



Avaya Solution & Interoperability Test Lab

Application Notes for Rogers Business Solutions SIP Trunking Service with Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise Release 6.2- Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Rogers Business Solutions Session Initiation Protocol (SIP) Trunking Service with Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise Release 6.2.

Rogers Business Solutions SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Rogers Business Solutions networks as an alternative to legacy analog or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

Rogers Business Solutions 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.....	5
3. Reference Configuration	6
4. Equipment and Software Validated	8
5. Configure IP Office	9
5.1 LAN	10
5.2 IP Route	13
5.3 System Telephony and Codecs	14
5.4 Twinning Calling Party Information.....	16
5.5 Administer SIP Line	16
5.5.1 Administer SIP Line Settings.....	16
5.5.2 Administer Transport Settings	18
5.5.3 Administer SIP URI Settings	19
5.5.4 Administer VoIP Settings	21
5.5.5 Administer T38 Fax Settings	21
5.6 Short Code	23
5.7 User	25
5.8 Incoming Call Route	27
5.9 Privacy/Anonymous Calls	28
5.10 Save Configuration	29
6. Configure the Avaya Session Border Controller for Enterprise	30
6.1 Log into the Avaya Session Border Controller for Enterprise.....	31
6.2 Global Profiles	34
6.2.1 Uniform Resource Identifier (URI) Groups.....	34
6.2.2 Routing Profiles	35
6.2.3 Topology Hiding.....	36
6.2.4 Server Interworking	37
6.2.5 Server Configuration.....	39
6.3 Domain Policies	41
6.3.1 Application Rules.....	41
6.3.2 Media Rules	42
6.3.3 Signaling Rules	45
6.3.4 Endpoint Policy Groups.....	47
6.3.5 Session Policy	48
6.4 Device Specific Settings	50
6.4.1 Network Management.....	50
6.4.2 Media Interface	51
6.4.3 Signaling Interface	52
6.4.4 End Point Flows - Server Flow	52
6.4.5 Session Flows.....	54

7. RBS SIP Trunking Service Configuration.....	56
8. Verification and Troubleshooting	57
8.1 Verification Steps.....	57
8.2 Protocol Traces	57
8.3 Troubleshooting	57
8.3.1 IP Office System Status	57
8.3.2 Sniffer Traces Analysis.....	58
9. Conclusion	61
10. References.....	62

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Rogers Business Solutions and Avaya IP Office solution. In the sample configuration, Avaya IP Office solution consists of Avaya IP Office (IP Office) Release 8.1, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2, and various Avaya endpoints.

Rogers Business Solutions (RBS) SIP Trunking Service referenced within these Application Notes is designed for business customers. The service enables PSTN calling via a broadband WAN connection using SIP protocol. This converged network solution is a cost effective alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using IP Office to connect to RBS 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 RBS SIP Trunking interoperability, following features and functionalities were exercised during the compliance testing:

- Incoming PSTN calls to various phone types including SIP, H.323, digital and analog telephones at the enterprise. All incoming calls from PSTN are routed to the enterprise across the SIP Trunk from the service provider networks.
- Outgoing PSTN calls from various phone types including SIP, H.323, digital and analog telephone at the enterprise. All outgoing calls to PSTN are routed from the enterprise across the SIP trunk to the service provider networks.
- Incoming and outgoing PSTN calls to/from Avaya IP Office Softphone using both SIP and H.323 protocols.
- Dialing plans including local, long distance, outgoing toll-free calls, local directory assistance (411), etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Proper codec negotiation of G.711MU and G.729 codecs.
- Proper early media transmissions G.711MU and G.729 codecs.
- Proper media transmission using G.711MU and G.729 codecs.
- Proper fax over IP with T.38 codes.
- DTMF tone transmissions as out-of-band RTP event 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 transfer with re-INVITE method.
- Off-net call forward with Diversion method.
- Mobility Twinning incoming calls to mobile phones with Diversion method.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.

This test plan does not include the Operator Assisted Call 0- i.e., dial 0 as the RBS test environment does not support the 0- call. However RBS does support 0- in their production SIP Trunking service.

RBS SIP trunk service does not support the following:

- RBS SIP REFER method for call transfer.
- Fax G.711.
- Dialling 0+10 digits.

2.2 Test Results

Interoperability testing of RBS with Avaya IP Office solution was successfully completed with the exception of the observations/limitations described below.

- 1. RBS does not send OPTIONS but responds to IP Office OPTIONS with 200OK.**
- 2. Calling Party Name and Number are not updated if IP Office off-net redirects (by transferring or forwarding) an incoming or outgoing call back to PSTN.** Before (and after) completing the off-net redirection, IP Office did not send UPDATE or re-INVITE signaling to update the call display on PSTN parties. This is a known behavior of IP Office with no available resolution at this time. This issue has low user impact, it is listed here simply as an observation.
- 3. Calling Party Name and Number are not updated if IP Office off-net redirects (by transferring or forwarding) an incoming or outgoing call to internal station.** Before (or after) completing the local redirection to internal station, IP Office did not send UPDATE or re-INVITE signaling to update the call display on PSTN party. This is a known behavior of IP Office with no available resolution at this time. This issue has low user impact, it is listed here simply as an observation.

2.3 Support

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

For technical support on Rogers Business Solutions SIP Trunking Service, contact Rogers Business Solutions technical support at <http://www.rogersbusinesssolutions.com/sip-trunking/>.

3. Reference Configuration

Figure 1 below illustrates the test configuration. It shows an enterprise site connected to the RBS networks through the Internet.

For confidentiality and privacy purposes, actual public IP addresses and PSTN routable phone numbers used in the certification testing have been replaced with fictitious parameters throughout the Application Notes.

The Avaya components used to create the simulated customer site including:

- Avaya IP Office v500
- 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 soft-phones (SIP and H.323 modes)
- Avaya 9508 Digital Telephones
- Avaya Analog 8809 Telephones

Located at the enterprise site is Avaya IP Office 500v2 with the MOD DGTL STA16 expansion to provide connection for 16 digital stations, the PHONE 8 module to provide connection for 8 analog stations and the 64-channel Voice Compression Module (VCM) for supporting VoIP codec. IP Office has the LAN port that connects to the internal interface of the Avaya SBCE across the enterprise network. On another side, the external interface of the Avaya SBCE connects to RBS networks via the Internet.

Mobility Twinning is configured for some IP Office users so that incoming calls to these user phones can also be delivered to the configured mobile phones.

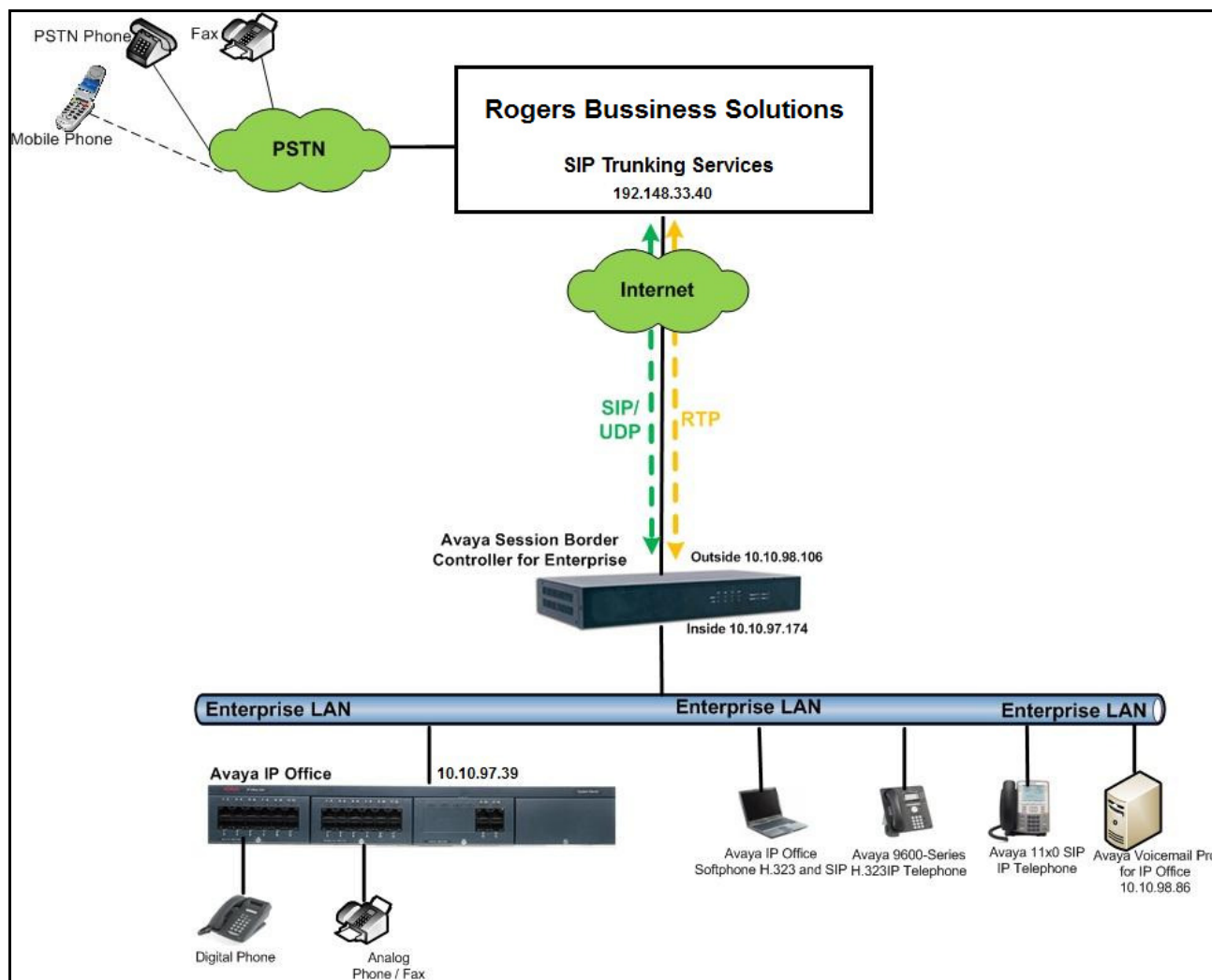


Figure 1: Avaya IP Telephony Network Connecting to RBS SIP Trunking Service

For the compliance testing, RBS provided the service provider public SIP domain as its Central Office (CO) IP address **192.148.33.40** and the enterprise public SIP domain as the Avaya SBCE external IP address **10.10.98.106**. These public SIP domains will be used for public SIP and RTP traffics between RBS and the Avaya SBCE using transport protocol UDP.

For outgoing calls, IP Office sent 11 digits in destination headers, e.g., “Request-URI” and “To”, and sent 10 digits in source headers, e.g., “From”, “Contact”, and “P-Asserted-Identity”. For incoming calls, RBS sent 10 digits in destination headers and sent 11 digits in source headers.

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	8.1 (67)
Avaya IP Office DIG DCP*16 V2	8.1 (67)
Avaya IP Office Ext Card Phone 8	8.1
Avaya IP Office Manager	10.1 (67)
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2 (6.2.0 Q30)
Avaya Voicemail Pro for IP Office	8.1.1003.0
Avaya 9630G IP Telephone (H.323)	Avaya one-X® Deskphone Edition S3.2
Avaya 11x0 IP Telephone (SIP)	SIP11x0e04.03.12.00
Avaya IP Office Softphone	3.2.3.20 64770
Avaya Digital Telephone (9508)	N/A
Avaya Analog 8809 Telephone	N/A

Rogers Business Solutions SIP Trunking Service Components	
Equipment/Software	Release/Version
Switch	RBS SIP Core 2.5.9130122
Media Gateway	AudioCodes M5K 6.1
Session Border Controller	ACME packet Net-Net 6.2

Testing was performed with IP Office 500v2 R8.1, but it also applies to IP Office Server Edition R8.1. Note that IP Office Server Edition requires an Expansion IP Office 500 v2 R8.1 to support analog or digital endpoints or trunks.

5. Configure IP Office

This section describes IP Office configuration required to interwork with RBS. It 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 proper IP Office from pop-up window, and log in with the appropriate credentials. A management window will appear as shown below. 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.

The screenshot displays the Avaya IP Office Manager interface for configuring 'DevCon IPO 2'. The left pane, titled 'IP Offices', shows a hierarchical tree of system components including BOOTP (7), Operator (3), DevCon IPO 2, System (1), DevCon IPO 2, Line (9), Control Unit (4), Extension (42), User (44), HuntGroup (7), Short Code (65), Service (0), RAS (1), Incoming Call Route (13), WanPort (0), Directory (0), Time Profile (0), Firewall Profile (1), IP Route (2), Account Code (0), License (41), Tunnel (0), User Rights (8), ARS (1), Authorization Code (0), and E911 System (1). The right pane, titled 'DevCon IPO 2*', contains configuration tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, Twinning, VCM, CCR, and Codecs. The 'System' tab is active, showing fields for Name (DevCon IPO 2), Locale (United States (US English)), and a 'Contact Information' section with a text box for special control. Below this are fields for Device ID, TFTP Server IP Address (10.10.97.39), HTTP Server IP Address (10.10.97.39), Phone File Server Type (Memory Card), Manager PC IP Address (10.10.98.74), and checkboxes for Avaya HTTP Clients Only, Enable Softphone HTTP Provisioning, and Automatic Backup. The 'Time Settings' section includes Time Server Address (0.0.0.0), Time Offset (00:00), File Writer IP Address (10.10.98.74), Dongle Serial Number (Local 1326478092), and AVPP IP Address (0.0.0.0). A 'Provider' field is set to 0, and a 'Branch Prefix' field is empty. A checkbox for 'Favor RIP Routes, over static routes' is present. The bottom of the window has OK, Cancel, and Help buttons.

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 LAN

In the sample configuration, IP Office was configured with the system name **DevCon IPO2** and LAN port was used to connect to RBS networks via the Internet. **LAN1** settings correspond to the LAN port on IP Office. To access **LAN1** settings, navigate to **System (1) → DevCon IPO2** in Navigation Pane then in 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., **10.10.97.39**.
- Set the **IP Mask** field to the subnet mask of the public network, e.g., **255.255.255.240**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.

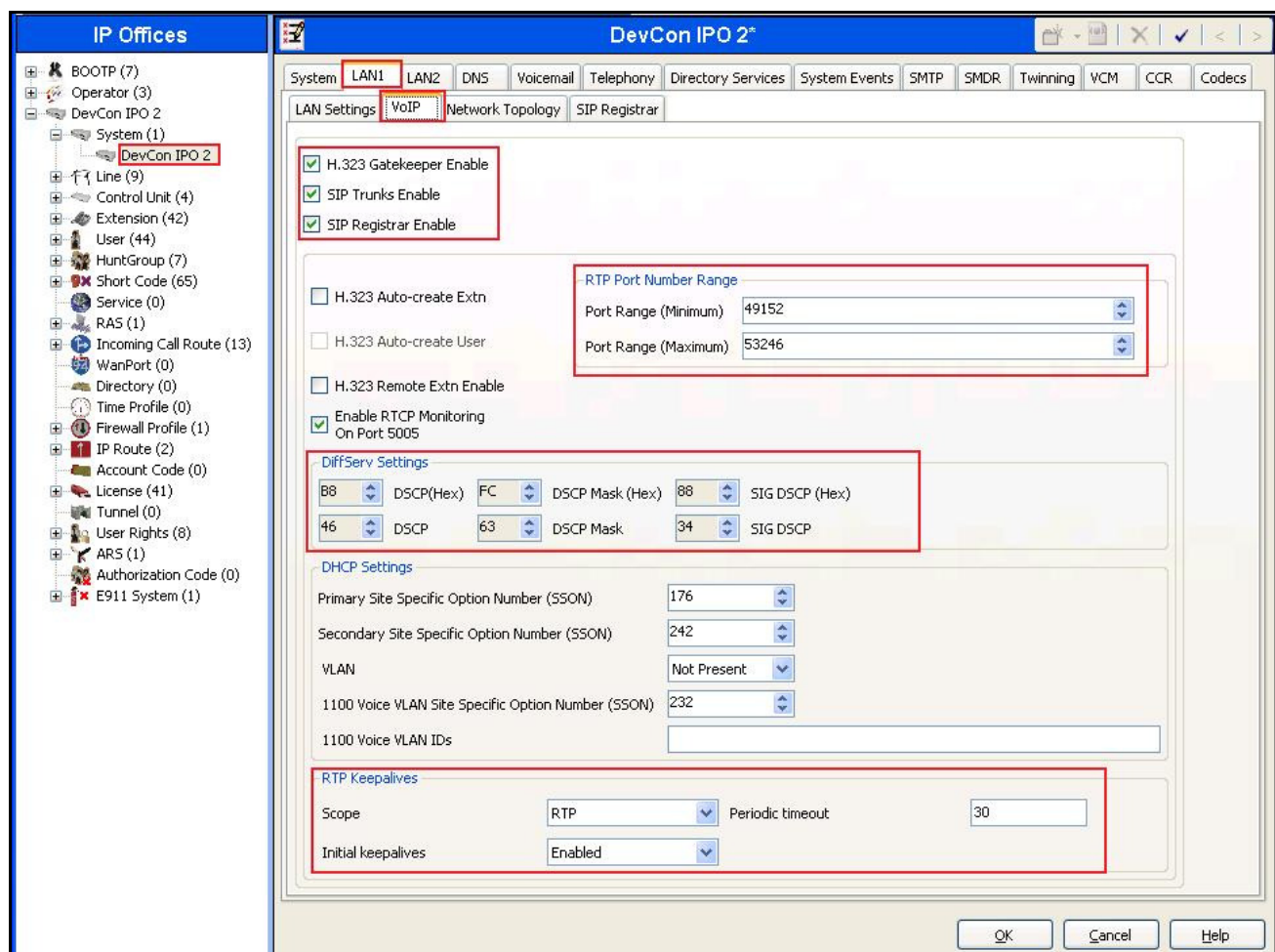
The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'DevCon IPO 2' selected. The main pane is titled 'DevCon IPO 2*' and contains several tabs: 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN1' tab is active, and within it, the 'LAN Settings' sub-tab is selected. The 'LAN Settings' form contains the following fields and values:

IP Address	10 . 10 . 97 . 39
IP Mask	255 . 255 . 255 . 240
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
Enable NAT	<input type="checkbox"/>
Number Of DHCP IP Addresses	2
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled

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

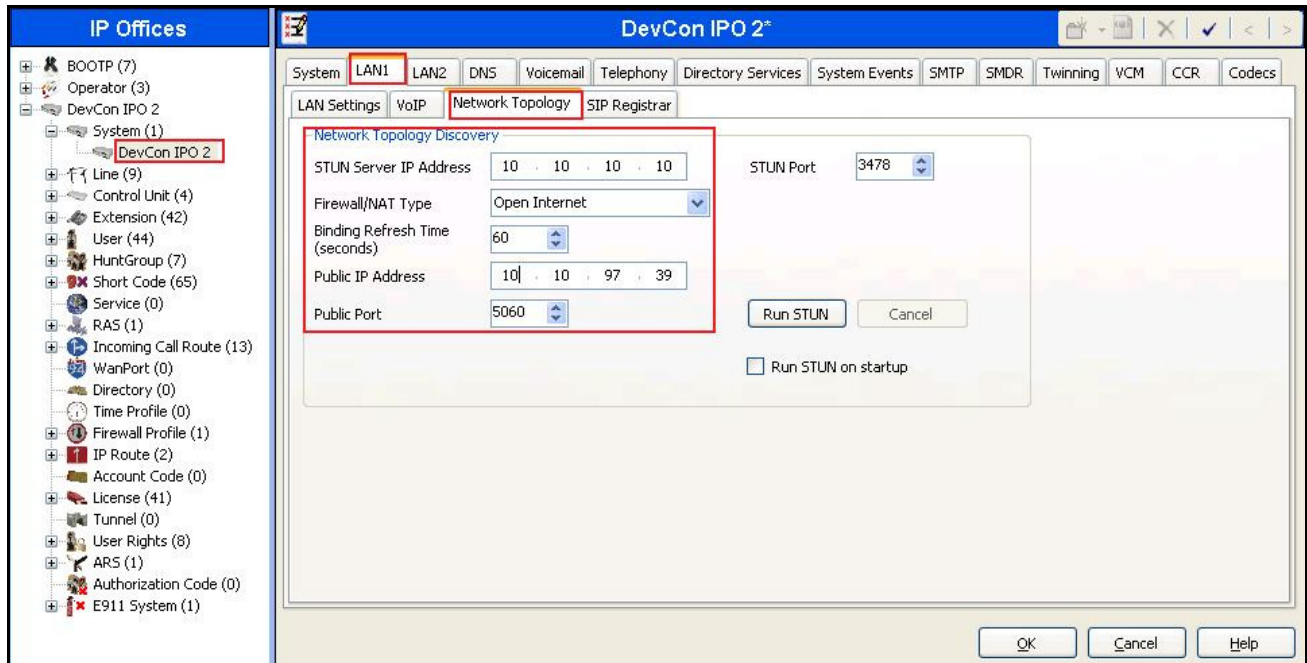
The **VoIP** tab as shown in the screenshot below was configured with following settings.

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphones using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to RBS.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphones to register using the SIP protocol.
- 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.
- Verify the **DiffServ Settings** were kept as default for the Differentiated Services Code Point (DSCP) parameters in the IP packet headers to support Quality of Services policies for both signaling and media, the **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling.
- Verify **RTP Keepalives** settings were enabled with **Scope** as **RTP**, **Periodic timeout** in **30** seconds, and **Initial keepalives** as **Enabled**. This allows IP Office to send IP packets to keep the active RTP session alive in every 30 seconds if there is no audio detected on the SIP Trunk.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.



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 **60**. This value is used to determine the frequency that IP Office will send OPTIONS heartbeat to the service provider.
- Set the **Public IP Address** to IP Office LAN IP address, e.g., **10.10.97.39**.
- Set the **Public Port** is set to **5060**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.



5.2 IP Route

IP Route settings include an IP Route **0.0.0.0** on LAN1 connecting to the Avaya SBCE for SIP, RTP traffics to RBS and connecting to the private enterprise networks.

To create an IP Route, select **IP Route** in the Navigation Pane, then click “**Create a New Record**” icon (not shown).

The IP Routes were configured using the following settings.

- Set the **IP Address** to the address of the destination network.
- Set the **IP Mask** to the subnet mask of the destination network.
- Set the **Gateway IP Address** to the IP address of the enterprise gateway that routes traffic to the destination network.
- Set the **Destination** to the interface **LAN1**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.

The following screenshot shows the IP Route **0.0.0.0** that was created on **LAN1** for SIP and RTP traffics to RBS via the Avaya SBCE. **LAN1** was assigned to the network address **0.0.0.0** and default subnet mask **0.0.0.0**. The default gateway was set to IP address **10.10.97.33** which is an internal gateway on the enterprise network that connects to **LAN1**.

The screenshot displays the configuration for an IP Route with the title bar showing '0.0.0.0'. On the left, the 'IP Offices' navigation pane shows a tree structure where 'IP Route (2)' is selected, and the specific route '0.0.0.0' is highlighted. The main configuration area contains the following fields:

- IP Address:** 0 . 0 . 0 . 0
- IP Mask:** 0 . 0 . 0 . 0
- Gateway IP Address:** 10 . 10 . 97 . 33
- Destination:** LAN1 (selected from a dropdown menu)
- Metric:** 1 (selected from a dropdown menu)
- Proxy ARP:** ☐ (unchecked)

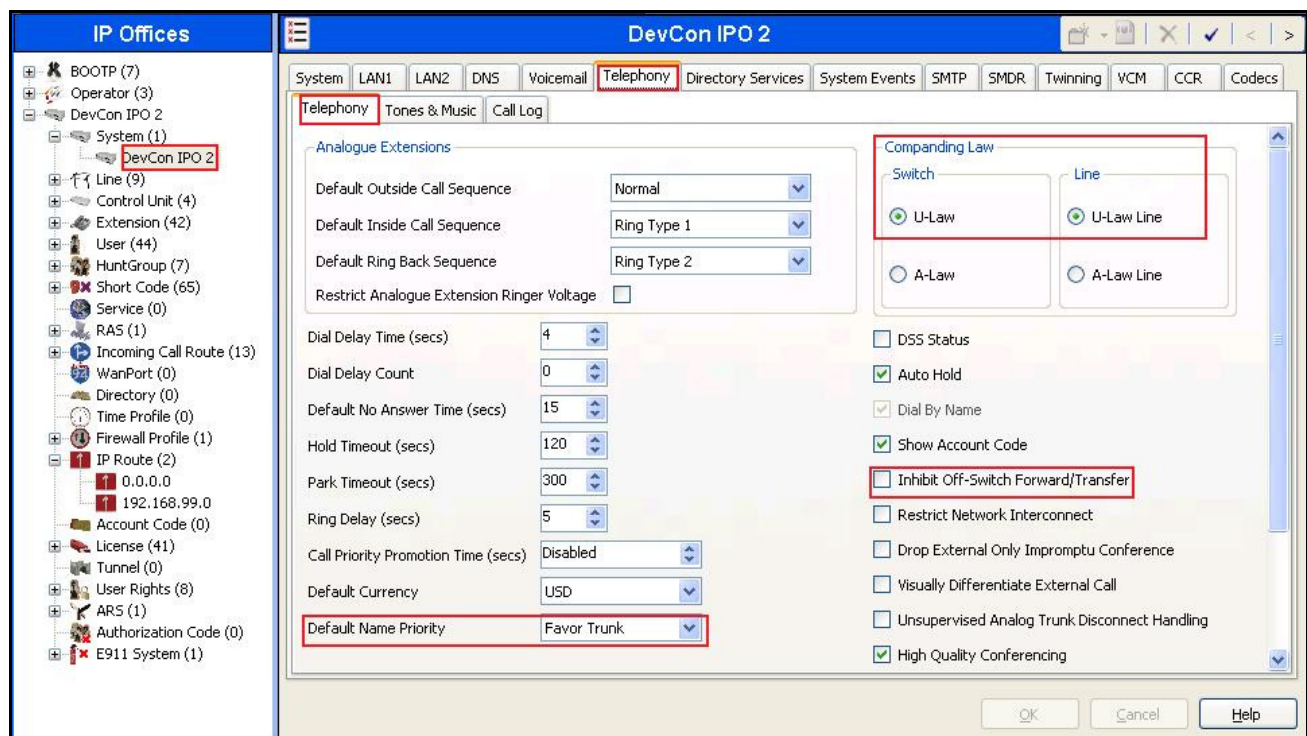
At the bottom of the window are three buttons: 'OK', 'Cancel', and 'Help'.

5.3 System Telephony and Codecs

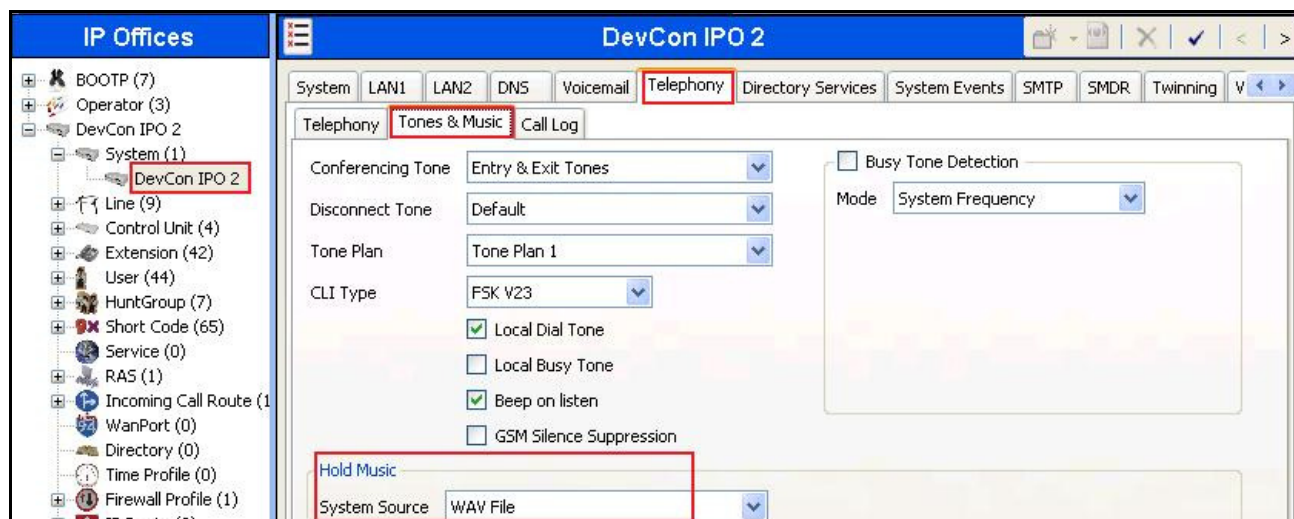
Navigate to the **System (1) → DevCon IPO2** in the Navigation Pane then select **Telephony** → **Telephony** tab in the Details Pane.

The **Telephony** settings were configured with following parameters.

- Choose the **Companding Law** typical for the enterprise location. For North America, **U-LAW** was used for both **Switch** and **Line**.
- Set **Default Name Priority** to **Favor Trunk**. This allows IP Office to use information received from SIP Trunk for call display purpose rather than overriding it with pre-defined internal settings.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to PSTN via the service provider SIP Trunk.
- Click OK to commit (not shown) then press Ctrl + S to save.



Under **Tones & Music** tab as shown below, **Hold Music** was configured with **System Source** to use **WAV File** which is an uploaded medium to provide Music on Hold on the SIP Trunk.



For **Codecs** settings, navigate to the **System (1) → DevCon IPO2** in the Navigation Pane, and then select **Codecs**. The **Codecs** settings are shown in the screenshot below with G.729 and G.711MU were selected. In the compliance testing, RBS supported both G.729 and G.711MU.



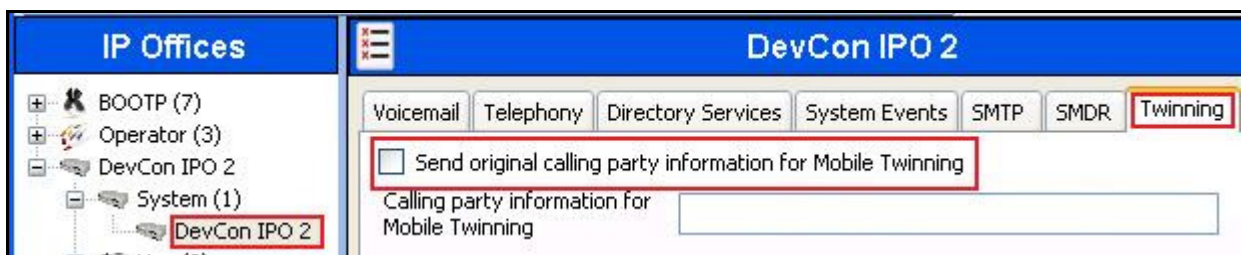
Click OK to commit (not shown) then press Ctrl + S to save.

5.4 Twinning Calling Party Information

When using Twinning, Calling Party Number displayed on the twinned phone is controlled by two parameters. The first parameter is the **Send original calling party information for Mobile Twinning** box on the **System→Twining** tab. The second parameter is the **Send Caller ID** parameter on the **SIP Line** form shown in **Section 5.5.1**.

For the compliance testing, the **Send original calling party information for Mobile Twinning** as shown below was unchecked. This setting allows **Send Caller ID** parameter that was set to **Diversion Header** in **Section 5.5** to be used. IP Office will send the following in the “From” header:

- On calls from an internal extension to a twinned phone, IP Office sends Calling Party Number of the originating extension.
- On calls from the PSTN to a twinned phone, IP Office sends Calling Party Number of the originating PSTN party.



5.5 Administer SIP Line

A SIP Line was needed to establish the SIP Trunk between IP Office and RBS.

To create a SIP Line, navigate to **Line** in the left Navigation Pane then select **New → SIP Line** (not shown).

5.5.1 Administer SIP Line Settings

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

- Set the **Line Number** to an unassigned number, e.g., **19**.
- Set the **ITSP Domain Name** to the FQDN or IP address that will be used as the enterprise SIP domain so that IP Office uses this domain as the URI-Host of the “From”, “P-Asserted-Identity” and “Diversion” headers. In the compliance testing, the enterprise SIP domain was defined as **avayalab.com** for the internal traffic between IP Office and the Avaya SBCE. This domain will be changed by Topology-Hiding configured on the Avaya SBCE (see **Section 6.2.3**) to the public IP address of the Avaya SBCE **10.10.98.106**, it is to meet the requirement from RBS.
- Set the **Send Caller ID** to **Diversion Header**. For the compliance testing, this parameter was used for Caller ID since **Send original calling party information for Mobile Twinning** was unchecked in **Section 5.4**.
- Set the **Association Method** to **By Source IP address**. This setting allows IP Office to apply the configuration for the public SIP Trunk to incoming and outgoing calls from/ to RBS if the traffics were originated from/ to the pre-defined IP address of the far end proxy server which is the internal IP address of the Avaya SBC.

- Uncheck the **REFER Support**, since RBS does not supported REFER method.
- Set the **UPDATE Supported** field to **Allow** as RBS supported the UPDATE method in this certification testing.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will send the OPTIONS heartbeat to check status of the SIP Trunk.
- Set the **Call Routing Method** field to **Request URI**.
- Set the **Name Priority** field to **System Default**.
- Check the **Call ID from From header** box.
- Default values may be used for all other parameters.
- Click OK to commit (not shown) then press Ctrl + S to save.

The screenshot displays the 'SIP Line - Line 19*' configuration window in Avaya IP Office. The left sidebar shows a tree view of the system configuration, with 'Line (9)' expanded and 'Line 19' selected. The main configuration area is divided into several sections:

- Line Information:** Line Number is set to 19, and ITSP Domain Name is set to avayaalab.com.
- Service Status:** In Service is checked, and Check OOS is checked.
- Call Routing:** Call Routing Method is set to Request URI.
- Name Priority:** Name Priority is set to System Default.
- Caller ID:** Call ID from From header is checked.
- Send From In Clear:** Send From In Clear is unchecked.
- User-Agent and Server Headers:** This section is currently empty.
- Send Caller ID:** Send Caller ID is set to Diversion Header.
- Association Method:** Association Method is set to By Source IP address.
- REFER Support:** REFER Support is unchecked.
- Incoming/Outgoing:** Incoming and Outgoing are both set to Auto.
- UPDATE Supported:** UPDATE Supported is set to Allow.

At the bottom right, there are buttons for OK, Cancel, and Help.

5.5.2 Administer Transport Settings

Select the **Transport** tab then configure the parameters as shown below.

- The **ITSP Proxy Address** was set to the internal IP Address of the Avaya SBCE **10.10.97.174** as shown in **Figure 1**.
- In the **Network Configuration** area, **UDP** was selected as the **Layer 4 Protocol** and the **Send Port** was set to **5060** which is the port that the Avaya SBCE opens for SIP traffic.
- The **Use Network Topology Info** parameter was set to **LAN 1**. This associates the SIP Line 19 with the parameters in the **System → LAN1 → Network Topology** tab.
- The **Calls Route via Registrar** was unchecked. In this certification testing, RBS did not support the dynamic Registration on the SIP Trunk.
- Other parameters retain default values.
- Click OK to commit (not shown) then press Ctrl + S to save.

The screenshot displays the 'SIP Line - Line 19*' configuration window. On the left, the 'IP Offices' tree shows a hierarchy including 'Line (9)' with sub-items 1, 2, 17, 18, 19, 20, 21, 22, and 23. Item 19 is selected and highlighted with a red box. The main configuration area has several tabs: 'SIP Line', 'Transport' (selected), 'SIP URI', 'VoIP', 'T38 Fax', and 'SIP Credentials'. The 'Transport' tab contains the following settings:

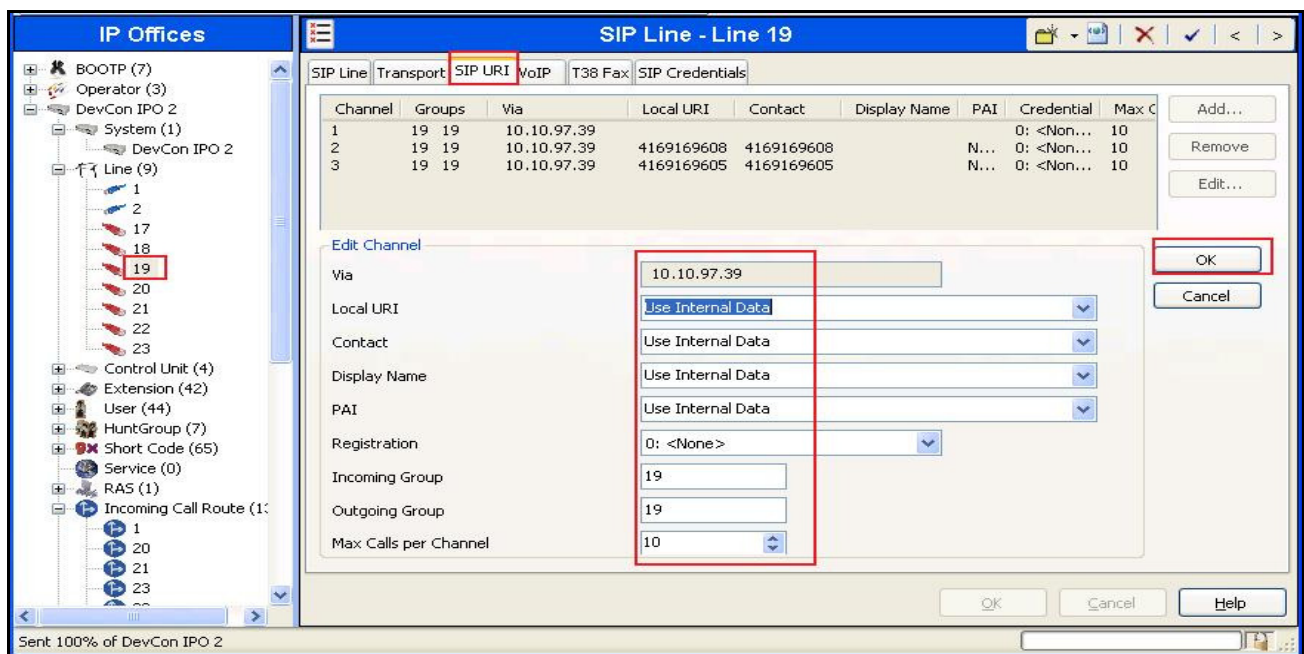
- ITSP Proxy Address:** 10.10.97.174 (highlighted with a red box)
- Network Configuration:**
 - Layer 4 Protocol:** UDP (dropdown menu)
 - Send Port:** 5060 (spin box)
 - Use Network Topology Info:** LAN 1 (dropdown menu)
 - Listen Port:** 5060 (spin box)
- Explicit DNS Server(s):** 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0
- Calls Route via Registrar:** ☐ (unchecked, highlighted with a red box)
- Separate Registrar:** (empty text field)

5.5.3 Administer SIP URI Settings

SIP URIs entry must be created to match Calling Party Number for incoming calls or to present Calling Party Number for outgoing calls on the SIP Line. Select the **SIP URI** tab then click the **Add** button and the **New Channel** area will appear at the bottom of the pane (not shown). To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button (not shown). In the example screenshot below, previously configured entries were edited.

For the compliance testing, SIP URI entry with **Channel 1** was created for incoming and outgoing calls. Its parameters are shown below:

- Set the **Local URI**, **Contact**, **Display Name** and **PAI** to **Internal Data**. This setting will use Calling Party Number defined under the **SIP** tab of **User** as shown in **Section 5.7** for the public SIP calls.
- For the **Registration** field, select **<None>** to disable the Registration.
- Associate SIP Line 19 to the **Incoming Group** and **Outgoing Group**. The line group number will be used in defining incoming or outgoing call routes for this SIP Line.
- Set the **Max Calls per Channel** to **10** which is the number of simultaneous SIP calls that are allowed using this SIP URI pattern.



SIP URI entry **Channel 2** and **Channel 3** were similarly created for incoming calls appropriately to pre-define DID numbers **4169169608** and **4169169605** to access to Feature Name Extension 00 (FNE00) and Voicemail respectively. The Short Codes for FNE00 was defined in **Section 5.6** to provide Dial Tone and Mobile Callback for mobility extension.

The **Channel 2** as shown in the screenshot below, was configured with following parameters.

- Set the **Local URI** and **Contact** fields to pre-define DID number **4169169608** appropriately for **Channel 2**.
- Associate **Incoming Group** and **Outgoing Group** to SIP Line 19.

- Set the **Max Calls per Channel** field to **10**.
- Other parameters retain default values.
- Click OK to commit.

SIP URI entry for **Channel 2** and **Channel 3** are shown below respectively:

The screenshot shows the 'SIP Line - Line 19' configuration window. The 'SIP URI' tab is selected. The 'Edit Channel' section is highlighted with a red box, showing the following values:

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max C
1	19 19	10.10.97.39					0: <Non...	10
2	19 19	10.10.97.39	4169169608	4169169608		N...	0: <Non...	10
3	19 19	10.10.97.39	4169169605	4169169605		N...	0: <Non...	10

The 'Edit Channel' section shows the following values:

Via	10.10.97.39
Local URI	4169169608
Contact	4169169608
Display Name	Use Internal Data
PAI	None
Registration	0: <None>
Incoming Group	19
Outgoing Group	19
Max Calls per Channel	10

The 'OK' button is highlighted with a red box.

The screenshot shows the 'SIP Line - Line 19' configuration window. The 'SIP URI' tab is selected. The 'Edit Channel' section is highlighted with a red box, showing the following values:

Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Credential	Max C
1	19 19	10.10.97.39					0: <Non...	10
2	19 19	10.10.97.39	4169169608	4169169608		N...	0: <Non...	10
3	19 19	10.10.97.39	4169169605	4169169605		N...	0: <Non...	10

The 'Edit Channel' section shows the following values:

Via	10.10.97.39
Local URI	4169169605
Contact	4169169605
Display Name	Use Internal Data
PAI	None
Registration	0: <None>
Incoming Group	19
Outgoing Group	19
Max Calls per Channel	10

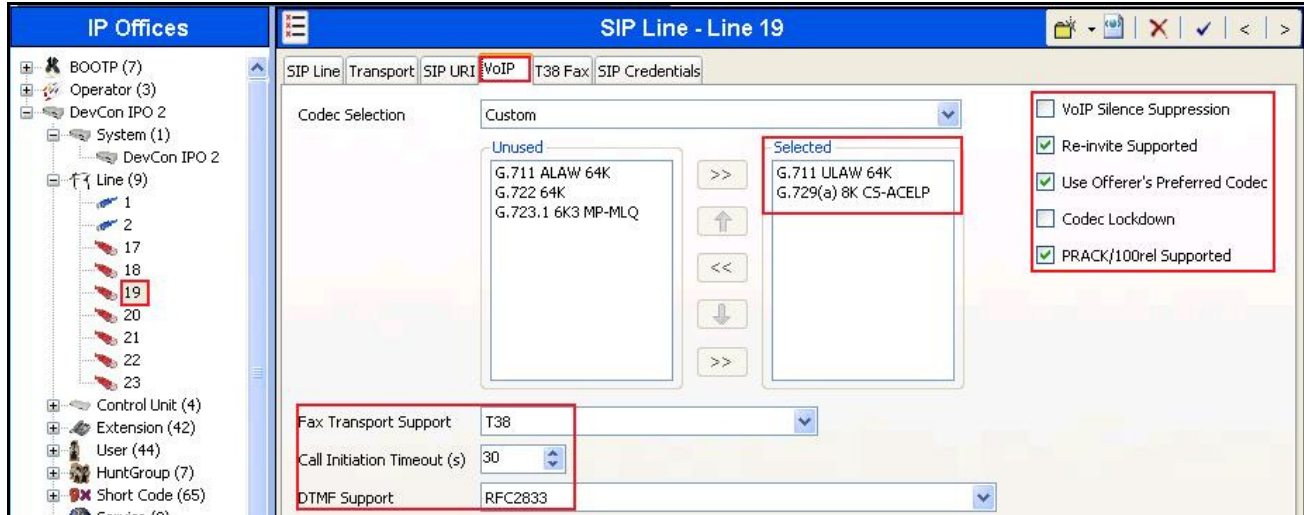
The 'OK' button is highlighted with a red box.

Click OK to commit (not shown) then press Ctrl + S to save.

5.5.4 Administer VoIP Settings

Select the **VoIP** tab then set the Voice over Internet Protocol parameters of the SIP Line as following:

- The **Codec Selection** can be selected by choosing **Custom** from the pull-down menu to use the System Codecs as defined in **Section 5.3**. The codec order was configured as **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** which are supported by RBS. IP Office includes these codes in the right prioritized order in the Session Description Protocol (SDP) offer or answer defined for the RTP traffic.
- Set the **Fax Transport Support** to **T.38** from the pull-down menu.
- Set the **Call Initiation Timeout (s)** to **30** seconds to allow a long enough duration for a public call to be established over the SIP Trunk.
- Set the **DTMF Support** to **RFC2833** from the pull-down menu. This directs IP Office to send out-of-band DTMF tones using RTP events per RFC 2833.
- Uncheck the **VoIP Silence Suppression** box. By unchecking the **VoIP Silence Suppression** box, calls can be established with the G.729 codec but without silence suppression.
- Check the **Re-invite Supported** box.
- Check **Use Offerer's Preferred Codec** box.
- Uncheck **Codec Lockdown** box.
- Check the **PRACK/100rel** because RBS supported the "100rel" signaling as described in RFC 3262.
- Default values may be used for all other parameters.
- Click OK to commit (not shown) then press Ctrl + S to save.



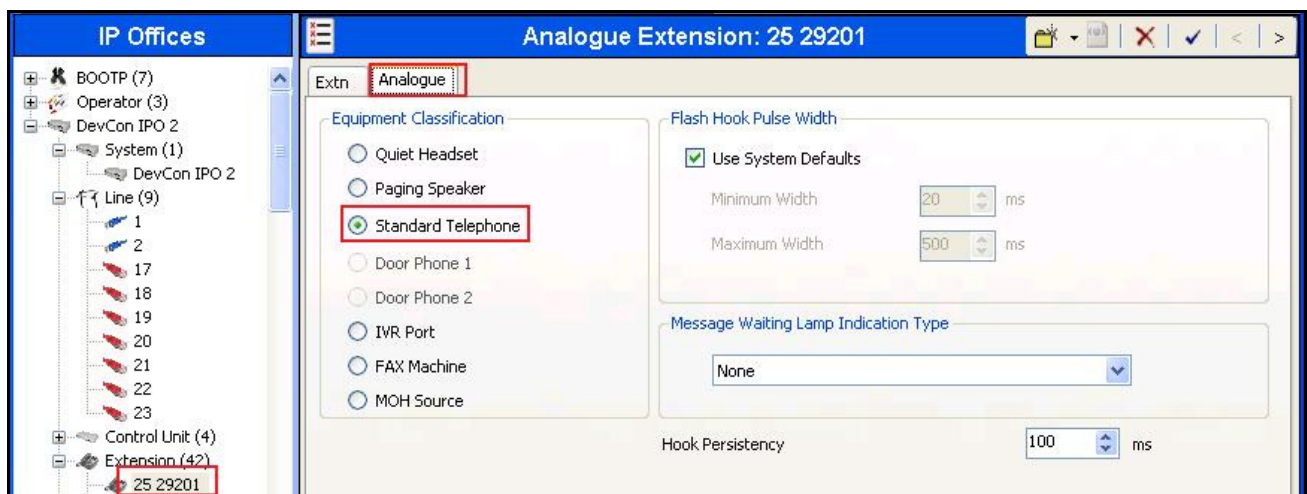
5.5.5 Administer T38 Fax Settings

Select the **T38 Fax** tab then check the **Use Default Values** to retain the default settings for T38 Fax (not shown).

Note: In this testing, the configuration for IP Office to work with RBS SIP trunk service in Fax T.38 mode, the analog extension (where the fax equipment is connected to) is being configured as follow: Navigate to **Extension** in the left Navigation Pane then select an Analog Extension, **25 29201**. On the **Extn** tab on the Details Pane confirm the settings are as shown.



Select **Analogue** tab on the Details Pane, confirm the settings are as shown.



5.6 Short Code

Short Codes were defined to route general outgoing calls and private outgoing calls to PSTN over the SIP Line, incoming calls from mobility extension to access FNE hosted on IP Office or incoming calls to retrieve voice message on IP Office VoiceMail Pro.

To create a short code, select **Short Code** in the left Navigation Pane then right-click and select **New** (not shown). On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created.

The screenshot below shows the details of the Short Code **9N;** that was created for outgoing calls in the test configuration. The digit **9** was used as a prefix that IP Office user will dial to access to SIP Trunk for outgoing calls to PSTN.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, it is **9N;**. This short code will be invoked when the user dials **9** followed by any number.
- Set the **Feature** to **Dial**. This is the feature that the short code will invoke.
- Set the **Telephone Number** to **N"@avayalab.com"**. This field is used to construct the "Request URI" and "To" headers of outgoing calls. The value **N** represents the number dialed by the user. The host part following the "@" is the enterprise SIP domain.
- Set the **Line Group ID** field to **19** which is the outgoing line group number defined on the **SIP URI** tab of the **SIP Line** in **Section 5.5.1**. This short code will use this line group when placing outgoing calls.
- Set **Locale** to **United State (US English)**.

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' navigation pane lists various extensions, with '9N;' highlighted. The main area shows the 'Short Code' configuration for '9N;: Dial'. The configuration fields are as follows:

Field	Value
Code	9N;
Feature	Dial
Telephone Number	N"@avayalab.com"
Line Group ID	19
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

For incoming calls from mobility extension to FNE features hosted by IP Office to provide **Dial Tone** functionality, Short Code **FNE00** was created. The **FNE00** was configured with the following parameters.

- In the **Code** field, enter the FNE feature code as **FNE00** for **Dial Tone**.
- Set the **Feature** field to **FNE Service**.
- Set the **Telephone Number** field to **00** for **FNE00**.
- Set the **Line Group ID** field to **0**.
- Retain default values for other fields.

Following screenshots illustrate **FNE00** configuration.

The screenshot displays the IP Office configuration interface. On the left, the 'IP Offices' tree shows a list of short codes, with 'FNE00' highlighted in a red box. The main panel is titled 'FNE00: FNE Service' and contains the following configuration fields:

Short Code	
Code	FNE00
Feature	FNE Service
Telephone Number	00
Line Group ID	0
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.7 User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line as defined in **Section 5.5**. To configure these settings, first select **User** in the left Navigation Pane, and then select the name of the user to be modified. In the example below, with the user **Extn29237** selected, select the **SIP** tab in the Details Pane.

- The values entered for the **SIP Name** and **Contact** fields are used as the URI-User in the “From” header for outgoing calls. They also allow matching of URI-User for incoming calls without having to enter this number as an explicit SIP URI for the SIP Line (see **Section 5.5**). The **SIP Name** and **Contact** fields were set to one of the DID numbers assigned to the enterprise by RBS, e.g., **4169169608**.
- The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name, e.g., **RCx9608**. If all calls involving this user and a SIP Line should be considered private
- The **Anonymous** box may be checked to withhold the user information from the networks.

The screenshot shows the Avaya SIP configuration interface. On the left, the 'IP Offices' pane displays a tree structure with 'Extension (42)' and 'User (44)'. Under 'User (44)', several users are listed, including '29237 Extn29237', which is highlighted with a red box. On the right, the 'Extn29237: 29237' details pane is shown with tabs for 'Mobility', 'Phone Manager Options', 'Hunt Group Membership', 'Announcements', and 'SIP'. The 'SIP' tab is selected and highlighted with a red box. Within the 'SIP' tab, the 'SIP Name' field contains '4169169608', the 'SIP Display Name (Alias)' field contains 'RCx9608', and the 'Contact' field contains '4169169608'. These three fields are grouped by a red box. Below these fields, the 'Anonymous' checkbox is visible and unchecked, also highlighted with a red box.

Mobile Twinning feature may be enabled on the user to allow incoming calls to simultaneously alert the desk phone and the mobile phone. The following screenshot shows the **Mobility** tab.

- The **Mobility Features** and **Mobile Twinning** boxes were checked.
- The **Twinned Mobile Number** was configured with the number to reach the twinned mobile telephone, in this case it was **91613XXX5279** including digit 9 as the dial access code and 1613XXX5279 as the mobility extension.
- Check **Mobile Call Control** to allow incoming call from mobility extension to access FNE00 (see **Section 5.6**).
- Other options can be set according to customer requirements.

The screenshot displays the Avaya UIMS interface for configuring extension 29237. The left pane shows a tree view of IP Offices with extension 29237 highlighted. The right pane shows the configuration for extension 29237, with the Mobility tab selected. The Mobility Features section is checked, and the Twinned Mobile Number is set to 96139675279. The Mobile Call Control and Mobile Callback options are also checked.

Section	Option	Value
Internal Twinning	Internal Twinning	<input type="checkbox"/>
	Twinned Handset	<None>
	Maximum Number of Calls	1
	Twin Bridge Appearances	<input type="checkbox"/>
Mobility Features	Mobility Features	<input checked="" type="checkbox"/>
	Mobile Twinning	<input checked="" type="checkbox"/>
	Twinned Mobile Number (including dial access code)	96139675279
	Twinning Time Profile	<None>
	Mobile Dial Delay (secs)	2
	Mobile Answer Guard (secs)	0
	Hunt group calls eligible for mobile twinning	<input type="checkbox"/>
	Forwarded calls eligible for mobile twinning	<input type="checkbox"/>
	Twin When Logged Out	<input type="checkbox"/>
	one-X Mobile Client	<input type="checkbox"/>
Mobile Call Control	<input checked="" type="checkbox"/>	
Mobile Callback	<input checked="" type="checkbox"/>	

When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.8 Incoming Call Route

An Incoming Call Route maps an incoming call on a specific SIP Line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an Incoming Call Route, right click on the **Incoming Call Route** in the left Navigation Pane and select **New** (not shown). On the **Standard** tab of the Details Pane, enter the following parameters.

- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group ID** to SIP Line **19** as defined in **Section 5.5**.
- Set the **Incoming Number** to the DID number that associate to the internal extension.
- Set **Locale** to **United State (US English)**
- Default values can be used for all other fields.

The screenshot below shows Incoming Call Route **19 4169169607** configured to receive incoming call to DID number **4169169607** then alert local station **291227**.

The screenshot shows the 'Standard' tab of the Incoming Call Route configuration for SIP Line 19 4169169607. The left pane shows a tree view of IP Offices with 'Incoming Call Route (1)' expanded, and '19 4169169607' selected. The right pane contains the following fields:

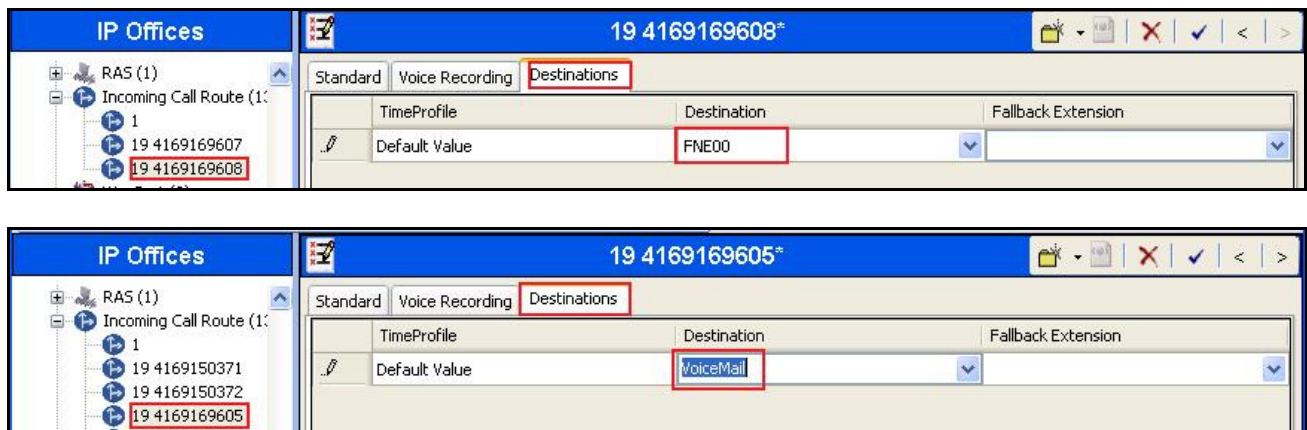
Field	Value
Bearer Capability	Any Voice
Line Group ID	19
Incoming Number	4169169607
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **4169169607** on SIP Line 19 are routed to extension **29237 Extn29237**.

The screenshot shows the 'Destinations' tab of the Incoming Call Route configuration for SIP Line 19 4169169607. The left pane shows the same tree view with '19 4169169607' selected. The right pane contains a table with the following data:

TimeProfile	Destination	Fallback Extension
Default Value	29227 Extn29227	

Following screenshots show Incoming Call Routes to receive incoming calls on DID number **4169169608** that similarly configured to access **FNE00** and **VoiceMail**. The **Destinations** were appropriately defined as FNE00 and VoiceMail. **Note:** FNE00 was entered manually by selecting **Destination** as **DialIn** (not shown) then input the appropriate FNE feature code.



When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.9 Privacy/Anonymous Calls

For outgoing calls with privacy (anonymous) enabled, IP Office will replace Calling Party Number in the “From” and “Contact” headers with “restricted” and “anonymous” respectively. IP Office can be configured to use the “P-Preferred-Identity” or “P-Asserted-Identity” header to pass the actual Calling Party information for authentication and billing purposes. For the compliance testing, the “P-Asserted-Identity” header was used.

To configure IP Office to use the “P-Asserted-Identity” header for private calls, navigate to **User** → **noUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button (not shown).

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

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



When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.10 Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screenshot to save the configuration performed in the preceding sections (not shown).

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** [4], [5] and [6].

The compliance testing comprised the configuration for two major components, 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 in the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - RBS:

- 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**.



AVAYA

Log In

Username:

Password:

Session Border Controller for Enterprise

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

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

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

© 2011 - 2012 Avaya Inc. All rights reserved.

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

Alarms
Incidents
Statistics
Logs
Diagnostics
Users
Settings
Help
Log Out

Session Border Controller for Enterprise

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

Dashboard

Information

System Time	09:47:44 AM GMT	Refresh
Version	6.2.0.Q30	
Build Date	Wed Dec 19 15:22:21 UTC 2012	

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

Add

Notes

No notes found.

Installed Devices

EMS

mSBCE

To view 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 **mSBCE** was already added. To view the configuration of this device, click the **View** as shown in the screenshot below.

Session Border Controller for Enterprise
AVAYA

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

System Management

Devices

Updates

SSL VPN

Licensing

Device Name (Serial Number)	Management IP	Version	Status	
mSBCE (IPCS21020002)	10.10.98.70	6.2.0.Q30	Commissioned	Reboot Shutdown Restart Application View Edit 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: mSBCE

X

General Configuration

Appliance Name

mSBCE

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
135.10.97.174	10.10.97.174	255.255.255.192	10.10.97.129	A1
135.10.98.106	10.10.98.106	255.255.255.224	10.10.98.97	B1

DNS Configuration

Primary DNS

10.10.98.60

Secondary DNS

DNS Location

DMZ

DNS Client IP

10.10.97.174

Management IP(s)

IP

10.10.98.70

6.2 Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.2.1 Uniform Resource Identifier (URI) Groups

URI Group feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

To add an URI Group, select **Global Profiles → URI Groups** and click on the **Add Group** button (not shown).

In the compliance testing, URI Group **RC** was added with URI type as **Regular Expression**. It consists of the following:

- Enterprise SIP domains “***.avaya.com**” for regular calls.
- “***.anonymous.invalid**” for private calls.
- IP address based service provider SIP domains “***.20.148.33.40**” and “***.10.10.98.106**”.
- IP addresses based URI-Host of the OPTIONS heartbeat originated by IP Office “***.10.10.97.39**” and “***.10.10.97.174**”.

The URI-Group **RC** was used to match the “From” and “To” headers in a SIP call dialog received from both IP Office and RBS. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see Section 6.2.2) and Server Flow (see Section 6.4.4) to route incoming and outgoing calls to the right destinations.

The screenshot below illustrates the URI listing for URI Group **RC**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'URI Groups' highlighted. The main content area is titled 'URI Groups: RC' and includes an 'Add' button. Below this, there is a list of URI Groups: 'URI Groups', 'MTSAllstream', 'RC' (highlighted with a red box), and 'Emergency'. The 'RC' group is selected, and its configuration is shown. A blue bar at the top of the configuration area says 'Click here to add a description.' Below this, the 'URI Listing' table is displayed, showing a list of URIs with 'Edit' and 'Delete' buttons for each entry. The URIs listed are: *.10.10.97.174, *.10.10.97.39, *.10.10.98.106, *.20.148.33.40, *.avaya.com, and *.anonymous.invalid. The first two URIs are highlighted with a red box.

URI Listing	
*.10.10.97.174	Edit Delete
*.10.10.97.39	Edit Delete
*.10.10.98.106	Edit Delete
*.20.148.33.40	Edit Delete
*.avaya.com	Edit Delete
*.anonymous.invalid	Edit Delete

6.2.2 Routing Profiles

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing profiles include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

To create a Routing profile, select **Global Profiles → Routing** then click on the **Add Profile** button (not shown).

In the compliance testing, Routing profile **To_RC** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) defined for IP Office. This entry is to route outgoing calls from the enterprise to RBS.

On the opposite direction, Routing profile **To_IPO_97_39** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) defined for RBS. This entry is to route incoming calls from RBS to the enterprise.

6.2.2.1 Routing Profile for RBS

To display **Edit Routing Rule** dialog of Routing profile **To_RC**, select **Global Profiles → Routing: To_RC**. As shown in the screenshot below, if there is a match on the SIP domain of the “To” header with the URI Group **RC** defined in **Section 6.2.1**, outgoing calls will be routed to the **Next Hop Server 1** as defined as **20.148.33.40** which is the IP address of RBS Trunk Server, on port **5060**. As shown in **Figure 1**, RBS SIP Trunking Service was connected with transportation protocol **UDP**. The other options were kept as default.

Edit Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group: RC

Next Hop Server 1: 20.148.33.40:5060

Next Hop Server 2:

Routing Priority based on Next Hop Server: ☒

Use Next Hop for In Dialog Messages: ☐

Ignore Route Header for Messages Outside Dialog: ☐

NAPTR: ☐

SRV: ☐

Outgoing Transport: ☐ TLS ☐ TCP ☒ UDP

Finish

6.2.2.2 Routing Profile for Avaya IP Office

Similarly, Routing profile **To_IPO_97_39** was created to route incoming calls to the **Next Hop Server 1** as defined as **10.10.97.39** which is the IP address of IP Office, on port **5060** if there is a match on the SIP domain of the “To” header with the URI Group **CL** defined in **Section 6.2.1**. As shown in **Figure 1**, IP Office was connected with transportation protocol **UDP**.

To display **Edit Routing Rule** dialog of Routing profile **To_IPO_97_39**, select **Global Profiles → Routing: To_IPO_97_39** then click **Edit** (not shown).

Note: The **Routing Priority based on Next Hop Server** was checked to use the default settings.

6.2.3 Topology Hiding

Topology Hiding is a security feature of the Avaya SBCE which allows changing certain key SIP message parameters to ‘hide’ or ‘mask’ how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding** then click on the **Add Profile** (not shown).

In the compliance testing, two Topology Hiding profiles were created: **To_RC** and **To_IPO_97_39**.

6.2.3.1 Topology Hiding Profile for RBS

Topology Hiding profile **To_RC** was defined for outgoing calls to RBS:

- Mask URI-Host of the “Request-URI” and “To” headers with service provider SIP domain **20.148.33.40** to meet the requirements of RBS.
- Mask URI-Host of the “From” header to service provider SIP domain **10.10.98.106**.
- Change the “Record-Route”, “Via” headers and SDP added by IP Office with external IP address known to RBS.

This implementation is to secure the enterprise network topology and also to meet the SIP requirements from the service provider.

The screenshots below illustrate the Topology Hiding profile **To_RC**.

The screenshot shows the Avaya Session Border Controller for Enterprise configuration interface. On the left, a sidebar lists various configuration categories, with 'Topology Hiding' highlighted. The main area is titled 'Topology Hiding Profiles: To_RC'. It features a list of profiles on the left, including 'default', 'cisco_th_profile', 'To_IPO', 'To_MTSAllstr...', 'To_IPO_97_39', and 'To_RC' (which is selected). The right pane shows the configuration for 'To_RC'. It includes a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	20.148.33.40
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	20.148.33.40
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	10.10.98.106

6.2.3.2 Topology Hiding Profile for IP Office

Topology Hiding profile **To_IPO_97_39** was defined for incoming calls to IP Office to:

- Mask URI-Host of the “Request-URI”, “To”, and “From” headers with the enterprise SIP domain **avayalab.com**.
- Change the “Record-Route”, “Via” headers and SDP added by RBS with internal IP address known to IP Office.

The screenshots below illustrate the Topology Hiding profile **To_IPO_97_39**.

The screenshot shows the Avaya Session Border Controller for Enterprise configuration interface. On the left, a sidebar lists various configuration categories, with 'Topology Hiding' highlighted. The main area is titled 'Topology Hiding Profiles: To_IPO_97_39'. It features a list of profiles on the left, including 'default', 'cisco_th_profile', 'To_IPO', 'To_MTSAllstr...', 'To_IPO_97_39' (which is selected), and 'To_CL'. The right pane shows the configuration for 'To_IPO_97_39'. It includes a table with the following data:

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

6.2.4 Server Interworking

Server Interworking profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **UC-Sec Control Center** → **Global Profiles** → **Server Interworking** then click on the **Add Profile** button (not shown). In the compliance testing,

two Server Interworking profiles **RC** and **IPO_97_39** were created for RBS (Trunk Server) and IP Office (Call Server).

6.2.4.1 Server Interworking Profile for RBS

Server Interworking profile **RC** was defined to match the specification of RBS. The **General** and **Advanced** tabs were configured with the following parameters while the other tabs **Timers**, **URI Manipulation** and **Header Manipulation** were kept as default. General settings are being set as shown in capture bellow. Others are left as default.

Editing Profile: RC

General

Hold Support: ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling: ☒ None ☐ SDP ☐ No SDP

181 Handling: ☒ None ☐ SDP ☐ No SDP

182 Handling: ☒ None ☐ SDP ☐ No SDP

183 Handling: ☒ None ☐ SDP ☐ No SDP

Refer Handling: ☐

3xx Handling: ☐

Diversion Header Support: ☐

Delayed SDP Handling: ☐

T.38 Support: ☒

URI Scheme: ☒ SIP ☐ TEL ☐ ANY

Via Header Format: ☒ RFC3261 ☐ RFC2543

Advanced settings are being set as shown in capture bellow and others are left as default.

Editing Profile: RC

Record Routes: ☐ None ☐ Single Side ☒ Both Sides

Topology Hiding: Change Call-ID: ☒

Call-Info NAT: ☐

Change Max Forwards: ☒

Include End Point IP for Context Lookup: ☐

OCS Extensions: ☐

AVAYA Extensions: ☐

NORTEL Extensions: ☐

Diversion Manipulation: ☐

Diversion Header URI:

Metaswitch Extensions: ☐

Reset on Talk Spurt: ☐

Reset SRTP Context on Session Refresh: ☐

Has Remote SBC: ☒

Route Response on Via Port: ☐

Cisco Extensions: ☐

Finish

6.2.4.2 Server Interworking Profile for IP Office

Server Interworking profile **IPO_97_39** shown in the screenshots below, was similarly defined to match the specification of IP Office with the exception of the support for **Avaya Extensions** was enabled.

Editing Profile: IPO_97_39

General

Hold Support: ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling: ☒ None ☐ SDP ☐ No SDP

181 Handling: ☒ None ☐ SDP ☐ No SDP

182 Handling: ☒ None ☐ SDP ☐ No SDP

183 Handling: ☒ None ☐ SDP ☐ No SDP

Refer Handling: ☐

3xx Handling: ☐

Diversion Header Support: ☐

Delayed SDP Handling: ☐

T.38 Support: ☒

URI Scheme: ☒ SIP ☐ TEL ☐ ANY

Via Header Format: ☒ RFC3261 ☐ RFC2543

Editing Profile: IPO_97_39

Record Routes: ☐ None ☐ Single Side ☒ Both Sides

Topology Hiding: Change Call-ID: ☒

Call-Info NAT: ☐

Change Max Forwards: ☒

Include End Point IP for Context Lookup: ☐

OCS Extensions: ☐

AVAYA Extensions: ☒

NORTEL Extensions: ☐

Diversion Manipulation: ☐

Diversion Header URI:

Metaswitch Extensions: ☐

Reset on Talk Spurt: ☐

Reset SRTP Context on Session Refresh: ☐

Has Remote SBC: ☒

Route Response on Via Port: ☐

Cisco Extensions: ☐

Finish

6.2.5 Server Configuration

Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create a Server Configuration entry, select **Global Profiles → Server Configuration** then click on the **Add Profile** button (not shown).

In the compliance testing, two separate Server Configurations were created, server entry **RC** for RBS and server entry **IPO_97_39** for IP Office.

6.2.5.1 Server Configuration for RBS

The Server Configuration **RC** was added for RBS, it is discussed in detail as below. The **General** and **Advanced** tabs were provisioned. The **Heartbeat** tab, however, was disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat originated from IP Office to RBS to query for the status of the SIP Trunk. The **Authentication** tab was also kept disabled as default. The **General** setting for Server Configuration **RC** is being set as shown in following capture.

The screenshot shows the 'Server Configuration: RC' page in the Avaya Session Border Controller for Enterprise. The left sidebar lists 'Global Profiles' with 'Server Configuration' highlighted. The main area shows the 'General' tab selected. The 'Server Profiles' list on the left includes 'IPO', 'MTSAlltream', 'IPO_97_39', and 'RC' (highlighted). The 'General' tab settings are as follows:

Setting	Value
Server Type	Trunk Server
IP Addresses / FQDNs	20.148.33.40
Supported Transports	UDP
UDP Port	5060

The Advanced setting is being set as shown in capture. Where the **RC** Interworking Profile is selected as defined in **Section 6.2.4.1**.

The screenshot shows the 'Server Configuration: RC' page in the Avaya Session Border Controller for Enterprise, with the 'Advanced' tab selected. The 'Server Profiles' list on the left includes 'IPO', 'MTSAlltream', 'IPO_97_39', and 'RC' (highlighted). The 'Advanced' tab settings are as follows:

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	RC
Signaling Manipulation Script	None
UDP Connection Type	SUBID

6.2.5.2 Server Configuration for Avaya IP Office

The Server Configuration **IPO_97_39** was similarly created for IP Office. It is discussed in detail as below. Only the **General** and **Advanced** tabs required provisioning. The **Heartbeat** tab was kept disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from RBS to IP Office to query for the status of the SIP Trunk. The **General** setting for Server Configuration **IPO_97_39** is being set as shown in following capture.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. On the left, a sidebar lists 'Global Profiles' including Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and 'Server Configuration' (highlighted with a red box). The main area is titled 'Server Configuration: IPO_97_39' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a 'Server Profiles' list with 'IPO' (selected), 'MTSAllstream', 'IPO_97_39' (highlighted with a red box), and 'CL'. The 'General' tab is active, displaying a table of settings: Server Type (Call Server), IP Addresses / FQDNs (10.10.97.39), Supported Transports (UDP), and UDP Port (5060). The 'Advanced' tab is also visible.

Server Type	Call Server
IP Addresses / FQDNs	10.10.97.39
Supported Transports	UDP
UDP Port	5060

The Advanced setting is being set as shown in capture. Where the **IPO_97_39** Interworking Profile is selected as defined in **Section 6.2.4.2**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface, specifically the 'Advanced' tab of the 'Server Configuration: IPO_97_39'. The 'Server Profiles' list on the left still has 'IPO_97_39' highlighted. The 'Advanced' tab is active, showing settings: 'Enable DoS Protection' (unchecked), 'Enable Grooming' (unchecked), 'Interworking Profile' (IPO_97_39, highlighted with a red box), 'Signaling Manipulation Script' (None), and 'UDP Connection Type' (SUBID).

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	IPO_97_39
Signaling Manipulation Script	None
UDP Connection Type	SUBID

6.3 Domain Policies

Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

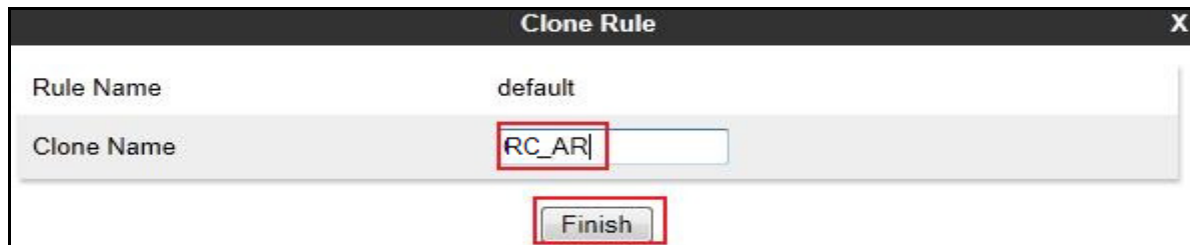
6.3.1 Application Rules

Application Rules define which types of SIP-based applications the Avaya SBCE security device will protect: voice, video, and/or instant messaging (IM). In addition, it is possible to configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

For the certification testing, Application Rule was created to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

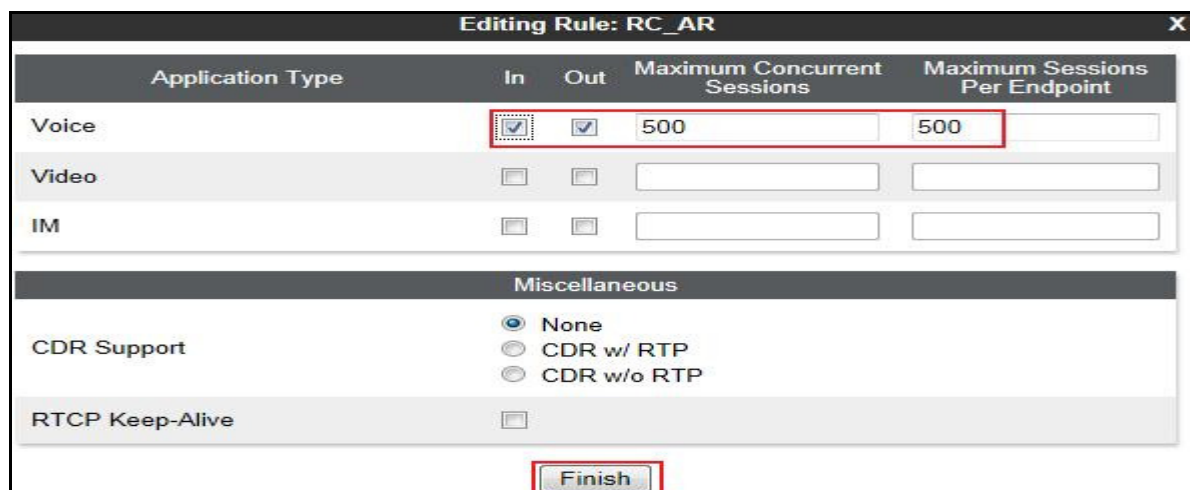
To clone an application rule, navigate to **Domain Policies → Application Rules**, select the default rule then click on the **Clone Rule** button (not shown).

Enter a descriptive name e.g., **RC_AR** for the new rule then click on the **Finish** button.



The screenshot shows a 'Clone Rule' dialog box. It has two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'RC_AR'. Below these fields is a 'Finish' button, which is highlighted with a red rectangular box.

Click **Edit** button (not shown) to modify the rule. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified Application Rule.



The screenshot shows the 'Editing Rule: RC_AR' dialog box. It contains a table with columns: 'Application Type', 'In', 'Out', 'Maximum Concurrent Sessions', and 'Maximum Sessions Per Endpoint'. The 'Voice' row is selected, and its 'In' and 'Out' checkboxes are checked. The 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint' fields for 'Voice' are both set to 500. Below the table is a 'Miscellaneous' section with radio buttons for 'CDR Support' (None, CDR w/ RTP, CDR w/o RTP) and a checkbox for 'RTCP Keep-Alive'. The 'Finish' button at the bottom is highlighted with a red rectangular box.

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, ☐ CDR w/ RTP, ☐ CDR w/o RTP

RTCP Keep-Alive: ☐

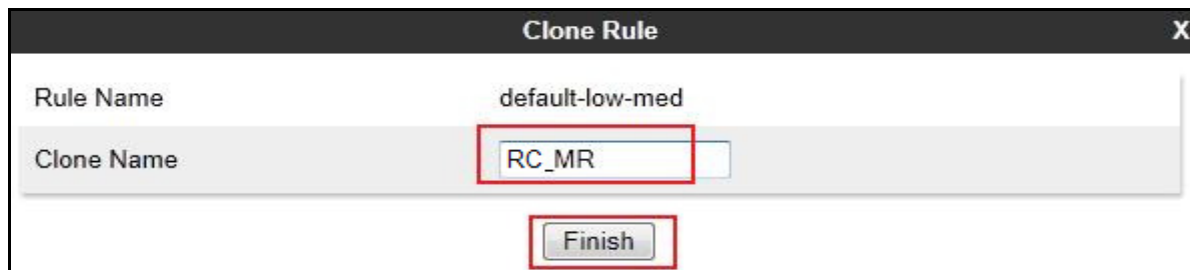
6.3.2 Media Rules

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

A custom Media Rule was created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration showed Media Rule **RC_MR** which was used for both the enterprise and RBS networks.

To create a **Media Rule**, navigate to **Domain Policies** → **Media Rules**, select the **default-low-med** rule then click on the **Clone Rule** button (not shown).

Enter a descriptive name e.g., **RC_MR** for the new rule then click on **Finish** button.

A screenshot of the 'Clone Rule' dialog box. It has a title bar with 'Clone Rule' and a close button 'X'. Inside, there are two input fields: 'Rule Name' with the value 'default-low-med' and 'Clone Name' with the value 'RC_MR'. The 'Clone Name' field is highlighted with a red rectangle. Below the fields is a 'Finish' button, also highlighted with a red rectangle.

When the RTP changes when the call is in progress, the Avaya SBCE interprets this as an anomaly and an alert will be created in the **Incidents Log**. Disabling **Media Anomaly Detection** could prevent the **RTP Injection Attack** alerts from being created in the log when the audio attributes change.

To modify Media Anomaly, select the **Media Anomaly** tab and click on the **Edit** button (not shown). Then uncheck **Media Anomaly Detection** and click on the **Finish** button.

A screenshot of the 'Media Anomaly' dialog box. It has a title bar with 'Media Anomaly' and a close button 'X'. Inside, there is a checkbox labeled 'Media Anomaly Detection' which is currently checked. The checkbox is highlighted with a red rectangle. Below it is a 'Finish' button, also highlighted with a red rectangle.

On the Avaya SBCE, Media Silencing feature detects the silence when the call is in progress. If the silence is detected and exceeds the allowed duration, the Avaya SBCE generates alert in the **Incidents Log**. In the compliance testing, the Media Silencing detection was disabled to prevent the call from unexpectedly disconnected due to a RTP packet lost on the public Internet.

To modify Media Silencing, select the **Media Silencing** tab and click on the **Edit** button (not shown). Then uncheck **Media Silencing** and click on the **Finish** button.

A screenshot of the 'Media Silencing' dialog box. It has a title bar with 'Media Silencing' and a close button 'X'. Inside, there is a checkbox labeled 'Media Silencing' which is currently checked. The checkbox is highlighted with a red rectangle. Below it is a 'Timeout' field with a text input and the label 'second(s)'. At the bottom is a 'Finish' button, also highlighted with a red rectangle.

Under **Media QoS** tab, click on the **Edit** button (not shown) to configure the Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP)

in the IP packet header with specific values to support Quality of Services policy for the media. The following screen shows the QoS values used for the compliance testing.

Media QoS

Media QoS Reporting

RTCP Enabled☐

Media QoS Marking

Enabled☒

ToS

Audio Precedence

Routine

000

Audio ToS

Minimize Delay

1000

Video Precedence

Routine

000

Video ToS

Minimize Delay

1000

DSCP

Audio

EF

101110

Video

EF

101110

Finish

6.3.3 Signaling Rules

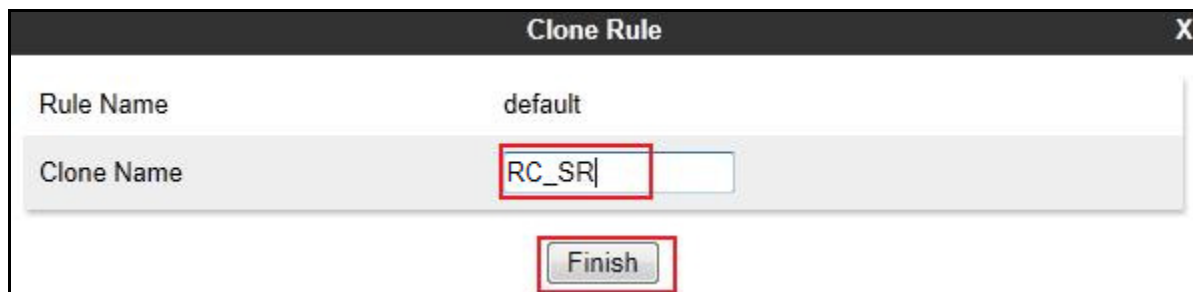
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined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

To clone a signaling rule, navigate to **Domain Policies** → **Signaling Rules**, select the **default** rule then click on the **Clone Rule** button (not shown).

In the compliance testing, two **Signaling Rules** were created for RBS and IP Office.

6.3.3.1 Signaling Rule for RBS

Clone a Signaling Rule with a descriptive name e.g., **RC_SR** and click on the **Finish** button.



The screenshot shows a 'Clone Rule' dialog box. It has a 'Rule Name' field with the value 'default'. Below it is a 'Clone Name' field with the value 'RC_SR'. At the bottom, there is a 'Finish' button. Red boxes highlight the 'Clone Name' field and the 'Finish' button.

Cloning the Signaling Rule default, verify that **General** settings of **RC_SR** with **Inbound** and **Outbound Request** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** (not shown).

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance testing.



The screenshot shows the 'Session Border Controller for Enterprise' interface. The left sidebar shows a tree view with 'Domain Policies' expanded and 'Signaling Rules' selected. The main area shows the configuration for 'Signaling Rules: RC_SR'. The 'Signaling QoS' tab is selected, showing a table with 'QoS Type' set to 'DSCP' and 'DSCP' set to 'EF'. Red boxes highlight the 'Signaling Rules' in the sidebar, the 'RC_SR' rule, and the 'Signaling QoS' tab and its content.

6.3.3.2 Signaling Rule for IP Office

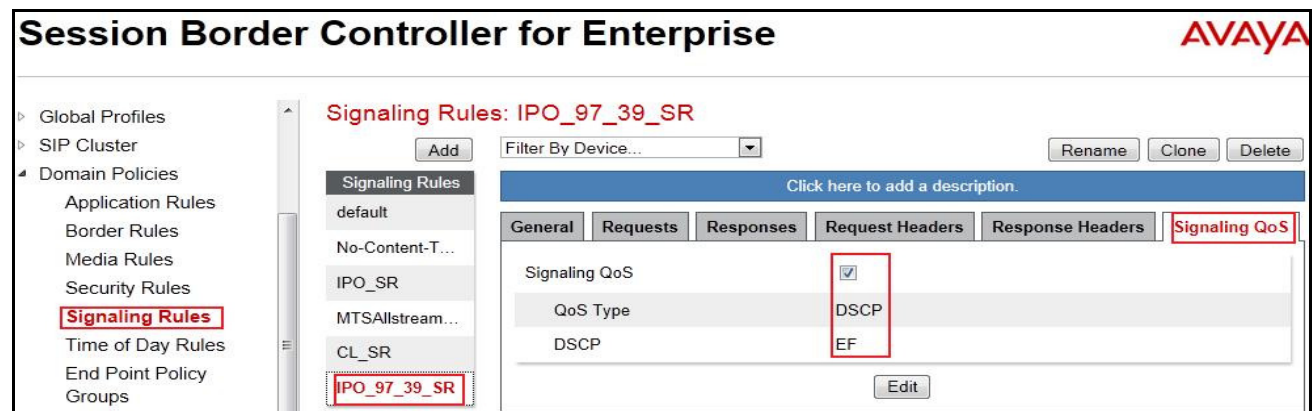
Clone a Signaling Rule with a descriptive name e.g., **IPO_97_39_SR** for IP Office and click on the **Finish** button.



The image shows a 'Clone Rule' dialog box. It has a title bar with 'Clone Rule' and a close button 'X'. Inside, there are two text input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'IPO_97_39_SR'. Below these fields is a 'Finish' button. Red boxes highlight the 'Clone Name' field and the 'Finish' button.

Cloning the Signaling Rule default, verify that **General** settings of **IPO_97_39_SR** with **Inbound** and **Outbound Request** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** (not shown).

Similarly the Signaling QoS rules are set as shown in Figure bellow.



The image shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation tree with 'Signaling Rules' highlighted. The main area is titled 'Signaling Rules: IPO_97_39_SR'. It contains a list of signaling rules: 'default', 'No-Content-T...', 'IPO_SR', 'MTSAllstream...', 'CL_SR', and 'IPO_97_39_SR'. The 'IPO_97_39_SR' rule is selected. To the right of the list are buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'. Below the list is a tabbed interface with tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'Signaling QoS' tab is active. It shows a 'Signaling QoS' checkbox which is checked, and a 'QoS Type' dropdown menu set to 'DSCP'. Below that, a 'DSCP' dropdown menu is set to 'EF'. There is an 'Edit' button at the bottom right of the 'Signaling QoS' tab.

6.3.4 Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to Server Flow defined in **Section 6.4.4**.

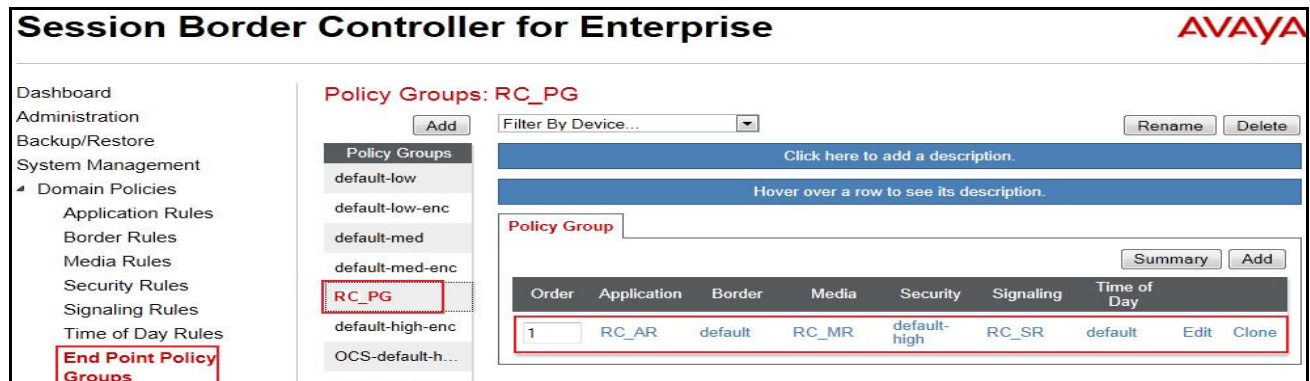
Endpoint Policy Groups were separately created for RBS and IP Office.

To create a policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on the **Add Group** button (not shown).

6.3.4.1 Endpoint Policy Group for RBS

The following screen shows **RC_PG** created for RBS.

- Set Application Rule to **RC_AR** which was created in **Section 6.3.1**.
- Set Media Rule to **RC_MR** which was created in and **Section 6.3.2**.
- Set Signaling Rule to **RC_SR** which was created in **Section 6.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.



Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Time of Day Rules
End Point Policy Groups

Policy Groups: RC_PG

Filter By Device...

Click here to add a description.

Hover over a row to see its description.

Policy Group

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	RC_AR	default	RC_MR	default-high	RC_SR	default	Edit Clone

6.3.4.2 Endpoint Policy Group for IP Office

The following screen shows policy group **IPO_97_39_PG** created for IP Office.

- Set Application Rule to **CL_AR** which was created in **Section 6.3.1**.
- Set Media Rule to **CL_MR** which was created in and **Section 6.3.2**.
- Set Signaling Rule **IPO_97_39_SR** which was created in **Section 6.3.3.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. On the left is a 'Dashboard' menu with 'Domain Policies' expanded, showing a list of policy groups. 'IPO_97_39_PG' is highlighted with a red box. The main area shows the configuration for 'Policy Groups: IPO_97_39_PG'. It includes an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename' and 'Delete' buttons. Below this is a table of policy groups with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The first row is highlighted with a red box and contains the following values: 1, RC_AR, default, RC_MR, default-low, IPO_97_39_SR, default. At the bottom of the table are 'Edit' and 'Clone' buttons.

6.3.5 Session Policy

Session Policy is applied based on the source and destination of a media session i.e., which codec is to be applied to the media session between its source and destination. The source and destination are defined in URI Group in **Section 6.2.1**.

In the compliance testing, the Session Policy **RC_SP** was created to match the codec configuration on RBS. The policy also allows the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.

To clone a common Session Policy which applies to both RBS and IP Office, navigate to **Domain Policies → Session Policies**, select the **default** rule then click on the **Clone Rule** button (not shown).

Enter a descriptive name e.g., **RC_SP** for the new policy and click on the **Finish** button.

The screenshot shows a 'Clone Policy' dialog box. It has two input fields: 'Policy Name' with the value 'default' and 'Clone Name' with the value 'RC_SP'. The 'Clone Name' field is highlighted with a red box. Below the fields is a 'Finish' button, also highlighted with a red box.

RBS supports both G.729 and G.711MU voice codecs in prioritized order and payload **101** for RFC2833/ DTMF. To define **Codec Prioritization** for **Audio Codec**, select the profile **CL_SP** created above, click on the **Edit** button (not shown). Select **Preferred Codec #1** as **PCMU (0)**, **Preferred Codec #2** as **G.729 (18)**, and **Preferred Codec #3** as **Dynamic (101)** for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent the unsupported codec from being sent to both ends.

Audio Codec	
Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input checked="" type="checkbox"/>
Preferred Codec #1	PCMU (0)
Preferred Codec #2	G729 (18)
Preferred Codec #3	Dynamic (101)
Preferred Codec #4	None
Preferred Codec #5	None

Video Codec	
Codec Prioritization	<input type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
Preferred Codec #1	CelB (25)
Preferred Codec #2	None
Preferred Codec #3	None
Preferred Codec #4	None
Preferred Codec #5	None

Finish

Under **Media** tab of the Session Policy **RC_SP** created above, click on the **Edit** button (not shown) then check on **Media Anchoring** to allow the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.

Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None

Finish

6.4 Device Specific Settings

Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

6.4.1 Network Management

Network Management page is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address, public IP address, subnet mask, gateway, etc. to interface the device to the networks. This information populates the various Network Management tabs which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management**, under **Network Configuration** tab, verify the IP addresses assigned to the interfaces and that the interfaces were enabled. The following screen shows the private interface was assigned to **A1** and the public interface was assigned to **B1** appropriate to the parameters shown in the **Figure 1**.

Session Border Controller for Enterprise AVAYA

▸ 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

Network Management: mSBCE

Devices
 mSBCE

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: 255.255.255.192 A2 Netmask: B1 Netmask: 255.255.255.224

IP Address	Public IP	Gateway	Interface	
10.10.97.174		10.10.97.129	A1	Delete
10.10.98.106		10.10.98.97	B1	Delete

On the **Interface Configuration** tab, enable the interfaces connecting to the inside enterprise and outside service provider networks. To enable an interface click it's **Toggle State** button. The following screen shows interface **A1** and **B1** were **Enabled**.

Session Border Controller for Enterprise

Network Management: mSBCE

Devices: mSBCE

Network Configuration: Interface Configuration

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

6.4.2 Media Interface

Media Interface screen is where the media ports are defined. The Avaya SBCE will open connection for RTP traffic on the defined ports.

To create a new **Media Interface**, navigate to **Device Specific Settings** → **Media Interface** and click on the **Add Media Interface** button (not shown).

Two separate Media Interfaces are needed for both the inside and outside interfaces. The following screen shows the Media Interfaces **InsideMedia** and **OutsideMedia** were created for the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.

Session Border Controller for Enterprise

Media Interface: mSBCE

Devices: mSBCE

Media Interface

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

Add

Name	Media IP	Port Range	
InsideMedia	135.10.97.174	35000 - 40000	Edit Delete
OutsideMedia	135.10.98.106	35000 - 40000	Edit Delete

6.4.3 Signaling Interface

Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP request on the defined port.

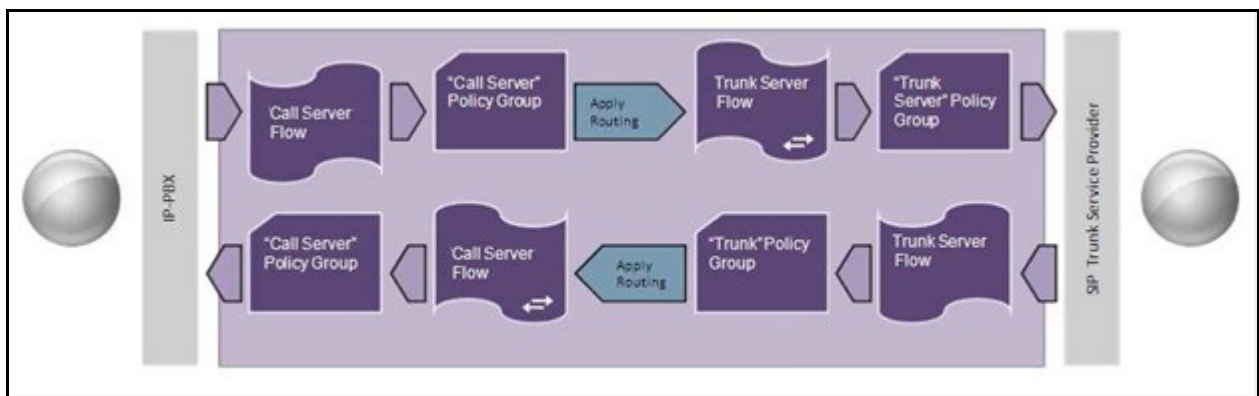
To create a new **Signaling Interface**, navigate to **Device Specific Settings → Signaling Interface** and click on the **Add Signaling Interface** button (not shown).

Two separate Signaling Interfaces are needed for both inside and outside interfaces. The following screen shows the Signaling Interfaces **InsideSIP** and **OutsideSIP** were created in the compliance testing with **TCP/5060** and **UDP/5060** respectively configured for inside and outside interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	10.10.97.174	---	5060	---	None	Edit Delete
OutsideSIP	10.10.98.106	---	5060	---	None	Edit Delete

6.4.4 End Point Flows - Server Flow

When a packet is received by the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to 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.



In the compliance testing, two separate Server Flows were created for RBS and IP Office.

To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the other fields were kept as default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 6.2.5** which the Server Flow associates to.
- **URI Group:** Select the URI Group **CL** created in **Section 6.2.1**.
- **Received Interface:** Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration is designed to send the SIP signaling to.
- **Media Interface:** Select the Media Interface created in **Section 6.4.2** which is the Server Configuration is designed to send the RTP to.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 6.3.4**.
- **Routing Profile:** Select the Routing Profile created in **Section 6.2.2** which is used to which is the Server Configuration is designed to route the calls to.
- **Topology Hiding Profile:** Select the Topology Hiding profile created in **Section 6.2.3** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows the Server Flow **RC** for RBS.

The screenshot displays the 'Edit Flow: RC' configuration window. The fields are as follows:

Field	Value
Flow Name	RC
Server Configuration	RC
URI Group	RC
Transport	*
Remote Subnet	*
Received Interface	InsideSIP
Signaling Interface	OutsideSIP
Media Interface	OutsideMedia
End Point Policy Group	RC_PG
Routing Profile	To_IPO_97_39
Topology Hiding Profile	To_RC
File Transfer Profile	None

The 'Finish' button is located at the bottom of the window.

The following screen shows the Server Flow **IPO_97_39** for IP Office.

Flow Name: IPO_97_39

Server Configuration: IPO_97_39

URI Group: RC

Transport: *

Remote Subnet: *

Received Interface: OutsideSIP

Signaling Interface: InsideSIP

Media Interface: InsideMedia

End Point Policy Group: IPO_97_39_PG

Routing Profile: To_RC

Topology Hiding Profile: To_IPO_97_39

File Transfer Profile: None

Finish

6.4.5 Session Flows

Session Flows feature allows defining certain parameters that pertain to the media portions of a call, whether it originates from the enterprise or outside the enterprise. This feature provides the complete and unparalleled flexibility to monitor, identify and control very specific types of calls based upon these user-definable parameters. Session Flows profiles SDP media parameters, to completely identify and characterize a call placed through the network.

A common Session Flow **RC_SF** was created for both the RBS and IP Office.

To create a Session Flow, navigate to **Device Specific Settings → Session Flows** then click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the remaining fields were kept as default.

- **Flow Name:** Enter a descriptive name.
- **URI Group #1:** Select the URI Group **RC** created in **Section 6.2.1** to assign to the Session Flow as the source URI Group.

- **URI Group #2:** Select the URI Group **RC** created in **Section 6.2.1** to assign to the Session Flow as the destination URI Group.
- **Session Policy:** Select the Session Policy **RC_SP** created in **Section 6.3.5** to assign to the Session Flow.
- Click on the **Finish** button.

Note: A unique URI Group is used for source and destination, since it contains multiple URIs defined for the source as well as for the destination.

The following screen shows the Session Flow named **RC_SF**.

Flow Name: RC_SF

URI Group #1: RC

URI Group #2: RC

Subnet #1: *
Ex: 192.168.0.1/24

Subnet #2: *
Ex: 192.168.0.1/24

Session Policy: RC_SP

Finish

7. RBS SIP Trunking Service Configuration

RBS is responsible for the configuration of RBS SIP Trunking Service. RBS will provide the customer with necessary information to configure SIP Trunk for the Avaya IP Office solution. The provided information from RBS includes:

- IP address of the RBS SIP proxy.
- DID numbers.
- Supported codecs.
- A customer specific SIP signaling reference.

The sample configuration between the enterprise and RBS for the compliance testing was a static configuration. There was no registration on the SIP Trunk implemented on either RBS or enterprise side.

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 activities are made to each test scenario:

- Verify that endpoints at the enterprise site can place calls to PSTN and that the call remains 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 the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an 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 Troubleshooting

8.3.1 IP Office System Status

The following steps may be used to verify the configuration.

- Use the Avaya IP Office System Status application to verify the state of the SIP connection. Launch the application from **Start → Programs → IP Office → System Status** on the PC where 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 (8)
Extensions (28)
Trunks (9)
 Line: 1
 Line: 2
 Line: 17
 Line: 18
Line: 19
 Line: 20
 Line: 21
 Line: 22
 Line: 23
Active Calls
Resources
Voicemail
IP Networking

Status Utilization Summary Alarms

SIP Trunk Summary

Peer Domain Name: avayalab.com
 Resolved Address: 10.10.97.174
 Line Number: 19
 Number of Administered Channels: 20
 Number of Channels in Use: 0
 Administered Compression: G711 Mu, G729 A
 Silence Suppression: Off
 SIP Trunk Channel Licenses: Unlimited
 SIP Trunk Channel Licenses in Use: 0
 SIP Device Features: UPDATE (Incoming and Outgoing)

0%

Channel Number	UR	Call Ref	Current State	Time in State	Remote Media A...	Co...	Conne...	Caller ID or Dial...	Other Party on Call	Direction of Call	Round Trip D...	Receive Jitter	Receive Packet...	Transmit Jitter	Transmit Packet...
1			Idle	3 days...											
2			Idle	3 days...											
3			Idle	3 days...											
4			Idle	3 days...											
5			Idle	3 days...											
6			Idle	3 days...											
7			Idle	3 days...											
8			Idle	3 days...											
9			Idle	3 days...											
10			Idle	3 days...											

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 (8)
Extensions (28)
Trunks (9)
 Line: 1
 Line: 2
 Line: 17
 Line: 18
Line: 19
 Line: 20
 Line: 21
 Line: 22
 Line: 23
Active Calls
Resources
Voicemail
IP Networking

Status Utilization Summary **Alarms**

Alarms for Line: 19 SIP avayalab.com

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

Ping Clear Clear All Print... Save As...

5:23:56 PM Online

8.3.2 Sniffer Traces Analysis

Using a network sniffing tool e.g., Wireshark to monitor the SIP signaling between the enterprise and RBS. The sniffer traces are captured at the public interface of the Avaya SBCE.

Following screenshots show an example incoming call from RBS to the enterprise.

- Incoming INVITE request from RBS.


```
INVITE sip:4169169605@10.10.98.106 SIP/2.0
Via: SIP/2.0/UDP 192.148.33.40:5060;branch=z9hG4bK6rcop2001g31ni4ur6h1.1
Max-Forwards: 68
To: <sip:4169169605@10.10.98.106:5060>
From: "16139675280" <sip:16139675280@192.148.33.40:5060>;tag=as384f7157
Call-ID: 4fcba3da5fd24fb33c4c0e003987fb3b@192.148.30.11
Contact: <sip:16139675280@192.148.33.40:5060;transport=udp>
CSeq: 102 INVITE
User-Agent: Rogers SIP Core
Remote-Party-ID: "16139675280" <sip:16139675280@192.148.30.11>;privacy=off;screen=no
Date: Fri, 17 May 2013 13:51:23 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
Supported: replaces
Content-Type: application/sdp
Content-Length: 277

v=0
o=root 338969693 338969693 IN IP4 192.148.33.40
s=Rogers SIP
c=IN IP4 192.148.33.40
t=0 0
m=audio 23072 RTP/AVP 0 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - - -
a=ptime:20
a=sendrecv
```

- 200OK response from the enterprise.

```
SIP/2.0 200 OK
From: "16139675280" <sip:16139675280@192.148.30.11>;tag=as384f7157
To: <sip:4169169605@10.10.98.106:5060>;tag=c10d14c985aeb23b
CSeq: 102 INVITE
Call-ID: 4fcba3da5fd24fb33c4c0e003987fb3b@192.148.30.11
Contact: "RCx9605" <sip:4169169605@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=120708;lr;transport=udp>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
Supported: timer,100rel
Via: SIP/2.0/UDP 192.148.33.40:5060;branch=z9hG4bK6rcop2001g31ni4ur6h1.1
Server: IP Office 8.1 (67)
Content-Type: application/sdp
Content-Length: 202

v=0
o=UserA 1444702547 4004390731 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 36728 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Following screenshots show an example outgoing call from the enterprise to RBS.

- Outgoing INVITE request from the enterprise.

```
INVITE sip:6139675258@192.148.33.40 SIP/2.0
From: "CLx9607" <sip:4169169607@10.10.98.106>;tag=8afc0e9561e572d3
To: <sip:6139675258@192.148.33.40>
CSeq: 1919735175 INVITE
Call-ID: 69d45f7ec202d4777903272b74b23636
Contact: "CLx9607" <sip:4169169607@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=120784;lr;transport=udp>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
Supported: timer,100rel
User-Agent: IP Office 8.1 (67)
Max-Forwards: 69
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-000285809090-1--s1632-
P-Asserted-Identity: "CLx9607" <sip:4169169607@10.10.98.106>
Content-Type: application/sdp
Content-Length: 249

v=0
o=UserA 4008471752 2564834054 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 36748 RTP/AVP 0 18 101
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

- Incoming 200OK response from RBS.

```
SIP/2.0 200 OK
From: "CLx9607" <sip:4169169607@10.10.98.106>;tag=8afc0e9561e572d3
To: <sip:6139675258@192.148.33.40>;tag=as0c73eachb
CSeq: 1919735175 INVITE
Call-ID: 69d45f7ec202d4777903272b74b23636
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-000285809090-1--s1632-
Record-Route: <sip:10.10.98.106:5060;ipcs-line=120784;lr;transport=udp>
Contact: <sip:6139675258@192.148.33.40:5060;transport=udp>
Server: Rogers SIP Core
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
Supported: replaces
Content-Type: application/sdp
Content-Length: 255

v=0
o=root 2128885401 2128885402 IN IP4 192.148.33.40
s=Rogers SIP
c=IN IP4 192.148.33.40
t=0 0
m=audio 21974 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - -
a=ptime:20
a=sendrecv
```

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise R6.2 to RBS SIP Trunking Service.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The RBS SIP Trunking Service is considered **compliant** with Avaya IP Office Release 8.1.

10. References

- [1] *IP Office 8.1 IP500/IP500 V2 Installation*, Document Number 15-601042, Issue 27f, 04 March 2013.
- [2] *IP Office 8.1 Manager FP1 10.1*, Document Number 15-601011, Issue 29t, 20 February 2013.
- [3] *IP Office 8.1 Administering Voicemail Pro*, Document Number 15-601063, Issue 8b, 11 December 2012.
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013.
- [5] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013.
- [6] *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 RBS SIP Trunking Service is available from RBS.

©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.