



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Voice Carrier IntelliSIP Trunking Service with Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise 6.2 – Issue 1.0

Abstract

These Application Notes describes the steps to configure Session Initiation Protocol (SIP) Trunking between Voice Carrier and an enterprise solution using Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise 6.2.

The Voice Carrier IntelliSIP Trunking Service provides PSTN access via a SIP trunk between the enterprise and the Voice Carrier network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise. Voice Carrier 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 Voice Carrier and an enterprise solution using Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise 6.2.

The Voice Carrier IntelliSIP 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 Voice Carrier IntelliSIP Trunking Service will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection.

2. General Test Approach and Test Results

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.

The general test approach was to connect a simulated enterprise site to the Voice Carrier IntelliSIP 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.

The Voice Carrier IntelliSIP Trunking Service passed compliance testing with the observations or limitations described in **Section 2.2**.

2.1. Interoperability Compliance Testing

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

- Use of UDP or TCP for the transport layer to the service provider
- Sending and receiving SIP OPTIONS queries to the service provider
- Incoming PSTN calls to SIP and H.323 telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from SIP and H.323 at the enterprise. All outgoing PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from soft clients. Avaya IP Office Video Softphone and Avaya Flare® Experience for Windows were tested.
- Various call types including: local, long distance, outbound toll-free, international and local directory assistance.
- Codec G.711MU

- Caller ID presentation and Caller ID restriction
- DTMF transmission using RFC 2833
- Voicemail navigation using DTMF for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and twinning
- G.711 pass-through fax
- REFER message for network call redirection

Inbound toll-free calls and 911 emergency calls are supported but were not tested as part of the compliance test.

The following items are not supported:

- G.729 codec
- Operator (dial 0) and operator-assisted (dial 0 + 10 digits) services
- T.38 Fax

2.2. Test Results

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

- **Codec not locked down on outbound calls:** On outbound calls, Voice Carrier responds to the INVITE request with multiple codecs, instead of selecting one from the INVITE SDP list. IP Office uses the first compatible codec in the list. This behavior has no user impact. Calls were successful.
- **Inconsistent SIP headers on inbound Calling Party Number blocked calls:** On inbound Calling Party Number (CPN) blocked calls, Voice Carrier sends a SIP INVITE message containing two headers which contradict each other. The INVITE contains the Privacy = none header which indicates that the calling party number should not be blocked. The INVITE also contains the Remote-Party-ID header with parameter privacy=full which indicates that the calling party number should be blocked. In this scenario, IP Office blocked the calling party number as intended. The call was successful.
- **Blind transfer with Avaya 1100 IP Deskphones calling party number:** An Avaya 1100 Series IP Deskphone (SIP) places an outbound call to the PSTN, then performs a blind transfer of this call to another PSTN endpoint. In this scenario, the wrong calling party number is displayed on the second PSTN endpoint. The display shows the number dialed by the Avaya 1100 Series IP Deskphone for the initial outbound call including the short code (9) + 1 + 10 digits. The behavior is expected to be the same as with IP Office H.323 endpoints which is to display the transferring party number. This is an IP Office issue and is under investigation by the IP Office development team.

2.3. Support

For technical support on the Voice Carrier IntelliSIP Trunking Service, contact Voice Carrier using the Support links at www.voicecarrier.com or by calling 1-888-830-6230.

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 Voice Carrier IntelliSIP 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).

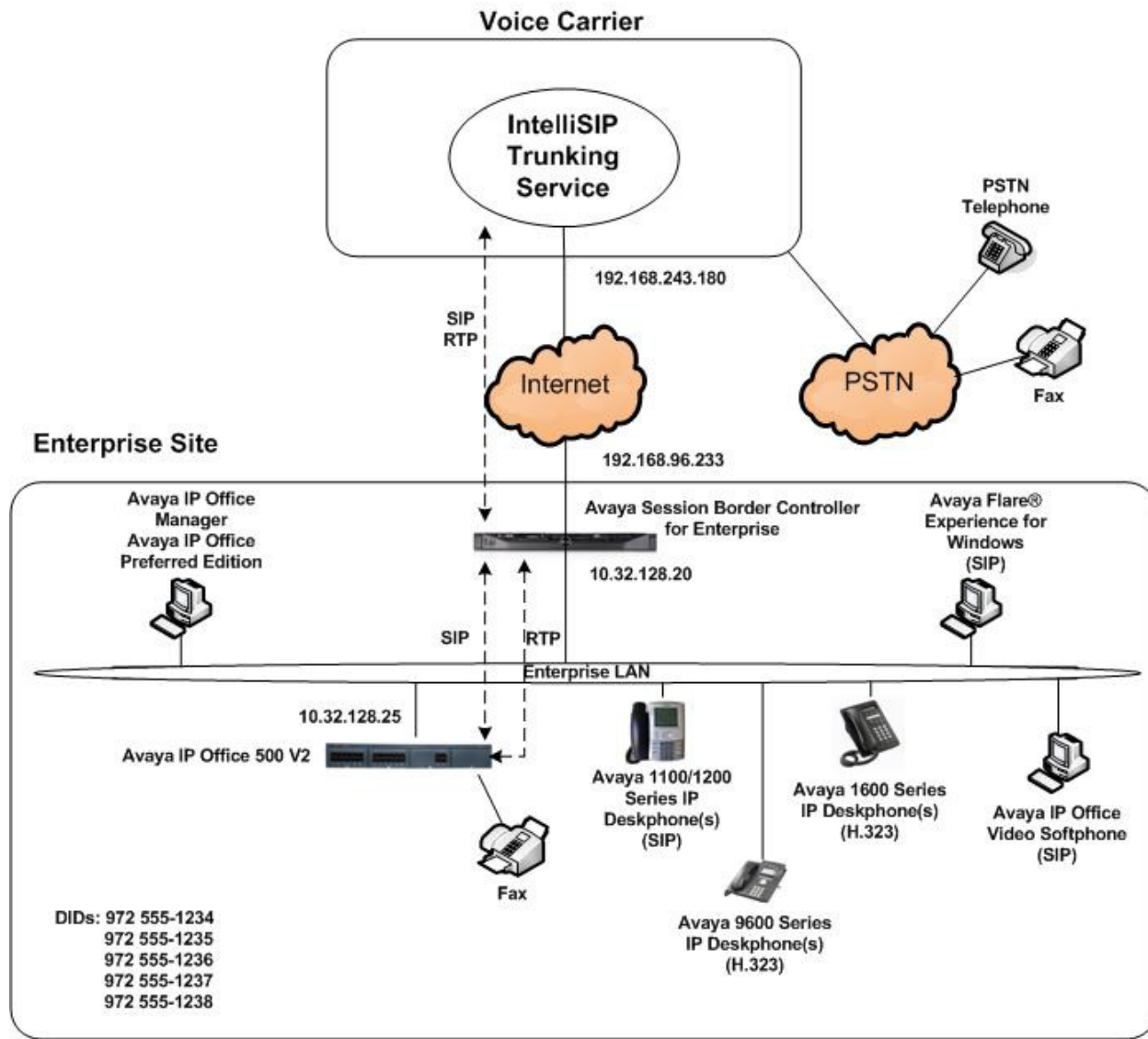


Figure 1: Avaya Interoperability Test Lab Configuration

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 Voice Carrier. The short code of 9 and any preceding 1 is stripped off by Avaya IP Office and the remaining 10 digits were sent unaltered to Voice Carrier. For outbound calls, Avaya IP Office sent 10 digits in all headers. For inbound calls, the Voice Carrier IntelliSIP Trunking Service sent 10 digits in the Request URI and the To field of inbound SIP INVITE messages.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment	Software
Avaya IP Office 500 v2	8.1 (69)
Avaya IP Office Manager	10.1 (69)
Avaya IP Office Preferred Edition (Voicemail)	8.1 (9203)
Avaya Session Border Controller for Enterprise running on a Portwell CAD-0208 server	6.2.0.Q36
Avaya 1140E IP Deskphone (SIP)	4.3 SP1 (04.03.12.00)
Avaya 1608 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP3 (1.3.3)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.2 SP2 (6.2209)
Avaya IP Office Video Softphone (SIP)	3.2.3.48 (67009)
Avaya Flare® Experience for Windows	1.1.2.11

Voice Carrier Components	
Equipment	Software
IntelliSIP	2.1 – av1.6.2.18

Testing was performed with IP Office 500 V2 R8.1, but this testing also applies to IP Office Server Edition R8.1. Note that IP Office Server Edition requires an Expansion IP Office 500 V2 R8.1 to support analog or digital endpoints or trunks. Also, IP Office 500 V2 does not support SIP Direct Media so Server Edition SIP Direct Media functionality was not compliance tested.

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:

WELCOME to IP Office Administration

What would you like to do ?

[Create an Offline Configuration](#)

[Open Configuration from System](#)

[Read a Configuration from File](#)

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.

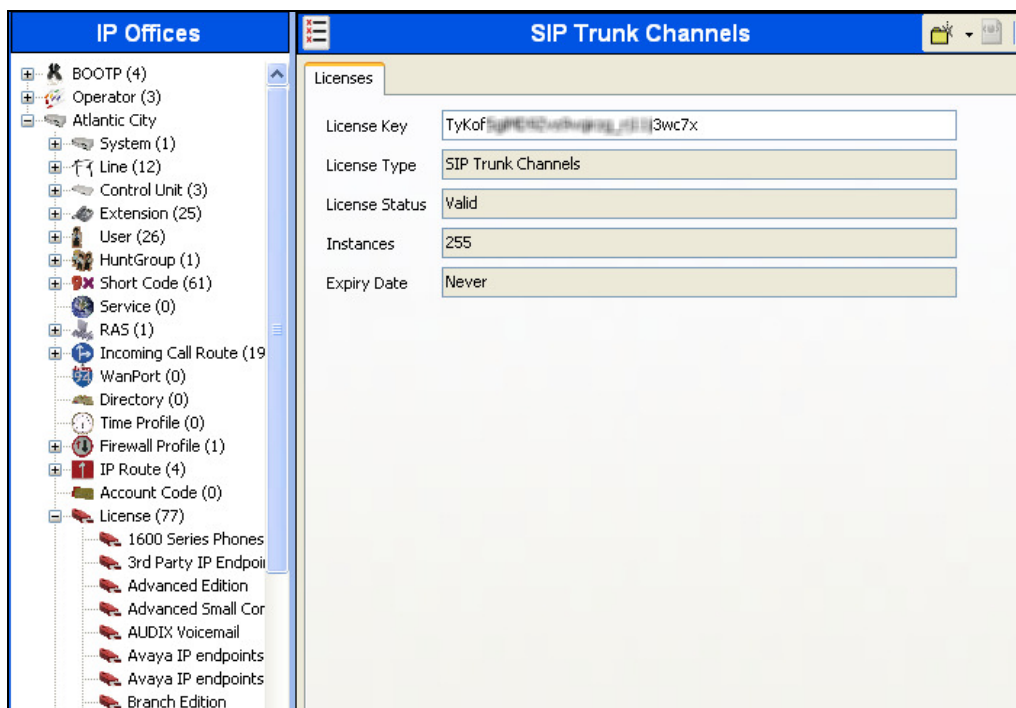
The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this document, the **View** menu was configured to show the Navigation pane on the left side, omit the Group pane in the center, and show the Details pane on the right side. Since the Group 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 the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License** → **SIP Trunk Channels** in the Navigation pane. Confirm a valid license with sufficient **Instances** (trunk channels) in the Details pane.



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**.

IP Offices

- + BOOTP (4)
- + Operator (3)
- + Atlantic City
 - + System (1)
 - + Line (14)
 - + Control Unit (3)
 - 1 IP 500 V2
 - 2 COMBO6210/ATM4
 - 3 DIGSTA8/ATM4
- + Extension (25)
- + User (27)
- + HuntGroup (1)
- + Short Code (61)
- + Service (0)

IP 500 V2

Unit	
Device Number	1
Unit Type	IP 500 V2
Version	8.1 (69)
Serial Number	00000000e3
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 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 contains 'System (1)' and 'Atlantic City'. The 'Atlantic City' system is selected. The main pane on the right is titled 'Atlantic City' and contains 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 'LAN Settings' section includes the following fields and options:

- 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 (radio buttons). The 'Disabled' option is selected.
- Advanced:** A button to expand advanced settings.

On the **VoIP** tab in the Details Pane, 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. 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 Voice Carrier. All other parameters should be set according to customer requirements.

Atlantic City

System LAN1 LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR Twinning VCM CCR C

LAN Settings VoIP Network Topology SIP Registrar

☒ H.323 Gatekeeper Enable

☒ SIP Trunks Enable

☒ SIP Registrar Enable

☐ H.323 Auto-create Extn

☐ H.323 Auto-create User

☐ H.323 Remote Extn Enable

☒ Enable RTCP Monitoring On Port 5005

RTP Port Number Range

Port Range (Minimum) 49152

Port Range (Maximum) 53246

DiffServ Settings

B8 DSCP(Hex) FC DSCP Mask (Hex) 88 SIG DSCP (Hex)

46 DSCP 63 DSCP Mask 34 SIG DSCP

DHCP Settings

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

RTP Keepalives

Scope Disabled Periodic timeout 0

Initial keepalives Disabled

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 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 Avaya IP Office will listen on.
- All other parameters should be set according to customer requirements.

The screenshot shows the 'Atlantic City' configuration window. The 'Network Topology' tab is selected. The 'Network Topology Discovery' section contains the following fields and controls:

- STUN Server IP Address: 10 . 90 . 168 . 13
- STUN Port: 3478
- Firewall/NAT Type: Open Internet (dropdown menu)
- Binding Refresh Time (seconds): 30
- Public IP Address: 0 . 0 . 0 . 0
- Public Port: 5060
- Buttons: Run STUN, Cancel
- Checkbox: ☐ Run STUN on startup

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 window with the 'Telephony' tab selected. The interface is divided into several sections:

- System Navigation:** A top bar with tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony (selected), Directory Services, System Events, SMTP, SMDR, Twinning, VCM, CCR, and Codecs.
- Sub-Tabs:** Under the 'Telephony' tab, there are sub-tabs for Telephony, Tones & Music, and Call Log.
- Analogue Extensions:** A section on the left containing:
 - Default Outside Call Sequence: Normal (dropdown)
 - Default Inside Call Sequence: Ring Type 1 (dropdown)
 - Default Ring Back Sequence: Ring Type 2 (dropdown)
 - Restrict Analogue Extension Ringer Voltage: ☐
 - Dial Delay Time (secs): 4 (spinner)
 - Dial Delay Count: 0 (spinner)
 - Default No Answer Time (secs): 25 (spinner)
 - Hold Timeout (secs): 0 (spinner)
 - Park Timeout (secs): 300 (spinner)
 - Ring Delay (secs): 5 (spinner)
 - Call Priority Promotion Time (secs): Disabled (dropdown)
 - Default Currency: USD (dropdown)
 - Default Name Priority: Favor Trunk (dropdown)
- Companding Law:** A section on the right with two columns:
 - Switch:** U-Law (selected), A-Law (radio button).
 - Line:** U-Law Line (selected), A-Law Line (radio button).
- Advanced Settings:** A list of checkboxes on the right:
 - ☐ DSS Status
 - ☒ Auto Hold
 - ☒ Dial By Name
 - ☒ Show Account Code
 - ☐ Inhibit Off-Switch Forward/Transfer
 - ☐ Restrict Network Interconnect
 - ☐ Drop External Only Impromptu Conference
 - ☐ Visually Differentiate External Call
 - ☐ Unsupervised Analog Trunk Disconnect Handling
 - ☒ High Quality Conferencing

5.2.3. System - Twinning Tab

To view or change the System Twinning settings, navigate to the **Twining** 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).

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

5.3. 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 for the enterprise network.
- Set **Destination** to **LAN1** from the drop-down list.

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

The screenshot shows the 'IP Route' configuration window for the '0.0.0.0' route. The left pane shows the 'IP Offices' tree with '0.0.0.0' selected. The main pane shows the configuration for the 'IP Route' with the following values: IP Address (0.0.0.0), IP Mask (0.0.0.0), Gateway IP Address (10.32.128.254), Destination (LAN1), and Metric (0). The 'Proxy ARP' checkbox is unchecked.

5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Voice Carrier IntelliSIP Trunking Service. To create a SIP line, right-click **Line** in the Navigation Pane and select **New → SIP Line**.

5.4.1. SIP Line – SIP Line Tab

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

- Set **ITSP Domain Name** to the domain provided by Voice Carrier.
- Set **Send Caller ID** to **Diversion Header**. With this setting and the related configuration in **Section 5.2.3**, IP Office will include the Diversion Header for calls that are directed via Mobile Twinning out the SIP Line to Voice Carrier. It will also include the Diversion Header for calls that are call forwarded out the SIP Line.
- Check **REFER Support**.
- Check the **In Service** box. This makes the trunk available to incoming and outgoing calls.
- Check the **Check OOS** box. IP Office will use the SIP OPTIONS method to periodically check the SIP Line. The time between SIP OPTIONS sent by IP Office will use the **Binding Refresh Time** for LAN1, as shown in **Section 5.2.1**.
- Default values may be used for all other parameters.

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane with a tree structure including BOOTP (4), Operator (3), Atlantic City, System (1), Line (14) (selected), Control Unit (3), Extension (25), User (27), HuntGroup (1), Short Code (61), Service (0), RAS (1), Incoming Call Route (28), WanPort (0), Directory (0), Time Profile (0), Firewall Profile (1), IP Route (4), Account Code (0), License (77), Tunnel (0), User Rights (8), ARS (2), RAS Location Request (0), and E911 System (1). The main area is titled 'SIP Line - Line 22' and contains several tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, and SIP Credentials. The 'SIP Line' tab is active, showing the following configuration fields:

Line Number	22	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name	avayatest.callingcloud.net	Use Tel URI	<input type="checkbox"/>
Prefix		Check OOS	<input checked="" type="checkbox"/>
National Prefix	0	Call Routing Method	Request URI
Country Code		Originator number for forwarded and twinning calls	
International Prefix	00	Name Priority	System Default
Send Caller ID	Diversion Header	Caller ID from From header	<input type="checkbox"/>
Association Method	By Source IP address	Send From In Clear	<input type="checkbox"/>
<input checked="" type="checkbox"/> REFER Support		User-Agent and Server Headers	
Incoming	Auto		
Outgoing	Auto		
UPDATE Supported	Never		

5.4.2. SIP Line - Transport Tab

Select the **Transport** tab. Set 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 'SIP Line - Line 22' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' is set to '10.32.128.20'. The 'Network Configuration' section shows 'Layer 4 Protocol' set to 'UDP', 'Send Port' set to '5060', 'Use Network Topology Info' set to 'LAN 1', and 'Listen Port' set to '5060'. The 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0' and '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is checked. The 'Separate Registrar' field is empty.

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
Calls Route via Registrar	<input checked="" type="checkbox"/>
Separate Registrar	

5.4.3. 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**, **Display Name** and **PAI** to **Use Internal Data**. This setting allows calls on this line whose SIP URI matches the number set in the **SIP** tab of any User as shown in **Section 5.7**.
- For **Registration**, select **0: <None>** 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**. 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 **22** was defined that only contained this line (line 22).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

Click **OK**.

The screenshot displays the 'SIP Line - Line 22*' configuration window. The 'SIP URI' tab is selected. The main area contains a table with columns: Channel, Groups, Via, Local URI, Contact, Display Name, PAI, Credential, and Max Calls. Below the table is the 'New Channel' section. The fields in this section are: Via (10.32.128.25), Local URI (Use Internal Data), Contact (Use Internal Data), Display Name (Use Internal Data), PAI (Use Internal Data), Registration (0: <None>), Incoming Group (22), Outgoing Group (22), and Max Calls per Channel (10). Buttons for 'Add...', 'Remove', 'Edit...', 'OK', and 'Cancel' are located on the right side of the window.

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**, **Display Name** and **PAI** fields.

5.4.4. SIP Line - VoIP Tab

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

- For **Codec Selection**, select **System Default** from the pull-down menu. A list of the codecs in their current order of preference is shown on the right in the **Selected** column. The compliance test used the default codec list. 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.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box.
- Set the **Fax Transport Support** to **G.711**.
- 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 shows the 'SIP Line - Line 22' configuration window with the 'VoIP' tab selected. The window has a title bar with standard icons and a tab bar with 'SIP Line', 'Transport', 'SIP URI', 'VoIP', 'T38 Fax', and 'SIP Credentials'. The 'VoIP' tab is active. The 'Codec Selection' dropdown is set to 'System Default'. Below it are two columns: 'Unused' (empty) and 'Selected' (containing G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP, and G.723.1 6K3 MP-MLQ). Between the columns are buttons for moving items (>>, <<, up, down) and a '>>' button at the bottom. To the right of the columns are checkboxes for 'VoIP Silence Suppression' (unchecked), 'Re-invite Supported' (checked), 'Use Offerer's Preferred Codec' (unchecked), 'Codec Lockdown' (unchecked), and 'PRACK/100rel Supported' (unchecked). Below the codec columns are three fields: 'Fax Transport Support' set to 'G.711', 'Call Initiation Timeout (s)' set to '4', and 'DTMF Support' set to 'RFC2833'.

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 Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, which includes a tree view with categories like BOOTP (4), Operator (3), Atlantic City, System (1), Line (14), Control Unit (3), Extension (25), User (27), HuntGroup (1), Short Code (61), Service (0), and RAS (1). The 'Short Code (61)' item is selected. The main area on the right is titled '9N;; Dial' and contains the 'Short Code' configuration tab. This tab has several fields: 'Code' with the value '9N;;', 'Feature' set to 'Dial' via a dropdown, 'Telephone Number' with the value 'N', 'Line Group ID' set to '51: SP SIP Route' via a dropdown, 'Locale' with an empty dropdown, and 'Force Account Code' which is an unchecked 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 Voice Carrier documented in these Application Notes, when a user dials *67 plus the number, IP Office will include the user’s telephone number in the P-Asserted-Identity (PAI) header and will include the Privacy: Id header. Voice Carrier will allow the call due to the presence of a valid DID in the PAI header, but will prevent presentation of the caller id to the called PSTN destination.

*67N;; Dial	
Short Code	
Code	<input type="text" value="*67N;"/>
Feature	<input type="text" value="Dial"/>
Telephone Number	<input type="text" value="WN"/>
Line Group ID	<input type="text" value="51: SP SIP Route"/>
Locale	<input type="text"/>
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, two entries were created. The first entry matches on any 1 + 10 digit number (**1XXXXXXXXXX**) and then sends only 10 digits (**N**) in the SIP INVITE message on the line group defined in **Section 5.4.3** (e.g., line group 22). The second entry matches on any other number (**N**) and passes it unaltered to the line group.

To create an entry, click the **Add** button and enter the following in the pop-up window.

- 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 short code will perform.
- Set **Telephone Number** to **N"@avayatest.callingcloud.net"**. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. In the first entry, **N** represents the remaining 10 digits after removing the preceding 1. In the second entry, the value **N** represents the complete number passed to ARS. The domain **avayatest.callingcloud.net** is the service provider domain provided by Voice Carrier.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4.3**. This short code will use this line group when placing the outbound call.

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

Code	Telephone Number	Feature	Line Group ID
1XXXXXXXXXX;	N"@avayatest.callingcloud.net"	Dial	22
N;	N"@avayatest.callingcloud.net"	Dial	22

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 5.4.3**). 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 Voice Carrier. 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 the 'IP Offices' navigation pane with a tree structure including: BOOTP (4), Operator (3), Atlantic City, System (1), Line (14), Control Unit (3), Extension (25), User (27) (highlighted), HuntGroup (1), Short Code (61), Service (0), and RAS (1). The main area is titled 'Extn243: 243' and contains a tabbed interface. The 'SIP' tab is selected, showing the following fields: 'SIP Name' with value '9725551236', 'SIP Display Name (Alias)' with value 'Extn243', and 'Contact' with value '9725551236'. Below these fields is an 'Anonymous' checkbox, which is currently unchecked. Other tabs visible include User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, Menu Programming, Mobility, Phone Manager Options, Hunt Group Membership, Announcements, and Pers.

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 5.4.3**.
- 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 'Incoming Call Route' configuration window with the 'Standard' tab selected. The title bar displays '22 9725551236'. The left navigation pane shows a tree structure with 'Incoming Call Route (28)' selected. The main area contains the following fields:

Field	Value
Bearer Capacity	Any Voice
Line Group ID	22
Incoming Number	9725551236
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source

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 9725551236 on line 22 are routed to extension 243.

The screenshot shows the 'Incoming Call Route' configuration window with the 'Destinations' tab selected. The title bar displays '22 9725551236'. The left navigation pane shows a tree structure with 'Incoming Call Route (28)' selected. The main area contains a table with the following data:

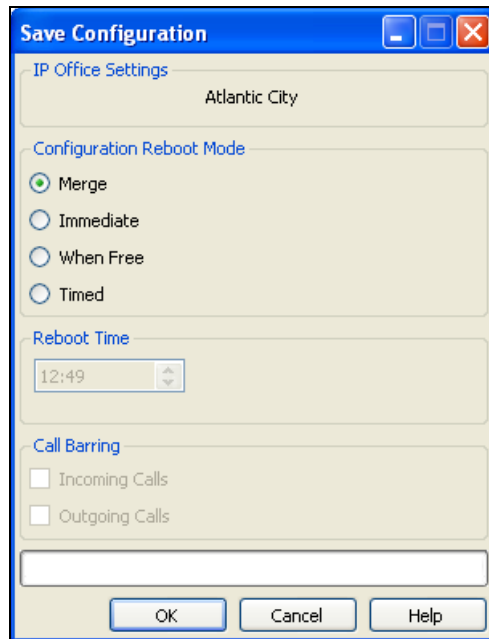
TimeProfile	Destination	Fallback Extension
Default Value	243 Extn243	

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

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 image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold. On the right, under the heading 'Log In', there are two input fields for 'Username:' and 'Password:', followed by a 'Log In' button. Below the login fields, there is a disclaimer: '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.' This is followed by a statement: '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.' Then, 'All users must comply with all corporate instructions regarding the protection of information assets.' At the bottom, it says '© 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



Dashboard

Administration

Backup/Restore

System Management

- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- TLS Management
- Device Specific Settings

Dashboard

Information		
System Time	02:41:48 PM EDT	Refresh
Version	6.2.0.Q36	
Build Date	Thu Feb 14 23:25:50 UTC 2013	

Alarms (past 24 hours)	
None found.	

Incidents (past 24 hours)	
None found.	

Notes

No notes found.

Add

Installed Devices	
EMS	
vnj-sbce2	

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
‣ TLS Management
‣ Device Specific Settings

System Management

Devices Updates SSL VPN Licensing

Device Name (Serial Number)	Management IP	Version	Status						
vnj-sbce2 (IFCS11010169)	10.32.101.20	6.2.0.Q36	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. 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

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 left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. Under Device Specific Settings, the 'Network Management' option is highlighted in red. The main content area is titled 'Network Management: vnj-sbce2'. It features a 'Devices' tab with 'vnj-sbce2' selected. Below this, there are two tabs: 'Network Configuration' and 'Interface Configuration'. The 'Interface Configuration' tab is active, showing a table with the following data:

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

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. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the private interface (A1) 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 SIP requests from Avaya IP Office for each transport protocol. For the compliance test, the **UDP Port** was set to **5060**.

Signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- 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 SIP requests from the service provider for each transport protocol. For the compliance test, both UDP and TCP were tested with Voice Carrier. Thus, the **UDP Port** and **TCP Port** were set to **5060**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings (expanded). Under Device Specific Settings, there are links for Network Management, Media Interface, and Signaling Interface (highlighted in red). The main content area is titled 'Signaling Interface: vnj-sbce2'. It features a 'Devices' tab with 'vnj-sbce2' selected, and a 'Signaling Interface' tab with an 'Add' button. Below the tabs is a table listing the configured signaling interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig_Intf	10.32.128.20	---	5060	---	None	Edit Delete
Ext_Sig_Intf	192.168.96.233	5060	5060	---	None	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, signaling interface **Int_Media_Intf** was created for the Avaya SBCE internal interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 6.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and Avaya IP Office. For the compliance test, the port range used was selected arbitrarily.

Signaling interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- 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 service provider. For the compliance test, the port range used was selected arbitrarily.

Session Border Controller for Enterprise



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

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	
Int_Media_Intf	10.32.128.20	35000 - 40000	Edit Delete
Ext_Media_Intf	192.168.96.233	35000 - 40000	Edit Delete

CTM; Reviewed:
SPOC 9/20/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

30 of 56
VCIPO81SBCE62

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 sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Fingerprint, **Server**, **Interworking** (highlighted), Phone Interworking, Media Forking, Routing, and Server Configuration. The main content area is titled "Interworking Profiles: cs2100" and includes an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this, there are tabs for "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of interworking parameters:

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No

6.5.1. Server Interworking – Avaya IP Office

For the compliance test, server interworking profile **IPOffice** was created for Avaya IP Office by creating a new profile and accepting the default values for all settings. The **General** tab parameters are shown below.

The screenshot displays the configuration interface for the Avaya IP Office, specifically the 'General' tab. The interface includes a top navigation bar with tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing a list of settings. The settings are organized into three sections: 'General', 'Privacy', and 'DTMF'. Each section has a dark header bar. The 'General' section includes settings for 'Hold Support', '180 Handling', '181 Handling', '182 Handling', '183 Handling', 'Refer Handling', '3xx Handling', 'Diversion Header Support', 'Delayed SDP Handling', 'T.38 Support', 'URI Scheme', and 'Via Header Format'. The 'Privacy' section includes 'Privacy Enabled', 'User Name', 'P-Asserted-Identity', 'P-Preferred-Identity', and 'Privacy Header'. The 'DTMF' section includes 'DTMF Support'. An 'Edit' button is located at the bottom right of the configuration area.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

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

DTMF	
DTMF Support	None

[Edit](#)

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
				Edit

6.5.2. Server Interworking – Voice Carrier

For the compliance test, server interworking profile **SP-General** was created for the Voice Carrier SIP server. When creating the profile, the default values were used for all parameters. Thus, the **SP-General** profile is identical to the **IPOffice** profile created in **Section 6.5.1**.

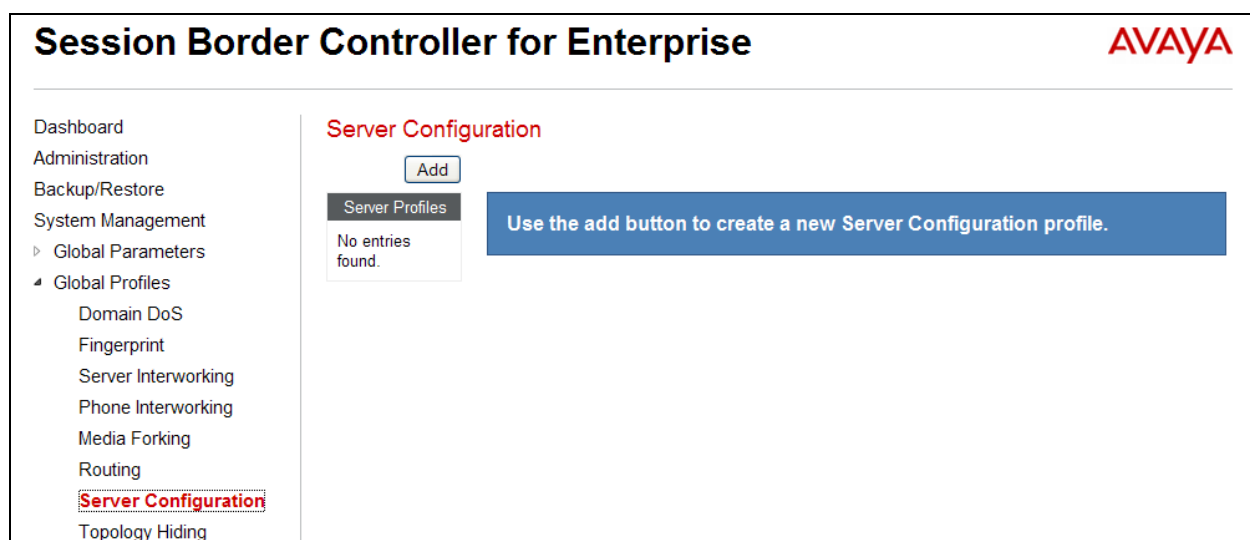
6.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be done by other configuration within the Avaya SBCE. It was not necessary to create any signaling manipulation scripts for interoperability with Voice Carrier.

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.



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 used for SIP signaling between Avaya IP Office and the Avaya SBCE.
- Set the **UDP Port** to the port Avaya IP Office will listen on for SIP requests from the Avaya SBCE.

The screenshot shows the 'General' tab of a configuration window. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below the tabs are four configuration rows, each with a label and a value, followed by an 'Edit' button at the bottom.

General	Authentication	Heartbeat	Advanced
Server Type	Call Server		
IP Addresses / FQDNs	10.32.128.25		
Supported Transports	UDP		
UDP Port	5060		

Edit

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 'Advanced' tab of the same configuration window. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below the tabs are five configuration rows, each with a label and a value, followed by an 'Edit' button at the bottom.

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

Edit

6.7.2. Server Configuration – Voice Carrier

For the compliance test, server configuration profile **VoiceCarrier** was created for Voice Carrier. 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 Voice Carrier SIP server.
- Set **Supported Transports** to the transport protocol used for SIP signaling between Voice Carrier and the Avaya SBCE. In the compliance test, both UDP and TCP were tested.
- Set the **UDP Port** or **TCP Port**, whichever applies, to the standard SIP port of 5060. This is the port Voice Carrier will listen on for SIP requests from the Avaya SBCE. The example below shows the use of UDP.

The screenshot shows the 'General' tab of a configuration interface. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below these are tabs for 'General' (selected), 'Authentication', 'Heartbeat', and 'Advanced'. The configuration table below has the following data:

Server Type	Trunk Server
IP Addresses / FQDNs	192.168.243.180
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 Voice Carrier defined in **Section 6.5.2**.

The screenshot shows the 'Advanced' tab of the same configuration interface. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below these are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced' (selected). The configuration table below has the following data:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	None
TCP 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 Voice Carrier 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.

Session Border Controller for Enterprise

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▸ Global Profiles

▸ SIP Cluster

▸ Domain Policies

▸ **Application Rules**

▸ Border Rules

▸ Media Rules

▸ Security Rules

▸ Signaling Rules

▸ Time of Day Rules

▸ End Point Policy Groups

▸ Session Policies

▸ TLS Management

Application Rules: default-trunk

Add

Filter By Device...

Clone

Application Rules

default

default-trunk

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

Application Rule

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

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

CTM; Reviewed:
SPOC 9/20/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

37 of 56
VCIPO81SBCE62

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 Voice Carrier 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 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with 'Media Rules' highlighted. The main 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 'Media NAT' section with the text 'Learn Media IP dynamically' and an 'Edit' button.

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

The screenshot shows the 'Media Encryption' tab selected. It contains three sections: 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'. Each section has 'Preferred Formats' set to 'RTP' and 'Interworking' checked with a green checkmark. The 'Miscellaneous' section has 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom.

Audio Encryption	
Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

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

Media NAT	Media Encryption	Media Anomaly	Media Silencing	Media QoS
Media Anomaly Detection <input checked="" type="checkbox"/>				
Detect RTP Injection Attack <input checked="" type="checkbox"/>				
Asymmetric RTP <input type="checkbox"/>				
Action		Alert		
Edit				

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

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

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

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 Voice Carrier 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.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left navigation pane lists various configuration areas, with 'Domain Policies' expanded to show 'Signaling Rules'. The main content area is titled 'Signaling Rules: default' 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, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'General' tab is active, displaying settings for 'Inbound' and 'Outbound' traffic. The 'Inbound' section has four rows: 'Requests' (Allow), 'Non-2XX Final Responses' (Allow), 'Optional Request Headers' (Allow), and 'Optional Response Headers' (Allow). The 'Outbound' section has four rows: 'Requests' (Allow), 'Non-2XX Final Responses' (Allow), 'Optional Request Headers' (Allow), and 'Optional Response Headers' (Allow). Below these is the 'Content-Type Policy' section, which includes a checkbox for 'Enable Content-Type Checks' (checked) and a table with two rows: 'Action' (Allow) and 'Multipart Action' (Allow).

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	<input checked="" type="checkbox"/>
Action	Allow
Multipart Action	Allow

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

The screenshot shows the 'Signaling QoS' tab in the configuration interface. It features a checkbox for 'Signaling QoS' (checked), a 'QoS Type' dropdown set to 'DSCP', and a 'DSCP' dropdown set to 'AF41'. An 'Edit' button is located at the bottom.

Signaling QoS	<input checked="" type="checkbox"/>
QoS Type	DSCP
DSCP	AF41

[Edit](#)

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.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with 'Domain Policies' expanded, showing 'End Point Policy Groups' as the selected option. The main content area is titled 'Policy Groups: default-low' and includes an 'Add' button and a 'Filter By Device...' dropdown. A warning message states: 'It is not recommended to edit the defaults. Try adding a new group instead.' Below this is a table of policy groups. The 'default-low' group is selected, and its details are shown in a pop-up window. The details window has a 'Policy Group' tab and a table with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and actions (Edit, Clone). The table contains one row with the following values: Order 1, Application default, Border default, Media default-low-med, Security default-low, Signaling default, Time of Day default.

Order	Application	Border	Media	Security	Signaling	Time of Day	
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 created 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.

The screenshot shows a 'Policy Group' details window. It contains a table with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and actions (Edit, Clone). The table contains one row with the following values: Order 1, Application default-trunk, Border default, Media default-low-med, Security default-low, Signaling default, Time of Day default.

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

6.11.2. Endpoint Policy Group – Voice Carrier

For the compliance test, endpoint policy group **SP-EP-Policy** was created for the Voice Carrier 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 created 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 '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 (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 includes an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, there is a 'Routing Profile' section with an 'Add' button. A table lists the routing profiles:

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

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**.

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 – Voice Carrier

For the compliance test, routing profile **To-Trunks** was created for Voice Carrier. 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 Voice Carrier SIP server.
- Enable **Next Hop Priority**.
- Set the **Outgoing Transport** field to **UDP** or **TCP** as defined by Voice Carrier.

View Routing Rule		X
Priority	1	
URI Group	*	
Next Hop Server 1	192.168.243.180	
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 both Avaya IP Office and the Voice Carrier 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.

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▾ Global Profiles

Domain DoS

Fingerprint

Server Interworking

Phone Interworking

Media Forking

Routing

Server Configuration

Topology Hiding

Signaling Manipulation

URI Groups

Topology Hiding Profiles: default

AddClone

Topology Hiding Profiles

default

cisco_th_profile

Topology Hiding

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

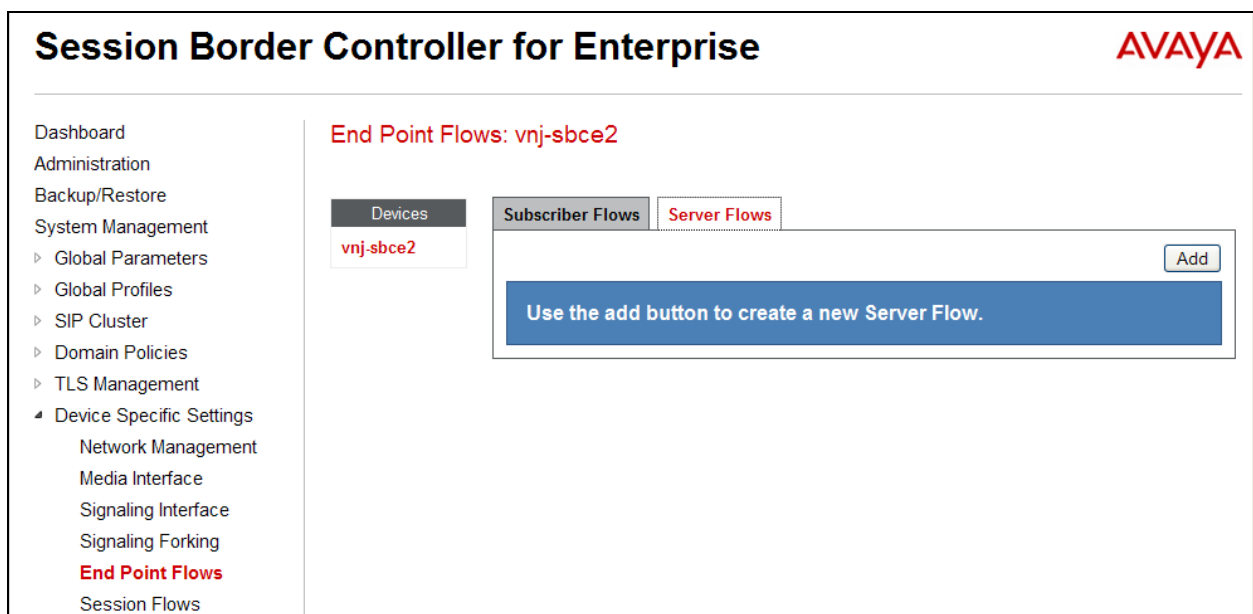
Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

Edit

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.



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 Voice Carrier 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		X	
Criteria		Profile	
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-Trunks
Remote Subnet	*	Topology Hiding Profile	default
Received Interface	Ext_Sig_Intf	File Transfer Profile	None

6.14.2. End Point Flow – Voice Carrier

For the compliance test, endpoint flow **VoiceCarrier** was created for the Voice Carrier SIP server. All traffic from Voice Carrier 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 Voice Carrier 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 Voice Carrier 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 Voice Carrier in **Section 6.13**.

View Flow: VoiceCarrier				X
Criteria		Profile		
Flow Name	VoiceCarrier	Signaling Interface	Ext_Sig_Intf	
Server Configuration	VoiceCarrier	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	default	
Received Interface	Int_Sig_Intf	File Transfer Profile	None	

7. Voice Carrier IntelliSIP Trunking Configuration

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

- Voice Carrier SIP domain
- IP address of the Voice Carrier SIP proxy
- Supported codecs
- DID numbers

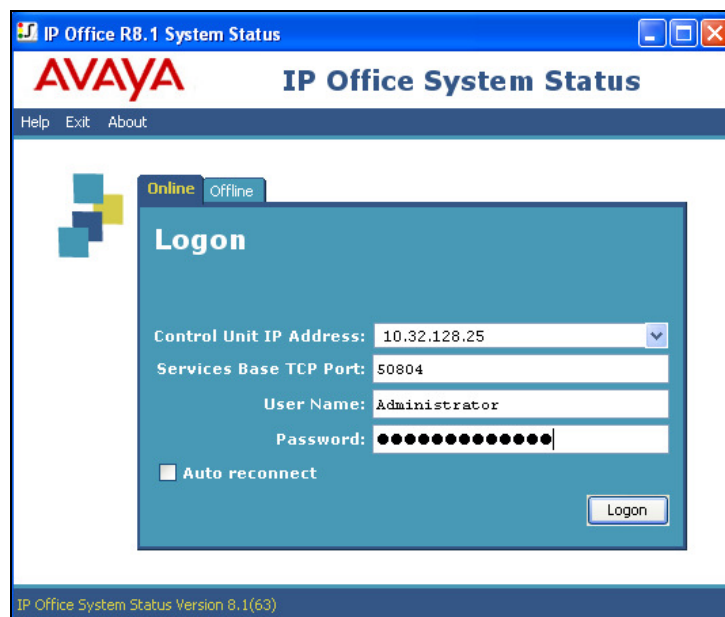
8. Verification Steps

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 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 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** for each channel. If no active call is currently in session (as shown below), the state should be **Idle**. If some channels are taken by active calls, then the **Current State** will be shown as **Connected**.

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System

- Alarms (10)
- Extensions (20)
- Trunks (14)
 - Lines: 1 - 4
 - Lines: 5 - 8
 - Line: 17
 - Line: 18
 - Line: 19
 - Line: 20
 - Line: 21
 - Line: 22
- Active Calls
- Resources
- Voicemail
- IP Networking

Status Utilization Summary Alarms

SIP Trunk Summary

Peer Domain Name: avayatest.callingcloud.net
 Resolved Address: 192.168.243.180
 Line Number: 22
 Number of Administered Channels: 10
 Number of Channels in Use: 0
 Administered Compression: G711 Mu, G711 A, G729 A, G7231
 Silence Suppression: Off
 SIP Trunk Channel Licenses: Unlimited
 SIP Trunk Channel Licenses in Use: 0
 SIP Device Features: REFER (Incoming and Outgoing)

Channel Number	U...	Call Ref	Current State	Time in State	Remote Media A...	Co...	Conne...	Caller ID or ...	Other Party on Call	Directi...	Round Trip D...	Receive Jitter	Receive Packe...	Transmit Jitter	Trans...
1			Idle	21:39...											
2			Idle	21:46...											
3			Idle	1 day ...											
4			Idle	1 day ...											

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

Status Utilization Summary **Alarms**

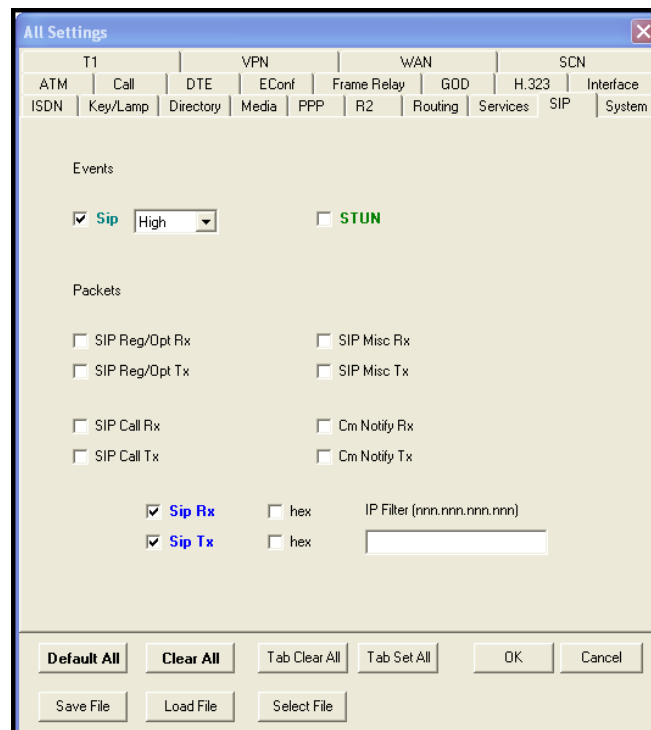
Alarms for Line: 22 SIP avayatest.callingcloud.net

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

8.2. Monitor

The Monitor application can also be used to monitor and troubleshoot 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, the **SIP Rx** and **SIP Tx** boxes are checked.



9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office 8.1 to the Voice Carrier IntelliSIP Trunking Service. The Voice Carrier IntelliSIP 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 Voice Carrier IntelliSIP 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 8.1 IP500/IP500 V2 Installation*, Document Number 15-601042, Issue 27m, July 2, 2013.
- [2] *IP Office Release 8.1 Manager 10.1*, Document Number 15-601011, Issue 29u, April 5, 2013.
- [3] *IP Office System Status Application*, Document Number 15-601758, Issue 07a, November 26, 2012.
- [4] *IP Office Release 8.1 Administering Voicemail Pro*, Document Number 15-601063, Issue 8b, December 11, 2012.
- [5] *IP Office System Monitor*, Document Number 15-601019, Issue 03c, March 1, 2013.

Additional IP Office documentation can be found at:

<http://marketingtools.avaya.com/knowledgebase/>

11. Appendix A: SIP Line Template

Avaya IP Office supports a SIP Line Template (in xml format) that can be created from an existing configuration and imported into a new installation to simplify configuration procedures as well as to reduce potential configuration errors.

Note that not all of the configuration information, particularly items relevant to a specific installation environment, is included in the SIP Line Template. Therefore, it is critical that the SIP Line configuration be verified/updated after a template has been imported and additional configuration be supplemented using **Section 5.4** in these Application Notes as a reference.

The SIP Line Template created from the configuration as documented in these Application Notes is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<Template xmlns="urn:SIPTrunk-schema">
  <TemplateType>SIPTrunk</TemplateType>
  <Version>20130816</Version>
  <SystemLocale>enu</SystemLocale>
  <DescriptiveName>Voice Carrier</DescriptiveName>
  <ITSPDomainName>avayatest.callingcloud.net</ITSPDomainName>
  <SendCallerID>CallerIDDIV</SendCallerID>
  <ReferSupport>true</ReferSupport>
  <ReferSupportIncoming>2</ReferSupportIncoming>
  <ReferSupportOutgoing>2</ReferSupportOutgoing>
  <RegistrationRequired>false</RegistrationRequired>
  <UseTelURI>false</UseTelURI>
  <CheckOOS>true</CheckOOS>
  <CallRoutingMethod>1</CallRoutingMethod>
  <OriginatorNumber />
  <AssociationMethod>SourceIP</AssociationMethod>
  <LineNamePriority>SystemDefault</LineNamePriority>
  <UpdateSupport>UpdateNever</UpdateSupport>
  <UserAgentServerHeader />
  <CallerIDfromFromheader>false</CallerIDfromFromheader>
  <PerformUserLevelPrivacy>false</PerformUserLevelPrivacy>
  <ITSPProxy>10.32.128.20</ITSPProxy>
  <LayerFourProtocol>SipUDP</LayerFourProtocol>
  <SendPort>5060</SendPort>
  <ListenPort>5060</ListenPort>
  <DNSServerOne>0.0.0.0</DNSServerOne>
  <DNSServerTwo>0.0.0.0</DNSServerTwo>
  <CallsRouteViaRegistrar>true</CallsRouteViaRegistrar>
  <SeparateRegistrar />
  <CompressionMode>AUTOSELECT</CompressionMode>
  <UseAdvVoiceCodecPrefs>false</UseAdvVoiceCodecPrefs>
  <CallInitiationTimeout>4</CallInitiationTimeout>
  <DTMFSupport>DTMF_SUPPORT_RFC2833</DTMFSupport>
  <VoipSilenceSupression>false</VoipSilenceSupression>
  <ReinviteSupported>true</ReinviteSupported>
  <FaxTransportSupport>FOIP_G711</FaxTransportSupport>
  <UseOffererPreferredCodec>false</UseOffererPreferredCodec>
```

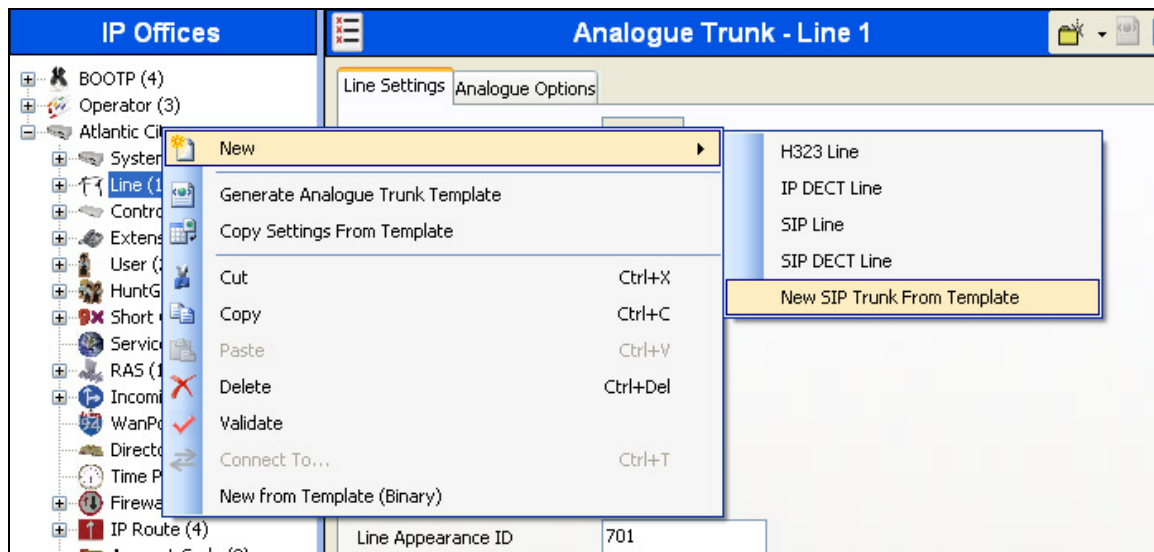
```

<CodecLockdown>false</CodecLockdown>
<Rel100Supported>false</Rel100Supported>
<T38FaxVersion>3</T38FaxVersion>
<Transport>UDPTL</Transport>
<LowSpeed>0</LowSpeed>
<HighSpeed>0</HighSpeed>
<TCFMethod>Trans_TCF</TCFMethod>
<MaxBitRate>FaxRate_14400</MaxBitRate>
<EflagStartTimer>2600</EflagStartTimer>
<EflagStopTimer>2300</EflagStopTimer>
<UseDefaultValues>true</UseDefaultValues>
<ScanLineFixup>true</ScanLineFixup>
<TFOPENenhancement>true</TFOPENenhancement>
<DisableT30ECM>false</DisableT30ECM>
<DisableEflagsForFirstDIS>false</DisableEflagsForFirstDIS>
<DisableT30MRCompression>false</DisableT30MRCompression>
<NSFOVERRIDE>false</NSFOVERRIDE>
</Template>

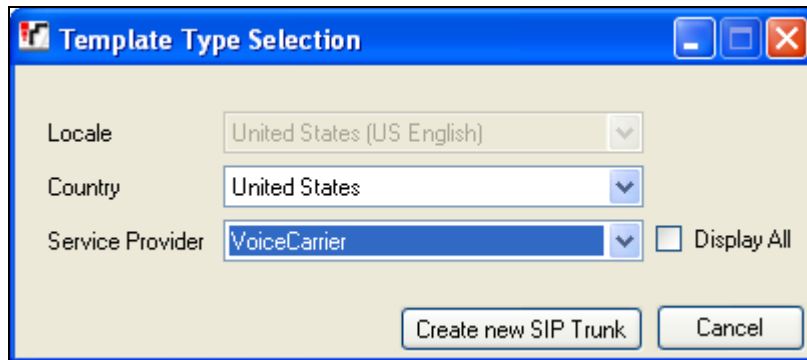
```

To import the above template into a new installation:

1. On the PC where IP Office Manager was installed, copy and paste the above template into a text document named **US_VoiceCarrier_SIPTrunk.xml**. Move the .xml file to the IP Office Manager template directory (C:\Program Files\Avaya\IP Office\Manager\Templates). It may be necessary to create this directory.
2. Import the template into an IP Office installation by creating a new SIP Line as shown in the screenshot below. In the Navigation Pane on the left, right-click on **Line** then navigate to **New → New SIP Trunk From Template**:



3. Verify that **United States** is automatically populated for **Country** and **VoiceCarrier** is automatically populated for **Service Provider** in the resulting Template Type Selection screen as shown below. Click **Create new SIP Trunk** to finish the importing process.



Template Type Selection

Locale: United States (US English)

Country: United States

Service Provider: VoiceCarrier

☐ Display All

Create new SIP Trunk Cancel

©2013 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.