



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Windstream SIP Trunking Service (Sonus Platform) with Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise Release 6.2 – Issue 1.0

Abstract

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) trunking between the Windstream (Sonus Platform) and an Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of Avaya Session Border Controller for Enterprise Release 6.2, an Avaya IP Office 500 V2 Release 9.0, Avaya Voicemail Pro, and Avaya SIP, H.323, digital, and analog endpoints.

The Windstream SIP Trunking Service provides PSTN access via a SIP trunk between the enterprise and the Windstream network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Windstream 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 in the Avaya Solution & Interoperability Test Lab.

1. Introduction

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) trunking between Windstream (Sonus platform) and an Avaya IP Office solution. In the sample configuration, the Avaya IP Office solution consists of an Avaya Session Border Controller for Enterprise Release 6.2, Avaya IP Office 500 V2 Release 9.0, Avaya Voicemail Pro, and Avaya SIP, H.323, digital, and analog endpoints.

Customers using Avaya IP Office with the Windstream SIP Trunk service are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Windstream SIP Trunking service as a non-registering device via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Avaya IP Office, Avaya Session Border Controller and various Avaya endpoints.

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 SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming calls from the PSTN were routed to the DID numbers assigned by Windstream to the Avaya IP Office location. These incoming PSTN calls arrived via the SIP Line and were answered by Avaya SIP telephones, Avaya H.323 telephones, Avaya digital telephones, analog telephones, analog fax machines, Avaya IP Office Softphone, Avaya Flare® Experience, and Avaya Voicemail Pro. The display of caller ID on display-equipped Avaya IP Office telephones was verified.
- Outgoing calls from the Avaya IP Office location to the PSTN were routed via the SIP Line to Windstream. These outgoing PSTN calls were originated from Avaya SIP phones, Avaya H.323 telephones, Avaya digital telephones, analog endpoints, Avaya IP Office Softphone, Avaya Flare® Experience, and Avaya Voicemail Pro. The display of caller ID on display-equipped PSTN telephones was verified.
- Inbound / Outbound fax calls were verified.
- Proper disconnect when the caller abandoned a call before answer for both inbound and outbound calls.
- Proper disconnect when the IP Office party or the PSTN party terminated an active call.

- Proper busy tone heard when an IP Office user called a busy PSTN user, or a PSTN user called a busy IP Office user (i.e., if no redirection was configured for user busy conditions).
- Various outbound PSTN call types were tested including long distance, international, toll-free, and directory assistance calls.
- Requests for privacy (i.e., caller anonymity) for IP Office outbound calls to the PSTN were verified. That is, when privacy is requested by IP Office, outbound PSTN calls were successfully completed while withholding the caller ID from the displays of display-equipped PSTN telephones.
- Privacy requests for inbound calls from the PSTN to IP Office users were verified. That is, when privacy is requested by a PSTN caller, the inbound PSTN call was successfully completed to an IP Office user while presenting an “anonymous” display to the IP Office user.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified.
- Incoming and outgoing calls using the G.729A and G.711MU codecs.
- DTMF transmission (RFC 2833) with successful voice mail navigation for incoming and outgoing calls. Successful navigation of a simple auto-attendant application configured on Avaya Voicemail Pro.
- Inbound and outbound long holding time call stability.
- Telephony features such as call waiting, hold, transfer, and conference.
- Inbound calls from Windstream SIP Trunk service that were call forwarded back to PSTN destinations, presenting true calling party information to the PSTN phone, via Windstream.
- Mobile twinning to a mobile phone, presenting true calling party information to the mobile phone. Outbound mobile call control was also verified successfully (e.g., using DTMF on a twinned call to place new calls and create a conference via a mobile phone).
- DiffServ markings in accordance with network requirements for IP Office SIP signaling and RTP media.

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls (911) are supported but were not tested as part of the compliance test.
- Operator (0) calls are not supported by Windstream.
- Network Call Redirection using the SIP REFER method is not supported by Windstream.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results. The following observations were noted.

- **T.38 Fax** – When the fax call is initiated with G.729A codec as the first choice on an outbound fax call, Windstream will send a re-Invite to G.711MU first before the call is negotiated to T.38. The G.711MU codec needs to an available codec on IP Office for the fax call to properly negotiate to T.38. See **Section 5.4.5**.

On an inbound fax call, IP Office will send a re-Invite with the original voice codec when the fax transmission is complete. If the original voice codec is G.729A, Windstream will return a “488 Not Acceptable Here” error. This does not have a negative effect on fax calls because it happens after the fax has been sent at the end of the call.

- **Direct Media** – Starting with R9.0, Avaya IP Office offers a new Direct Media capability on IP Office 500 V2 that allows IP endpoints to send RTP media directly to each other rather than having all the media flow through the IP Office, using up VoIP resources. Though Direct Media was tested and verified for straight inbound / outbound calls during testing, the following issues were experienced when Direct Media was enabled:
 - Avaya IP Office IP endpoints did not send RTP Events.
 - Only Direct Media *or* T.38 fax is supported on a SIP Line. The use of both features on the same SIP Line is not supported.

As a result of these issues, the recommended configuration is to have Direct Media disabled (see **Section 5.4.5**).

2.3. Support

Contact information for technical support on the Windstream SIP Trunking service:

- Web: <http://www.windstreambusiness.com/customer/support>
- Telephone: (866) 445-5882

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 sample configuration used for the DevConnect compliance testing. The sample configuration shows an enterprise site connected to the Windstream SIP Trunk service.

Located at the enterprise site are an Avaya Session Border Controller for Enterprise (Avaya SBCE) and an Avaya IP Office 500 V2. The LAN port of Avaya IP Office is connected to the enterprise LAN while the WAN port is connected to the public network. Endpoints include an Avaya 1616 IP Telephone (with H.323 firmware), an Avaya 1140E IP Telephone (with SIP firmware), an Avaya 9611 IP Telephone (with H.323 firmware), an Avaya IP Office Softphone, Flare® Experience for Windows, an Avaya 9508 Digital Telephone, an Avaya T7316E and an Avaya 6210 Analog Telephone. The site also has an IP Office Application Server running the Voicemail Pro for voicemail and one-X® Portal.

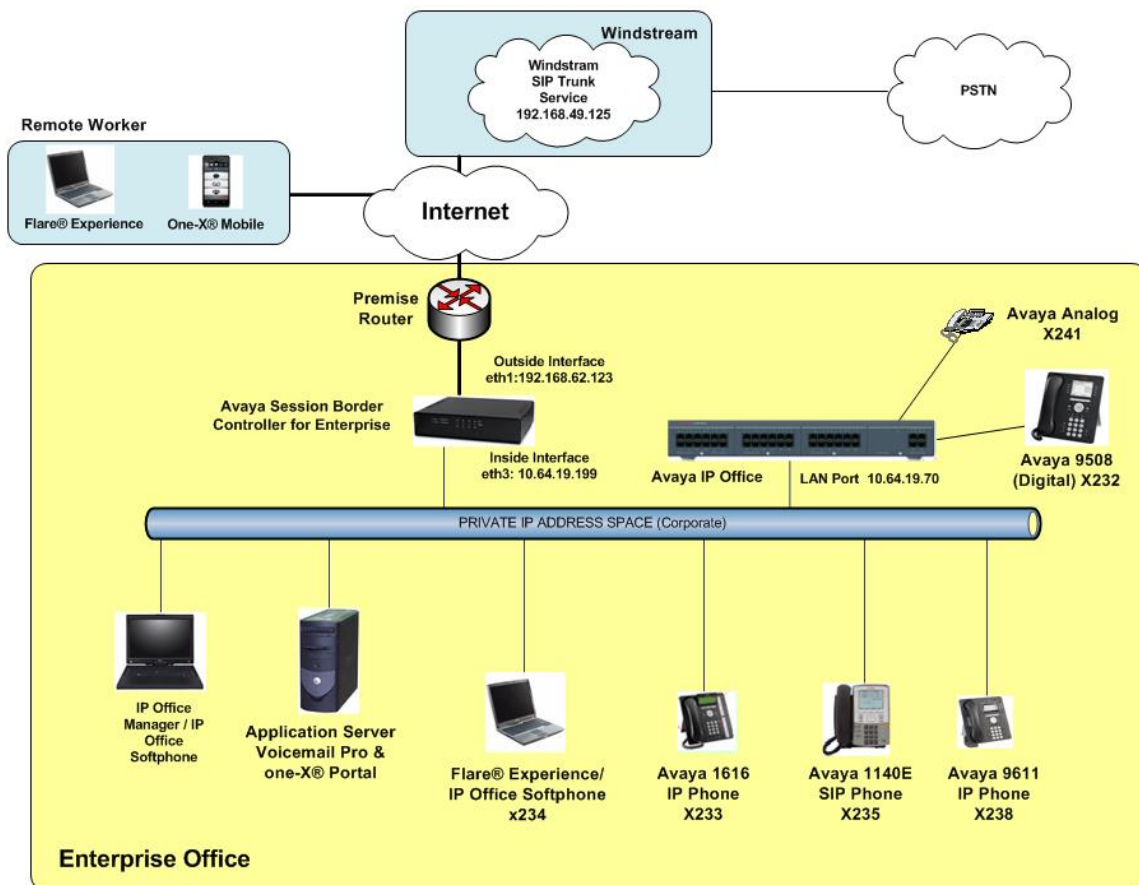


Figure 1: Avaya Interoperability Test Lab Configuration

For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, public IP addresses have been replaced with private addresses and all phone numbers have been replaced with numbers that cannot be routed.

Additionally, the reference configuration included remote worker functionality, introduced with Avaya IP Office 9.0 with Avaya SBCE. A remote worker is a SIP endpoint that resides in the untrusted network, registered to IP Office via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint within the enterprise. This functionality was successfully tested during the compliance test, using the following endpoints and protocols:

- Avaya Flare® Experience for Windows (using TLS and SRTP)
- Avaya one-X® Mobile Preferred for IP Office on Android (using TCP and RTP)

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. For more information on configuring the Avaya SBCE for IP Office remote workers, consult **Section 10** reference [6].

4. Equipment and Software Validated

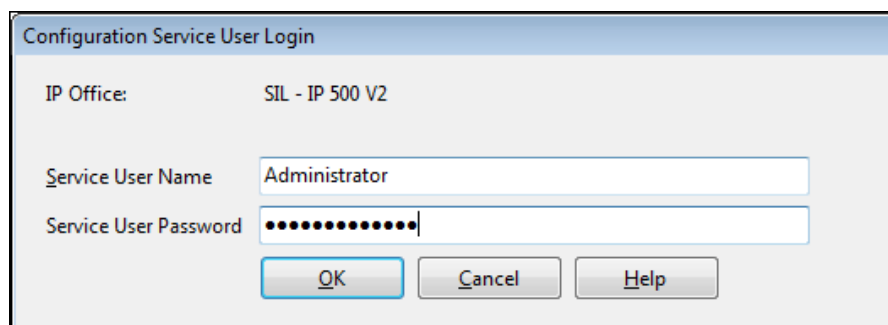
Table 1 shows the equipment and software used in the sample configuration

Avaya IP Telephony Solution Components	
Equipment	Software
Avaya Session Border Controller for Enterprise	Release 6.2.1 (Q07)
Avaya IP Office 500 V2	Release 9.0.200.860
Avaya Application Server	Release 9.0.200-860
Avaya IP Office Manager	Release 9.0.2.0 Build 860
Avaya 1616SW IP Telephone (H.323)	Release 1.343A
Avaya 9611SW IP Telephone (H.323)	Release 6.2209
Avaya 1140E IP Telephone (SIP)	Release 04.04.10
Avaya 9508 Digital Telephone	Release 0.45
Avaya IP Office Softphone	Release 3.2.3.49
Avaya Flare® Experience for Windows	Release 1.1.4.23
Windstream Components	
Equipment	Software
Sonus	Release 9.1.0

Table 1: Equipment and Software Tested

5. Avaya IP Office Configuration

IP Office is configured via the IP Office Manager program. For more information on IP Office Manager, consult Reference [2]. From the IP Office Manager PC, select **Start → Programs → IP Office → Manager** to launch the Manager application. Provided that the IP Office system is accessible to IP Office Manager, the following will be displayed in the center of the opening screen:



Configuration Service User Login

IP Office: SIL - IP 500 V2

Service User Name: Administrator

Service User Password: [Masked]

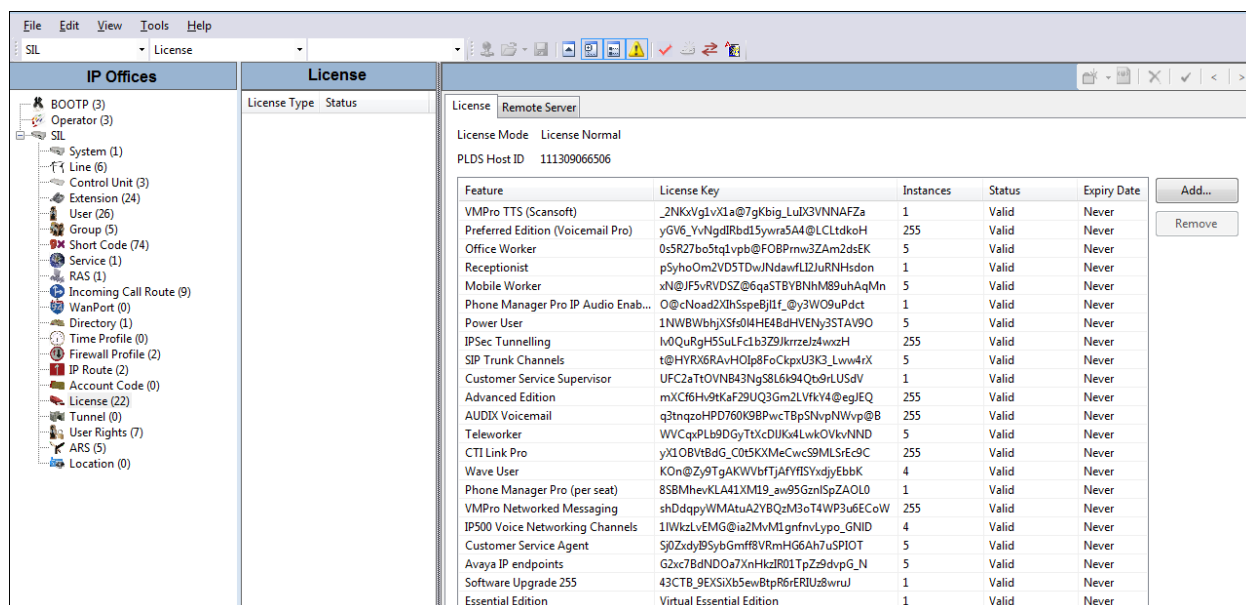
Buttons: OK, Cancel, Help

Log in with the appropriate configuration credentials. The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center, and the Details pane on the right side.

5.1. Licensing and Physical Hardware

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. Confirm a valid **SIP Trunk Channels** license with sufficient **Instances** (trunk channels). If Avaya IP Telephones will be used as is the case in these Application Notes, verify the **Avaya IP endpoints** license.



License Type	Status
License	Remote Server
License Mode	License Normal
PLDS Host ID	111309066506

Feature	License Key	Instances	Status	Expiry Date
VMP Pro TTS (ScanSoft)	_2NKxVg1vX1a@7gKbig_LuIX3VNNaFZa	1	Valid	Never
Preferred Edition (Voicemail Pro)	yGV6_YvNgdlRbd15ywna5A4@LCLtdkoH	255	Valid	Never
Office Worker	0sR27bo5tqLvpb@F0BPrmw3ZAm2dsEK	5	Valid	Never
Receptionist	pSyhoOm2VD5TDwJNdawfLJ2JuRNHsdon	1	Valid	Never
Mobile Worker	xN@JF5vRVD5Z@6qa5TBVBNhM89uhAqMn	5	Valid	Never
Phone Manager Pro IP Audio Enab...	O@cNoad2XlhSspeBjllf_@y3WO9uPdct	1	Valid	Never
Power User	1NWBWbhyXSf04H4BdHvENy3STAV90	5	Valid	Never
IPSec Tunneling	h0QuRgh5SuLfc1b3Z9JkmzeJ4wxzH	255	Valid	Never
SIP Trunk Channels	t@HYR6RAvH0lp8FoCkpxU3K3_Lww4iX	5	Valid	Never
Customer Service Supervisor	UFC2aTtOVNB43Ng58L6k94Qb6rLUSdV	1	Valid	Never
Advanced Edition	mXCf6Hv9KaF29UQ3Gm2Lvfky4@egIEQ	255	Valid	Never
AUDDX Voicemail	q3tnqzoHPD760K9BpwcTBpSNvpNWvp@B	255	Valid	Never
Teleworker	WVCqyPLb9DgyTxcDUK4LwkOVkvNND	5	Valid	Never
CTI Link Pro	yX10BVtBdG_C05KXMcCwc59MLSrEc9C	255	Valid	Never
Wave User	KOn@Zy9TgAKWVbftJAfYfSYxdjyEbbK	4	Valid	Never
Phone Manager Pro (per seat)	8SBMhevKLA41XM19_au95GznSpZAOL0	1	Valid	Never
VMP Pro Networked Messaging	shDdqpWMAAtuA2YBQzM3oT4WP3u6CoW	255	Valid	Never
IP500 Voice Networking Channels	1IWkzLvEMG@ia2MvM1gnfnvLypo_GNID	4	Valid	Never
Customer Service Agent	S0ZxdyB5ybGmfHVRmHG6Ah7uSPiOT	5	Valid	Never
Avaya IP endpoints	G2xc7BdNDOa7XnHkzR01TpZ9dvpG_N	5	Valid	Never
Software Upgrade 255	43CTB_9EX5xb5ewBtpR6rERIUz8wruJ	1	Valid	Never
Essential Edition	Virtual Essential Edition	1	Valid	Never

In the sample configuration, looking at the IP Office 500 V2 from left to right, the first module is a TCM 8 Digital Station Module. This module supports BCM / Norstar T-Series and M-Series telephones. The second module is a Combination Card. This module has 6 Digital Stations ports, 2 Analog Station ports, 4 Analog Trunk ports and 10 VCM channels. The VCM is a Voice Compression Module supporting VoIP codecs. An IP Office hardware configuration with a VCM component is necessary to support SIP trunking.

The following screen shows the modules in the IP Office used in the sample configuration. To access such a screen, select **Control Unit** in the Navigation pane. The modules appear in the Group pane. In the screen below, **IP 500 V2** is selected in the Group pane, revealing additional information about the IP 500 V2 in the Details pane.

The screenshot displays the IP Office configuration software interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu is a toolbar with various icons. The main window is divided into three panes:

- Navigation pane (left):** Shows a tree structure of the configuration. The 'Control Unit' is selected under the 'IP Offices' group.
- Group pane (middle):** Displays a table of modules installed in the selected Control Unit.
- Details pane (right):** Shows the configuration details for the selected module, 'IP 500 V2'.

Control Unit Table:

Dev No.	Dev Type	Version
1	IP 500 V2	9.0.200.860
2	TCM8	9.0.200.860
3	COMBO6210/ATM4	9.0.200.860

IP 500 V2 Details:

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	9.0.200.860
Serial Number	00e007058e33
Unit IP Address	10.64.19.70
Interconnect Number	0
Module Number	Control Unit

5.2. System Settings

This section illustrates the configuration of system settings. The settings presented here simply illustrate the sample configuration and are not intended to be prescriptive. Select **System** in the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings.

5.2.1. LAN 1 Settings

The IP500/IP500 V2 control units have 2 RJ45 Ethernet ports, physically marked as LAN and WAN. Within the system configuration, the physical LAN port is LAN1, the physical WAN port is LAN2.

In the sample configuration, LAN1 is used to connect the IP Office to the enterprise network. To view or configure the **IP Address** of LAN1, select the **LAN1** tab followed by the **LAN Settings** tab. As shown in **Figure 1**, the IP address of the IP Office is 10.64.19.70. **DHCP Mode** is also set to **Server** so that IP phones will get an IP address from the IP Office Server. Other parameters on this screen may be set according to customer requirements.

The screenshot shows the SIL configuration window with the following details:

- System** tab selected in the top navigation bar.
- LAN1** tab selected in the sub-navigation bar.
- LAN Settings** sub-tab selected.
- IP Address**: 10 . 64 . 19 . 70
- IP Mask**: 255 . 255 . 255 . 0
- Primary Trans. IP Address**: 0 . 0 . 0 . 0
- RIP Mode**: None (dropdown menu)
- Enable NAT**: ☐
- Number Of DHCP IP Addresses**: 200 (spinner box)
- DHCP Mode**: ☒ Server ☐ Client ☐ Dialin ☐ Disabled
- Advanced** button

Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 1600-Series Telephones used in the sample configuration. The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to Windstream. The **SIP Registrar Enable** box is checked to allow Avaya 1140E, Avaya IP Office Softphone, and Avaya Flare® Experience usage.

If desired, the **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media paths from Avaya SBCE to IP Office. The defaults are used here.

The screenshot shows the SIL configuration window with the VoIP tab selected. The following settings are visible:

- H323 Gatekeeper Enable**: Checked
- Auto-create Extn**: Unchecked
- Auto-create User**: Unchecked
- H323 Remote Extn Enable**: Unchecked
- SIP Trunks Enable**: Checked
- SIP Registrar Enable**: Checked
- Auto-create Extn/User**: Unchecked
- SIP Remote Extn Enable**: Unchecked
- Domain Name**: avayalab.com
- Layer 4 Protocol**:
 - UDP**: Checked, UDP Port: 5060, Remote UDP Port: 5060
 - TCP**: Checked, TCP Port: 5060, Remote TCP Port: 5060
 - TLS**: Checked, TLS Port: 5061, Remote TLS Port: 5061
- Challenge Expiry Time (secs)**: 10
- RTP**:
 - Port Number Range**:
 - Minimum: 49152, Maximum: 53246
 - Port Number Range (NAT)**:
 - Minimum: 49152, Maximum: 53246

Scroll down to the **DiffServ Settings** section. Avaya IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. The specific values used for the compliance test are shown in the screen below and are also the default values. For a customer installation, if the default values are not sufficient, appropriate values should be provided by the customer.

The screenshot shows the DiffServ Settings section with the following values:

Field	Value	Field	Value	Field	Value	Field	Value
DSCP (Hex)	B8	Video DSCP (Hex)	B8	DSCP Mask (Hex)	FC	SIG DSCP (Hex)	88
DSCP	46	Video DSCP	46	DSCP Mask	63	SIG DSCP	34

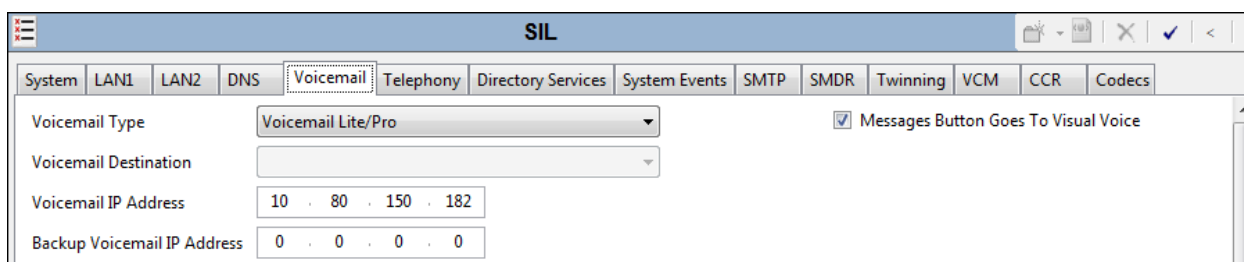
Select the **Network Topology** tab as shown in the following screen. In the sample configuration, the default settings are used and the **Use Network Topology Info** in the **SIP Line** is set to “None” in **Section 5.4.3**. The **Binding Refresh Time (seconds)** can be used to lower the SIP OPTIONS timing from the default of 300 seconds. During the testing, the Binding Refresh Time was varied (e.g., 90 seconds, 120 seconds) to test SIP OPTIONS timing.

The screenshot shows the 'SIL' application window with the 'Network Topology' tab selected. The 'Network Topology Discovery' section contains the following fields and controls:

- STUN Server Address:** 0.0.0.0
- STUN Port:** 3478
- Firewall/NAT Type:** Unknown (dropdown menu)
- Binding Refresh Time (seconds):** 120 (spinner control)
- Public IP Address:** 0 . 0 . 0 . 0
- Run STUN** and **Cancel** buttons
- Public Port:**
 - UDP: 0
 - TCP: 0
 - TLS: 0
- ☐ **Run STUN on startup**

5.2.2. Voicemail Settings

To view or change voicemail settings, select the **Voicemail** tab as shown in the following screen. The **Voicemail Type** in the sample configuration is “Voicemail Lite/Pro”. Other Voicemail types may be used. The Voicemail IP address in the sample configuration is 10.80.150.182, the IP address of the IP Office Application Server running the Voicemail Pro software, as shown in **Figure 1**.



The screenshot shows the 'Voicemail' tab selected in a configuration window titled 'SIL'. The tab bar includes System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, CCR, and Codecs. The Voicemail settings are as follows:

Field	Value
Voicemail Type	Voicemail Lite/Pro
Voicemail Destination	
Voicemail IP Address	10 . 80 . 150 . 182
Backup Voicemail IP Address	0 . 0 . 0 . 0

A checkbox labeled 'Messages Button Goes To Visual Voice' is checked.

In the sample configuration, the “Callback” application of Avaya Voicemail Pro was used to allow Voicemail Pro to call out via the SIP Line to Windstream when a message is left in a voice mailbox. The **SIP Settings** shown in the screen below enable IP Office to populate the SIP headers for an outbound “callback” call from Voicemail Pro, similar to the way the fields with these same names apply to calls made from telephone users (e.g., see **Section 5.5**).



The screenshot shows the 'SIP Settings' window with the following fields:

Field	Value
SIP Name	8645553749
SIP Display Name (Alias)	Voicemail
Contact	8645553749
Anonymous	<input type="checkbox"/>

5.2.3. System Telephony Configuration

To view or change telephony settings, select the **Telephony** tab and **Telephony** sub-tab as shown in the following screen. In the sample configuration, the **Inhibit Off-Switch Forward/Transfer** box is unchecked so that call forwarding and call transfer to PSTN destinations via the Windstream service can be tested. That is, a call can arrive to IP Office via Windstream, and be forwarded or transferred back to the PSTN with the outbound leg of the call using the Windstream SIP Trunk service. The **Companding Law** parameters are set to “ULAW” as is typical in North American locales. Other parameters on this screen may be set according to customer requirements.

The screenshot displays the SIL configuration window with the 'Telephony' tab selected. The 'Telephony' sub-tab is active, showing various configuration options. The 'Analogue Extensions' section includes dropdowns for 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), and 'Default Ring Back Sequence' (Ring Type 2). A checkbox for 'Restrict Analogue Extension Ringer Voltage' is present. The 'Companding Law' section shows 'Switch' set to 'U-Law' and 'Line' set to 'U-Law Line'. A list of checkboxes on the right includes 'DSS Status', 'Auto Hold', 'Dial By Name', 'Show Account Code', 'Inhibit Off-Switch Forward/Transfer' (unchecked), 'Restrict Network Interconnect', 'Drop External Only Impromptu Conference', 'Visually Differentiate External Call', 'Unsupervised Analog Trunk Disconnect Handling', 'High Quality Conferencing', 'Strict SIPs', and 'Digital/Analogue Auto Create User'.

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	Twinning	VCM	CCR	Codecs
Telephony													
Park & Page													
Tones & Music													
Ring Tones													
SM													
Call Log													
TUI													

Analogue Extensions

Default Outside Call Sequence: Normal

Default Inside Call Sequence: Ring Type 1

Default Ring Back Sequence: Ring Type 2

Restrict Analogue Extension Ringer Voltage: ☐

Companding Law

Switch: ☒ U-Law ☐ A-Law

Line: ☒ U-Law Line ☐ A-Law Line

Other Settings:

Dial Delay Time (secs): 4

Dial Delay Count: 0

Default No Answer Time (secs): 15

Hold Timeout (secs): 0

Park Timeout (secs): 300

Ring Delay (secs): 5

Call Priority Promotion Time (secs): Disabled

Default Currency: USD

Default Name Priority: Favor Trunk

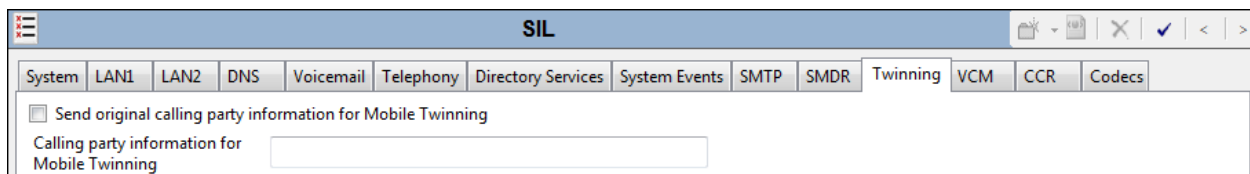
Media Connection Preservation: Disabled

Checkboxes:

- ☐ DSS Status
- ☒ Auto Hold
- ☒ Dial By Name
- ☒ Show Account Code
- ☐ Inhibit Off-Switch Forward/Transfer
- ☐ Restrict Network Interconnect
- ☐ Drop External Only Impromptu Conference
- ☒ Visually Differentiate External Call
- ☐ Unsupervised Analog Trunk Disconnect Handling
- ☒ High Quality Conferencing
- ☐ Strict SIPs
- ☒ Digital/Analogue Auto Create User

5.2.4. System Twinning Configuration

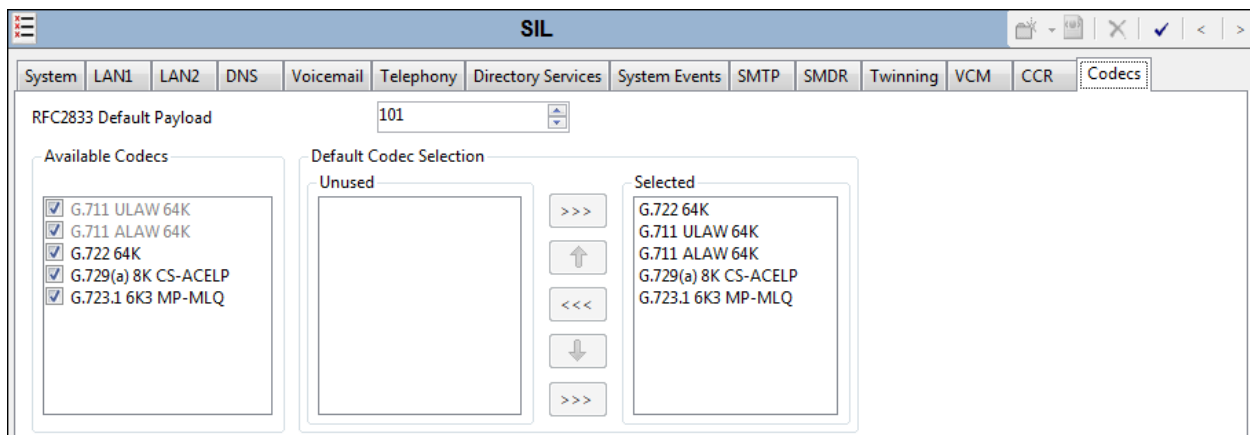
To view or change Twinning settings, select the **Twining** tab as shown in the following screen. The **Send original calling party information for Mobile Twinning** box is not checked in the sample configuration, and the **Calling party information for Mobile Twinning** is left blank. With this configuration, and related configuration of “Diversion header” on the SIP Line (Section 5.4.2), the true identity of a PSTN caller can be presented to the twinning destination (e.g., a user’s mobile phone) when a call is twinned out via the Windstream SIP Trunk service.



The screenshot shows the SIL configuration window with the 'Twining' tab selected. The 'Send original calling party information for Mobile Twinning' checkbox is unchecked. Below it, the 'Calling party information for Mobile Twinning' field is empty.

5.2.5. System Codecs Configuration

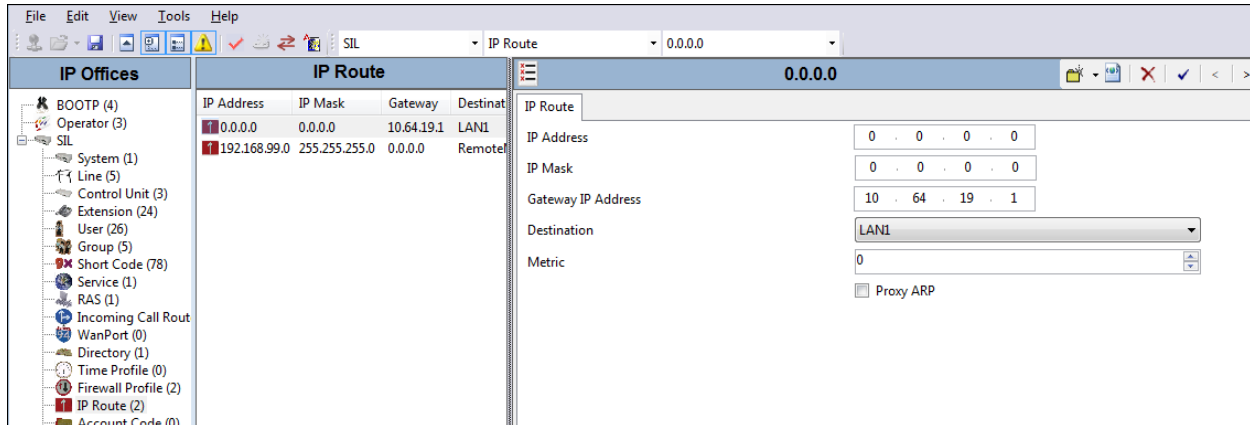
To view or change system codec settings, select the **Codecs** tab. On the left, observe the list of **Available Codecs**. In the example screen below, the box next to each codec is checked, making all the codecs available in other screens where codec configuration may be performed (such as the SIP Line in Section 5.4.5). The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis, using the up, down, left, and right arrows. By default, all IP (SIP and H.323) lines and extensions will assume the system default codec selection, unless configured otherwise for the specific line or extension. The **RFC2833 Default Payload** parameter is new in IP Office 9.0. Set the payload parameter to “101”, the value preferred by Windstream.



The screenshot shows the SIL configuration window with the 'Codecs' tab selected. The 'RFC2833 Default Payload' is set to '101'. The 'Available Codecs' list on the left includes G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ, all of which are checked. The 'Default Codec Selection' area shows an 'Unused' list and a 'Selected' list. The 'Selected' list contains G.722 64K, G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ. Navigation buttons (left, right, up, down) are present between the lists.

5.3. IP Route

In the sample configuration, the IP Office LAN1 port is physically connected to the local area network switch at the IP Office customer site. The default gateway for this network is 10.64.19.1. To add an IP Route in IP Office, right-click **IP Route** from the Navigation pane, and select **New**. To view or edit an existing route, select **IP Route** from the Navigation pane, and select the appropriate route from the Group pane. The following screen shows the Details pane with the relevant route using **Destination** “LAN1”.



5.4. SIP Line

This section shows the configuration screens for the SIP Line in IP Office Release 9. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.4.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 – 5.4.6**.

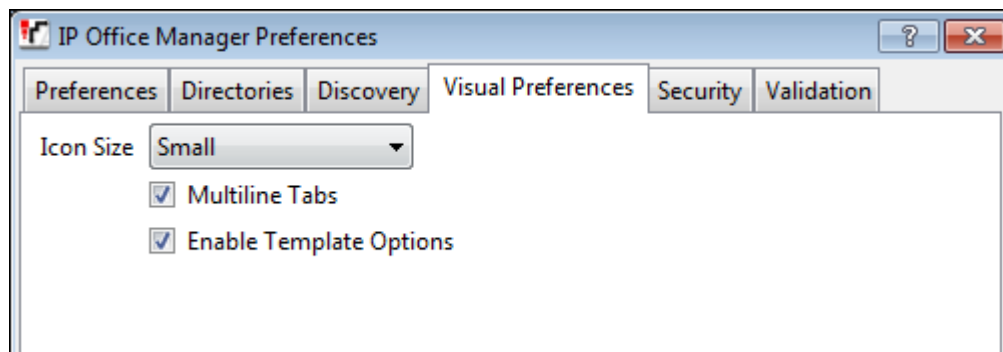
Also, the following SIP Line settings are not supported on Basic Edition:

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

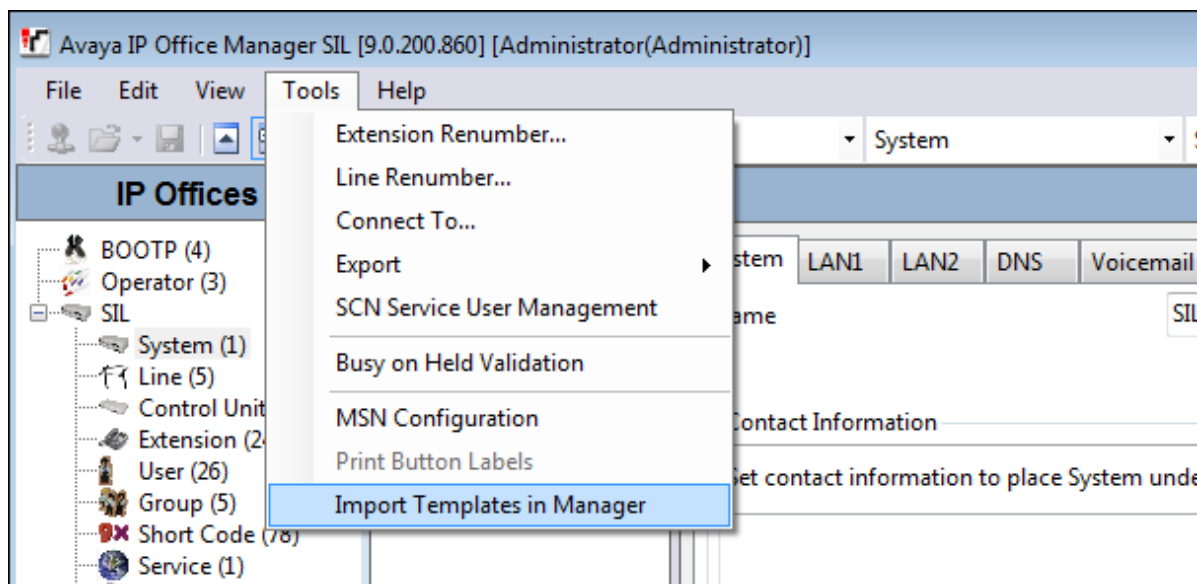
Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2 – 5.4.6**.

5.4.1. SIP Line From Template

1. Copy the template file embedded in the zip file with these Application Notes to the computer where IP Office Manager is installed. Rename the template file to **US_AvayaSBCE-WindstreamSonus.xml**. The file name is important in locating the proper template file in **Step 5**.
2. Verify that template options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the **Visual Preferences** tab. Verify that the box is checked next to **Enable Template Options**. Click **OK** (not shown).

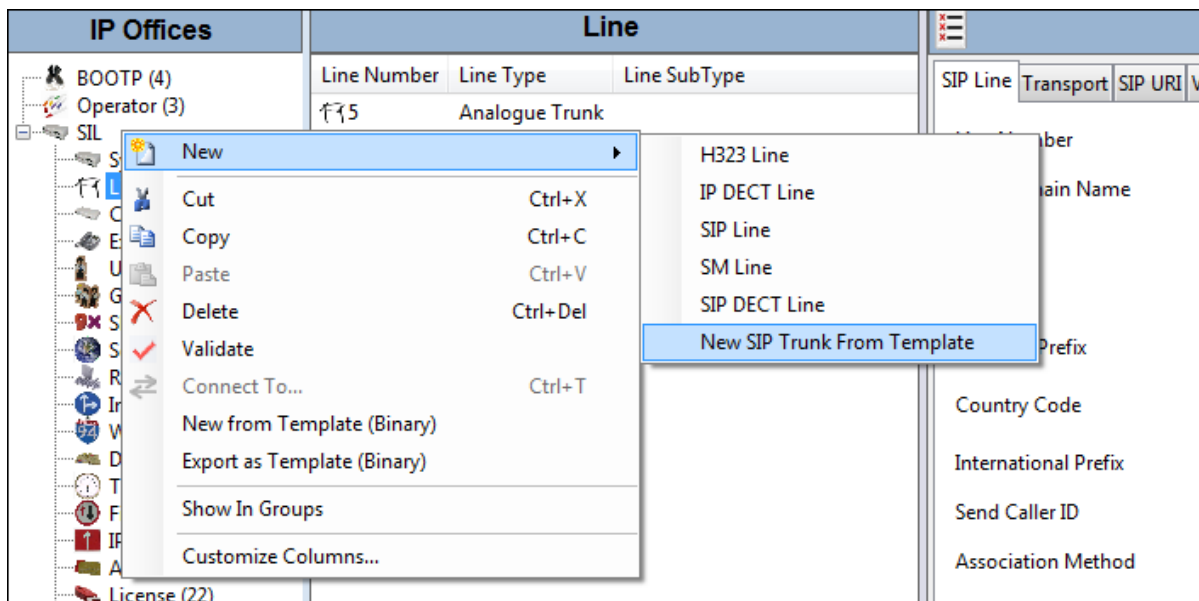


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template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

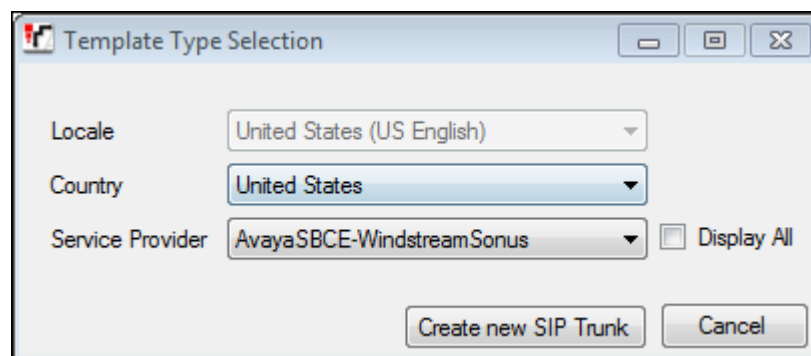


In the pop-up window (not shown) that appears, select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

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



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



Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2 – 5.4.6**.

5.4.2. SIP Line – SIP Line Tab

The **SIP Line** tab in the Details pane is shown below for **Line Number 18**, used for Avaya SBCE to the Windstream SIP Trunk service. The **ITSP Domain Name** is configured with the inside IP address of the Avaya SBCE as shown in **Figure 1**. By default, the **In Service** and **Check OOS** boxes are checked. In the sample configuration, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.

The **Send Caller ID** parameter is set to “Diversion Header”. With this setting and the related configuration in **Section 5.2.4**, IP Office will include the Diversion Header for calls that are directed via Mobile Twinning out the SIP Line to Windstream. The Diversion Header will contain the number associated with the Twinning user, allowing Windstream to admit the call. The From Header will be populated with the true calling party identity, allowing the twinning destination (e.g., mobile phone) to see the true caller id. IP Office will also include the Diversion header for calls that are call forwarded out the SIP Line to Windstream. **REFER Support** is unchecked as Windstream does not support REFER.

The **Method for Session Refresh** parameter and the related **Session Timer (seconds)** parameter are new with IP Office Release 9.0. The **Method for Session Refresh** is set to “Auto” and the **Session Timer (seconds)** is set to “1800”. With this configuration, IP Office will send UPDATE messages every 15 minutes (half of the set value) to keep the active session alive. If UPDATE is not supported, re-INVITE messages are sent. The **Media Connection Preservation** parameter retains the default setting “Disabled”

The screenshot displays the 'SIP Line - Line 18' configuration window. The 'SIP Line' tab is selected. The configuration is as follows:

Field	Value
Line Number	18
ITSP Domain Name	10.64.19.199
Prefix	
National Prefix	
Country Code	
International Prefix	
Send Caller ID	Diversion Header
Association Method	By Source IP address
In Service	<input checked="" type="checkbox"/>
URI Type	SIP
Check OOS	<input checked="" type="checkbox"/>
Call Routing Method	Request URI
Originator number for forwarded and twinning calls	
Name Priority	System Default
Caller ID from From header	<input type="checkbox"/>
Send From In Clear	<input type="checkbox"/>
User-Agent and Server Headers	
Service Busy Response	486 - Busy Here
Action on CAC Location Limit	Allow Voicemail
REFER Support	<input type="checkbox"/>
Incoming	Always
Outgoing	Always
Method for Session Refresh	Auto
Session Timer (seconds)	1800
Media Connection Preservation	Disabled

5.4.3. SIP Line - Transport Tab

Select the **Transport** tab. The **ITSP Proxy Address** is set to the inside IP address of the Avaya SBCE as shown in **Figure 1**. In the **Network Configuration** area, “UDP” is selected as the **Layer 4 Protocol**. The **Send Port** and **Listen Port** can retain the default value 5060. The **Use Network Topology Info** parameter is set to “None”.

The screenshot shows the 'SIP Line - Line 18' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.64.19.199'. In the 'Network Configuration' section, 'UDP' is selected for 'Layer 4 Protocol', and 'None' is selected for 'Use Network Topology Info'. The 'Send Port' and 'Listen Port' are both set to '5060'. The 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is checked. The 'Separate Registrar' field is empty.

SIP Line - Line 18					
SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials
ITSP Proxy Address: 10.64.19.199					
Network Configuration					
Layer 4 Protocol		UDP		Send Port	5060
Use Network Topology Info		None		Listen Port	5060
Explicit DNS Server(s)		0 . 0 . 0 . 0		0 . 0 . 0 . 0	
Calls Route via Registrar		<input checked="" type="checkbox"/>			
Separate Registrar					

5.4.4. SIP Line - SIP URI Tab

Select the **SIP URI** tab. To add a new SIP URI, click the **Add...** button. In the bottom of the screen, a New Channel area will be opened. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the bottom of the screen, the Edit Channel area will be opened. In the example screen below, a previously configured entry is edited. “Use Internal Data” is selected for the **Local URI**, **Contact**, and **Display Name**. Information configured on the SIP Tab for individual users will be used to populate the SIP headers. The **PAI** parameter is set to “None”. The **Registration** parameter is set to the default “0: <None>” since Windstream service does not require registration. The **Incoming Group** parameter, set here to “18”, will be referenced when configuring Incoming Call Routes to map inbound SIP trunk calls to IP Office destinations in **Section 5.7**. The **Outgoing Group** parameter, set here to “18”, will be used for routing outbound calls to Windstream via the Short Codes (**Section 5.6**) or ARS configuration (**Section 5.8**). The **Max Calls per Channel** parameter, configured here to “10”, sets the maximum number of simultaneous calls that can use the URI before IP Office returns busy to any further calls. Click **OK**.

The screenshot displays the 'SIP Line - Line 18' configuration window. The 'SIP URI' tab is selected, showing a table with two entries. The first entry is selected, and the 'Edit...' button is clicked, opening the 'Edit Channel' dialog.

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	18 18	<...>	<...>	<...>	<...>	N...	0: <Non...	10
2	18 0	<...>	864555...	86455...	8645553749	N...	0: <Non...	10

Edit Channel

Via: <None>

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

PAI: None

Registration: 0: <None>

Incoming Group: 18

Outgoing Group: 18

Max Calls per Channel: 10

Buttons: Add..., Remove, Edit..., OK, Cancel

In the sample configuration, the single SIP URI shown above is sufficient to allow incoming calls for Windstream DID numbers destined for specific IP Office users or IP Office hunt groups. The calls are accepted by IP Office since the incoming number will match the SIP Name configured for the user or hunt group that is the destination for the call. Channel 2 displays a service number, such as a DID number routed directly to voicemail or DID used for Mobile Call Control. DID numbers that IP Office should admit can be entered into the **Local URI** and **Contact** fields instead of “Use Internal Data”. The number 864-555-3749 will be assigned as a service number in the Incoming Call Routes in **Section 5.7**.

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max Calls
1	18 18	<...>				N...	0: <Non...	10
2	18 0	<...>	864555...	86455...	8645553749	N...	0: <Non...	10

Edit Channel

Via: <None>

Local URI: 8645553749

Contact: 8645553749

Display Name: 8645553749

PAI: None

Registration: 0: <None>

Incoming Group: 18

Outgoing Group: 0

Max Calls per Channel: 10

OK Cancel

5.4.5. SIP Line - VoIP Tab

Select the **VoIP** tab. The **Codec Selection** drop-down box **System Default** (default) will match the codecs set in the system wide Default Selection list (**System → Codecs**). In the sample configuration, “Custom” is selected and codecs preferred by Windstream are included (i.e., G729(a) 8K CS-ACELP and G.711 ULAW 64K). This will cause IP Office to include G.729a and G.711MU in the Session Description Protocol (SDP) offer, in that order. Set the **Fax Transport Support** drop-down to “T38”. This enables T.38 fax relay to be used when fax tones are detected during the call. The **DTMF Support** parameter can remain set to the default value “RFC2833”. The **Re-invite Supported** parameter can be checked 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. The **Re-invite Supported** parameter should be checked and the G.711 ULAW codec should be an available choice if the SIP Line will be used for fax. For PSTN originations, Windstream preferred the G.729 codec in the SDP, while also allowing the G.711MU codec. Click **OK** (not shown).

The screenshot shows the 'SIP Line - Line 18' configuration window with the 'VoIP' tab selected. The window has a title bar with standard icons and a tab bar with 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', and 'SIP Credentials'. The 'VoIP' tab is active. The 'Codec Selection' dropdown is set to 'Custom'. Below it, there are two lists: 'Unused' and 'Selected'. The 'Unused' list contains 'G.711 ALAW 64K', 'G.722 64K', and 'G.723.1 6K3 MP-MLQ'. The 'Selected' list contains 'G.729(a) 8K CS-ACELP' and 'G.711 ULAW 64K'. Between the lists are buttons for moving items: '>>>', '<<<', and '<<<' (for moving from unused to selected) and '>>>' (for moving from selected to unused). To the right of the lists are checkboxes for various options: 'VoIP Silence Suppression', 'Allow Direct Media Path', 'Re-invite Supported' (checked), 'Codec Lockdown', 'PRACK/100rel Supported', 'Force direct media with phones', and 'G.711 Fax ECAN' (checked). Below the codec lists, there are dropdown menus for 'Fax Transport Support' (set to 'T38'), 'Location' (set to 'Cloud'), and 'DTMF Support' (set to 'RFC2833'). There is also a 'Call Initiation Timeout (s)' field set to '4'.

5.4.6. SIP Line- T38 Fax

The settings on this tab are only accessible if **Re-invite Supported** is checked and a value for **Fax Transport Support** other than “None” are selected on the **VoIP** tab. Fax relay is only supported on IP500/IP500 V2 systems with an IP500 VCM card. Uncheck **Use Default Values** at the bottom of the screen and set **T38 Fax Version** to “0”. This is the version supported by Windstream.

The screenshot shows the 'SIP Line - Line 18' configuration window with the 'T38 Fax' tab selected. The window has a title bar with standard OS controls and a toolbar with icons for help, save, cancel, apply, and navigation. Below the title bar is a tabbed interface with 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', and 'SIP Credentials'. The 'T38 Fax' tab contains the following settings:

- T38 Fax Version:** A dropdown menu set to '0'.
- Transport:** A dropdown menu set to 'UDPTL'.
- Redundancy:** A section containing two spinners: 'Low Speed' set to 0 and 'High Speed' set to 0.
- TCF Method:** A dropdown menu set to 'Trans TCF'.
- Max Bit Rate (bps):** A dropdown menu set to '14400'.
- EFlag Start Timer (msecs):** A spinner set to 2600.
- EFlag Stop Timer (msecs):** A spinner set to 2300.
- Tx Network Timeout (secs):** A spinner set to 150.
- Checkboxes on the right:**
 - ☒ Scan Line Fix-up
 - ☒ TFOP Enhancement
 - ☐ Disable T30 ECM
 - ☐ Disable EFlags For First DIS
 - ☐ Disable T30 MR Compression
 - ☐ NSF Override
- Country Code:** A spinner set to 0.
- Vendor Code:** A spinner set to 0.
- Use Default Values:** An unchecked checkbox at the bottom left.

5.5. Users

In this section, an example of an IP Office User will be illustrated. In the interests of brevity, not all users shown in **Figure 1** will be presented, since the configuration can be easily extrapolated to other users. To add a User, right click on **User** in the Navigation pane, and select **New**. To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane.

The following screen shows the **User** tab for User 232. As shown in **Figure 1**, this user corresponds to the Avaya Digital 9508.

The screenshot displays the configuration interface for User 232, titled "Avaya9508: 232". The interface includes a navigation pane on the left with tabs for Mobility, Group Membership, Announcements, SIP, and Personal Directory. The main content area has a sub-navigation bar with tabs for User, Voicemail, DND, Short Codes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, Button Programming, and Menu Programming. The "User" tab is active, showing the following configuration fields:

- Name: Avaya9508
- Password: ****
- Confirm Password: ****
- Account Status: Enabled (dropdown)
- Full Name: (empty field)
- Extension: 232
- Email Address: (empty field)
- Locale: (empty dropdown)
- Priority: 5 (dropdown)
- System Phone Rights: None (dropdown)
- Profile: Office Worker User (dropdown)
- Receptionist: ☐
- Enable Softphone: ☐
- Enable one-X Portal Services: ☒
- Enable one-X TeleCommuter: ☐
- Enable Remote Worker: ☐
- Enable Flare: ☒
- Enable Mobile VoIP Client: ☐
- Send Mobility Email: ☐
- Ex Directory: ☐
- Device Type: Avaya 9508 (with a small phone icon)

The following screen shows the **SIP** tab for User 232. The **SIP Name** and **Contact** parameters are configured with the DID number of the user, 864-555-3744. These parameters configure the user part of the SIP URI in the From header for outgoing SIP trunk calls, and allow matching of the SIP URI for incoming calls, without having to enter this number as an explicit SIP URI for the SIP Line. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network.

See **Section 5.6** for a method of using a short code (rather than static user provisioning) to place an anonymous call.

The screenshot shows the configuration window for user 232, titled "Avaya9508: 232". The "SIP" tab is selected. The configuration fields are as follows:

Field	Value
SIP Name	8645553744
SIP Display Name (Alias)	Avaya9508
Contact	8645553744

There is an unchecked checkbox labeled "Anonymous" at the bottom.

From **Figure 1**, note that user 232 will use the Mobile Twinning feature. The following screen shows the **Mobility** tab for User 232. 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 mobile telephone, in this case 913035552215. Other options can be set according to customer requirements.

The screenshot shows the configuration window for user 232, titled "Avaya9508: 232". The "Mobility" tab is selected. The configuration fields are as follows:

Field	Value
Internal Twinning	<input type="checkbox"/>
Twinned Handset	<None>
Maximum Number of Calls	1
Twin Bridge Appearances	<input type="checkbox"/>
Twin Coverage Appearances	<input type="checkbox"/>
Twin Line Appearances	<input type="checkbox"/>
Mobility Features	<input checked="" type="checkbox"/>
Mobile Twinning	<input checked="" type="checkbox"/>
Twinned Mobile Number (including dial access code)	913035552215
Twining Time Profile	<None>
Mobile Dial Delay (secs)	0
Mobile Answer Guard (secs)	0
Hunt group calls eligible for mobile twinning	<input type="checkbox"/>
Forwarded calls eligible for mobile twinning	<input type="checkbox"/>
Twin When Logged Out	<input type="checkbox"/>
one-X Mobile Client	<input type="checkbox"/>
Mobile Call Control	<input checked="" type="checkbox"/>
Mobile Callback	<input checked="" type="checkbox"/>

5.6. Short Codes

In this section, various examples of IP Office short codes will be illustrated. To add a short code, right click on **Short Code** in the Navigation pane, and select **New**. To edit an existing short code, click **Short Code** in the Navigation pane, and the short code to be configured in the Group pane.

In the screen shown below, the short code “8N;” is illustrated. The **Code** parameter is set to “8N;”. The **Feature** parameter is set to “Dial”. The **Telephone Number** parameter is set to N“@10.64.19.199”. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message. The value “N” represents the number dialed by the user. The IP address 10.64.19.199 represents the IP address of the Avaya SBCE inside interface. The **Line Group ID** parameter is set to “18”, matching the number of the **Outgoing Group** configured on the **SIP URI** tab of SIP Line 18 to Windstream (**Section 5.4.4**).

This simple short code will allow an IP Office user to dial the digit 8 followed by any telephone number, symbolized by the letter N, to reach the SIP Line to Windstream. “N” can be any number such as a 1+10 digit number, a toll free number, directory assistance (e.g., 411), etc. This short code approach has the virtue of simplicity, but does not provide for alternate routing or an awareness of the end of a dialed digit string. When users dial 8 plus the number, IP Office must wait for an end of dialing timeout before sending the SIP INVITE to Windstream.

The screenshot shows a configuration window for a short code. The title bar reads "8N;; Dial". The window contains the following fields:

Short Code	
Code	8N;
Feature	Dial
Telephone Number	N"@10.64.19.199"
Line Group ID	18
Locale	
Force Account Code	<input type="checkbox"/>

The simple “8N;” short code previously illustrated does not provide a means of alternate routing if the configured SIP Line is out of service or temporarily not responding. When alternate routing options and/or more customized analysis of the digits following the short code are desired, the Automatic Route Selection (ARS) feature may be used. In the following example screen, the short code “9N” is illustrated for access to ARS. When the Avaya IP Office user dials 9 plus any number “N”, rather than being directed to a specific **Line Group Id**, the call is directed to “50:Main”, configurable via ARS. See **Section 5.8** for example ARS route configuration for “50:Main” as well as a backup route.

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

Optionally, add or edit a short code that can be used to access the SIP Line anonymously. In the screen shown below, the short code “*67N;” is illustrated. This short code is similar to the “8N;” short code except that the **Telephone Number** field begins with the letter “W”, which means “withhold the outgoing calling line identification”. In the case of the SIP Line connecting to Windstream documented in these Application Notes, when a user dials *67 plus any number “N”, IP Office will include the user’s telephone number in the P-Preferred-Identity header along with “Privacy: id”. With these headers, Windstream will prevent presentation of the caller id to the called PSTN destination.

*67N;: Dial	
Short Code	
Code	*67N;
Feature	Dial
Telephone Number	WN"@10.64.19.199"
Line Group ID	18
Locale	
Force Account Code	<input type="checkbox"/>

The following screen illustrates a short code that acts like a feature access code rather than a means to access a SIP Line. In this case, the **Code** “FNE31” is defined for **Feature** “FNE Service” to **Telephone Number** “31” (Mobile Call Control). This short code will be used as means to allow a Windstream DID to be programmed to route directly to this feature, via inclusion of this short code as the destination of an Incoming Call Route. See **Section 5.7**. This feature is used to provide dial tone to twinned mobile devices (e.g., cell phone) directly from IP Office; once dial tone is received the user can perform dialing actions including making calls and activating short codes.

5.7. Incoming Call Routes

In this section, IP Office Incoming Call Routes are illustrated. To add an incoming call route, right click on **Incoming Call Route** in the Navigation pane, and select **New**. To edit an existing incoming call route, select **Incoming Call Route** in the Navigation pane, and the appropriate incoming call route to be configured in the Group pane.

In the screen shown below, the incoming call route for **Incoming Number** “8645553744” is illustrated. The **Line Group Id** is “18”, matching the **Incoming Group** field configured in the **SIP URI** tab for the SIP Line to Windstream in **Section 5.4.4**.

Line Group ID	Incoming Number	Destination
18	8645553744	232 Avaya9508
18	8645553745	233 Avaya1616
18	8645553746	234 Softphone
18	8645553747	235 Avaya1140E
18	8645553748	239 oneXMobile
18	8645553749	VoiceMail

Standard	Voice Recording	Destinations
Bearer Capability: Any Voice		
Line Group ID: 18		
Incoming Number: 8645553744		
Incoming Sub Address:		
Incoming CLI:		
Locale:		
Priority: 1 - Low		
Tag:		
Hold Music Source: System Source		
Ring Tone Override: None		

Select the **Destinations** tab. From the **Destination** drop-down, select the extension to receive the call when a PSTN user dials 864-555-3744.

Incoming Call Route			18 8645553744		
Line Group ID	Incoming Number	Destination			
18	8645553744	232 Avaya9508			
18	8645553745	233 Avaya1616			
18	8645553746	234 Softphone			
18	8645553747	235 Avaya1140E			
18	8645553748	239 oneXMobile			
18	8645553749	VoiceMail			

Standard			Voice Recording			Destinations		
TimeProfile			Destination			Fallback Extension		
Default Value			232 Avaya9508					

Incoming Call Routes for other direct mappings of DID numbers to IP Office users listed in **Figure 1** are omitted here, but can be configured in the same fashion.

When configuring an Incoming Call Route, the **Destination** field can be manually configured with a number such as a short code, or certain keywords available from the pull-down menu. For example, the following **Destinations** tab for an incoming call route contains the **Destination** “VoiceMail” entered manually. An incoming call to 864-555-3749 will be delivered directly to voicemail, allowing the caller to log-in to voicemail and access messages.

Incoming Call Route			18 8645553749		
Line Group ID	Incoming Number	Destination			
18	8645553744	232 Avaya9508			
18	8645553745	233 Avaya1616			
18	8645553746	234 Softphone			
18	8645553747	235 Avaya1140E			
18	8645553748	239 oneXMobile			
18	8645553749	VoiceMail			

Standard			Voice Recording			Destinations		
TimeProfile			Destination			Fallback Extension		
Default Value			VoiceMail					

At different times during testing, the destination for 864-555-3749 was changed to test the IP Office Mobile Call Control feature. The following **Destinations** tab for the incoming call route contains the **Destination** “FNE31” entered manually. With this destination, an incoming call to 864-555-3749 will be delivered directly to internal dial tone from the IP Office, allowing the caller to perform dialing actions including making calls and activating Short Codes. The incoming caller ID must match the Twinned Mobile Number entered in the User Mobility tab (**Section 5.5**); otherwise the IP Office responds with a 486 Busy Here and the caller will hear a busy tone.

Incoming Call Route			18 8645553749		
Line Group ID	Incoming Number	Destination			
18	8645553744	232 Avaya9508			
18	8645553745	233 Avaya1616			
18	8645553746	234 Softphone			
18	8645553747	235 Avaya1140E			
18	8645553748	239 oneXMobile			
18	8645553749	FNE31			

Standard			Voice Recording			Destinations		
TimeProfile			Destination			Fallback Extension		
Default Value			FNE31					

5.8. ARS and Alternate Routing

While detailed coverage of ARS is beyond the scope of these Application Notes, this section includes basic ARS screen illustrations and considerations. ARS is illustrated here mainly to demonstrate alternate routing should the SIP Line be out of service or temporarily not responding.

Optionally, Automatic Route Selection (ARS) can be used rather than the simple “8N;” short code approach documented in **Section 5.6**. With ARS, secondary dial tone can be provided after the access code, time-based routing criteria can be introduced, 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. ARS also facilitates more specific dialed telephone number matching, enabling immediate routing and alternate treatment for different types of numbers following the access code. For example, if all 1+10 digit calls following an access code should use the SIP Line preferentially, but certain service numbers following the access code should prefer a different outgoing line group, ARS can be used to distinguish the call behaviors.

To add a new ARS route, right-click **ARS** in the Navigation pane, and select **New**. To view or edit an existing ARS route, select **ARS** in the Navigation pane, and select the appropriate route name in the Group pane.

The following screen shows an example ARS configuration for the route named “Main”. The **In Service** parameter refers to the ARS form itself, not the Line Groups that may be referenced in the form. If the **In Service** box is un-checked, calls are routed to the ARS route name specified in the **Out of Service Route** parameter. IP Office short codes may also be defined to allow an ARS route to be disabled or enabled from a telephone. The configurable provisioning of an Out of Service Route and the means to manually activate the Out of Service Route can be helpful for scheduled maintenance or other known service-affecting events for the primary route.

Main

ARS

ARS Route Id: 50

Route Name: Main

Dial Delay Time: System Default (4)

☒ Secondary Dial tone: SystemTone

☒ Check User Call Barring

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

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

Code	Telephone Number	Feature	Line Group ID
011N;	011N"@10.64.19.199"	Dial	18
0N;	0N"@10.64.19.199"	Dial	18
1010288XXXXXX...	1010288N"@10.64.19.199"	Dial	18
11	911"@10.64.19.199"	Dial Emergency	0
1XXXXXXXXXX	1N"@10.64.19.199"	Dial	18
311	311"@10.64.19.199"	Dial	18
411	411"@10.64.19.199"	Dial	18

Buttons: Add..., Remove, Edit...

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

Alternate Route: 52: backup

Assuming the primary route is in-service, the number passed from the short code used to access ARS (e.g., 9N in **Section 5.6**) can be further analyzed to direct the call to a specific Line Group ID. Per the example screen above, if the user dialed 9-1-303-555-1234, the call would be directed to Line Group 18. If Line Group 18 cannot be used, the call can automatically route to the route name configured in the **Alternate Route** parameter in the lower right of the screen. Since alternate routing can be considered a privilege not available to all callers, IP Office can control access to the alternate route by comparing the calling user's priority to the value in the **Alternate Route Priority Level** field.

The following screen shows an example ARS configuration for the route named “backup”, **ARS Route Id** “52”. Continuing the example, if the user dialed 9-1-303-555-1234, and the call could not be routed via the primary route “50: Main” described above, the call will be delivered to this “backup” route. Per the configuration shown below, the call will be delivered to Line Group 0 using the analog lines. The configuration of the **Code**, **Telephone Number**, **Feature**, and **Line Group ID** for an ARS route is similar to the configuration already shown for short codes in **Section 5.6**.

The screenshot shows the ARS configuration window for a route named "backup". The window has a title bar with the name "backup" and standard window controls. The configuration is organized into several sections:

- ARS Section:**
 - ARS Route Id:** 52
 - Route Name:** backup
 - Dial Delay Time:** System Default (4)
 - Secondary Dial tone:** ☒ (checked), SystemTone (dropdown)
 - Check User Call Barring:** ☒ (checked)
- Service and Routing Section:**
 - In Service:** ☒ (checked). An arrow points to **Out of Service Route**, which is set to <None>.
 - Time Profile:** <None> (dropdown). An arrow points to **Out of Hours Route**, which is set to <None>.
- Code Table:**

Code	Telephone Number	Feature	Line Group ID
0N;	0N	Dial 3K1	0
11	911	Dial Emergency	0
1XXXXXXXXXX	1N	Dial 3K1	0
911	911	Dial Emergency	0
XXXXXXXXXX	N	Dial 3K1	0

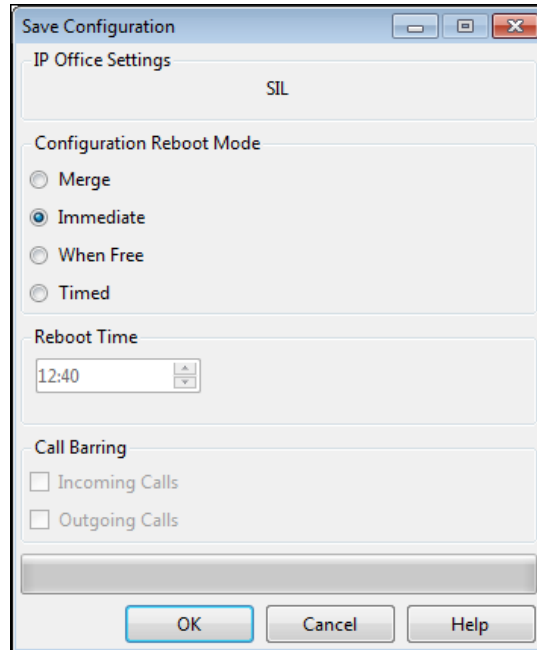
Buttons: Add..., Remove, Edit...
- Alternate Route Section:**
 - Alternate Route Priority Level:** 3 (dropdown). An arrow points to **Alternate Route**, which is set to <None>.
 - Alternate Route Wait Time:** 30 (spin box). An arrow points to **Alternate Route**, which is set to <None>.

If a primary route experiences a network outage such that no response is received to an outbound INVITE, IP Office successfully routes the call via the backup route. The user receives an audible tone when the re-routing occurs and may briefly see “Waiting for Line” on the display.

5.9. Save Configuration

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

The following will appear, with either **Merge** or **Immediate** selected, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** if desired.



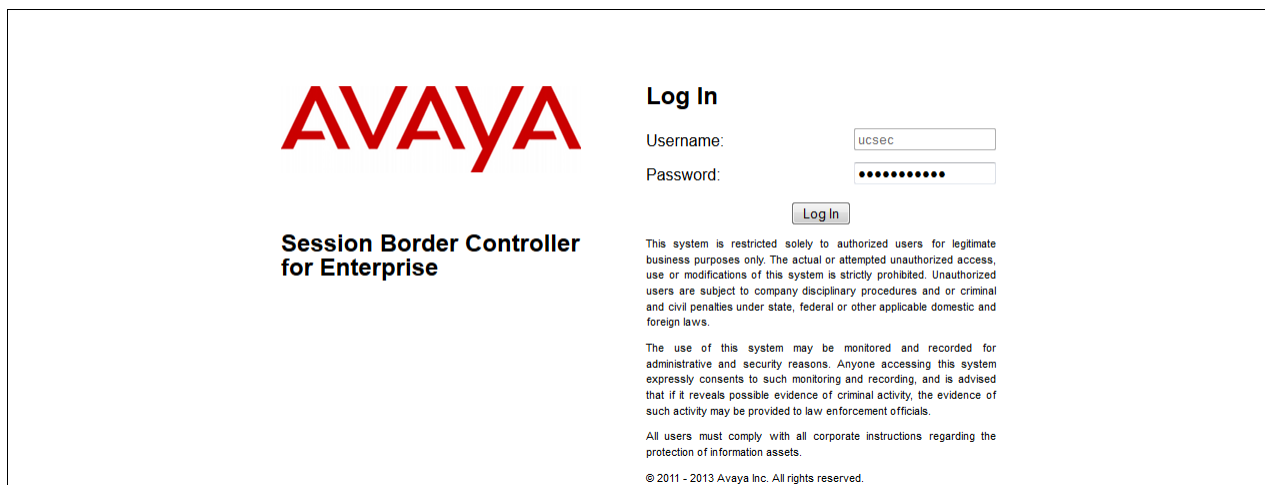
The image shows a 'Save Configuration' dialog box with a title bar containing minimize, maximize, and close buttons. The dialog is divided into several sections. The first section is 'IP Office Settings' with a text field containing 'SIL'. The second section is 'Configuration Reboot Mode' with four radio button options: 'Merge', 'Immediate' (which is selected), 'When Free', and 'Timed'. The third section is 'Reboot Time' with a time picker showing '12:40'. The fourth section is 'Call Barring' with two checkboxes: 'Incoming Calls' and 'Outgoing Calls', both of which are unchecked. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

6. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed.

Use a WEB browser to access the Element Management Server (EMS) web interface, and enter `https://ipaddress/sbc` in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE.

Log in with the appropriate credentials. Click **Log In**.



The login page features the Avaya logo on the left and a 'Log In' section on the right. The 'Log In' section includes a 'Username' field with the value 'ucsec', a 'Password' field with masked characters, and a 'Log In' button. Below the login fields, there is a disclaimer text block.

AVAYA

Log In

Username:

Password:

Session Border Controller for Enterprise

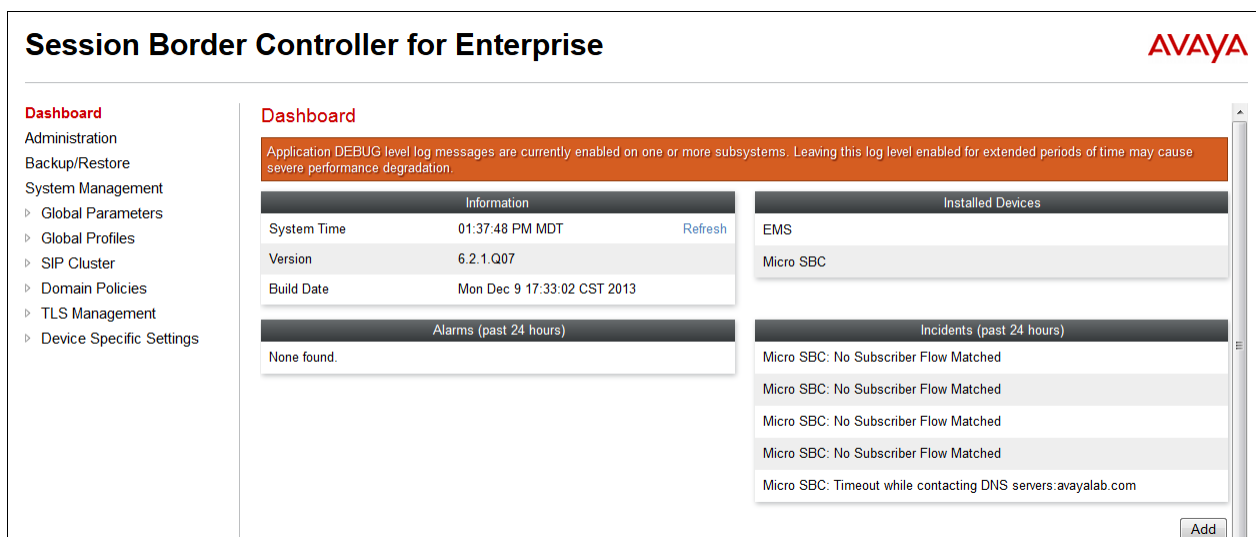
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under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

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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

The Dashboard for the Avaya SBCE will appear.



The dashboard displays system information, installed devices, and incidents. It includes a navigation menu on the left and a main content area with several sections.

Session Border Controller for Enterprise

AVAYA

Dashboard

Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation.

Information	
System Time	01:37:48 PM MDT Refresh
Version	6.2.1.Q07
Build Date	Mon Dec 9 17:33:02 CST 2013

Alarms (past 24 hours)	
None found.	

Installed Devices	
EMS	
Micro SBC	

Incidents (past 24 hours)	
Micro SBC:	No Subscriber Flow Matched
Micro SBC:	No Subscriber Flow Matched
Micro SBC:	No Subscriber Flow Matched
Micro SBC:	No Subscriber Flow Matched
Micro SBC:	Timeout while contacting DNS servers:avayalab.com

To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named “Micro SBC” is shown. To view the configuration of this device, click **View** as highlighted below.

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies

System Management

Devices
Updates
SSL VPN
Licensing

Device Name (Serial Number)	Management IP	Version	Status	
Micro SBC (IPCS11099999)	10.80.150.199	6.2.1.Q07	Commissioned	Reboot Shutdown Restart Application View Edit Delete

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Windstream. Other IP addresses assigned to these interfaces on the screen below are used to support remote workers and they are not discussed in these Application Notes.

System Information: Micro SBC

General Configuration

Appliance Name	Micro SBC
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.64.19.199	10.64.19.199	255.255.255.0	10.64.19.1	A1
192.168.62.123	192.168.62.123	255.255.255.128	192.168.62.1	B1
10.64.19.198	10.64.19.198	255.255.255.0	10.64.19.1	A1
192.168.62.72	192.168.62.72	255.255.255.128	192.168.62.1	B1
192.168.62.92	192.168.62.92	255.255.255.128	192.168.62.1	B1

DNS Configuration

Primary DNS	172.30.209.4
Secondary DNS	
DNS Location	DMZ

Management IP(s)

IP	10.80.150.199
----	---------------

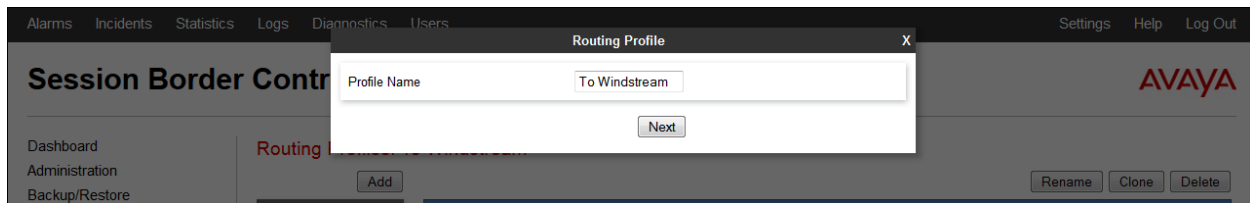
The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the enterprise interface is assigned to **A1** and the interface towards Windstream is assigned to **B1**.

The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click the corresponding **Toggle** button.

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include

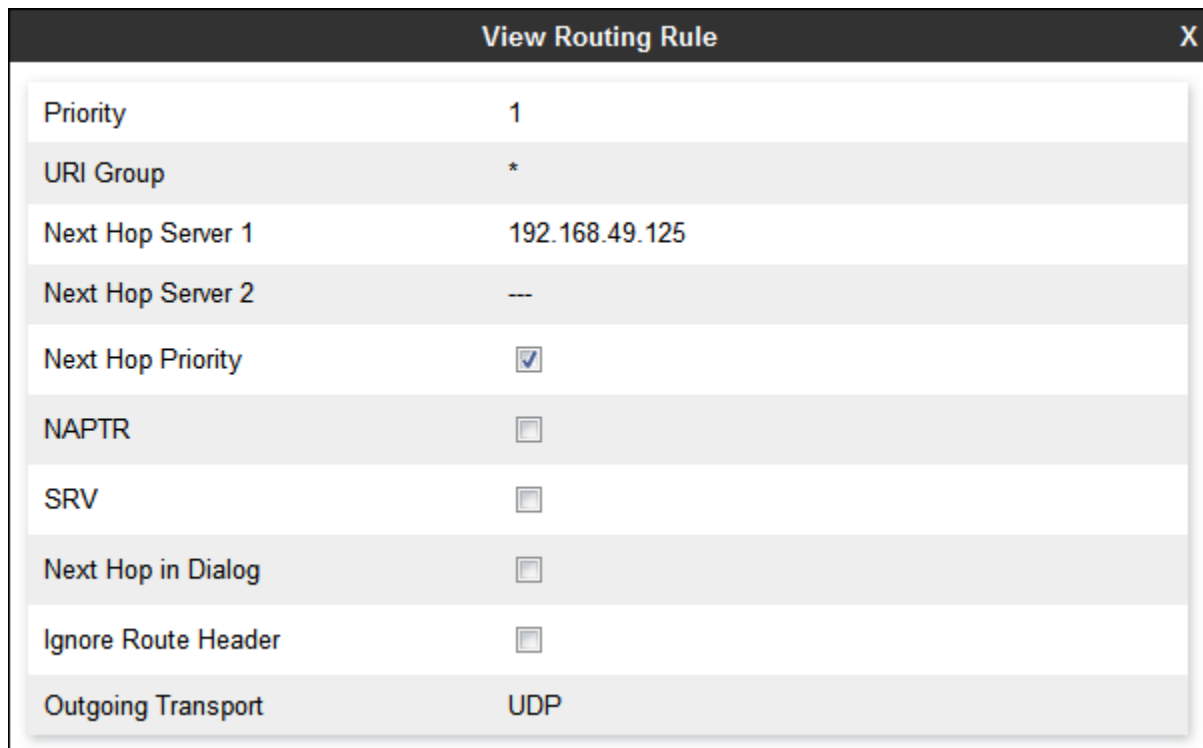
packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Create a Routing Profile for IP Office and Windstream. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.



The screenshot shows the Session Border Controller (SBC) interface. A modal dialog titled "Routing Profile" is open, allowing the user to create a new routing profile. The "Profile Name" field is populated with "To Windstream". A "Next" button is visible at the bottom of the dialog. In the background, the "Routing" section of the SBC interface is visible, showing a list of routing profiles and an "Add" button.

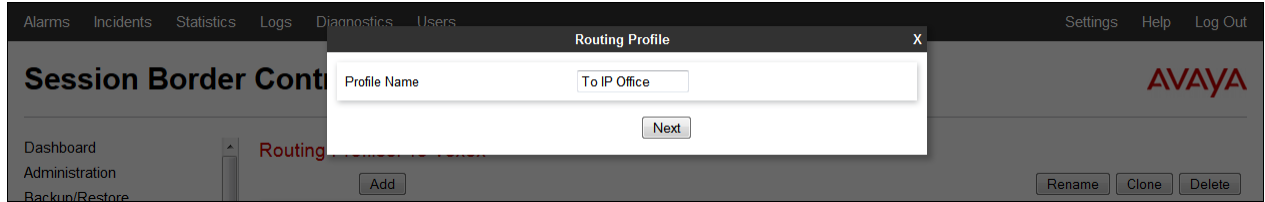
The following screen shows the Routing Profile to Windstream. In the **Next Hop Server 1** field enter the IP address that Windstream uses to listen for SIP traffic. In the sample configuration “192.168.49.125” is used. Verify **Next Hop Priority** is checked and enter “UDP” for the **Outgoing Transport** field.



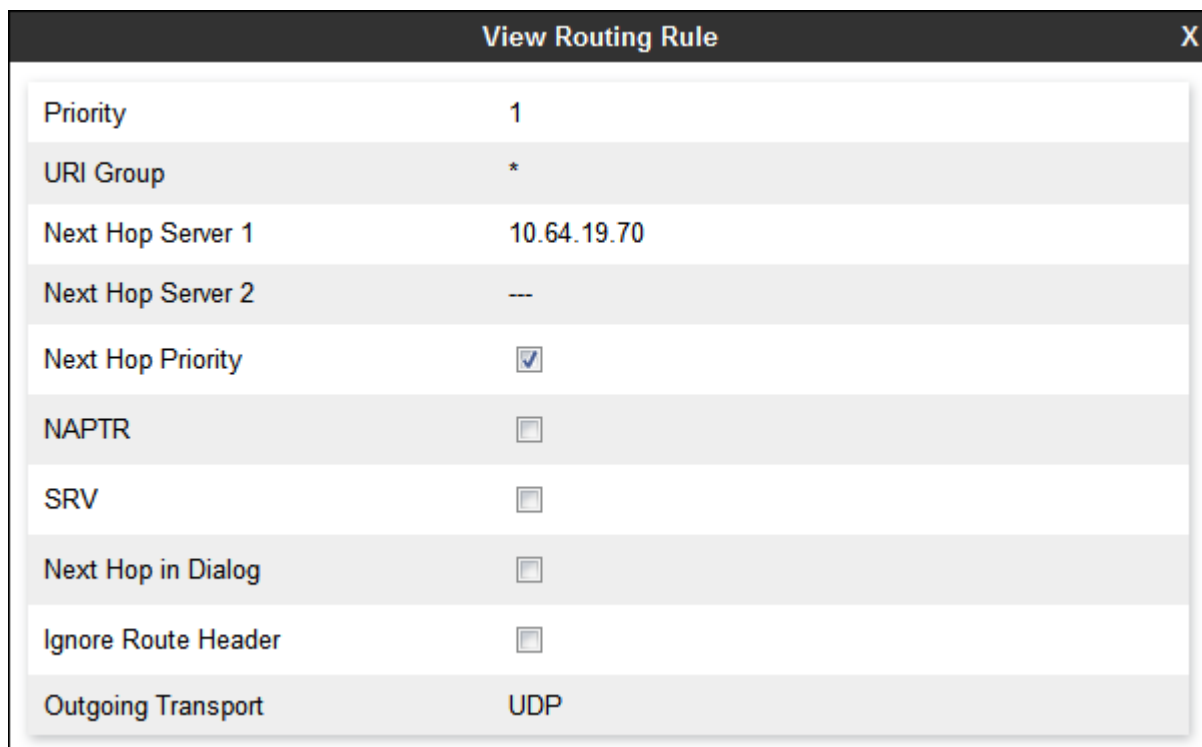
The screenshot shows the "View Routing Rule" dialog box. The dialog box displays the configuration for a routing rule. The "Priority" is 1, "URI Group" is *, "Next Hop Server 1" is 192.168.49.125, "Next Hop Server 2" is ---, "Next Hop Priority" is checked, "NAPTR" is unchecked, "SRV" is unchecked, "Next Hop in Dialog" is unchecked, "Ignore Route Header" is unchecked, and "Outgoing Transport" is UDP.

Field	Value
Priority	1
URI Group	*
Next Hop Server 1	192.168.49.125
Next Hop Server 2	---
Next Hop Priority	<input checked="" type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input type="checkbox"/>
Next Hop in Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>
Outgoing Transport	UDP

Similarly add a Routing Profile to IP Office.



The following screen shows the Routing Profile to IP Office. The **Next Hop Server 1** IP address must match the IP address of the IP Office LAN settings entered in **Section 5.2.1**. The **Outgoing Transport** is set to “UDP” and matches the **Layer 4 Protocol** set in IP Office **SIP Line → Transport** in **Section 5.4.3**.



View Routing Rule	
Priority	1
URI Group	*
Next Hop Server 1	10.64.19.70
Next Hop Server 2	---
Next Hop Priority	<input checked="" type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input type="checkbox"/>
Next Hop in Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>
Outgoing Transport	UDP

6.1. Topology Hiding Profile

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the sample configuration, the “default” profile is used for IP Office and Windstream.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), Signaling Manipulation, and URI Groups. The main content area is titled "Topology Hiding Profiles: default" and includes an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this, a table titled "Topology Hiding" displays the following data:

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

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

6.2. Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given flow through the Avaya SBCE web interface. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of Signaling Manipulation but will show an example of a script created during compliance testing. The sample script is used to remove a Remote-Address header from SIP messages (INVITE and 200 OK) originated from IP Office. This header needed to be removed since it could contain an IP address on the private enterprise network.

To create a new Signaling Manipulation, navigate to **Global Profiles → Signaling Manipulation** and click on **Add**. A new blank SigMa Editor window will pop up.

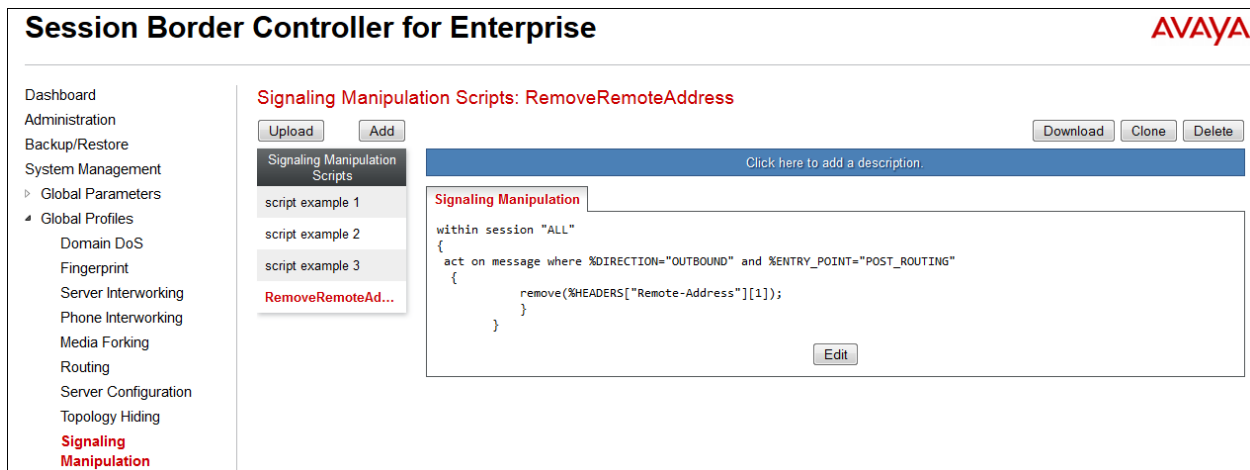


The following screen illustrates the “RemoveRemoteAddress” script.

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"][1]);
  }
}
```

In the Signaling Manipulation script above, the statement **act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"** specifies the portion of the script that will take effect on all outbound SIP messages and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

The following screen shows the finished Signaling Manipulation Script “RemoveRemoteAddress” used during compliance testing. This script will later be applied to the Windstream Server Configuration in **Section 6.4.2**



6.3. Server Interworking Profile

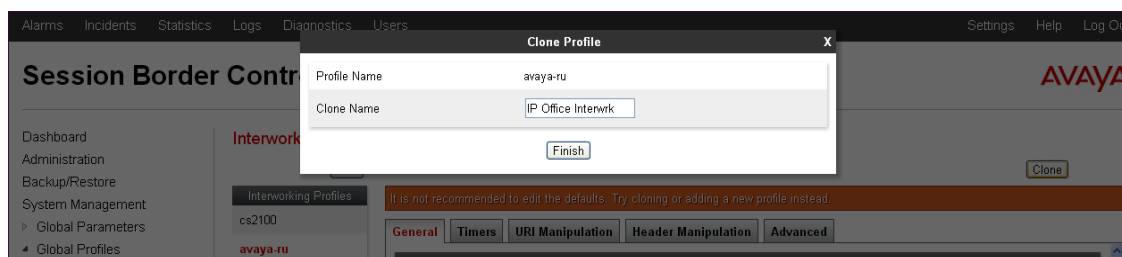
The Server Interworking profile configures and manages various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. Interworking Profile features are

configured based on different Trunk Servers. There are default profiles available that may be used as is, or new profiles can be configured as described below.

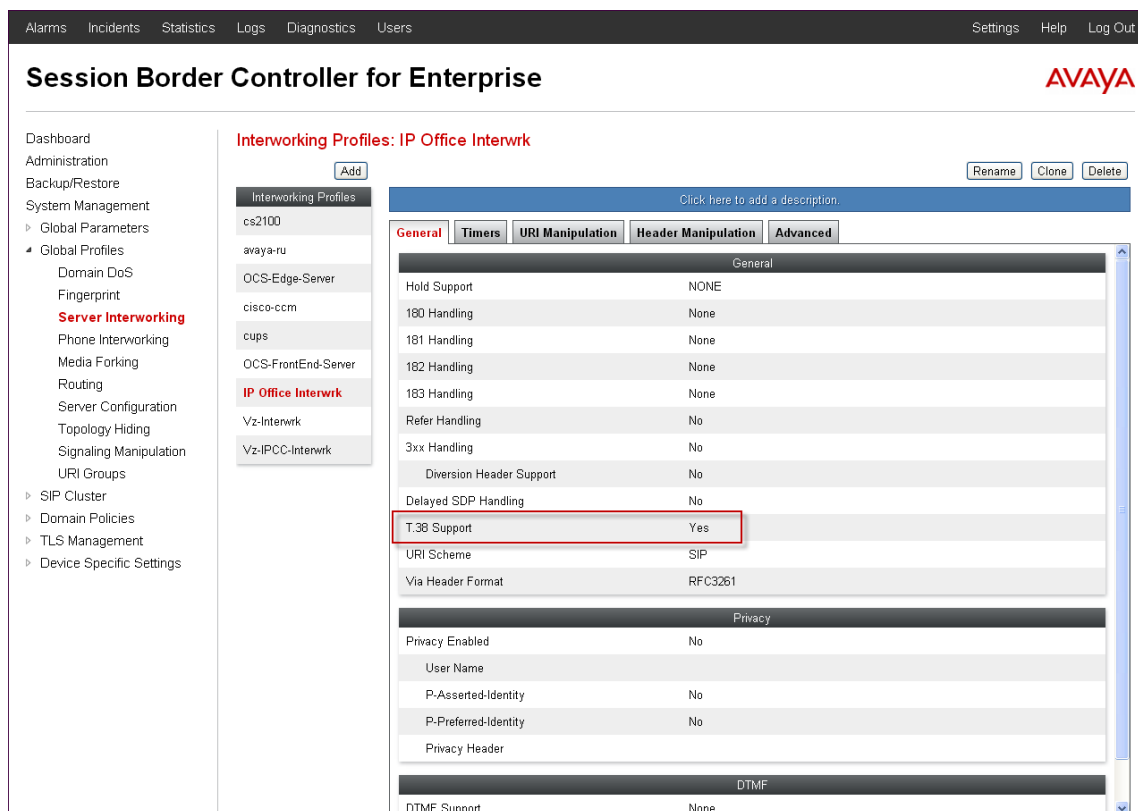
In the sample configuration, separate Server Interworking Profiles were created for IP Office and Windstream.

6.3.1. Server Interworking Profile – IP Office

In the sample configuration, the IP Office Server Interworking profile was cloned from the default “avaya-ru” profile. To clone a Server Interworking Profile for IP Office, navigate to **Global Profiles → Server Interworking**, select the “avaya-ru” profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.

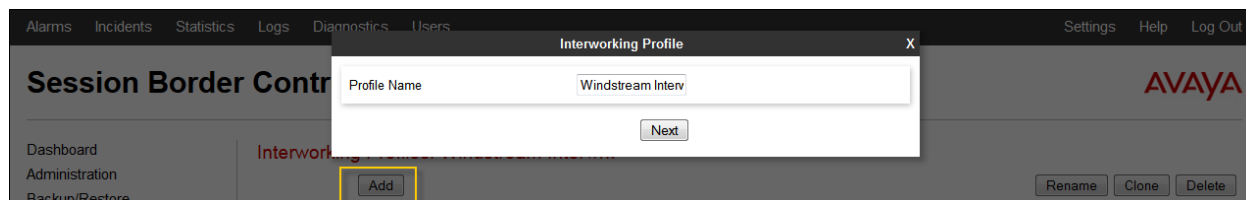


The following screen shows the “IP Office Interwrk” profile used in the sample configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to “Yes”. Default values can be used for all other fields.

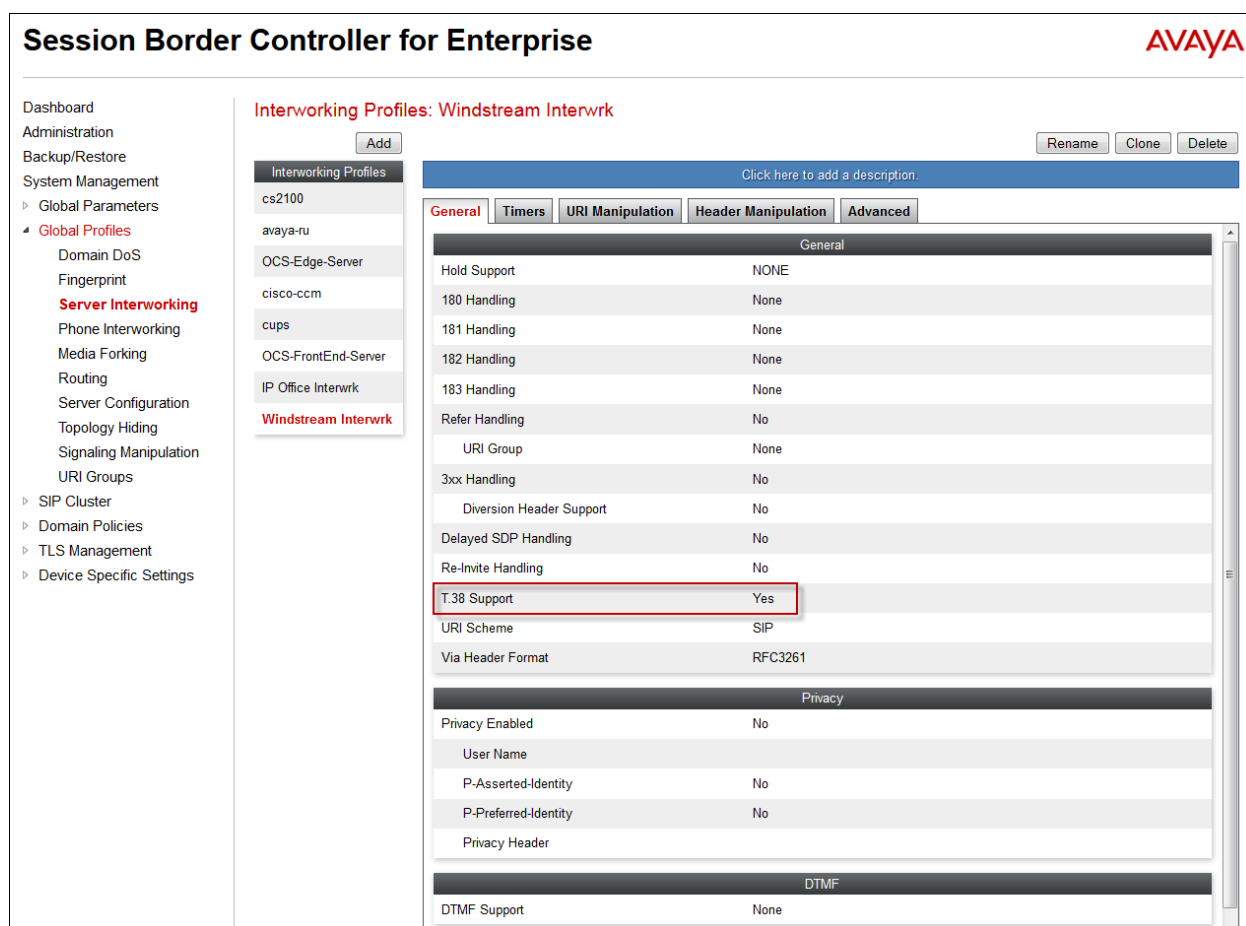


6.3.2. Server Interworking Profile – Windstream

To create a new Server Interworking Profile for Windstream, navigate to **Global Profiles** → **Server Interworking** and click **Add** as highlighted below. Enter a **Profile Name** and click **Next**.



The following screens show the “Windstream Interwrk” profile used in the sample configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to “Yes”. Default values can be used for all other fields.



The **Advanced** tab maintains the default settings.

The screenshot shows the 'Session Border Controller for Enterprise' configuration interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and SIP Cluster. The main content area is titled 'Interworking Profiles: Windstream Interwrk'. It features a list of profiles on the left, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-Server', 'IP Office Interwrk', and 'Windstream Interwrk'. The 'Windstream Interwrk' profile is selected, and its configuration is shown in the 'Advanced' tab. The configuration table lists various settings and their values:

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

6.4. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

In the sample configuration, separate Server Configurations were created for IP Office and Windstream.

6.4.1. Server Configuration – IP Office

To add a Server Configuration Profile for IP Office, navigate to **Global Profiles** → **Server Configuration** and click **Add**. Enter a descriptive name for the new profile and click **Next**.

The screenshot shows the 'Add Server Configuration Profile' dialog box. It has a title bar with 'Add Server Configuration Profile' and a close button (X). The dialog contains a 'Profile Name' label and a text input field with the value 'IP Office'. Below the input field is a 'Next' button. The background shows the 'Session Border Controller for Enterprise' interface with the 'Server Configuration' tab selected.

The following screens illustrate the Server Configuration for the Profile name “IP Office”. In the **General** parameters, the **Server Type** is set to “Call Server”. In the **IP Addresses / FQDNs** area, the IP address of the IP Office LAN 1 interface in the sample configuration is entered. This IP address is 10.64.19.70. In the **Supported Transports** area, “TCP” and “UDP” are selected, and the **TCP Port** and **UDP Port** are set to “5060”. The UDP port is used for SIP trunking, while the TCP port is for remote SIP end-points.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
 ▸ Global Parameters
 ▾ Global Profiles
 Domain DoS
 Fingerprint
 Server Interworking
 Phone Interworking
 Media Forking
 Routing
 Server Configuration

Server Configuration: IP Office Add Rename Clone Delete

Server Profiles
 IP Office
 Windstream

General Authentication Heartbeat Advanced

Server Type	Call Server
IP Addresses / FQDNs	10.64.19.70
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

Edit

Default values can be used on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, **Enable Grooming** can be selected to allow the same TCP connection to be used for all SIP messages from this device. In the sample configuration, this server configuration is also used for remote workers and IP Office uses different TCP connections to each endpoint, therefore “Grooming” is disabled. The **Interworking Profile** is set to “IP Office Interwrk” created in **Section 6.3.1** for IP Office.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
 ▸ Global Parameters
 ▾ Global Profiles
 Domain DoS
 Fingerprint
 Server Interworking
 Phone Interworking
 Media Forking
 Routing
 Server Configuration
 Topology Hiding

Server Configuration: IP Office Add Rename Clone Delete

Server Profiles
 IP Office
 Windstream

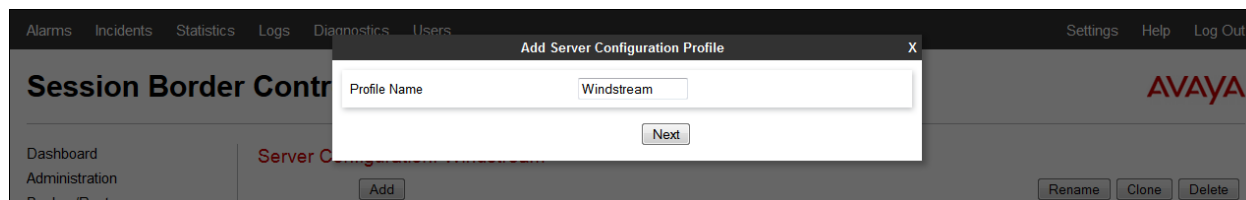
General Authentication Heartbeat **Advanced**

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	IP Office Interwrk
Signaling Manipulation Script	None
TCP Connection Type	SUBID
UDP Connection Type	SUBID

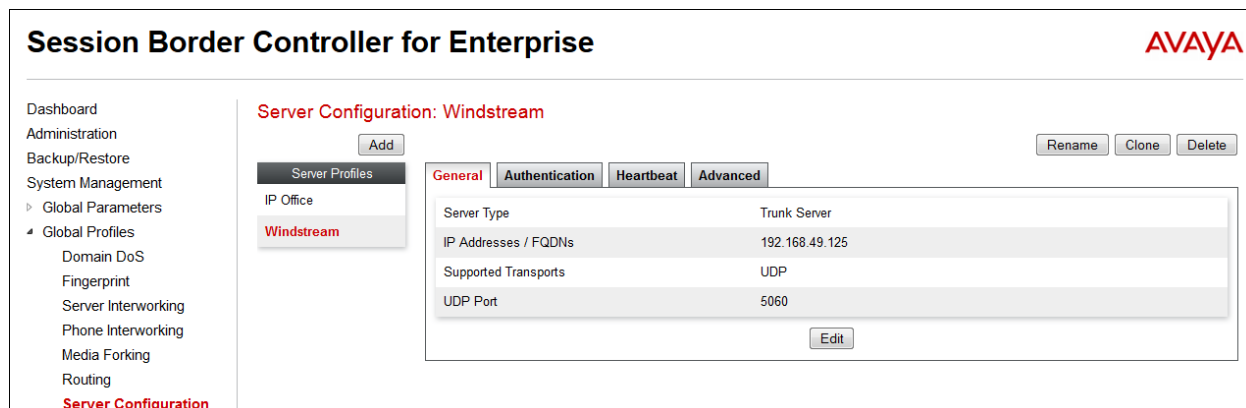
Edit

6.4.2. Server Configuration - Windstream

To add a Server Configuration Profile for Windstream, navigate to **Global Profiles → Server Configuration** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



The following screens illustrate the Server Configuration for the Profile name “Windstream”. In the **General** parameters, the **Server Type** is set to “Trunk Server”. In the **IP Addresses / FQDNs** area, the Windstream provided IP address is entered. This is “192.168.49.125”. In the **Supported Transports** area, “UDP” is selected, and the **UDP Port** is set to “5060”.



Default values can be used on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and left unchecked. The **Interworking Profile** is set to “Windstream-Interwrk” created in **Section 6.3.2** for Windstream. For **Signaling Manipulation Script**, select the script created in **Section 6.2**.

The screenshot shows the 'Session Border Controller for Enterprise' configuration interface. The left sidebar lists various configuration areas, with 'Server Configuration' highlighted. The main panel is titled 'Server Configuration: Windstream' and includes tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'Advanced' tab is selected, showing settings for 'Enable DoS Protection', 'Enable Grooming', 'Interworking Profile' (set to 'Windstream Interwrk'), 'Signaling Manipulation Script' (set to 'RemoveRemoteAddress'), and 'UDP Connection Type' (set to 'SUBID'). A red box highlights the 'Interworking Profile' and 'Signaling Manipulation Script' fields.

6.5. Media Rule

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

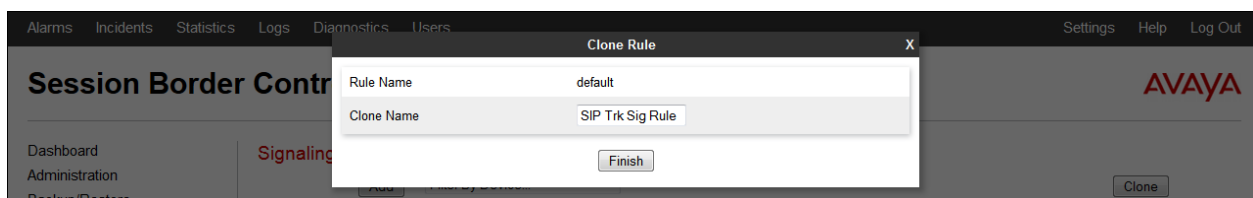
Select **Domain Policies** → **Media Rules** from the left-side menu as shown below. In the sample configuration, a single default media rule “default-low-med” is used with the DSCP values “EF” for expedited forwarding (default value) for **Media QoS** as shown below.

The screenshot shows the 'Session Border Controller for Enterprise' configuration interface. The left sidebar lists various configuration areas, with 'Domain Policies' → 'Media Rules' highlighted. The main panel is titled 'Media Rules: default-low-med' and includes tabs for 'Media NAT', 'Media Encryption', 'Media Anomaly', 'Media Silencing', and 'Media QoS'. The 'Media QoS' tab is selected, showing settings for 'Media QoS Reporting' (RTCP Enabled), 'Media QoS Marking' (Enabled, QoS Type DSCP), 'Audio QoS' (Audio DSCP EF), and 'Video QoS' (Video DSCP EF). A red box highlights the 'Media QoS Marking' section.

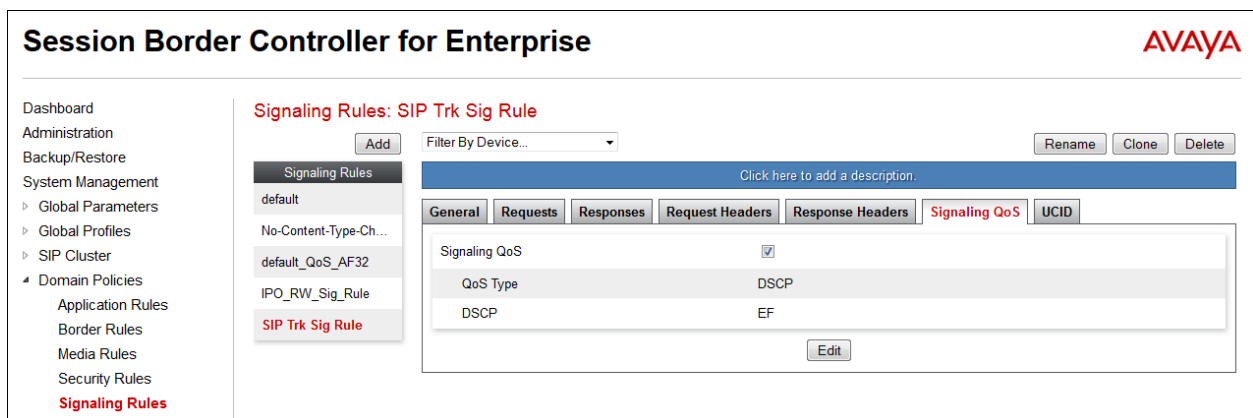
6.6. Signaling Rule

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Clone and modify the default signaling rule to add the proper quality of service to the SIP signaling. To clone a signaling rule, navigate to **Domain Policies** → **Signaling Rules**. With the **default** rule chosen, click **Clone** (not shown). Enter a descriptive name for the new rule and click **Finish**.



In the sample configuration, signaling rule “SIP Trk Sig Rule” is used with the DSCP values “EF” for expedited forwarding set for **Signaling QoS** as shown below.



6.7. Application Rule

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

Select **Domain Policies** → **Application Rules** from the left-side menu as shown below. In the sample configuration, a single default application rule “default-trunk” is used and will be applied to the Endpoint Policy Group in the next section.

Alarms
Incidents
Statistics
Logs
Diagnostics
Users

Settings
Help
Log Out

Session Border Controller for Enterprise

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

Application Rules: default-trunk

Add
Filter By Device...
Clone

Application Rules

default
default-trunk
default-subscriber-low
default-subscriber-high
default-server-low
default-server-high
IPO_RW_app_rule

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

6.8. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 6.11**.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** as highlighted below. The following screen shows the “SIP-Trunk-Policy” with defaults selected for all fields, with the exception of **Application** set to “default-trunk”, and **Signaling**, which is set to “SIP Trk Sig Rule” as shown below. The details of the non-default rules chosen are shown in previous sections.

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

Policy Groups: SIP-Trunk-Policy

Add
Filter By Device...
Rename
Clone
Delete

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary Add

Order	Application	Border	Media	Security	Signaling	Time of Day
1	default-trunk	default	default-low-med	default-low	SIP Trk Sig Rule	default

Edit Clone

6.9. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP media interface for the inside and outside IP interfaces.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**. Enter a descriptive name and select the corresponding **IP Address** from the drop-down box and select **Finish** (not shown). The following screen shows the media interfaces defined for the sample configuration.

The screenshot shows the 'Media Interface: Micro SBC' configuration page. On the left is a navigation menu with 'Media Interface' selected. The main area has a 'Media Interface' tab and a table of configured interfaces. A red box highlights the first two rows of the table.

Name	Media IP	Port Range	
SIP Trk Media Inside	10.64.19.199	35000 - 40000	Edit Delete
SIP Trk Media Outside	192.168.62.123	35000 - 40000	Edit Delete
RW Media Outside	192.168.62.92	35000 - 40000	Edit Delete
RW Media Inside	10.64.19.198	35000 - 40000	Edit Delete

6.10. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a signaling interface for the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add**. Enter a descriptive name and select the corresponding **IP Address** from the drop-down box and enter “5060” for the **UDP Port** (not shown). Select **Finish** (not shown). The following screen shows the signaling interfaces defined for the sample configuration.

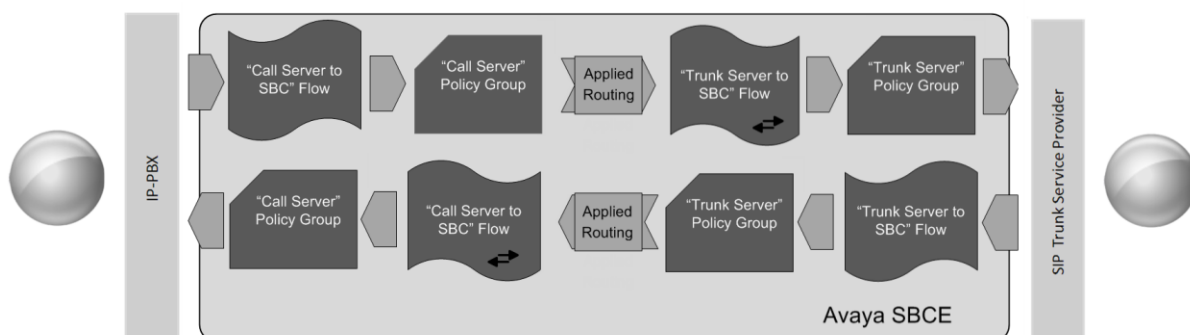
The screenshot shows the 'Signaling Interface: Micro SBC' configuration page. On the left is a navigation menu with 'Signaling Interface' selected. The main area has a 'Signaling Interface' tab and a table of configured interfaces. A red box highlights the first two rows of the table.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
SIP Trk Sig Inside	10.64.19.199	---	5060	---	None	Edit Delete
SIP Trk Sig Outside	192.168.62.123	---	5060	---	None	Edit Delete
RW Sig Outside-92	192.168.62.92	5060	---	5061	AvayaSBCServer	Edit Delete
RW Sig Inside-198	10.64.19.198	5060	---	---	None	Edit Delete

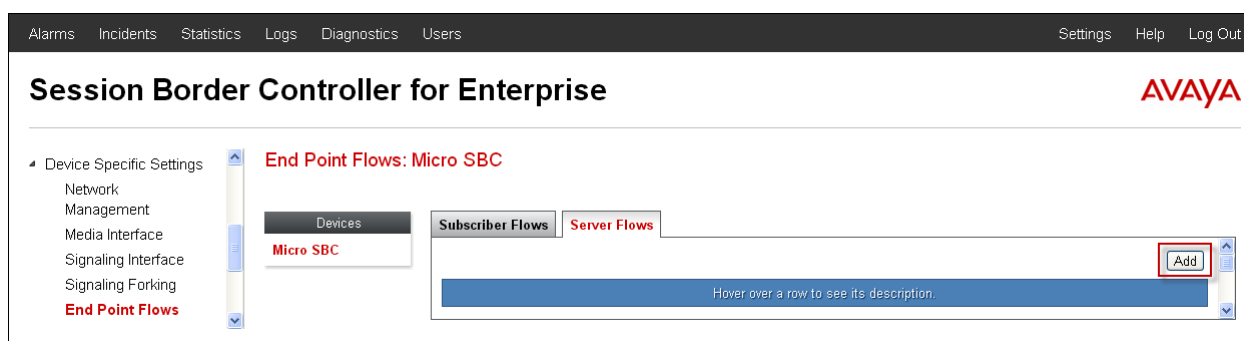
6.11. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing,

etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the SBC to secure a SIP Trunk call.



Create a Server Flow for IP Office and Windstream. To create a Server Flow, navigate to **Device Specific Settings** → **End Point Flows**. Select the **Server Flows** tab and click **Add** as highlighted below.



The following screen shows the flow named “Windstream Flow” viewed from the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections.

Criteria		Profile	
Flow Name	Windstream Flow	Signaling Interface	SIP Trk Sig Outside
Server Configuration	Windstream	Media Interface	SIP Trk Media Outside
URI Group	*	End Point Policy Group	SIP-Trunk-Policy
Transport	*	Routing Profile	To IP Office
Remote Subnet	*	Topology Hiding Profile	default
Received Interface	SIP Trk Sig Inside	File Transfer Profile	None

Once again, select the **Server Flows** tab and click **Add**. The following screen shows the flow named “IP Office SIP Trunk Flow” viewed from the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections.

View Flow: IP Office SIP Trunk Flow					
Criteria			Profile		
Flow Name	IP Office SIP Trunk Flow		Signaling Interface	SIP Trk Sig Inside	
Server Configuration	IP Office		Media Interface	SIP Trk Media Inside	
URI Group	*		End Point Policy Group	SIP-Trunk-Policy	
Transport	*		Routing Profile	To Windstream	
Remote Subnet	*		Topology Hiding Profile	default	
Received Interface	SIP Trk Sig Outside		File Transfer Profile	None	

The following screen summarizes the Server Flows configured in the sample configuration.

Session Border Controller for Enterprise

AVAYA

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

End Point Flows: Micro SBC

Devices

Micro SBC

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: IP Office

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IP Office SIP Trunk Flow	*	SIP Trk Sig Outside	SIP Trk Sig Inside	SIP-Trunk-Policy	To Windstream	View Clone Edit Delete
2	Remote Worker	*	RW Sig Outside-92	RW Sig Inside-198	default-low	default	View Clone Edit Delete

Server Configuration: Windstream

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Windstream Flow	*	SIP Trk Sig Inside	SIP Trk Sig Outside	SIP-Trunk-Policy	To IP Office	View Clone Edit Delete

DDT; Reviewed:
SPOC 6/10/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

52 of 59
WindsIPO9SBCE62

7. Windstream Configuration

Windstream is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise site (i.e., the IP address of the public interface on the Avaya SBCE). Windstream will provide the customer the necessary information to configure the Avaya IP Office and Avaya SBCE including:

- Network edge IP addresses of the Windstream SIP Trunking Service
- Transport and port for the Windstream SIP Trunking connection to the Avaya SBCE at the enterprise
- DID numbers to assign to users at the enterprise
- Supported codecs and their preference order

8. Verification Steps

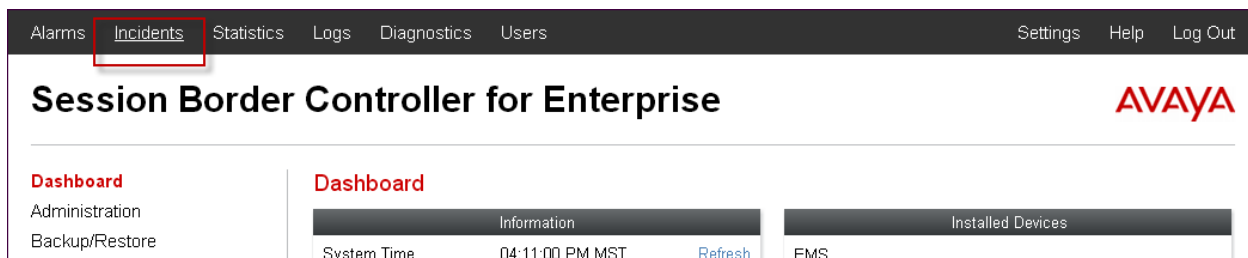
This section provides example verifications of the Avaya configuration with Windstream SIP Trunk service.

8.1. Avaya SBCE

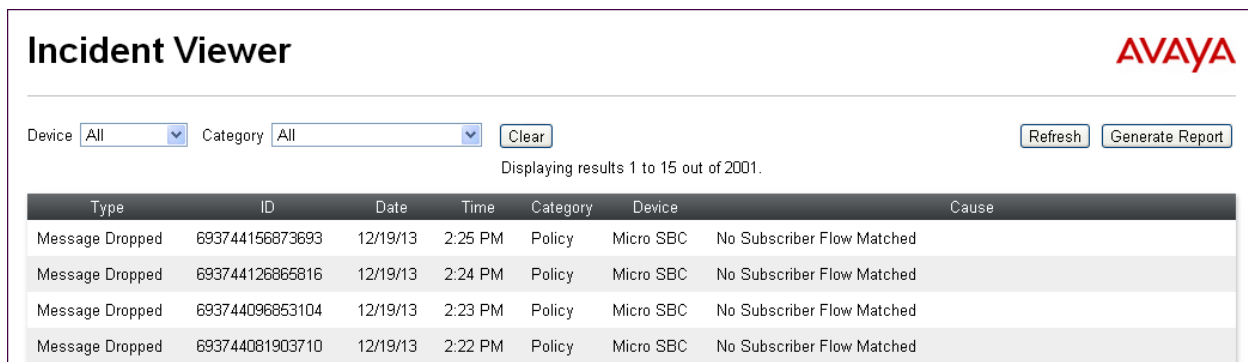
This section provides verification steps that may be performed with the Avaya SBCE.

8.1.1. Incidents

The Incident Viewer can be accessed from the Avaya SBCE Dashboard as highlighted in the screen shot below.



Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.



Type	ID	Date	Time	Category	Device	Cause
Message Dropped	693744156873693	12/19/13	2:25 PM	Policy	Micro SBC	No Subscriber Flow Matched
Message Dropped	693744126865816	12/19/13	2:24 PM	Policy	Micro SBC	No Subscriber Flow Matched
Message Dropped	693744096853104	12/19/13	2:23 PM	Policy	Micro SBC	No Subscriber Flow Matched
Message Dropped	693744081903710	12/19/13	2:22 PM	Policy	Micro SBC	No Subscriber Flow Matched

8.1.2. Tracing

To take a call trace, navigate to **Device Specific Settings** → **Troubleshooting** → **Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, Signaling Interface, Signaling Forking, End Point Flows, Session Flows, Relay Services, SNMP, Syslog Management, Advanced Options, and Troubleshooting (expanded). Under Troubleshooting, the following items are listed: Debugging, Trace (highlighted in red), DoS, and Learning. The main content area is titled "Trace: Micro SBC" and contains a "Devices" tab with "Micro SBC" selected. Below this is a "Packet Capture Configuration" form with the following fields: Status (Ready), Interface (A1), Local Address (10.64.19.199), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (1000), and Capture Filename (IPO-test.pcap). The form also includes "Start Capture" and "Clear" buttons.

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface, similar to the previous one, but with the "Trace" option highlighted in red in the sidebar. The main content area is titled "Trace: Micro SBC" and contains a "Devices" tab with "Micro SBC" selected. Below this is a "Packet Capture Configuration" form. At the top of the form, a blue banner states: "A packet capture is currently in progress. This page will automatically refresh until the capture completes." The form fields are: Status (In Progress), Interface (A1), Local Address (10.64.19.199), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (1000), and Capture Filename (IPO-test.pcap). The form also includes a "Stop Capture" button.

Select the **Captures** tab to view the files created during the packet capture.

Session Border Controller for Enterprise

Media Interface

Signaling Interface

Signaling Forking

End Point Flows

Session Flows

Relay Services

SNMP

Syslog Management

Advanced Options

Troubleshooting

Debugging

Trace

Trace: Micro SBC

Devices

Micro SBC

Call Trace

Packet Capture

Captures

Last Modified

Descending

Sort

Reset

Refresh

File Name	File Size (bytes)	Last Modified	
IPO-test_20140327161355.pcap	4,096	March 27, 2014 4:14:30 PM MDT	Delete
DSCPVerification_20131219142811.pcap	95,520	December 19, 2013 2:28:41 PM MST	Delete
test-trace_20130204084632.pcap	4,096	February 4, 2013 8:47:00 AM MST	Delete

The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like Wireshark.

IPO-test_20140327162038.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: sip Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
5	10.155603	10.80.150.70	10.64.19.199	SIP/SDP	942	Request: INVITE sip:13035551000@10.64.19.199
7	10.159213	10.64.19.199	10.80.150.70	SIP	359	Status: 100 Trying
10	10.274944	10.64.19.199	10.80.150.70	SIP	585	Status: 180 Ringing
12	10.562420	10.64.19.199	10.80.150.70	SDP	544	Status: 502 No Route

Frame 5: 942 bytes on wire (7536 bits), 942 bytes captured (7536 bits)

Ethernet II, Src: Avaya_a3:a2:1c (90:fb:5b:a3:a2:1c), Dst: Portwell_13:45:b:c6 (00:90:fb:34:5b:c6)

Internet Protocol Version 4, Src: 10.80.150.70 (10.80.150.70), Dst: 10.64.19.199 (10.64.19.199)

Transmission Control Protocol, Src Port: 1go-incognito (4100), Dst Port: sip (5060), Seq: 1, Ack: 1, Len: 888

Session Initiation Protocol (INVITE)

Request-Line: INVITE sip:13035551000@10.64.19.199 SIP/2.0

Message Header

Via: SIP/2.0/TCP 10.80.150.70:5060;rport;branch=z9hG4bK64ec004b8323e47c839464d8f489ae96

From: "Avaya9508" <sip:13605554982@10.64.19.199>;tag=64e4e1343d73eda1

To: <sip:13035551000@10.64.19.199>

Call-ID: 6cf394c2755b6dd4e9ea7a75a8fa2509

CSeq: 1225937205 INVITE

Contact: "Avaya9508" <sip:13605554982@10.80.150.70:5060;transport=tcp>

Max-Forwards: 70

Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY

Content-Type: application/sdp

Supported: timer

Min-SE: 1200

Session-Expires: 1200;refresher=uac

User-Agent: IP office 9.0.1.0 build 845

Content-Length: 275

Message Body

Session Description Protocol

Session Description Protocol version (v): 0

Owner/Creator, Session Id (o): UserA 2395131953 2665571401 IN IP4 10.80.150.70

Session Name (s): Session SDP

Connection Information (c): IN IP4 10.80.150.70

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 49152 RTP/AVP 9 18 0 101

Media Attribute (a): rtpmap:9 G722/8000

Media Attribute (a): rtpmap:18 G729/8000

Media Attribute (a): fmtp:18 annexb=no

Media Attribute (a): rtpmap:0 PCMU/8000

Media Attribute (a): rtpmap:101 telephone-event/8000

Media Attribute (a): fmtp:101 0-15

DDT; Reviewed:
SPOC 6/10/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

55 of 59
WindsIPO9SBCE62

8.2. IP Office

The following steps may be used to verify the configuration:

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Manager was installed. Select the SIP line of interest from the left pane. On the **Status** tab in the right pane, verify that the Current Stat for each channel (The following screen shot shows an active call).

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
Alarms (1)
Extensions (19)
Trunks (6)
Lines: 5 - 8
Line: 17
Line: 18
Active Calls
Resources
Voicemail
IP Networking
Locations

Status Utilization Summary Alarms

SIP Trunk Summary

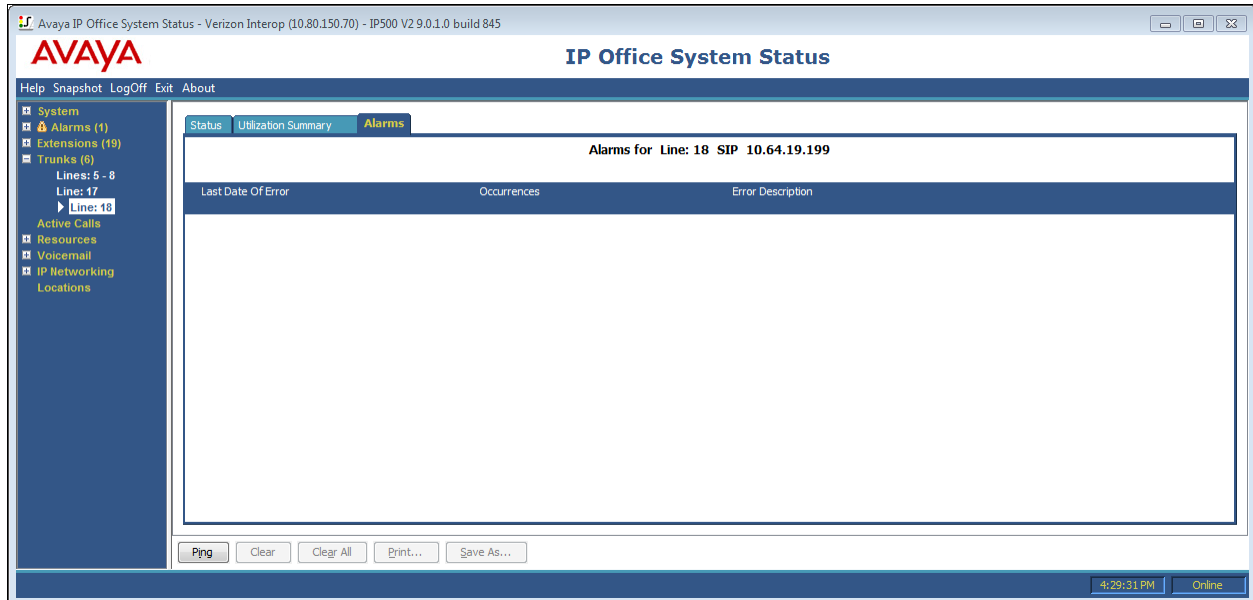
Peer Domain Name: 10.64.19.199
Resolved Address: 10.64.19.199
Line Number: 18
Number of Administered Channels: 50
Number of Channels in Use: 1
Administered Compression: G711 Mu, G729 A
Silence Suppression: Off
Layer 4 Protocol: TCP
SIP Trunk Channel Licenses: 5
SIP Trunk Channel Licenses in Use: 1
SIP Device Features: 20%

Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Lo...	Transmit Jitter	Transmit Packet Lo...
1	0	8	Connected	00:00:10	10.64.19.199	G711...	VCM		Extn 232, Avaya9508	Outgoing	0ms	0.4ms	0%	0ms	0%
2			Idle	01:14:57											
3			Idle	01:14:57											
4			Idle	01:14:57											
5			Idle	01:14:57											
6			Idle	01:14:57											

Trace Trace All Pause Ping Call Details Print... Save As...

4:28:47 PM Online

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



9. Conclusion

IP Office is a highly modular IP telephone system designed to meet the needs of home offices, standalone businesses, and networked branch and head offices for small and medium enterprises. These Application Notes demonstrated how IP Office Release 9.0 can be successfully combined with Avaya Session Border Controller and a Windstream SIP Trunk service connection to create an end-to-end SIP Telephony business solution. By following the example configurations provided in this document, customers using Avaya IP Office and Avaya Session Border Controller can connect to the PSTN via a Windstream SIP Trunk service connection, thus eliminating the costs of analog or digital trunk connections previously required to access the PSTN. Utilizing this solution, IP Office customers can leverage the operational efficiencies and cost savings associated with SIP trunking while gaining the advanced technical features provided through the marriage of best of breed technologies from Avaya and Windstream.

10. Additional References

This section references documentation relevant to these Application Notes. In general, Avaya product documentation is available at <http://support.avaya.com>

- [1] *IP Office 9.0 Installing IP500/IP 500 V2*, Document Number 15-601042, November 2013
- [2] *IP Office Manager*, Document Number 15-601011, November 2013
- [3] *IP Office Application server 9.0 Installation and Maintenance*, August 2013
- [4] *IP Office 9.0 Using System Status*, Document Number 15-601758, August 2013
- [5] *Administering Avaya Flare® Experience for iPad Devices and Windows*, September 2013
- [6] *Configuring the Avaya Session Border Controller for IP office Remote Workers*, Sept 2013
- [7] *Installing Avaya Session Border Controller for Enterprise*, June 2013
- [8] *Administering Avaya Session Border Controller*, December 2013
- [9] RFC 3261 *SIP: Session Initiation Protocol* <http://www.ietf.org/rfc/rfc3261.txt>

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

©2014 Avaya Inc. All Rights Reserved.

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

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