



Application Notes for Telecommunications Services of Trinidad and Tobago SIP Trunking Service with Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Telecommunications Services of Trinidad and Tobago Session Initiation Protocol (SIP) Trunking Service with Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise Release 6.2.

Telecommunications Services of Trinidad and Tobago SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Telecommunications Services of Trinidad and Tobago network as an alternative to legacy analog or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

Telecommunications Services of Trinidad and Tobago is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction.....	4
2. General Test Approach and Test Results.....	4
2.1 Interoperability Compliance Testing	4
2.2 Test Results.....	5
2.3 Support.....	6
3. Reference Configuration.....	6
4. Equipment and Software Validated	8
5. Configure IP Office	9
5.1 Licensing.....	9
5.2 LAN1 Settings	10
5.3 System Telephony Settings.....	13
5.4 Twinning Calling Party Settings.....	13
5.5 Codec's settings	14
5.6 IP Route	15
5.7 Administer SIP Line	16
5.7.1 SIP Line Tab	16
5.7.2 Transport Tab.....	17
5.7.3 SIP URI Tab.....	18
5.7.4 VoIP Tab.....	19
5.8 Extension.....	20
5.9 Users	21
5.10 Incoming Call Route.....	25
5.11 Outbound Call Routing.....	27
5.11.1 Short Codes and Automatic Route Selection.....	27
5.12 Privacy/Anonymous Calls	29
5.13 Save Configuration	30
6. Configure the Avaya Session Border Controller for Enterprise.....	31
6.1 Log into the Avaya Session Border Controller for Enterprise.....	32
6.2 Global Profiles	35
6.2.1 Server Interworking Avaya.....	35
6.2.2 Server Interworking Service Provider	37
6.2.3 Routing Profiles	38
6.2.4 Server Configuration.....	40
6.2.5 Topology Hiding.....	43
6.2.6 Signaling Manipulation.....	45
6.3 Domain Policies	45
6.3.1 Create Application Rules	45
6.3.2 Media Rules	46
6.3.3 Signaling Rules	47
6.3.4 End Point Policy Groups.....	47
6.4 Device Specific Settings	49
6.4.1 Network Management.....	49
6.4.2 Media Interface	51

6.4.3 Signaling Interface	52
6.4.4 End Point Flows	53
7. Telecommunications Services of Trinidad and Tobago SIP Trunking Configuration	56
8. Verification and Troubleshooting	57
8.1 Verification Steps	57
8.2 Protocol Traces	57
8.3 IP Office System Status	57
8.4 IP Office Monitor	59
9. Conclusion	60
10. References	61
11. SIP Line Template	62
11.1 Create a New SIP Trunk from Template	62

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Telecommunications Services of Trinidad and Tobago and Avaya IP Office solution.

In the sample configuration, Avaya IP Office solution consists of Avaya IP Office (IP Office) 500v2 Release 9.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2, Avaya IP Office Softphones and Avaya Deskphones, including SIP, H.323, digital, and analog endpoints. The Avaya SBCE provides security for the Avaya IP Office solution, as well as interoperability features for the SIP trunk.

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

Telecommunications Services of Trinidad and Tobago will be referred to as **TSTT** here after.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using IP Office to connect to TSTT via the Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the feature and functionality tests listed in **Section 2.1**.

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

2.1 Interoperability Compliance Testing

To verify TSTT SIP Trunking interoperability, the following features and functionalities were exercised during the compliance testing:

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints including SIP, H.323, digital and analog at the enterprise. All incoming calls from PSTN were routed to the enterprise across the SIP Trunk from the service provider networks.
- Outgoing PSTN calls from Avaya endpoints including SIP, H.323, digital and analog telephone at the enterprise. All outgoing calls to PSTN were routed from the enterprise across the SIP trunk to the service provider networks.
- Incoming and outgoing PSTN calls to/from Avaya IP Office Softphone.
- Incoming and outgoing PSTN calls to/from IP Office Flare® Experience for Windows.

- Dialing plans including long distance, international, outbound toll-free, etc.
- Caller ID presentation and Caller ID restriction.
- Codec's G.711MU and G.729A (For Codec G.729A Test Results refer to **Section 2.2**).
- Proper early media transmissions using G.711MU codec.
- DTMF tone transmissions per RFC 2833.
- Voicemail navigation for incoming and outgoing calls.
- Telephony features such as hold and resume, call transfer, call forward and conferencing.
- Off-net call forwards and transfers.
- Mobility Twinning of incoming calls to mobile phones.
- Response to incomplete call attempts and trunk errors.

2.2 Test Results

Interoperability testing with TSTT with was successfully completed with the exception of observations/limitations described below:

- **SIP REFER** – On PSTN calls to or from IP Office that are transferred back to the PSTN on the SIP trunk, TSTT responds with a “202 Accepted” to the REFER message sent by IP Office, but the call between the two PSTN endpoints drops, the PSTN phone receives re-order tone. REFER needs to be disabled in IP Office for the Call Transfer to complete successfully, otherwise the call transfer will fail. The implication is that IP Office SIP trunk channels are not released after the call transfer is completed, two (2) trunk channels will remain connected/busy for the duration of the call..
- **T.38 or G.711 Pass-Through fax calls** – With IP Office **Fax Transport Support** set as **T.38** or **T.38 Fallback** on the **SIP Line/VoIP**, on outbound calls (IPO→PSTN) TSTT did not send a re-INVITE to switch from G.711 to T.38. TSTT's recommendation is **not** to use T.38 fax transport, only G.711 fax Pass-through. With IP Office **Fax Transport Support** set as **G.711** on the **SIP Line/VoIP**, fax calls were unsuccessful, thus **T.38 or G.711** fax transports **are not** recommended for this solution.
- **Codec G.729A** – TSTT supports codec's G.711MU and G.729A, but during the testing, TSTT was rejecting calls with G.729A codec offer with **488 Invalid Media Type**. This issue is under investigation by TSTT.
- **Direct Media** – With Direct Media enabled in IP office, when calling IVR systems (or any recorded messaging system) from IP Office, a noticeable clipping of the recorded message is heard when IP Office sends the re-Invite to establish the direct media connection to the IP Phone. Testing was done with Direct Media disabled in IP Office. This issue is being investigated by Avaya.
- **Outbound Calling Party Number (CPN) Blocking** – On outbound calls from the enterprise to the PSTN with Calling Party Number Block (CPN) enabled on the IP Office station, TSTT responds with a **503 Service Unavailable**.
- **Call Forward Off-Net** – When inbound calls from the PSTN to IP Office are forwarded back out to another PSTN endpoint, TSTT responds with **503 Service Unavailable**, the reason is that TSTT is looking at the **Contact Header** instead of the **Diversion Header**. The work around for this issue is to set the **Send Caller ID** field under **SIP Line** to **None** instead **Diversion Header**.

2.3 Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on TSTT SIP Trunking Service visit <http://tstt.co.tt/>

3. Reference Configuration

Figure 1 below illustrates the test configuration. It shows an enterprise site connected to the TSTT network through the public internet.

For confidentiality and privacy purposes, actual public IP addresses and PSTN routable phone numbers (DIDs) used during the compliance testing have been replaced with fictitious IP addresses and PSTN routable phone numbers throughout the Application Notes.

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

- Avaya IP Office 500v2.
- Avaya Session Border Controller for Enterprise.
- Avaya Voicemail Pro for IP Office.
- Avaya 9600 Series H.323 IP Telephones.
- Avaya 11x0 Series SIP IP Telephones.
- Avaya IP Office Softphone.
- IP Office Flare® Experience for Windows.
- Avaya 1408 Digital Telephones.
- Avaya 9508 Digital Telephones.

Located at the enterprise site is Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codec's. The IP Office has LAN1 port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to TSTT networks via the public internet.

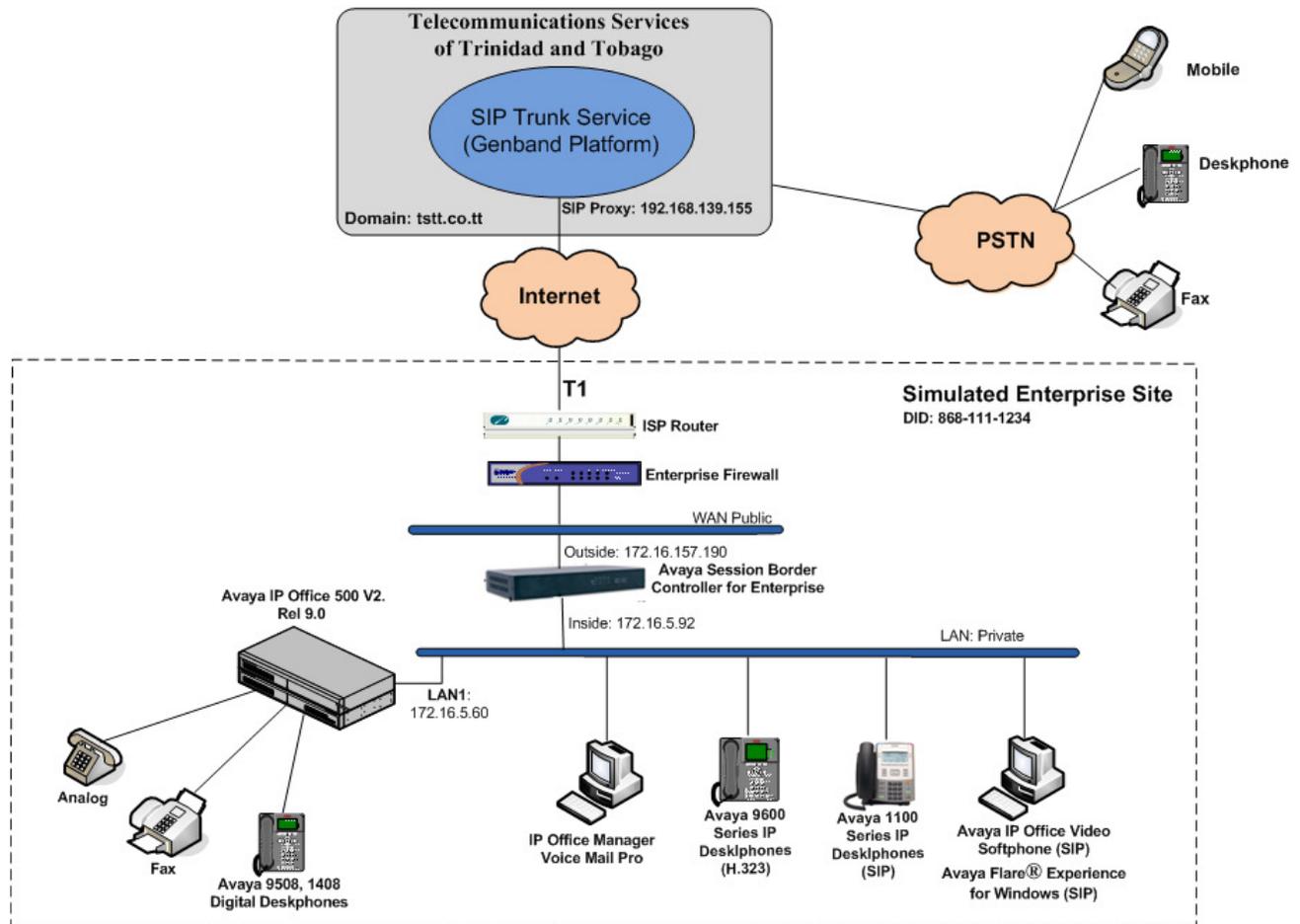


Figure 1: Avaya IP Telephony Network Connecting to TSTT SIP Trunking Service.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to TSTT. The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network. Since Trinidad and Tobago is a country member of the North American Numbering Plan (NANP), the users dialed 10 digits for local calls, including the area code, and 11 (1 + 10) digits for other calls between the NANP.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the enterprise such as a 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 the enterprise must be allowed to pass through these devices.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment/Software	Release/Version
Avaya IP Office 500v2	9.0 (829)
Avaya IP Office DIG DCPx16 V2	9.0 (829)
Avaya IP Office Manager	9.0 (829)
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2 (6.2.0.Q48)
Avaya Voicemail Pro for IP Office	9.0 Built 311
Avaya 9620 IP Telephone (H.323)	Avaya one-X® Deskphone Edition S3.2
Avaya 1140 IP Telephone (SIP)	SIP1140 Ver. 04.03.18.00
Avaya IP Office Softphone	3.2.3.49 68975
IP Office Flare® Experience for Windows	1.1.4.23
Avaya Digital Telephones 1408	32
Avaya Digital Telephones 9508	0.45

Telecommunications Services of Trinidad and Tobago SIP Trunk Service	
Equipment/Software	Release/Version
Genband Softswitch	CVM13

Testing was performed with IP Office 500v2 R9.0, but it also applies to IP Office Server Edition R9.0. Note that IP Office Server Edition requires an Expansion IP Office 500 v2 R9.0 to support analog or digital endpoints or trunks.

5. Configure IP Office

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

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

5.1 Licensing

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

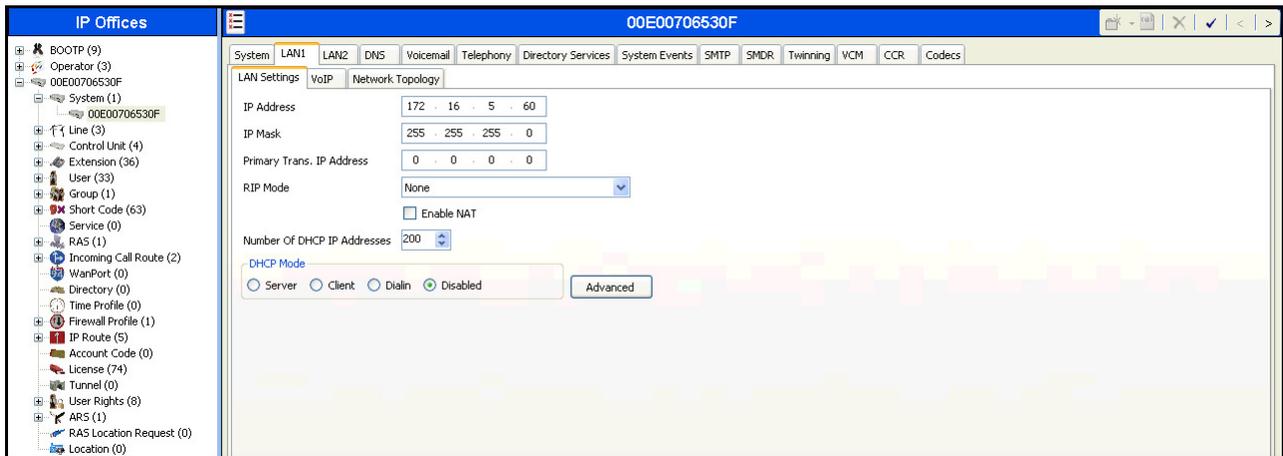
To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License** in the Navigation pane and **SIP Trunk Channels** in the Group pane. Confirm that there is a valid license with sufficient “Instances” (trunk channels) in the Details pane. Note that the actual License Keys in the screen below were edited for security purposes.

Feature	License Key	Instances	Status	Expiry Date	Source
VMPro VB Script	AnDK	255	Valid	Never	ADI Nodal
VMPro Recordings Administrators	j4@	255	Valid	Never	ADI Nodal
VMPro Outlook Interface	ZySu	255	Valid	Never	ADI Nodal
VMPro TTS (Scansoft)	hq9X	255	Valid	Never	ADI Nodal
VMPro TTS (Generic)	nIcm	255	Valid	Never	ADI Nodal
Conferencing Center	CAH+	255	Obsolete	Never	ADI Nodal
Small Office Edition VCM (channels)	2K07	255	Obsolete	Never	ADI Nodal
Small Office Edition WiFi	eAWA	255	Obsolete	Never	ADI Nodal
IPSec Tunneling	MIKcr	255	Valid	Never	ADI Nodal
Proactive Reporting	ttDpE	255	Valid	Never	ADI Nodal
Report Viewer	Tvtc7	255	Valid	Never	ADI Nodal
Mobility Features	0IClu	255	Obsolete	Never	ADI Nodal
Advanced Small Community Networking	DaQJ	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	TS98I	255	Valid	Never	ADI Nodal
IP500 Upgrade Standard to Profession...	QaHqS	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	JaHL	4	Valid	Never	ADI Nodal
SIP Trunk Channels	l3CO	255	Valid	Never	ADI Nodal
VPN IP Extensions	@qm	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional chan...	2TXC	255	Valid	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	hVIRx	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Standard E...	4AOC	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Profession...	dlyY	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Stand...	d95F	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Profes...	LHFz	255	Valid	Never	ADI Nodal
UMS Web Services	pGcS	255	Valid	Never	ADI Nodal
Customer Service Agent	j10xh	255	Valid	Never	ADI Nodal
1600 Series Phones	UaKn	255	Valid	Never	ADI Nodal
Third Party API	Fan7c	255	Valid	Never	ADI Nodal
Software Upgrade 255	oh1W	1	Valid	Never	ADI Nodal
one-X Portal for IP Office	8w@C	255	Valid	Never	ADI Nodal
Avaya IP endpoints	JTBvc	255	Valid	Never	ADI Nodal
Customer Service Supervisor	oh2N	255	Valid	Never	ADI Nodal
Essential Edition Additional Voicemail ...	DveF	255	Valid	Never	ADI Nodal
Teleworker	tUIRq	255	Valid	Never	ADI Nodal
Mobile Worker	tGu@	255	Valid	Never	ADI Nodal
Power User	H6x@	255	Valid	Never	ADI Nodal

5.2 LAN1 Settings

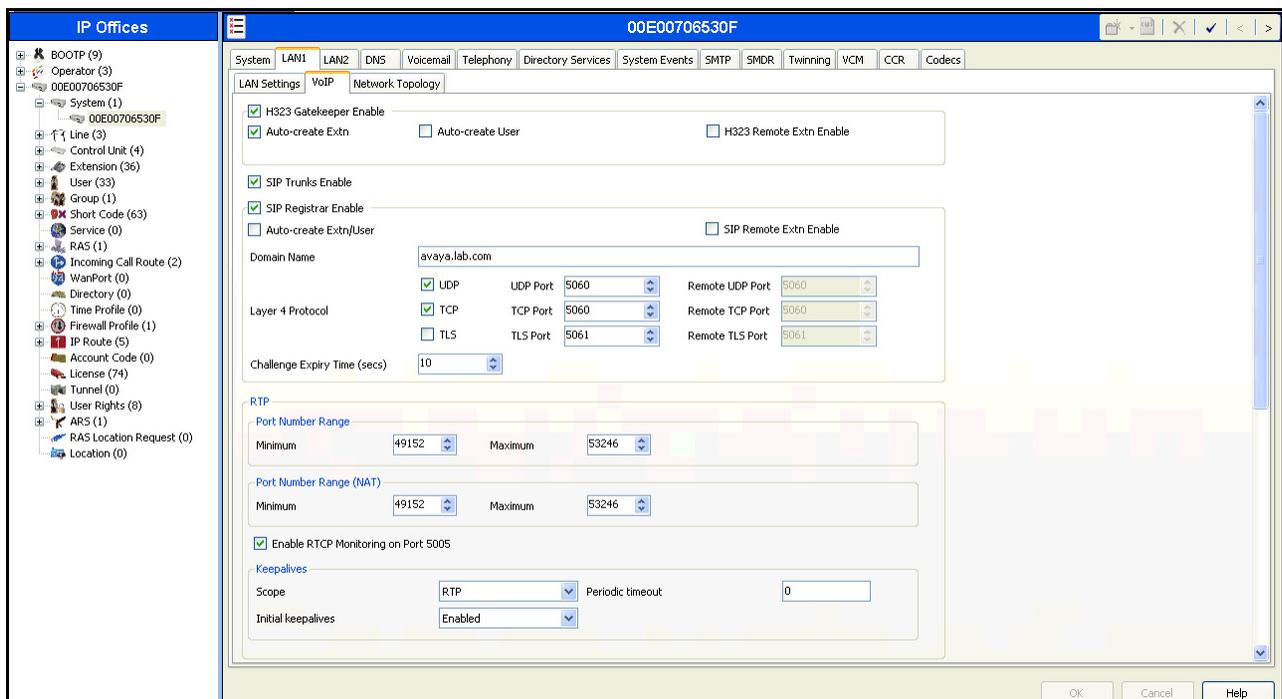
In the sample configuration, the MAC address **00E00706530F** was used as the system name and the **LAN** port connects to the inside interface of the Avaya SBCE across the enterprise LAN (private) network. The outside interface of the Avaya SBCE connects to TSTT networks via the public internet. The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

- Set the **IP Address** field to the LAN IP address, e.g. **172.16.5.60**.
- Set the **IP Mask** field to the subnet mask of the public network, e.g. **255.255.255.0**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown).



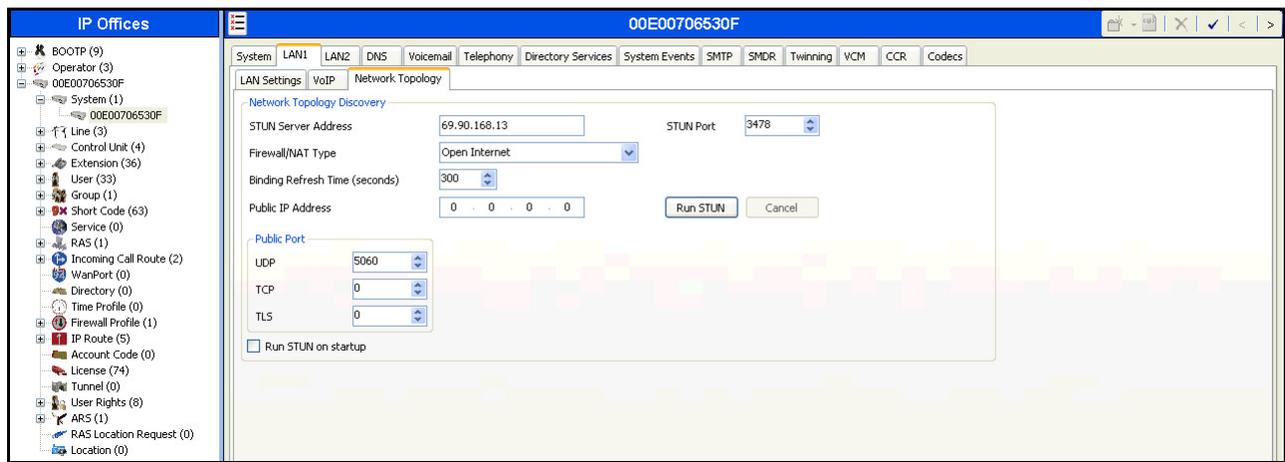
The **VoIP** tab as shown in the screenshot below was configured with following settings.

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to TSTT.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name under **Domain Name**.
- Verify the **UDP Port** and **TCP Port** numbers under **Layer 4 Protocol** are set to **5060**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP**, and **Initial keepalives** to **Enabled**. This will cause the IP Office to send RTP keepalive packets at the beginning of the calls, to avoid problems of media deadlock that can occur with certain types of forwarded calls that are routed from the IP Office back to the network, over the same SIP trunk.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown).



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

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even the default STUN settings are populated but they will not be used.
- Set the **Binding Refresh Time (seconds)** to a desired value, the value of **300 (or every 5 minutes)** was used during the compliance testing. This value is used to determine the **frequency** that IP Office will send OPTIONS heartbeat to the service provider.
- Leave the **Public IP Address** as **0.0.0.0**
- Set the **Public Port** to **5060 for UDP**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown).

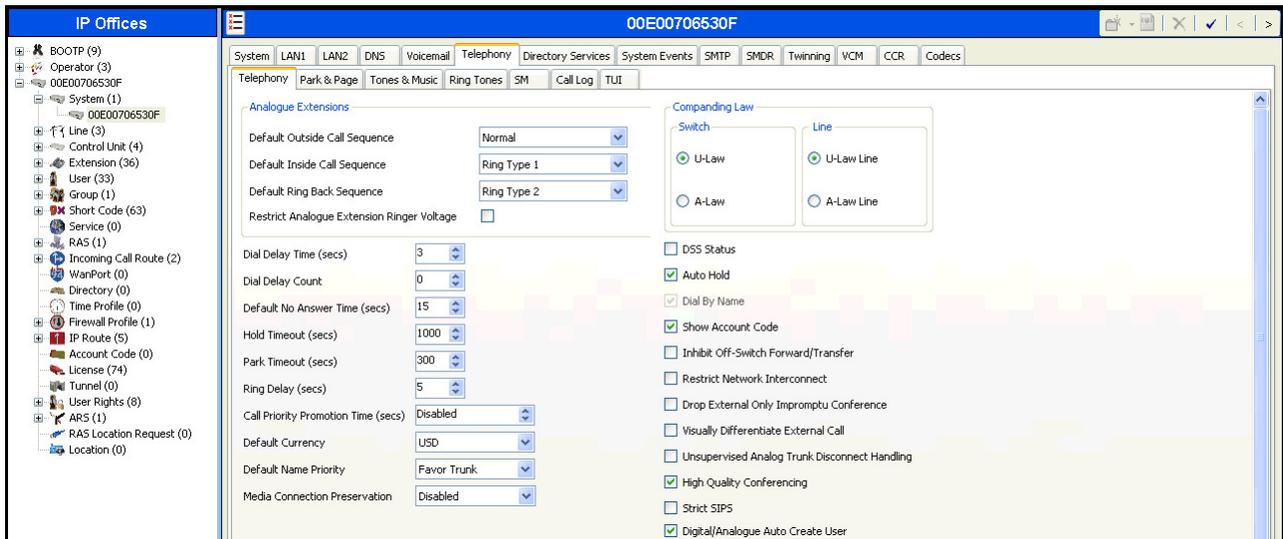


In the compliance test, the **LAN1** interface was used to connect Avaya IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.3 System Telephony Settings

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

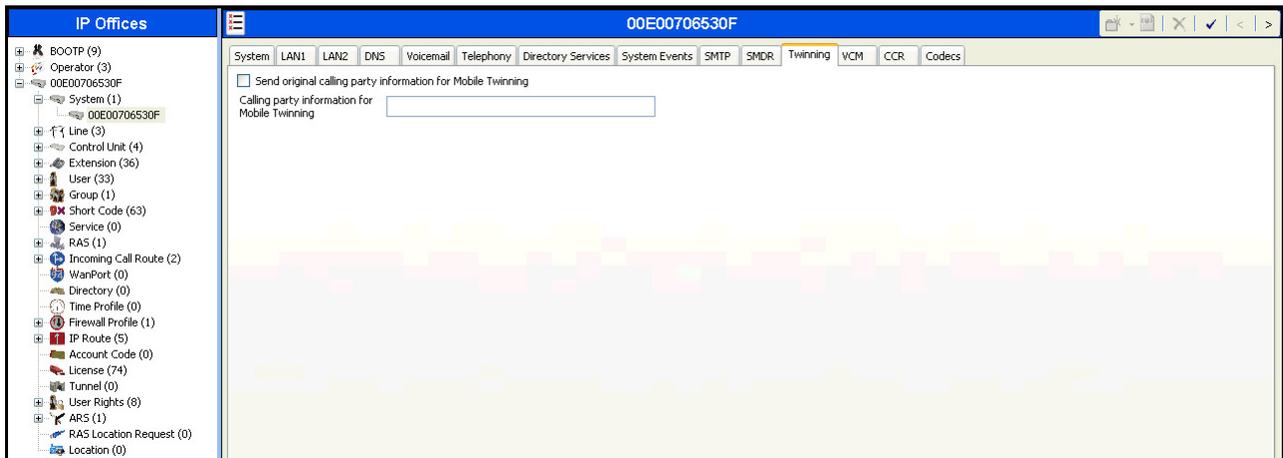
- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer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



5.4 Twinning Calling Party Settings

Navigate to the **Twinning** tab on the Details Pane, configure the following parameters:

- Uncheck the **Send original calling party information for Mobile Twinning** box. This will allow the Caller ID for Twinning to be controlled by the setting on the SIP Line (**Section 5.7**). This setting also impacts the Caller ID for call forwarding.
- Click OK to commit (not shown).

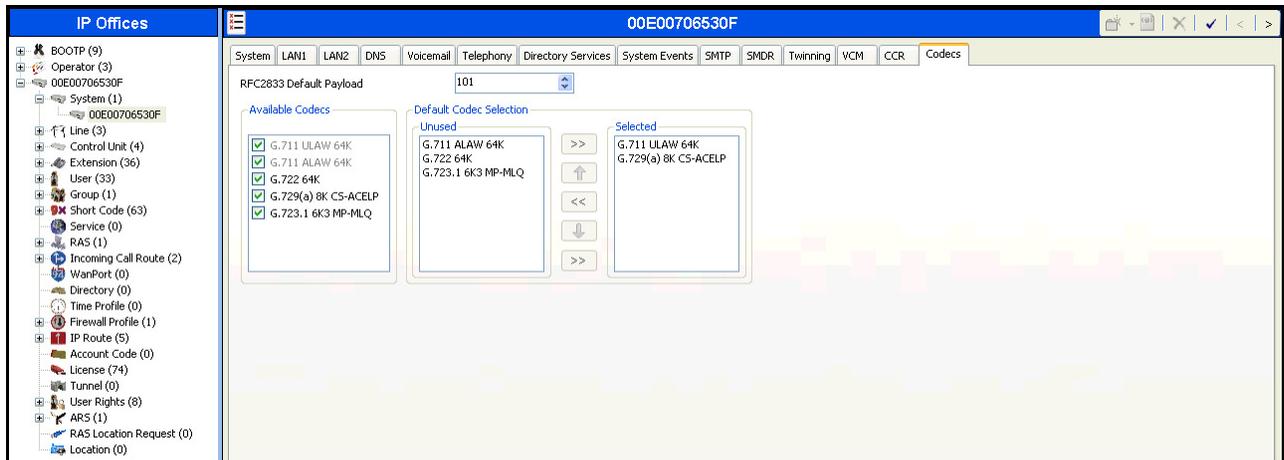


5.5 Codec's settings

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

- Select the **Codecs**.
- Click OK to commit (not shown).

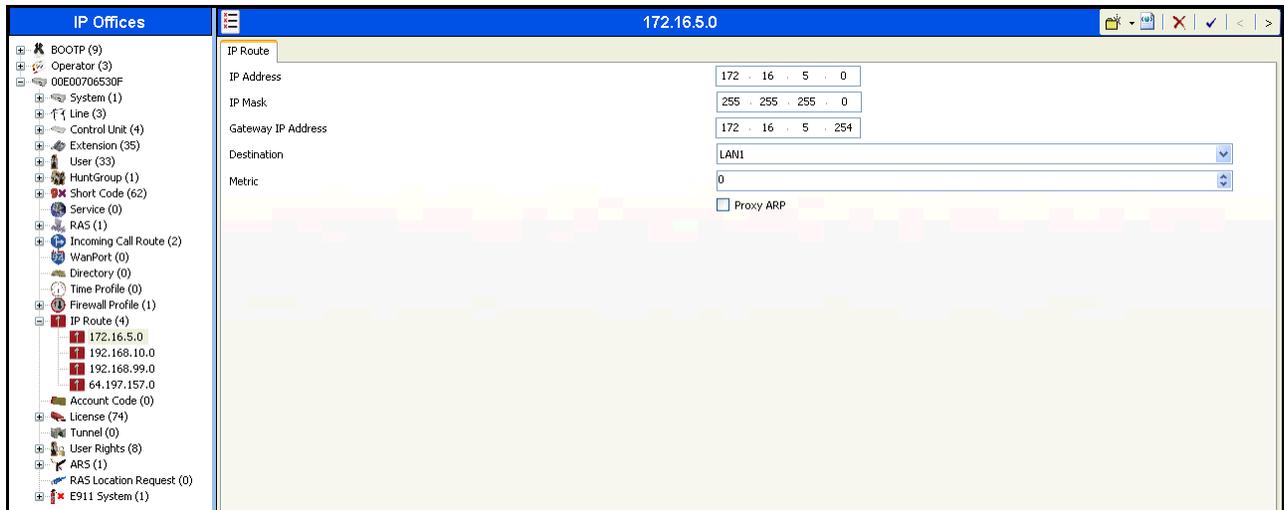
The **Codec's** settings are shown in the screenshot below with G.711ULAW and G.729(a) were selected in prioritized order. During the compliance testing, only codec G.711ULAW was tested (For Codec G.729A Test Results refer to **Section 2.2**).



5.6 IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to reach the subnet where the SIP proxy is located on the TSTT network. On the left navigation pane, right-click on **IP Route** and select **New**.

- Set the **IP Address** and **IP Mask** of LAN1 connecting to the Avaya SBCE for SIP and RTP traffics to TSTT.
- Set **Gateway IP Address** to the IP Address of the router used to reach the external network.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click OK to commit (not shown).



5.7 Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the TSTT SIP Trunk Service. To create a SIP line, begin by navigating to **Line** in the Navigation Pane. Right-click and select **New**→ **SIP Line**.

5.7.1 SIP Line Tab

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

- Leave the **ITSP Domain Name** blank.
- Verify that **In Service** box is checked.
- Verify that **Check OOS** box is checked. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Call Routing Method** is set to **Request URI**.
- Set **Send Caller ID** to **None**.
- Uncheck the **REFER support** box. IP Office will not send REFER messages for calls that are transferred back to the PSTN. See **Section 2.2** for more information.
- Set **Method for Session Refresh** to **Auto**.
- Set **Session Timer (Seconds)** to **On Demand**.
- Set **Media Connection Preservation** to **Disabled**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

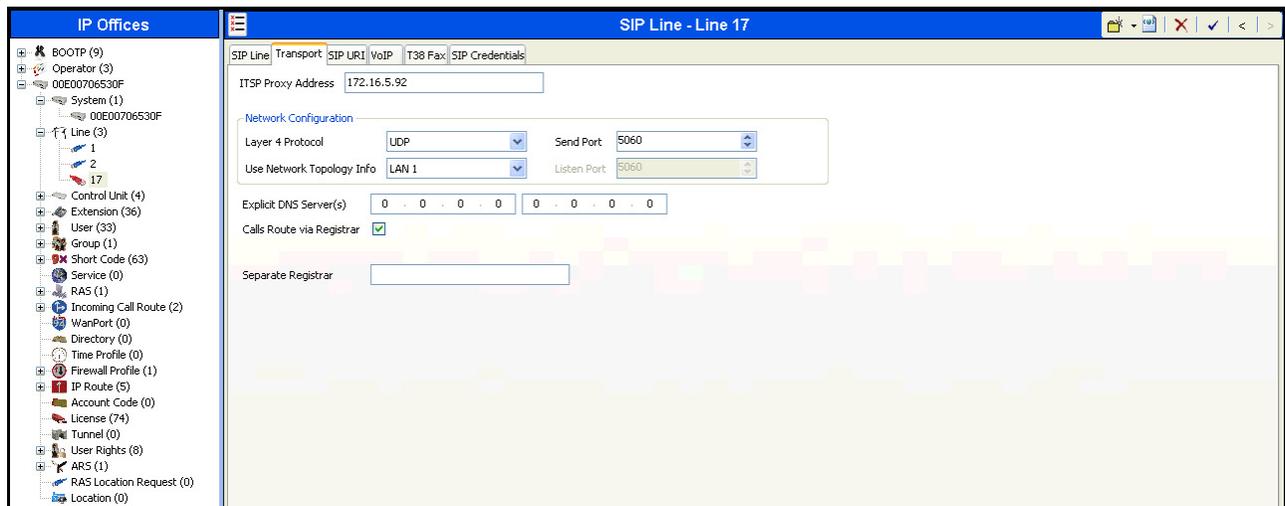
The screenshot displays the configuration window for a SIP Line in Avaya IP Office. The left pane shows the system hierarchy, and the right pane contains the following configuration details:

Field	Value
Line Number	17
ITSP Domain Name	
Prefix	
National Prefix	0
Country Code	
International Prefix	00
Send Caller ID	None
Association Method	By Source IP address
In Service	<input checked="" type="checkbox"/>
URI Type	SIP
Check OOS	<input checked="" type="checkbox"/>
Call Routing Method	Request URI
Originator number for forwarded and twinning calls	
Name Priority	System Default
Caller ID from From header	<input type="checkbox"/>
Send From In Clear	<input type="checkbox"/>
User-Agent and Server Headers	
Service Busy Response	486 - Busy Here
Action on CAC Location Limit	Allow Voicemail
REFER Support	<input type="checkbox"/>
Incoming	Always
Outgoing	Always
Method for Session Refresh	Auto
Session Timer (seconds)	On Demand
Media Connection Preservation	Disabled

5.7.2 Transport Tab

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

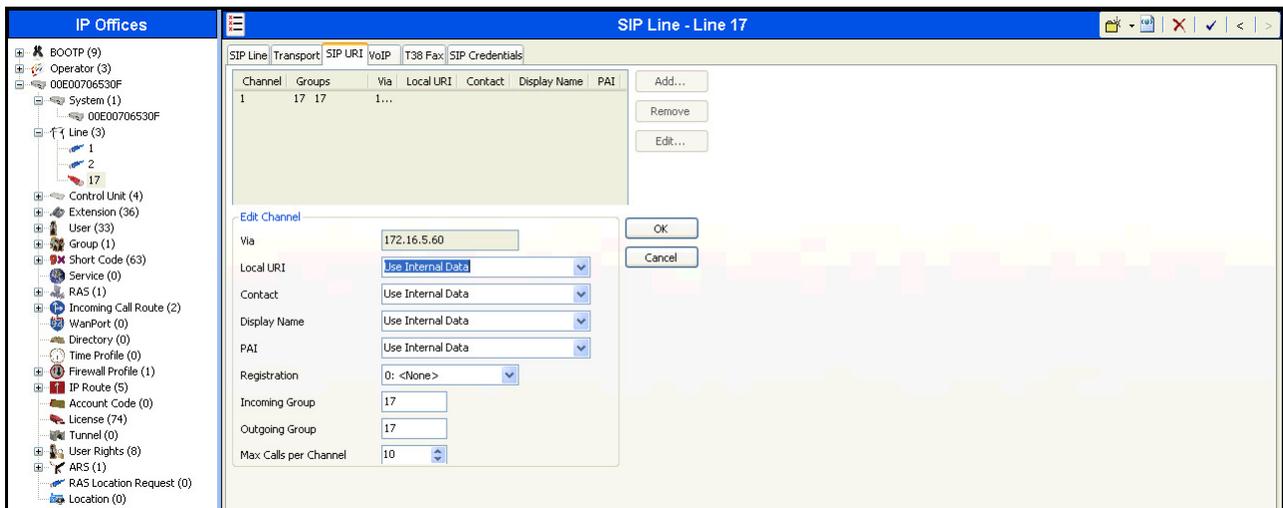
- Set the **ITSP Proxy Address** was set to the inside IP Address of the Avaya SBCE **172.16.5.92** as shown in **Figure 1**.
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



5.7.3 SIP URI Tab

A SIP URI entry needs to be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab, and then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the example screen below, a previously configured entry was edited. For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

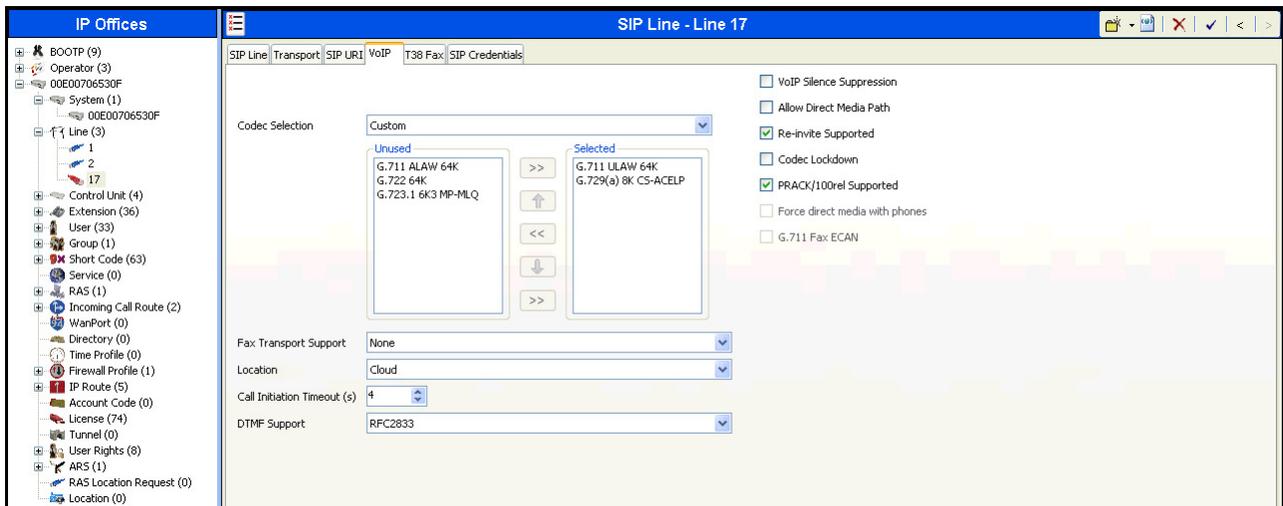
- Set **Local URI, Contact, Display Name and PAI** to **Use Internal Data**. This setting allows calls on this line whose SIP URI match the number set in the **SIP** tab of any User as shown in **Section 5.9**.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit (not shown).



5.7.4 VoIP Tab

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

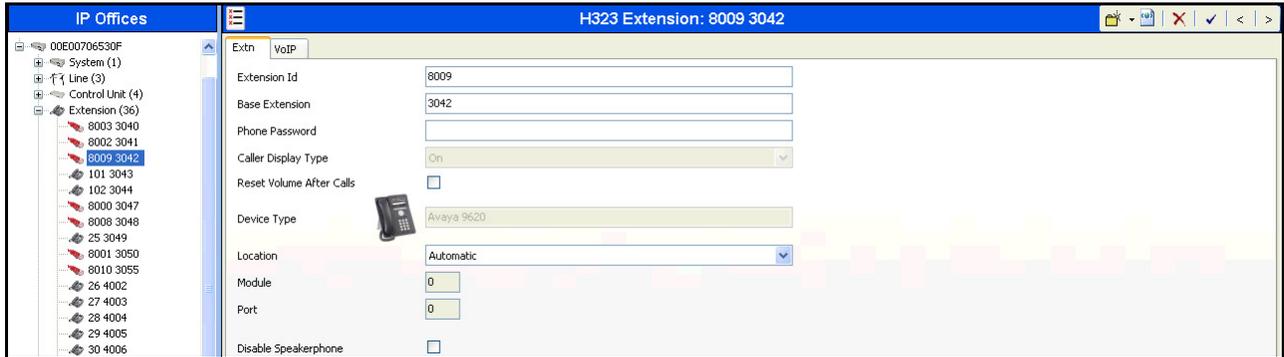
- In the sample configuration, the **Codec Selection** was configured using the **Custom** option, allowing an explicit ordered list of codec's to be specified. The buttons allow setting the specific order of preference for the codec's to be used on the line, as shown. TSTT supports codec's G.711MU and G.729A, during the compliance testing, only codec G.711ULAW was tested (For Codec G.729A Test Results refer to **Section 2.2**).
- Set **Fax Transport Support** to **None**. **T.38** or **G.711** fax transports **are not** recommended for this solution, as described in **Section 2.2**.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Verify that **Allow Direct Media Path** is unchecked. Testing was done with Direct Media disabled (Refer to **Section 2.2**).
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check the **PRACK/100rel Supported** box, to advertise the support for reliable provisional responses and Early Media to TSTT.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



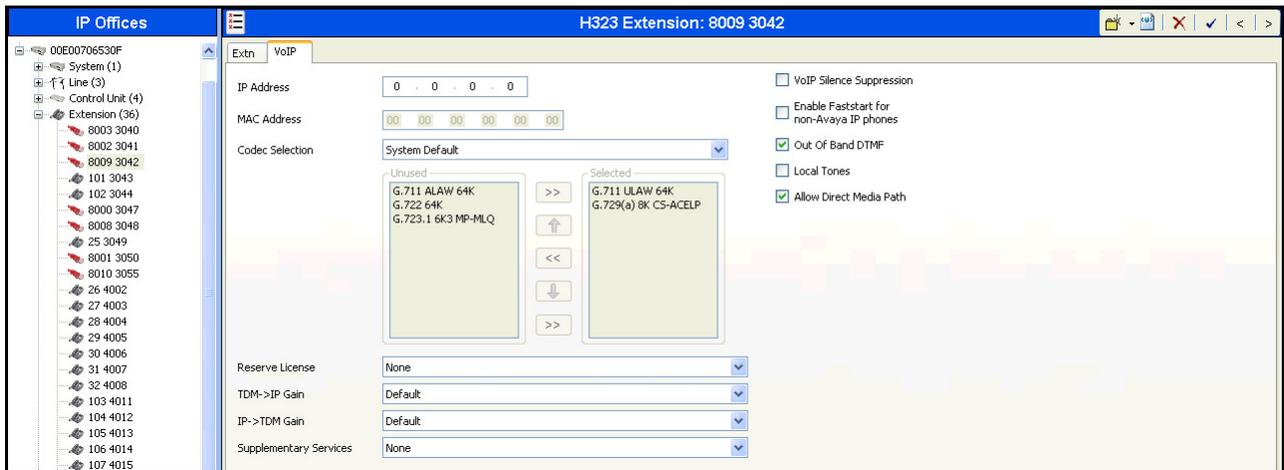
5.8 Extension

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

Select the **Extn** tab. Following is an example of extension 3042; this extension corresponds to an H.323 extension.



Select the **VOIP** tab. Use default values on VoIP tab. Following is an example for Extension 3042; this extension corresponds to an H.323 extension.



5.9 Users

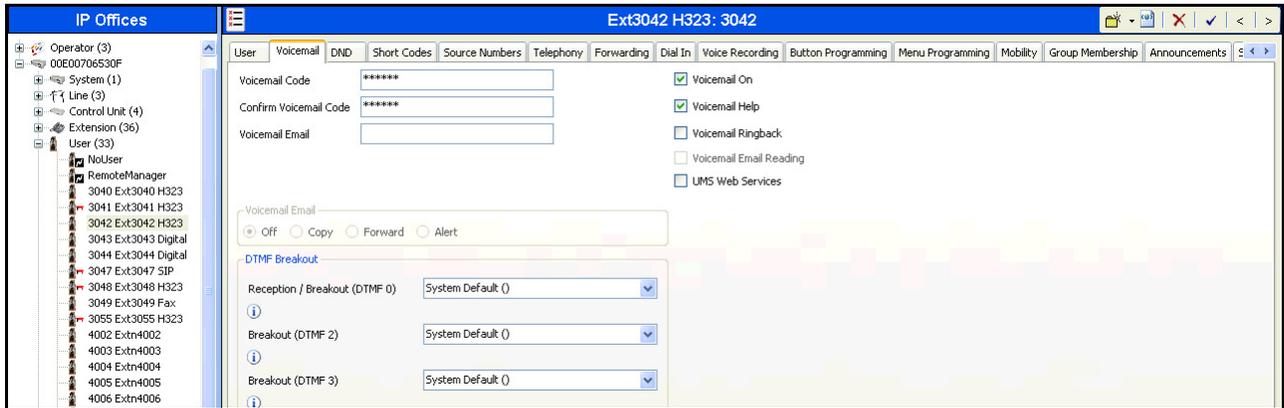
Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.7**. To configure these settings, first navigate to **User** in the left Navigation Pane, and then select the name of the user to be modified in the center Group Pane. In the example below, the name of the user is **Ext3042 H323**.

The screenshot shows the Avaya IP Office user configuration interface. The left navigation pane is expanded to 'User (33)', and '3042 Ext3042 H323' is selected. The main pane displays the configuration for this user. The 'Name' field is 'Ext3042 H323', 'Password' and 'Confirm Password' are '****', 'Account Status' is 'Enabled', 'Full Name' is 'Ext3042 H323', 'Extension' is '3042', 'Email Address' is empty, 'Locale' is empty, 'Priority' is '5', 'System Phone Rights' is 'None', and 'Profile' is 'Basic User'. Under 'Profile', several options are listed with checkboxes: 'Receptionist' (unchecked), 'Enable Softphone' (unchecked), 'Enable one-X Portal Services' (unchecked), 'Enable one-X TeleCommuter' (unchecked), 'Enable Remote Worker' (unchecked), 'Enable Flare' (unchecked), 'Enable Mobile VoIP Client' (unchecked), 'Send Mobility Email' (unchecked), and 'Ex Directory' (unchecked). The 'Device Type' is 'Avaya 9620' and 'User Rights view' is 'User data'.

In the example below, the name of the user is “Ext3047 SIP”. This is an Avaya IP Office Softphone user, set the Profile to **Teleworker User** and check **Enable Softphone**.

The screenshot shows the Avaya IP Office user configuration interface for 'Ext3047 SIP: 3047'. The left navigation pane is expanded to 'User (33)', and '3047 Ext3047 SIP' is selected. The main pane displays the configuration for this user. The 'Name' field is 'Ext3047 SIP', 'Password' and 'Confirm Password' are '****', 'Account Status' is 'Enabled', 'Full Name' is 'Ext3047 SIP', 'Extension' is '3047', 'Email Address' is empty, 'Locale' is empty, 'Priority' is '5', 'System Phone Rights' is 'None', and 'Profile' is 'Teleworker User'. Under 'Profile', several options are listed with checkboxes: 'Receptionist' (unchecked), 'Enable Softphone' (checked), 'Enable one-X Portal Services' (checked), 'Enable one-X TeleCommuter' (checked), 'Enable Remote Worker' (unchecked), 'Enable Flare' (unchecked), 'Enable Mobile VoIP Client' (unchecked), 'Send Mobility Email' (unchecked), and 'Ex Directory' (unchecked). The 'Device Type' is 'Unknown SIP device' and 'User Rights view' is 'User data'.

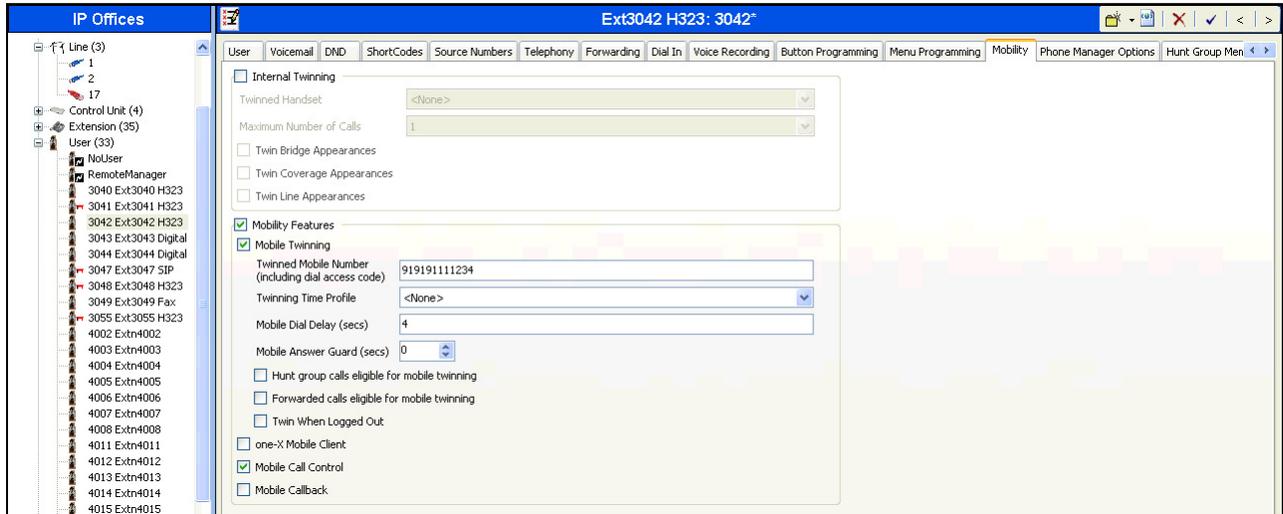
Select the **Voice Mail** tab. The following screen shows the **Voicemail** tab for the user with extension 3042. The **Voicemail On** box is checked. Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters. In the verification of these Application Notes, incoming calls from TSTT SIP Trunk to this user were redirected to Voicemail Pro after no answer. Voicemail messages were recorded and retrieved successfully. Voice mail navigation and retrieval were performed locally and from PSTN telephones to test DTMF using RFC 2833.



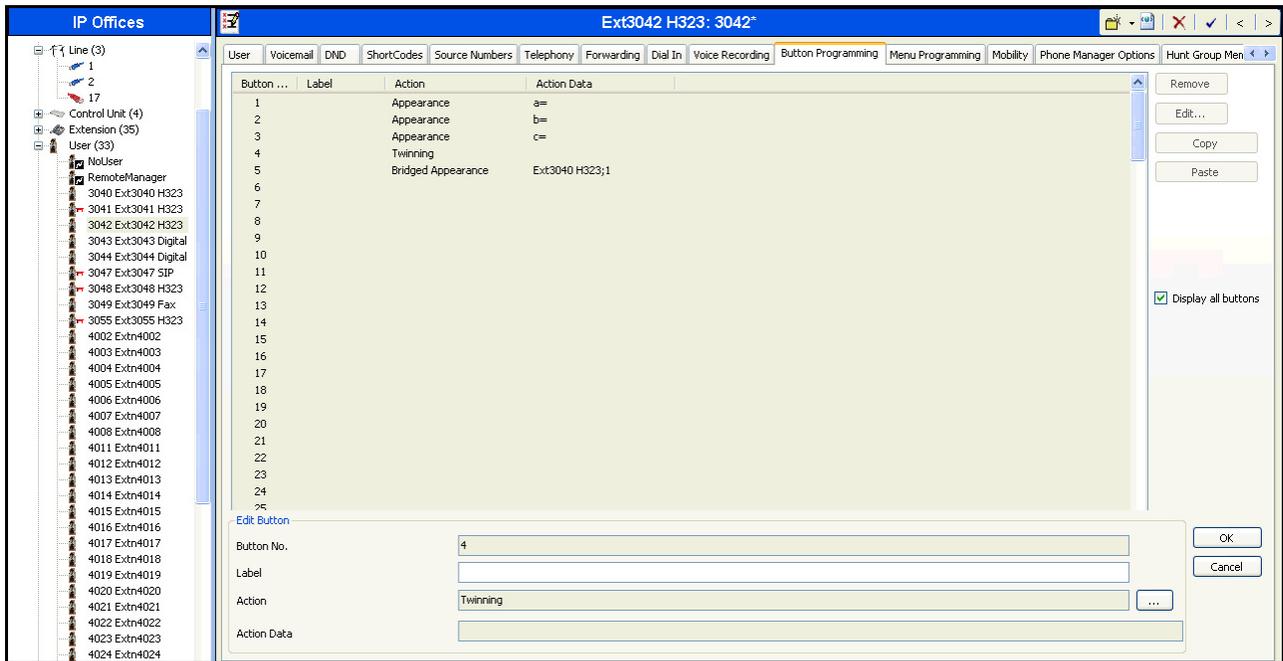
Select the **Telephony** tab, then **Call Settings** tab as shown below. Check the **Call Waiting On** box to allow an Avaya IP Office phone logged in as this extension to have multiple call appearances. Note: **Call Waiting On** is necessary for call transfer.



Select the **Mobility** tab. In the sample configuration user 3042 was one of the users configured to test the Mobile Twinning feature. The following screen shows the **Mobility** tab for User 3042. The **Mobility Features** and **Mobile Twinning** boxes are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned telephone, in this case **91919111234**. Other options can be set according to customer requirements.



To program a key on the telephone to turn Mobil Twinning on and off, select the **Button Programming** tab on the user, then select the button to program to turn Mobil Twinning on and off, click on **Edit → Emulation → Twinning**. In the sample below, button **4** was programmed to turn Mobil Twinning on and off on user 3042.



Select the **SIP** tab, the values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls. In addition, these settings are used to match against the SIP URI of incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.7**). The example below shows the settings for user “Ext3042 H323”. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by TSTT. In the example, DID number **1111234** was used. Only the last seven digits of the DID were assigned since TSTT only sends seven digits without the area code (868). The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

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



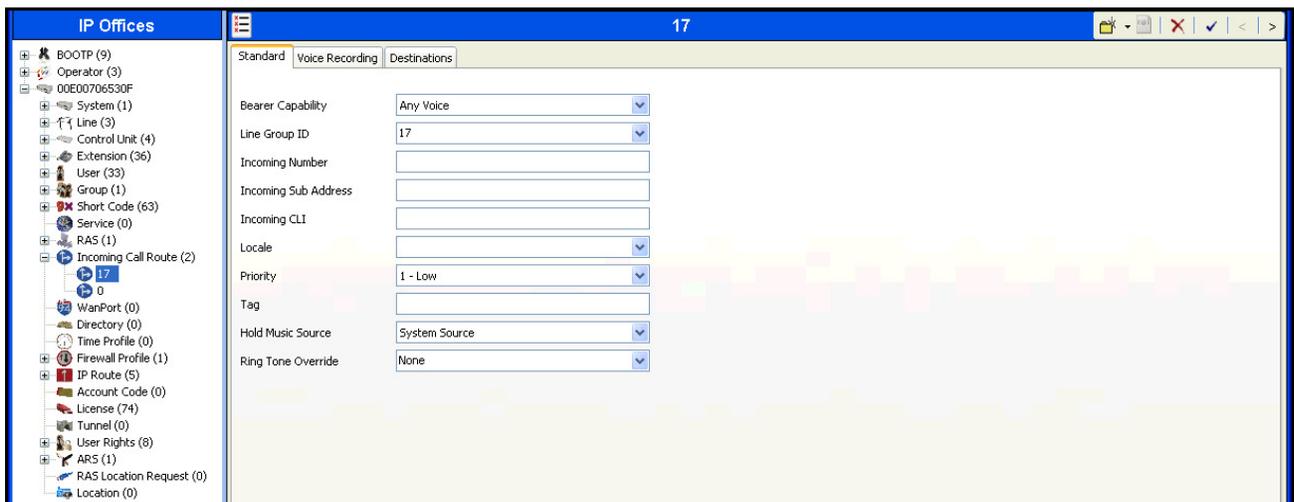
5.10 Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc, within the IP Office system. Incoming call routes should be defined for each DID number assigned by the service provider.

In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** and **SIP URI (Section 5.7)** and the users **SIP Name** and **Contact**, already populated with the assigned TSTT DID numbers (**Section 5.9**)

From the left Navigation Pane, right-click on **Incoming Call Route** and select **New**. On the Details Pane, under the **Standard** tab, set the parameters as show bellow:

- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.7**.
- Default values may be used for all other parameters.



- Under the **Destinations** tab, enter “.” for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User**, which matches the number present on the user part of the incoming Request URI.

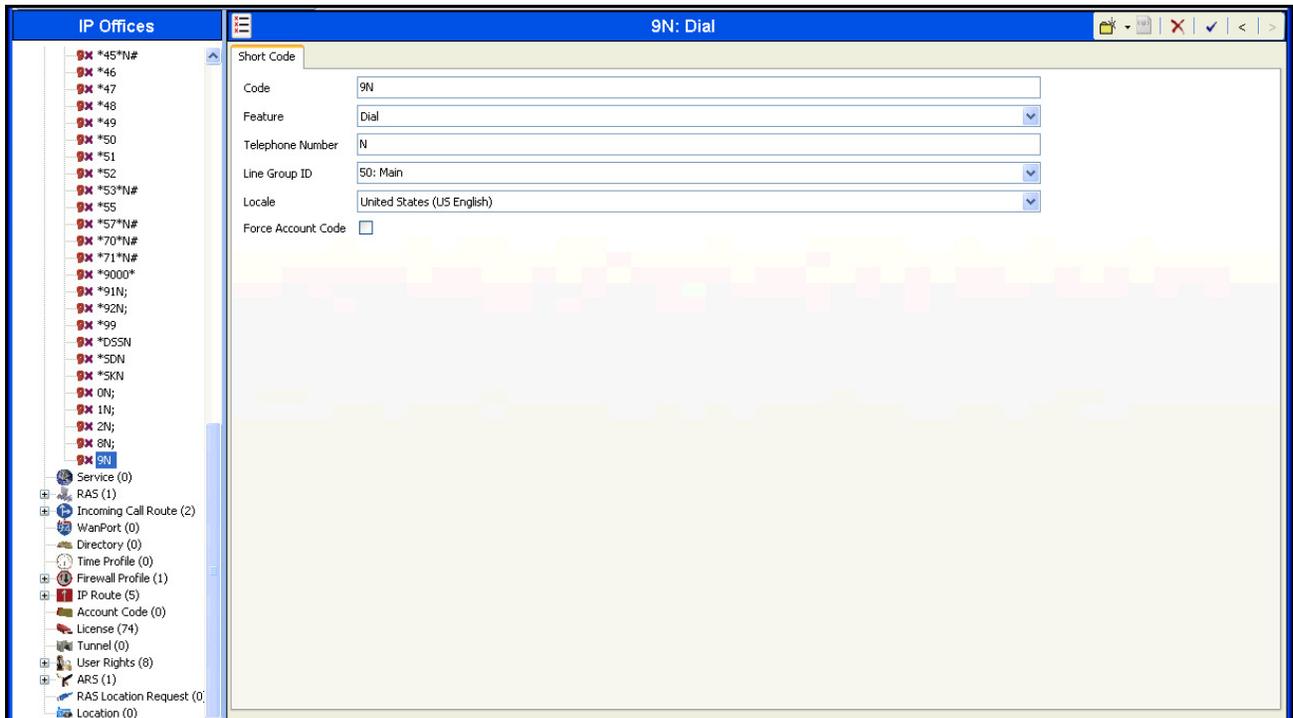


5.11 Outbound Call Routing

For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. While detailed coverage of ARS is beyond the scope of these Application Notes and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance test

5.11.1 Short Codes and Automatic Route Selection

To create a short code to be used for ARS, right-click on **Short Code** in the Navigation Pane and select **New**. The screen below shows the short code **9N** created. Note that the semi-colon is not used here. In this case, when the Avaya IP Office user dials 9 plus any number **N**, instead of being directed to a specific Line Group ID, the call is directed to **Line Group 50: Main**, which is configurable via ARS.



The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **Xs** used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first digit on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office. The example below shows that for local calls, the user dialed 9, then 10 digit numbers starting with an 8. For calls to other area codes in the North American Numbering Plan, the user dialed 9, followed by 11 digits, starting with a 1.

The screenshot shows the configuration for an ARS (Automatic Route Selection) route named 'Main' with ARS Route Id 50. The configuration includes various settings such as 'Secondary Dial tone' set to 'SystemTone', 'Check User Call Barring' checked, and 'In Service' checked. The 'Time Profile' is set to '<None>'. Below these settings is a table of ARS entries:

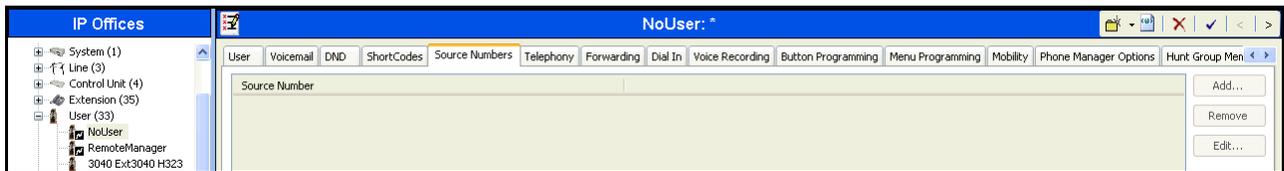
Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0XXXXXXXXXX	0N	Dial	17
6XXXXXX	6N	Dial	17
8XXXXXXXXXX	8N	Dial	17
1XXXXXXXXXX	1N	Dial	17

Additional settings include 'Alternate Route Priority Level' set to 3 and 'Alternate Route Wait Time' set to 30. The 'Alternate Route' is set to '<None>'. The left sidebar shows the 'IP Offices' tree with 'ARS (1)' expanded to show '50: Main'.

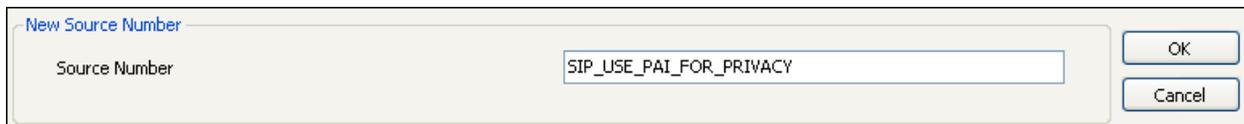
5.12 Privacy/Anonymous Calls

For outbound calls with privacy (anonymous) enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with “restricted” and “anonymous” respectively. Avaya IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity (PAI) header to pass the actual calling party information for authentication and billing. By default, Avaya IP Office will use PPI for privacy. For the compliance test, PAI was used for the purposes of privacy.

To configure Avaya IP Office to use PAI for privacy calls, navigate to **User** → **NoUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



At the bottom of the Details Pane, the **Source Number** field will appear. Enter **SIP_USE_PA1_FOR_PRIVACY**. Click **OK**.



The **SIP_USE_PA1_FOR_PRIVACY** parameter will appear in the list of Source Numbers as shown below.

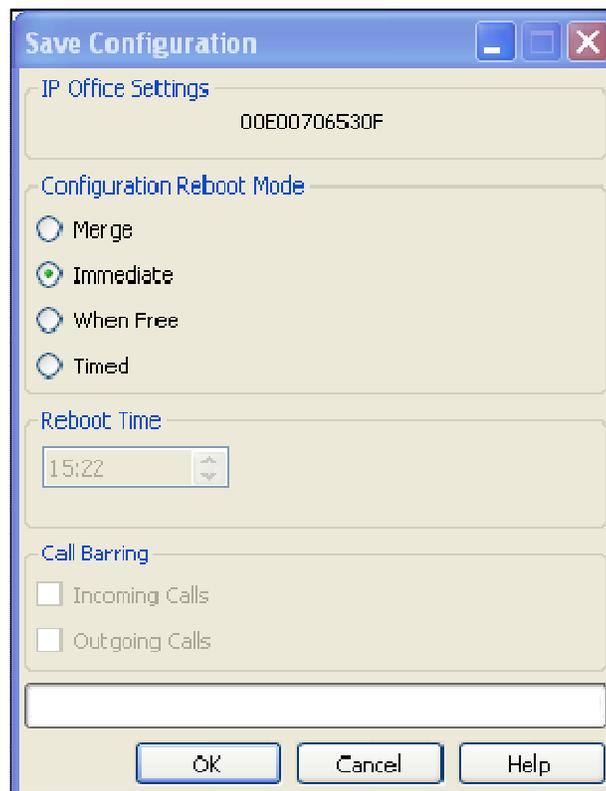


5.13 Save Configuration

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

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

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



The image shows a 'Save Configuration' dialog box with a blue title bar and standard window controls. It contains several sections: 'IP Office Settings' with a text field containing '00E00706530F'; 'Configuration Reboot Mode' with four radio buttons: 'Merge', 'Immediate' (selected), 'When Free', and 'Timed'; 'Reboot Time' with a spinner box showing '15:22'; and 'Call Barring' with two checkboxes: 'Incoming Calls' and 'Outgoing Calls', both of which are unchecked. At the bottom, there is an empty text field and three buttons: 'OK', 'Cancel', and 'Help'.

6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see **References** [6], [7] and [8] in **Section 10**.

The configuration of the Avaya SBCE covers two major components, the Trunk Server for the service provider and Call Server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration was defined using the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - TSTT:

- Global Profiles:
 - URI Groups
 - Routing
 - Topology Hiding
 - Server Interworking
 - Signaling Manipulation
 - Server Configuration
- Domain Policies:
 - Application Rules
 - Media Rules
 - Signaling Rules
 - Endpoint Policy Group
 - Session Policy
- Device Specific Settings:
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows → Server Flows
 - Session Flows

Call Server configuration elements for the enterprise - IP Office:

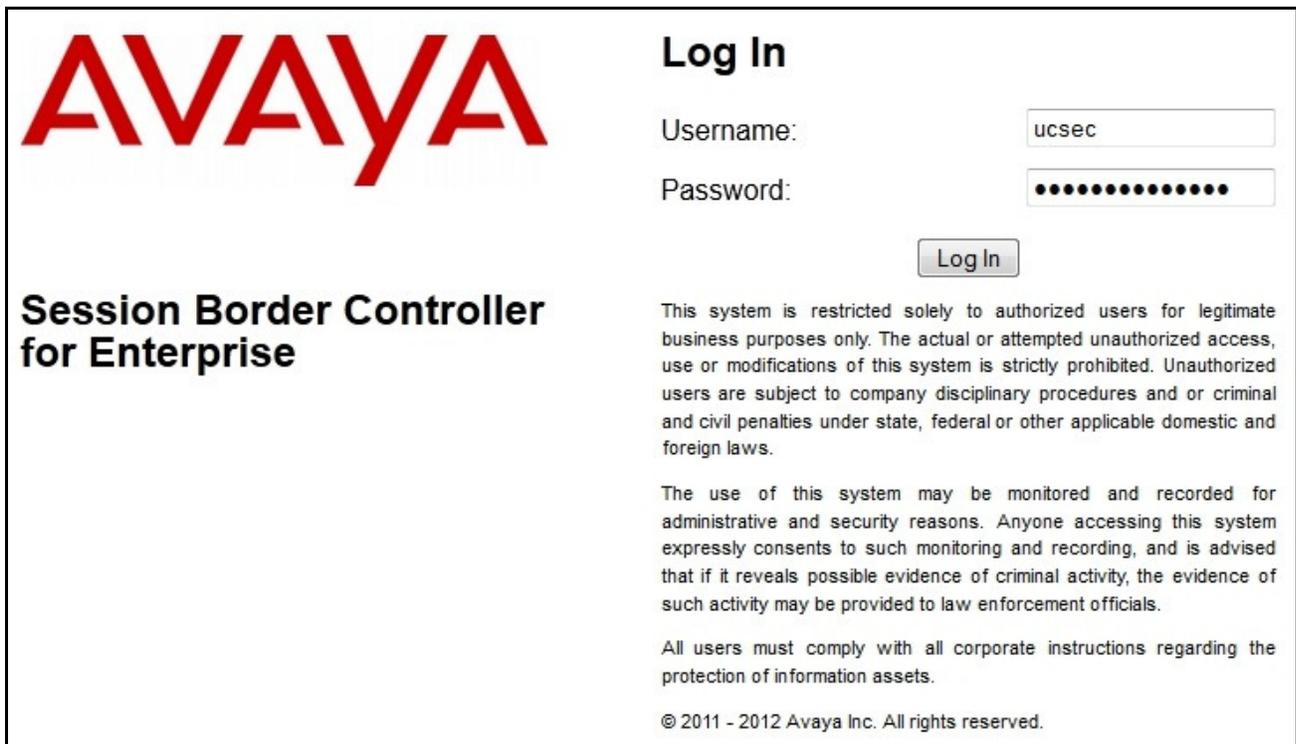
- Global Profiles:
 - URI Groups
 - Routing
 - Topology Hiding
 - Server Interworking
 - Server Configuration
- Domain Policies:
 - Application Rules
 - Media Rules
 - Signaling Rules
 - Endpoint Policy Group
 - Session Policy
- Device Specific Settings:

- Network Management
- Media Interface
- Signaling Interface
- End Point Flows → Server Flows
- Session Flows

6.1 Log into the Avaya Session Border Controller for Enterprise

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

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



The screenshot shows the Avaya Session Border Controller for Enterprise login interface. 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:" field with the value "ucsec", a "Password:" field with masked characters, 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." followed by a consent 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." and a compliance statement: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, the copyright notice reads: "© 2011 - 2012 Avaya Inc. All rights reserved."

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

The screenshot shows the Avaya Session Border Controller for Enterprise Dashboard. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the AVAYA logo. A left sidebar contains a 'Dashboard' menu with options like Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Dashboard' and is divided into four panels: 'Information' (System Time: 09:37:35 AM GMT, Version: 6.2.0.Q48, Build Date: Wed May 22 22:52:47 UTC 2013), 'Installed Devices' (listing EMS and Avaya_SBCE), 'Alarms (past 24 hours)' (None found), and 'Incidents (past 24 hours)' (None found). A 'Notes' section at the bottom shows 'No notes found' and an 'Add' button.

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

The screenshot shows the 'System Management' page in the Avaya Session Border Controller for Enterprise. The top navigation bar is the same as in the dashboard. The main header displays 'Session Border Controller for Enterprise' and the AVAYA logo. The left sidebar now highlights 'System Management' with sub-options: Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'System Management' and has tabs for 'Devices', 'Updates', 'SSL VPN', and 'Licensing'. The 'Devices' tab is active, showing a table of installed devices:

Device Name (Serial Number)	Management IP	Version	Status
Avaya_SBCE (IP:52:10c20000)	192.168.10.75	6.2.0.Q48	Commissioned

Below the table, there are action links: Reboot, Shutdown, Restart Application, View, Edit, and Delete.

The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponded to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

System Information: Avaya_SBCE
X

General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
172.16.5.92	172.16.5.92	255.255.255.0	172.16.5.254	A1
172.16.157.190	172.16.157.190	255.255.255.192	172.16.157.129	B1

DNS Configuration

Primary DNS	192.168.10.100
Secondary DNS	
DNS Location	DMZ
DNS Client IP	172.16.5.92

Management IP(s)

IP	192.168.10.75
----	---------------

6.2 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the UC-Sec control Center.

6.2.1 Server Interworking Avaya

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

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

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone Profile**.

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

For the newly created **Avaya** profile, click **Edit** (not shown) at the bottom of the General tab

- Click **Next**.
- Click **Finish** on the **Privacy and DTMF** tab.
- Leave other fields with their default values.

The following screen capture shows the newly added Avaya Profile.

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

The left sidebar contains a navigation menu with categories such as Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The 'Server Interworking' option is highlighted in red.

The main content area is titled 'Interworking Profiles: Avaya'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A list of profiles is shown, with 'Avaya' selected and highlighted in red. The configuration details for the 'Avaya' profile are displayed in a tabbed interface with the 'General' tab active.

The 'General' tab configuration includes the following settings:

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

Privacy	
Privacy Enabled	No
User Name	

6.2.2 Server Interworking Service Provider

A second Server Interworking profile named **Service Provider** was created for the Service Provider.

On the left navigation pane, select **Global Profiles** → **Server Interworking**. From the **Interworking Profiles** list, select **Add**.

Enter the new profile name (not shown), the name of **Service Provider** was chosen in this example. Accept the default values for all fields by clicking **Next** and then Click **Finish**.

The following screen capture shows the newly added **Service Provider** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Profiles', 'Server Interworking', 'Phone Interworking', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Server Interworking' option is highlighted in red.

The main content area is titled 'Interworking Profiles: Service Provider'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a table of existing profiles: cs2100, avaya-ru, OCS-Edge-Server, cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd-Server, Avaya, and 'Service Provider' (highlighted in red). A blue bar above the configuration pane says 'Click here to add a description.' The configuration pane has tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing a table of settings:

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

Below the 'General' tab is a 'Privacy' section with the following settings:

Privacy	
Privacy Enabled	No
User Name	

6.2.3 Routing Profiles

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

Two Routing Profiles were created in the test configuration, one for inbound calls, with IP Office as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select the **Routing** tab (not shown).
- Select **Add**.
- Enter Profile Name: **Route to IP Office**.
- Click **Next** (not shown).

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.60** (IP Office IP address).
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish**.

The following screen shows the newly added **Route to IP Office** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various configuration areas, with 'Routing' highlighted in red. The main content area is titled 'Routing Profiles: Route to IP Office' and features an 'Add' button. Below this, a table lists the routing profiles:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	172.16.5.60	---	View Edit

Similarly, for the outbound route:

- Select **Add**.
- Enter Profile Name: **Route to SP**
- Click **Next**.
- **Next Hop Server 1: 192.168.139.155** (IP address for Service Provider's proxy server)
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish**.

The following screen capture shows the newly added **Route_to_SP** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Global Profiles', 'Routing', and 'SIP Cluster'. The main content area is titled 'Routing Profiles: Route to SP' and features an 'Add' button, a 'Click here to add a description' link, and a table of routing profiles. The table has columns for 'Priority', 'URI Group', 'Next Hop Server 1', and 'Next Hop Server 2'. One profile is listed with a priority of 1, a URI Group of '*', and a Next Hop Server 1 of 192.168.139.155. There are 'View' and 'Edit' links for this profile. A secondary 'Add' button is also present in the table area.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	192.168.139.155	---	View Edit

6.2.4 Server Configuration

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

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add** and enter the profile name: **Session Manager**.

On the **Add Server Configuration Profile** Tab (not shown):

- Select Server Type: **Call Server**.
- **IP Address: 172.16.5.60** (IP Address of IP Office).
- **Supported Transports: Check UDP**.
- **TCP Port: 5060**.
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

The following screen capture shows the **General** tab of the newly added **IP Office** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation pane lists various system management options, with 'Server Configuration' highlighted in red. The main content area is titled 'Server Configuration: IP Office' and features an 'Add' button, a 'Service Provider' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a table with the following configuration:

Property	Value
Server Type	Call Server
IP Addresses / FQDNs	172.16.5.60
Supported Transports	UDP
UDP Port	5060

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

The following screen capture shows the **Advanced** tab of the added **IP Office** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', and 'Server Configuration'. The main content area is titled 'Server Configuration: IP Office' and features an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. Below this are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'Advanced' tab is active, showing a table of configuration options: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (set to 'Avaya'), 'Signaling Manipulation Script' (set to 'None'), and 'UDP Connection Type' (set to 'SUBID'). An 'Edit' button is located at the bottom right of the configuration table.

To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** and enter the profile name: **Service Provider**.

On the **Add Server Configuration Profile** Tab (not shown):

- Select Server Type: **Trunk Server**.
- **IP Address: 192.168.139.155** (service provider's SIP Proxy IP address).
- **Supported Transports: Check UDP**.
- **UDP Port: 5060**.
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Service Provider** from the **Interworking Profile** drop down menu.
Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

The following screen capture shows the **General** tab of the **Service Provider** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Server Configuration' section is active, showing 'Server Profiles' and 'IP Office' with an 'Add' button. The 'Service Provider' profile is selected, and the 'General' tab is active. The configuration table is as follows:

General	Authentication	Heartbeat	Advanced
Server Type	Trunk Server		
IP Addresses / FQDNs	192.168.139.155		
Supported Transports	UDP		
UDP Port	5060		

Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

The following screen capture shows the **Advanced** tab of the **Service Provider** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface, showing the 'Advanced' tab of the 'Service Provider' configuration. The top navigation bar and main header are identical to the previous screenshot. The left sidebar is also the same. The 'Server Configuration' section is active, and the 'Advanced' tab is selected. The configuration table is as follows:

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

Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

6.2.5 Topology Hiding

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

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

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

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name: IP Office**.
- Click **Finish**.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Topology Hiding' highlighted in red. The main content area is titled 'Topology Hiding Profiles: IP Office' and features an 'Add' button, a 'Click here to add a description' link, and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a table with the following data:

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

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

To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**
- Enter the **Profile Name: Service_Provider**.
- Click **Finish**.
- Click **Edit** on the newly added **Service Provider** Topology Hiding profile.
- In the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the enterprise (**tsst.co.tt**) under **Overwrite Value**.
- In the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Enterprise (**tsst.co.tt**) under **Overwrite Value**.
- In the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Enterprise (**tsst.co.tt**) under **Overwrite Value**.

The following screen capture shows the newly added **Service_Provider** Profile.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, **Topology Hiding** (highlighted), Signaling Manipulation, URI Groups, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "Topology Hiding Profiles: Service Provider" and contains an "Add" button, a list of profiles (default, cisco_th_profile, IP Office, and **Service Provider**), and a table of configuration rules. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. Below the table is an "Edit" button.

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

6.2.6 Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows to perform a granular header manipulation on the headers in the SIP messages, which sometimes is not possible by direct configuration on the web interface. The ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

Signaling Manipulation was not necessary and was not used during the compliance testing.

6.3 Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, only a new Application Rule was defined. All other rules under Domain Policies, linked together on End Point Policy Groups, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

6.3.1 Create Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select

Domain Policies → Application Rules

Select **default trunk** Rule (not shown)

Select **Clone Rule** button (not shown)

Name: **Sessions=500**

Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **500** was used in the sample configuration.

Click Finish (not shown).

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

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

Application Rules: Sessions=500

Add Filter By Device... Rename Clone Delete

Click here to add a description.

Application Rule

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

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

6.3.2 Media Rules

For the compliance test, the **default-low-med** Media Rule was used.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

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

Media Rules: default-low-med

Add Filter By Device... Clone

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

Media NAT Media Encryption Media Anomaly Media Silencing Media QoS

Media NAT Learn Media IP dynamically

Edit

6.3.3 Signaling Rules

For the compliance test, the **default** Signaling Rule was used.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar menu lists various configuration areas, with 'Signaling Rules' highlighted in red. The main content area is titled 'Signaling Rules: default' and features an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'General' tab is active, showing a table with three sections: 'Inbound', 'Outbound', and 'Content-Type Policy'. The 'Inbound' and 'Outbound' sections each have a table with four rows: 'Requests', 'Non-2XX Final Responses', 'Optional Request Headers', and 'Optional Response Headers', all with an 'Allow' action. The 'Content-Type Policy' section has a table with three rows: 'Enable Content-Type Checks' (checked), 'Action' (Allow, Multipart Action, Allow), and 'Exception List' (Exception List). An 'Edit' button is located at the bottom right of the configuration area.

6.3.4 End Point Policy Groups

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

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add**.

- **Group Name: Enterprise.**
- **Application Rule: Sessions=500.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Time of Day: default.**
- **Click Finish.**

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Domain Policies', and 'End Point Policy Groups'. The 'End Point Policy Groups' section is expanded, showing a list of policy groups including 'Enterprise'. The main content area is titled 'Policy Groups: Enterprise' and features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename' and 'Delete' buttons. Below this, there are two blue bars with instructions: 'Click here to add a description.' and 'Hover over a row to see its description.'. A 'Policy Group' modal window is open, showing a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: Order: 1, Application: Sessions=500, Border: default, Media: default-low-med, Security: default-low, Signaling: default, Time of Day: default. The modal also includes 'Summary' and 'Add' buttons and 'Edit' and 'Clone' links for the row.

Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add**.

- **Group Name: Service Provider.**
- **Application Rule: Sessions=500.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Time of Day: default.**
- **Click Finish.**

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various management options, with 'End Point Policy Groups' highlighted in red. The main content area is titled 'Policy Groups: Service Provider' and features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename' and 'Delete' buttons. Below this, there are two blue bars with instructions: 'Click here to add a description.' and 'Hover over a row to see its description.' A 'Policy Group' table is visible, with a 'Summary' and 'Add' button above it. The table has columns for Order, Application, Border, Media, Security, Signaling, and Time of Day. One row is shown with the following data: Order: 1, Application: Sessions=500, Border: default, Media: default-low-med, Security: default-low, Signaling: default, Time of Day: default. Action buttons 'Edit' and 'Clone' are present at the end of the row.

6.4 Device Specific Settings

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

6.4.1 Network Management

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

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

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

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

Network Management: Avaya_SBCE

Devices
Avaya_SBCE

Network Configuration Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

A1 Netmask A2 Netmask B1 Netmask

IP Address	Public IP	Gateway	Interface	
<input type="text" value="172.16.5.92"/>	<input type="text"/>	<input type="text" value="172.16.5.254"/>	<input type="text" value="A1"/>	<input type="button" value="Delete"/>
<input type="text" value="172.16.157.190"/>	<input type="text"/>	<input type="text" value="172.16.157.129"/>	<input type="text" value="B1"/>	<input type="button" value="Delete"/>

On the Interface Configuration tab, click the **Toggle** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **disabled**, so it is important to perform this step, or the Avaya SBCE will not be able to communicate on any of its interfaces.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

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

Network Management: Avaya_SBCE

Devices
Avaya_SBCE

Network Configuration **Interface Configuration**

Name	Administrative Status	
A1	Enabled	<input type="button" value="Toggle"/>
A2	Disabled	<input type="button" value="Toggle"/>
B1	Enabled	<input type="button" value="Toggle"/>

6.4.2 Media Interface

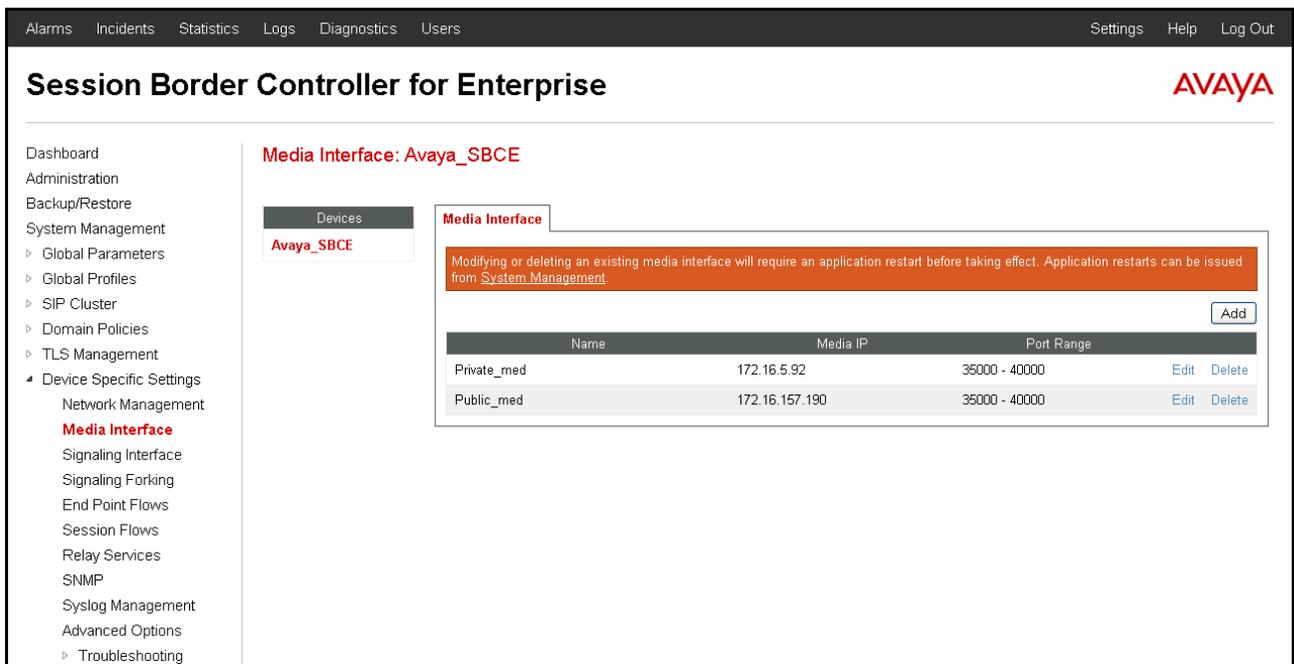
Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE ports range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**.

Select **Add Media Interface** (not shown)

- **Name: Private.**
- Select **IP Address: 172.16.5.92** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **Port Range: 35000-40000.**
- Click **Finish.**
- Select **Add Media Interface.**
- **Name: Public.**
- Select **IP Address: 172.16.157.190** (Outside IP Address of the Avaya SBCE, toward Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish.**

The following screen capture shows the added **Media Interfaces**.



The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The page title is "Session Border Controller for Enterprise" and the Avaya logo is in the top right. The left navigation menu includes "Device Specific Settings" > "Media Interface". The main content area is titled "Media Interface: Avaya_SBCE" and shows a table of configured media interfaces. A warning message states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management". An "Add" button is visible in the top right of the table area.

Name	Media IP	Port Range	Edit	Delete
Private_med	172.16.5.92	35000 - 40000	Edit	Delete
Public_med	172.16.157.190	35000 - 40000	Edit	Delete

6.4.3 Signaling Interface

To create the Signaling Interface toward Session Manager, from the **Device Specific** menu on the left hand side, select **Signaling Interface**. Select **Add Signaling Interface** (not shown):

- **Name: Private.**
- Select **IP Address: 172.16.5.92** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port: 5060.**
- Click **Finish.**
- Select **Add Signaling Interface:**
- **Name: Public**
- Select **IP Address: 172.16.157.190** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish.**

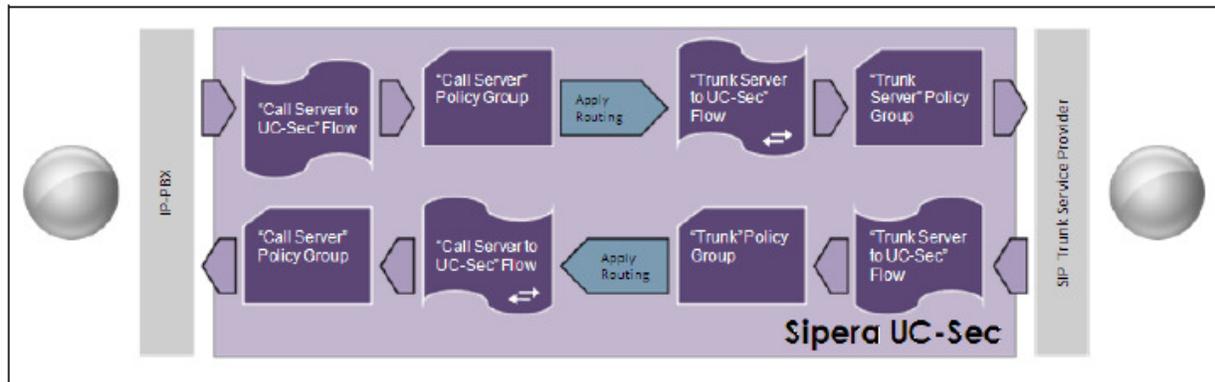
The following screen capture shows the newly added **Signaling Interfaces**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar menu lists various configuration options, with 'Device Specific Settings' expanded to show 'Signaling Interface' selected. The main content area is titled 'Signaling Interface: Avaya_SBCE' and features a sub-tab 'Signaling Interface' with an 'Add' button. Below this is a table listing the configured signaling interfaces:

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Private_sig	172.16.5.92	---	5060	---	None	Edit	Delete
Public_sig	172.16.157.190	---	5060	---	None	Edit	Delete

6.4.4 End Point Flows

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



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

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, tab **Server Flows**. Click **Add Flow**.

- **Name: SIP Trunk Flow.**
- **Server Configuration: Service Provider.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Private_sig.**
- **Signaling Interface: Public_sig.**
- **Media Interface: Public_med.**
- **End Point Policy Group: Service Provider.**
- **Routing Profile: Route to IP Office** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service Provider.**
- **File Transfer Profile: None.**
- **Click Finish.**

Criteria		Profile	
Flow Name	SIP Trunk Flow	Signaling Interface	Public_sig
Server Configuration	Service Provider	Media Interface	Public_med
URI Group	*	End Point Policy Group	Service Provider
Transport	*	Routing Profile	Route to IP Office
Remote Subnet	*	Topology Hiding Profile	Service Provider
Received Interface	Private_sig	File Transfer Profile	None

To create the call flow toward the IP Office, click **Add Flow**.

- **Name: IP Office Flow.**
- **Server Configuration: IP Office.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Public_sig.**
- **Signaling Interface: Private_sig.**
- **Media Interface: Private_med.**
- **End Point Policy Group: Enterprise.**
- **Routing Profile: Route to SP** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: IP Office.**
- **File Transfer Profile: None.**
- Click **Finish**.

Criteria		Profile	
Flow Name	IP Office Flow	Signaling Interface	Private_sig
Server Configuration	IP Office	Media Interface	Private_med
URI Group	*	End Point Policy Group	Enterprise
Transport	*	Routing Profile	Route to SP
Remote Subnet	*	Topology Hiding Profile	IP Office
Received Interface	Public_sig	File Transfer Profile	None

The following screen capture shows the added **End Point Flows**.

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

The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, Signaling Interface, Signaling Forking, **End Point Flows** (highlighted), Session Flows, Relay Services, SNMP, Syslog Management, Advanced Options, and Troubleshooting.

The main content area is titled "End Point Flows: Avaya_SBCE". It features two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing an "Add" button and a blue bar with the text "Click here to add a row description."

Below this, there are two sections for "Server Configuration":

- Server Configuration: IP Office**: A table with columns: Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. It contains one row: Priority 1, Flow Name IP Office Flow, URI Group *, Received Interface Public_sig, Signaling Interface Private_sig, End Point Policy Group Enterprise, and Routing Profile Route to SP. Action buttons: View, Clone, Edit, Delete.
- Server Configuration: Service Provider**: A table with the same columns. It contains one row: Priority 1, Flow Name SIP Trunk Flow, URI Group *, Received Interface Private_sig, Signaling Interface Public_sig, End Point Policy Group Service Provider, and Routing Profile Route to IP Office. Action buttons: View, Clone, Edit, Delete.

7. Telecommunications Services of Trinidad and Tobago SIP Trunking Configuration

TSTT is responsible for the configuration of the SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya IP Office at the enterprise. TSTT will provide the customer the necessary information to configure the Avaya IP Office SIP trunk connection, including:

- IP address of the TSTT SIP Proxy server.
- Supported codec's and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

8. Verification and Troubleshooting

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

8.1 Verification Steps

The following steps may be used to verify the configuration:

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

8.2 Protocol Traces

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

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

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

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

8.3 IP Office System Status

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

- Use the Avaya IP Office **System Status** application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed. Select the SIP Line of interest from the left pane. On the **Status** tab in the right pane, verify that the **Current State** is **Idle** for each channel (assuming no active calls at present time).

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
 Alarms (10)
 Extensions (28)
 Trunks (3)
 Line: 1
 Line: 2
 Line: 17
 Active Calls
 Resources
 Voicemail
 IP Networking
 Locations

Status Utilization Summary Alarms

SIP Trunk Summary

Peer Domain Name: sip://172.16.5.92
 Resolved Address: 172.16.5.92
 Line Number: 17
 Number of Administered Channels: 10
 Number of Channels in Use: 0
 Administered Compression: G711 Mu, G729 A
 Silence Suppression: Off
 Layer 4 Protocol: UDP
 SIP Trunk Channel Licenses: Unlimited
 SIP Trunk Channel Licenses in Use: 0 0%
 SIP Device Features:

Channel Number	LRI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Los...	Transmit Jitter	Transmit Packet Los...
1			Idle	19:54:46											
2			Idle	2 days 00:...											
3			Idle	2 days 22:...											
4			Idle	7 days 01:...											
5			Idle	7 days 01:...											
6			Idle	7 days 01:...											
7			Idle	7 days 01:...											
8			Idle	7 days 01:...											
9			Idle	7 days 01:...											
10			Idle	7 days 01:...											

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

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

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
 Alarms (10)
 Configuration (0)
 Service (1)
 Trunks (4)
 Line: 1 (2)
 Line: 2 (2)
 Line: 17 (0)
 Link (0)
 Call Quality of Ser
 TLS (0)
 Extensions (28)
 Trunks (3)
 Active Calls
 Resources
 Voicemail
 IP Networking
 Locations

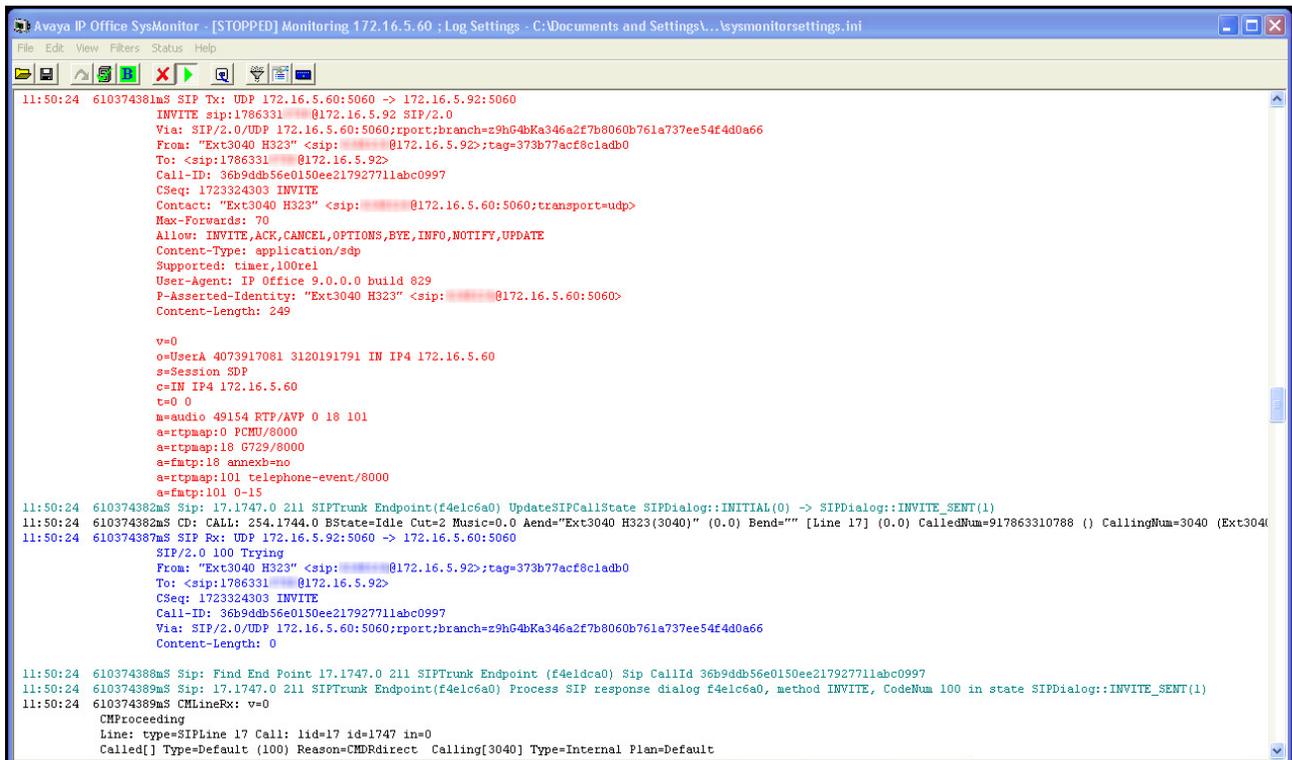
Alarms for Line: 17 SIP sip://172.16.5.92

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

8.4 IP Office Monitor

The Avaya IP Office Monitor application can also be used to monitor and troubleshoot SIP signaling messaging between TSTT and IP Office. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where Avaya IP Office Manager was installed.

The sample screen below shows part of the messages on an outbound call.



```
Avaya IP Office SysMonitor - [STOPPED] Monitoring 172.16.5.60 : Log Settings - C:\Documents and Settings\...sysmonitortestsettings.ini
File Edit View Filters Status Help
11:50:24 610374381mS SIP Tx: UDP 172.16.5.60:5060 -> 172.16.5.92:5060
INVITE sip:1786331@172.16.5.92 SIP/2.0
Via: SIP/2.0/UDP 172.16.5.60:5060;rport:branch=z9hG4bKa346a2f7b8060b761a737ee54f4d0a66
From: "Ext3040 H323" <sip:1786331@172.16.5.92>;tag=373b77acf8cladb0
To: <sip:1786331@172.16.5.92>
Call-ID: 36b9ddb56e0150ee217927711abc0997
CSeq: 1723324303 INVITE
Contact: "Ext3040 H323" <sip:1786331@172.16.5.60:5060;transport=udp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Content-Type: application/sdp
Supported: timer,100rel
User-Agent: IP Office 9.0.0.0 build 829
P-Asserted-Identity: "Ext3040 H323" <sip:1786331@172.16.5.60:5060>
Content-Length: 249

v=0
o=UserA 4073917081 3120191791 IN IP4 172.16.5.60
s=Session SDP
c=IN IP4 172.16.5.60
t=0 0
m=audio 49154 RTP/AVP 0 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fatp:18 amnxb=no
a=rtpmap:101 telephone-event/8000
a=fatp:101 0-15
11:50:24 610374382mS Sip: 17.1747.0 211 SIPTrunk Endpoint(f4elc6a0) UpdateSIPCallState SIPDialog::INITIAL(0) -> SIPDialog::INVITE_SENT(1)
11:50:24 610374382mS CD: CALL: 254.1744.0 BState=Idle Cut=2 Music=0.0 Aend="Ext3040 H323(3040)" (0.0) Bend="" [Line 17] (0.0) CalledNum=917863310788 () CallingNum=3040 (Ext3040)
11:50:24 610374387mS SIP Rx: UDP 172.16.5.92:5060 -> 172.16.5.60:5060
SIP/2.0 100 Trying
From: "Ext3040 H323" <sip:1786331@172.16.5.92>;tag=373b77acf8cladb0
To: <sip:1786331@172.16.5.92>
CSeq: 1723324303 INVITE
Call-ID: 36b9ddb56e0150ee217927711abc0997
Via: SIP/2.0/UDP 172.16.5.60:5060;rport:branch=z9hG4bKa346a2f7b8060b761a737ee54f4d0a66
Content-Length: 0
11:50:24 610374388mS Sip: Find End Point 17.1747.0 211 SIPTrunk Endpoint (f4elc6a0) Sip CallId 36b9ddb56e0150ee217927711abc0997
11:50:24 610374389mS Sip: 17.1747.0 211 SIPTrunk Endpoint(f4elc6a0) Process SIP response dialog f4elc6a0, method INVITE, CodeNum 100 in state SIPDialog::INVITE_SENT(1)
11:50:24 610374389mS CMLineRx: v=0
CMProceeding
Line: type=SIPLine 17 Call: lid=17 id=1747 in=0
Called[] Type=Default (100) Reason=CMRdirect Calling[3040] Type=Internal Plan=Default
```

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office 9.0, Avaya Session Border Controller for Enterprise R6.2 and Telecommunications Services of Trinidad and Tobago SIP Trunk Service, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations noted in **Section 2.2**

10. References

- [1] *IP Office 9.0 Installing IP500/IP500 V2*, Document Number 15-601042 Issue 28g - (11 October 2013)
- [2] *IP Office Manager Release 9.0*, Document Number 15-601011 Issue 9.01 (Monday, September 09, 2013).
- [3] *IP Office 9.0 Administering Voicemail Pro*, Document Number 15-601063 Issue 9.01.0 - (Tuesday, September 10, 2013)
- [4] *IP Office 9.0 Installing IP Office Video Softphone*, Issue 4c - (21 August 2013)
- [5] *Administering Avaya Flare ® Experience for iPad devices and Windows*, Release 9.0 Issue 02.01 September 2013.
- [6] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013.
- [7] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013.
- [8] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013.

Documentation for Avaya products may be found at <http://support.avaya.com>.

Product documentation for TSTT SIP Trunking Service is available from TSTT.

11. SIP Line Template

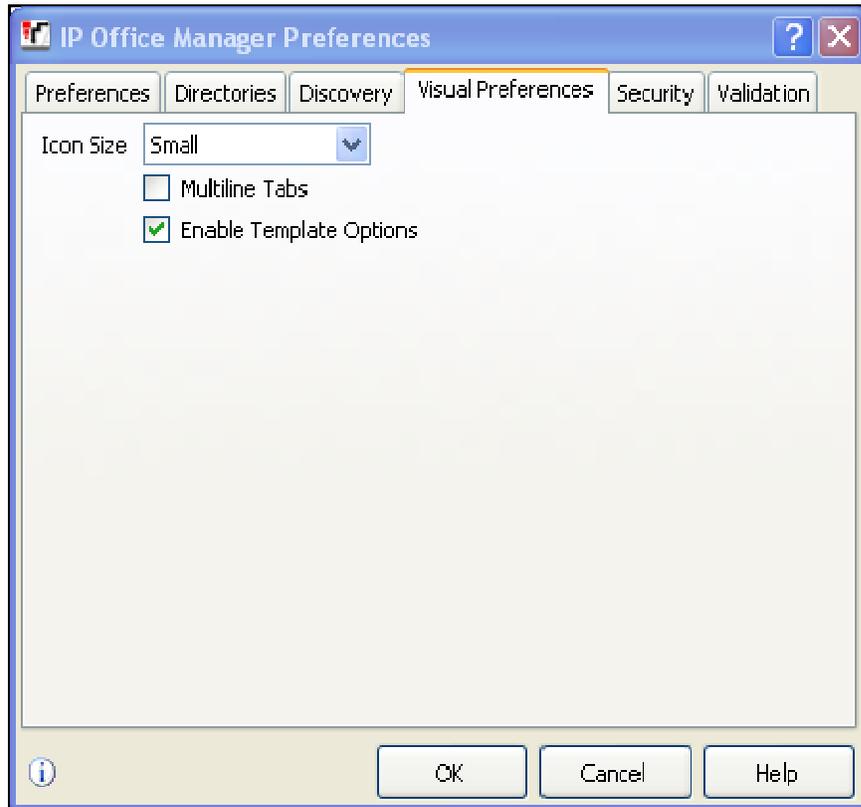
This Appendix describes how IP Office Manager Template Provisioning can be used to simplify the configuration of SIP Lines in IP Office. The Template Provisioning feature was introduced in IP Office Release 7.0.

11.1 Create a New SIP Trunk from Template

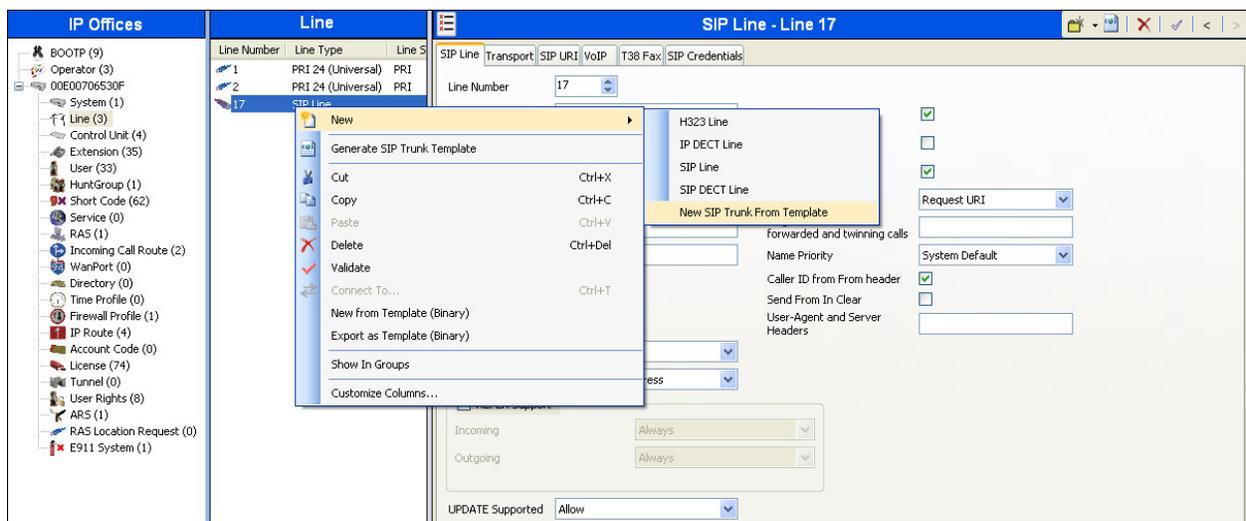
This section describes the steps performed by an IP Office system administrator to use Manager to create a new SIP Line using a previously generated template. Please follow these steps very carefully to avoid using 'New from Template (Binary)'. The binary templates ARE NOT to be used because binary templates also include IP Office system specific details to the customers IP Office including SIP line credentials and SIP line SIP URIs.

- The IP Office system administrator must place the template xml file in the Manager Templates folder. The default folder is the Templates folder under the Manager installation folder. On Windows XP the folder is C:\Program Files\Avaya\IP Office\Manager\Templates. Templates stored in a non default folder can be imported into Manager using Tools → Import Templates in Manager.
- In Manager, the administrator must ensure Manager template options are enabled. When enabled, the Manager can be used to apply trunk templates. SIP trunk templates can be used to add SIP trunks.

To enable template support in the IP Office Manager, select **File**, then **Preferences**. On the **Visual Preferences** tab, check the **Enable Template Options** box.



Next, import the template into the new IP Office system by creating a new SIP Line as shown in the screenshot below. In the Navigation Pane on the left, right-click on **Line** then navigate to **New, New SIP Trunk From Template**:



On the next screen, **Template Type Selection**, verify that the information in the **Country** and **Service Provider** fields is correct. If more than one template is present, use the drop-down menus to select the required template. Click **Create new SIP Trunk** to finish the process.



The following is the exported SIP Line Template file **TT_TSTT_SIPTrunk.xml** created after the testing was completed:

```
<?xml version="1.0" encoding="utf-8" ?>
<Template xmlns="urn:SIPTrunk-schema">
<TemplateType>SIPTrunk</TemplateType>
<Version>20131101</Version>
<SystemLocale>enu</SystemLocale>
<DescriptiveName>TSTT IPO 9.0</DescriptiveName>
<ITSPDomainName>tstt.co.tt</ITSPDomainName>
<SendCallerID>CallerIDDIV</SendCallerID>
<ReferSupport>false</ReferSupport>
<ReferSupportIncoming>1</ReferSupportIncoming>
<ReferSupportOutgoing>1</ReferSupportOutgoing>
<RegistrationRequired>false</RegistrationRequired>
<UseTelURI>false</UseTelURI>
<CheckOOS>true</CheckOOS>
<CallRoutingMethod>1</CallRoutingMethod>
<OriginatorNumber />
<AssociationMethod>SourceIP</AssociationMethod>
<LineNamePriority>SystemDefault</LineNamePriority>
<UpdateSupport>UpdateAuto</UpdateSupport>
<URIType>SIPURI</URIType>
<UserAgentServerHeader />
<CallerIDfromFromheader>true</CallerIDfromFromheader>
<PerformUserLevelPrivacy>false</PerformUserLevelPrivacy>
<ITSPProxy>172.16.5.92</ITSPProxy>
<LayerFourProtocol>SipUDP</LayerFourProtocol>
<SendPort>5060</SendPort>
<ListenPort>5060</ListenPort>
<DNSServerOne>0.0.0.0</DNSServerOne>
<DNSServerTwo>0.0.0.0</DNSServerTwo>
<CallsRouteViaRegistrar>true</CallsRouteViaRegistrar>
<SeparateRegistrar />
```

<CompressionMode>**AUTOSELECT**</CompressionMode>
<UseAdvVoiceCodecPrefs>**true**</UseAdvVoiceCodecPrefs>
<AdvCodecPref>**G.711 ULAW 64K,G.729(a) 8K CS-ACELP**</AdvCodecPref>
<CallInitiationTimeout>**4**</CallInitiationTimeout>
<DTMFSupport>**DTMF_SUPPORT_RFC2833**</DTMFSupport>
<VoipSilenceSupression>**false**</VoipSilenceSupression>
<ReinviteSupported>**true**</ReinviteSupported>
<FaxTransportSupport>**FOIP_NONE**</FaxTransportSupport>
<UseOffererPrefferedCodec>**false**</UseOffererPrefferedCodec>
<CodecLockdown>**false**</CodecLockdown>
<Rel100Supported>**true**</Rel100Supported>
<T38FaxVersion>**3**</T38FaxVersion>
<Transport>**UDPTL**</Transport>
<LowSpeed>**0**</LowSpeed>
<HighSpeed>**0**</HighSpeed>
<TCFMethod>**Trans_TCF**</TCFMethod>
<MaxBitRate>**FaxRate_14400**</MaxBitRate>
<EflagStartTimer>**2600**</EflagStartTimer>
<EflagStopTimer>**2300**</EflagStopTimer>
<UseDefaultValues>**true**</UseDefaultValues>
<ScanLineFixup>**true**</ScanLineFixup>
<TFOPEnhancement>**true**</TFOPEnhancement>
<DisableT30ECM>**false**</DisableT30ECM>
<DisableEflagsForFirstDIS>**false**</DisableEflagsForFirstDIS>
<DisableT30MRCompression>**false**</DisableT30MRCompression>
<NSFOVERRIDE>**false**</NSFOVERRIDE>
</Template>

©2013 Avaya Inc. All Rights Reserved.

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

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