



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring ThinkTel SIP Trunking Service with Avaya IP Office 9.1 and Avaya Session Border Controller for Enterprise 7.0 - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between the ThinkTel SIP Trunking Service and an enterprise solution using Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise 7.0.

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

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

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

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results .....	5
2.3.	Support .....	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated .....	9
5.	Configure Avaya IP Office .....	10
5.1.	Licensing and Physical Hardware .....	11
5.2.	System .....	13
5.2.1.	System - LAN1 Tab .....	13
5.2.2.	System - Voicemail Tab.....	17
5.2.3.	System - Telephony Tab .....	18
5.2.4.	System - Twinning Tab.....	19
5.2.5.	System – Codecs Tab.....	19
5.3.	IP Route.....	20
5.4.	Administer SIP Line.....	21
5.4.1.	Create SIP Line from Template .....	22
5.4.2.	SIP Line – SIP Line Tab .....	25
5.4.3.	SIP Line – Transport Tab.....	26
5.4.4.	SIP Line – SIP Credentials Tab .....	27
5.4.5.	SIP Line – SIP URI Tab.....	28
5.4.6.	SIP Line – VoIP Tab.....	30
5.4.7.	SIP Line – T.38 Fax Tab.....	31
5.4.8.	SIP Line – Advanced Tab .....	32
5.5.	Short Code.....	33
5.6.	User .....	35
5.7.	Incoming Call Route .....	36
5.7.1.	Incoming Call Route – Standard Tab.....	36
5.7.2.	Incoming Call Route – Destination Tab .....	36
5.8.	Alternate Route Selection (ARS).....	38
5.9.	Save Configuration.....	39
6.	Configure Avaya Session Border Controller for Enterprise .....	40
6.1.	Access the Management Interface.....	40
6.2.	Verify Network Configuration and Enable Interfaces .....	42
6.3.	Signaling Interface .....	44
6.4.	Media Interface .....	45
6.5.	Server Interworking.....	46
6.5.1.	Server Interworking – Avaya IP Office .....	47
6.5.2.	Server Interworking – ThinkTel .....	49
6.6.	Server Configuration.....	51
6.6.1.	Server Configuration – Avaya IP Office .....	52

6.6.2.	Server Configuration – ThinkTel.....	53
6.7.	Application Rules.....	54
6.8.	Media Rules.....	55
6.9.	Signaling Rules .....	58
6.9.1.	Signaling Rules – Avaya IP Office.....	59
6.9.2.	Signaling Rules – ThinkTel .....	60
6.10.	End Point Policy Groups .....	62
6.10.1.	End Point Policy Group – Avaya IP Office .....	62
6.10.2.	End Point Policy Group – ThinkTel.....	63
6.11.	Routing .....	63
6.11.1.	Routing – Avaya IP Office.....	64
6.11.2.	Routing – ThinkTel .....	65
6.12.	Topology Hiding.....	66
6.13.	End Point Flows.....	67
6.13.1.	End Point Flow – Avaya IP Office.....	68
6.13.2.	End Point Flow – ThinkTel.....	69
7.	ThinkTel SIP Trunking Configuration .....	70
8.	Verification Steps .....	71
8.1.	Avaya IP Office System Status .....	71
8.2.	Avaya IP Office Monitor.....	73
8.3.	Avaya Session Border Controller for Enterprise Protocol Trace.....	74
9.	Conclusion .....	74
10.	Additional References.....	75

# 1. Introduction

These Application Notes describe the procedures for configuring an enterprise solution using Avaya IP Office Release 9.1 and Avaya Session Border Controller for Enterprise 7.0 to interoperate with the ThinkTel SIP Trunking Service.

The ThinkTel SIP Trunking Service referenced within these Application Notes is positioned for customers who have an IP-PBX or IP-based network equipment with SIP functionality, but need a network service to access the PSTN from the enterprise using IP transport to complete their solution.

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

For brevity, the remainder of this document sometimes uses ThinkTel to refer to the ThinkTel SIP Trunking Service.

## 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the ThinkTel SIP Trunking Service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site comprised of Avaya IP Office 500 V2 running Release 9.1 software, Avaya Voicemail Pro messaging application, Avaya H.323 and SIP hard phones, and SIP-based Avaya softphones. The enterprise solution connects to the ThinkTel network via the Avaya Session Border Controller for Enterprise (Avaya SBCE).

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:

- Establishment of the SIP Trunk
- SIP OPTIONS queries and responses
- Incoming PSTN calls (via the ThinkTel SIP trunk) to SIP and H.323 telephones at the enterprise
- Outgoing PSTN calls (via the ThinkTel SIP trunk) to SIP and H.323 telephones at the enterprise
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows
- Various call types including: local, long distance, outbound toll-free, international (011 + country code + number) and local directory assistance (411)

- G.711u and G.729a codecs
- Caller ID presentation and Caller ID restriction
- DTMF transmission using RFC 2833
- Voicemail access and navigation for inbound and outbound calls
- Voicemail message waiting indicator (MWI)
- Telephony supplementary features such as hold and resume, call forward, transfer, and conference
- Twinning on inbound calls to PSTN mobile phones
- Use of the SIP REFER method for call redirection to the PSTN
- Inbound and outbound long-duration call stability
- Inbound and outbound long hold time call stability
- Response to incomplete call attempts and trunk busy or error conditions
- T.38 fax
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones

Items not supported or not tested include the following:

- Inbound toll-free and emergency calls (911) were not tested as part of the compliance test.
- ThinkTel does not support Operator (0) and Operator-Assisted (0 + 10-digits) calls.
- ThinkTel does not support SIP session timer refresh. In the compliance test, session refresh for active calls was initiated from the Avaya IP Office.

## 2.2. Test Results

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

- **OPTIONS Response** – On the test circuit used for the compliance test, ThinkTel responded to OPTIONS from Avaya IP Office with "401 Unauthorized". For ThinkTel to respond to OPTIONS with "200 OK", it requires that the OPTIONS message contain an Authorization header, but Avaya IP Office cannot be configured to satisfy this requirement. However, Avaya IP Office treats any response to OPTIONS as an indication that the far end is active and responding, therefore will not take the SIP connection to the far end out of service. This OPTIONS response is listed here simply as an observation since it had no impact on the status of the SIP connection between Avaya IP Office and ThinkTel.
- **Codec Lockdown** – When the SDP of an outbound call INVITE contained the codec list of G.729a and G.711u in that preference order, ThinkTel's call connect "200 OK" contained the same codecs in the same order in the SDP instead of the single preferred codec (G.729a). However, when the SDP of an outbound INVITE contained the codec list in the order of G.711u and G.729a, ThinkTel's call connect "200 OK" contained the single preferred codec (G.711u). This difference in codec lockdown behavior is listed here simply as an observation since there was no user impact.
- **Unsupported Codec** – When an outbound call was configured to use a codec unsupported by ThinkTel, ThinkTel would return a "183 Session In Progress" message whose SDP

contained G.711u. Avaya IP Office would then terminate the call by issuing the CANCEL message. While this behavior was acceptable, it would be more desirable for ThinkTel to return an explicit status message, like "488 Not Acceptable Here" or "415 Media Type Missing" in response to the outbound INVITE.

- **Use of REFER and Call Disconnect (BYE)** – When the SIP REFER method was used for off-net call re-direction (e.g., call forward and call transfer), after accepting the REFER from the enterprise and issuing a BYE, ThinkTel would incorrectly send an INVITE towards the Avaya IP Office caller. This INVITE would elicit an Avaya IP Office response of “481 Dialog/Transaction Does Not Exist” since the call had already been terminated by the previous BYE. In addition, this 481 response was not passed by the Avaya SBCE to ThinkTel, causing ThinkTel to retransmit the INVITE until a timeout was reached. Fortunately, this untidy signaling exchange had no impact on the success of the redirected call.
- **Use of REFER and Authentication** – During off-net call redirection, if the REFER message sent from the enterprise is challenged by ThinkTel, then the enterprise will resend the REFER with credentials but with a new Call-ID instead of the existing Call-ID. This results in an error response from ThinkTel. The result is the redirected call is successful; however, the media will remain anchored at the enterprise. This is an Avaya SBCE issue and is under investigation.

## 2.3. Support

For technical support on ThinkTel SIP Trunking Service, contact ThinkTel at:

- Phone: 1 (866) 928-4465
- Email: [support@thinktel.ca](mailto:support@thinktel.ca)
- Website: <http://support.thinktel.ca/>

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

### 3. Reference Configuration

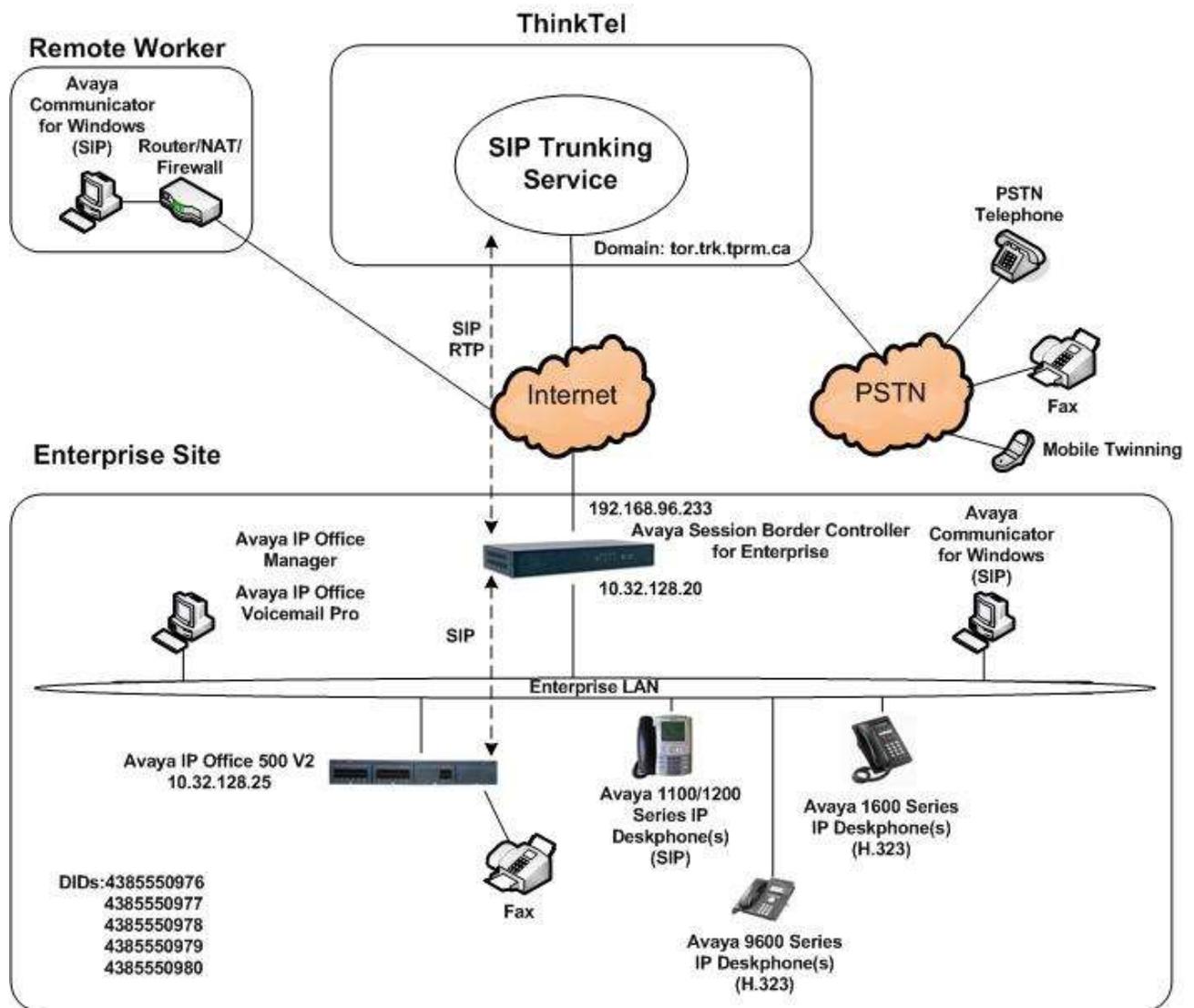
**Figure 1** illustrates the sample configuration used for the DevConnect compliance testing. The sample configuration shows an enterprise site connected to the ThinkTel SIP Trunking Service.

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 endpoints include both local extensions and Remote Worker phones that are connected directly to the public Internet. The same Avaya SBCE was configured to connect to both the service provider network and Remote Worker using separate sets of public/private interfaces (**Figure 1** only shows the public/private interfaces used for connecting to the service provider network).

The Avaya IP Office 500 V2 at the enterprise site runs Avaya IP Office Release 9.1 software. Endpoints include various Avaya IP Telephones (with H.323 and SIP firmware) and a SIP-based Avaya softphone (Avaya Communicator for Windows). The site also has a Windows PC running Avaya Voicemail Pro for providing voice messaging to the Avaya IP Office users, and Avaya IP Office Manager for administering the Avaya IP Office.

Mobility Twinning is configured for some of the Avaya IP Office users so that calls to these user phones will also ring and can be answered at the configured mobile phones.



**Figure 1: Test Configuration**

For security purposes, any actual public IP addresses used in the compliance test were changed to 192.168.x.x throughout these Application Notes.

For the purposes of the compliance test, users dialed a prefix digit 9 plus N digits to send an outbound call to the number N across the SIP trunk to ThinkTel. The short code of 9 was stripped off by Avaya IP Office but the remaining N digits were sent to the service provider network. For calls within the North American Numbering Plan (NANP), the user dialed 11 (1 + 10) digits for long distance and local calls. Thus, for these NANP calls, Avaya IP Office sent 11 digits in the Request URI and the To header of an outbound SIP INVITE message. ThinkTel sent 10 digits in the Request URI and the To header of inbound SIP INVITE messages.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the enterprise network such as a data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application

Notes. However, it should be noted that SIP and RTP traffic between the service provider and Avaya IP Office must be allowed to pass through these devices.

The administration of the Avaya Voicemail Pro messaging service and endpoints on Avaya IP Office are standard. Since these configuration tasks are not directly related to the inter-operation with the ThinkTel SIP Trunking Service, they are not included in these Application Notes.

## 4. Equipment and Software Validated

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

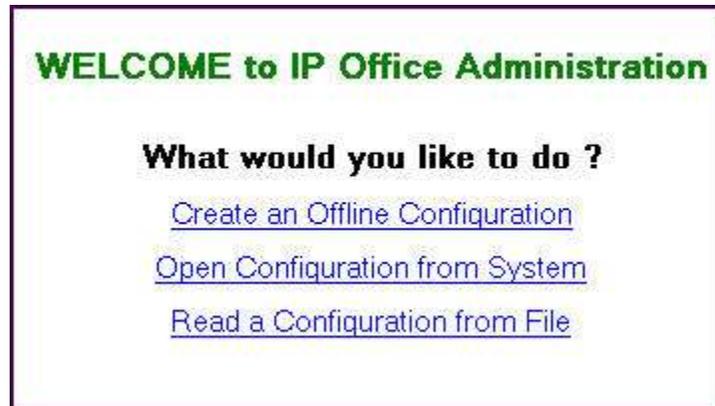
<b>Avaya Telephony Components</b>	
<b>Equipment / Software</b>	<b>Release / Version</b>
Avaya IP Office 500 V2	9.1.5 Build 145
Avaya IP Office COMBO6210/ATM4 Module	9.1.5 Build 145
Avaya IP Office Manager	9.1.5 Build 145
Avaya Preferred Edition (a.k.a Voicemail Pro)	9.1.5.02
Avaya Session Border Controller for Enterprise running on Portwell CAD-0208 server	7.0.0-21-6602
Avaya 1140E IP Telephone (SIP)	4.4 SP2 (4.04.18)
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP5 (1.3.50B)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.6.0 (6.6.0.29)
Avaya Communicator for Windows	2.0.3.30
<b>ThinkTel Components</b>	
<b>Equipment / Software</b>	<b>Release / Version</b>
Metaswitch	8.1
Opensips Session Border Controller	1.11.6 (LTS)

This compliance testing is applicable when the tested solution is deployed with a standalone Avaya IP Office 500 V2 and also when deployed with all configurations of Avaya IP Office Server Edition without T.38 Fax Service.

Avaya IP Office Server Edition requires an Expansion Avaya IP Office 500 V2 to support analog/digital endpoints or trunks.

## 5. Configure Avaya IP Office

Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running Avaya IP Office Manager, 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 menu of the Avaya IP Office Manager window. Select the proper Avaya IP Office system from the pop-up window (not shown) and log in with the appropriate credentials.

The appearance of the Avaya 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 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 Avaya Communicator for Windows 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. The configuration screens only highlight values/settings configured for the compliance test. Defaults were used for other values and may be customized based upon requirements in the field.

## 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 shows the 'IP Offices' configuration window with the 'License' tab selected. The 'Remote Server' sub-tab is active, displaying the following license information:

- License Mode: License Normal
- Licensed Version: 9.1
- Serial Number (ADI): [REDACTED]
- PLDS Host ID: [REDACTED]
- PLDS File Status: Not Present / Invalid

Below this information is a table listing features and their license status:

Feature	License Key	Instances	Status
IP500 Voice Networking Channels	[REDACTED]	4	Valid
VCM Channel Migration	[REDACTED]	255	Valid
<b>SIP Trunk Channels</b>	[REDACTED]	255	Valid
VPN IP Extensions	[REDACTED]	255	Obsolete
IP500 Universal PRI (Additional cha...	[REDACTED]	255	Valid
RAS LRQ Support (Rapid Response)	[REDACTED]	255	Valid

Buttons for 'Add...' and 'Remove' are visible on the right side of the table.

To view the physical hardware comprising the Avaya IP Office system, 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 station 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 screen below 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 configuration details for the selected 'IP 500 V2' unit.

IP Offices		IP 500 V2	
<ul style="list-style-type: none"> <li>BOOTP (2)</li> <li>Operator (3)</li> <li>Atlantic City <ul style="list-style-type: none"> <li>System (1)</li> <li>Line (25) <ul style="list-style-type: none"> <li>Control Unit (3) <ul style="list-style-type: none"> <li>1 IP 500 V2</li> <li>2 COMBO6210/ATM4</li> <li>3 DIGSTA8/ATM4</li> </ul> </li> </ul> </li> <li>Extension (25)</li> <li>User (27)</li> <li>Group (1)</li> <li>Short Code (64)</li> <li>Service (0)</li> <li>RAS (1)</li> <li>Incoming Call Route (73)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Unit</li> <li>Device Number: 1</li> <li>Unit Type: IP 500 V2</li> <li>Version: 9.1.500.145</li> <li>Serial Number: [Redacted]</li> <li>Unit IP Address: 10.32.128.25</li> <li>Interconnect Number: 0</li> <li>Module Number: Control Unit</li> </ul>		

The screen below shows the details of the Combination Card:

The screenshot displays the Avaya IP Office configuration interface. On the left is the 'IP Offices' navigation pane, and on the right is the configuration details for the selected 'COMBO6210/ATM4' unit.

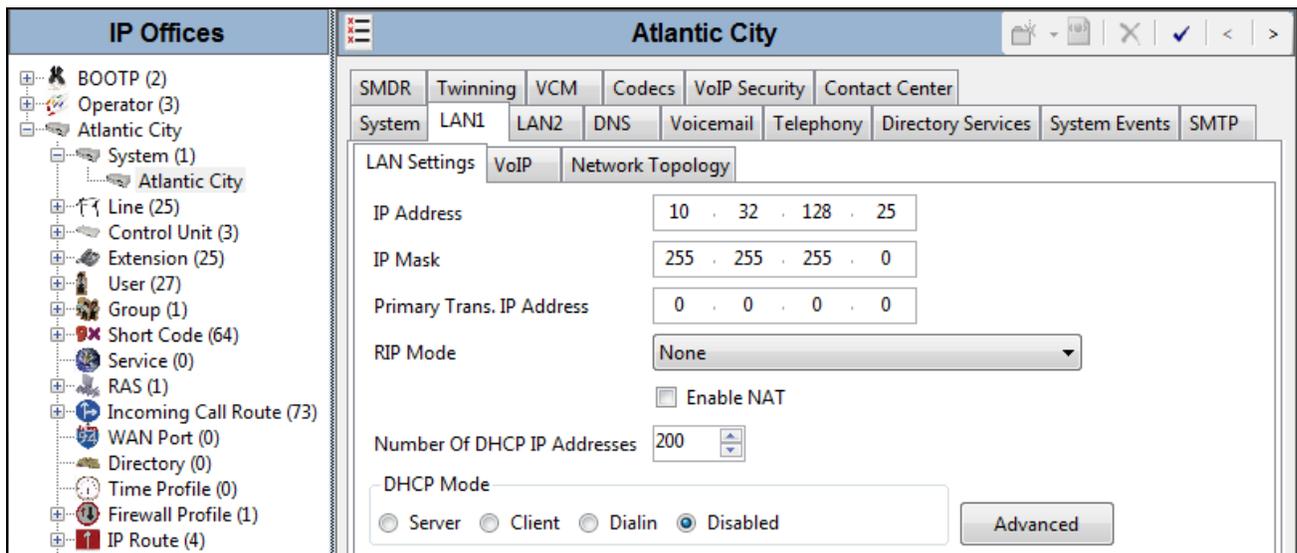
IP Offices		COMBO6210/ATM4	
<ul style="list-style-type: none"> <li>BOOTP (2)</li> <li>Operator (3)</li> <li>Atlantic City <ul style="list-style-type: none"> <li>System (1)</li> <li>Line (25) <ul style="list-style-type: none"> <li>Control Unit (3) <ul style="list-style-type: none"> <li>1 IP 500 V2</li> <li>2 COMBO6210/ATM4</li> <li>3 DIGSTA8/ATM4</li> </ul> </li> </ul> </li> <li>Extension (25)</li> <li>User (27)</li> <li>Group (1)</li> <li>Short Code (64)</li> <li>Service (0)</li> <li>RAS (1)</li> <li>Incoming Call Route (73)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Unit</li> <li>Device Number: 2</li> <li>Unit Type: COMBO6210/ATM4</li> <li>Version: 9.1.500.145</li> <li>Serial Number: [Redacted]</li> <li>Unit IP Address: 0.0.0.0</li> <li>Interconnect Number: 0</li> <li>Module Number: Control Unit</li> </ul>		

## 5.2. System

This section configures 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.



The screenshot displays the Avaya IP Office configuration interface for the system named "Atlantic City". The left-hand pane shows a tree view of system components, including BOOTP (2), Operator (3), Atlantic City, System (1), Atlantic City, Line (25), Control Unit (3), Extension (25), User (27), Group (1), Short Code (64), Service (0), RAS (1), Incoming Call Route (73), WAN Port (0), Directory (0), Time Profile (0), Firewall Profile (1), and IP Route (4). The main pane is titled "Atlantic City" and contains several tabs: SMDR, Twinning, VCM, Codecs, VoIP Security, Contact Center, System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, and SMTP. The "LAN1" tab is active, and the "LAN Settings" sub-tab is selected. The configuration fields are as follows:

Field	Value
IP Address	10 . 32 . 128 . 25
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
Enable NAT	<input type="checkbox"/>
Number Of DHCP IP Addresses	200
DHCP Mode	Server <input type="radio"/> Client <input type="radio"/> Dialin <input type="radio"/> Disabled <input checked="" type="radio"/>

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

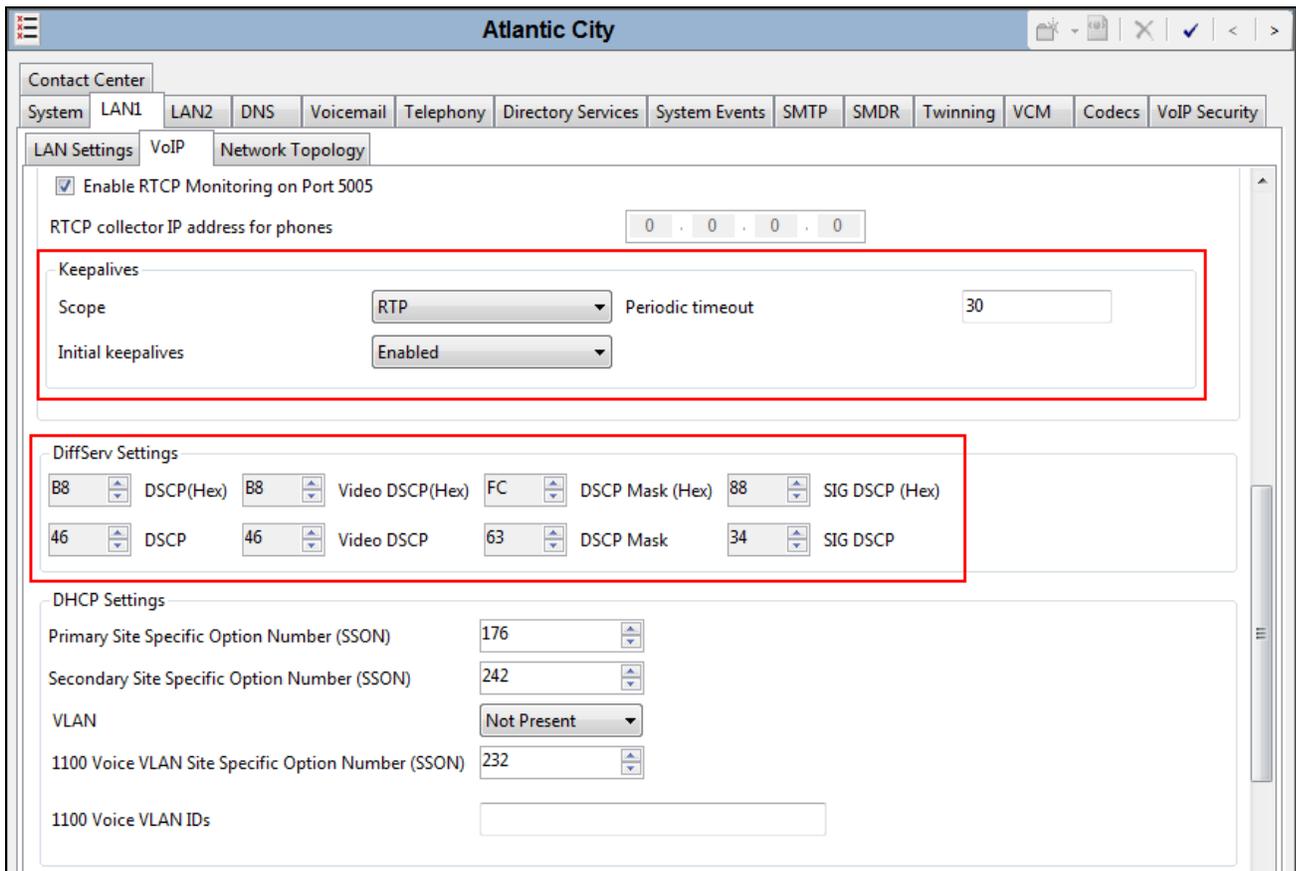
On the **VoIP** tab of LAN1 in the Details Pane, configure the following parameters:

- 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 ports that Avaya IP Office will use for RTP media. This port range will be used to select a destination port for incoming RTP and a source port for outgoing RTP for calls using LAN1. The default values were used.

The screenshot displays the configuration interface for Atlantic City, specifically the VoIP tab for LAN1. The interface includes a navigation bar with tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, Codecs, and VoIP Security. The VoIP tab is active, and the configuration is divided into sections: LAN Settings, VoIP, and Network Topology. The VoIP section contains several checkboxes and input fields. The 'SIP Trunks Enable' checkbox is highlighted with a red box. Below it, the 'SIP Registrar Enable' checkbox is checked, and the 'SIP Remote Extn Enable' checkbox is also checked. The 'Domain Name' field is empty. The 'Layer 4 Protocol' section has checkboxes for UDP, TCP, and TLS, with their respective ports (5060, 5060, 5061) and remote ports (5060, 5060, 5061) displayed. The 'Challenge Expiry Time (secs)' is set to 10. The 'RTP' section is highlighted with a red box, showing a 'Port Number Range' with a minimum of 49152 and a maximum of 53246. Below this, the 'Port Number Range (NAT)' section also shows a minimum of 49152 and a maximum of 53246.

Scroll down the page.

- In the **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.
- In the **DiffServ Settings** 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 were the Avaya IP Office default values and are shown in the screenshot below. Quality of Service (QoS) is not specifically tested as part of the compliance test. These DSCP values defined for LAN1 are used within the enterprise and not sent to the service provider.
- All other parameters should be set according to customer requirements.



On the **Network Topology** tab of LAN1 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*. With the *Open Internet* setting, the **STUN Server Address** is not used.
- Set **Binding Refresh Time (seconds)** to the desired value. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. The compliance test used a value of **300** seconds.
- Set **Public Port** to **5060** for **UDP**.

The screenshot shows 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): 300
- Public IP Address: 0 . 0 . 0 . 0
- Public Port: UDP (5060), TCP (0), TLS (0)
- Run STUN on startup:

Buttons: Run STUN, Cancel

## 5.2.2. System - Voicemail Tab

In the **Voicemail** tab of the Details Pane, configure the **SIP Settings** section. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise from ThinkTel. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. Uncheck the **Anonymous** box to allow the Voicemail Caller ID information to be sent to the network.

Note the selection in **Voicemail Type** and the IP address setting for **Voicemail IP Address**. These are for configuring Voicemail Pro as the voice messaging service for Avaya IP Office (part of the standard Avaya IP Office setup beyond the scope of these Application Notes).

The screenshot shows the configuration interface for the Voicemail tab in the Atlantic City system. The 'SIP Settings' section is highlighted with a red box. The configuration includes:

- Voicemail Type:** Voicemail Lite/Pro
- Voicemail Destination:** (empty)
- Voicemail IP Address:** 10 . 32 . 128 . 79
- Backup Voicemail IP Address:** 0 . 0 . 0 . 0
- Voicemail Channel Reservation:**
  - Unreserved Channels: 259
  - Auto-Attendant: 0
  - Voice Recording: 0
  - Mandatory Voice Recording: 0
  - Announcements: 0
  - Mailbox Access: 0
- DTMF Breakout:**
  - Reception / Breakout (DTMF 0): (empty)
  - Breakout (DTMF 2): (empty)
  - Breakout (DTMF 3): (empty)
- Voicemail Code Complexity:**
  - Enforcement:
  - Minimum length: 3
  - Complexity:
- SIP Settings (highlighted):**
  - SIP Name: 4385550980
  - SIP Display Name (Alias): Voicemail
  - Contact: 4385550980
  - Anonymous:
- Call Recording:** (empty)

### 5.2.3. System - Telephony Tab

Navigate to the **Telephony** → **Telephony** tab in the Details Pane. Enter or select **0** for **Hold Timeout (secs)** so that calls on hold will not time out. Choose the **Companding Law** typical for the enterprise site. For the compliance test, **U-Law** was used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the service provider across the SIP trunk per customer business policies. Note that this configuration might pose a security issue (Toll Fraud). Customers should exercise caution with this configuration.

The screenshot shows the configuration page for 'Atlantic City' under the 'Telephony' tab. The 'Hold Timeout (secs)' field is set to 0. The 'Companding Law' section is configured with 'U-Law' for the Switch and 'U-Law Line' for the Line. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked.

Field	Value
Default Outside Call Sequence	Normal
Default Inside Call Sequence	Ring Type 1
Default Ring Back Sequence	Ring Type 2
Restrict Analogue Extension Ringer Voltage	<input type="checkbox"/>
Dial Delay Time (secs)	4
Dial Delay Count	0
Default No Answer Time (secs)	25
Hold Timeout (secs)	0
Park Timeout (secs)	300
Ring Delay (secs)	5
Call Priority Promotion Time (secs)	Disabled
Default Currency	USD
Default Name Priority	Favor Trunk
Media Connection Preservation	Disabled
Phone Failback	Manual
Login Code Complexity	<input type="checkbox"/> Enforcement Minimum length: 4 <input type="checkbox"/> Complexity

**Companding Law**

Switch	Line
<input checked="" type="radio"/> U-Law	<input checked="" type="radio"/> U-Law Line
<input type="radio"/> A-Law	<input type="radio"/> A-Law Line

DSS Status

Auto Hold

Dial By Name

Show Account Code

Inhibit Off-Switch Forward/Transfer

Restrict Network Interconnect

Include location specific information

Drop External Only Impromptu Conference

Visually Differentiate External Call

Unsupervised Analog Trunk Disconnect Handling

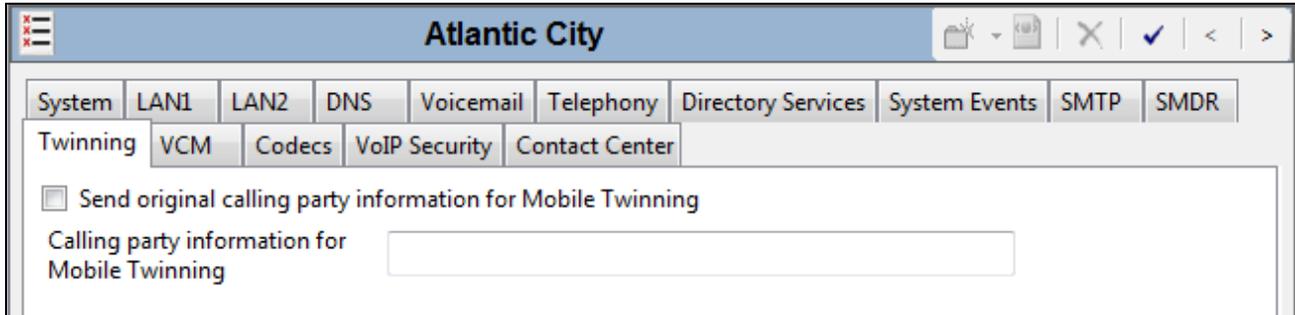
High Quality Conferencing

Digital/Analogue Auto Create User

Directory Overrides Barring

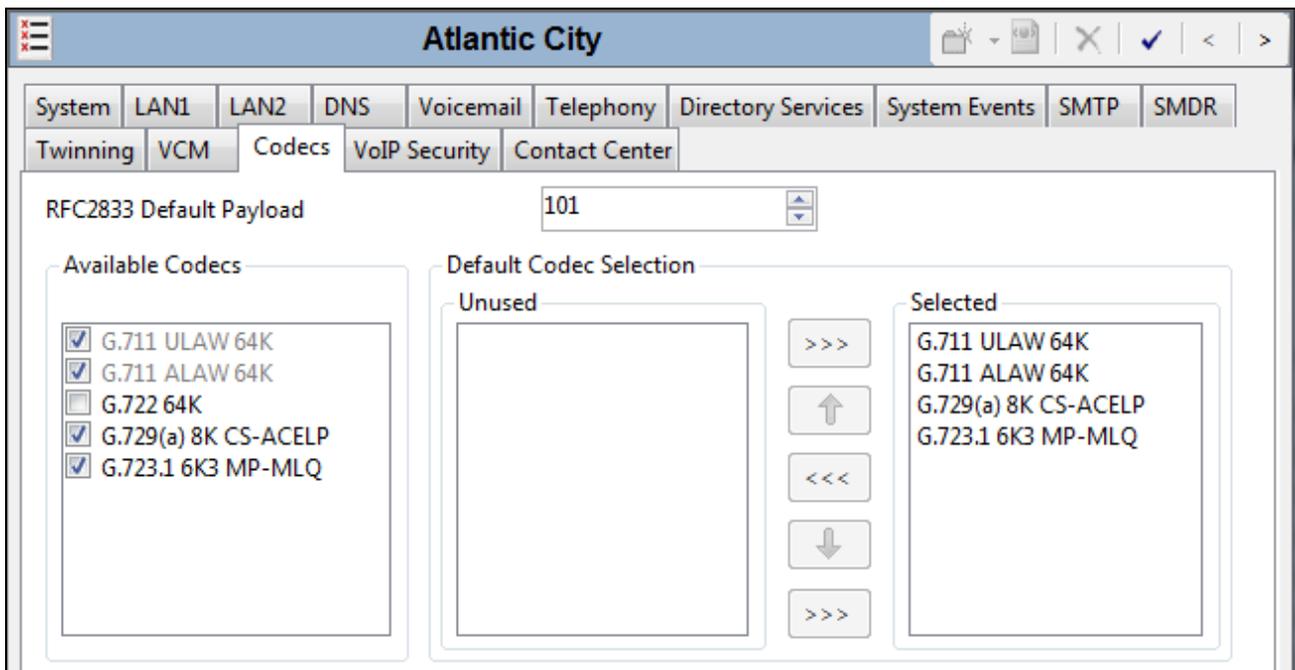
## 5.2.4. System - Twinning Tab

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 Twining** box is not checked in the sample configuration, and the **Calling party information for Mobile Twining** is left blank.



## 5.2.5. System – Codecs Tab

In the **Codecs** tab of the Details Pane, select or enter **101** for **RFC2833 Default Payload**. This setting matched the ThinkTel configuration for use with out-of-band DTMF tone transmissions.



### 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 enterprise LAN gateway for the subnet where the Avaya IP Office is connected.
- Set **Destination** to **LAN1** from the drop-down list.

The screenshot displays the Avaya IP Office configuration interface. On the left is a navigation tree under 'IP Offices' with various categories and counts. The main area shows the configuration for an IP Route with the address 0.0.0.0. The fields are as follows:

Field	Value
IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	10 . 32 . 128 . 254
Destination	LAN1
Metric	0
Proxy ARP	<input type="checkbox"/>

## 5.4. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the ThinkTel 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 settings can be verified against the manual configuration shown in **Sections 5.4.2 – 5.4.8**.

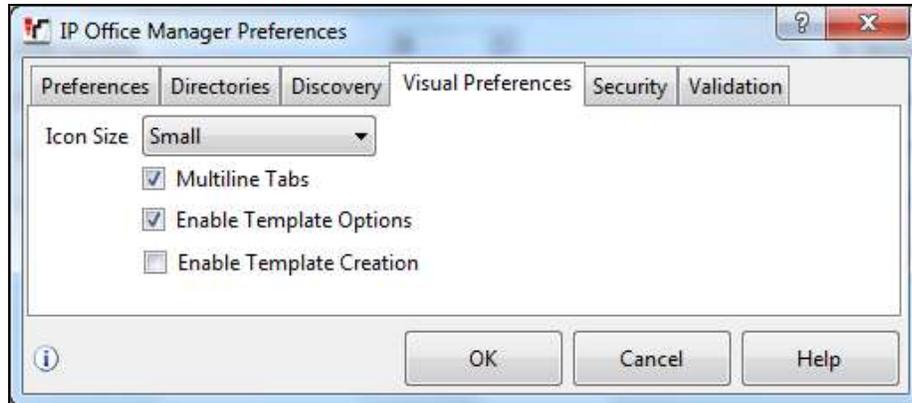
Also, the following SIP Line settings are not supported on Basic Edition:

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

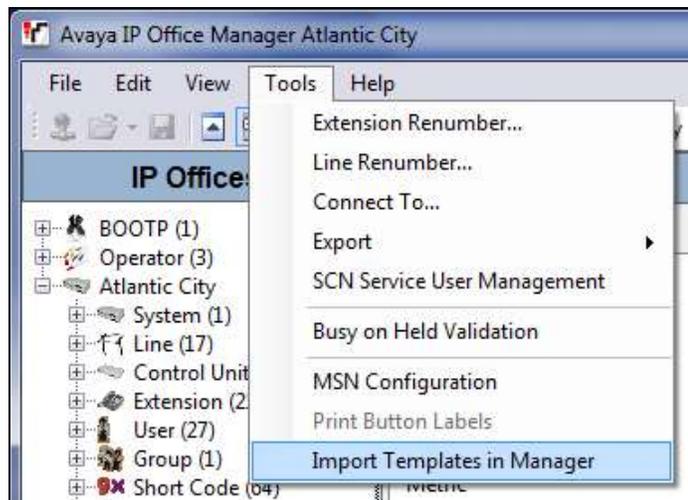
To create a SIP Line manually, right-click **Line** in the Navigation Pane and select **New → SIP Line**; then, follow the steps outlined in **Sections 5.4.2 – 5.4.8**.

### 5.4.1. Create SIP Line from Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **AF\_ThinkTel\_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 option box is checked next to **Enable Template Options**. Click **OK**.



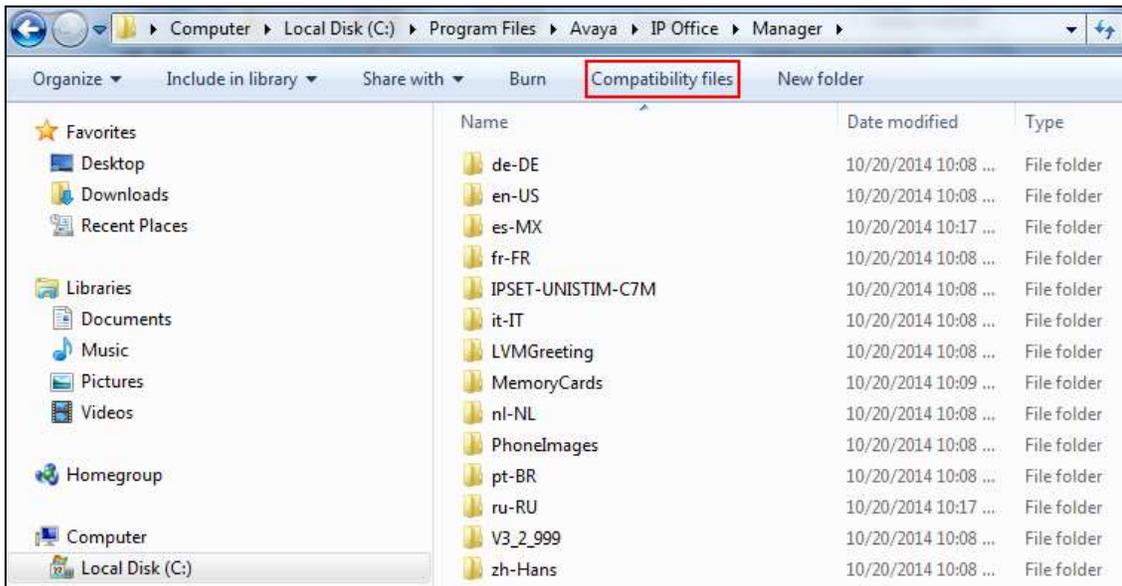
3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template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



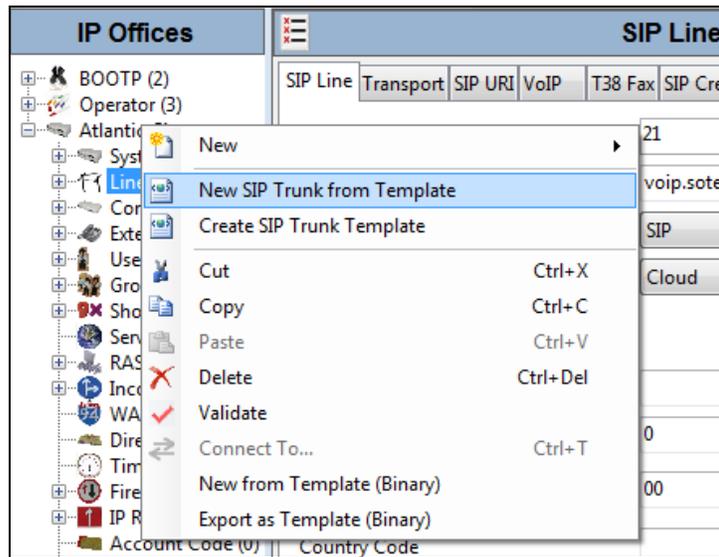
In the pop-up window (not shown) that appears, select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** to continue.

If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

**Note** –Windows 7 (and later) locks the Avaya IP Office 9.1 **\Templates** directory, and it cannot be viewed. To enable browsing of the **\Templates** directory, open Windows Explorer, navigate to **C:\Program Files\Avaya\IP Office\Manager** (or *C:\Program Files (x86)\Avaya\IP Office\Manager*), and then click on the **Compatibility files** option shown below. The **\Templates** directory and its contents can then be viewed.



- 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**.



- In the subsequent **Template Type Selection** pop-up window, select **ThinkTel** from the **Service Provider** drop-down list as shown below. This value corresponds to part of the file name (**AF\_ThinkTel\_SIPTrunk.xml**) created in **Step 1**. Click **Create new SIP Trunk** to finish creating the trunk.



- Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2 – 5.4.8**.

## 5.4.2. SIP Line – SIP Line Tab

In the **SIP Line** tab of the Details Pane, configure the parameters as shown below:

- Leave the **ITSP Domain Name** blank. The **ITSP Proxy Address** on the Transport tab (**Section 5.4.3**) will be used as the domain.
- 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**.
- Set **Refresh Method** to **Auto**. With this setting, Avaya IP Office will send UPDATE messages for session refresh if the remote party supports UPDATE. If UPDATE is not supported, re-INVITE messages are sent.
- Set **Timer (seconds)** to a desired value. With the value as shown below, Avaya IP Office will send session refresh UPDATE or re-INVITE to the service provider every 5 minutes (half of the specified value).
- Set **Send Caller ID** to **Diversion Header**. With this setting and the related configuration in **Section 5.2.4**, Avaya IP Office will include the Diversion Header for calls that are redirected via Mobile Twinning out the SIP Line to the PSTN. It will also include the Diversion Header for calls that are forwarded out the SIP Line.
- ThinkTel supports using either REFER or re-INVITE for off-net call re-direction as in call transfer. If REFER is used, the media path will be released from the enterprise after the call is redirected. To use REFER, under **Redirect and Transfer**, set the **Incoming Supervised REFER** field and **Outgoing Supervised REFER** field to **Always**. To use reINVITE, set these fields to **Never**.

Field	Value	Field	Value
Line Number	33	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name		Check OOS	<input checked="" type="checkbox"/>
URI Type	SIP	Session Timers	
Location	Cloud	Refresh Method	Auto
Prefix		Timer (seconds)	600
National Prefix	0	Forwarding and Twinning	
International Prefix	00	Originator number	
Country Code		Send Caller ID	Diversion Header
Name Priority	System Default	Redirect and Transfer	
Description		Incoming Supervised REFER	Always
		Outgoing Supervised REFER	Always
		Send 302 Moved Temporarily	<input type="checkbox"/>
		Outgoing Blind REFER	<input type="checkbox"/>

### 5.4.3. SIP Line – Transport Tab

Navigate to the **Transport** tab and set the following:

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

The screenshot shows the configuration window for 'SIP Line - Line 33'. 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 empty.

#### 5.4.4. SIP Line – SIP Credentials Tab

SIP Credentials are used to register or authenticate the SIP Trunk with a service provider if required. SIP Credentials are unique per customer and therefore customers must contact the service provider to obtain the proper registration credentials for their deployment.

To enter the SIP Credentials, select the **SIP Credentials** tab and click **Add**. In the **New SIP Credentials** area that appears, enter the information as shown below.

- Set **User name**, **Authentication Name** and **Contact** to the string provided by ThinkTel. This is generally a 10-digit telephone number as shown below.
- In the **Password** and **Confirm Password** field, enter the password provided by ThinkTel.
- In the **Expiry (mins)** field, enter the time in minutes recommended by ThinkTel.
- Uncheck the **Registration required** box. ThinkTel did not require trunk registration.

Click **OK**.

The screenshot shows a software window titled "SIP Line - Line 33". At the top, there are several tabs: "SIP Line", "Transport", "SIP URI", "VoIP", "T38 Fax", "SIP Credentials" (which is selected), "SIP Advanced", and "Engineering". Below the tabs is a table with the following columns: "Index", "UserName", "Authentication Name", "Contact", "Expiry (mins)", and "Register". The table is currently empty. To the right of the table are three buttons: "Add...", "Remove", and "Edit...". Below the table is a section titled "New SIP Credentials" containing several input fields: "User name" (text box with "4385550976"), "Authentication Name" (text box with "4385550976"), "Contact" (text box with "4385550976"), "Password" (password box with 10 dots), "Confirm Password" (password box with 10 dots), "Expiry (mins)" (spin box with "60"), and "Registration required" (checkbox, which is unchecked). To the right of these fields are two buttons: "OK" and "Cancel".

### 5.4.5. SIP Line – SIP URI Tab

Select the **SIP URI** tab to create a SIP URI entry or edit an existing entry. A SIP URI entry matches each incoming number that Avaya IP Office will accept on this line. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane. For the compliance test, a single SIP URI entry was created to match any DID number assigned to Avaya IP Office users.

- Set **Local URI** to *Use Internal Data*. This setting allows calls on this line whose incoming Request-URI matches the **SIP Name** set on the **SIP** tab of any **User** as shown in **Section 5.6**. For outbound calls, the From header is populated with the **SIP Name** configured for the **User** placing the call.
- Set **Contact** and **Display Name** to *Use Internal Data*. This setting will cause the Contact and Display Name data for outbound messages to be set from the corresponding fields on the **SIP** tab of the individual **User** as shown in **Section 5.66**.
- Set **PAI** to *Use Internal Data*. This setting directs Avaya IP Office to send the PAI header (P-Asserted-Identity) when appropriate. The PAI header will be populated from the data set in the **SIP** tab of the call initiating **User** as shown in **Section 5.66**.
- Set the **Registration** value to the credentials that was configured in **Section 5.4.4**.
- Associate this line with an incoming line group by entering line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. For the compliance test, the incoming and outgoing group **33** was specified. Note that this group number can be different than the SIP Line number.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls allowed using this SIP URI pattern.

Click **OK**.

The screenshot shows the 'SIP Line - Line 33' configuration window. The 'SIP URI' tab is selected, displaying a table with columns: Channel, Groups, Via, Local URI, Contact, Display Name, PAI, Credential, and Max Calls. Below the table is a 'New Channel' form with 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 Internal Data
Registration	1: 4385550976
Incoming Group	33
Outgoing Group	33
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**, **Display Name** and **PAI** fields.

## 5.4.6. SIP Line – VoIP Tab

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

- Set the **Codec Selection** to *System Default*. The default codec set includes codecs **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** which were used in the compliance test. G.711u was configured as the preferred codec. If a different codec set is needed in a specific customer deployment, set **Codec Selection** to *Custom* and use the left/right arrow buttons to move the desired codecs between the **Unused** and **Selected** columns. Use the up/down arrows to reorder the codec priority list.
- Select **T38 Fallback** for **Fax Transport Support** so that Avaya IP Office uses T.38 for sending and receiving faxes on this SIP line. If the called destination does not support T.38, the system will send a re-INVITE to change the transport method to G.711 (for falling back to G.711 pass-through fax).
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones as out-of-band RTP events as per RFC2833.
- Uncheck the **VoIP Silence Suppression** option box.
- Check the **Re-invite Supported** option box.
- Check the **PRACK/100rel Supported** option box. This setting enables support by Avaya IP Office for the PRACK (Provisional Reliable Acknowledgement) message on SIP trunks.

The screenshot shows the configuration interface for a SIP Line (Line 33) in the VoIP tab. The interface includes several sections:

- Codec Selection:** A dropdown menu 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). Navigation buttons (right arrow, up arrow, left arrow, down arrow, and another right arrow) are positioned between the columns.
- Fax Transport Support:** A dropdown menu is set to "T38 Fallback".
- DTMF Support:** A dropdown menu is set to "RFC2833".
- Media Security:** A dropdown menu is set to "Disabled".
- Options:** A list of checkboxes on the right side:
  - VoIP Silence Suppression
  - Re-invite Supported
  - Codec Lockdown
  - Allow Direct Media Path
    - Force direct media with phones
  - PRACK/100rel Supported
  - G.711 Fax ECAN

### 5.4.7. SIP Line – T.38 Fax Tab

Select the **T38 Fax** tab. Leave the T.38 settings at the default values.

The screenshot shows the 'SIP Line - Line 33' configuration window with the 'T38 Fax' tab selected. The window has a title bar with standard OS icons and a tabbed interface with the following tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax (active), SIP Credentials, SIP Advanced, and Engineering. The 'T38 Fax' tab contains the following settings:

- T38 Fax Version: 3 (dropdown)
- Transport: UDPTL (dropdown)
- Redundancy section:
  - Low Speed: 0 (spin box)
  - High Speed: 0 (spin box)
- TCF Method: Trans TCF (dropdown)
- Max Bit Rate (bps): 14400 (dropdown)
- EFlag Start Timer (msecs): 2600 (spin box)
- EFlag Stop Timer (msecs): 2300 (spin box)
- Tx Network Timeout (secs): 150 (spin box)
- Use Default Values:  (checkbox)

On the right side of the window, there is a panel with the following options:

- Scan Line Fix-up
- TFOP Enhancement
- Disable T30 ECM
- Disable EFlags For First DIS
- Disable T30 MR Compression
- NSF Override (checkbox)
  - Country Code: 0 (spin box)
  - Vendor Code: 0 (spin box)

At the bottom right of the window are three buttons: OK, Cancel, and Help.

## 5.4.8. SIP Line – Advanced Tab

Select the **SIP Advanced** tab. Set the parameter as shown below.

- Check the **Emulate NOTIFY for REFER** box. With REFER enabled, the Avaya 1100 Series Deskphones and Avaya Communicator for Windows expects to receive a NOTIFY message to indicate that the referred (i.e., transferred) call was successful. If the NOTIFY is not received from the far-end, then the call display will indicate that the transfer failed even if the transfer was successful. If the **Emulate NOTIFY for REFER** box is checked, then Avaya IP Office will send a NOTIFY message (on behalf of the far-end) to the Avaya 1100 Series Deskphones and Avaya Communicator for Windows.

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

The screenshot shows the 'SIP Line - Line 33' configuration window with the 'SIP Advanced' tab selected. The window is divided into several sections:

- Addressing:** Association Method is set to 'By Source IP address' and Call Routing Method is set to 'Request URI'. Suppress DNS SRV Lookups is unchecked.
- Identity:** A list of checkboxes for various identity settings. 'Cache Auth Credentials' is checked. 'User-Agent and Server Headers' is an empty text field.
- Media:** A list of checkboxes and dropdowns for media-related settings. 'Emulate NOTIFY for REFER' is checked. 'No REFER if using Diversion' is unchecked.
- Call Control:** A list of settings for call control, including timeouts and responses. 'Call Initiation Timeout (s)' is 4, 'Call Queuing Timeout (m)' is 5, 'Service Busy Response' is '486 - Busy Here', 'on No User Responding Send' is '408-Request Timeout', and 'Action on CAC Location Limit' is 'Allow Voicemail'.

## 5.5. Short Code

Define a short code to route outbound calls to the SIP line. To create a short code, right-click on **Short Code** in the Navigation Pane and select **New** (not shown). 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. The **9N;** short code, used for the compliance test, 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 (**Section 5.8**).
- Set the **Line Group ID** to the ARS route to be used (**Section 5.8**).

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

The screenshot displays the Avaya Management System interface. On the left is the 'IP Offices' navigation pane with a tree view including: BOOTP (2), Operator (3), Atlantic City, System (1), Line (25), Control Unit (3), Extension (25), User (27), Group (1), Short Code (64), Service (0), RAS (1), Incoming Call Route (73), and WAN Port (0). The main area is titled '9N;; Dial' and contains the following configuration fields:

Short Code	
Code	9N;
Feature	Dial
Telephone Number	N
Line Group ID	51: SP SIP Route
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization 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 compliance test, when a user dialed \*67 plus the number, Avaya IP Office would include the user’s telephone number (DID number assigned to the user) in the **P-Asserted-Identity** (PAI) header and would include the **Privacy: id** header in the outbound INVITE message. Consequently, ThinkTel would prevent presentation of the caller id to the called PSTN destination.

The screenshot shows a configuration window titled '\*67N;: Dial'. The window contains the following fields and controls:

- Code:** \*67N;
- Feature:** Dial (dropdown menu)
- Telephone Number:** WN
- Line Group ID:** 51: SP SIP Route (dropdown menu)
- Locale:** (dropdown menu)
- Force Account Code:**
- Force Authorization Code:**

## 5.6. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line. 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 **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by ThinkTel. The **SIP Display Name (Alias)** can optionally be configured with a descriptive text string. The value entered for the **Contact** field will be used in the Contact header for outgoing SIP INVITE to the service provider. The value entered for the **SIP Name** is used as the user part of the SIP URI in the From header for outgoing SIP trunk calls.

If outbound 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 (or alternatively use the **\*67N**; short code as defined in **Section 5.5**).

IP Offices		Extn243: 243	
BOOTP (2)		User	Voicemail
Operator (3)		DND	Short Codes
Atlantic City		Source Numbers	Telephony
System (1)		Forwarding	Dial In
Line (25)		Voice Recording	Button Programming
Control Unit (3)		Menu Programming	Mobility
Extension (25)		Group Membership	
User (27)		Announcements	SIP
Group (1)		Personal Directory	Web Self-Administration
Short Code (64)			
Service (0)			
RAS (1)			
Incoming Call Route (73)			

SIP Name	4385550978
SIP Display Name (Alias)	Extn243
Contact	4385550978
<input type="checkbox"/> Anonymous	

## 5.7. 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 Route** in the Navigation Pane and select **New** (not shown).

### 5.7.1. Incoming Call Route – Standard Tab

On the **Standard** tab in the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capability** to *Any Voice*.
- Set the **Line Group ID** to the **Incoming Group** of the SIP Line defined in **Section 5.4.5**.
- Set the **Incoming Number** to the incoming DID number on which this route should match.

The screenshot shows the configuration window for an Incoming Call Route. The left pane shows a tree view of system components, with 'Incoming Call Route (73)' selected. The right pane shows the 'Standard' tab configuration for the route 33 4385550978. The configuration fields are as follows:

Bearer Capability	Any Voice
Line Group ID	33
Incoming Number	4385550978
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

### 5.7.2. Incoming Call Route – Destination Tab

On the **Destinations** tab, select the destination from the pull-down list of the **Destination** field. In this example, incoming calls to the DID number 4385550978 on Incoming Group 33 are to be routed to the user “Extn243” at extension 243.

The screenshot shows the 'Destinations' tab configuration for the route 33 4385550978. The configuration table is as follows:

TimeProfile	Destination	Fallback Extension
Default Value	243 Extn243	

The screen below shows the mapping of inbound calls to IP Office Voicemail Pro for message retrieval.

The screenshot shows a software window with a title bar containing the phone number "33 4385550980". Below the title bar are three tabs: "Standard", "Voice Recording", and "Destinations". The "Destinations" tab is active and displays a table with the following structure:

	TimeProfile	Destination	Fallback Extension
▶	Default Value	VoiceMail	

## 5.8. Alternate Route Selection (ARS)

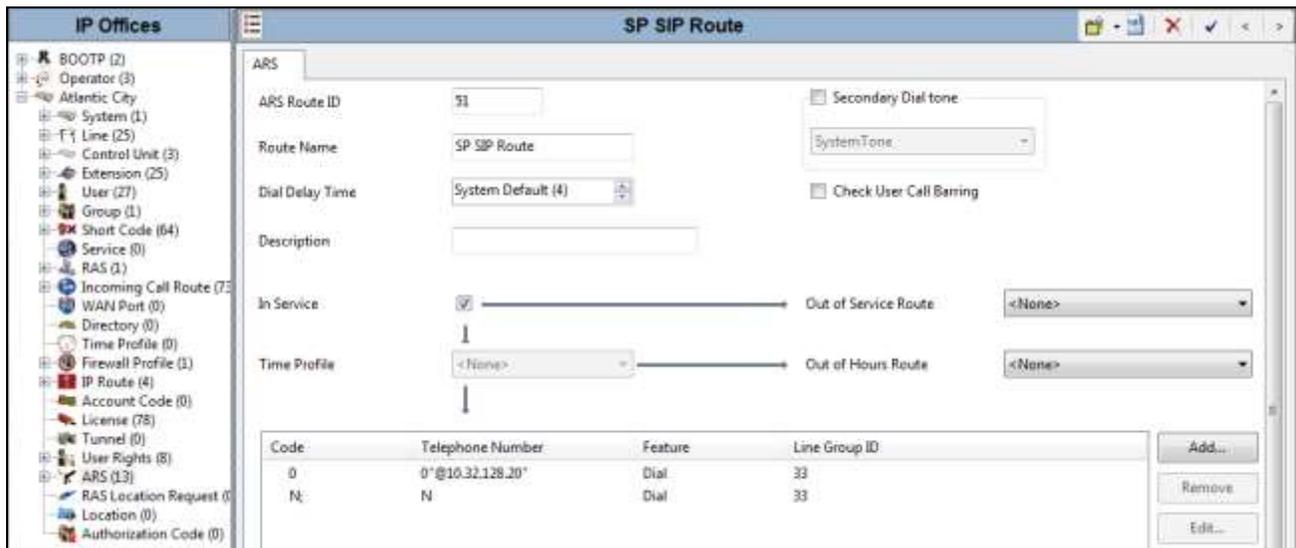
Alternate Route Selection (ARS) is used to route outbound traffic to the SIP line. To define a new ARS route, right-click **ARS** in the Navigation pane and select **New**. In the Details pane that appears, a collection of matching patterns (similar to short codes) can be entered to route calls as shown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

For the compliance test, two entries were created. The first entry matches on **0** and the second entry matches on any other number **N**.

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. The value **N** will match any number.
- Set **Feature** to **Dial**. This is the action that the entry will perform.
- For **Code 0**, set **Telephone Number** to **0"@ipaddr"**, where *ipaddr* is the IP address of the internal interface of the Avaya SBCE and used to configure the trunk in **Section 5.4.3**. Adding the IP address in this field was required to ensure that the correct host appeared in the outbound Request-URI header when dialing 0. This was not required when matching on any other dialed number as shown next.
- For **Code N;**, set **Telephone Number** to **N**. 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.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.4.5**. This entry will use this line group when placing the outbound call.

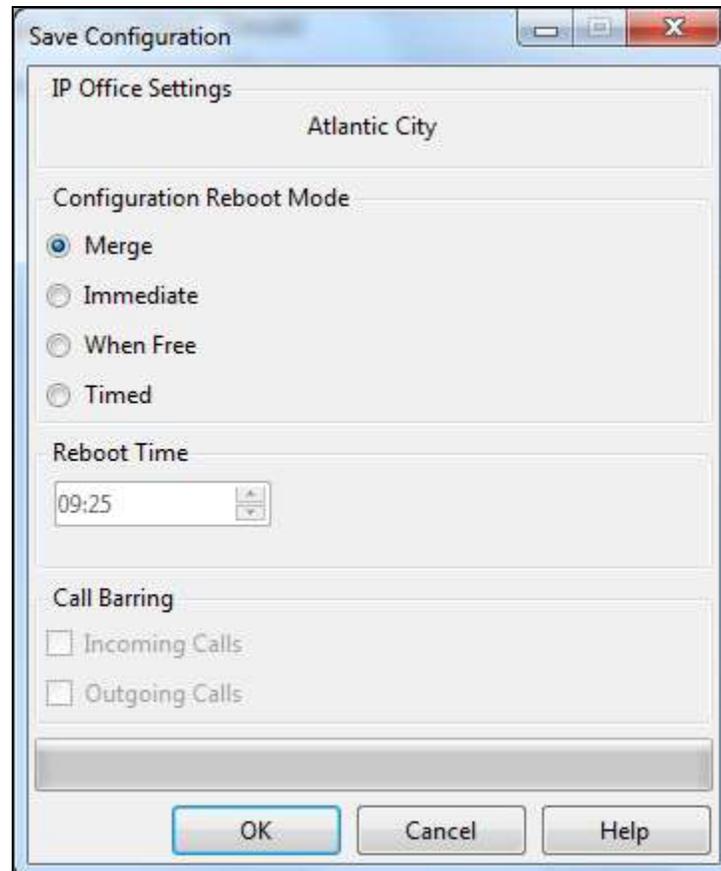
Click the **OK** button (not shown).



## 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.



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

- IP Office Settings:** Atlantic City
- Configuration Reboot Mode:** Radio buttons for Merge (selected), Immediate, When Free, and Timed.
- Reboot Time:** A time selection field showing 09:25.
- Call Barring:** Checkboxes for Incoming Calls and Outgoing Calls, both of which are unchecked.
- Buttons:** OK, Cancel, and Help.

## 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 (i.e., 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 the 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 with a text input field containing "ucsec", a "Password:" label with an empty text input field, and 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." Below that, it says: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, the copyright notice reads: "© 2011 - 2015 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.

**Session Border Controller for Enterprise** AVAYA

**Dashboard**

**Information**

System Time	12:40:17 PM EST	<a href="#">Refresh</a>
Version	7.0.0-21-6602	
Build Date	Sun Aug 9 21:08:40 EDT 2015	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	-	
Failed Login Attempts	7	

**Installed Devices**

EMS
vnj-sbce2

**Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

None found.

**Notes**

No notes found.

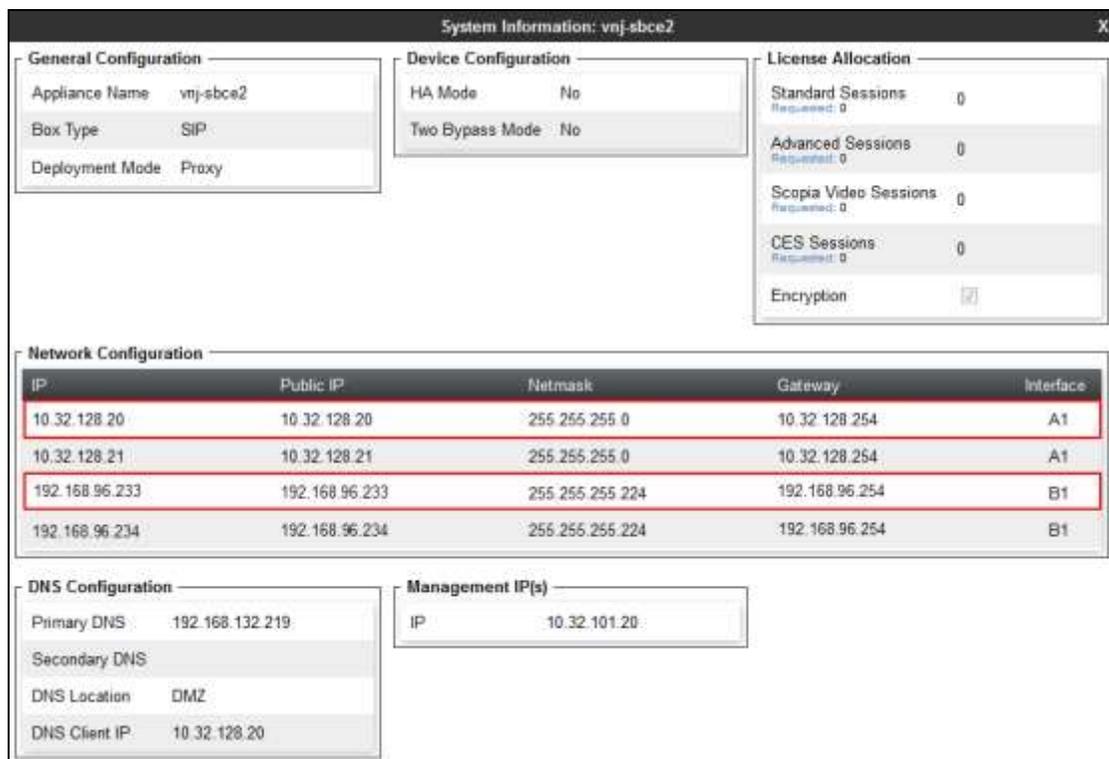
[Add](#)

## 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.



A System Information page will appear showing the information provided during installation. 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** highlighted below represent the private (or internal) and public (or external) interfaces of the Avaya SBCE for SIP Trunking. Each of these interfaces must be enabled after installation. Note that the **Management IP** is on a different subnet than either the A1 and B1 interfaces. Lastly, the **DNS Configuration** must be configured since DNS will be used to resolve the ThinkTel domain to an IP address.



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 shows the Avaya Session Border Controller for Enterprise web interface. The title bar reads "Session Border Controller for Enterprise" and the AVAYA logo is in the top right. The left navigation pane includes "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "SIP Cluster", "Domain Policies", "TLS Management", "Device Specific Settings", "Network Management", and "Media Interface". The "Network Management" section is expanded, showing "Devices" with "vnj-sbce2" selected. The "Interface Configuration" tab is active, displaying a table with the following data:

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

### 6.3. Signaling Interface

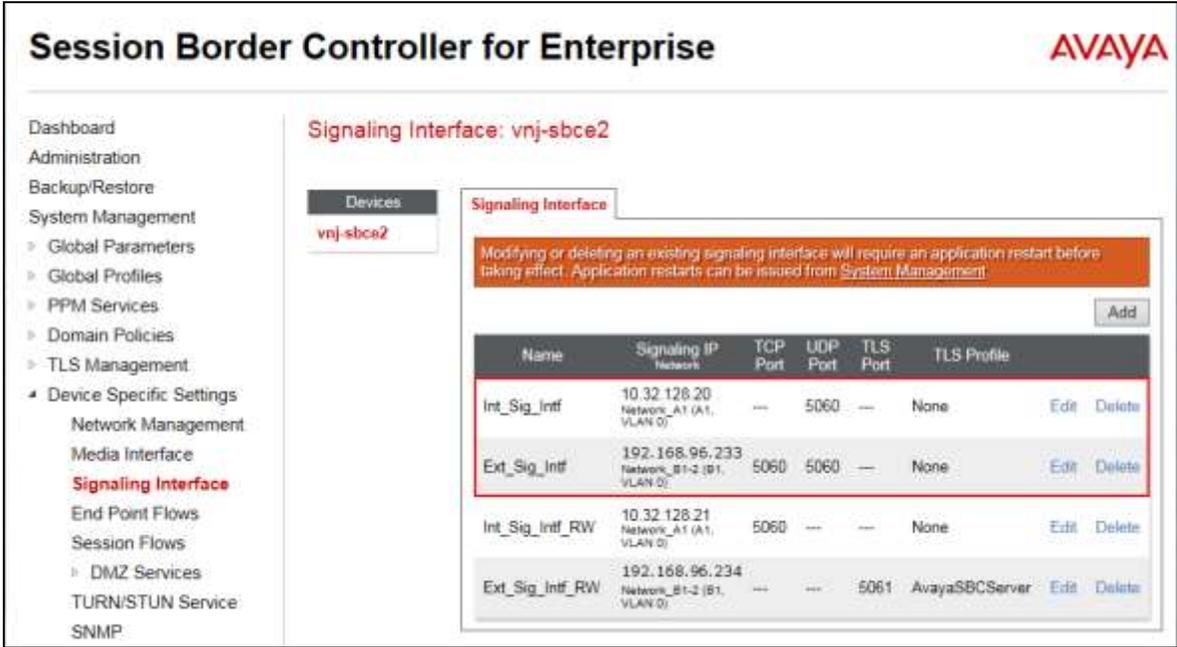
A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

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 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. These two signaling interfaces are shown 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) specified in **Section 6.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) specified 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 ThinkTel uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.



Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig_Intf	10.32.128.20 Network_A1 (A1, VLAN 0)	---	5060	---	None	Edit Delete
Ext_Sig_Intf	192.168.96.233 Network_B1-2 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
Int_Sig_Intf_RW	10.32.128.21 Network_A1 (A1, VLAN 0)	5060	---	---	None	Edit Delete
Ext_Sig_Intf_RW	192.168.96.234 Network_B1-2 (B1, VLAN 0)	---	---	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 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 shown 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) specified in **Section 6.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) specified 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.



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo. The left navigation pane includes "Device Specific Settings" > "Media Interface". The main content area is titled "Media Interface: vnj-sbce2" and contains a table of configured media interfaces. A warning message at the top states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." The table lists four interfaces: Int\_Media\_Intf, Ext\_Media\_Intf, Int\_Media\_Intf\_RW, and Ext\_Media\_Intf\_RW, each with its Name, Media IP Network, Port Range, and Edit/Delete actions.

Name	Media IP Network	Port Range	Edit	Delete
Int_Media_Intf	10.32.128.20 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.233 Network_B1-2 (B1, VLAN 0)	35000 - 40000	Edit	Delete
Int_Media_Intf_RW	10.32.128.21 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Ext_Media_Intf_RW	192.168.96.234 Network_B1-2 (B1, VLAN 0)	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 one server interworking profile for Avaya IP Office and another for the service provider SIP server. These profiles will be applied to the appropriate servers in **Section 6.6.1** and **6.6.2**.

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.

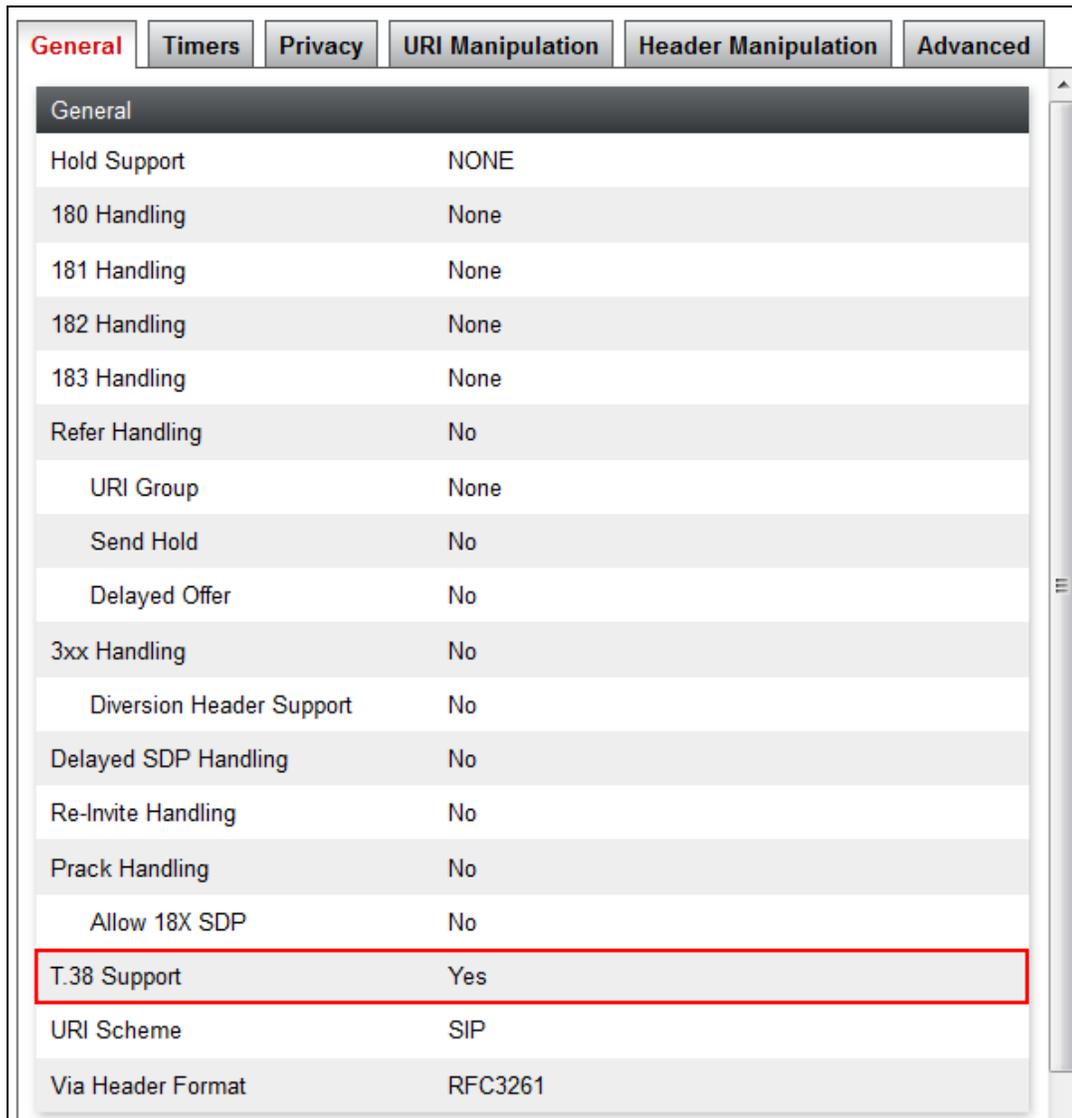
The screen below shows the user interface as described above, before creating the specific server interworking profiles used for the compliance test.

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", "Domain DoS", "Fingerprint", "Server Interworking", "Phone Interworking", "Media Forking", "Routing", and "Server Configuration". The main content area is titled "Interworking Profiles: cs2100" 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, there are tabs for "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of settings:

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

The recommended method of creating a server interworking profile for Avaya IP Office is to first clone the predefined profile **avaya-ru** and then make any changes necessary to support a specific service provider. For the compliance test, server interworking profile **IPOffice-T38** was created for Avaya IP Office using this approach and the **T.38 Support** parameter was set to **Yes**. The **General** tab parameters are shown below.



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

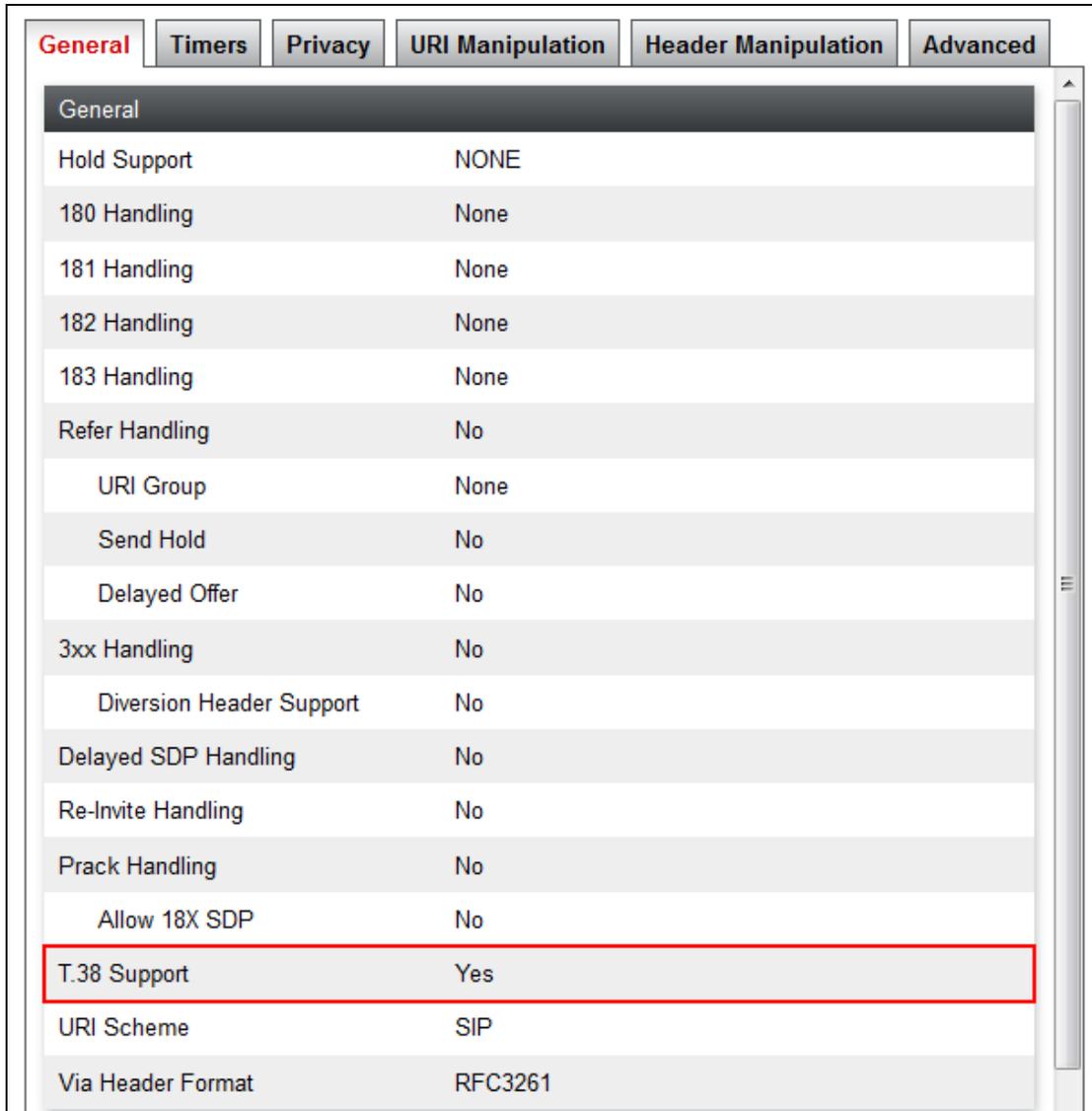
The **Timers**, **URI Manipulation** and **Header Manipulation** tabs have no configured entries.

The **Advanced** tab parameters are shown below. Highlighted values below indicate differences between the cloned profile and the default value.

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes					Both Sides
Include End Point IP for Context Lookup					Yes
Extensions					Avaya
Diversion Manipulation					No
Has Remote SBC					Yes
Route Response on Via Port					No
<b>DTMF</b>					
DTMF Support					None
<input type="button" value="Edit"/>					

## 6.5.2. Server Interworking – ThinkTel

For the compliance test, server interworking profile *SP-General-T38* was created for the ThinkTel SIP server. When creating the profile, the default values were used for all parameters except that the **T.38 Support** parameter was set to **Yes**.



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

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

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

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes					---
Include End Point IP for Context Lookup					No
Extensions					None
Diversion Manipulation					No
Has Remote SBC					Yes
Route Response on Via Port					No
<b>DTMF</b>					
DTMF Support					None
<input type="button" value="Edit"/>					

## 6.6. Server Configuration

A server configuration profile defines the attributes of the physical server. Create one server configuration profile for Avaya IP Office and another for 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 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 (expanded), Domain DoS, Server Interworking, Media Forking, Routing, and Server Configuration (highlighted in red). The main content area is titled "Server Configuration: IPO-ACity" and features an "Add" button, "Rename", "Clone", and "Delete" buttons. Below the title are tabs for "General", "Authentication", "Heartbeat", and "Advanced". The "General" tab is active, showing "Server Type" as "Call Server". A table lists server configurations:

IP Address / FQDN	Port	Transport
10.32.128.25	5060	UDP
10.32.128.25	5060	TCP

An "Edit" button is located below the table.

### 6.6.1. Server Configuration – Avaya IP Office

For the compliance test, the 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 Address / FQDN** to the Avaya IP Office LAN1 address (**Section 5.2.1**).
- Enter a valid combination of **Port** and **Transport** that Avaya IP Office will use to listen for SIP requests. The standard SIP UDP/TCP port is 5060. Additional combinations can be entered by clicking the **Add** button (not shown).

IP Address / FQDN	Port	Transport
10.32.128.25	5060	UDP
10.32.128.25	5060	TCP

The **Authentication** and **Heartbeat** tabs have no entries.

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

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

## 6.6.2. Server Configuration – ThinkTel

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

- Set **Server Type** to *Trunk Server*.
- Set **IP Address / FQDN** to the ThinkTel domain. The Avaya SBCE will use DNS to convert the FQDN to an IP address.
- Enter a valid combination of **Port** and **Transport** that the ThinkTel SIP proxy will use to listen for SIP requests. Additional combinations can be entered by clicking the **Add** button (not shown).

The screenshot shows the 'General' tab of a configuration interface. It features four tabs: 'General' (selected), 'Authentication', 'Heartbeat', and 'Advanced'. The configuration is as follows:

Server Type	Trunk Server	
IP Address / FQDN	Port	Transport
tor.trk.tprm.ca	5060	UDP

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

The **Authentication** and **Heartbeat** tabs have no entries.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for ThinkTel defined in **Section 6.5.2**.

The screenshot shows the 'Advanced' tab of the configuration interface. It features four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced' (selected). The configuration is as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General-T38
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	<input type="checkbox"/>

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

## 6.7. 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 6.10**.

To create a new profile, navigate to **Domain Policies** → **Application Rules** 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.

For the compliance test, the application rules profile named **low-AudioSessions** was cloned from the **default-trunk** profile in which the settings for both **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** were adjusted down to **500** (from 2000) for **Audio**. This change was to accommodate the maximum capacity on the Avaya SBCE running on the Portwell CAD-0208 server. The **low-AudioSessions** application rules profile was used for both Avaya IP Office and the ThinkTel SIP server.



The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies (selected), Application Rules (selected), 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: low-AudioSessions" and includes an "Add" button, a "Filter By Device" dropdown, and "Rename", "Clone", and "Delete" buttons. A blue bar prompts to "Click here to add a description...". Below this is a table for the application rule configuration:

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

Below the table is a "Miscellaneous" section with two rows: "CDR Support" set to "None" and "RTCP Keep-Alive" set to "No". An "Edit" button is located at the bottom right of the configuration area.

## 6.8. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger end point policy group defined in **Section 6.10**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Avaya IP Office and the ThinkTel 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 is shown below.

The **Media Encryption** tab shows the **Preferred Formats** field for both Audio Encryption and Video Encryption is set to *RTP* (as opposed to SRTP) indicating that no encryption was used.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top header shows the product name and the AVAYA logo. A left-hand navigation menu lists various management sections, with 'Media Rules' highlighted under 'Domain Policies'. 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 banner states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are five tabs: 'Media Encryption', 'Media Silencing', 'Media QoS', 'Media BFCP', and 'Media FECC'. The 'Media Encryption' tab is active, showing settings for 'Audio Encryption' and 'Video Encryption'. Both sections have 'Preferred Formats' set to 'RTP' and 'Interworking' checked. A 'Miscellaneous' section at the bottom has 'Capability Negotiation' unchecked. An 'Edit' button is located at the bottom right of the configuration area.

The **Media Silencing** tab shows **Media Silencing** was disabled.

The screenshot shows a configuration interface with five tabs: Media Encryption, Media Silencing (highlighted in red), Media QoS, Media BFCP, and Media FECC. Below the tabs is a section titled "Media Silencing" with a single checkbox that is unchecked. An "Edit" button is located at the bottom right of the section.

The **Media QoS** settings used for the compliance test are shown below. This QoS setting is not a requirement for interoperability and QoS was not tested as part of the compliance test. If the QoS setting shown here does not meet the needs of the customer then it should be set as per customer requirements. Clone any predefined profile (e.g., **default-low-med**) before making changes.

The screenshot shows a configuration interface with five tabs: Media Encryption, Media Silencing, Media QoS (highlighted in red), Media BFCP, and Media FECC. The "Media QoS" section is expanded and contains several sub-sections: "Media QoS Reporting" with "RTCP Enabled" (unchecked); "Media QoS Marking" with "Enabled" (checked) and "QoS Type" set to "DSCP"; "Audio QoS" with "Audio DSCP" set to "EF"; and "Video QoS" with "Video DSCP" set to "EF". An "Edit" button is located at the bottom right of the section.

On the **Media BFCP** tab, BFCP is disabled.

The screenshot shows a configuration interface with five tabs: Media Encryption, Media Silencing, Media QoS, Media BFCP (highlighted in red), and Media FECC. Below the tabs is a section titled "Binary Floor Control Protocol" with a single checkbox for "BFCP Enabled" that is unchecked. An "Edit" button is located at the bottom right of the section.

On the **Media FECC** tab, FECC is disabled.



The image shows a configuration interface with five tabs: Media Encryption, Media Silencing, Media QoS, Media BFCP, and Media FECC. The Media FECC tab is selected and highlighted in red. Below the tabs is a dark grey header bar labeled "Far End Camera Control". Underneath this header is a white area containing the text "FECC Enabled" followed by an unchecked checkbox. At the bottom center of this area is an "Edit" button.

## 6.9. 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 end point policy group defined in **Section 6.10**.

To create a new profile, navigate to **Domain Policies** → **Signaling Rules** 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 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 screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the menu structure, with "Signaling Rules" selected under "Domain Policies". 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", "Signaling QoS", and "UCID". The "General" tab is active, showing a table of settings for "Inbound" and "Outbound" traffic.

Category	Setting	Value
Inbound	Requests	Allow
	Non-2XX Final Responses	Allow
	Optional Request Headers	Allow
	Optional Response Headers	Allow
Outbound	Requests	Allow

### 6.9.1. Signaling Rules – Avaya IP Office

For the compliance test, the predefined **default** signaling rule was used for Avaya IP Office. The **General** tab settings of the default signaling rule are shown below.

<b>General</b>	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
<b>Inbound</b>						
Requests		Allow				
Non-2XX Final Responses		Allow				
Optional Request Headers		Allow				
Optional Response Headers		Allow				
<b>Outbound</b>						
Requests		Allow				
Non-2XX Final Responses		Allow				
Optional Request Headers		Allow				
Optional Response Headers		Allow				
<b>Content-Type Policy</b>						
Enable Content-Type Checks		<input checked="" type="checkbox"/>				
Action	Allow	Multipart Action		Allow		
Exception List		Exception List				
<input type="button" value="Edit"/>						

The **Requests**, **Responses**, **Request Headers**, and **Response Headers** tabs have no entries.

The **Signaling QoS** tab is shown below.

General	Requests	Responses	Request Headers	Response Headers	<b>Signaling QoS</b>	UCID
Signaling QoS <input checked="" type="checkbox"/>						
QoS Type		DSCP				
DSCP		AF41				
<input type="button" value="Edit"/>						

The **UCID** setting is shown below.

<b>General</b>	Requests	Responses	Request Headers	Response Headers	Signaling QoS	<b>UCID</b>
<div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> UCID <input type="checkbox"/> </div> <div style="text-align: center;"> <input type="button" value="Edit"/> </div>						

### 6.9.2. Signaling Rules – ThinkTel

For the compliance test, the **SrvPrvder-SR** signaling rule was used for ThinkTel. The signaling rule was created using all default values with the exception of the QoS settings. The **General** tab settings are shown below.

<b>General</b>	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
<b>Inbound</b>						
Requests			Allow			
Non-2XX Final Responses			Allow			
Optional Request Headers			Allow			
Optional Response Headers			Allow			
<b>Outbound</b>						
Requests			Allow			
Non-2XX Final Responses			Allow			
Optional Request Headers			Allow			
Optional Response Headers			Allow			
<b>Content-Type Policy</b>						
Enable Content-Type Checks				<input checked="" type="checkbox"/>		
Action	Allow		Multipart Action	Allow		
Exception List			Exception List			
<input type="button" value="Edit"/>						

The **Requests**, **Responses**, **Request Headers**, and **Response Headers** tabs have no entries.

The **Signaling QoS** tab is shown below. This QoS setting is not a requirement for interoperability and QoS was not tested as part of the compliance test. If the QoS setting shown here does not meet the needs of the customer then it should be set as per customer requirements.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID						
<table border="1"> <tr> <td>Signaling QoS</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>QoS Type</td> <td>DSCP</td> </tr> <tr> <td>DSCP</td> <td>EF</td> </tr> </table>							Signaling QoS	<input checked="" type="checkbox"/>	QoS Type	DSCP	DSCP	EF
Signaling QoS	<input checked="" type="checkbox"/>											
QoS Type	DSCP											
DSCP	EF											
<input type="button" value="Edit"/>												

The **UCID** setting is shown below.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID		
<table border="1"> <tr> <td>UCID</td> <td><input type="checkbox"/></td> </tr> </table>							UCID	<input type="checkbox"/>
UCID	<input type="checkbox"/>							
<input type="button" value="Edit"/>								

## 6.10. End Point Policy Groups

An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the service provider SIP server. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 6.13**.

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 screen below shows the user interface as described above, before creating the specific end point policy groups used for the compliance test.

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

### 6.10.1. End Point Policy Group – Avaya IP Office

For the compliance test, the end point 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 specified in **Section 6.7**. The details of the default settings for **Media** and **Signaling** are shown in **Section 6.8** and **Section 6.9.1** respectively.

Order	Application	Border	Media	Security	Signaling
1	low-AudioSessions	default	default-low-med	default-low	default

## 6.10.2. End Point Policy Group – ThinkTel

For the compliance test, the end point policy group *SP-EP-Policy* was created for the ThinkTel SIP server. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Signaling**. For **Application**, enter the application rule specified in **Section 6.7**. For **Signaling**, enter the signaling rule specified in **Section 6.9.2**. The details of the default settings for **Media** are shown in **Section 6.8**.

Order	Application	Border	Media	Security	Signaling	
1	low-AudioSessions	default	default-low-med	default-low	SrvPrvder-SR	Edit

## 6.11. 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 6.13**. Create one routing profile for Avaya IP Office and another for 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.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.32.128.25	UDP	Edit Delete

### 6.11.1. Routing – Avaya IP Office

For the compliance test, the 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 **Load Balancing** to *Priority* from the pull-down menu.
- Enable **Next Hop Priority**.
- Click **Add** to enter the following for the Next Hop Address:
  - Set **Priority/Weight** to **1**.
  - For **Server Configuration**, select *IPO-ACity* (Section 6.6.1) from the pull-down menu. The **Next Hop Address** will be filled-in automatically.

Click **Finish**.

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IPO-ACity	10.32.128.25:5060 (UDP)	None	Delete

Buttons: Add, Finish

## 6.11.2. Routing – ThinkTel

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

- Set the **URI Group** to the wild card \* to match on any URI.
- Set **Load Balancing** to **DNS/SRV** from the pull-down menu.
- Click **Add** to enter the following for the Next Hop Address:
  - For **Server Configuration**, select **ThinkTel (Section 6.6.2)** from the pull-down menu. The **Next Hop Address** will be filled-in automatically.

Click **Finish**.

URI Group	Time of Day
*	default
Load Balancing	NAPTR
DNS/SRV	<input type="checkbox"/>
Transport	Next Hop Priority
None	<input type="checkbox"/>
Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
0	ThinkTel	tor.trk.tprm.ca:5060 (UDP)	None	Delete

Finish

## 6.12. 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 end point flow in **Section 6.13**. For the compliance test, the predefined **default** topology hiding profile (shown below) was used for both Avaya IP Office and the ThinkTel 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, or 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  
Server Interworking  
Media Forking  
Routing  
Server Configuration  
**Topology Hiding**  
Signaling Manipulation  
URI Groups  
SNMP Traps  
Time of Day Rules  
PPM Services  
Domain Policies

**Topology Hiding Profiles: default** Add Close

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

**Topology Hiding**

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

Edit

## 6.13. End Point Flows

End point 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 end point flow and the destination end point 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 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 top header shows "Session Border Controller for Enterprise" and the "AVAYA" logo. The left navigation pane includes "Device Specific Settings" with "End Point Flows" selected. The main content area is titled "End Point Flows: vnj-sbce2" and features a "Devices" list with "vnj-sbce2" selected. The "Server Flows" tab is active, showing a table of configurations. An "Add" button is visible in the top right of the configuration area.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	View	Cl
1	IPO-ACity	*	Ext_Sig_Intf	Int_Sig_Intf	IPO-EP-Policy	To-ThinkTel	View	Cl
2	IPO-ACity-RW	*	Ext_Sig_Intf_RW	Int_Sig_Intf_RW	RTP-EP-RW	default_RW	View	Cl

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

For the compliance test, the end point 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-ThinkTel* 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 6.6.1**.
- 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 6.10.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.11.2** used to direct traffic to the ThinkTel SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Avaya IP Office in **Section 6.12**.

Criteria	
Flow Name	IPO-ACity
Server Configuration	IPO-ACity
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf

Profile	
Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	IPO-EP-Policy
Routing Profile	To-ThinkTel
Topology Hiding Profile	default
Signaling Manipulation Script	None
Remote Branch Office	Any

### 6.13.2. End Point Flow – ThinkTel

For the compliance test, the end point flow *ThinkTel* was created for the ThinkTel SIP server. All traffic from ThinkTel 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 ThinkTel SIP server created in **Section 6.6.2**.
- 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 ThinkTel in **Section 6.10.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 6.11.1** used to direct traffic to Avaya IP Office.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for ThinkTel in **Section 6.12**.

Criteria	
Flow Name	ThinkTel
Server Configuration	ThinkTel
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Intf

Profile	
Signaling Interface	Ext_Sig_Intf
Media Interface	Ext_Media_Intf
End Point Policy Group	SP-EP-Policy
Routing Profile	To-IPO-ACity
Topology Hiding Profile	default
Signaling Manipulation Script	None
Remote Branch Office	Any

## 7. ThinkTel SIP Trunking Configuration

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

- ThinkTel SIP Trunking Service domain.
- Transport and port for the ThinkTel SIP connection to the Avaya SBCE at the enterprise.
- SIP Credentials
- DID numbers to assign to users at the enterprise.
- Supported codecs and their preference order.

## 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. Avaya IP Office System Status

Use the Avaya IP Office System Status application to verify the SIP Line channels state and to check alarms:

- Launch the application from **Start → Programs → IP Office → System Status** on the Avaya IP Office Manager PC. Login with appropriate credentials. 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 channels where no active calls are currently in session. The state should be **Connected** for channels engaged in active calls.

**AVAYA IP Office System Status**

Help Snapshot LogOff Exit About

**System**  
**Alarms (4)**  
**Extensions (19)**  
**Trunks (25)**  
 Lines:1 - 4  
 Lines:5 - 8  
 Line:17  
 Line:18  
 Line:19  
 Line:20  
 Line:21  
 Line:22  
 Line:23  
 Line:24  
 Line:25  
 Line:26  
 Line:27  
 Line:28  
 Line:29  
 Line:30  
 Line:31  
 Line:32  
**Line:33**  
 Active Calls  
**Resources**  
**Voicemail**  
**IP Networking**  
 Locations

**Status** Utilization Summary Alarms Registration

**SIP Trunk Summary**

Line Service State: In Service  
 Peer Domain Name: sip://10.32.128.20  
 Resolved Address: 10.32.128.20  
 Line Number: 33  
 Number of Administered Channels: 10  
 Number of Channels in Use: 0  
 Administered Compression: G711 Mu, G711 A, G729 A, G7231  
 Enable Faststart: Off  
 Silence Suppression: Off  
 Media Stream: RTP  
 Layer 4 Protocol: UDP  
 SIP Trunk Channel Licenses: Unlimited  
 SIP Trunk Channel Licenses in Use: 0  
 SIP Device Features: REFER (Incoming and Outgoing)

Chan...	U...	Call Ref	Curr...	Time in State	Remote Media ...	Co...	Conn...	Caller ID or...	Other Party on Call	Dirac...	Round Trip ...	Recei...	Recei...	Trans...	Tran...
1			Idle	5 da...											
2			Idle	5 da...											
3			Idle	7 da...											
4			Idle	7 da...											
5			Idle	7 da...											
6			Idle	7 da...											
7			Idle	7 da...											
8			Idle	7 da...											

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

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

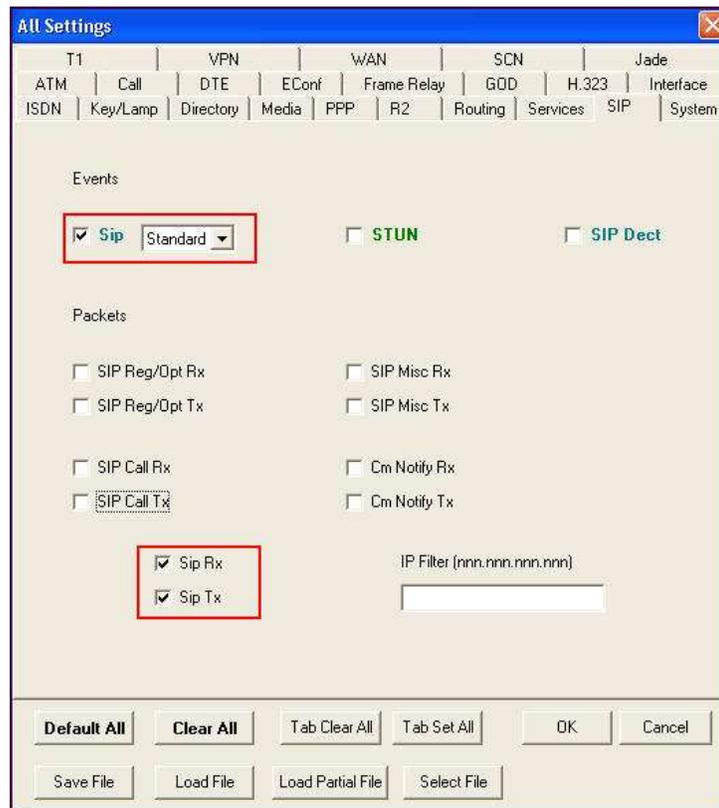
Status	Utilization Summary	<b>Alarms</b>	Registration
<b>Alarms for Line: 33 SIP sip://10.32.128.20</b>			
Last Date Of Error	Occurrences	Error Description	

## 8.2. Avaya IP Office Monitor

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



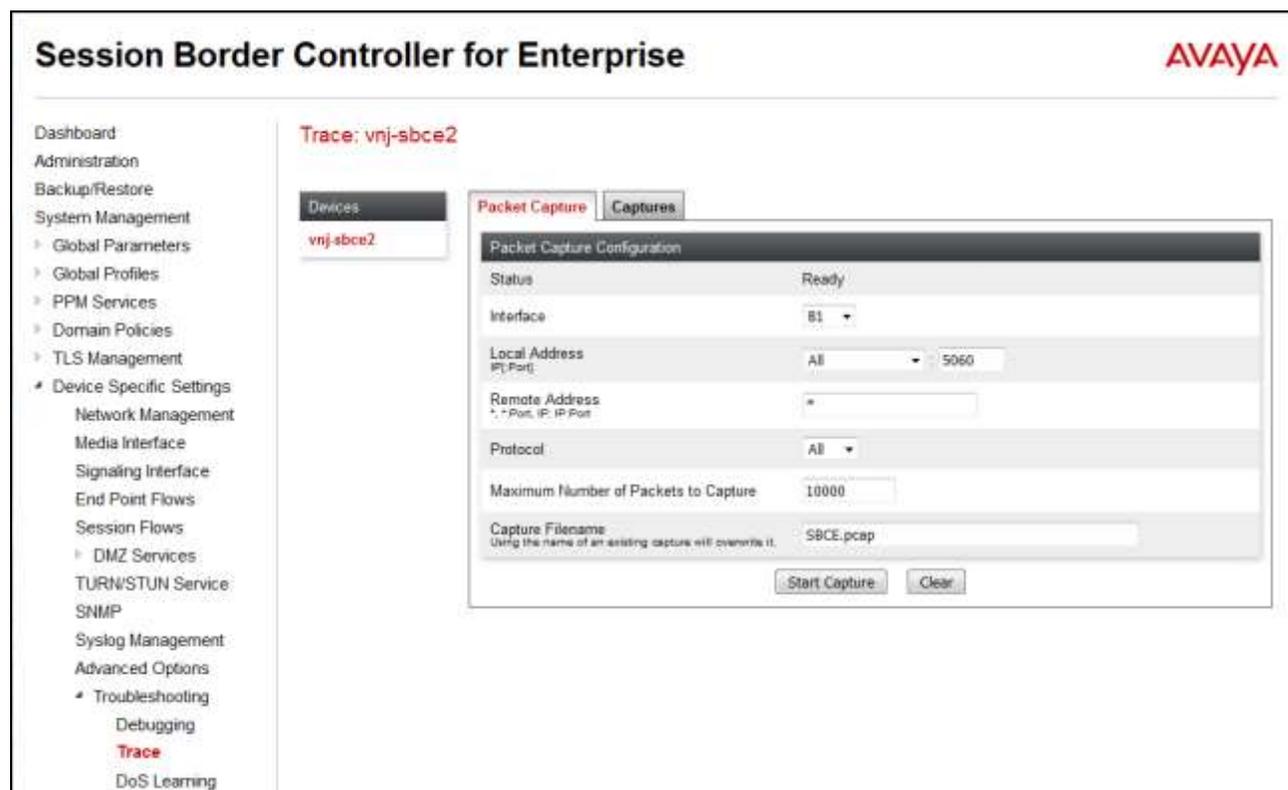
The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, **Standard** SIP Events and the **SIP Rx** and **SIP Tx** boxes are checked.



### 8.3. Avaya Session Border Controller for Enterprise Protocol Trace

The Avaya SBCE can take internal traces on specified interfaces. SIP signaling crossing both interfaces A1 and B1 can be captured for troubleshooting. In the Avaya SBCE web interface, navigate to **Device Specific Settings** → **Troubleshooting** → **Trace** to invoke this facility. In the **Packet Capture** tab, select or supply the relevant information (e.g., A1 or B1 or any interfaces, IP/port, protocol, number of packets to capture, capture file name, etc.), then press the **Start Capture** button to start the trace. The captured trace file can then be downloaded from the **Captures** tab for examination using a protocol sniffer application such as Wireshark.

The screen below shows the setup for capturing packets on port 5060 on the public interface of the Avaya SBCE (**B1**).



## 9. Conclusion

The ThinkTel SIP Trunking Service passed compliance testing with Avaya IP Office 9.1 and Avaya Session Border Controller for Enterprise 7.0. These Application Notes describe the configuration necessary to connect Avaya IP Office 9.1 and Avaya SBCE 7.0 to ThinkTel as shown in **Figure 1**. Test results and observations are noted in **Section 2.2**.

## 10. Additional References

### Avaya IP Office 9.1

- [1] *IP Office Documentation Catalog*, Release 9.1, Documentation number 16-604278 Issue 2.1, December 2014.
- [2] *IP Office 9.1 Platform Solution Description*, Issue 01.17, February 2016.
- [3] *Avaya IP Office 9.1 Deploying Avaya IP Office Platform IP500 V2*, Document Number 15-601042 Issue 30za, February 2016.
- [4] *Avaya IP Office 9.1 Administering Voicemail Pro*, Document number 15-601063 Issue 10m, February 2016.
- [5] *Administering Avaya IP Office Platform with Manager*, Issue 10.38, February 2016.
- [6] *Avaya IP Office 9.1 Using System Status*, Document Number 15-601758 Issue 10f, August 2015.
- [7] *Avaya IP Office 9.1 Using IP Office System Monitor*, Document Number 15-601019, Issue 06g, February 2016.
- [8] *Avaya IP Office 9.1 H.323 Telephone Installation Notes*, Document Number 15-601046, Issue 20h, December 2015.
- [9] *Avaya IP Office 9.1 SIP Extension Installation*, Issue 4a, May 2015.

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

### Avaya Session Border Controller for Enterprise

- [10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.0, Issue 1, August 2015.
- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 3, January 2016.
- [12] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*, September 2013.

Product documentation for the ThinkTel SIP Trunking Service is available from ThinkTel. See **Section 2.3** on how to contact ThinkTel.

---

**©2016 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).