



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring the Cogeco SIP Trunking Service with Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise 6.2 – Issue 1.0**

### **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Cogeco and an enterprise solution using Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise 6.2.

The Cogeco SIP Trunking Service provides PSTN access via a SIP trunk between the enterprise and the Cogeco network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise. Cogeco is a member of the Avaya DevConnect Service Provider program.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describes the steps to configure Session Initiation Protocol (SIP) Trunking between Cogeco and an enterprise solution using Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise 6.2.

The Cogeco SIP Trunking Service referenced within these Application Notes is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

The Cogeco SIP Trunking Service will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE).

## 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Cogeco SIP Trunking Service 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 for Enterprise (Avaya SBCE) and various Avaya endpoints listed in **Section 4**.

The Cogeco SIP Trunking Service passed compliance testing with observations/limitations described in **Section 2.2**.

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:

- Registration of the SIP line with the service provider
- Sending/receiving SIP OPTIONS queries to/from the service provider
- Incoming PSTN calls (via the Cogeco SIP trunk) to SIP and H.323 telephones at the enterprise
- Outgoing PSTN calls (via the Cogeco SIP trunk) from SIP and H.323 telephones at the enterprise
- Inbound and outbound PSTN calls to/from soft clients (Avaya IP Office Video Softphone and Avaya Flare® Experience for Windows)

- Various call types including: local (10 digits), long distance (1 + 10 digits), outbound toll-free, international (011 + country code + number), operator, operator-assisted (0 + 10 digits) and local directory assistance (411)
- Codec G.711MU
- T.38 Fax
- Caller ID presentation and Caller ID restriction
- DTMF transmission using RFC 2833
- Response to incomplete call attempts and trunk errors
- Voicemail navigation using DTMF input for inbound and outbound calls
- Voicemail message waiting indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and twinning
- REFER message for call redirection
- Direct media
- Remote worker

Emergency calls (911) and inbound toll-free calls are supported but were not tested as part of the compliance test.

The following item is not supported:

- G.729 codec

In addition, the Cogeco SIP Trunking Service requires the following behavior in the SIP messaging:

- Eleven (1+10) digits must be sent in the Request-URI and To headers of an outbound SIP INVITE message for long distance calls and 10 digits must be sent for local calls. International calls are dialed with 011 as the international dialing prefix for North America followed by the country code and then the number. See related routing in **Sections 5.5 and 5.6**.
- As a best practice, the Uniform Resource Identifier (URI) of the P-Asserted-Identity (PAI) header in an outbound SIP message should contain the pilot number as the host and the Cogeco provided domain as the domain (instead of the local IP address). See configuration in **Sections 5.4.4, and 5.4.6**.

## 2.2. Test Results

Interoperability testing of the Cogeco SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **“Ring No Answer” call from analog PSTN phone:** If an inbound call from an analog PSTN phone to an enterprise extension is allowed to “ring no answer” for roughly 3 minutes (until the timer expires) then both parties should be disconnected. However, it was observed that the enterprise destination was disconnected but the PSTN caller

remained connected and continued to hear ringing. Troubleshooting indicated that this most likely was an issue with an upstream provider beyond Cogeco's network. In general, this issue would not impact a customer since it would be rare that calls are allowed to ring for 3 minutes. In addition, the PSTN caller can hang up the line to clear the call. If it should occur at a customer site, Cogeco would work with all upstream providers to resolve the issue.

- **No matching codec condition returns a 480 response:** In the case where the enterprise is misconfigured so that it does not use any codec shared by Cogeco, an outbound call from the enterprise will result in Cogeco returning a "480 Temporarily Unavailable" response instead of a "488 Not Acceptable Here". This behavior has no impact on the caller. The caller still hears an error treatment.
- **Operator-assisted calls fail:** Operator-assisted calls (0 + 10 digits) placed from the enterprise do not connect. The caller hears an error announcement. This issue is under investigation by Cogeco.
- **Call Forwarding and EC500:** For inbound PSTN calls that were forwarded back to the PSTN or ring to an EC500 (enterprise mobility) PSTN endpoint, the PSTN destination phone display (if equipped) showed the forwarding party/EC500 host instead of the original PSTN caller. A SIP header manipulation was added on the Avaya SBCE to correct the phone display to show the original PSTN caller. See **Section 6.6.1** for details.
- **T.38 Fax – Network Coverage:** Not all media gateways in the Cogeco network support T.38 fax. Avaya IP Office supports fallback to G.711 pass-through fax from T.38 fax if configured on the SIP Line form (**See Section 5.4.5**). This is the recommended setting if all gateways in the service provider network do not support T.38 fax.
- **Conferencing with IP Office Video Softphone:** IP Office Video Softphone calls a PSTN phone or internal extension and then conferences in another internal extension. This call scenario intermittently fails to conference all parties. This is not related to the interoperability test and is under investigation by Avaya.

## 2.3. Support

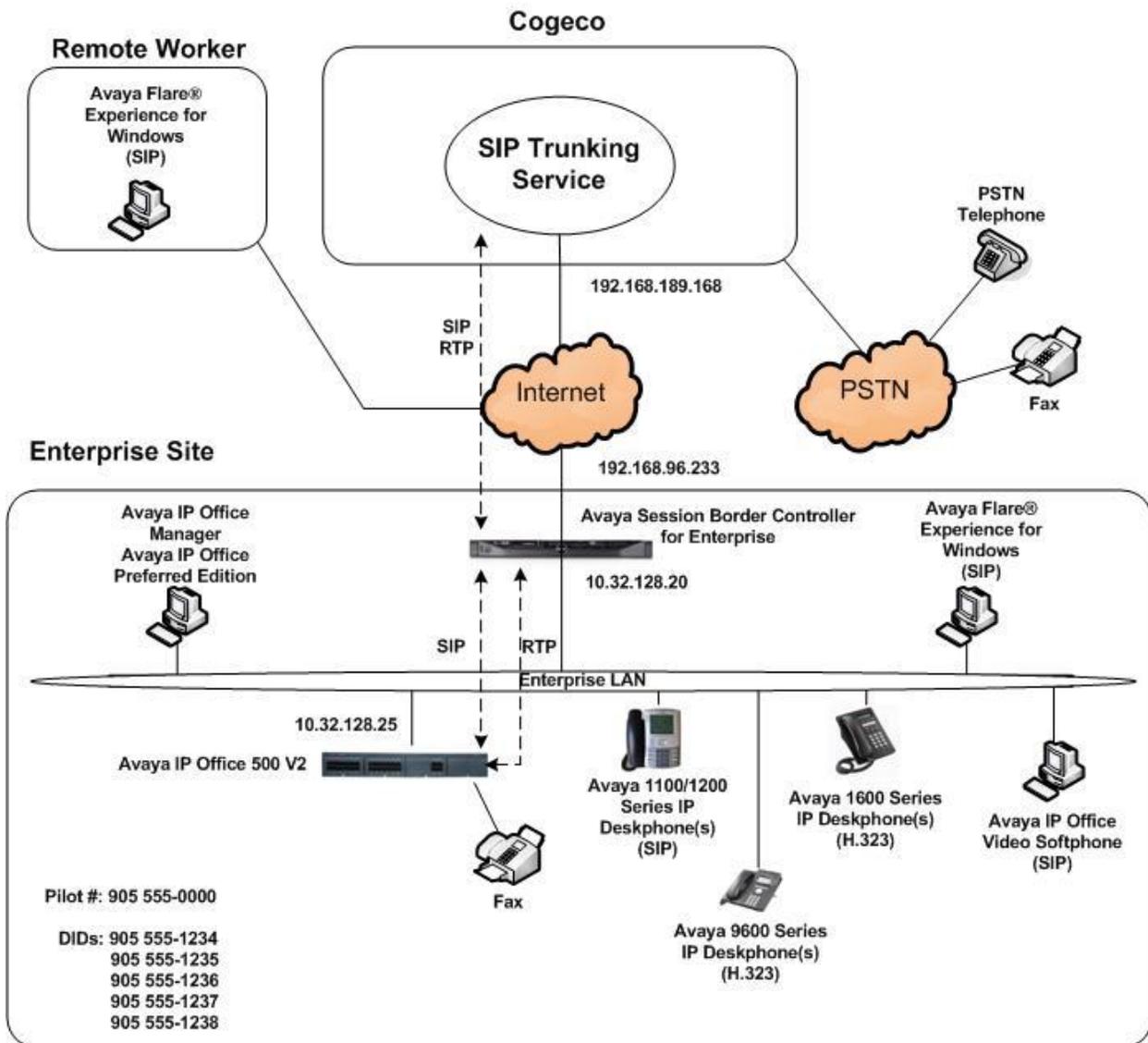
For technical support on the Cogeco SIP Trunking Service, use the contact information for business customers in a specific geographic region at [www.cogeco.com](http://www.cogeco.com).

## 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 Cogeco SIP Trunking Service.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers.

The enterprise site contains an Avaya IP Office 500 V2 with various endpoints and a Windows 2003 Server running both Avaya IP Office Manager to configure the Avaya IP Office and Avaya Preferred Edition for voicemail (also known as VoiceMail Pro).



**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 over the PSTN.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to send digits across the SIP trunk to Cogeco. The short code of 9 is stripped off by Avaya IP Office and the remaining digits were sent unaltered to Cogeco. Cogeco requires 11 digits (1+10 digits) be sent in the Request URI header for long distance calls and 10 digits for local calls. On inbound calls, Cogeco will send 10 digits in the Request-URI.

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

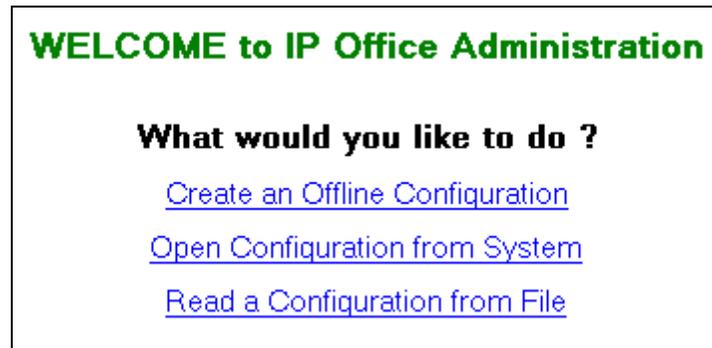
<b>Avaya Telephony Components</b>	
<b>Equipment</b>	<b>Software</b>
Avaya IP Office 500 v2	9.0 SP1 (845)
Avaya IP Office Manager	9.0 SP1 (845)
Avaya IP Office Preferred Edition (Voicemail)	9.0 SP1 (53)
Avaya Session Border Controller for Enterprise running on a Portwell CAD-0208 server	6.2.1.Q07
Avaya 1140E IP Deskphone (SIP)	4.3 SP2 (04.03.18.00)
Avaya 1608 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP4 (1.343A)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.3 (6.3037)
Avaya IP Office Video Softphone (SIP)	3.2.3.48 (67009)
Avaya Flare® Experience for Windows	1.1.4.23

<b>Cogeco Components</b>	
<b>Equipment</b>	<b>Software</b>
Acme Packet 4500 Session Border Controller	SCX6.1.0 MR-10 Patch 1 (Build 985)
BroadSoft BroadWorks Softswitch / Core Telephony Application Server	18

Testing was performed with Avaya IP Office 500 V2, but this testing also applies to Avaya IP Office Server Edition running the same software release. Note that Avaya IP Office Server Edition requires an Expansion IP Office 500 V2 R9 to support analog or digital endpoints or trunks.

## 5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the Avaya IP Office Manager PC, select **Start → Programs → IP Office → Manager** to launch the application. A screen that includes the following in the center may be displayed:



Select **Open Configuration from System**. If the above screen does not appear, the configuration may be alternatively opened by navigating to **File → Open Configuration** at the top of the Avaya IP Office Manager window. Select the proper Avaya IP Office system from the pop-up window and log in with the appropriate credentials.

The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the Group Pane has been omitted, its content is shown as submenus in the Navigation pane. These panes (Navigation, Group and Details) will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the service provider (such as twinning and IP Office Video Softphone support) is assumed to already be in place.

In the sample configuration, **Atlantic City** was used as the system name. All navigation described in the following sections (e.g., **License → SIP Trunk Channels**) appears as submenus underneath the system name **Atlantic City** in the Navigation Pane.

## 5.1. Licensing and Physical Hardware

The configuration and features described in these Application Notes require Avaya IP Office 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 license with sufficient **Instances** (trunk channels) in the Details pane.

The screenshot displays the Avaya IP Office software interface. On the left is a navigation pane titled 'IP Offices' with a tree view of system components. The main area is titled 'License' and shows a table of installed licenses. The 'SIP Trunk Channels' license is highlighted with a red border. The table columns are Feature, License Key, Instances, Status, and Expiry Date. The 'SIP Trunk Channels' row shows 255 instances, a 'Valid' status, and an expiry date of 'Never'. Other licenses include IP500 Voice Networking Channels, WCM Channel Migration, VPN IP Extensions, and various support services.

Feature	License Key	Instances	Status	Expiry Date
IP500 Voice Networking Channels		4	Valid	Never
WCM Channel Migration		255	Valid	Never
<b>SIP Trunk Channels</b>		<b>255</b>	<b>Valid</b>	<b>Never</b>
VPN IP Extensions		255	Obsolete	Never
IP500 Universal PRI (Additional chan...		255	Valid	Never
RAS LRQ Support (Rapid Response)		255	Valid	Never
IP Office Dealer Support - Standard E...		255	Valid	Never
IP Office Dealer Support - Profession...		255	Valid	Never
IP Office Distributor Support - Standa...		255	Valid	Never
IP Office Distributor Support - Profes...		255	Valid	Never
UMS Web Services		255	Valid	Never
CCR SUP		255	Valid	Never
Customer Service Agent		255	Valid	Never
CCR Designer		255	Valid	Never
CCR CCC UPG		255	Valid	Never
1600 Series Phones		255	Valid	Never
Third Party API		255	Valid	Never

To view the physical hardware comprising Avaya IP Office, expand the components under the **Control Unit** in the Navigation pane. In the sample configuration, the second component listed is a Combination Card. This module has 6 digital stations ports, two analog extension ports, 4 analog trunk ports and 10 VCM channels. The VCM is a Voice Compression Module supporting VoIP codecs. An Avaya IP Office hardware configuration with a VCM component is necessary to support SIP trunking.

To view the details of the component, select the component in the Navigation pane. The following screen shows the details of the **IP 500 V2**.

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, and on the right is the 'IP 500 V2' details pane.

**IP Offices Navigation Pane:**

- BOOTP (4)
- Operator (3)
- Atlantic City
  - System (1)
  - Line (16)
  - Control Unit (3)
    - 1 IP 500 V2**
    - 2 COMBO6210/ATM4
    - 3 DIGSTA8/ATM4
  - Extension (25)
  - User (27)
  - Group (1)
  - Short Code (64)
  - Service (0)

**IP 500 V2 Details Pane:**

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	9.0.100.845
Serial Number	
Unit IP Address	10.32.128.25
Interconnect Number	0
Module Number	Control Unit

## 5.2. System

Configure the necessary system settings.

### 5.2.1. System – LAN1 Tab

In the sample configuration, the Avaya IP Office LAN port was used to connect to the enterprise network. The LAN1 settings correspond to the LAN port on the Avaya IP Office 500 V2. To access the LAN1 settings, first navigate to **System** → <Name>, where <Name> is the system name assigned to the Avaya IP Office. In the case of the compliance test, the system name is **Atlantic City**. Next, navigate to the **LAN1** → **LAN Settings** tab in the Details Pane. Set the **IP Address** field to the IP address assigned to the Avaya IP Office LAN port. Set the **IP Mask** field to the mask used on the enterprise network. All other parameters should be set according to customer requirements.

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' tree shows a hierarchy starting with 'Atlantic City', which includes a 'System (1)' sub-entry. The main pane is titled 'Atlantic City' and has several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The configuration fields are as follows:

- IP Address: 10 . 32 . 128 . 25
- 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)
- DHCP Mode:  Server,  Client,  Dialin,  Disabled

An 'Advanced' button is located at the bottom right of the configuration area.

On the **VoIP** tab in the Details Pane configure the following parameters:

- Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks.
- The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, Avaya IP Office would request RTP media be sent to a UDP port in the configurable range for calls using LAN1.
- In the **RTP Keepalives** section, set the **Scope** to **RTP**. Set the periodic timeout to **30** and the **Initial Keepalives** parameter to **Enabled**. These settings will cause Avaya IP Office to send a RTP keepalive packet starting at the time of initial connection and every 30 seconds thereafter if no other RTP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting to see media from the other, as well as helping to keep firewall ports open for the duration of the call.

The screenshot displays the configuration interface for Atlantic City, specifically the VoIP tab. The interface is organized into several sections:

- System Navigation:** Includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, CCR, and Codecs.
- LAN Settings:** Contains sub-tabs for LAN Settings, VoIP, and Network Topology.
- H323 Settings:** Includes checkboxes for H323 Gatekeeper Enable (checked), Auto-create Extn, Auto-create User, and H323 Remote Extn Enable.
- SIP Settings:** Includes checkboxes for SIP Trunks Enable (checked), SIP Registrar Enable (checked), Auto-create Extn/User, and SIP Remote Extn Enable. It also features a Domain Name input field.
- Layer 4 Protocol:** Includes checkboxes for UDP (checked), TCP (checked), and TLS. Each has associated port number dropdowns for Local and Remote ports.
- Challenge Expiry Time (secs):** A dropdown menu set to 10.
- RTP Section:** Contains sub-sections for:
  - Port Number Range:** Minimum 49152, Maximum 53246.
  - Port Number Range (NAT):** Minimum 49152, Maximum 53246.
  - Enable RTCP Monitoring on Port 5005:** Checked.
  - Keepalives:** Scope set to RTP, Periodic timeout set to 30, and Initial keepalives set to Enabled.

Scroll down the same page to the **DiffServ** section.

- Avaya IP Office can also 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 example below and are also the default values. For a customer installation, if the default values are not sufficient, appropriate values will be provided by the customer.
- All other parameters should be set according to customer requirements.

The screenshot displays the configuration interface for 'Atlantic City'. The top navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, CCR, and Codecs. The 'LAN1' tab is active, and the 'VoIP' sub-tab is selected. The 'DiffServ Settings' section is expanded, showing the following configuration:

Parameter	Value
Scope	RTP
Periodic timeout	30
Initial keepalives	Enabled
DSCP (Hex)	B8
Video DSCP (Hex)	FC
DSCP Mask (Hex)	88
SIG DSCP (Hex)	46
DSCP	46
Video DSCP	63
DSCP Mask	34
SIG DSCP	
Primary Site Specific Option Number (SSON)	176
Secondary Site Specific Option Number (SSON)	242
VLAN	Not Present
1100 Voice VLAN Site Specific Option Number (SSON)	232
1100 Voice VLAN IDs	

On the **Network Topology** tab in the Details Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. The Avaya SBCE will perform network address translation of SIP traffic but it is not necessary for Avaya IP Office to have any knowledge of this translation. Thus, the parameter was set to **Open Internet**.
- Set **Binding Refresh Time (seconds)** to **30**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set the **Public Port** to the port on which Avaya IP Office will listen.
- All other parameters should be set according to customer requirements.

The screenshot displays the configuration interface for 'Atlantic City'. The 'Network Topology' tab is selected, showing the following settings:

- STUN Server Address:** 10.90.168.13
- STUN Port:** 3478
- Firewall/NAT Type:** Open Internet
- Binding Refresh Time (seconds):** 30
- Public IP Address:** 0 . 0 . 0 . 0
- Public Port:**
  - UDP: 5060
  - TCP: 0
  - TLS: 0
- Run STUN on startup

Buttons for 'Run STUN' and 'Cancel' are visible next to the Public IP Address field.

## 5.2.2. System - Telephony Tab

To access the System Telephony settings, navigate to the **Telephony** → **Telephony** tab in the Details Pane. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.

The screenshot shows the 'Atlantic City' configuration interface for the 'Telephony' tab. The interface is divided into several sections:

- System Navigation:** Includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony (selected), Directory Services, System Events, SMTP, SMDR, Twinning, VCM, CCR, and Codecs.
- Telephony Sub-Tabs:** Includes Telephony (selected), Park & Page, Tones & Music, Ring Tones, SM, Call Log, and TUI.
- Analogue Extensions:** Contains settings for Default Outside Call Sequence (Normal), Default Inside Call Sequence (Ring Type 1), Default Ring Back Sequence (Ring Type 2), and Restrict Analogue Extension Ringer Voltage (unchecked).
- Companing Law:** Divided into 'Switch' and 'Line' sections. Both have radio buttons for U-Law (selected) and A-Law (unchecked).
- General Settings:** Includes Dial Delay Time (4), Dial Delay Count (0), Default No Answer Time (25), Hold Timeout (0), Park Timeout (300), Ring Delay (5), Call Priority Promotion Time (Disabled), Default Currency (USD), Default Name Priority (Favor Trunk), and Media Connection Preservation (Disabled).
- Advanced Settings:** Includes DSS Status (unchecked), Auto Hold (checked), Dial By Name (checked), Show Account Code (checked), Inhibit Off-Switch Forward/Transfer (unchecked), Restrict Network Interconnect (unchecked), Drop External Only Impromptu Conference (unchecked), Visually Differentiate External Call (unchecked), Unsupervised Analog Trunk Disconnect Handling (unchecked), High Quality Conferencing (checked), Strict SIPs (unchecked), and Digital/Analogue Auto Create User (checked).

### 5.2.3. System - Twinning Tab

To view or change the System Twinning settings, navigate to the **Twinning** tab in the Details Pane 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. Click the **OK** button at the bottom of the page (not shown).

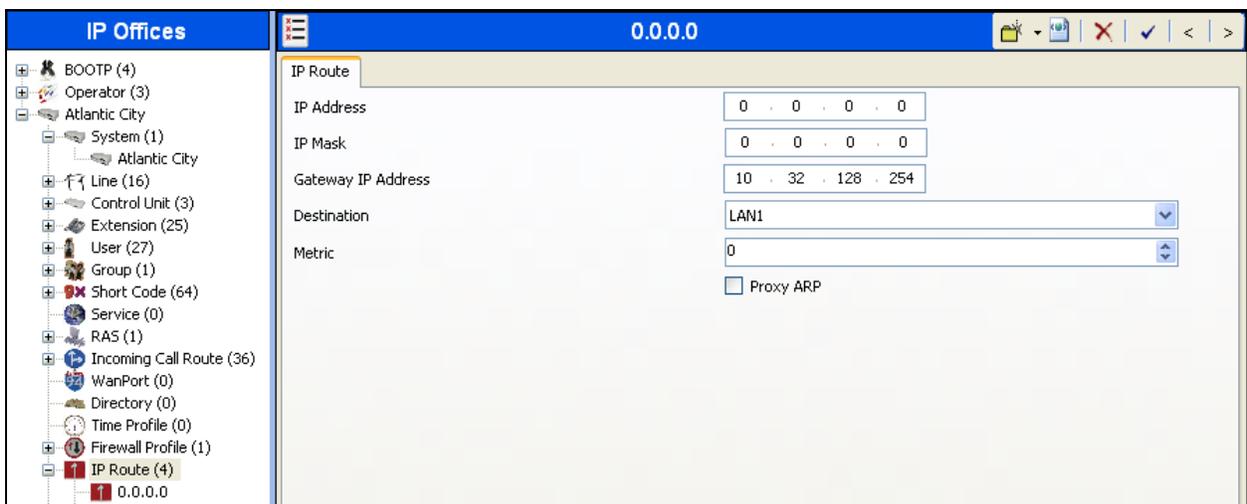


### 5.3. IP Route

Navigate to **IP Route → 0.0.0.0** in the left Navigation Pane if a default route already exists. Otherwise, to create the default route, right-click on **IP Route** and select **New**. Create/verify a default route with the following parameters:

- Set **IP Address** and **IP Mask** to **0.0.0.0**.
- Set **Gateway IP Address** to the IP address of the default router on the network where Avaya IP Office is connected.
- Set **Destination** to **LAN1** from the drop-down list.

Click the **OK** button at the bottom of the page (not shown).



## 5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Cogeco SIP Trunking Service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.4.1** to create the SIP Line from the template.

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

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- 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**.

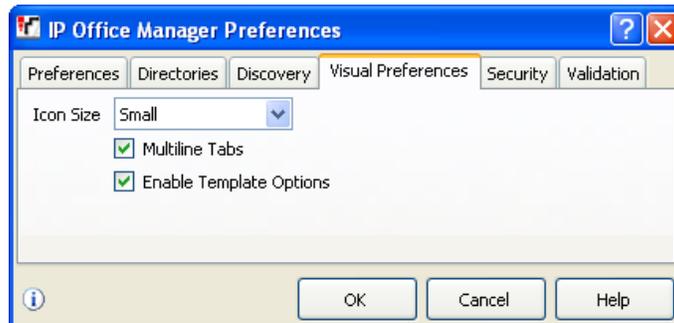
Also, the following SIP Line settings are not supported on Basic Edition:

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

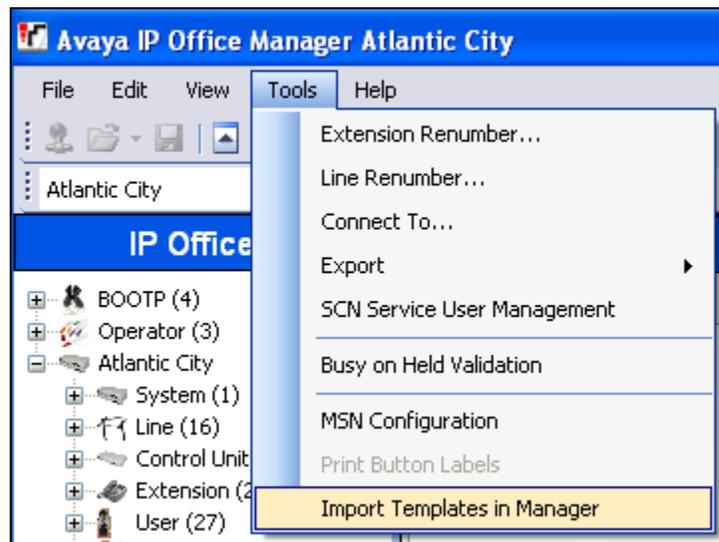
To create a SIP Line manually, right-click **Line** in the Navigation Pane and select **New → SIP Line**; then, follow the steps outlined in **Sections 5.4.2 – 5.4.6**.

### 5.4.1. SIP Line From Template

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



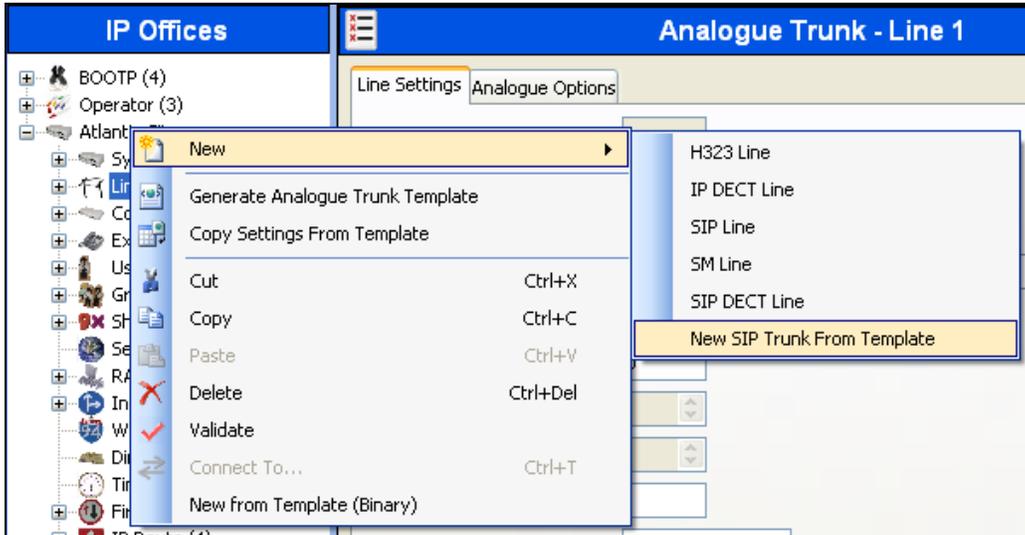
3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template 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 **Cogeco** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name (**US\_Cogeco\_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.

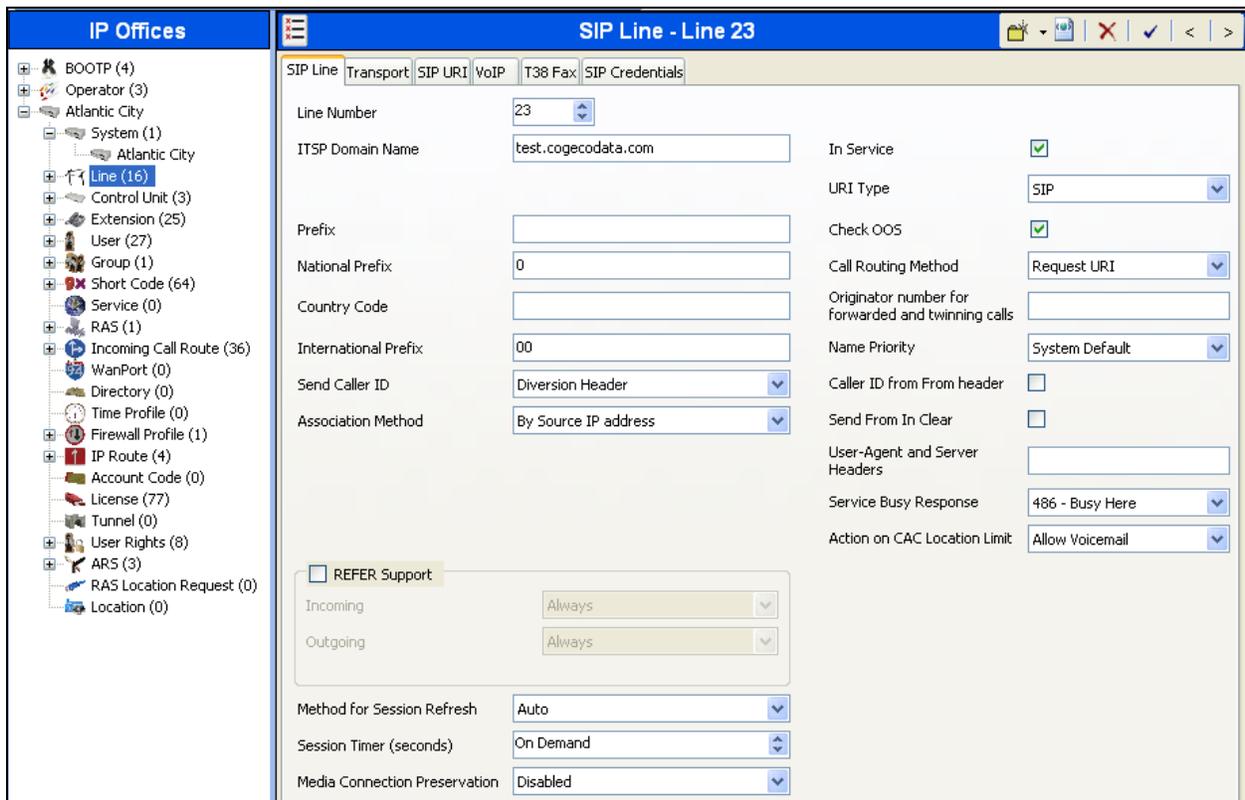


6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2 – 5.4.6**.

## 5.4.2. SIP Line – SIP Line Tab

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

- Set **ITSP Domain Name** to the domain provided by Cogeco.
- Set **Send Caller ID** to **Diversion Header**. With this setting and the related configuration in **Section 5.2.3**, Avaya IP Office will include the Diversion Header for calls that are directed via Mobile Twinning out the SIP Line to Cogeco. It will also include the Diversion Header for calls that are call forwarded out the SIP Line.
- Cogeco supports REFER. Thus, **REFER Support** may be checked or unchecked based on customer need. If checked, then both **Incoming** and **Outgoing** must be set to **Always**. This solution was tested both with REFER and without. The screenshot below shows the settings if REFER is not used.
- Check the **In Service** box. This makes the trunk available to incoming and outgoing calls.
- Check the **Check OOS** box. Avaya IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by Avaya IP Office will use the **Binding Refresh Time** for LAN1, as shown in **Section 5.2.1**.
- Default values may be used for all other parameters.



Field	Value
Line Number	23
ITSP Domain Name	test.cogecodata.com
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
Prefix	
National Prefix	0
Country Code	
International Prefix	00
Send Caller ID	Diversion Header
Association Method	By Source IP address
REFER Support	<input type="checkbox"/>
Incoming	Always
Outgoing	Always
Method for Session Refresh	Auto
Session Timer (seconds)	On Demand
Media Connection Preservation	Disabled

### 5.4.3. SIP Line - Transport Tab

Select the **Transport** tab. Set or verify the parameters as shown below.

- Set **ITSP Proxy Address** to the IP address of the internal signaling interface of the Avaya SBCE.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to the network port used by the SIP line to access the far-end and configured in **Section 5.2.1**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.

The screenshot shows the configuration window for 'SIP Line - Line 23'. The 'Transport' tab is selected. The 'ITSP Proxy Address' is set to '10.32.128.20'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'UDP', 'Send Port' is '5060', 'Use Network Topology Info' is set to 'LAN 1', and 'Listen Port' is '5060'. 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0' and '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. 'Separate Registrar' is an empty field.

Field	Value
ITSP Proxy Address	10.32.128.20
Layer 4 Protocol	UDP
Send Port	5060
Use Network Topology Info	LAN 1
Listen Port	5060
Explicit DNS Server(s)	0 . 0 . 0 . 0
Explicit DNS Server(s)	0 . 0 . 0 . 0
Calls Route via Registrar	<input checked="" type="checkbox"/>
Separate Registrar	

#### 5.4.4. SIP Line - SIP URI Tab

A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. In the example screen below, a new entry is created. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact**, and **Display Name** to **Use Internal Data**. This setting allows calls on this line that have a SIP URI that matches the number set in the **SIP** tab of any user as shown in **Section 5.7**.
- Set **PAI** to **Use Credentials User Name**. The **Credentials User Name** is set to the pilot number assigned to the enterprise by Cogeco as shown in **Section 5.4.6**. Cogeco recommends using the pilot number in the P-Asserted-Identity (PAI) header.
- For **Registration**, select the entry showing the pilot number from the pull-down menu.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line in **Section 5.8.1**. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining ARS entries for routing outbound traffic to this line in **Section 5.6**. For the compliance test, a new incoming and outgoing group **23** was defined that only contained this line (line 23).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

Click **OK**.

The screenshot shows the 'SIP Line - Line 23\*' configuration window with the 'SIP URI' tab selected. The 'New Channel' section contains the following fields and values:

Field	Value
Via	10.32.128.25
Local URI	Use Internal Data
Contact	Use Internal Data
Display Name	Use Internal Data
PAI	Use Credentials User Name
Registration	1: 9055550000
Incoming Group	23
Outgoing Group	23
Max Calls per Channel	10

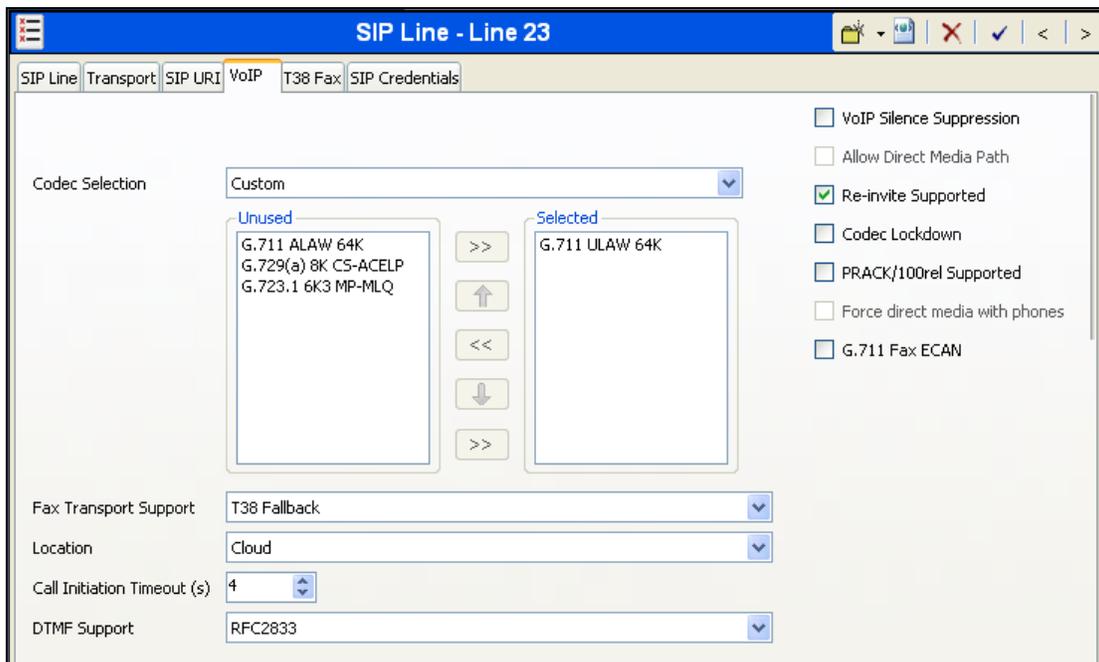
Additional SIP URIs may be required to allow inbound calls to numbers not associated with a user, such as a short code. These URIs are created in the same manner as shown above with the exception that the incoming DID number is entered directly in the **Local URI**, **Contact**, and **Display Name**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

### 5.4.5. SIP Line - VoIP Tab

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

- For **Codec Selection**, select **System Default** from the pull-down menu to use the default list of codecs. A list of the codecs in their current order of preference will be shown on the right in the **Selected** column. To use a custom list of codecs, select **Custom** for **Codec Selection**. Next, move unwanted codecs from the **Selected** column to the **Unused** column. Lastly, move the codecs up or down the list in the **Selected** column to achieve the desired order of preference. The example below shows the codecs used for the compliance test. Since Cogeco only supports the G.711MU codec, this is the only codec shown in the **Selected** column.
- Uncheck the **VoIP Silence Suppression** box.
- If desired, direct media may be used by checking the boxes for **Allow Direct Media Path** and **Force direct media with phones**. This will allow Avaya IP Office to redirect the media path directly between the phones and the Avaya SBCE. Direct media cannot be enabled if T.38 fax is also enabled on the same SIP Line.
- Check the **Re-invite Supported** box.
- Set the **Fax Transport Support** to **T.38 Fallback**. Not all media gateways in the Cogeco network support T.38 fax. This setting will allow the fax connection to fallback to G.711 fax if T.38 is not supported.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Default values may be used for all other parameters.

Click the **OK** button at the bottom of the page (not shown).



The screenshot displays the configuration interface for a SIP Line (Line 23) in the VoIP tab. The interface includes several sections:

- Codec Selection:** A dropdown menu is set to "Custom". Below it are two columns: "Unused" (containing G.711 ALAW 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ) and "Selected" (containing G.711 ULAW 64K). Navigation buttons (>>, <<, <-, >-, <-, >-, <-, >-) are positioned between the columns.
- Checkboxes:** A list of options on the right side, including "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".
- Other Settings:** "Fax Transport Support" is set to "T38 Fallback", "Location" is "Cloud", "Call Initiation Timeout (s)" is "4", and "DTMF Support" is "RFC2833".

### 5.4.6. SIP Line – SIP Credentials

Cogeco requires that the Avaya IP Office SIP Line registers with the Cogeco SIP Trunking Service using credentials provided by Cogeco. To configure the SIP Credentials, select the **SIP Credentials** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. Configure the parameters as shown below.

- Set **User Name**, **Authentication Name**, and **Contact** to the pilot number provided by Cogeco.
- Set **Password** to the password provided by Cogeco.
- Set **Expiry (mins)** to a value acceptable to Cogeco. For the compliance test, the value of **5** was used.
- Check the **Registration required** box.

The screenshot shows the 'SIP Line - Line 23' configuration window. The 'SIP Credentials' tab is selected. A table with columns 'Index', 'UserName', 'Authentication Name', 'Contact', 'Expiry (mins)', and 'Register' is visible. Below the table, the 'New SIP Credentials' form is displayed with the following fields:

User name	9055550000
Authentication Name	9055550000
Contact	9055550000
Password	*****
Expiry (mins)	5
Registration required	<input checked="" type="checkbox"/>

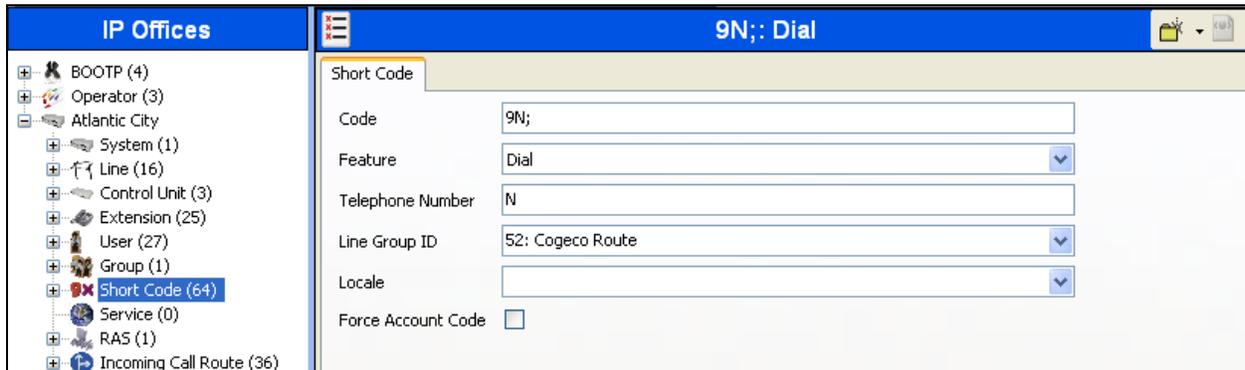
Buttons for 'Add...', 'Remove', 'Edit...', 'OK', and 'Cancel' are also present.

## 5.5. Short Codes

ARS is used to route outbound traffic to the SIP line. A short code is used to route outbound traffic to ARS. To create a short code, right-click on **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **9N;**. This short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group Id** to the ARS route to be used which is defined in **Section 5.6**.

Click the **OK** button (not shown).

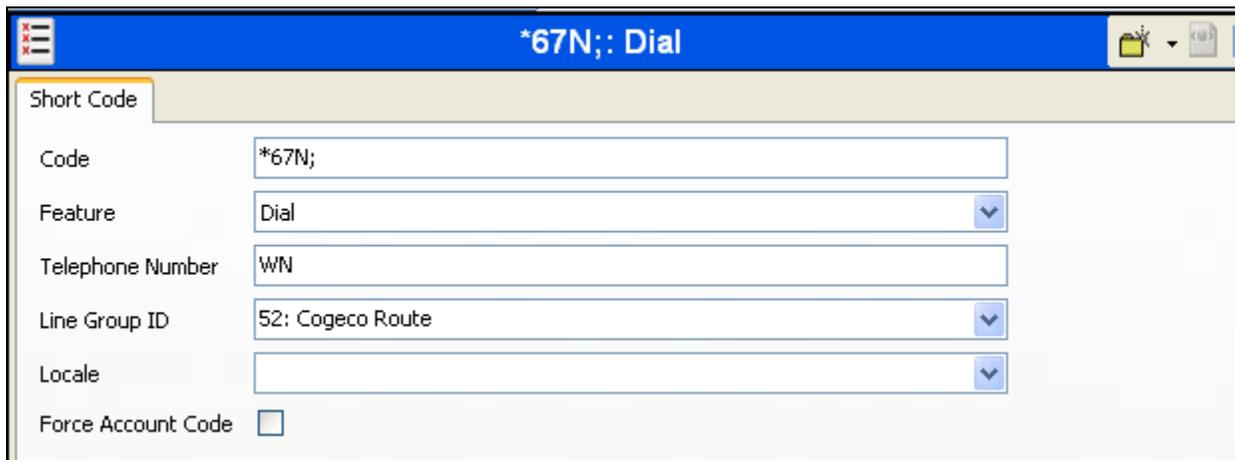


The screenshot displays the configuration interface for a Short Code. The left pane, titled 'IP Offices', shows a tree view with 'Short Code (64)' selected. The right pane, titled '9N;: Dial', shows the configuration details for a Short Code:

Field	Value
Code	9N;
Feature	Dial
Telephone Number	N
Line Group ID	52: Cogeco Route
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 9N; 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 to Cogeco documented in these Application Notes, when a user dials \*67 plus the number, Avaya IP Office will include the pilot number in the PAI header and will include the Privacy: Id header. Cogeco will allow the call due to the presence of the pilot number in the PAI header, but will prevent presentation of the caller id to the called PSTN destination. If a long distance number is dialed, then the pilot number must have long distance enabled or the call will fail.



Short Code	
Code	*67N;
Feature	Dial
Telephone Number	WN
Line Group ID	52: Cogeco Route
Locale	
Force Account Code	<input type="checkbox"/>

## 5.6. ARS

ARS is used to route outbound traffic to the SIP line. To define a new ARS route, right-click **ARS** in the Navigation pane and select **New**. In the Details pane that appears, a collection of matching patterns (similar to short codes) can be entered to route calls as shown below.

For the compliance test, one entry was created. The entry matches on any number **N** and then sends that number (**N**) in the SIP INVITE message on the line group defined in **Section 5.4.4** (e.g., line group 23).

To create an entry, click the **Add** button and enter the following in the pop-up window (not shown).

- In the **Code** field, enter the pattern to match the number passed to ARS from the short code in **Section 5.5** followed by a semi-colon.
- Set **Feature** to **Dial**. This is the action that the entry will perform.
- Set **Telephone Number** to **N"@test.cogecodata.com"**. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value **N** represents the complete number passed to ARS. The domain **test.cogecodata.com** is the SIP domain provided by Cogeco.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4.4**. This short code will use this line group when placing the outbound call.

Click the **OK** button (not shown).

The screenshot displays the 'Cogeco Route' configuration window. The left pane shows a tree view of 'IP Offices' with 'ARS (3)' expanded to show '52: Cogeco Route'. The main pane shows the configuration for ARS Route Id 52, named 'Cogeco Route'. The 'Code' field is 'N;', 'Telephone Number' is 'N"@test.cogecodata.com"', and 'Feature' is 'Dial'. The 'Line Group ID' is 23. The 'In Service' checkbox is checked. The 'Out of Service Route' and 'Out of Hours Route' are both set to '<None>'. A table at the bottom lists the ARS entries:

Code	Telephone Number	Feature	Line Group ID
N;	N"@test.cogecodata.com"	Dial	23

## 5.7. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.4**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **Extn243**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls 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 (**Section 5.4.4**). The example below shows the settings for user **Extn243**. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from Cogeco. 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.

Click the **OK** button (not shown).

The screenshot displays the Avaya user configuration interface. On the left is a navigation pane titled "IP Offices" with a tree view containing categories like BOOTP (4), Operator (3), Atlantic City, System (1), Line (16), Control Unit (3), Extension (25), User (27), Group (1), Short Code (64), and Service (0). The "User (27)" category is selected. The main pane is titled "Extn243: 243" and contains several tabs: User, Voicemail, DND, Short Codes, Source Numbers, Telephony, Forwarding, Dial In, Voice Record, Menu Programming, Mobility, Group Membership, Announcements, SIP, and Personal Directory. The "SIP" tab is active, showing three text input fields: "SIP Name" with the value "9055551236", "SIP Display Name (Alias)" with the value "Extn243", and "Contact" with the value "9055551236". Below these fields is an unchecked checkbox labeled "Anonymous".

## 5.8. Incoming Call Route

An incoming call route maps an inbound DID number on a specific line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**.

### 5.8.1. Incoming Call Route – Standard Tab

On the **Standard** tab of the Details Pane, enter the parameters as shown below.

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4.4**.
- Set the **Incoming Number** to the incoming number on which this route should match.
- Default values can be used for all other fields.

The screenshot shows the configuration interface for an Incoming Call Route. The left pane shows a tree view of IP Offices, with 'Incoming Call Route (36)' selected. The right pane shows the 'Standard' tab for the route '23 9055551236'. The fields are as follows:

Field	Value
Bearer Capability	Any Voice
Line Group ID	23
Incoming Number	9055551236
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

### 5.8.2. Incoming Call Route – Destinations Tab

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, incoming calls to 9055551236 on line 23 are routed to extension 243.

The screenshot shows the 'Destinations' tab for the route '23 9055551236'. The table below shows the destination configuration:

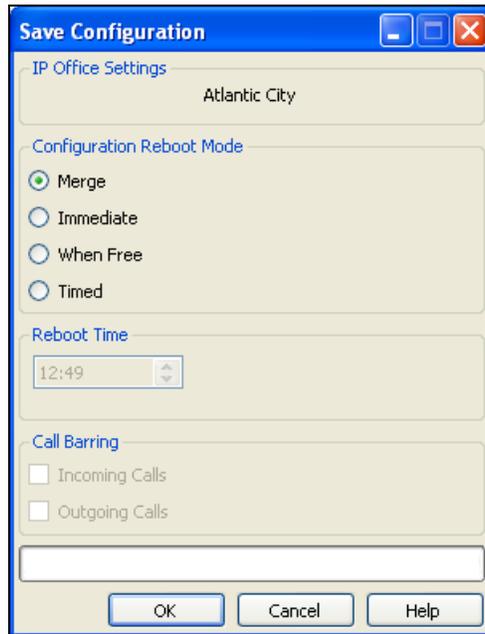
TimeProfile	Destination	Fallback Extension
Default Value	243 Extn243	

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

## 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** to proceed.



## 6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

### 6.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with appropriate credentials.



The screenshot shows the login page for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, the "Log In" section contains a "Username:" label followed by a text input field, a "Password:" label followed by a text input field, and a "Log In" button. Below the input fields, there are three paragraphs of text: a disclaimer about system access, a statement about monitoring, and a copyright notice.

**AVAYA**

**Session Border Controller  
for Enterprise**

**Log In**

Username:

Password:

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

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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

After logging in, the Dashboard screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

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

## Session Border Controller for Enterprise

**AVAYA**

**Dashboard**

- Administration
- Backup/Restore
- System Management
  - Global Parameters
  - Global Profiles
  - SIP Cluster
  - Domain Policies
  - TLS Management
  - Device Specific Settings

**Dashboard**

Information		
System Time	03:26:23 PM EDT	<a href="#">Refresh</a>
Version	6.2.1.Q07	
Build Date	Mon Dec 9 17:33:02 CST 2013	

Installed Devices
EMS
vnj-sbce2

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

[Add](#)

Notes
No notes found.

## 6.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.

**Session Border Controller for Enterprise** AVAYA

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						
vnj-sbce2 (IFCS11010168)	10.32.101.20	6.2.1.Q07	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Delete

A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**vnj-sbce2**). This name will be referenced in other configuration screens. Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE respectively. Each interface has multiple IP addresses assigned to it. The IP addresses used for SIP Trunking and thus applicable to this Application Note are highlighted below. Each of these interfaces must be enabled after installation.

**System Information: vnj-sbce2** X

**General Configuration**

Appliance Name vnj-sbce2  
Box Type SIP  
Deployment Mode Proxy

**Device Configuration**

HA Mode No  
Two Bypass Mode No

**Network Configuration**

IP	Public IP	Netmask	Gateway	Interface
10.32.128.20	10.32.128.20	255.255.255.0	10.32.128.254	A1
192.168.96.233	192.168.96.233	255.255.255.224	192.168.96.254	B1
10.32.128.21	10.32.128.21	255.255.255.0	10.32.128.254	A1
192.168.96.234	192.168.96.234	255.255.255.224	192.168.96.254	B1

**DNS Configuration**

Primary DNS 10.32.128.200  
Secondary DNS  
DNS Location DMZ  
DNS Client IP 10.32.128.20

**Management IP(s)**

IP 10.32.101.20

To enable the interfaces, first navigate to **Device Specific Settings** → **Network Management** in the left pane and select the device being managed in the center pane. In the right pane, click on the **Interface Configuration** tab. Verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click **Toggle** to enable the interface.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The title bar shows "Session Border Controller for Enterprise" and the Avaya logo. The left navigation pane includes "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "SIP Cluster", "Domain Policies", "TLS Management", and "Device Specific Settings". Under "Device Specific Settings", "Network Management" is selected. The main content area is titled "Network Management: vnj-sbce2". It features a "Devices" tab with "vnj-sbce2" selected. Below this are two tabs: "Network Configuration" and "Interface Configuration". The "Interface Configuration" tab contains a table with the following data:

Name	Administrative Status	
A1	Enabled	<a href="#">Toggle</a>
A2	Disabled	<a href="#">Toggle</a>
B1	Enabled	<a href="#">Toggle</a>

### 6.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings** → **Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**vnj-sbce2**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int\_Sig\_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext\_Sig\_Intf** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 6.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 6.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for UDP on port **5060**. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port **5060**. Since Cogeco uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The title is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. The left navigation pane includes: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management), and Device Specific Settings (with sub-items: Network Management, Media Interface, **Signaling Interface**, and Signaling Forking). The main content area is titled "Signaling Interface: vnj-sbce2". Under "Devices", "vnj-sbce2" is selected. A "Signaling Interface" tab is active, and an "Add" button is visible. A table lists the configured interfaces:

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Int_Sig_Intf	10.32.128.20	---	5060	---	None	Edit	Delete
Ext_Sig_Intf	192.168.96.233	5060	5060	---	None	Edit	Delete
Int_Sig_Intf_RW	10.32.128.21	5060	---	---	None	Edit	Delete
Ext_Sig_Intf_RW	192.168.96.234	---	---	5061	AvayaSBCServer	Edit	Delete

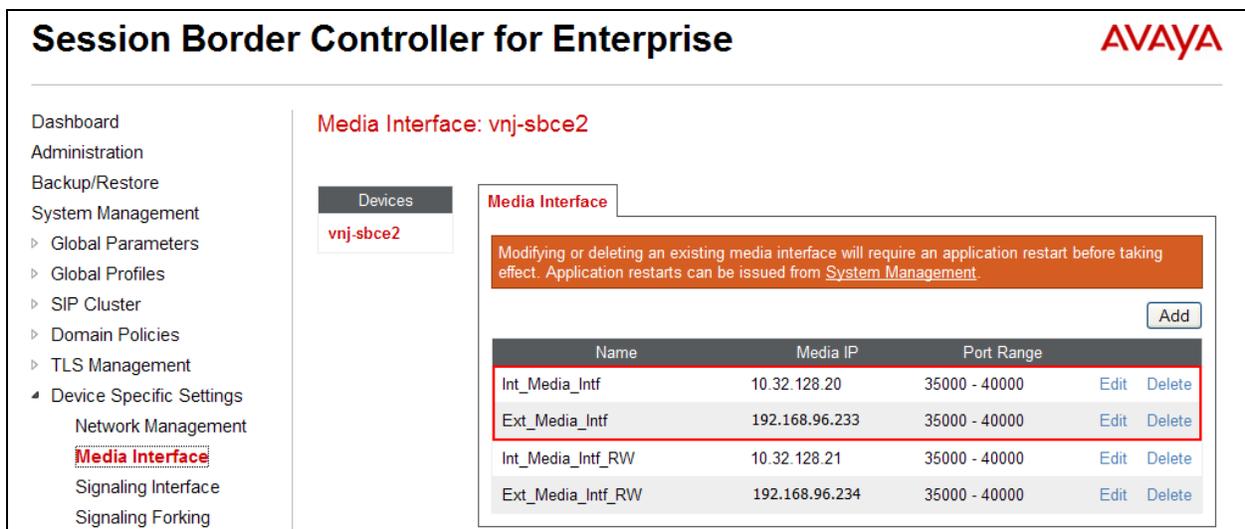
## 6.4. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings** → **Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**vnj-sbce2**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int\_Media\_Intf** was created for the Avaya SBCE internal interface and media interface **Ext\_Media\_Intf** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 6.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the compliance test, the default port range was used for both interfaces.



**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

**Media Interface: vnj-sbce2**

Devices  
vnj-sbce2

**Media Interface**

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

Add

Name	Media IP	Port Range	Edit	Delete
Int_Media_Intf	10.32.128.20	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.233	35000 - 40000	Edit	Delete
Int_Media_Intf_RW	10.32.128.21	35000 - 40000	Edit	Delete
Ext_Media_Intf_RW	192.168.96.234	35000 - 40000	Edit	Delete

## 6.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create a server interworking profile for Avaya IP Office and the service provider SIP server. These profiles will be applied to the appropriate server in **Section 6.7.1** and **6.7.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the 'Server Interworking' menu item selected. The main content area is titled 'Interworking Profiles: IPOffice-T38'. A list of profiles is shown on the left, with 'IPOffice-T38' selected. The right pane shows the configuration for this profile, with the 'General' tab active. The configuration table is as follows:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No

### 6.5.1. Server Interworking – Avaya IP Office

For the compliance test, server interworking profile **IPOffice-T38** was created for Avaya IP Office by creating a new profile and accepting the default values for all settings with the exception of setting the **T.38 Support** to **Yes**. The **General** tab parameters are shown below.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
<b>T.38 Support</b>	<b>Yes</b>
URI Scheme	SIP
Via Header Format	RFC3261

Scroll down to see the rest of the **General** tab.

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

The **Timers**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

The **Advanced** tab parameters are shown below.

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

### 6.5.2. Server Interworking – Cogeco

For the compliance test, server interworking profile **SP-General-T38** was created for the Cogeco SIP server. When creating the profile, the default values were used for all parameters with the exception of **T.38 Support** set to **Yes**. Thus, the **SP-General-T38** profile is identical to the **IPOffice-T38** profile created in **Section 6.5.1**.

## 6.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be done by other configuration within the Avaya SBCE. It was necessary to create a signaling manipulation script that will be applied to the Cogeco SIP server in **Section 6.7.2**. The details of the script are shown in **Section 6.6.1**.

To create a script, navigate to **Global Profiles → Signalling Manipulation** in the left pane. In the center pane, select **Add**. An edit window (not shown) will appear in which a title for the script can be entered as well as the script itself. Once complete, click **Save** to save the new script. Alternatively, a new script may be created by selecting an existing script in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected script which can then be edited as needed. To view an existing script, select the script from the center pane. The script will appear in the right pane.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top header shows the product name and the Avaya logo. On the left is a navigation menu with categories like Dashboard, Administration, and System Management, with 'Signaling Manipulation' highlighted in red. The main content area is titled 'Signaling Manipulation Scripts: CogecoHdrManip'. It features buttons for 'Upload', 'Add', 'Download', 'Clone', and 'Delete'. Below these is a blue bar with the text 'Click here to add a description.' A list of scripts is shown, with 'CogecoHdrM...' selected. The right pane displays the script code for 'Signaling Manipulation':

```
//Remove Remote Address header in outbound INVITE and 200 OK
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"][1]);
  }
}

//Change Contact header in Register Message to external IP
within session "REGISTER"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["Contact"][1].URI.HOST = "135.10.96.233";
  }
}
```

### 6.6.1. Signaling Manipulation Script – Cogeco

A signaling manipulation script named **CogecoHdrManip** was created for Cogeco that performs three manipulations represented by three code segments highlighted in the screenshots below.

The first manipulation removes the Remote Address header from all outbound messages from the Avaya SBCE to Cogeco. It is removed because it is not used by the service provider and it contains an internal enterprise IP address which should not be shared outside the enterprise.

The second manipulation changes the host part of the Contact header of the Register message send from the Avaya SBCE to Cogeco. It was modified to use the external IP address of the Avaya SBCE instead of the internal address.

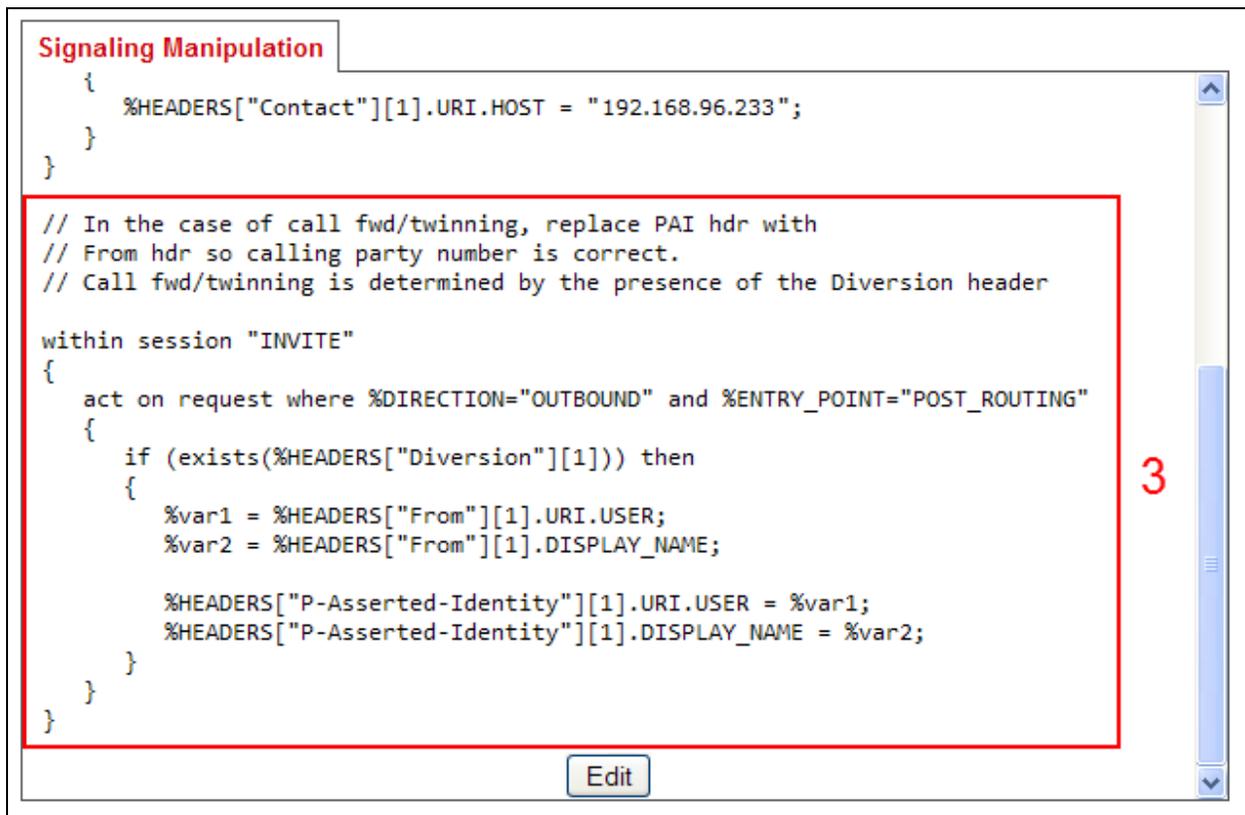
```
Signaling Manipulation

//Remove Remote Address header in outbound INVITE and 200 OK
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"][1]);
  }
}

//Change Contact header in Register Message to external IP
within session "REGISTER"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["Contact"][1].URI.HOST = "192.168.96.233";
  }
}

// In the case of call fwd/twinning, replace PAI hdr with
// From hdr so calling party number is correct.
// Call fwd/twinning is determined by the presence of the Diversion header
```

Lastly, the third manipulation modifies the P-Asserted-Identity (PAI) header in the case of call forwarding and twinning so that the calling party displayed at the far-end is the original PSTN caller instead of the Cogeco pilot number. The script first determines if call forwarding or twinning is in progress by the presence of the Diversion header in the outbound message. If the Diversion header is present, then the script overwrites the calling party information in the PAI header with the calling party information from the From header.



```
Signaling Manipulation
{
  %HEADERS["Contact"][1].URI.HOST = "192.168.96.233";
}

// In the case of call fwd/twinning, replace PAI hdr with
// From hdr so calling party number is correct.
// Call fwd/twinning is determined by the presence of the Diversion header

within session "INVITE"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    if (exists(%HEADERS["Diversion"][1])) then
    {
      %var1 = %HEADERS["From"][1].URI.USER;
      %var2 = %HEADERS["From"][1].DISPLAY_NAME;

      %HEADERS["P-Asserted-Identity"][1].URI.USER = %var1;
      %HEADERS["P-Asserted-Identity"][1].DISPLAY_NAME = %var2;
    }
  }
}
```

3

Edit

## 6.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create a server configuration profile for Avaya IP Office and the service provider SIP server.

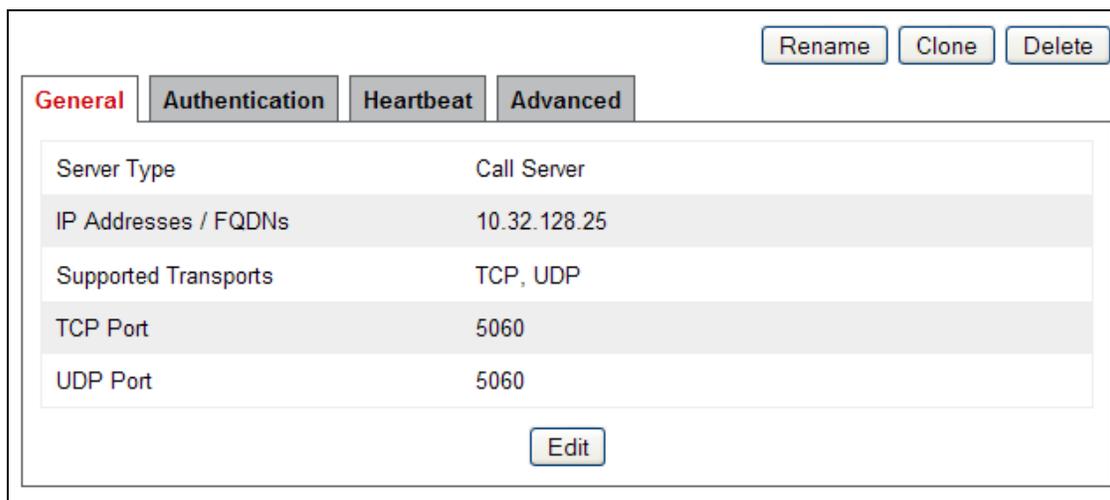
To create a new profile, navigate to **Global Profiles** → **Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The title bar at the top reads "Session Border Controller for Enterprise" on the left and the "AVAYA" logo on the right. A left-hand navigation pane lists various menu items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, **Server Configuration** (highlighted with a red box), and Topology Hiding. The main content area is titled "Server Configuration" and features an "Add" button. Below the button is a "Server Profiles" section that currently displays "No entries found." A prominent blue banner across the center of the main area contains the instruction: "Use the add button to create a new Server Configuration profile."

### 6.7.1. Server Configuration – Avaya IP Office

For the compliance test, server configuration profile **IPO-ACity** was created for Avaya IP Office. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Call Server**.
- Set **IP Addresses / FQDNs** to the IP address of the Avaya IP Office signaling interface.
- Set **Supported Transports** to the transport protocol(s) that can be used for SIP signaling by Avaya IP Office.
- Set the **UDP Port** and **TCP Port** to the ports Avaya IP Office will listen on for SIP requests. The standard SIP UDP/TCP port is 5060.

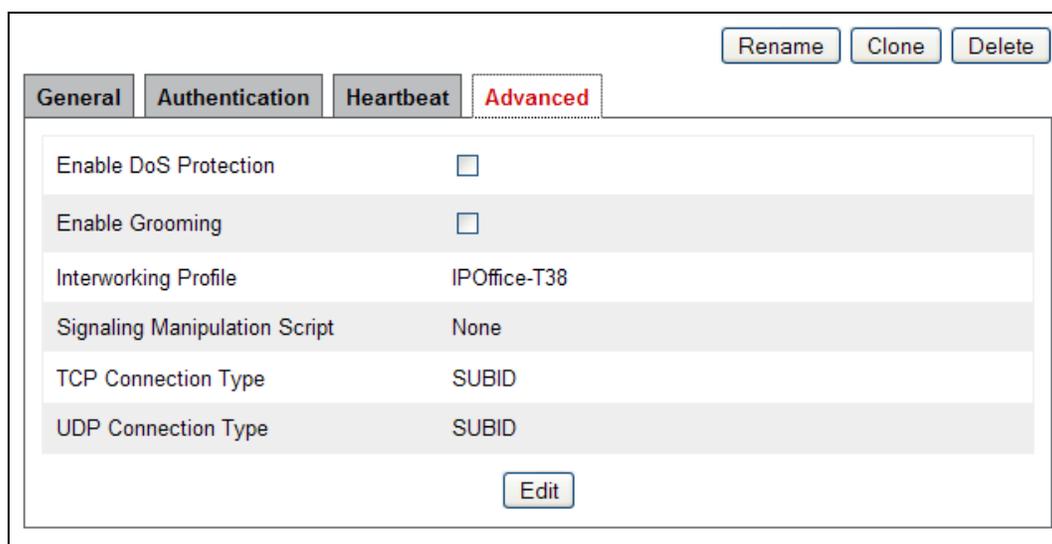


The screenshot shows the configuration interface for a server profile. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below these are four tabs: 'General' (selected), 'Authentication', 'Heartbeat', and 'Advanced'. The configuration table is as follows:

Server Type	Call Server
IP Addresses / FQDNs	10.32.128.25
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

An 'Edit' button is located at the bottom center of the configuration area.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Avaya IP Office defined in **Section 6.5.1**.



The screenshot shows the configuration interface for a server profile, specifically the 'Advanced' tab. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below these are four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced' (selected). The configuration table is as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	IPOffice-T38
Signaling Manipulation Script	None
TCP Connection Type	SUBID
UDP Connection Type	SUBID

An 'Edit' button is located at the bottom center of the configuration area.

## 6.7.2. Server Configuration – Cogeco

For the compliance test, server configuration profile **Cogeco** was created for Cogeco. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Trunk Server**.
- Set **IP Addresses / FQDNs** to the IP address of the Cogeco SIP server.
- Set **Supported Transports** to the transport protocol(s) that can be used for SIP signaling by Cogeco.
- Set the **UDP Port** to the port Cogeco will listen on for SIP requests. The standard SIP UDP port is 5060.

The screenshot shows the configuration interface for the 'Cogeco' server profile. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below these are four tabs: 'General' (selected), 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab contains a table with the following settings:

Server Type	Trunk Server
IP Addresses / FQDNs	192.168.189.168
Supported Transports	UDP
UDP Port	5060

An 'Edit' button is located at the bottom center of the configuration area.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for Cogeco defined in **Section 6.5.2**. Set the **Signaling Manipulation Script** to the SIP manipulation script created in **Section 6.6.1**.

The screenshot shows the configuration interface for the 'Cogeco' server profile, now on the 'Advanced' tab. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below these are four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced' (selected). The 'Advanced' tab contains a table with the following settings:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General-T38
Signaling Manipulation Script	CogecoHdrManip
UDP Connection Type	SUBID

An 'Edit' button is located at the bottom center of the configuration area.

## 6.8. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 6.11**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Avaya IP Office and the Cogeco SIP server.

To view an existing rule, navigate to **Domain Policies** → **Application Rules** in the left pane. In the center pane, select the rule (e.g., **default-trunk**) to be viewed.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies (expanded), Application Rules (highlighted), Border Rules, Media Rules, Security Rules, Signaling Rules, Time of Day Rules, End Point Policy Groups, Session Policies, and TLS Management. The main content area is titled 'Application Rules: default-trunk' and includes an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this is a table for the 'Application Rule' configuration:

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			

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

## 6.9. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 6.11**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Avaya IP Office and the Cogeco SIP server.

To view an existing rule, navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed.

Each of the tabs of the **default-low-med** media rule containing data is shown below.

The **Media NAT** tab has no entries.

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left navigation pane includes: Dashboard, Administration, Backup/Restore, System Management (Global Parameters, Global Profiles, SIP Cluster), and Domain Policies (Application Rules, Border Rules, and Media Rules). The main content area is titled "Media Rules: default-low-med" and includes an "Add" button, a "Filter By Device..." dropdown, and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this are tabs for "Media NAT", "Media Encryption", "Media Anomaly", "Media Silencing", and "Media QoS". The "Media NAT" tab is active, showing a text input field with "Media NAT" and "Learn Media IP dynamically" and an "Edit" button.

The **Media Encryption** tab indicates that no encryption was used.

The screenshot shows the "Media Encryption" configuration tab. It features five tabs: "Media NAT", "Media Encryption" (active), "Media Anomaly", "Media Silencing", and "Media QoS". The configuration is organized into three sections: "Audio Encryption", "Video Encryption", and "Miscellaneous". Under "Audio Encryption", "Preferred Formats" is set to "RTP" and "Interworking" is checked. Under "Video Encryption", "Preferred Formats" is set to "RTP" and "Interworking" is checked. Under "Miscellaneous", "Capability Negotiation" is unchecked. An "Edit" button is located at the bottom of the configuration area.

The **Media Anomaly** tab shows **Media Anomaly Detection** was disabled.

<b>Media NAT</b>	<b>Media Encryption</b>	<b>Media Anomaly</b>	<b>Media Silencing</b>	<b>Media QoS</b>
Media Anomaly Detection <input type="checkbox"/>				
<a href="#">Edit</a>				

The **Media Silencing** tab has no entries.

The **Media QoS** settings are shown below.

<b>Media NAT</b>	<b>Media Encryption</b>	<b>Media Anomaly</b>	<b>Media Silencing</b>	<b>Media QoS</b>
<b>Media QoS Reporting</b>				
RTCP Enabled <input type="checkbox"/>				
<b>Media QoS Marking</b>				
Enabled <input checked="" type="checkbox"/>				
QoS Type DSCP				
<b>Audio QoS</b>				
Audio DSCP EF				
<b>Video QoS</b>				
Video DSCP EF				
<a href="#">Edit</a>				

## 6.10. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 6.11**. For the compliance test, the predefined **default** signaling rule (shown below) was used for both Avaya IP Office and the Cogeco SIP server.

To view an existing rule, navigate to **Domain Policies** → **Signaling Rules** in the left pane. In the center pane, select the rule (e.g., **default**) to be viewed.

The **General** tab settings are shown below.

**Session Border Controller for Enterprise** AVAYA

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

**Signaling Rules: default**

Filter By Device...

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

**General** | Requests | Responses | Request Headers | Response Headers | Signaling QoS | UCID

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

**Content-Type Policy**

Enable Content-Type Checks

Action	Allow	Multipart Action	Allow
--------	-------	------------------	-------

Exception List

The **Requests**, **Responses**, **Request Headers**, **Response Headers** and **UCID** tabs have no entries. The **Signaling QoS** tab is shown below.

**General** | Requests | Responses | Request Headers | Response Headers | **Signaling QoS** | UCID

Signaling QoS

QoS Type DSCP

DSCP AF41

## 6.11. Endpoint Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, an endpoint policy group must be created for Avaya IP Office and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 6.14**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by series of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.

**Session Border Controller for Enterprise** AVAYA

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

**Policy Groups: default-low**

Filter By Device...

It is not recommended to edit the defaults. Try adding a new group instead.

Hover over a row to see its description.

**Policy Group**

Order	Application	Border	Media	Security	Signaling	Time of Day		
<input type="text" value="1"/>	default	default	default-low-med	default-low	default	default	Edit	Clone

### 6.11.1. Endpoint Policy Group – Avaya IP Office

For the compliance test, endpoint policy group **IPO-EP-Policy** was created for Avaya IP Office. Default values were used for each of the rules which comprise the group with the exception of **Application**. For **Application**, enter the application rule referenced in **Section 6.8**. The details of the default settings for **Media** and **Signaling** are showed in **Section 6.9** and **Section 6.10** respectively.

**Policy Group**

Order	Application	Border	Media	Security	Signaling	Time of Day		
<input type="text" value="1"/>	default-trunk	default	default-low-med	default-low	default	default	Edit	Clone

## 6.11.2. Endpoint Policy Group – Cogeco

For the compliance test, endpoint policy group **SP-EP-Policy** was created for the Cogeco SIP server. Default values were used for each of the rules which comprise the group with the exception of **Application**. For **Application**, enter the application rule referenced in **Section 6.8**. Thus, the **SP-EP-Policy** is identical to the **IPO-EP-Policy** created in **Section 6.11.1**.

## 6.12. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 6.14**. Create a routing profile for Avaya IP Office and the service provider SIP server.

To create a new profile, navigate to **Global Profiles** → **Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

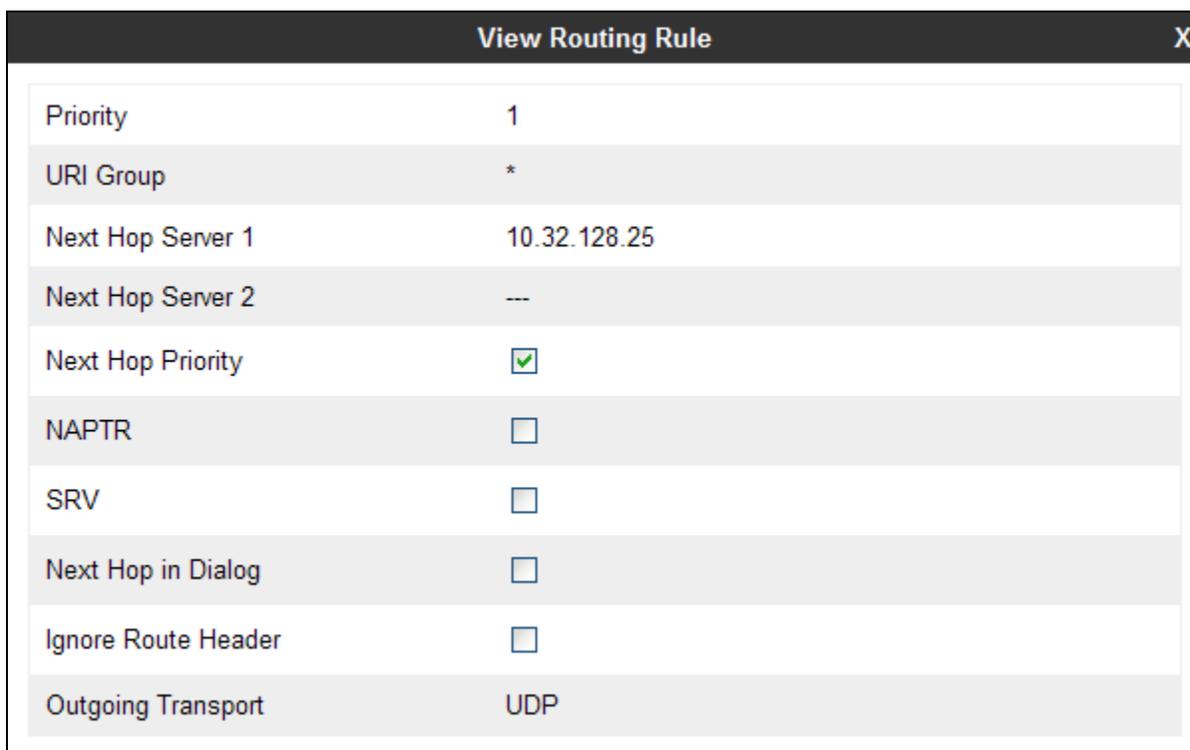
The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top left corner shows the title "Session Border Controller for Enterprise" and the Avaya logo. A navigation menu on the left includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing (highlighted), and Server Configuration. The main content area is titled "Routing Profiles: default" and features 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 "Routing Profile" table is shown with columns: Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. The table contains one entry with Priority "1" and URI Group "\*". "View" and "Edit" links are present for this entry. An "Add" button is also visible in the top right of the table area.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	---	---	<a href="#">View</a> <a href="#">Edit</a>

### 6.12.1. Routing – Avaya IP Office

For the compliance test, routing profile **To-IPO-ACity** was created for Avaya IP Office. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card \* to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of Avaya IP Office signaling interface.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP**. This is the transport protocol the Avaya SBCE will use to send SIP messages to the Avaya IP Office.



View Routing Rule		X
Priority	1	
URI Group	*	
Next Hop Server 1	10.32.128.25	
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	

### 6.12.2. Routing – Cogeco

For the compliance test, routing profile **To-Cogeco** was created for Cogeco. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card \* to match on any URI.
- Set the **Next Hop Server 1** field to the IP address of the Cogeco SIP server.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP** as defined by Cogeco. This is the transport protocol the Avaya SBCE will use to send SIP messages to the Cogeco.

View Routing Rule		X
Priority	1	
URI Group	*	
Next Hop Server 1	192.168.189.168	
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	

## 6.13. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 6.14**. For the compliance test, the predefined **default** topology hiding profile (shown below) was used for Avaya IP Office and a separate profile was created for the Cogeco SIP server.

To add a new profile or view an existing profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add** to add a new profile. In the center pane, select an existing profile (e.g., **default**) to be viewed.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left navigation pane includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, **Topology Hiding** (highlighted), Signaling Manipulation, URI Groups, SIP Cluster, and Domain Policies. The main content area is titled "Topology Hiding Profiles: default" and features 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 is a "Topology Hiding" tab and a table with the following data:

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

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

### 6.13.1. Topology Hiding – Cogeco

The topology hiding profile **Cogeco-TH** was created for the Cogeco SIP server. Since the service provider domain is configured on Avaya IP Office, Avaya IP Office is already sending the domain in most headers. Thus, the Avaya SBCE does not need to change the headers where the domain is present. As a result, the profile **Cogeco-TH** has the **Criteria** set to **IP** only. In addition, Avaya IP Office sends the IP address instead of the domain in the From header of the OPTIONS message. Thus, the topology hiding profile was used to overwrite the IP address in the From header of all messages to the Cogeco domain.

Header	Criteria	Replace Action	Overwrite Value
Referred-By	IP	Auto	---
Request-Line	IP	Auto	---
To	IP	Auto	---
SDP	IP	Auto	---
Record-Route	IP	Auto	---
From	IP	Overwrite	test.cogecodata.com
Via	IP	Auto	---
Refer-To	IP	Auto	---

## 6.14. End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the 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 policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the signaling endpoints are Avaya IP Office and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device (**vnj-sbce2**) to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the far right pane.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The page title is "Session Border Controller for Enterprise" with the AVAYA logo in the top right corner. On the left, a navigation menu lists various system management options, with "Device Specific Settings" expanded to show "End Point Flows" in red. The main content area is titled "End Point Flows: vnj-sbce2". It features two tabs: "Subscriber Flows" and "Server Flows", with "Server Flows" selected. Below the tabs, there is a list of devices, with "vnj-sbce2" selected. To the right of the device list is an "Add" button. A blue callout box contains the text: "Use the add button to create a new Server Flow."

### 6.14.1. End Point Flow – Avaya IP Office

For the compliance test, endpoint flow **IPO-ACity** was created for Avaya IP Office. All traffic from Avaya IP Office will match this flow as the source flow and use the specified **Routing Profile To-Trunks** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Avaya IP Office server created in **Section 6.7.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to \*.
- Set the **Received Interface** to the external signaling interface.
- Set the **Signaling Interface** to the internal signaling interface.
- Set the **Media Interface** to the internal media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Avaya IP Office in **Section 6.11.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.12.2** used to direct traffic to the Cogeco SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Avaya IP Office in **Section 6.13**.

View Flow: IPO-ACity			
<b>Criteria</b>		<b>Profile</b>	
Flow Name	IPO-ACity	Signaling Interface	Int_Sig_Intf
Server Configuration	IPO-ACity	Media Interface	Int_Media_Intf
URI Group	*	End Point Policy Group	IPO-EP-Policy
Transport	*	Routing Profile	To-Cogeco
Remote Subnet	*	Topology Hiding Profile	default
Received Interface	Ext_Sig_Intf	File Transfer Profile	None

## 6.14.2. End Point Flow – Cogeco

For the compliance test, endpoint flow **Cogeco** was created for the Cogeco SIP server. All traffic from Cogeco will match this flow as the source flow and use the specified **Routing Profile To-IPO-ACity** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Cogeco SIP server created in **Section 6.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to \*.
- Set the **Received Interface** to the internal signaling interface.
- Set the **Signaling Interface** to the external signaling interface.
- Set the **Media Interface** to the external media interface.
- Set the **End Point Policy Group** to the endpoint policy group defined for Cogeco in **Section 6.11.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.12.1** used to direct traffic to Avaya IP Office.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Cogeco in **Section 6.13.1**.

View Flow: Cogeco			
<b>Criteria</b>		<b>Profile</b>	
Flow Name	Cogeco	Signaling Interface	Ext_Sig_Intf
Server Configuration	Cogeco	Media Interface	Ext_Media_Intf
URI Group	*	End Point Policy Group	SP-EP-Policy
Transport	*	Routing Profile	To-IPO-ACity
Remote Subnet	*	Topology Hiding Profile	Cogeco-TH
Received Interface	Int_Sig_Intf	File Transfer Profile	None

## 7. Cogeco SIP Trunking Configuration

Cogeco is responsible for the configuration of the Cogeco SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. In the case of the compliance test, this is the Avaya SBCE public address. Cogeco will provide the customer the necessary information to configure the Avaya IP Office and Avaya SBCE including:

- IP address of the Cogeco SIP proxy
- SIP Credentials – user name and password
- Pilot number and DID numbers

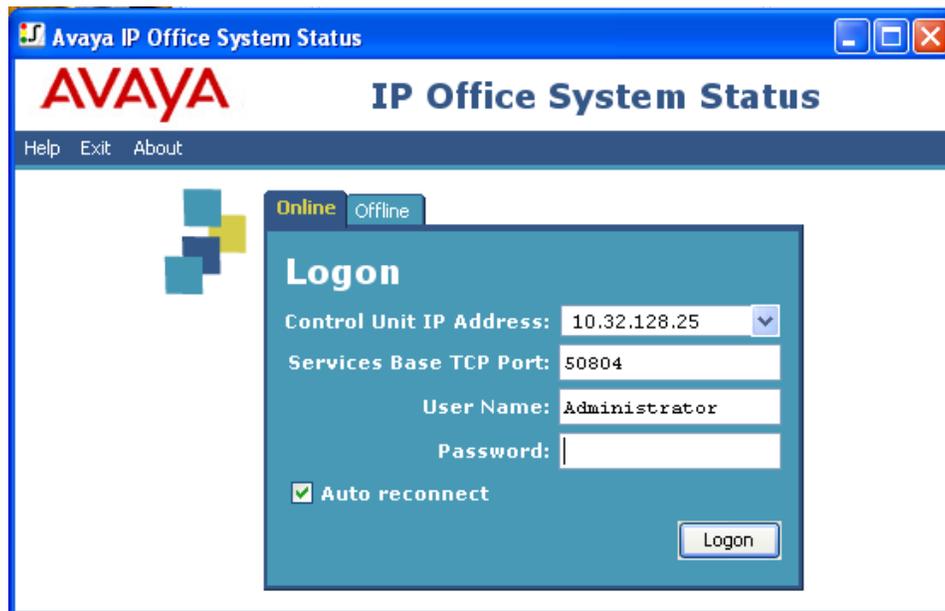
## 8. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

### 8.1. System Status

The System Status application is used to monitor and troubleshoot Avaya IP Office. Use the System Status application to verify the state of the SIP trunk. System Status can be accessed from **Start → Programs → IP Office → System Status**.

The following screen shows an example **Logon** screen. Enter the Avaya IP Office IP address in the **Control Unit IP Address** field, and enter an appropriate **User Name** and **Password**. Click **Logon**.



Select the SIP line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** is **Idle** for each channel.

The screenshot shows the AVAYA IP Office System Status interface. The left pane shows a tree view with 'Trunks (16)' expanded to 'Line: 23'. The right pane has tabs for 'Status', 'Utilization Summary', 'Alarms', and 'Registration'. The 'Status' tab is active, displaying a 'SIP Trunk Summary' with the following details:

- Peer Domain Name: test.cogecodata.com
- Resolved Address: 10.32.128.20
- Line Number: 23
- Number of Administered Channels: 10
- Number of Channels in Use: 0
- Administered Compression: G711 Mu
- Silence Suppression: Off
- Layer 4 Protocol: UDP
- SIP Trunk Channel Licenses: Unlimited
- SIP Trunk Channel Licenses in Use: 0
- SIP Device Features: (represented by a green circle and 0%)

Below the summary is a table with the following columns: Channel Number, U..., Call Ref, Current State, Time in State, Remote Media A..., Co..., Conne..., Caller ID or Dia..., Other Party on Call, Directi..., Round Trip D..., Receive Jitter, Receive Packe..., Transmit Jitter, and Transmit Packe... The table contains four rows, all with 'Idle' as the current state and '4 day...' as the time in state.

Channel Number	U...	Call Ref	Current State	Time in State	Remote Media A...	Co...	Conne...	Caller ID or Dia...	Other Party on Call	Directi...	Round Trip D...	Receive Jitter	Receive Packe...	Transmit Jitter	Transmit Packe...
1			Idle	4 day...											
2			Idle	4 day...											
3			Idle	4 day...											
4			Idle	4 day...											

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

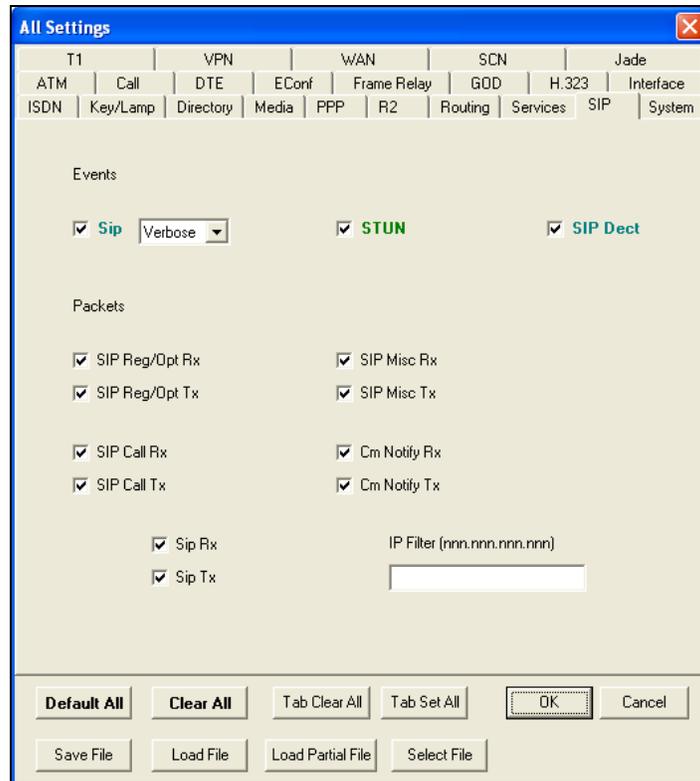
The screenshot shows the 'Alarms' tab selected in the AVAYA IP Office System Status interface. The title is 'Alarms for Line: 23 SIP test.cogecodata.com'. Below the title is a table with the following columns: Last Date Of Error, Occurrences, and Error Description. The table is currently empty, indicating no active alarms.

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

## 8.2. Monitor

The Monitor application can also be used to monitor and troubleshoot Avaya IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select **Filters → Trace Options**.

The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, all SIP settings are checked.



## 9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office 9.0 and the Avaya Session Border Controller for Enterprise 6.2 to the Cogeco SIP Trunking Service. The Cogeco SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks. The Cogeco SIP Trunking Service passed compliance testing. Please refer to **Section 2.2** for any exceptions.

## 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 IP500/IP500 V2 Installation*, Document Number 15-601042, Issue 28p, March 26, 2014.
- [2] *IP Office Release 9.0 Manager*, Document Number 15-601011, Issue 9.02.0, January 6, 2014.
- [3] *Using System Status*, Document Number 15-601758, Issue 09c, August 15, 2013.
- [4] *IP Office Release 9.0 Administering Voicemail Pro*, Document Number 15-601063, Issue 9.01.0, September 13, 2013.
- [5] *Using IP Office System Monitor*, Document Number 15-601019, Issue 05e, February 5, 2014.

Additional Avaya 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](mailto:devconnect@avaya.com).