Server Configuration

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

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

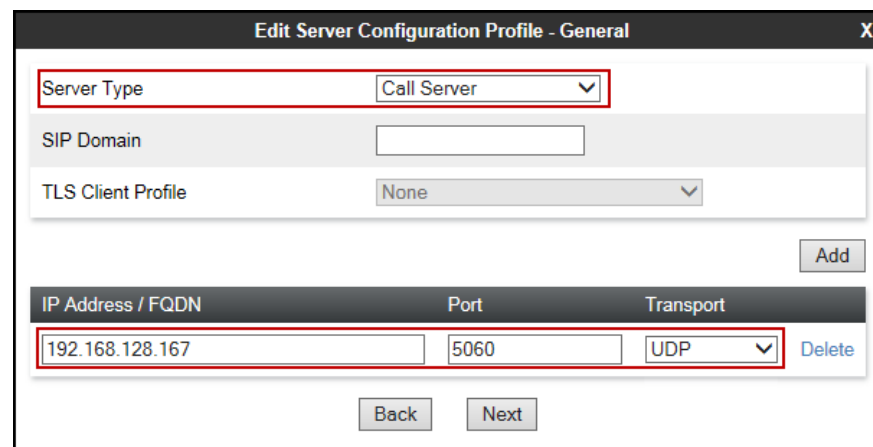
- Click **Next**.



The screenshot shows a window titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "IP Office". Below this field is a "Next" button.

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

- **Server Type:** Select **Call Server**.
- **IP Address / FQDN:** **192.168.128.167** (IP Address of IP Office).
- **Port:** **5060** (This port must match the port number defined in **Section 5.4.4**).
- **Transports:** Select **UDP**.
- Click **Next**.



The screenshot shows a window titled "Edit Server Configuration Profile - General" with a close button (X) in the top right corner. The window contains several fields: "Server Type" (a dropdown menu set to "Call Server"), "SIP Domain" (an empty text field), and "TLS Client Profile" (a dropdown menu set to "None"). Below these fields is an "Add" button. At the bottom, there is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row of the table has the values "192.168.128.167", "5060", and "UDP" (a dropdown menu). To the right of the table is a "Delete" button. Below the table are "Back" and "Next" buttons.

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

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

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

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

- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile **Avaya-IPO**

Signaling Manipulation Script **None**

Securable ☐

Enable FGDN ☐

TCP Failover Port 5060

TLS Failover Port 5061

Back **Finish**

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

Session Border Controller for Enterprise

Alarms 2 Incidents Status Logs Diagnostics Users Settings Help Log Out

Server Configuration: IP Office

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

Server Profiles
Com Manager
CS1000
Session Manager
Service Provider TLS
IP Office
Service Provider UDP

General Authentication Heartbeat Advanced

Server Type **Call Server**

TLS Client Profile

IP Address / FQDN	Port	Transport
192.168.128.167	5060	UDP

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 links for Alarms (2), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right.

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

The main content area is titled "Server Configuration: IP Office" and features an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a list of server profiles: Com Manager, CS1000, Session Manager, Service Provider TLS, IP Office (highlighted), and Service Provider UDP.

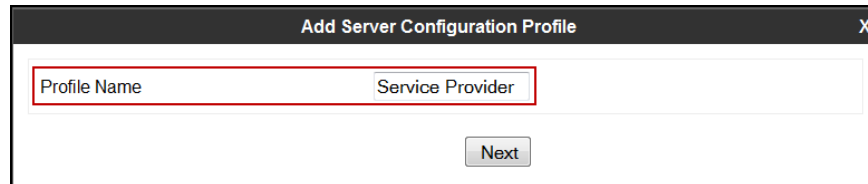
The "Advanced" tab is selected, showing the following configuration options:

Option	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya-IPO
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>

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

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

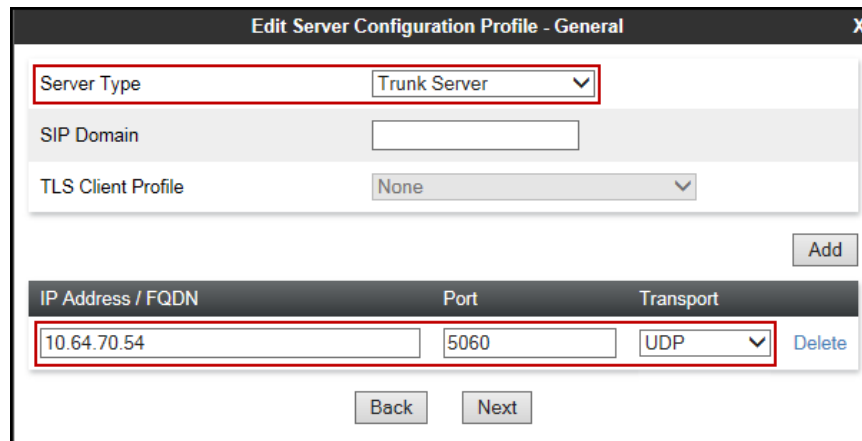
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has two input fields: "Profile Name" and "Service Provider". The "Profile Name" field contains the text "Service Provider". Below the fields is a "Next" button.

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

- **Server Type:** Select **Trunk Server**.
- **IP Address / FQDN:** **10.64.70.54** (Private IP Address of Charter's Modular Access Router).
- **Port:** **5060**.
- **Transports:** Select **UDP**.
- Click **Next**.



The screenshot shows a window titled "Edit Server Configuration Profile - General". It has several fields: "Server Type" (dropdown menu set to "Trunk Server"), "SIP Domain" (text field), "TLS Client Profile" (dropdown menu set to "None"), and a table for "IP Address / FQDN", "Port", and "Transport". The table has one row with values "10.64.70.54", "5060", and "UDP". There is an "Add" button and a "Delete" button. At the bottom are "Back" and "Next" buttons.

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

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

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

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

Signaling Manipulation Script None

Securable ☐

Enable FGDN ☐

TCP Failover Port 5060

TLS Failover Port 5061

Back Finish

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

Session Border Controller for Enterprise

Alarms 2 Incidents Status Logs Diagnostics Users Settings Help Log Out

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

Server Configuration: Service Provider UDP

Add Rename Clone Delete

General Authentication Heartbeat Advanced

Server Type Trunk Server

IP Address / FQDN	Port	Transport
10.64.70.54	5060	UDP

Edit

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

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes links for Alarms (2), Incidents, Status, Logs, Diagnostics, Users, and a dropdown menu. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration categories, with "Server Configuration" highlighted. The main content area is titled "Server Configuration: Service Provider UDP" and features an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this, a list of server profiles is shown, with "Service Provider U..." selected. The "Advanced" tab is active, displaying a table of configuration options:

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

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

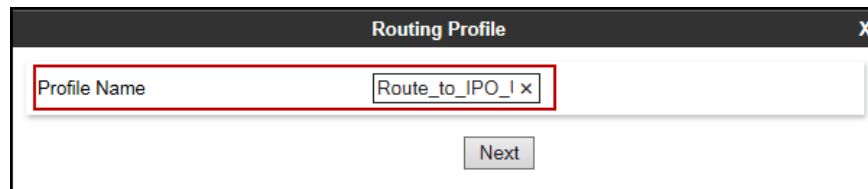
6.2.4 Routing Profiles

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

Two Routing profiles were created, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to Charter's Modular Access Router.

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

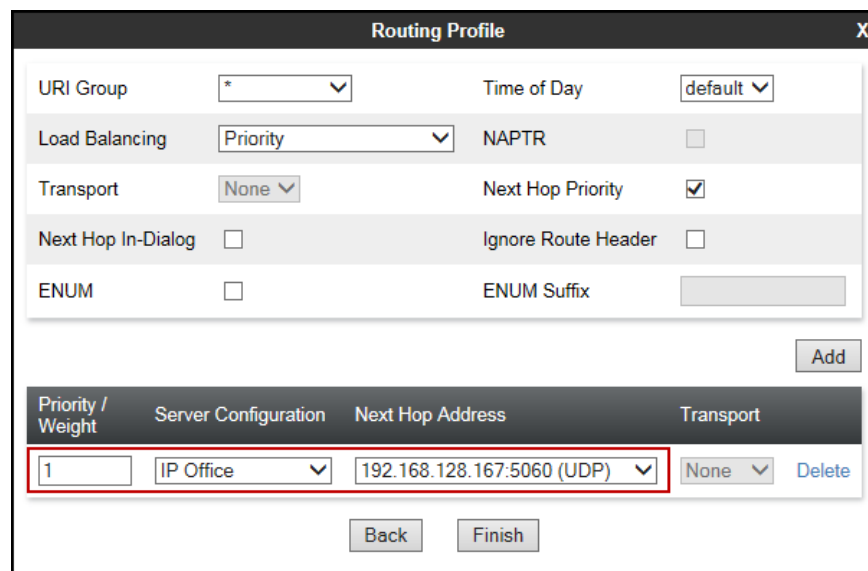
- Select **Routing** (not shown).
- Click **Add** in the **Routing Profiles** section (not shown).
- Enter Profile Name: **Route_to_IPO_UDP**.
- Click **Next**.



The screenshot shows a 'Routing Profile' dialog box. The 'Profile Name' field is highlighted with a red box and contains the text 'Route_to_IPO_UDP'. Below the field is a 'Next' button.

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

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **IP Office**.
- The **Next Hop Address** is populated automatically with **192.168.128.167:5060 (UDP)** (IP Office IP address, Port and Transport).
- Click **Finish**.



The screenshot shows the 'Routing Profile' configuration screen. It includes several settings: URI Group (set to '*'), Time of Day (set to 'default'), Load Balancing (set to 'Priority'), NAPTR (unchecked), Transport (set to 'None'), Next Hop Priority (checked), Next Hop In-Dialog (unchecked), Ignore Route Header (unchecked), ENUM (unchecked), and ENUM Suffix (empty). Below these settings is an 'Add' button. At the bottom, there is a table with one entry. The table has four columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport. The entry shows '1' in the first column, 'IP Office' in the second, '192.168.128.167:5060 (UDP)' in the third, and 'None' in the fourth. There are 'Back' and 'Finish' buttons at the bottom.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IP Office	192.168.128.167:5060 (UDP)	None

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like Dashboard, Administration, and System Management. Under 'Global Profiles', the 'Routing' option is highlighted. The main content area is titled 'Routing Profiles: Route_to_IPO_UDP'. It features a list of routing profiles on the left, including 'default', 'Route_to_SM', 'Route_to_CM', 'Route_to_IPO_UDP' (which is highlighted), 'To SM from Rem W', 'To IPO from Rem W', 'Route_to_IPO_TLS', 'Route_to_SP_TLS', 'Route_to_CS1000', and 'Route_to_SP_UDP'. An 'Add' button is at the top of this list. To the right, the configuration for the selected profile is shown. It includes a description field, an 'Update Priority' button, and a table with columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. A single row is visible with the values: 1, *, default, Priority, 192.168.128.167, and UDP. 'Edit' and 'Delete' buttons are next to this row. At the top right of the main area are 'Rename', 'Clone', and 'Delete' buttons.

Similarly, for the outbound route:

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

The screenshot shows a 'Routing Profile' dialog box. It has a title bar with 'Routing Profile' and a close button (X). Inside the dialog, there is a text input field labeled 'Profile Name' containing the text 'Route_to_SP_U'. A red rectangle highlights this input field. Below the input field is a 'Next' button.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **Service Provider UDP**.
- The **Next Hop Address** is populated automatically with **10.64.70.54:5060 (UDP)** (Private IP Address of Charter's Modular Access Router).
- Click **Finish**.

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

6.2.5 Topology Hiding

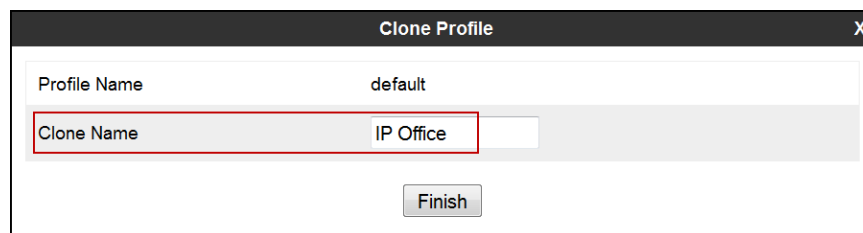
Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

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

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

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

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



Clone Profile	
Profile Name	default
Clone Name	IP Office
<button>Finish</button>	

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles' (highlighted with a red box), 'Domain DoS', 'Server Interworking', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding' (highlighted with a red box), 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The main content area is titled 'Topology Hiding Profiles: IP Office' and features an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. A blue bar indicates 'Click here to add a description.' Below this is a table titled 'Topology Hiding' with columns: Header, Criteria, Replace Action, and Overwrite Value. The table lists various headers (Record-Route, To, From, SDP, Refer-To, Referred-By, Request-Line, Via) all with 'IP/Domain' as the criteria and 'Auto' as the replace action, with 'Overwrite Value' set to '---'. An 'Edit' button is at the bottom right of the table.

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

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

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

The 'Clone Profile' dialog box is shown with a close button (X) in the top right corner. It contains two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Service_Provider' (highlighted with a red box). A 'Finish' button is located at the bottom center.

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

Session Border Controller for Enterprise AVAYA

Alarms 2 Incidents Status Logs Diagnostics Users lings Help Log Out

Topology Hiding Profiles: Service_Provider

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

Topology Hiding

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

Edit

6.3 Domain Policies

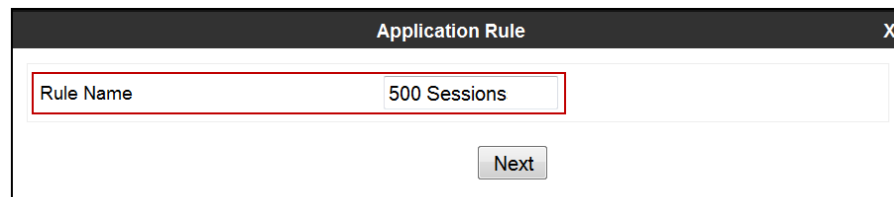
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.3.1 Application Rules

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

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

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

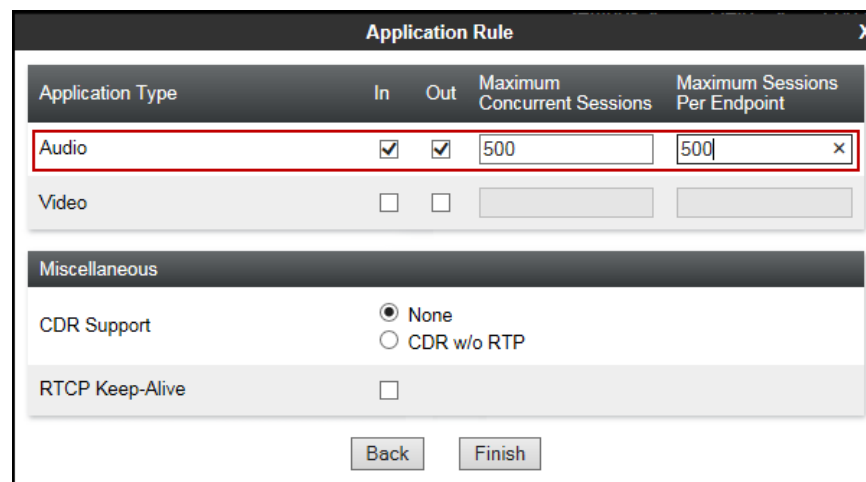


Application Rule

Rule Name 500 Sessions

Next

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



Application Rule

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

Miscellaneous

CDR Support ☒ None ☐ CDR w/o RTP

RTCP Keep-Alive ☐

Back Finish

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' expanded and 'Application Rules' selected. The main content area shows the configuration for the '500 Sessions' Application Rule. The rule is configured with the following settings:

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

Below the table, the 'Miscellaneous' section shows the following settings:

CDR Support	None
RTCP Keep-Alive	No

The '500 Sessions' rule is highlighted in the left sidebar and the 'Audio' row in the table is also highlighted.

6.3.2 End Point Policy Groups

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

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

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

The screenshot shows a 'Policy Group' dialog box with a single input field labeled 'Group Name' containing the text 'Enterprise'. A 'Next' button is located at the bottom right of the dialog.

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

Policy Group

Application Rule: 500 Sessions

Border Rule: default

Media Rule: default-low-med

Security Rule: default-low

Signaling Rule: default

Back Finish

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

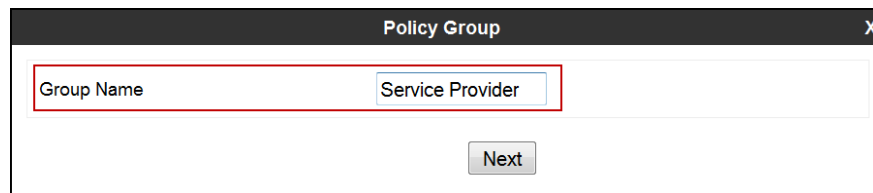
Session Border Controller for Enterprise

Policy Groups: Enterprise

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

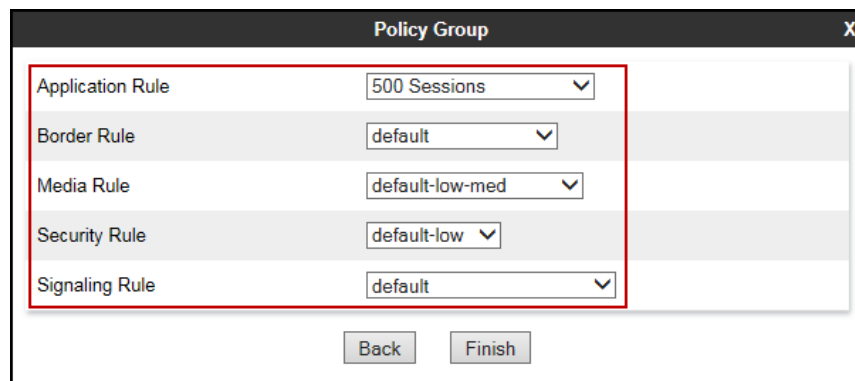
Similarly, to create an End Point Policy Group toward the Service Provider.

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



The screenshot shows a dialog box titled "Policy Group" 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". This field is highlighted with a red rectangular border. Below the input field, there is a button labeled "Next".

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



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a table with five rows, each representing a different rule type. The first row, "Application Rule", is highlighted with a red rectangular border and shows the value "500 Sessions". The other rows are "Border Rule" (default), "Media Rule" (default-low-med), "Security Rule" (default-low), and "Signaling Rule" (default). At the bottom of the dialog, there are two buttons: "Back" and "Finish".

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

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

Session Border Controller for Enterprise AVAYA

Alarms 2 Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

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-sub...
- avaya-def-high-server
- Enterprise
- Service Provider**

Policy Group

[Click here to add a description.](#)

[Hover over a row to see its description.](#)

[Summary](#)

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

6.4 Device Specific Settings

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

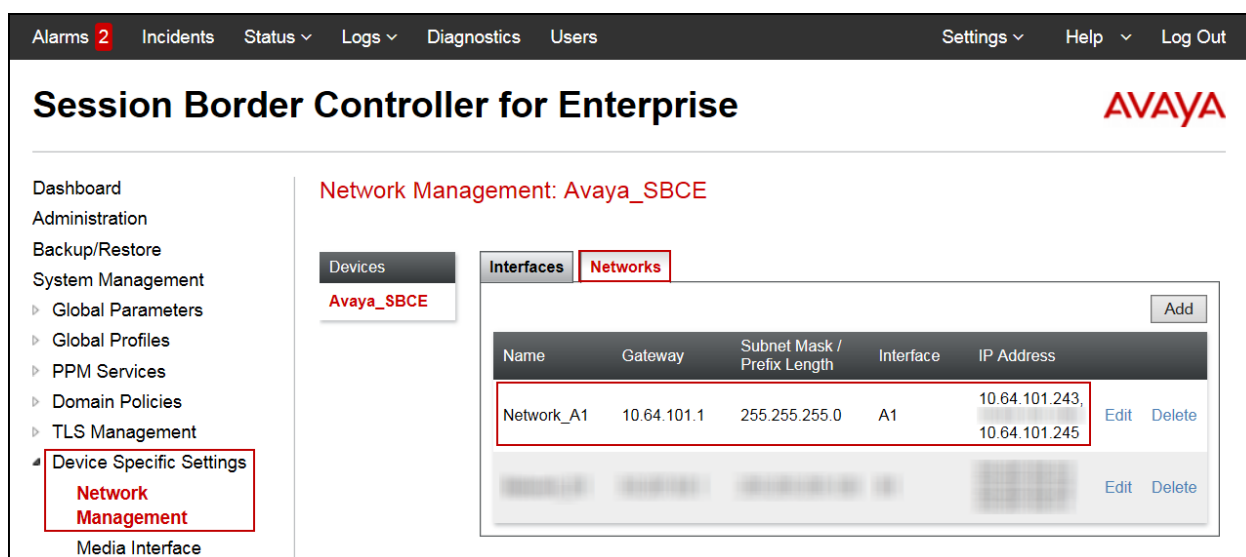
6.4.1 Network Management

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

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

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

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



Alarms 2 Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
▸ Global Parameters
▸ Global Profiles
▸ PPM Services
▸ Domain Policies
▸ TLS Management
▸ Device Specific Settings
 Network Management
Media Interface

Network Management: Avaya_SBCE

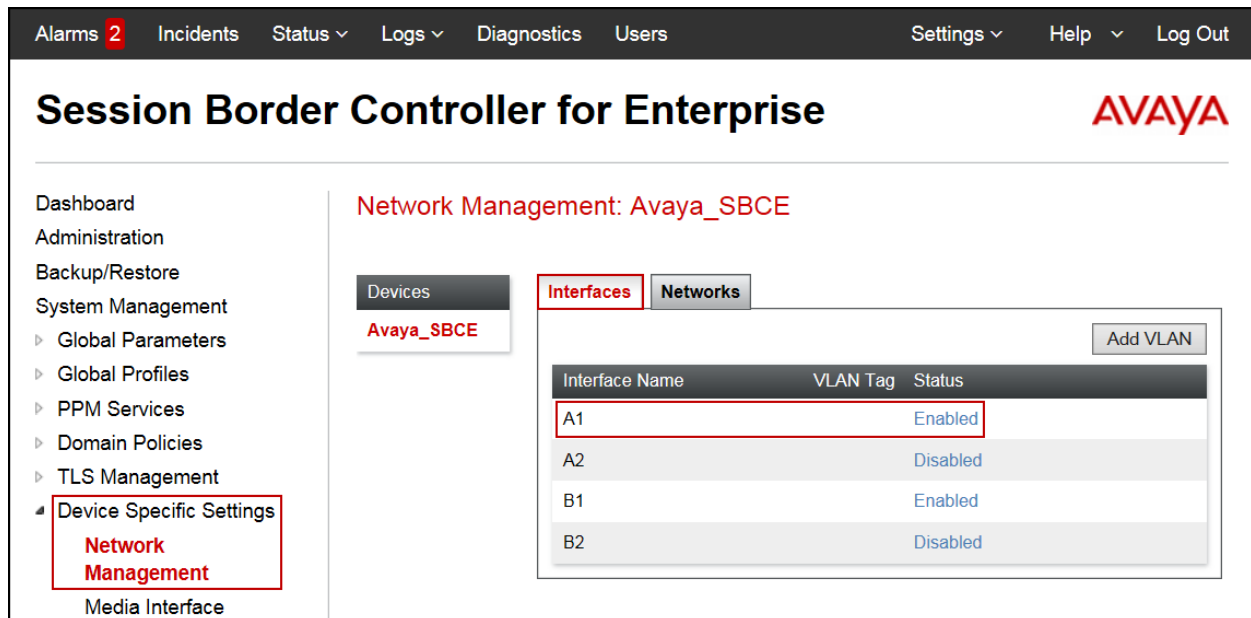
Devices
Avaya_SBCE

Interfaces **Networks**

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Network_A1	10.64.101.1	255.255.255.0	A1	10.64.101.243, 10.64.101.245	Edit Delete
					Edit Delete

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



6.4.2 Media Interface

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

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

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** **Private_med**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**.
- Select **IP Address:** **10.64.101.243** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office)
- **Port Range:** **35000-40000**.
- Click **Finish**.

- Select **Add** in the **Media Interface** area (not shown).
- **Name:** **Public_med**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**
Select **IP Address: 10.64.101.245** (Inside or A1 IP Address of the Avaya SBCE, toward Charter's Modular Access Router).
- **Port Range:** **35000-40000**.
- Click **Finish**.

The following screen capture shows the newly created Media Interfaces.

Name	Media IP Network	Port Range	Edit	Delete
Private_med	10.64.101.243 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Public_med	10.64.101.245 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete

6.4.3 Signaling Interface

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

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: Private_sig**.
- Under **IP Address** select: **Network_A1 (A1, VLAN 0)**.
- Select **IP Address: 10.64.101.243** (Inside or A1 IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port: 5060**.
- Click **Finish**.

The screenshot shows the 'Add Signaling Interface' configuration window. The fields are as follows:

Field	Value
Name	Private_sig
IP Address	Network_A1 (A1, VLAN 0) (dropdown) 10.64.101.243 (text field)
TCP Port	(text field) - Leave blank to disable
UDP Port	5060 (text field) - Leave blank to disable
TLS Port	(text field) - Leave blank to disable
TLS Profile	None (dropdown)
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	(text field)

Finish button is located at the bottom right.

- Select **Add** in the **Signaling Interface** area (not shown).
- **Name: Public_sig.**
- Under **IP Address** select: **Network_A1 (A1, VLAN 0).**
- Select **IP Address: 10.64.101.245** (Inside or A1 IP Address of the Avaya SBCE, toward Charter's Modular Access Router).
- **UDP Port: 5060.**
- Click **Finish.**

Add Signaling Interface X

Name

IP Address

TCP Port Leave blank to disable

UDP Port Leave blank to disable

TLS Port Leave blank to disable

TLS Profile

Enable Shared Control ☐

Shared Control Port

Finish

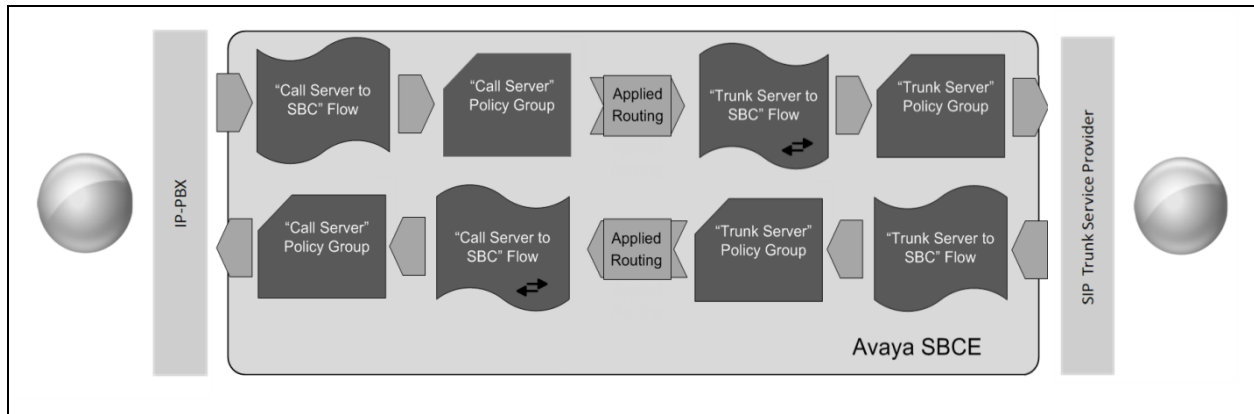
The following screen capture shows the newly created Signaling Interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Device Specific Settings' and 'Signaling Interface' highlighted. The main content area is titled 'Signaling Interface: Avaya_SBCE' and contains a table of configured signaling interfaces. A warning message at the top of the table states that modifying or deleting an existing interface requires an application restart. The table lists two interfaces: 'Private_sig' and 'Public_sig', both using the same IP address (10.64.101.243) but different ports (5060 and 5061 respectively). The 'Public_sig' interface is configured with 'None' for the TLS Profile.

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

6.4.4 End Point Flows

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



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

To create the call flow toward Charter's Modular Access Router, from the **Device Specific Settings** menu, select **End Point Flows** (not shown), then the **Server Flows** tab. Click **Add** (not shown).

- **Name:** SIP_Trunk_Flow.
- **Server Configuration:** Service Provider UDP.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Private_sig.
- **Signaling Interface:** Public_sig.
- **Media Interface:** Public_med.
- **Secondary Media Interface:** None.
- **End Point Policy Group:** Service Provider.
- **Routing Profile:** Route_to_IPO_UDP (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** Service_Provider.
- **Signaling Manipulation Script:** None.
- **Remote Branch Office:** Any.
- Click **Finish**.

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

Finish

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

- **Name: IP_Office_Flow.**
- **Server Configuration: IP Office.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Public_sig.**
- **Signaling Interface: Private_sig.**
- **Media Interface: Private_med.**
- **Secondary Media Interface: None.**
- **End Point Policy Group: Enterprise.**
- **Routing Profile: Route_to_SP_UDP** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: IP Office.**
- **Signaling Manipulation Script: None.**
- **Remote Branch Office: Any.**
- Click **Finish**.

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

Finish

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

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

On the left sidebar, the "Device Specific Settings" menu is expanded, and "End Point Flows" is selected. The main content area is titled "End Point Flows: Avaya_SBCE". It features two tabs: "Subscriber Flows" and "Server Flows", with "Server Flows" being the active tab. An "Add" button is located in the top right corner of the "Server Flows" section.

Below the tabs, there are two sections for server configurations:

- Server Configuration: IP Office**: This section includes an "Update" button and a table with the following data:

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_UDP	View Clone Edit Delete
- Server Configuration: Service Provider UDP**: This section includes a table with the following data:

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_UDP	View Clone Edit Delete

7. Charter Spectrum Enterprise SIP Trunking Service Configuration on legacy Charter Communications Platform

To use the Charter Spectrum Enterprise SIP Trunking Service offering on legacy Charter Communications Platform, a customer must request the service from Charter Communications using the established sales processes. The process can be started by contacting Charter Communications via the corporate web site at: <https://business.spectrum.com/content/sip-trunking> or call 888-692-8635.

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

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

8. Verification and Troubleshooting

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

8.1 Verification Steps

The following steps may be used to verify the configuration:

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

8.2 Protocol Traces

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

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

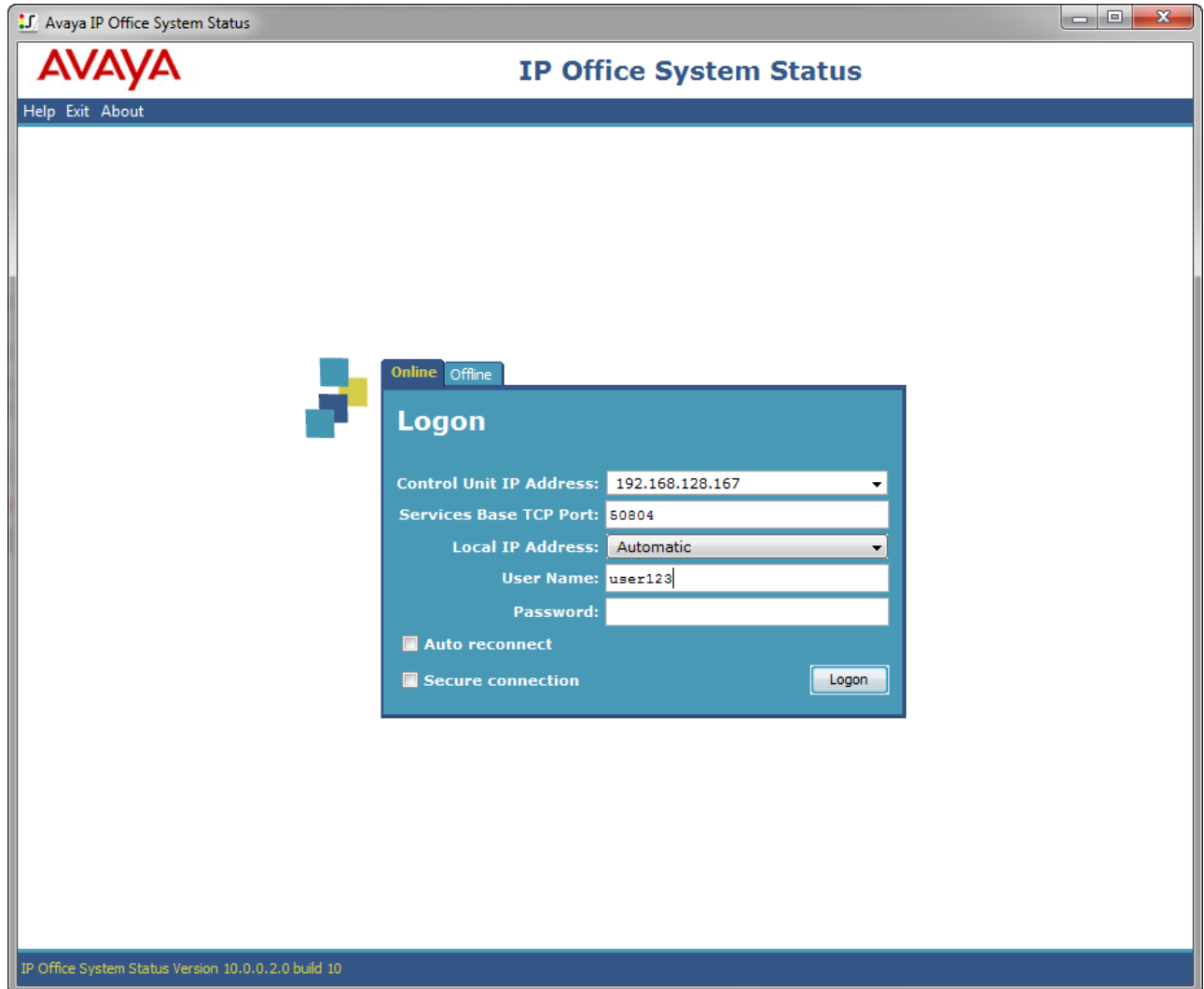
The following attributes in SIP message body are inspected using a sniffer trace analysis tool:

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

8.3 IP Office System Status

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

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



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


AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
Alarms (8)
Extensions (26)
Trunks (5)
Line: 1
Line: 2
Line: 17
Line: 18
Line: 19
Active Calls
Resources
Voicemail
IP Networking
Locations

Status Utilization Summary Alarms

SIP Trunk Summary

Line Service State: In Service
Peer Domain Name: sip://10.64.101.243
Resolved Address: 10.64.101.243
Line Number: 17
Number of Administered Channels: 10
Number of Channels in Use: 0
Administered Compression: G711 Mu
Enable Faststart: Off
Silence Suppression: Off
Media Stream: RTP
Layer 4 Protocol: UDP
SIP Trunk Channel Licenses: 128
SIP Trunk Channel Licenses in Use: 0  0%
SIP Device Features:

Channel Number	U...	Call Ref	Current State	Time in State	Remote Media A...	Co...	Conne...	Caller ID or Dia...	Other Party on Call	Direct...	Round Trip D...	Receive Jitter	Receive Packe...	Transmit Jitter	Trans...
1			Idle	02:09...											
2			Idle	02:09...											
3			Idle	02:09...											
4			Idle	02:09...											
5			Idle	02:09...											
6			Idle	02:09...											
7			Idle	02:09...											
8			Idle	02:09...											
9			Idle	02:09...											
10			Idle	02:09...											

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

Save As...

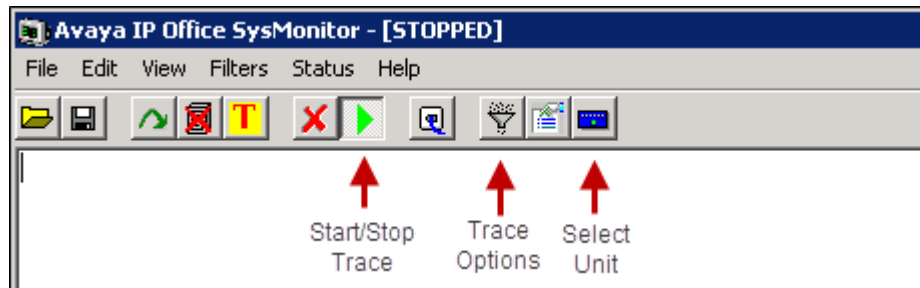
10:53:35 AM Online

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

The screenshot displays the Avaya IP Office System Status web interface. The left sidebar contains a navigation menu with the following items: System, Alarms (7), Extensions (26), Trunks (5), Line: 1, Line: 2, Line: 17 (highlighted with a red box), Line: 18, Line: 19, Active Calls, Resources, Voicemail, IP Networking, and Locations. The main content area has three tabs: Status, Utilization Summary, and Alarms (highlighted with a red box). Below the tabs, the title reads "Alarms for Line: 17 SIP sip://10.64.101.243". A table with the following headers is present: Last Date Of Error, Occurrences, and Error Description. The table body is empty. At the bottom of the interface, there is a row of buttons: Ping, Clear, Clear All, Graceful Shutdown, Force Out of Service, Print..., and Save As... The bottom status bar shows the time "10:54:43 AM" and the status "Online".

8.4 IP Office Monitor

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



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



8.5 Avaya Session Border Controller for Enterprise (Avaya SBCE)

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

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

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

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

Session Border Controller for Enterprise AVAYA

Dashboard

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

Information

System Time	10:15:19 AM EST	Refresh
Version	7.1.0.1-07-12368	
Build Date	Fri Nov 11 09:21:54 EST 2016	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	01/06/2017 15:28:20 EST	
Failed Login Attempts	0	

Installed Devices

EMS
Avaya_SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched

[Add](#)

Notes

No notes found.

The following screen shows the Incident Viewer page.

Incident Viewer AVAYA

Device: Avaya SBCE Category: Policy [Clear Filters](#) [Refresh](#) [Generate Report](#)

Displaying results 1 to 5 out of 5.

Type	ID	Date	Time	Category	Device	Cause
Message Dropped	722182809923738	10/8/15	11:40 PM	Policy	Avaya SBCE	No Subscriber Flow Matched
Server Heartbeat	721576665666258	9/24/15	10:55 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720627871533350	9/2/15	11:49 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720627092366599	9/2/15	11:23 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720581909185100	9/1/15	10:16 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down

<< < 1 > >>

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

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

Session Border Controller for Enterprise

Dashboard

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

Dashboard

Information

System Time	12:30:50 AM CDT	Refresh
Version	7.0.0-21-6602	
Build Date	Sun Aug 9 21:08:40 EDT 2015	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	10/08/2015 23:34:07 CDT	
Failed Login Attempts	0	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

[Add](#)

Notes
No notes found.

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

Diagnostics

Pinging 10.64.70.54 X

Average ping from 10.64.101.244 [A1] to 10.64.70.54 is 0.854ms.

Full Diagnostic **Ping Test**

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Source Device / IP: A1

Destination IP: 10.64.70.54

[Ping](#)

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left sidebar contains a menu with 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'PPM Services', 'Domain Policies', 'TLS Management', 'Device Specific Settings' (highlighted), 'Network Management', 'Media Interface', 'Signaling Interface', 'End Point Flows', 'Session Flows', 'DMZ Services', 'TURN/STUN Service', 'SNMP', 'Syslog Management', 'Advanced Options', 'Troubleshooting' (highlighted), 'Debugging', 'Trace' (highlighted), and 'DoS Learning'. The main content area is titled 'Trace: Avaya_SBCE' and features two tabs: 'Packet Capture' (selected) and 'Captures'. The 'Packet Capture Configuration' window is open, showing the following fields: 'Status' (Ready), 'Interface' (A1), 'Local Address' (IP:Port) (All), 'Remote Address' (*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (10000), and 'Capture Filename' (Wireshark_Capture_1.pcap). The 'Start Capture' and 'Clear' buttons are at the bottom of the configuration window.

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar contains a menu with categories like Dashboard, Administration, System Management, and Troubleshooting. The 'Troubleshooting' section is expanded, showing 'Debugging' and 'Trace'. The 'Trace' option is selected, leading to the 'Trace: Avaya_SBCE' page. This page has two tabs: 'Packet Capture' and 'Captures'. The 'Captures' tab is active, displaying a table of captured files. The table has columns for File Name, File Size (bytes), Last Modified, and a Delete button. Two files are listed: 'Wireshark_Capture_1_20161024173718.pcap' (135,168 bytes, Oct 24, 2016 5:37:35 PM EDT) and 'Wireshark_Capture_1_20161024173655.pcap' (8,192 bytes, Oct 24, 2016 5:37:06 PM EDT). Both files are highlighted with a red border.

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

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 10.0 and the Avaya Session Border Controller for Enterprise Release 7.1 to support Charter Spectrum Enterprise SIP Trunking Service on legacy Charter Communications Platform, as shown in **Figure 1**.

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

10. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya IP Office, including the following, is available at:
<http://support.avaya.com/>

- [1] *Avaya IP Office Platform Solution Description, Release 10.0.0.1*, September 2016.
- [2] *Avaya IP Office Platform Feature Description, Release 10.0*, August 2016.
- [3] *IP Office Platform 10.0 Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042, Issue 31m, 01 December 2016.
- [4] *Administering Avaya IP Office Platform with Manager*, Release 10.0, September 2016.
- [5] *IP Office Platform 10.0 Using Avaya IP Office Platform System Status*, Document 15-601758, Issue 11e, 07 July, 2016.
- [6] *IP Office Platform 10.0 Using IP Office System Monitor*, Document 15-601019, Issue 08b, 25 November, 2016.
- [7] *Using Avaya Communicator for Windows on IP Office*, Release 10, August 2016.
- [8] *Administering Avaya Communicator on IP Office, Release 10.0, Issue 01.01*, August 2016.
- [9] *Using Avaya Communicator for Web, Release 1.0, Issue 1.0.6*, May 2016.
- [9] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 1, June 2016.
- [10] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 1, June 2016.
- [11] *Troubleshooting and Maintaining Avaya session Border Controller for Enterprise, Release 7.1, Issue 1*, June 2016.

Additional Avaya IP Office documentation can be found at:
<http://marketingtools.avaya.com/knowledgebase/>

©2017 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.