



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.2 with Axtel SIP Trunking Service– Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between the service provider Axtel and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya IP Office 9.0 and Avaya Session Border Controller for Enterprise 6.2.

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

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

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider Axtel and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya IP Office release 9.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) release 6.2 and various Avaya endpoints.

The Axtel SIP Trunking service referenced within these Application Notes is designed for business customers in Mexico. The service enables local and long distance PSTN calling via standards based SIP trunks as an alternative to legacy analog or digital trunks, without the need for additional TDM enterprise gateways and the associated maintenance costs.

The Avaya enterprise solution can be configured to authenticate with the SIP service provider using either SIP Trunk Registration or Static IP Authentication. Even though these Application Notes cover the configuration of the Avaya SBCE using SIP Trunk Registration for the authentication with Axtel, both authentication methods were successfully tested during the compliance tests.

2. General Test Approach and Test Results

A simulated enterprise site containing all the Avaya equipment for the SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Axtel SIP Trunking Service via a broadband connection to the public Internet.

The configuration shown in **Figure 1** was used to exercise the features 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.

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

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types. Phone types included SIP, H.323, digital and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included SIP, H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya IP Office Softphone.
- Inbound and outbound PSTN calls to/from Avaya Flare® Experience for Windows softphones.
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya Flare® Experience for Windows softphones.
- Various call types including: local, long distance national, outbound toll-free, local directory assistance, etc.
- Codecs G729A, G.711A and G.711U.
- G.711 Fax.
- Caller ID presentation and Caller ID restriction.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and twinning.

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test
- Operator services such as dialing 0 or 0 + 10 digits are not supported.
- T.38 fax is not supported.
- International long distance calls were restricted on the SIP trunk assigned for testing, hence they were not tested.

2.2. Test Results

Interoperability testing of the Axtel SIP Trunking service was completed with successful results for all test cases with the exception of the observations and limitations described below:

- **Call Transfer to the PSTN:** Racing conditions were observed when using Network Call Redirection with REFER messages. REFER was disabled in the IP Office SIP Line and it was not used during the tests. Call transfers still were able to complete, with the limitation that two channels on the SIP trunk were occupied for the total duration of the call.
- **“anonymous” on IP Office phones displays:** On outbound calls, the 200OK message sent from Axtel as a response to the INVITE sent by the enterprise, included a P-Asserted-Identity (PAI) header with an “anonymous; phone-context=unknown” parameter that made the display on the IP Office extensions (calling party) change from the called number to “anonymous”, after the calls was answered by the PSTN party. To avoid this, a Signaling Rule was created on the Avaya SBCE to remove the PAI header in the 200OK sent by Axtel for outbound calls.
- **Direct Media:** Direct media had to be disabled in the IP Office, by unchecking **Allow Direct Media Path** in the SIP Line/VoIP tab, to avoid a noticeable clipping that was observed on outbound calls at the beginning of the audio stream. This issue has been previously reported and it is currently under investigation by the IP Office team (JIRA IPOFFICE-52060).
- **Outbound Calling Party Number (CPN) Block:** When an IP Office user activated “Withhold Number” on an outbound call, IP Office sent From:“anonymous” and the “Privacy:id” headers as expected, but the caller ID on the receiving end at the PSTN still showed the main number assigned to the SIP trunk. This may be a requirement on the PSTN in Mexico and it is listed here just as an observation.
- **Caller ID on outbound calls:** On outbound calls, the caller ID number shown on the PSTN end was always the main number assigned to the SIP trunk by Axtel, regardless of the specific DID number sent in the origination headers from the IP Office.
- **Remote-Address:** During the compliance test, a Sigma script was created to remove the “Remote-Address” parameter, used by the Avaya SBCE, from all outbound messages to the SIP trunk. This parameter contains private enterprise IP addresses that have no significance to the service provider.

2.3. Support

For technical support on the Axtel SIP Trunking service offer, visit <http://www.axtel.mx/>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Axtel SIP Trunking service through a public Internet WAN connection.

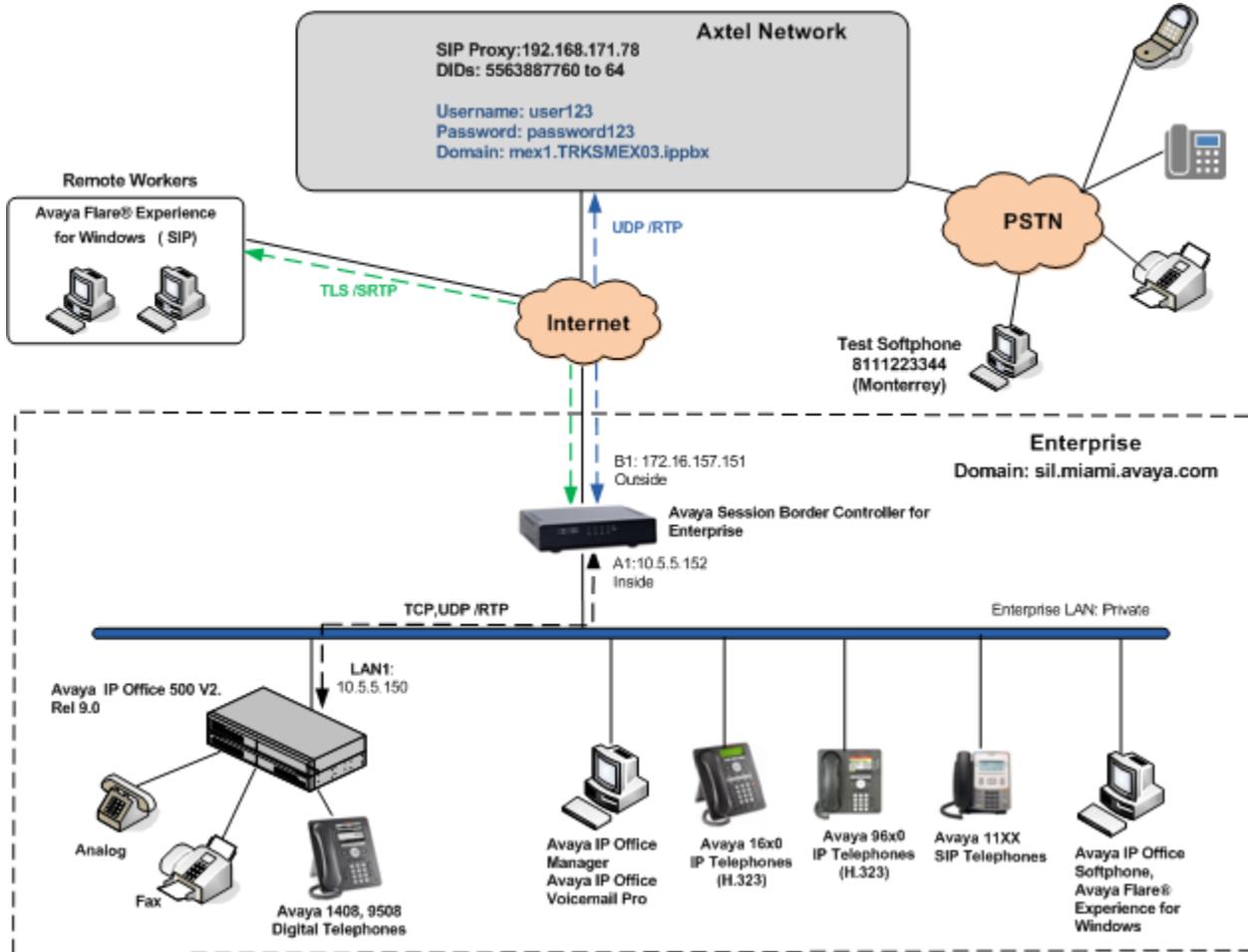


Figure 1: Test Configuration

Note that for security purposes, all public IP addresses, trunk credentials and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

The enterprise site contains the IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codecs. The LAN1 port of the IP Office is connected to the enterprise LAN. Endpoints include Avaya 1600 and 9600 Series IP Telephones (with H.323 firmware), Avaya 1140E IP Telephones (with SIP firmware), Avaya 1408 and 9508D Digital Telephones, analog telephones and PCs running Avaya IP Office Softphone and Avaya Flare® Experience for Windows. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the IP Office system, and Avaya Voicemail Pro providing voice messaging service to the IP Office users. Mobile Twinning is configured for some of the IP Office users so that calls to these users' extensions will also ring and can be answered at the configured mobile phones.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise LAN. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. Other functions of the Avaya SBCE include providing registration capability of the SIP trunk with the service provider, as well as performing network address translation at both the IP and SIP layers.

Additionally, the reference configuration included the support for IP Office soft-clients in a remote worker environment. This functionality was introduced with the software releases of Avaya IP Office 9.0 and the Avaya Session Border Controller for Enterprise (SBCE) 6.2. A remote worker is a SIP endpoint that resides in the untrusted network, registered to the IP Office at the enterprise via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint at the enterprise. The remote worker functionality was successfully tested during the compliance test. The Avaya Flare® Experience for Windows soft-client was used for this purpose, using Transport Layer Security (TLS) as the signaling protocol and Secure Real Time Protocol (SRTP) for the audio.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [9] in the **References** section for more information on this topic.

In an actual customer configuration, the enterprise site may include additional network components between the service provider and the Avaya SBCE, such as a router, data firewall, etc. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that all SIP and RTP traffic between the service provider and the IP Office system must be allowed to pass through these devices.

During the compliance test, in addition to the DID numbers assigned to the SIP trunk, Axtel provided a local test number in Monterrey, Mexico. A SIP-based softphone was registered to this local PSTN number and was used to originate and terminate local calls to and from the PSTN to the enterprise.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya IP Office 500v2	9.0.100.845
Avaya IP Office Digital Expansion Module DCPx16	9.0.100.845
Avaya IP Office Manager	9.0.100.845
Avaya IP Office Voicemail Pro	9.0.1.0.53
Avaya 1608 IP Telephone (H.323)	1.3 SP3
Avaya 9640 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.2
Avaya 1140E IP Telephone (SIP)	04.03.18.00
Avaya Digital Telephone 1408	32.0
Avaya Digital Phone 9508	0.45
Avaya IP Office Softphone	3.2.3.49.68975
Avaya Flare® Experience for Windows	1.1.4.23
Avaya Session Border Controller for Enterprise, on a Portwell CAD-0208 server	6.2.1.Q07
Axtel	
Sonus SBC 5200	V03.01.02R000
Genband CS2K	Release CVM 13

5. Configure Avaya IP Office

This section describes the IP Office configuration necessary to support connectivity to the Axtel SIP Trunking service. IP Office is configured through the Avaya IP Office Manager PC application. From the PC running IP Office Manager, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration** (not shown), select the proper IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one shown in the next section.

The appearance of the IP Office Manager can be customized using the **View** menu. In the screens 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 the IP Office configuration.

Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

5.1. Licensing

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

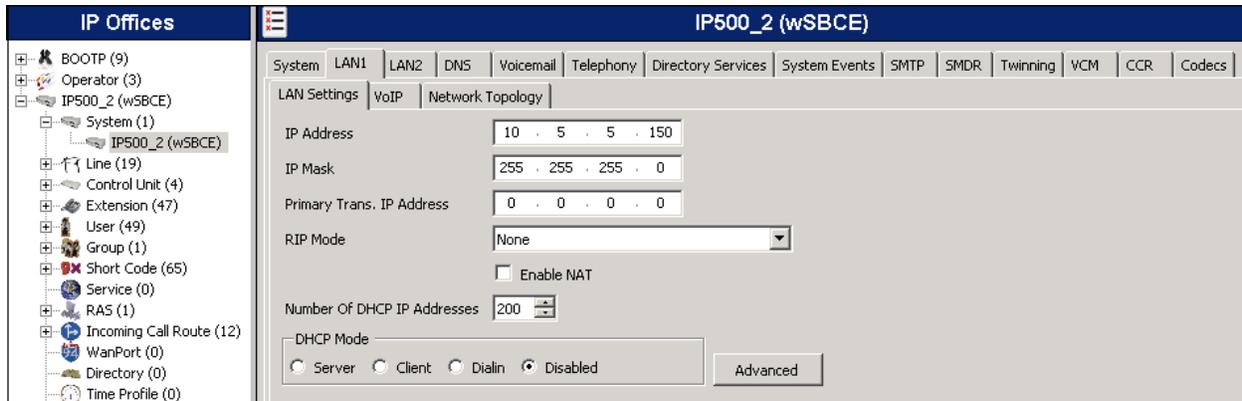
To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License** in the Navigation pane. Confirm that there is a valid license with sufficient “Instances” (trunk channels) in the Details pane. Note that the entries under **PLDS Host ID** and **License Key** in the screen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

The screenshot shows the 'IP Offices' configuration window with the 'License' tab selected. The 'Remote Server' license mode is active. The table below lists various licenses, with 'SIP Trunk Channels' highlighted in red. The 'PLDS Host ID' is 11132 and the license key is redacted.

Feature	License Key	Instances	Status	Expiry Date	Source
Conferencing Center	BK@z3Eb4vkt5TMLY59TH...	255	Obsolete	Never	ADI Nodal
Small Office Edition VCM (channels)	KtQJ_gvmXL8Nue4tu.Mcfr...	255	Obsolete	Never	ADI Nodal
Small Office Edition WiFi	NvaWRrdPEXq4OewjYs_m...	255	Obsolete	Never	ADI Nodal
IPSec Tunneling	OtxcaGo3EU1RvHPZWWHk...	255	Valid	Never	ADI Nodal
Proactive Reporting	tAW4bxVLSd@glvHGaSp5x...	255	Valid	Never	ADI Nodal
Report Viewer	XvxJ0Jyv9vRthD7ARs7Ak...	255	Valid	Never	ADI Nodal
Mobility Features	@KNCJmBkEsmjtPwgk7Qw...	255	Obsolete	Never	ADI Nodal
Advanced Small Community Networking	MTaeb8BrE5EVnprxz7ao7...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	ynBHHuBRtVeoIKrrgpzO1M...	255	Valid	Never	ADI Nodal
IP500 Upgrade Standard to Profession...	IyKkoG5MPOX1Un6sARex...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	@qDn5LuvjjuksrCZuDiZ...	4	Valid	Never	ADI Nodal
VCM Channel Migration	z4Muuvv5vhhizpna8Khw...	255	Valid	Never	ADI Nodal
SIP Trunk Channels	uanDkYmVAOpf@p7hNxC...	255	Valid	Never	ADI Nodal
VPN IP Extensions	54OUJF56XGxvnrPjfm77w...	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional chan...	nqWAZqSGDjwABE_WECM...	255	Valid	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	oIcZqPmYADjmOgQbkEmq...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Standard E...	PxZD74gwLkebFHgQUim6...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Profession...	FUM5FmHLV_9na92GVm5...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Stand...	6ZIo8R5vASPYngH8KM6ALL...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Profes...	kGYN0IsqQN_Xi06YJo_n9d...	255	Valid	Never	ADI Nodal
UMS Web Services	3JusJPBx0s9WwJgk0z16E...	255	Valid	Never	ADI Nodal
Customer Service Agent	FANcqb54gsalJ0p5jyL_cy...	255	Valid	Never	ADI Nodal
Third Party API	YnHxbxBcAqoFbuYkNMF...	255	Valid	Never	ADI Nodal
Software Upgrade 255	g4CSrd@d51Z2udk6oaol...	1	Valid	Never	ADI Nodal
one-X Portal for IP Office	LyahZn@pdtoM3IM_k@ejk...	255	Valid	Never	ADI Nodal
Avaya IP endpoints	pnv6WRmStz8DGA3g6p9m...	255	Valid	Never	ADI Nodal
Customer Service Supervisor	d4mgkoroYQId0GA3g6p9m...	255	Valid	Never	ADI Nodal
Essential Edition Additional Voicemal ...	Vtcm_LdgVX3QahSTA8fw3...	255	Valid	Never	ADI Nodal

5.2. LAN Settings

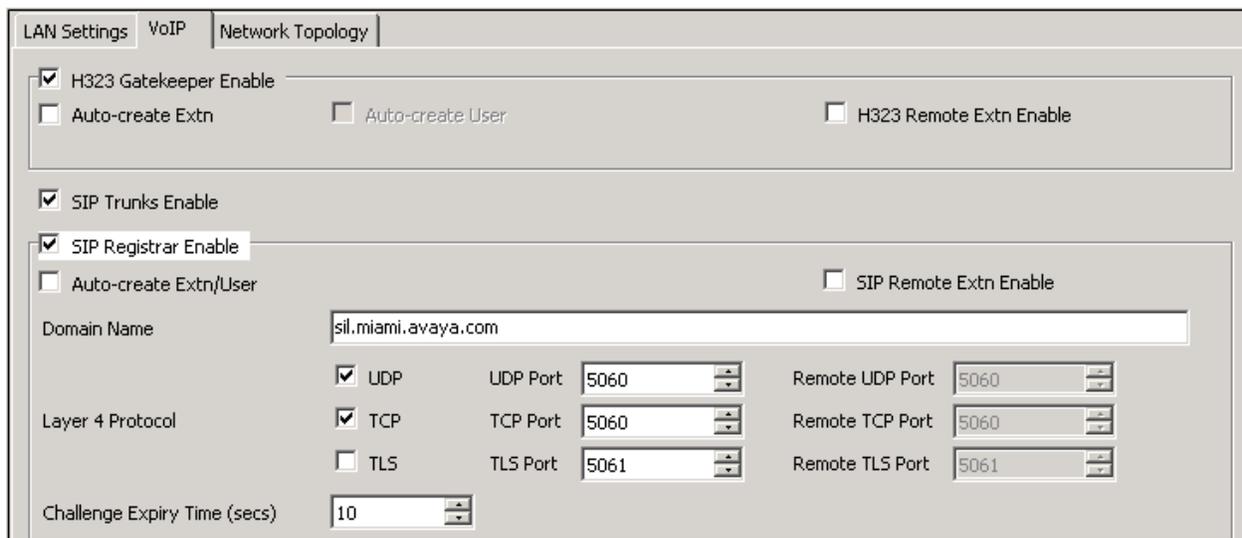
In the sample configuration, *IP500V2(w_SBCE)* was used as the system name, and the LAN1 port was used to connect the IP Office to the enterprise network. To access the LAN1 settings, first navigate to **System (1) → IP500V2(w_SBCE)** in the Navigation pane and select the **LAN1 → LAN Settings** tab in the Details pane. Set the **IP Address** field to the IP address assigned to the IP Office LAN1 port. Set the **IP Mask** field to the mask used on the public network. All other parameters should be set according to customer requirements.



The screenshot shows the configuration interface for IP500_2 (wSBCE). The left pane shows the navigation tree with 'IP500_2 (wSBCE)' selected. The right pane shows the 'LAN Settings' tab with the following fields:

- IP Address: 10 . 5 . 5 . 150
- IP Mask: 255 . 255 . 255 . 0
- Primary Trans. IP Address: 0 . 0 . 0 . 0
- RIP Mode: None
- Enable NAT:
- Number Of DHCP IP Addresses: 200
- DHCP Mode: Server Client Dialin Disabled

On the **VoIP** tab in the Details pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 1600 and 9600 Series IP Telephones present in the sample configuration. The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks on this interface. The **SIP Registrar Enable** box is checked to allow the registration of Avaya 1140E Telephones, Avaya Flare® Experience and Avaya IP Office Softphones using the SIP protocol. On the **Domain Name** field, the local SIP registrar domain name *sil.miami.avaya.com* was used. This domain name will need to be configured on the SIP endpoints in order to register with the system. On the **Layer 4 Protocol** section, the default **UDP** and **TCP** protocols and ports were used.



The screenshot shows the 'VoIP' tab configuration. The following options are checked:

- H323 Gatekeeper Enable
- SIP Trunks Enable
- SIP Registrar Enable

The Domain Name field contains: sil.miami.avaya.com

Layer 4 Protocol settings:

- UDP: UDP Port 5060, Remote UDP Port 5060
- TCP: TCP Port 5060, Remote TCP Port 5060
- TLS: TLS Port 5061, Remote TLS Port 5061

Challenge Expiry Time (secs): 10

The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Based on this setting, IP Office would request RTP media be sent to a UDP port in the configurable range for calls using LAN1.

IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. The specific values used for the compliance test are shown in the example below.

All other parameters should be set according to customer requirements.

The screenshot displays the configuration interface for IP Office, specifically the 'VoIP' tab under 'Network Topology'. The 'RTP' section includes:

- Port Number Range:** Minimum: 49152, Maximum: 53246
- Port Number Range (NAT):** Minimum: 49152, Maximum: 53246
- Enable RTCP Monitoring on Port 5005**
- Keepalives:**
 - Scope: Disabled
 - Periodic timeout: 0
 - Initial keepalives: Enabled

The **DiffServ Settings** section includes:

B8	DSCP(Hex)	B8	Video DSCP(Hex)	FC	DSCP Mask (Hex)	88	SIG DSCP (Hex)
46	DSCP	46	Video DSCP	63	DSCP Mask	34	SIG DSCP

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

- Select the **Firewall/NAT Type** from the pull-down menu to the option that matches the network configuration. Since no network address translation (NAT) was used in the compliance test, the parameter was set to ***Open Internet***. With this configuration, settings obtained by STUN lookups are ignored. The IP address used is the one assigned to the interface.
- Set **Binding Refresh Time (seconds)** to **180**. This value is used to determine the frequency at which IP Office will send SIP OPTION messages to the service provider.
- Defaults were used for all other fields.

LAN Settings | VoIP | Network Topology

Network Topology Discovery

STUN Server Address: 69.90.168.13 STUN Port: 3478

Firewall/NAT Type: Open Internet

Binding Refresh Time (seconds): 180

Public IP Address: 0 . 0 . 0 . 0 Run STUN Cancel

Public Port

UDP: 0

TCP: 0

TLS: 0

Run STUN on startup

5.3. System Telephony Settings

Navigate to the **Telephony** → **Telephony** Tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. In Mexico, **A-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.

The screenshot displays the configuration page for IP500_2 (wSBCE). The 'Telephony' tab is selected, and the 'Companding Law' section is visible. The 'Switch' section has 'A-Law' selected, and the 'Line' section has 'A-Law Line' selected. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked. Other settings include 'Dial Delay Time (secs)' at 4, 'Dial Delay Count' at 0, 'Default No Answer Time (secs)' at 15, 'Hold Timeout (secs)' at 0, 'Park Timeout (secs)' at 300, 'Ring Delay (secs)' at 5, 'Call Priority Promotion Time (secs)' at Disabled, 'Default Currency' at USD, 'Default Name Priority' at Favor Trunk, and 'Media Connection Preservation' at Disabled. Other checked options include 'Auto Hold', 'Dial By Name', 'Show Account Code', 'High Quality Conferencing', and 'Digital/Analogue Auto Create User'. Unchecked options include 'DSS Status', 'Restrict Network Interconnect', 'Drop External Only Impromptu Conference', 'Visually Differentiate External Call', and 'Unsupervised Analog Trunk Disconnect Handling'.

Setting	Value
Default Outside Call Sequence	Normal
Default Inside Call Sequence	Ring Type 1
Default Ring Back Sequence	Ring Type 2
Restrict Analogue Extension Ringer Voltage	<input type="checkbox"/>
Dial Delay Time (secs)	4
Dial Delay Count	0
Default No Answer Time (secs)	15
Hold Timeout (secs)	0
Park Timeout (secs)	300
Ring Delay (secs)	5
Call Priority Promotion Time (secs)	Disabled
Default Currency	USD
Default Name Priority	Favor Trunk
Media Connection Preservation	Disabled
Companding Law - Switch	<input checked="" type="radio"/> U-Law <input checked="" type="radio"/> A-Law
Companding Law - Line	<input type="radio"/> U-Law Line <input checked="" type="radio"/> A-Law Line
DSS Status	<input type="checkbox"/>
Auto Hold	<input checked="" type="checkbox"/>
Dial By Name	<input checked="" type="checkbox"/>
Show Account Code	<input checked="" type="checkbox"/>
Inhibit Off-Switch Forward/Transfer	<input type="checkbox"/>
Restrict Network Interconnect	<input type="checkbox"/>
Drop External Only Impromptu Conference	<input type="checkbox"/>
Visually Differentiate External Call	<input type="checkbox"/>
Unsupervised Analog Trunk Disconnect Handling	<input type="checkbox"/>
High Quality Conferencing	<input checked="" type="checkbox"/>
Strict SIPs	<input type="checkbox"/>
Digital/Analogue Auto Create User	<input checked="" type="checkbox"/>

5.4. Twinning Calling Party Settings

Navigate to the **Twining** tab on the Details Pane. Uncheck the **Send original calling party information for Mobile Twining** box. This will allow the Caller ID for Twining to be controlled by the setting on the SIP Line (**Section 5.6**). This setting also impacts the Caller ID for call forwarding.



IP500_2 (wSBCE)

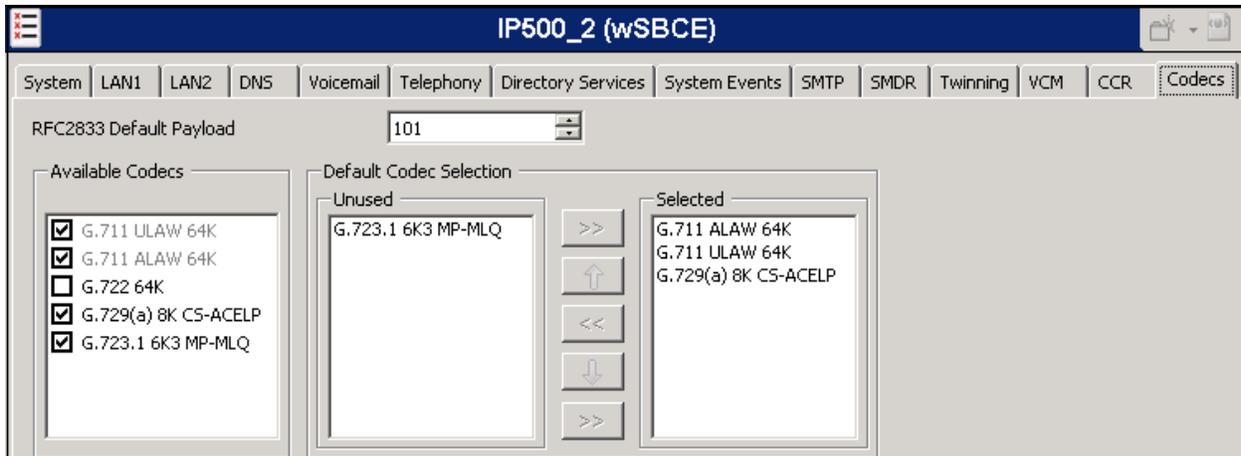
System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | **Twining** | VCM | CCR | Codecs

Send original calling party information for Mobile Twining

Calling party information for Mobile Twining:

5.5. System Codecs Settings

Navigate to the **Codecs** tab in the Details Pane. The **RFC2833 Default Payload** field is new in IP Office release 9.0. It allows the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used. The list of **Available Codecs** shows all the codecs supported by the system, and those selected as usable. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP (SIP and H.323) lines and extensions will use this system default codec selection, unless configured otherwise for a specific line or extension.



IP500_2 (wSBCE)

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | Twining | VCM | CCR | **Codecs**

RFC2833 Default Payload: 101

Available Codecs:

- G.711 ULAW 64K
- G.711 ALAW 64K
- G.722 64K
- G.729(a) 8K CS-ACELP
- G.723.1 6K3 MP-MLQ

Default Codec Selection:

Unused: G.723.1 6K3 MP-MLQ

Selected: G.711 ALAW 64K, G.711 ULAW 64K, G.729(a) 8K CS-ACELP

5.6. Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the private interface of the Avaya SBCE. This line will carry outbound and inbound traffic between to and from the service provider. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.6.1** to create the SIP Line from the template.

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

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- Setting of the **Use Network Topology Info** field on the Transport tab.

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.6.2 – 5.6.5**.

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

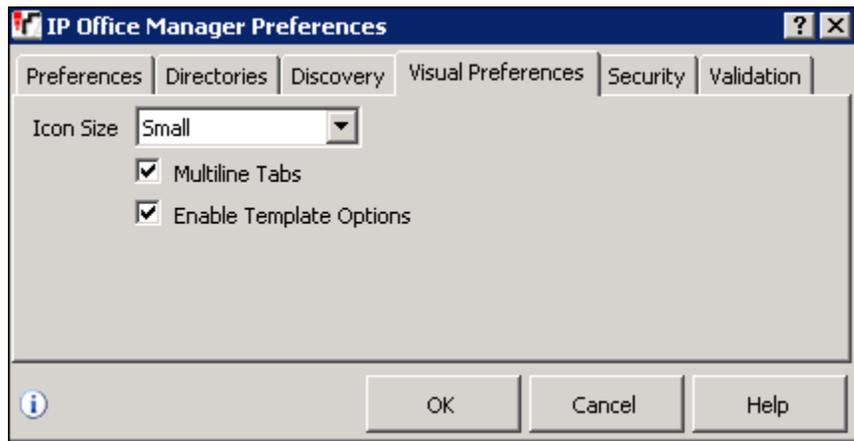
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.6.2 – 5.6.5**.

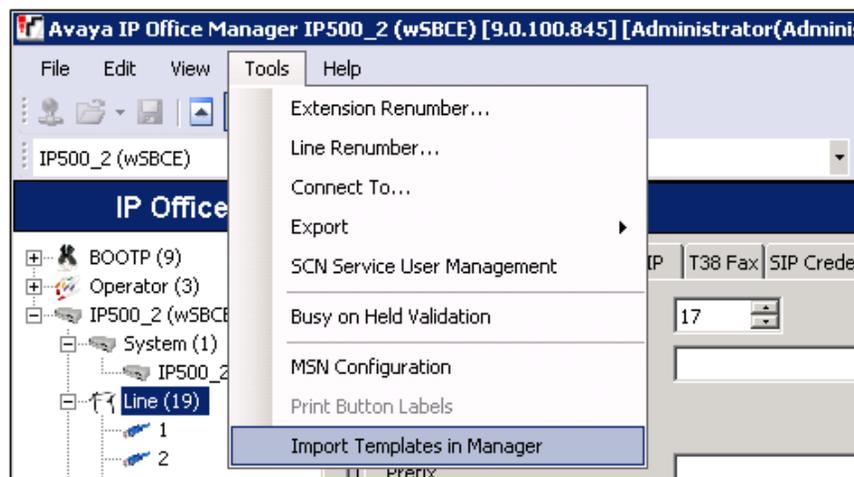
5.6.1. SIP Line From Template

Complete the following steps to create a SIP Line from the template associated with this Application Notes:

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

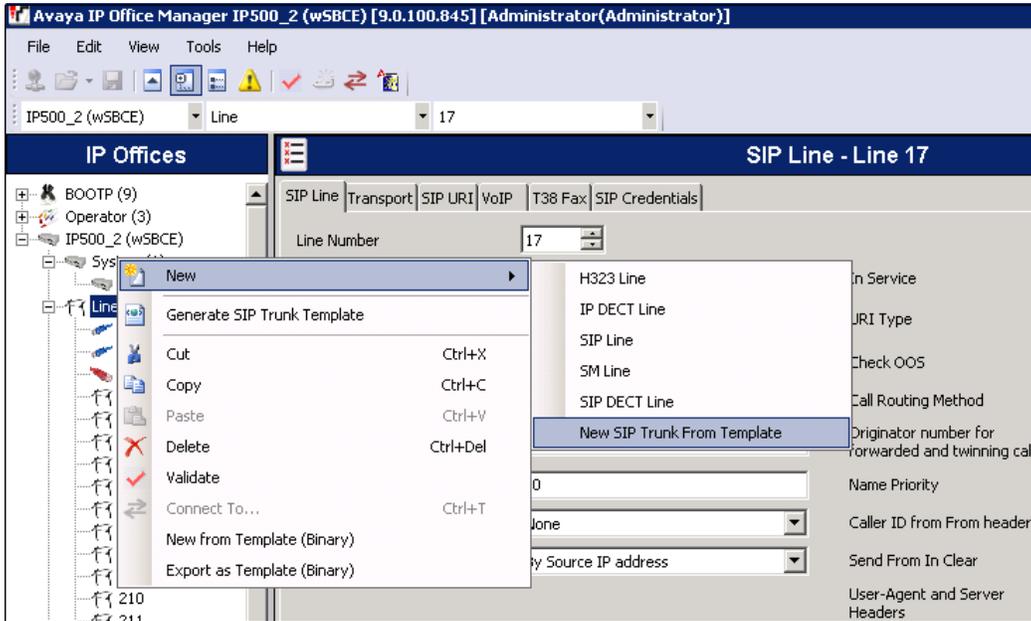


3. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**. This action will copy the template file into the IP Office template directory and make the template available in the IP Office Manager pull-down menus in **Step 5**. The default template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



In the pop-up window (not shown) that appears, select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

- To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New SIP Trunk From Template**.



- In the subsequent Template Type Selection pop-up window, select **Mexico** from the **Country** pull-down menu and select **Axtel** from the **Service Provider** pull-down menu as shown below. These values correspond to parts of the file name created in **Step 1** (**MX_Axtel_SIPTrunk.xml**). Click **Create new SIP Trunk** to finish creating the trunk.



- Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.6.2 – 5.6.5**.

5.6.2. SIP Line Tab

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

- Set the **ITSP Domain Name** to the IP address of the private interface of the Avaya SBCE.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will check the responses to SIP OPTIONS messages sent to the service provider to determine the operational status of the SIP Line.
- Set **Call Routing Method** to *Request URI*.
- Set **Send Caller ID** to *None*. This field is not used in this configuration. On outbound calls, the caller ID number shown on the PSTN end was always the main number assigned by Axtel to the enterprise, regardless of the actual number sent in any of the origination headers from the IP Office.
- Uncheck the **REFER support** box. REFER was not used in this configuration. See **Section 2.2** for more information.
- Default values may be used for all other parameters.

The screenshot displays the Avaya IP Office configuration interface. On the left, a tree view under 'IP Offices' shows a hierarchy: BOOTP (9), Operator (3), IP500_2 (wSBCE), System (1), IP500_2 (wSBCE), Line (19), and various numbered lines (1-216). Line 17 is selected. The main pane is titled 'SIP Line - Line 17' and contains several tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, and SIP Credentials. The 'SIP Line' tab is active, showing the following configuration:

Line Number	17	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name	10.5.5.152	URI Type	SIP
Prefix		Check OOS	<input type="checkbox"/>
National Prefix	0	Call Routing Method	Request URI
Country Code		Originator number for forwarded and twinning calls	
International Prefix	00	Name Priority	System Default
Send Caller ID	None	Caller ID from From header	<input type="checkbox"/>
Association Method	By Source IP address	Send From In Clear	<input type="checkbox"/>
<input type="checkbox"/> REFER Support		User-Agent and Server Headers	
Incoming: Always		Service Busy Response	486 - Busy Here
Outgoing: Always		Action on CAC Location Limit	Allow Voicemail
Method for Session Refresh	Auto		
Session Timer (seconds)	On Demand		
Media Connection Preservation	Disabled		

5.6.3. Transport Tab

Select the **Transport** tab and set the following:

- Set the **ITSP Proxy Address** to the IP address of the private interface of the Avaya SBCE.
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.

The screenshot shows the configuration interface for the Transport tab of a SIP Line. The tabs at the top are SIP Line, Transport, SIP URI, VoIP, T38 Fax, and SIP Credentials. The Transport tab is selected. The configuration fields are as follows:

- ITSP Proxy Address: 10.5.5.152
- Network Configuration section:
 - Layer 4 Protocol: UDP
 - Send Port: 5060
 - Use Network Topology Info: LAN 1
 - Listen Port: 5060
- Explicit DNS Server(s): 0 . 0 . 0 . 0
- Calls Route via Registrar:
- Separate Registrar: (empty field)

5.6.4. SIP URI Tab

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

- Set **Local URI**, **Contact** and **Display Name** to *Use Internal Data*. This setting allows calls on this line whose SIP URI matches the number set in the **SIP** tab of any User as shown in **Section 5.7**. Set **PAI** to *None*.
- For **Registration**, select **0: <None>** from the pull-down menu. Trunk registration with the service provider is achieved by the Avaya SBCE, later in **Section 6.3.3**.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials			
Channel	Groups	Via	Local URI	Contact	Display Name	PAI	Cre	Add...
								Remove
								Edit...

Edit Channel

Via: 10.5.5.150

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

PAI: None

Registration: 0: <None>

Incoming Group: 17

Outgoing Group: 17

Max Calls per Channel: 5

OK

Cancel

5.6.5. VoIP Tab

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

- In the sample configuration, the **Codec Selection** was configured using the *Custom* option, allowing an explicit ordered list of codecs to be specified. The buttons allow setting the specific order of preference for the codecs to be used on the line, as shown.
- Set **Fax Transport Support** to *G.711*.
- Set the **DTMF Support** field to *RFC2833*. This directs the IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Leave **Allow Direct Media Path** unchecked. Direct media was not used during the compliance test. See **Section 2.2** for more details.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check the **PRACK/100rel Supported** box, to advertise the support for provisional responses and Early Media to Axtel.
- Default values may be used for all other parameters.

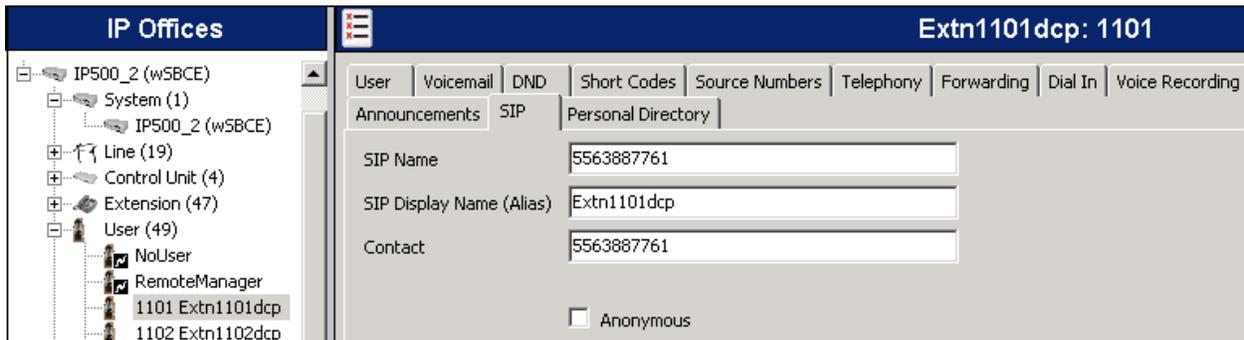
The screenshot displays the VoIP configuration interface with the following settings:

- Tab:** VoIP
- Codec Selection:** Custom
- Unused Codecs:** G.723.1 6K3 MP-MLQ
- Selected Codecs:** G.729(a) 8K CS-ACELP, G.711 ALAW 64K, G.711 ULAW 64K
- Fax Transport Support:** G.711
- Location:** Cloud
- Call Initiation Timeout (s):** 4
- DTMF Support:** RFC2833
- Checkboxes:**
 - VoIP Silence Suppression
 - Allow Direct Media Path
 - Re-invite Supported
 - Codec Lockdown
 - PRACK/100rel Supported
 - Force direct media with phones
 - G.711 Fax ECAN

5.7. Users

Configure the SIP parameters for each user that will be placing calls via the SIP line defined in **Section 5.6**. To configure these settings, navigate to **User** in the left Navigation Pane, and select the name of the user to be modified. Select the **SIP** tab in the Details Pane.

The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls. The example below shows the settings for user “Extn1101dcp”. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Axtel. In the example, the DID number **5563887761** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.



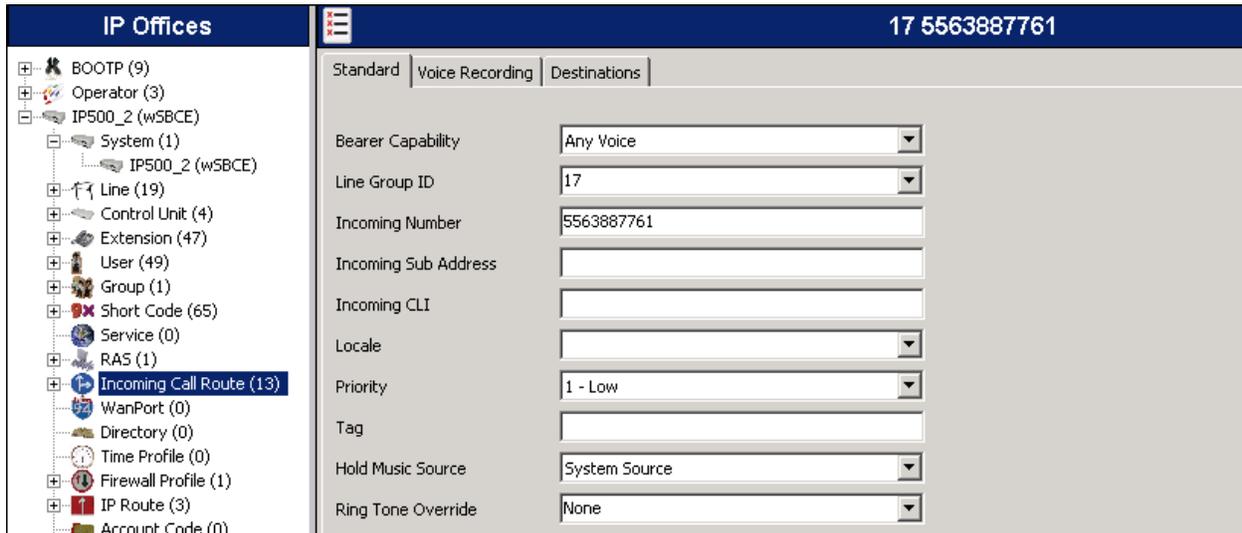
5.8. Incoming Call Route

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

To add a new incoming call route, from the left Navigation Pane, right-click on **Incoming Call Route** and select **New** (not shown). The screen below shows the route for one of the DID numbers assigned to the enterprise by Axtel, 5563887761 in this example.

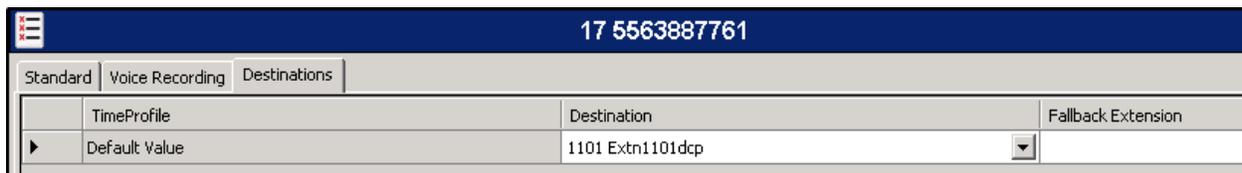
On the Details Pane, under the **Standard** tab, set the parameters as shown below:

- Set **Bearer Capacity** to *Any Voice*.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.6**.
- Set the **Incoming Number** to the incoming number on which this route should match.
- Default values may be used for all other parameters.



IP Offices		17 5563887761	
<ul style="list-style-type: none"> BOOTP (9) Operator (3) IP500_2 (wSBCE) <ul style="list-style-type: none"> System (1) IP500_2 (wSBCE) <ul style="list-style-type: none"> Line (19) Control Unit (4) Extension (47) User (49) Group (1) Short Code (65) Service (0) RAS (1) Incoming Call Route (13) WanPort (0) Directory (0) Time Profile (0) Firewall Profile (1) IP Route (3) Account Code (0) 	<ul style="list-style-type: none"> Standard Voice Recording Destinations 	<ul style="list-style-type: none"> Bearer Capacity: Any Voice Line Group ID: 17 Incoming Number: 5563887761 Incoming Sub Address: Incoming CLI: Locale: Priority: 1 - Low Tag: Hold Music Source: System Source Ring Tone Override: None 	

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, incoming calls to 5563887761 on line 17 are routed to extension 1101.

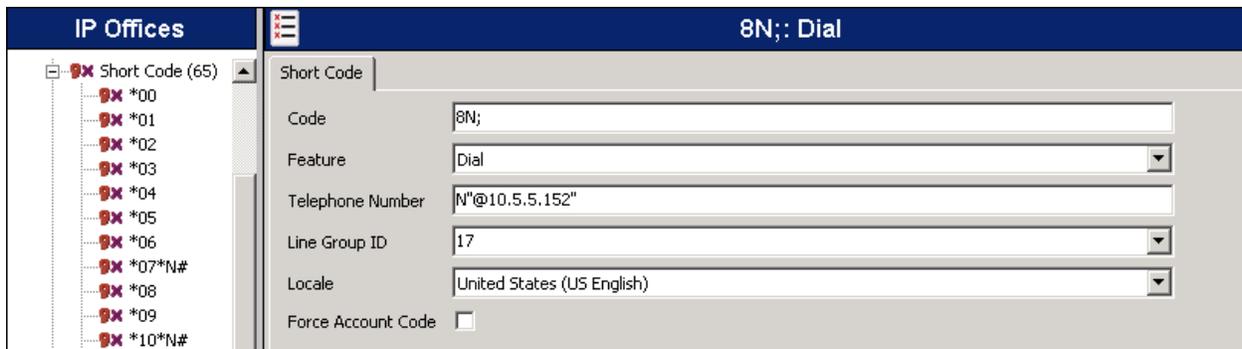


17 5563887761	
Standard	Voice Recording Destinations
TimeProfile	Destination Fallback Extension
▶ Default Value	1101 Extn1101dcp

5.9. Short Code

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

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, **8N;**. This short code will be invoked when the user dials 8 followed by any number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N"@10.5.5.152"**. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value *N* represents the number dialed by the user. The IP address 10.5.5.152 is the IP address of the private interface of the Avaya SBCE.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.6.4**. This short code will use this line group when placing outbound calls.
- Default values may be used for all other parameters.

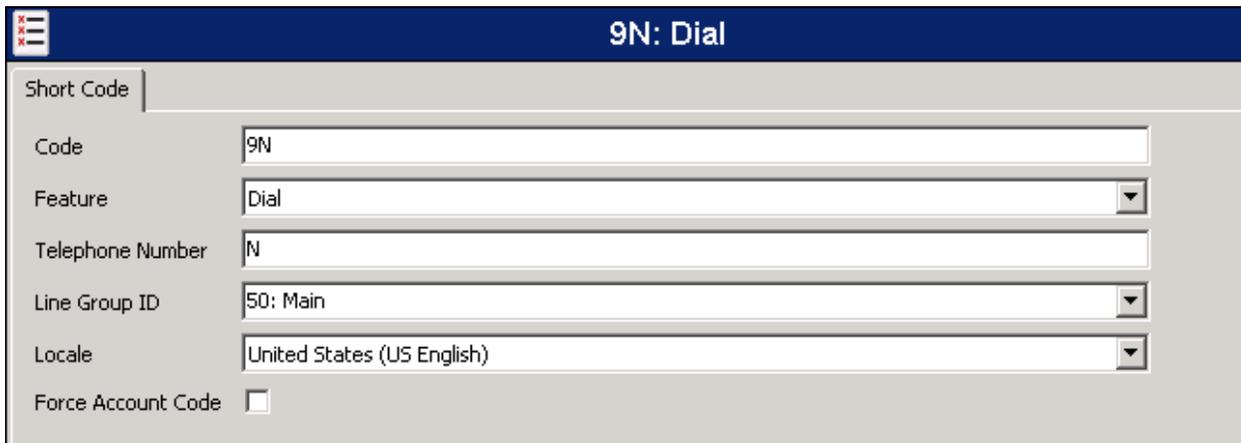


IP Offices	8N;; Dial
Short Code (65)	Short Code
*00	Code: 8N;;
*01	Feature: Dial
*02	Telephone Number: N"@10.5.5.152"
*03	Line Group ID: 17
*04	Locale: United States (US English)
*05	Force Account Code: <input type="checkbox"/>
*06	
*07*N#	
*08	
*09	
*10*N#	

5.10. Automatic Route Selection

Optionally, Automatic Route Selection (ARS) can be used rather than the simple short code approach described above. With ARS, secondary dial tone can be provided after the access code. Other features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. ARS also facilitates a more granular treatment for different types of calls, and permits a more specific matching of the telephone number dialed following the access code. While detailed coverage of ARS is beyond the scope of these Application Notes, and alternate routing was not used in the reference configuration, this section includes some basic screen illustrations of the ARS settings used during the compliance test.

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



The screenshot displays a configuration window titled "9N: Dial". The window contains the following fields and options:

Field	Value
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	50: Main
Locale	United States (US English)
Force Account Code	<input type="checkbox"/>

The following screen shows the example ARS configuration for the route *Main*. Note the sequence of *X*s used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first digit on the string. This type of setting results in a much quicker response in the delivery of the call by the IP Office. The screen below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. The highlighted entries show that for example, for local calls, the user dialed 9 plus the 8 digit local number, starting with a 6, which was the range of local numbers used during the compliance test. For national long distance calls in Mexico, the user dialed 9, then 01, followed by 10 digit numbers.

The screenshot displays the ARS configuration for the 'Main' route. The left sidebar shows the IP Office hierarchy, with 'ARS (1)' > '50: Main' selected. The main configuration area includes the following fields:

- ARS Route Id: 50
- Route Name: Main
- Dial Delay Time: System Default (4)
- In Service: (Out of Service Route: <None>)
- Time Profile: <None> (Out of Hours Route: <None>)
- Secondary Dial tone: (SystemTone)
- Check User Call Barring:

The ARS entries table is as follows:

Code	Telephone Number	Feature	Line Group ID
6XXXXXXXXX	6N	Dial	17
001XXXXXXXXX	001N	Dial	17
81XXXXXXXXXX	0181N	Dial	17
01800XXXXXXXX	01800N	Dial	17
040	040	Dial	17
01XXXXXXXXXX	01N	Dial	17
045XXXXXXXXXX	045N	Dial	17

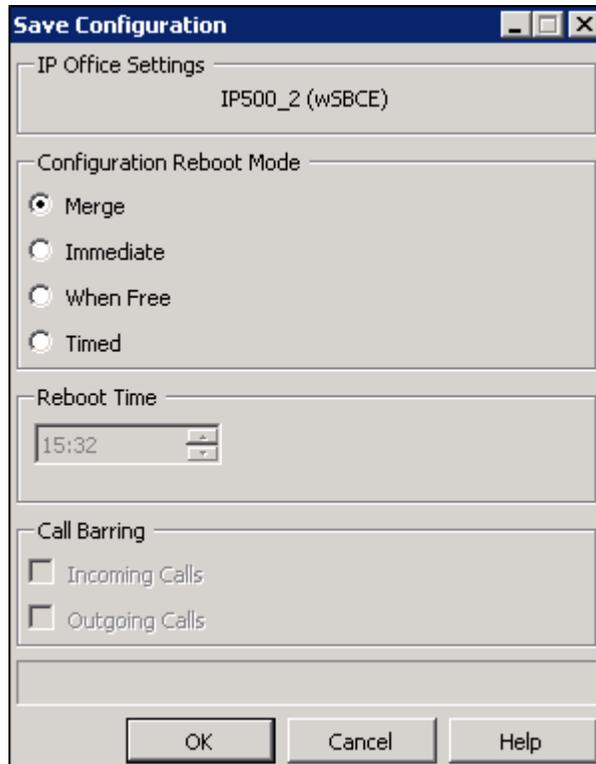
Additional settings at the bottom include:

- Alternate Route Priority Level: 3
- Alternate Route Wait Time: 30
- Alternate Route: <None>

5.11. Save Configuration

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

The following will appear, with either **Merge** or **Immediate** selected, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to proceed.



6. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Axtel SIP Trunking service. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult [6] and [7] in the **Additional References** section.

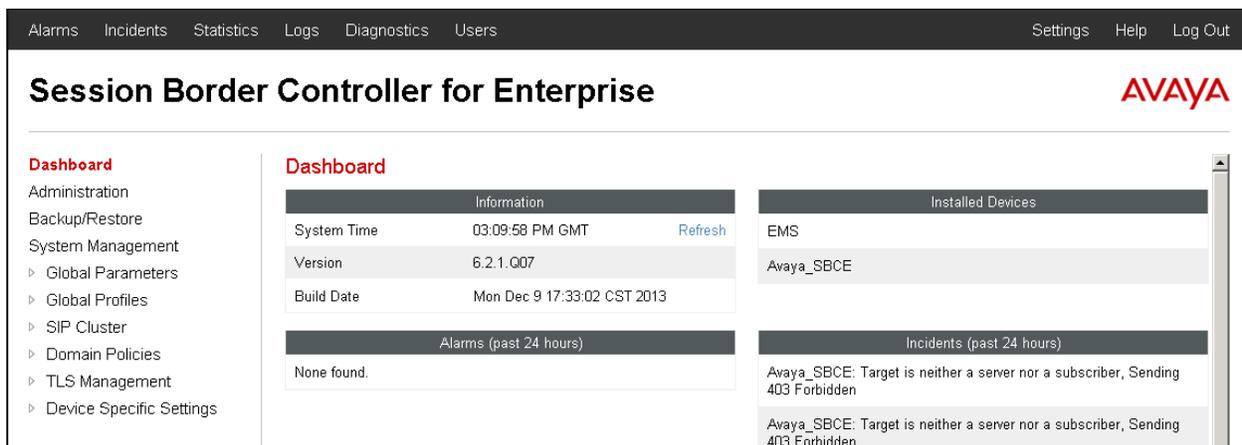
6.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL <https://<ip-address>>, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The screenshot shows the login page for the Avaya Session Border Controller for Enterprise. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right is a "Log In" section with fields for "Username:" and "Password:", a "Log In" button, and a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials. All users must comply with all corporate instructions regarding the protection of information assets. © 2011 - 2013 Avaya Inc. All rights reserved."

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.



The screenshot shows the dashboard of the Avaya Session Border Controller for Enterprise. The top navigation bar includes "Alarms", "Incidents", "Statistics", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out". The main header displays "Session Border Controller for Enterprise" and the Avaya logo. The left navigation pane lists menu items: "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "SIP Cluster", "Domain Policies", "TLS Management", and "Device Specific Settings". The main content area is titled "Dashboard" and contains three sections: "Information" (System Time: 03:09:58 PM GMT, Version: 6.2.1.Q07, Build Date: Mon Dec 9 17:33:02 CST 2013), "Installed Devices" (EMS, Avaya_SBCE), and "Alarms (past 24 hours)" (None found). The "Incidents (past 24 hours)" section shows two entries: "Avaya_SBCE: Target is neither a server nor a subscriber, Sending 403 Forbidden".

6.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named **Avaya_SBCE** is shown. The management IP address that was configured during installation and the current software version are shown here. Note that the management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.

The screenshot shows the 'System Management' section of the Avaya SBCE interface. The 'Devices' tab is active, displaying a table of installed devices. The table has columns for Device Name (Serial Number), Management IP, Version, and Status. A single device, 'Avaya_SBCE (IPCS21020006)', is listed with a Management IP of 192.168.10.75 and a Version of 6.2.1.Q07. The status is 'Commissioned'. Action buttons for 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Delete' are visible for this device.

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device and the network settings.

The 'System Information: Avaya_SBCE' window displays the following configuration details:

- General Configuration:** Appliance Name: Avaya_SBCE, Box Type: SIP, Deployment Mode: Proxy.
- Device Configuration:** HA Mode: No, Two Bypass Mode: No.
- Network Configuration:**

IP	Public IP	Netmask	Gateway	Interface
10.5.5.152	10.5.5.152	255.255.255.0	10.5.5.254	A1
172.16.157.151	172.16.157.151	255.255.255.192	172.16.157.129	B1
10.5.5.153	10.5.5.153	255.255.255.0	10.5.5.254	A1
172.16.157.160	172.16.157.160	255.255.255.192	172.16.157.129	B1
- DNS Configuration:** Primary DNS: 192.168.10.100, Secondary DNS: (empty), DNS Location: DMZ, DNS Client IP: 10.5.5.152.
- Management IP(s):** IP: 192.168.10.75.

On the previous screen, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces for the Avaya SBCE. The highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Axtel. Other shown IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document.

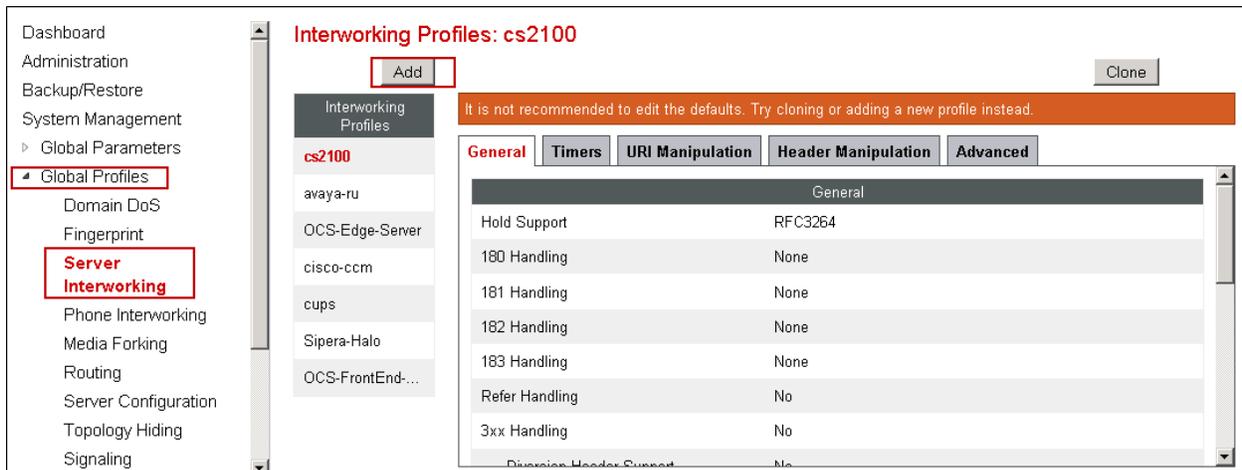
6.3. Global Profiles

The Global Profiles Menu on the left navigation pane allows the configuration of parameters across all Avaya SBCE appliances.

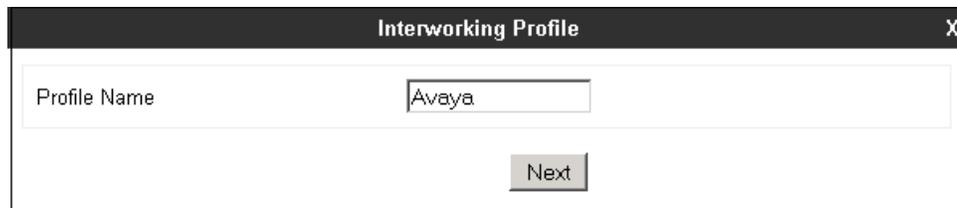
6.3.1. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server). In the compliance test, the IP Office functions as the Call Server and the Axtel SIP Proxy as the Trunk Server.

To configure the interworking profile in the enterprise direction, select **Global Profiles** → **Server Interworking** on the left navigation pane. Click **Add**.



Enter a descriptive name for the new profile. Click **Next**.



On the **General** screen, all parameters retain their default values. Click **Next**.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Click **Next** on the **Privacy/DTMF** and **SIP Timers/Transport Timers** tabs (not shown). On the **Advanced Settings** tab, uncheck the **Topology Hiding: Change Call-ID** box and check the **AVAYA Extensions** box. Click **Finish** to save and exit.

Interworking Profile	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input checked="" type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

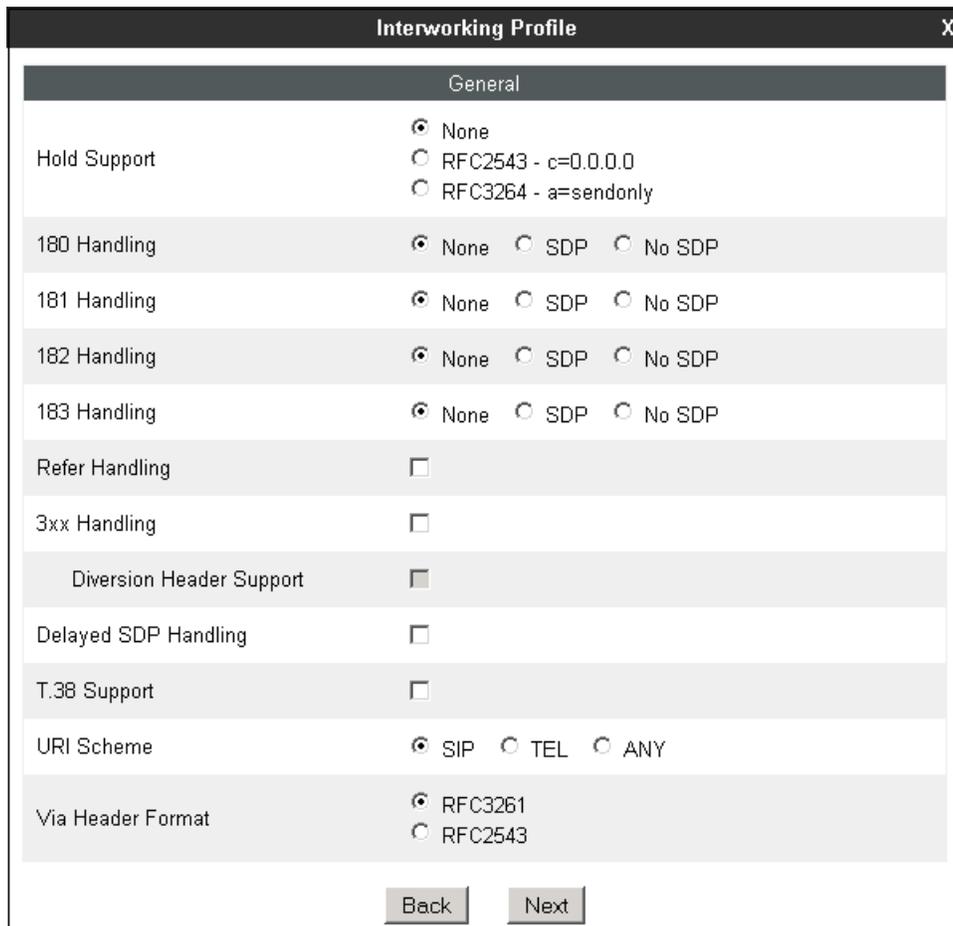
Back Finish

A second interworking profile named **Service Provider** in the direction of the SIP trunk to Axtel was similarly created. For this profile default values were used for all parameters.



The screenshot shows a window titled "Interworking Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Service Provider". Below the input field is a "Next" button.

General tab:



The screenshot shows the "Interworking Profile" window with the "General" tab selected. The settings are as follows:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

At the bottom of the window, there are "Back" and "Next" buttons.

Advanced Settings tab:

Interworking Profile X

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

6.3.2. Signaling Manipulation

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

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [7] on the **References** section for more information on this topic.

During the compliance test, a Sigma script was created to remove the “Remote-Address” parameter, used by the Avaya SBCE, from all outbound messages. This parameter contains private enterprise IP addresses that have no significance to the service provider.

From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click **Add** to open the SigMa Editor screen, where the text of the script can be entered. The screen below shows the finished Signaling Manipulation script named **Remove Remote Address**.

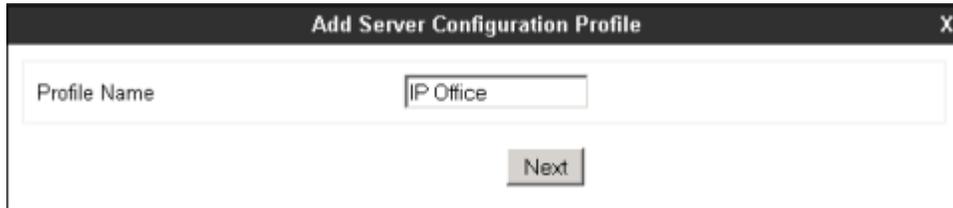
The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top left corner shows the title "Session Border Controller for Enterprise" and the Avaya logo. A navigation menu on the left includes "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles" (expanded), "Domain DoS", "Fingerprint", "Server Interworking", "Phone Interworking", "Media Forking", "Routing", "Server Configuration", "Topology Hiding", "Signaling", and "Manipulation". The main content area is titled "Signaling Manipulation Scripts: Remove Remote Address". It features buttons for "Upload", "Add", "Download", "Clone", and "Delete". A blue bar contains the text "Click here to add a description." Below this, a "Signaling Manipulation" script editor is shown with the following code:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"][1]);
  }
}
```

An "Edit" button is located at the bottom right of the script editor.

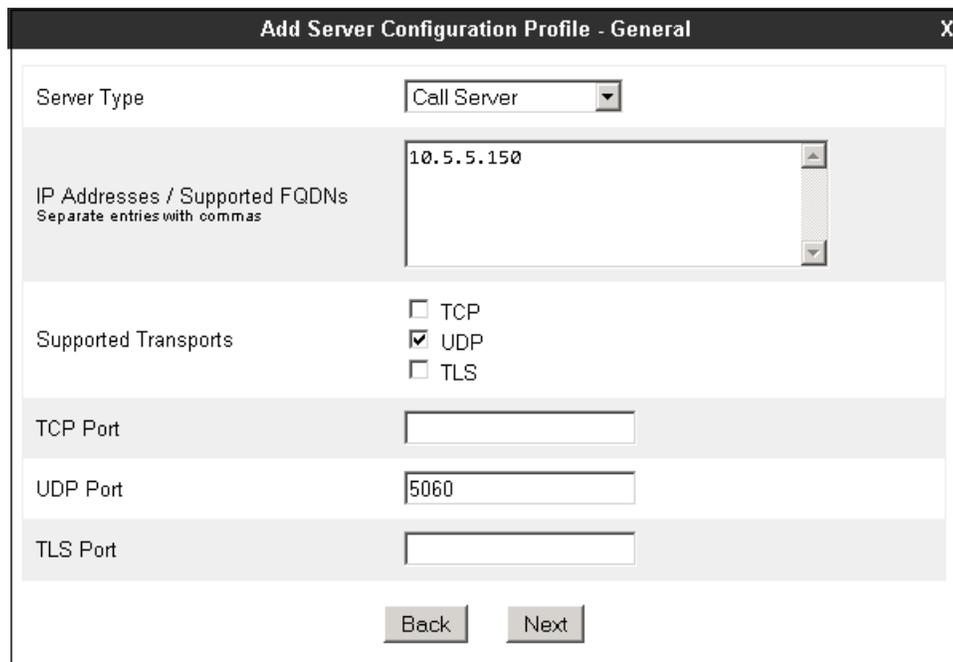
6.3.3. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE two peers, i.e., IP Office (Call Server) and the SIP Proxy at the service provider's network (Trunk Server). From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server. Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. The main area contains a text input field labeled "Profile Name" with the text "IP Office" entered. Below the input field is a "Next" button.

On the **Add Server Configuration Profile - General** Tab select **Call Server** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter the IP address of the IP Office LAN1, as defined in **Section 5.2**. Select **UDP** for **Supported Transports**, and enter **5060** under **UDP Port**. The transport protocol and port selected here must match the values used on the IP Office SIP line on **Section 5.6**. Click **Next**.

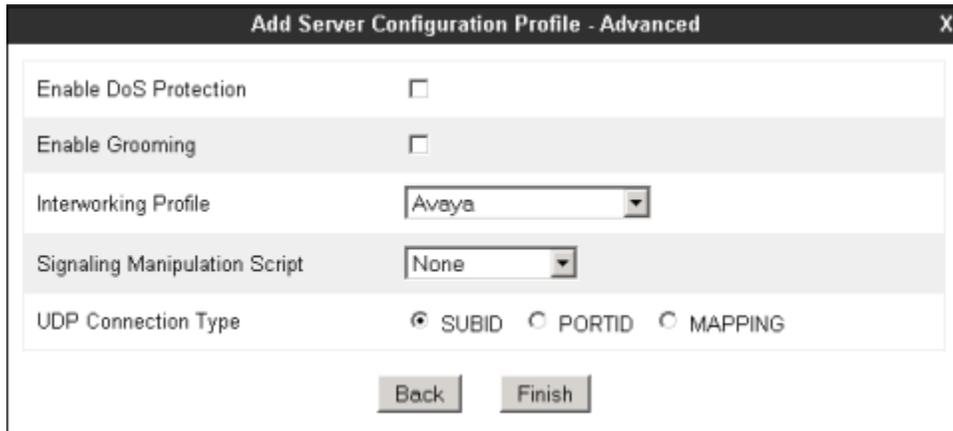


The screenshot shows a dialog box titled "Add Server Configuration Profile - General". It has a close button (X) in the top right corner. The form contains the following fields and options:

- Server Type:** A dropdown menu with "Call Server" selected.
- IP Addresses / Supported FQDNs:** A text area with "10.5.5.150" entered. Below the text area is the instruction "Separate entries with commas".
- Supported Transports:** Three checkboxes: "TCP" (unchecked), "UDP" (checked), and "TLS" (unchecked).
- TCP Port:** An empty text input field.
- UDP Port:** A text input field containing "5060".
- TLS Port:** An empty text input field.

At the bottom of the dialog are "Back" and "Next" buttons.

Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Click **Finish**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains the following settings:

- Enable DoS Protection:
- Enable Grooming:
- Interworking Profile: Avaya (selected in a dropdown menu)
- Signaling Manipulation Script: None (selected in a dropdown menu)
- UDP Connection Type: SUBID PORTID MAPPING

At the bottom of the dialog, there are two buttons: "Back" and "Finish".

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown). Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It contains the following settings:

- Profile Name: Service Provider (entered in a text field)

At the bottom of the dialog, there is a "Next" button.

On the **Add Server Configuration Profile-General** Tab select *Trunk Server* from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter *192.168.171.78*, the IP Address of the Axtel’s SIP proxy server. Select **UDP** for **Supported Transports**, and enter *5060* under **UDP Port**, as specified by Axtel. Click **Next**.

The screenshot shows a configuration window titled "Add Server Configuration Profile - General". It contains the following fields and options:

- Server Type:** A dropdown menu set to "Trunk Server".
- IP Addresses / Supported FQDNs:** A text area containing "192.168.171.78". Below the text area is the instruction "Separate entries with commas".
- Supported Transports:** Three checkboxes: "TCP" (unchecked), "UDP" (checked), and "TLS" (unchecked).
- TCP Port:** An empty text input field.
- UDP Port:** A text input field containing "5060".
- TLS Port:** An empty text input field.
- At the bottom, there are two buttons: "Back" and "Next".

On the **Authentication** tab, check the **Enable Authentication** box. Enter the **User Name**, **Realm** and **Password** credential information supplied by the service provider for the authentication of the SIP trunk. Click **Next**.

The screenshot shows a configuration window titled "Add Server Configuration Profile - Authentication". It contains the following fields and options:

- Enable Authentication:** A checkbox that is checked.
- User Name:** A text input field containing "user123".
- Realm:** A text input field containing "Realm". Below the field is the instruction "(Leave blank to detect from server challenge)".
- Password:** A text input field filled with 12 black dots.
- Confirm Password:** A text input field filled with 12 black dots.
- At the bottom, there are two buttons: "Back" and "Next".

On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Axtel proxy server in order to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **60** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the **User Name** entered in the **Authentication** screen, and the external IP addresses of the Avaya SBCE (From URI) and the proxy server at Axtel (To URI) , like shown on the screen below.
- Click **Next**.

The screenshot shows a dialog box titled "Add Server Configuration Profile - Heartbeat". It contains the following fields and controls:

- Enable Heartbeat**: A checked checkbox.
- Method**: A dropdown menu set to "REGISTER".
- Frequency**: A text input field containing "60" followed by the label "seconds".
- From URI**: A text input field containing "user123@172.16.157.15".
- To URI**: A text input field containing "user123@192.168.171.7".
- At the bottom, there are two buttons: "Back" and "Next".

On the **Advanced** tab, select **Service Provider** from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the **Remove Remote Address** created in **Section 6.3.2**. Click **Finish**.

The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains the following fields and controls:

- Enable DoS Protection**: An unchecked checkbox.
- Enable Grooming**: An unchecked checkbox.
- Interworking Profile**: A dropdown menu set to "Service Provider".
- Signaling Manipulation Script**: A dropdown menu set to "Remove Remote Address".
- UDP Connection Type**: Three radio buttons: "SUBID" (selected), "PORTID", and "MAPPING".
- At the bottom, there are two buttons: "Back" and "Finish".

6.3.4. Routing Profiles

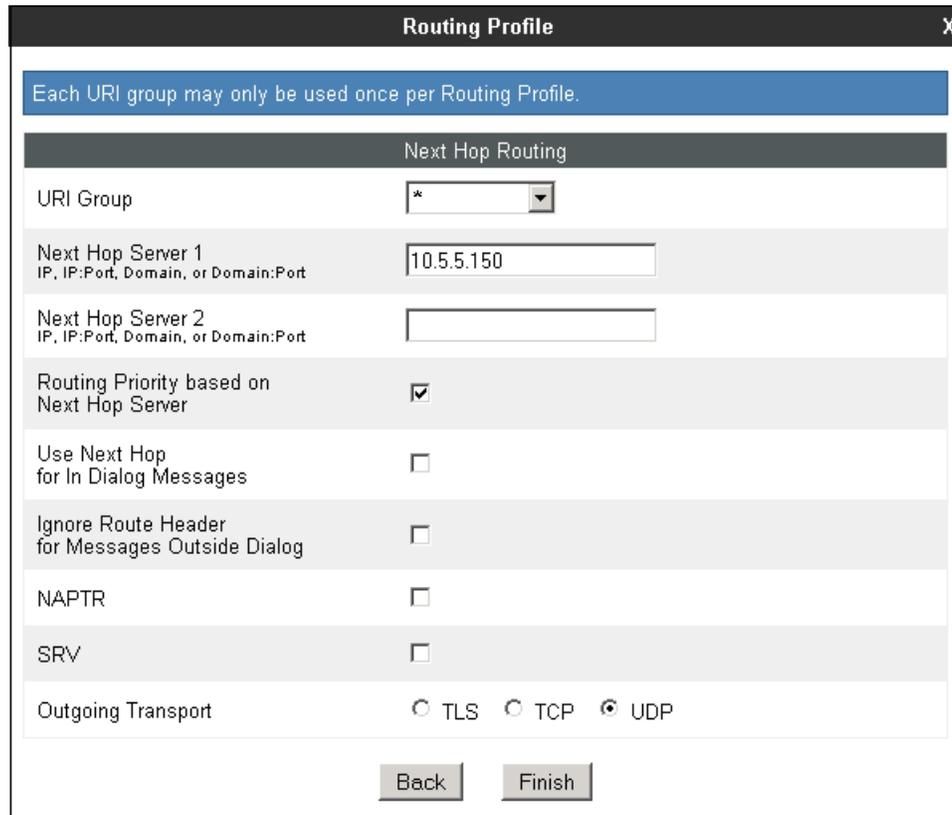
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces.

Two Routing Profiles were created in the test configuration, one for inbound calls, with the IP Office as the destination, and the second one for outbound calls, which are routed to the Axtel SIP trunk. To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown). Enter an appropriate **Profile Name** similar to the example below. Click **Next**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Below the title bar, there is a text input field labeled "Profile Name" containing the text "Route to IP Office". Below the input field, there is a "Next" button.

On the **Next Hop Routing** tab, enter the IP Address of the IP Office LAN1 interface as **Next Hop Server 1**. Since the default well-known port value of 5060 for UDP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **UDP** for **Outgoing Transport**. Click **Finish**.



The screenshot shows the "Routing Profile" dialog box with the "Next Hop Routing" tab selected. A blue banner at the top states "Each URI group may only be used once per Routing Profile." Below this, the "Next Hop Routing" section contains the following fields and options:

- URI Group: * (dropdown menu)
- Next Hop Server 1: 10.5.5.150 (text input field)
- Next Hop Server 2: (empty text input field)
- 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

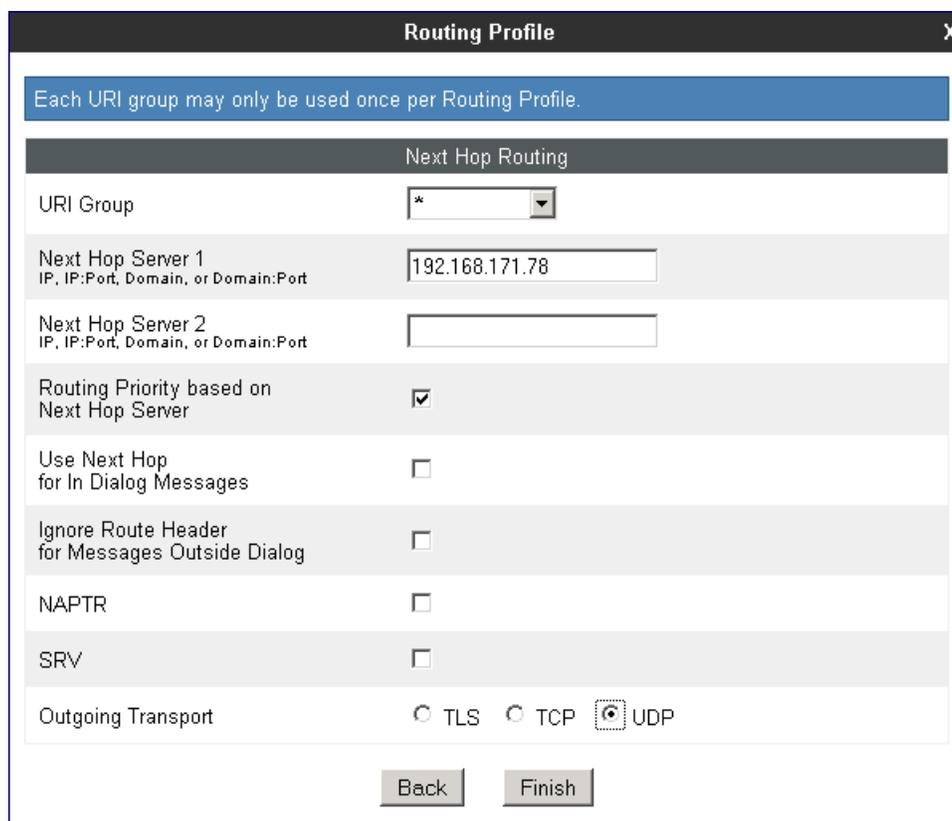
At the bottom of the dialog box, there are "Back" and "Finish" buttons.

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route. Enter an appropriate **Profile Name** similar to the example below. Click **Next**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route to SP". Below the input field is a "Next" button.

On the Next Hop Routing tab, enter the IP Address of the service provider SIP proxy server as **Next Hop Server 1**. Since the default well-known port value of 5060 for UDP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **UDP** for **Outgoing Transport**. Click **Finish**.



The screenshot shows the "Routing Profile" dialog box with the "Next Hop Routing" tab selected. A blue banner at the top states "Each URI group may only be used once per Routing Profile." Below this, the "Next Hop Routing" section contains the following fields and options:

- URI Group: A dropdown menu showing an asterisk (*).
- Next Hop Server 1: A text input field containing "192.168.171.78". Below the field is the text "IP, IP:Port, Domain, or Domain:Port".
- Next Hop Server 2: An empty text input field. Below the field is the text "IP, IP:Port, Domain, or Domain:Port".
- Routing Priority based on Next Hop Server: A checked checkbox.
- Use Next Hop for In Dialog Messages: An unchecked checkbox.
- Ignore Route Header for Messages Outside Dialog: An unchecked checkbox.
- NAPTR: An unchecked checkbox.
- SRV: An unchecked checkbox.
- Outgoing Transport: Three radio buttons labeled "TLS", "TCP", and "UDP". The "UDP" radio button is selected.

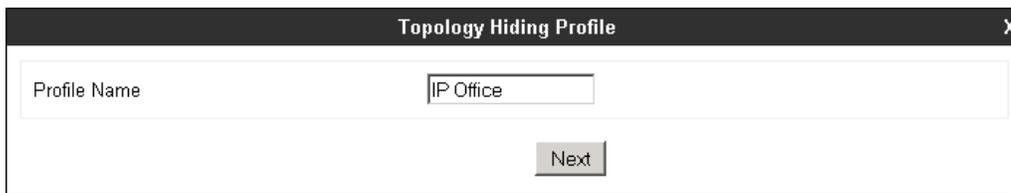
At the bottom of the dialog, there are "Back" and "Finish" buttons.

6.3.5. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side and click the **Add** button (not shown). Enter a **Profile Name** such as the one shown below. Click **Next**.



The screenshot shows a window titled "Topology Hiding Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "IP Office". Below the input field is a "Next" button.

On the **Topology Hiding Profile** screen, click the **Add Header** button repeatedly to show the rest of the headers in the profile.



The screenshot shows a window titled "Topology Hiding Profile" with a close button (X) in the top right corner. In the top right of the window content area, there is an "Add Header" button. Below this is a table with the following structure:

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

Below the table, there is a "Delete" button next to the first row. At the bottom of the window, there are "Back" and "Finish" buttons.

During the compliance test, IP addresses instead of domains were used in all SIP messages between the IP Office and the Avaya SBCE. Note that since the default action of *Auto* implies the insertion of IP addresses in the host portion of these headers, it was not necessary to modify any of the headers sent to the enterprise. Default values were used for all fields. Click **Finish**.

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

A Topology Hiding profile named **Service Provider** was similarly created in the direction of the SIP trunk to Axtel. In this case, for the **Request-Line**, **To** and **From** headers, select **Overwrite** in the **Replace Action** column. In the **Overwrite Value** column, enter the SIP domain used and expected by the service provider on these headers. During the compliance test, this domain was *mex1.TRKSMEX03.ipbx*. Click **Finish**.

Header	Criteria	Replace Action	Overwrite Value
RequestLine	IP/Domain	Overwrite	mex1.TRKSMEX03.ipj
From	IP/Domain	Overwrite	mex1.TRKSMEX03.ipj
To	IP/Domain	Overwrite	mex1.TRKSMEX03.ipj
Record-Route	IP/Domain	Auto	
Via	IP/Domain	Auto	
SDP	IP/Domain	Auto	
Refer-To	IP/Domain	Auto	
Referred-By	IP/Domain	Auto	

6.4. Domain Policies

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

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

6.4.1. Application Rules

Application Rules define the types of SIP-based Unified Communications (UC) applications to be protected by the Avaya SBCE, as well as the maximum number of concurrent sessions allowed to be processed by the device. A single new Application Rule was created, by cloning the pre-defined **default-trunk** rule.

Select **Application Rules** under the **Domain Policies** menu on the left hand side, select the **default-trunk** Application Rule and click **Clone**.

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

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

Under **Clone Name** enter the new rule name. Click **Finish** to save.

Clone Rule

Rule Name: default-trunk

Clone Name: Sessions=500

Finish

On the Application Rules screen, select the newly created rule and click **Edit** (not shown). For SIP trunking, **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** should have the same value. In the example below, they were set to **500**, which is the number of maximum simultaneous sessions supported on the Avaya SBCE Portwell CAD-0208 platform. This parameter can have a different value on the field, and should be set according to customer requirements. Click **Finish**.

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

Finish

6.4.2. Signaling Rules

As mentioned previously in **Section 2.2**, for all outbound calls, in the 200OK message sent from the network as a response to the INVITE sent from the enterprise, Axtel included a P- Asserted-Identity (PAI) header with “anonymous;phone-context=unknown” parameters that made the display on the IP Office extensions (calling party) change to “anonymous” after the calls was answered by the PSTN party. To avoid this, a Signaling Rule was created to remove the PAI header in the 200OK message arriving from Axtel.

In the **Domain Policies** menu on the left-hand side, select **Signaling Rules**, then **Add Rule** (not shown). Enter an appropriate name like in the example below. Click **Next**.

Signaling Rule

Rule Name: Remove PAI

Next

Click **Next** on the next three tabs (not shown), leaving all fields in sections **Inbound Outbound**, **Content-Type Policies**, **QoS** and **UCDI** with their default values. Click **Finish**.

On the newly created **Remove PAI** Signaling Rule, select the **Response Headers** tab to create the manipulations performed on response messages. Select **Add In Header Control**.

The screenshot shows the configuration page for a signaling rule named "Remove PAI". The "Response Headers" tab is selected, and the "Add In Header Control" button is visible. The table below shows no existing header controls.

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction
No response header controls exist.							

In the **Add Header Control** screen select the following:

- **Header Name: P-Asserted Identity**
- **Response Code: 2XX**
- **Method Name: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- **Click Finish**

The "Add Header Control" dialog box is shown with the following configuration:

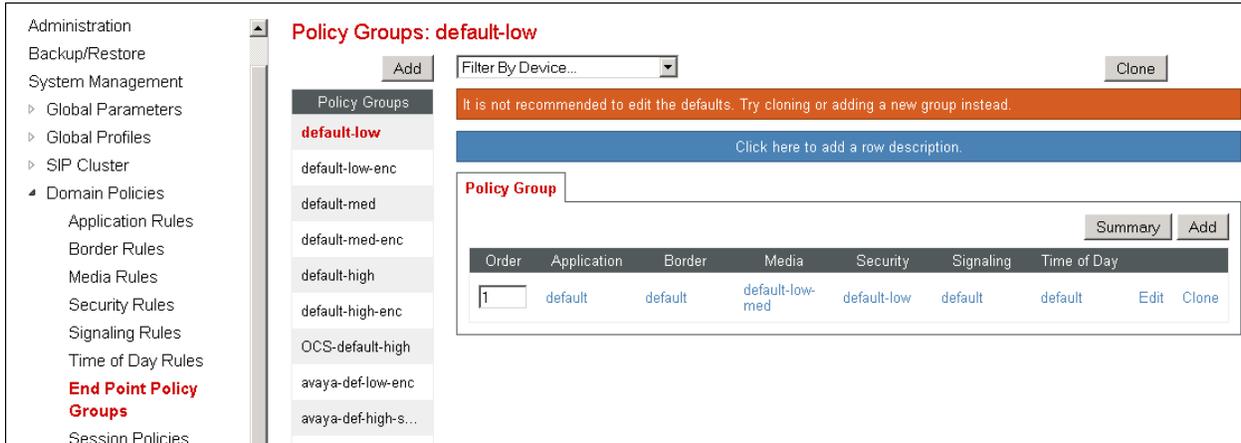
- Proprietary Response Header:
- Header Name: P-Asserted-Identity
- Response Code: 2XX
- Method Name: INVITE
- Header Criteria: Forbidden, Mandatory, Optional
- Presence Action: Remove header
- 486: Busy Here

The **Finish** button is visible at the bottom.

6.4.3. End Point Policy Groups

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

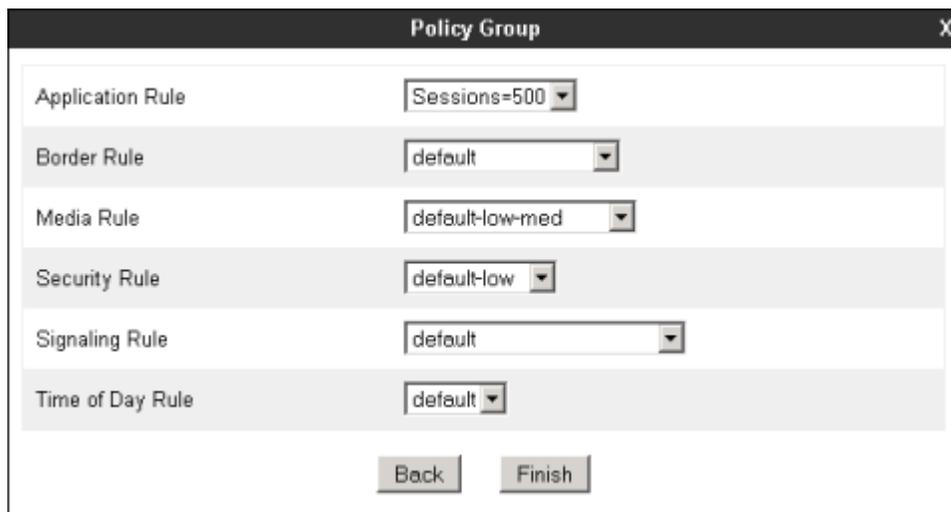
To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu. Select **Add**.



Enter an appropriate name in the **Group Name** field. Click **Next**.



In the Policy Group tab, defaults were used for all fields, with the exception of the **Application Rule**, where the *Sessions=500* rule created in **Section 6.4.1** was selected. Click **Finish**.



A second End Point Policy Group was similarly created for the service provider, repeating the steps described previously. This policy group will additionally be assigned the Signaling Rule **Remove PAI** created in **Section 6.4.2**. The screen below shows the **Service Provider** End Point Policy Group after the configuration was completed.

6.5. Device Specific Settings

The **Device Specific Settings** determine server specific parameters that determine how the device will work when deployed on the network. Among the parameters defined here are IP addresses, media and signaling interfaces, call flows, etc.

6.5.1. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu.

Under **Devices** in the centre pane, select the device being managed, **Avaya_SBCE** in the sample configuration. On the **Network Configuration** tab, verify or enter the network information as needed. Note that the **A1** interface is used for the internal side and **B1** is used for the external side of the Avaya SBCE.

On the **Interface Configuration** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. Click the **Toggle** buttons if necessary to enable the interfaces.

Network Management: Avaya_SBCE

Devices

Avaya_SBCE

Network Configuration

Interface Configuration

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

6.5.2. Media Interface

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address and one of the ports in this range as the listening IP address and port in which it will accept media from the Call or the Trunk Server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.

Add Media Interface X

Name

IP Address

Port Range -

A second Media Interface facing the public network side was similarly created with the name **Public_med**, as shown below. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. The **Port Range** was left at the default values.

Once the configuration is complete, the **Media Interface** screen will appear as follows.

Media Interface: Avaya_SBCE

Devices

Avaya_SBCE

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	
Private_med	10.5.5.152	35000 - 40000	Edit Delete
Public_med	172.16.157.151	35000 - 40000	Edit Delete

6.5.3. Signaling Interface

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in both the inside and outside networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. Enter **5060** for **UDP Port**, since UDP port 5060 is used to listen for signaling traffic from the IP Office in the sample configuration. Click **Finish**.

Name	Private_sig
IP Address	10.5.5.152
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	5060
Enable Stun	<input type="checkbox"/>
TLS Port <small>Leave blank to disable</small>	
TLS Profile	AvayaSBCServer
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

A second Signaling Interface with the name **Public_sig** was similarly created in the network direction. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. Under **UDP Port**, enter **5060** since these are the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.

Once the configuration is complete, the **Signaling Interface** screen will appear as follows:

Signaling Interface: Avaya_SBCE

Devices

Avaya_SBCE

Signaling Interface Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	10.5.5.152	---	5060	---	None	Edit Delete
Public_sig	172.16.157.151	---	5060	---	None	Edit Delete

6.5.4. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named **IP Office Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.

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

A second Server Flow with the name **SIP Trunk Flow** was similarly created in the network direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.

Edit Flow: SIP Trunk Flow X

Flow Name

Server Configuration

URI Group

Transport

Remote Subnet

Received Interface

Signaling Interface

Media Interface

End Point Policy Group

Routing Profile

Topology Hiding Profile

File Transfer Profile

The two Server Flows created in the sample configuration are summarized on the screen below.

Devices	Subscriber Flows	Server Flows					
<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">Avaya_SBCE</div>	Click here to add a row description.						
Server Configuration: IP Office							
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IP Office Flow	*	Public_sig	Private_sig	Enterprise	Route to SP View Clone Edit Delete	
Server Configuration: Service Provider							
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SIP Trunk Flow	*	Private_sig	Public_sig	Service Provider	Route to IP Office View Clone Edit Delete	

7. Axtel SIP Trunking Service Configuration

Axtel is responsible for the configuration of the Axtel SIP Trunking service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Axtel will provide the customer the necessary information to configure the SIP trunk connection in Avaya IP Office and Avaya SBCE, including:

- IP address of the Axtel SIP Proxy server.
- SIP domain.
- Credentials for the SIP trunk registration (username, password, realm).
- Supported codecs and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

8. Verification Steps

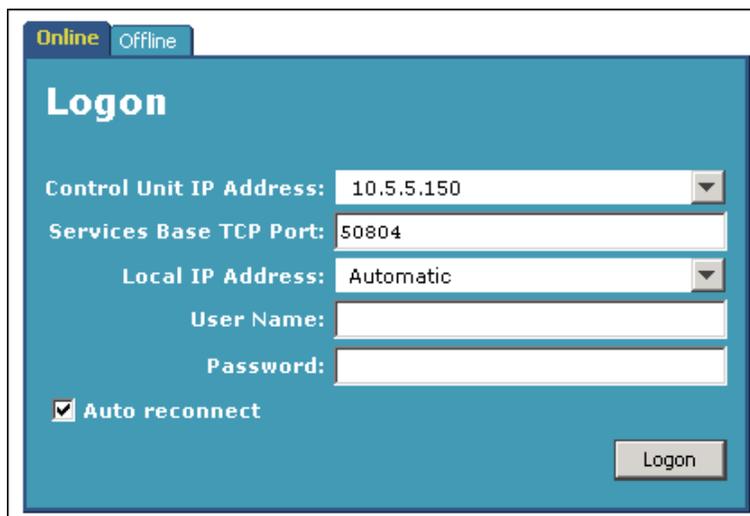
The following sections include steps that may be used to verify the configuration of the IP Office and the Avaya SBCE with the Axtel SIP Trunking service.

8.1. Avaya IP Office

The Avaya IP Office System Status and Monitor applications are useful tools used for the verification and troubleshooting of the SIP connection to the service provider via the Avaya SBCE.

8.1.1. System Status

The Avaya IP Office System Status application can be used to verify the service state of the SIP line. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager was installed. Under **Control Unit IP Address** select the IP address of the IP Office system under verification. Log in using the appropriate credentials



The screenshot shows the 'Logon' window of the Avaya IP Office System Status application. At the top, there are two tabs: 'Online' (selected) and 'Offline'. The window title is 'Logon'. Below the title, there are several input fields and a checkbox:

- Control Unit IP Address:** A dropdown menu with '10.5.5.150' selected.
- Services Base TCP Port:** A text input field containing '50804'.
- Local IP Address:** A dropdown menu with 'Automatic' selected.
- User Name:** An empty text input field.
- Password:** An empty text input field.
- Auto reconnect**

A 'Logon' button is located at the bottom right of the window.

Select the SIP line of interest from the left pane (**Line 17** in the reference configuration). 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).

The screenshot shows the Avaya IP Office System Status application. The left pane shows a tree view with 'Line: 17' selected. The main pane is on the 'Status' tab, displaying a 'SIP Trunk Summary' with the following details:

- Peer Domain Name: 10.5.5.152
- Resolved Address: 10.5.5.152
- Line Number: 17
- Number of Administered Channels: 15
- Number of Channels in Use: 0
- Administered Compression: G729 A, G711 A, G711 Mu
- Silence Suppression: Off
- Layer 4 Protocol: UDP
- SIP Trunk Channel Licenses: Unlimited
- SIP Trunk Channel Licenses in Use: 0 (indicated by a green circle and 0%)
- SIP Device Features:

Below the summary is a table with the following columns: Channel Number, URI G..., Call Ref, Current State, Time in State, Remote Media Ad..., Codec, Connec..., Caller ID or Diale..., Other Party on Call, Direction of Call, Round Trip De..., Receive Jitter, Receive Packet ..., Transmit Jitter, and Transmit Packet ...

Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media Ad...	Codec	Connec...	Caller ID or Diale...	Other Party on Call	Direction of Call	Round Trip De...	Receive Jitter	Receive Packet ...	Transmit Jitter	Transmit Packet ...
1			Idle	00:00:54											
2			Idle	5 days ...											
3			Idle	5 days ...											
4			Idle	5 days ...											
5			Idle	5 days ...											
6			Idle	5 days ...											
7			Idle	5 days ...											
8			Idle	5 days ...											
9			Idle	5 days ...											
10			Idle	5 days ...											
11			Idle	5 days ...											
12			Idle	5 days ...											
13			Idle	5 days ...											
14			Idle	5 days ...											
15			Idle	5 days ...											

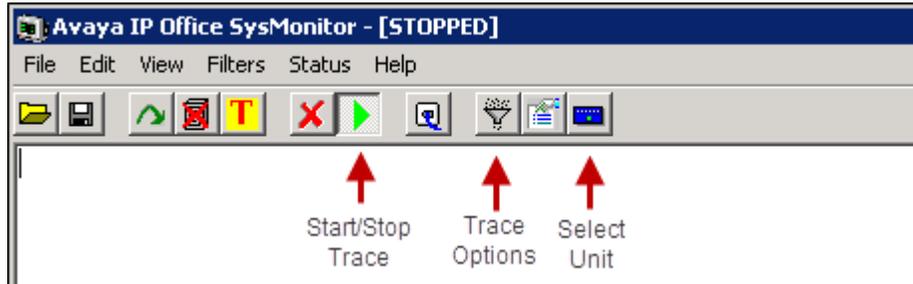
Select the **Alarms** tab and verify that no alarms are active on the SIP line.

The screenshot shows the 'Alarms' tab selected. The title is 'Alarms for Line: 17 SIP sip://10.5.5.152'. Below the title is a table with the following columns: Last Date Of Error, Occurrences, and Error Description.

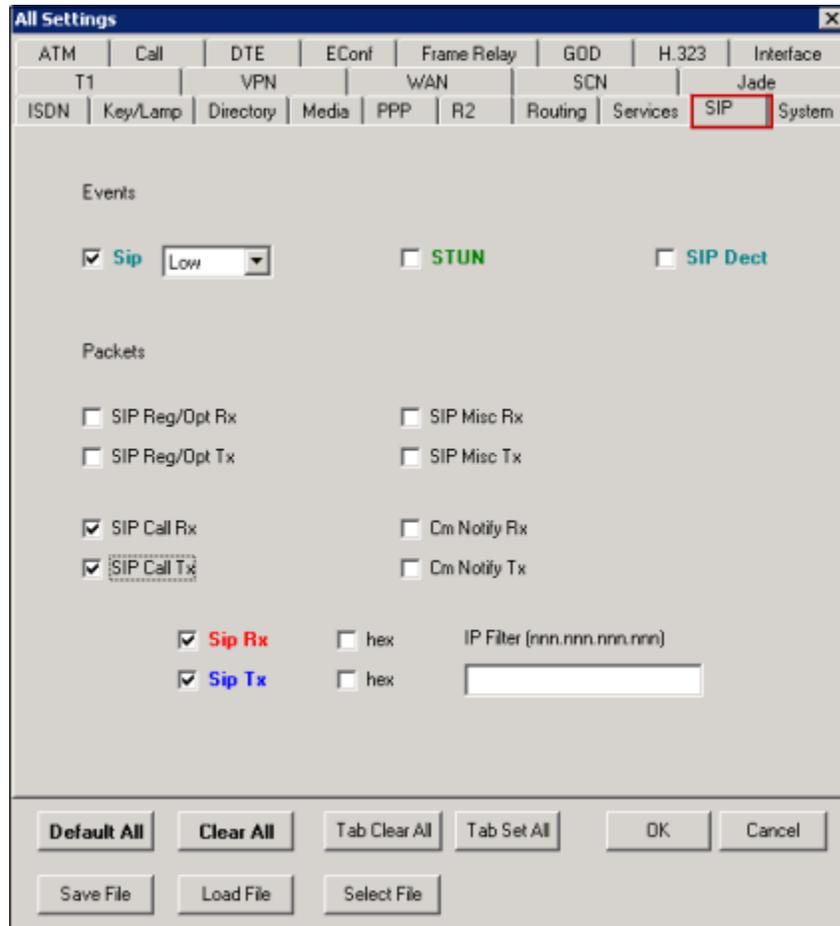
Last Date Of Error	Occurrences	Error Description

8.1.2. Monitor

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.



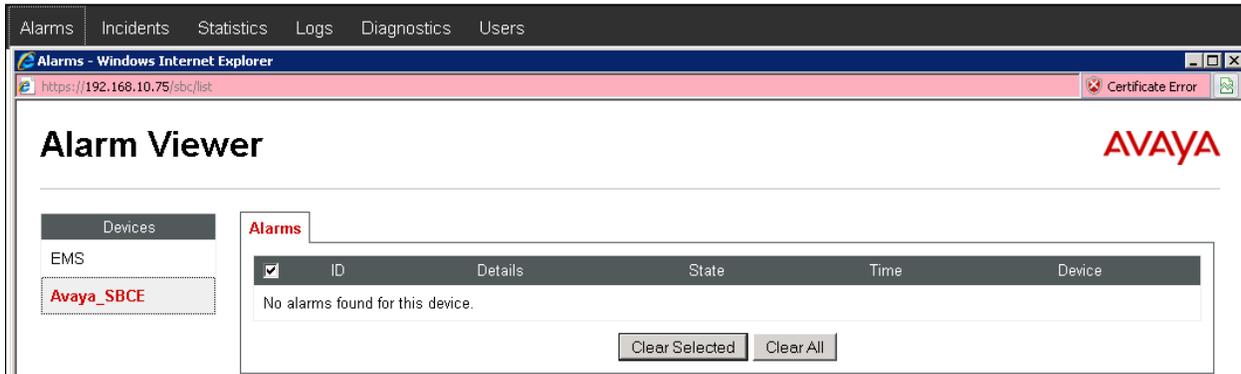
Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting to the desired color.



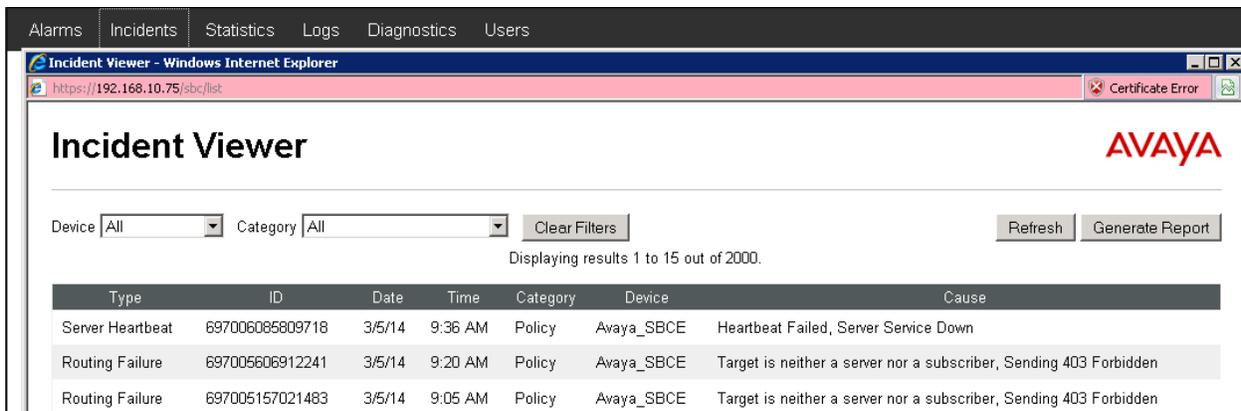
8.2. Avaya Session Border Controller for Enterprise

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

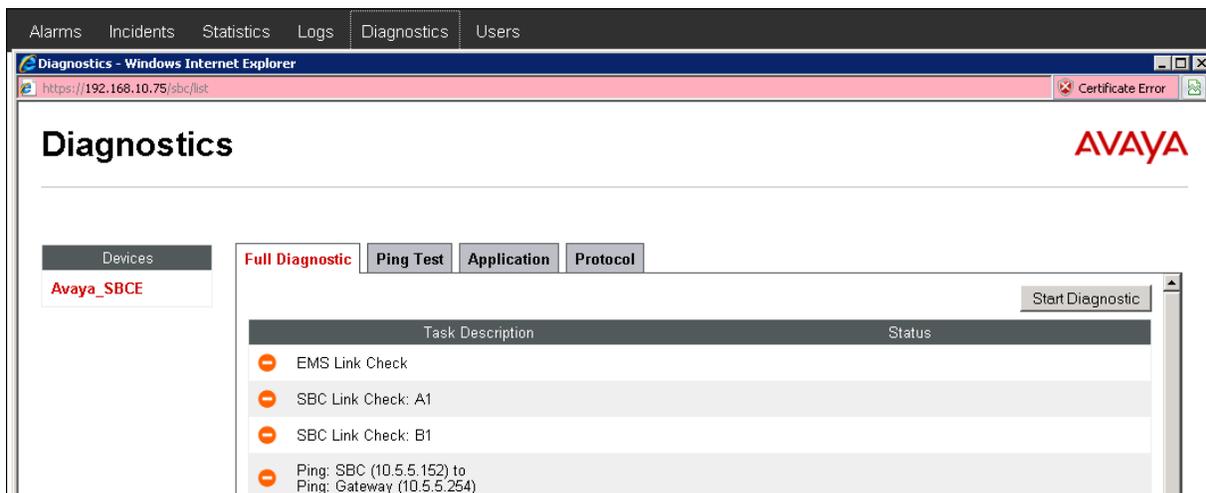
Alarms: Provides information about the health of the SBC.



Incidents: reports of anomalies, errors, policies violations, etc



Diagnostics: variety of tools to test and troubleshoot the SBC network connectivity.



Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

Session Border Controller for Enterprise AVAYA

Trace: Avaya_SBCE

Devices: Avaya_SBCE

Call Trace | **Packet Capture** | Captures

Packet Capture Configuration

Status: Ready

Interface: Any

Local Address IP[Port]: All

Remote Address: *

Protocol: All

Maximum Number of Packets to Capture: 10000

Capture Filename: test1.pcap
Using the name of an existing capture will overwrite it.

Start Capture Clear

Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

Call Trace | Packet Capture | **Captures**

Refresh

File Name	File Size (bytes)	Last Modified
test1_20140218134137.pcap	299,008	February 18, 2014 1:42:30 PM GMT

Delete

9. Conclusion

These Application Notes describe the procedures required to configure SIP trunk connectivity between Avaya IP Office release 9.0 and Avaya Session Border Controller with the Axtel SIP Trunking service, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the exception of the observations/limitations described in **Section 2.2**.

10. Additional References

- [1] *Avaya IP Office 9.0, Installing IP500/IP500 V2*. Document 15-601042, February 2014
<https://downloads.avaya.com/css/P8/documents/100174004>
- [2] *Avaya IP Office Manager Release 9.0*, Document 15-601011, January 2014
<https://downloads.avaya.com/css/P8/documents/100174478>
- [3] *Administering Avaya Flare® Experience for iPad devices and Windows, Release 9.0*, September 2013
<https://downloads.avaya.com/css/P8/documents/100175132>
- [4] *IP Office System Status Application*, Document Number 15-601758, May 2013
<https://downloads.avaya.com/css/P8/documents/100150298>
- [5] *Avaya IP Office Knowledgebase*
<http://marketingtools.avaya.com/knowledgebase>
- [6] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013
<https://downloads.avaya.com/css/P8/documents/100168983>
- [7] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, January 2014
<https://downloads.avaya.com/css/P8/documents/100168982>
- [8] *Avaya Session Border Controller for Enterprise Release Notes*. Release 6.2.1, December 2013
<https://downloads.avaya.com/css/P8/documents/100177285>
- [9] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*, Release 6.2 FP1. December 2013.
<https://downloads.avaya.com/css/P8/documents/100177285>

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

Product documentation for the Axtel SIP Trunking service is available from Axtel.

©2014 Avaya Inc. All Rights Reserved.

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

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