



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunk Service with Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0

Abstract

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

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

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

Table of Contents

1. Introduction.....	4
2. General Test Approach and Test Results.....	4
2.1 Interoperability Compliance Testing	4
2.2 Test Results	5
2.3 Support.....	6
3. Reference Configuration.....	6
4. Equipment and Software Validated	8
5. Configure IP Office	9
5.1 Licensing.....	9
5.2 LAN1 Settings	9
5.3 System Telephony Settings.....	13
5.4 Twinning Calling Party Settings.....	14
5.5 Codec's settings	14
5.6 IP Route	15
5.7 Administer SIP Line	16
5.7.1 Create a New SIP Trunk from Template	16
5.7.2 SIP Line Tab	19
5.7.3 Transport Tab.....	20
5.7.4 SIP URI Tab.....	21
5.7.5 VoIP Tab.....	22
5.8 Extension.....	24
5.9 Users	25
5.10 Incoming Call Route.....	29
5.11 Outbound Call Routing.....	31
5.11.1 Short Codes and Automatic Route Selection.....	31
5.12 Privacy/Anonymous Calls	33
5.13 Save Configuration	34
6. Configure the Avaya Session Border Controller for Enterprise.....	35
6.1 Log into the Avaya Session Border Controller for Enterprise.....	35
6.2 Global Profiles	38
6.2.1 Server Interworking profile - Avaya-IPO	38
6.2.2 Server Interworking profile – SP General	40
6.2.3 Routing Profiles	41
6.2.4 Server Configuration.....	43
6.2.5 Topology Hiding.....	46
6.2.6 Signaling Manipulation.....	48
6.3 Domain Policies	48
6.3.1 Create Application Rules	48
6.3.2 Media Rules	49
6.3.3 Signaling Rules	50
6.3.4 End Point Policy Groups.....	51
6.4 Device Specific Settings	53
6.4.1 Network Management.....	53

6.4.2 Media Interface	55
6.4.3 Signaling Interface	56
6.4.4 End Point Flows	57
7. MTS Allstream SIP Trunking Configuration	60
8. Verification and Troubleshooting	61
8.1 Verification Steps.....	61
8.2 Protocol Traces	61
8.3 IP Office System Status	61
8.4 IP Office Monitor.....	63
8.5 Avaya Session Border Controller for Enterprise	65
9. Conclusion	70
10. References.....	71

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service in between the service provider MTS Allstream and Avaya IP Office solution.

In the sample configuration, the Avaya IP Office solution consists of Avaya IP Office (IP Office) 500v2 Release 9.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2, Avaya IP Office Video Softphone, Avaya Flare® Experience for Windows and Avaya Deskphones, including SIP, H.323, digital, and analog. The Remote Worker capability was also tested. The Avaya SBCE provides security for the Avaya IP Office solution, as well as interoperability features for the SIP trunk.

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

2. General Test Approach and Test Results

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

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

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

2.1 Interoperability Compliance Testing

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

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

- Incoming and outgoing PSTN calls to/from Avaya Flare® Experience for Windows.
- Dialing plans including long distance, international, outbound toll-free, etc.
- Caller ID presentation and Caller ID restriction.
- Codec G.729A and G.711MU.
- T.38 fax.
- Proper early media transmissions.
- DTMF tone transmissions per RFC 2833.
- Voicemail navigation for incoming and outgoing calls.
- Telephony features such as hold and resume, call transfer, call forward and conferencing.
- Off-net call forwards and transfers.
- Mobility Twinning of incoming calls to mobile phones.
- Response to incomplete call attempts and trunk errors.

Note: Remote worker was tested as part of this solution; the configuration necessary to support remote workers is beyond the scope of these Application Notes and will not be discussed in these Application Notes.

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

The following items are not supported:

- **SIP REFER.**

2.2 Test Results

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

- **T.38 Fallback** – With **Fax Transport Support** set as **T38 Fallback** in IP Office (SIP Line→VoIP), incoming fax calls (PSTN→IP Office), will fail to connect with G.711 transport when T.38 is disabled at the Service Provider. Outbound fax calls will successfully default to G.711 transport. The problem is only seen with incoming (PSTN→IP Office) fax calls. **T.38** transport was successfully tested in both directions (PSTN→IP Office and IP Office→PSTN). For this solution Avaya recommends only using **T.38** as the fax transport (with **Transport Support** set as **T38** in IP Office (SIP Line→VoIP)). This issue is under investigation by Avaya.
- **Direct Media** – With Direct Media enabled in IP office, when calling IVR systems (or any recorded messaging system), from IP Office, a noticeable clipping of the recorded announcement/message is heard when IP Office sends the re-Invite to establish the direct media connection to the IP Phone. Testing was done with Direct Media disabled in IP Office. This issue is under investigation by Avaya.
- **Codec Lockdown on Outbound Calls** – On outbound calls, MTS Allstream responds to the INVITE request sent by IP Office, with multiple codecs instead of selecting one from the INVITE SDP list. IP Office uses the first compatible codec in the list. This behavior has no user impact, calls were successful.
- **INVITE message with m:audio and m:image in the SDP** – Voice/audio calls made from the PSTN to IP Office, mapped to a particular DID, contained multiple “m:” lines in the SDP of the INVITE message sent by MTS Allstream, with “m:” lines in the following order:

m:audio first (top) followed by m:image second (bottom). When the call was answered at the IP Office station, IP Office sends the 200 OK with “m:” lines in the reverse order or m:image first (top) followed by m:audio second (bottom), this behavior resulted in one-way audio. This behavior only occurs when “Fax Transport Support” is set to “None” under SIP Line/VoIP. With “Fax Transport Support” set only as “T.38” (Avaya recommended value for this solution) this behavior doesn’t occur, with it set as “T.38” IP Office will only include m:audio in the 200 OK message (m:image in not included) resulting in good audio in both directions. Since Avaya recommends only using **T.38** as the fax transport for this solution this behavior will not be seen.

- **Disable the use of PAI** – IP Office SIP Line; disable the use of P-Asserted-Identity (PAI) header. Disabling the use of the PAI header in IP Office provided the expected calling party number, such as for calls forwarded to the PSTN and for call twinning scenarios.

2.3 Support

For technical support on the MTS Allstream SIP Trunking service, visit the MTS Allstream customer support web page at <https://www.mts.ca/mts/contact+us>

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

3. Reference Configuration

Figure 1 below illustrates the test configuration. It shows a simulated enterprise site connected to the MTS Allstream network through the public internet.

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

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

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

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

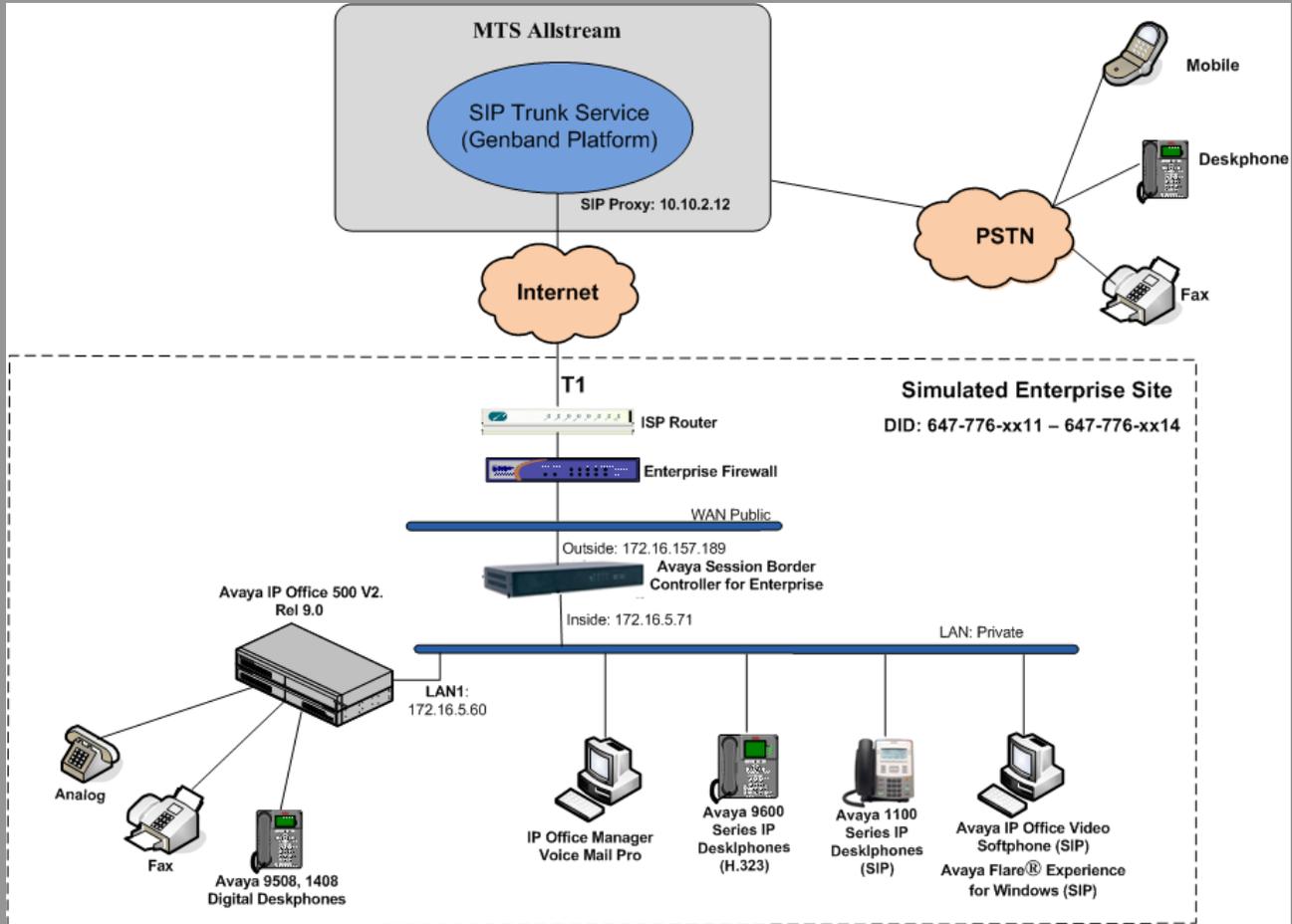


Figure 1: Avaya Interoperability Test Lab Configuration.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to MTS Allstream (refer to **Section 5.11**). The short code 9 was stripped off by Avaya IP Office but the remaining N digits were sent unaltered to the network. Since MTS Allstream is a Canadian company, and Canada is a country member of the North American Numbering Plan (NANP), the users dialed 10 digits for local calls, including the area code, and 11 (1 + 10) digits for other calls between the NANP.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the enterprise. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that SIP and RTP traffic between the service provider and the enterprise must be allowed to pass through these devices.

4. Equipment and Software Validated

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

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

MTS Allstream SIP Trunk Service	
Equipment/Software	Release/Version
Genband S3 Session Border Controller	7.1.13.1
Nortel CS2K	CVM15

5. Configure IP Office

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

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

5.1 Licensing

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

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

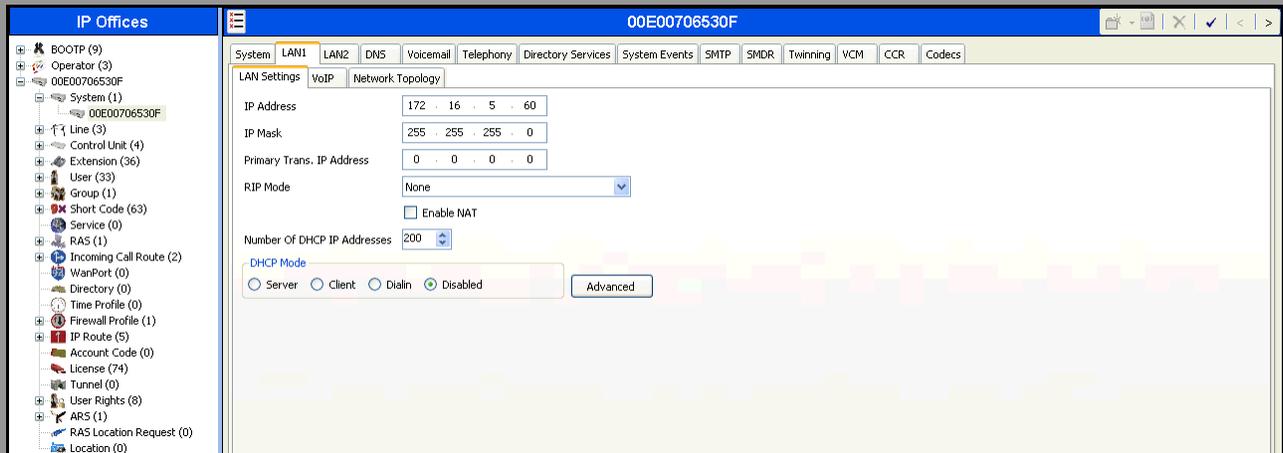
Feature	License Key	Instances	Status	Expiry Date	Source
VMPro Recordings Administrators	j4@Jwv6A5ksULB39ML...	255	Valid	Never	ADI Nodal
VMPro Outlook Interface	Zy5uTP6GdNqgas8ah7x...	255	Valid	Never	ADI Nodal
VMPro TTS (Scansoft)	hq9vF995VASISLmaBE...	255	Valid	Never	ADI Nodal
VMPro TTS (Generic)	nIcm7z54DDHh37uq9Im...	255	Valid	Never	ADI Nodal
Conferencing Center	CAH4HkdnvX2Idh8GrJ...	255	Obsolete	Never	ADI Nodal
Small Office Edition VCM (channels)	2K078F6LW4u32P5C_u9...	255	Obsolete	Never	ADI Nodal
Small Office Edition WiFi	eAWw835V03zsc6RT91...	255	Obsolete	Never	ADI Nodal
IPSec Tunneling	MIKcnXtjMKys3WedR2pt...	255	Valid	Never	ADI Nodal
Proactive Reporting	tDp8nbs9N@bd8jHV9y...	255	Valid	Never	ADI Nodal
Report Viewer	Tvct73mdgdGtXkV6h5_Fr...	255	Valid	Never	ADI Nodal
Mobility Features	0IClURgHvK0xjNk9k9o1...	255	Obsolete	Never	ADI Nodal
Advanced Small Community Networking	DaQJ7VesvUJFLz5vopY...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	T398k8v6ds41Rg1lq...	255	Valid	Never	ADI Nodal
IP500 Upgrade Standard to Prof...	QaHgn76v9j6CDJGPs9D...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	JaHtH4VFXjDX22bwrUzXk...	4	Valid	Never	ADI Nodal
SIP Trunk Channels	ISCOqGBVDUscEiXBLz29...	255	Valid	Never	ADI Nodal
VPN IP Extensions	@qmq3fOoRSS_R3RMVfy...	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional chan...	2TXC@OoNQxtZoPABD...	255	Valid	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	hXkRxBVCEKwD0w5vDe...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Standard E...	4AOCGBVSD9dALnCHRJH...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Profession...	dlyY_Dds5Uq7Sec3R9MT...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Stand...	dy95669YS_NKS8AAo_L...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Profes...	LHFz26B6TeQKv93h@...	255	Valid	Never	ADI Nodal

5.2 LAN1 Settings

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

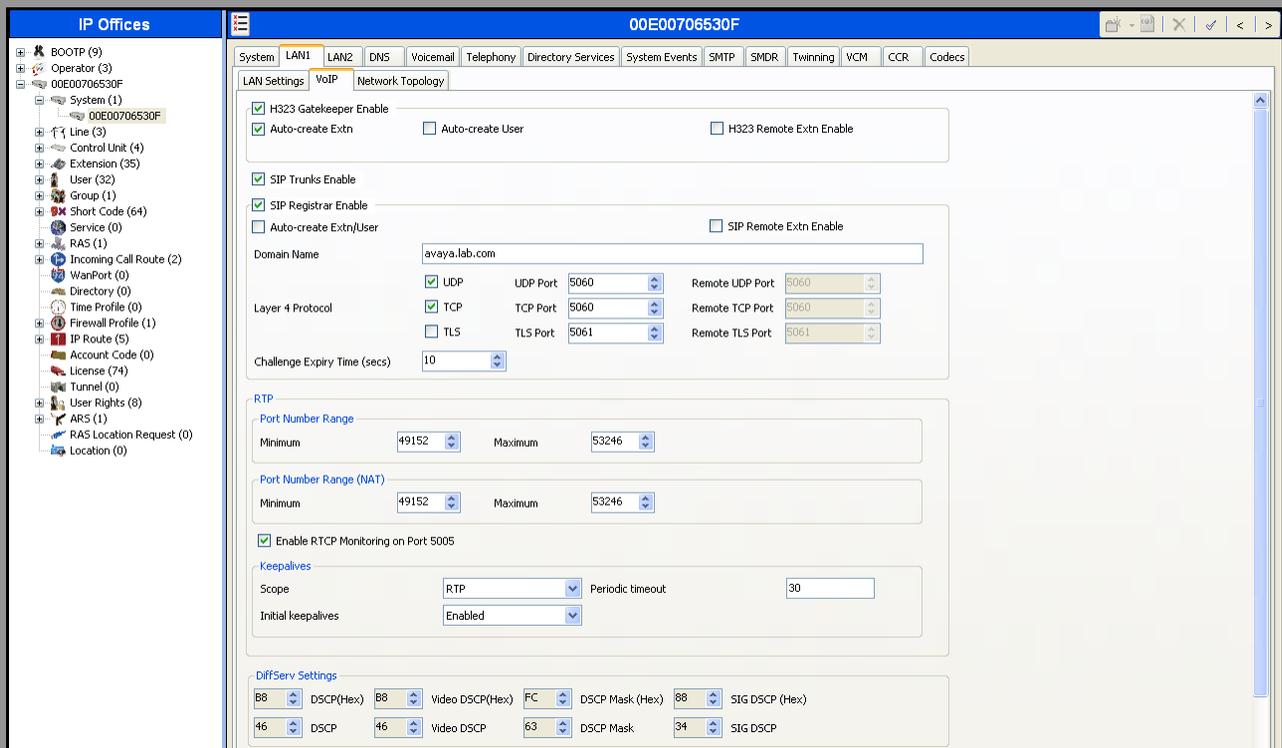
navigate to the LAN1→ LAN Settings tab. The LAN1 settings for the compliance testing were configured with following parameters.

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



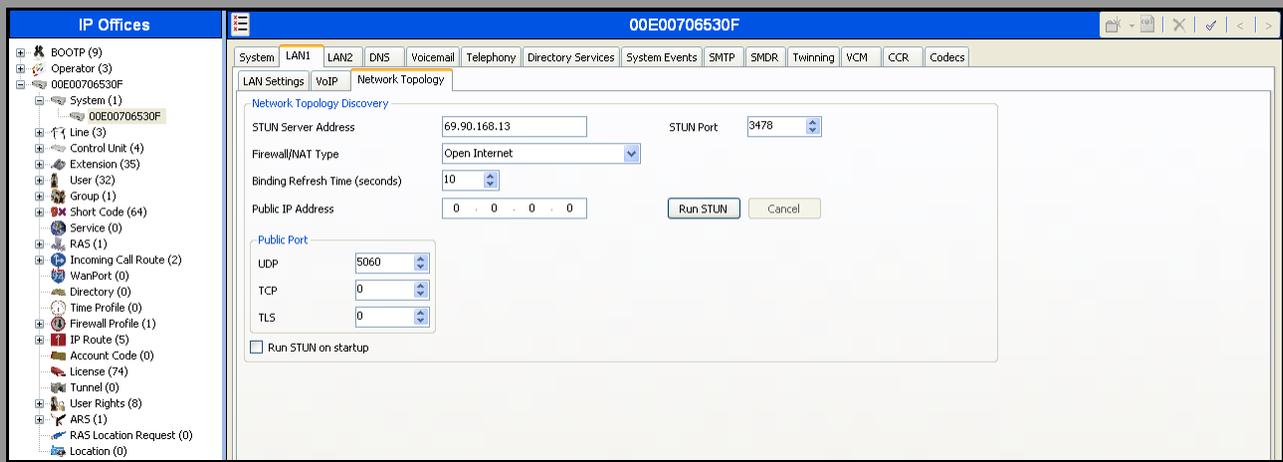
The **VoIP** tab as shown in the screenshot below was configured with following settings.

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphone using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to MTS Allstream.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphone to register using the SIP protocol.
- Enter the Domain Name of the enterprise under **Domain Name**.
- Verify the **UDP Port** and **TCP Port** numbers under **Layer 4 Protocol** are set to **5060**.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- In the **Keepalives** section at the bottom of the page, set the **Scope** field to **RTP**, **Periodic Timeout to 30**, and **Initial keepalives to Enabled**. This will cause the IP Office to send RTP keepalive packets at the beginning of the calls and every 30 seconds thereafter if no other RTP traffic is present.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown).



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

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

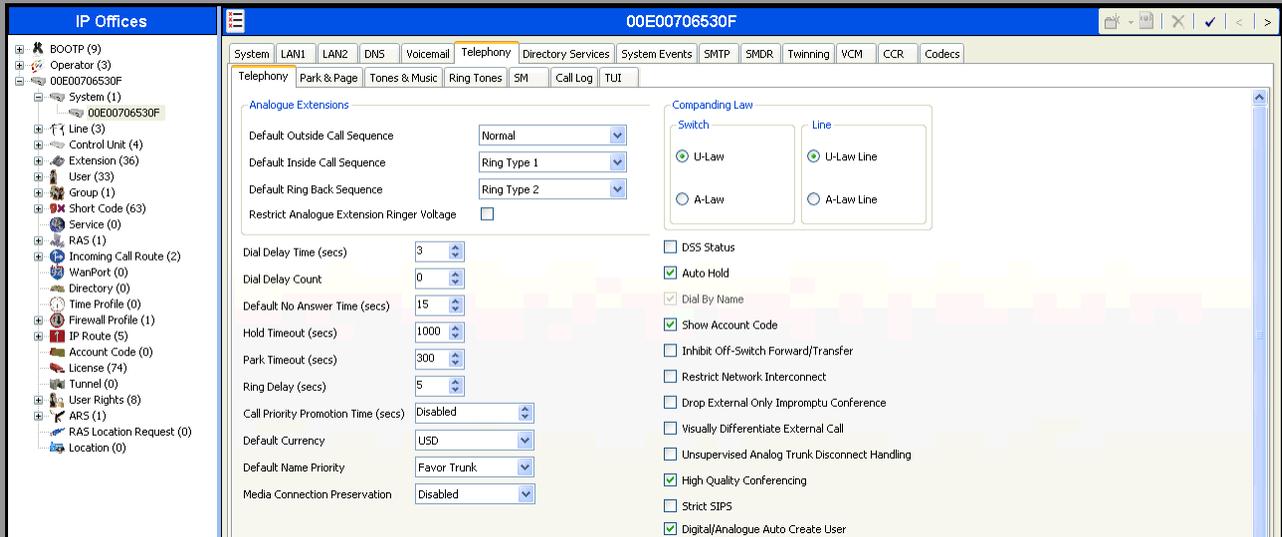


In the compliance test, the **LAN1** interface was used to connect Avaya IP Office to the enterprise private network (LAN), **LAN2** was not used.

5.3 System Telephony Settings

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

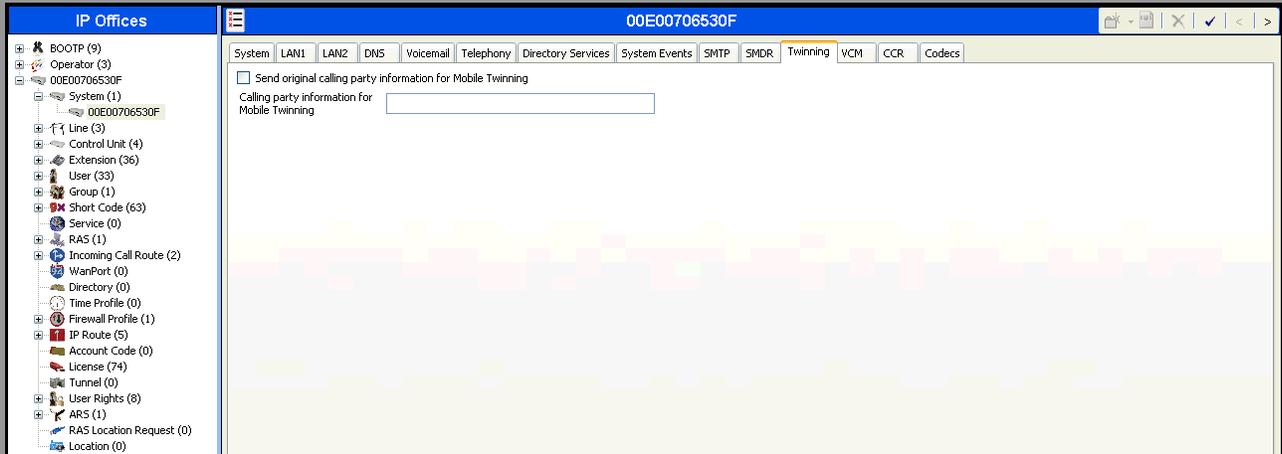
- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.
- All other parameters should be set according to customer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



5.4 Twinning Calling Party Settings

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

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



5.5 Codec's settings

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

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

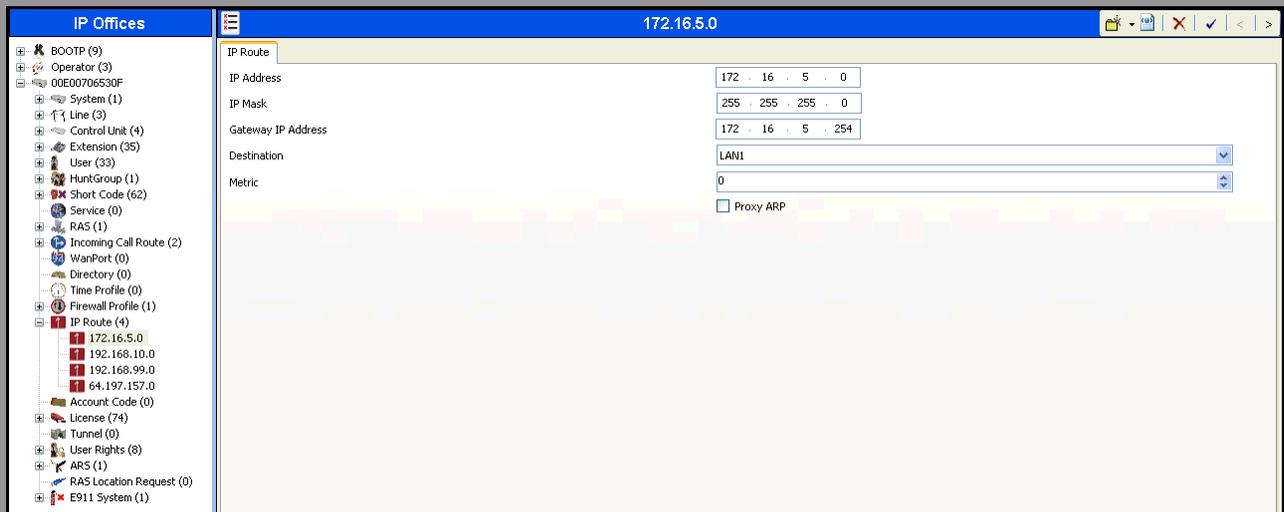
The **Codec's** settings are shown in the screenshot below with G.729(a) and G.711ULAW selected in prioritized order.



5.6 IP Route

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

- Set the **IP Address** and **IP Mask**.
- Set **Gateway IP Address** to the IP Address of the router used to reach the external network.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click OK to commit (not shown).



5.7 Administer SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the MTS Allstream SIP Trunk Service. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.7.1** 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 5.7.2 – 5.7.5**.

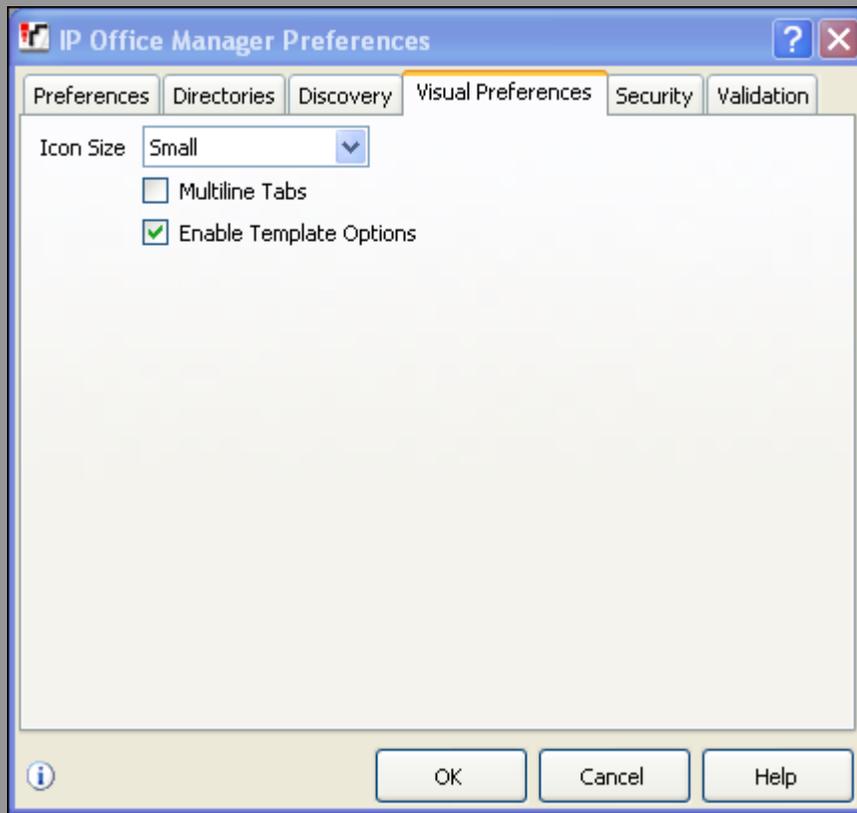
Also, the following SIP Line settings are not supported on Basic Edition:

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

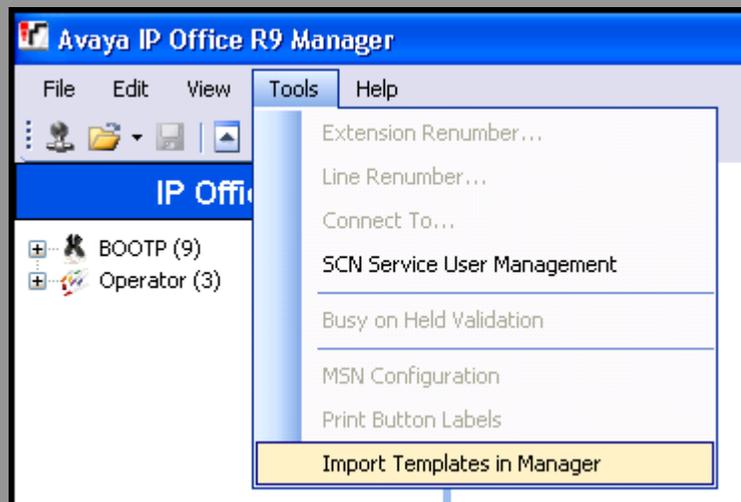
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.7.2 – 5.7.5**.

5.7.1 Create a New SIP Trunk from Template

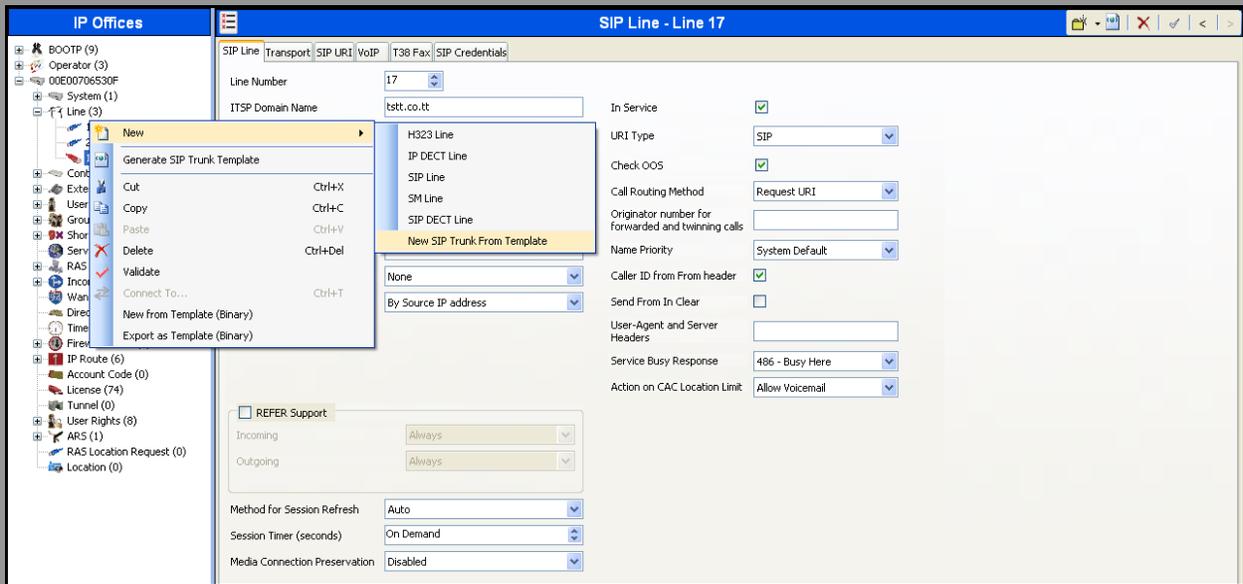
1. Copy the template file to the computer where IP Office Manager is installed. If needed rename the template file to **CA_MTS Allstream_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.
2. Verify that template options are enabled in IP Office Manager. In 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 is **C:\Program Files\Avaya\IP Office\Manager\Templates**.



4. 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.
5. 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**.



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



Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.7.2 – 5.7.5**.

Alternatively, a SIP Line can be created manually with the parameters shown below. To create a SIP line manually, begin by navigating to **Line** in the Navigation Pane. Right-click and select **New** → **SIP Line**.

5.7.2 SIP Line Tab

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

- Leave the **ITSP Domain Name** blank.
- Verify that **In Service** box is checked.
- Verify that **Check OOS** box is checked. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Call Routing Method** is set to **Request URI**.
- Set **Send Caller ID** to **Diversion Header**.
- Uncheck the **REFER support** box. IP Office will not send REFER messages for calls that are transferred back to the PSTN. MTS Allstream doesn't support SIP REFER messages.
- Set **Method for Session Refresh** to **Auto**.
- Set **Session Timer (Seconds)** to **On Demand**.
- Set **Media Connection Preservation** to **Disabled**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).

The screenshot shows the configuration window for a SIP Line in IP Office. The window title is "SIP Line - Line 17". The left pane shows a tree view of the system configuration, with "Line (3)" expanded to show "Line 17" selected. The main pane displays the configuration for the selected line, with tabs for "SIP Line", "Transport", "SIP URI", "VoIP", "T38 Fax", and "SIP Credentials".

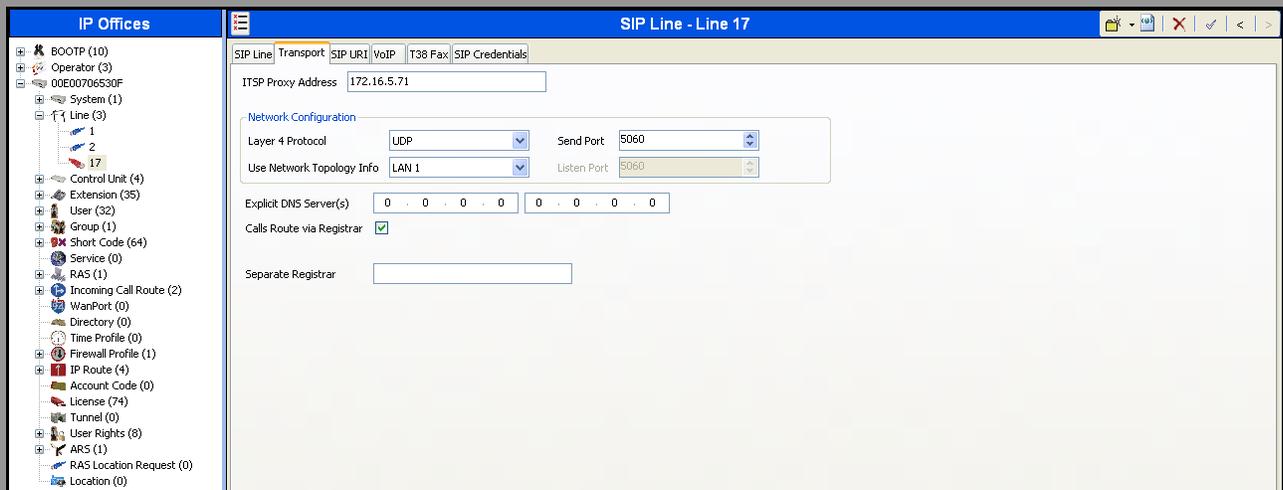
The configuration parameters are as follows:

- Line Number: 17
- ITSP Domain Name: (blank)
- Prefix: (blank)
- National Prefix: 0
- Country Code: (blank)
- International Prefix: (blank)
- Send Caller ID: Diversion Header
- Association Method: By Source IP address
- REFER Support: (unchecked)
 - Incoming: Auto
 - Outgoing: Auto
- Method for Session Refresh: Auto
- Session Timer (seconds): On Demand
- Media Connection Preservation: Disabled
- In Service:
- URI Type: SIP
- Check OOS:
- Call Routing Method: Request URI
- Originator number for forwarded and twinning calls: (blank)
- Name Priority: System Default
- Caller ID from From header:
- Send From In Clear:
- User-Agent and Server Headers: (blank)
- Service Busy Response: 486 - Busy Here
- Action on CAC Location Limit: Allow Voicemail

5.7.3 Transport Tab

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

- Set the **ITSP Proxy Address**, this address was set to the inside IP Address of the Avaya SBCE or **172.16.5.71** as shown in **Figure 1**.
- Set the **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **LAN1** as configured in **Section 5.2**.
- Set the **Send Port** to **5060**.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



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

- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**,
- Set **PAI** to **None**. IP Office will not include the PAI header in SIP messaging. Removing the use of the PAI header provided the expected calling party number across the PSTN carriers encountered in the compliance test, especially for the call forwarding and twinning scenarios.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya IP Office configuration interface. On the left is a tree view showing the hierarchy of IP Office components, including BOOTP, Operator, System, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WanPort, DirectoryPort, Time Profile, Firewall Profile, IP Route, Account Code, License, Tunnel, User Rights, ARS, RAS Location Request, and Location. The main window is titled 'SIP Line - Line 17' and shows the 'SIP URI' tab. A table lists the SIP URI entries:

Channel	Groups	Via	Local URI	Contact	Display Name	PAI
1	17 17	1...				

Below the table is an 'Edit Channel' dialog box with the following fields:

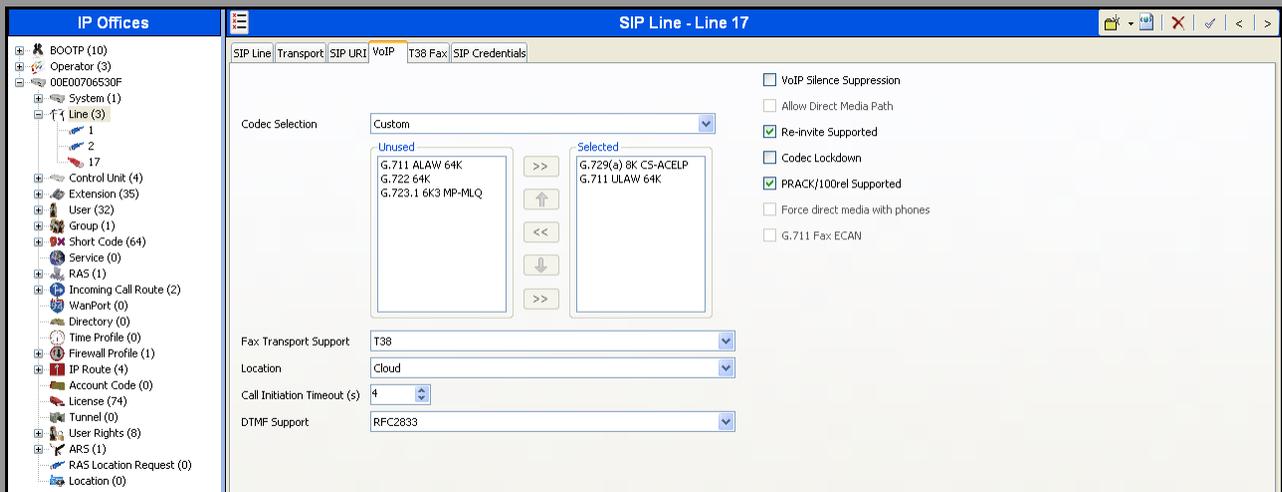
- Via: 172.16.5.60
- Local URI: Use Internal Data
- Contact: Use Internal Data
- Display Name: Use Internal Data
- PAI: None
- Registration: 0: <None>
- Incoming Group: 17
- Outgoing Group: 17
- Max Calls per Channel: 10

Buttons for 'Add...', 'Remove', 'Edit...', 'OK', and 'Cancel' are visible.

5.7.5 VoIP Tab

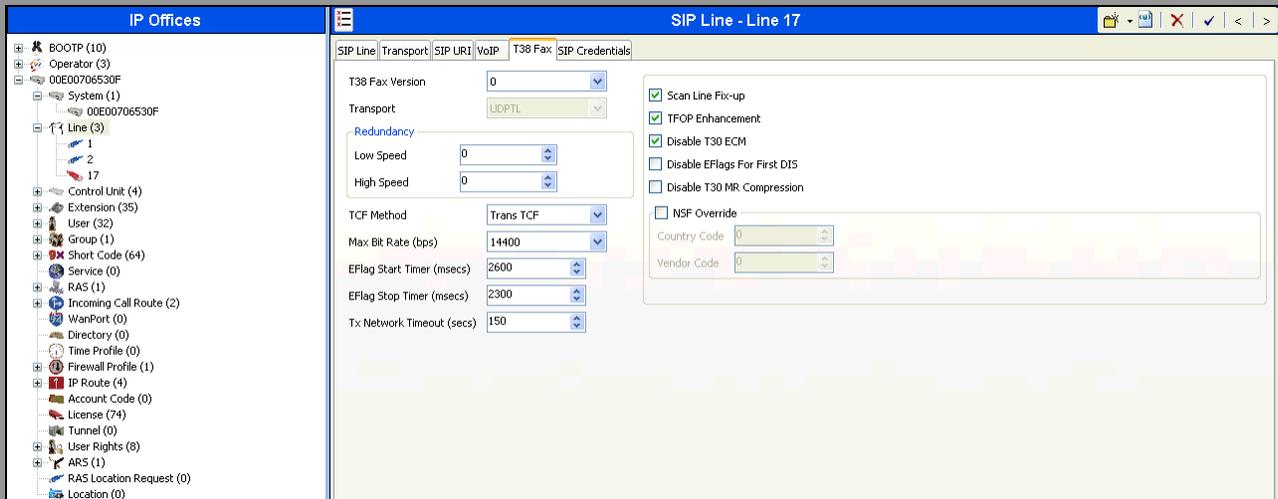
Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- In the sample configuration, the **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codec's to be specified. The buttons allow setting the specific order of preference for the codec's to be used on the line, as shown. MTS Allstream supports codec's G.729A and G.711ULAW (or G.711MU).
- Set **Fax Transport Support** to **T.38** (refer to **Section 2.2**).
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Verify that **Allow Direct Media Path** is unchecked. Testing was done with Direct Media disabled (Refer to **Section 2.2**).
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check the **PRACK/100rel Supported** box, to advertise the support for reliable provisional responses and Early Media to MTS Allstream.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



Select the **T38 Fax** tab to set the Fax over Internet Protocol parameters of the SIP line. Set the parameters as shown below.

- Uncheck **Use Default Values** at the bottom of the screen.
- Set **T38 Fax Version** to **0**. MTS Allstream SIP Trunking supports T.38 fax version 0.
- Set **Max Bit Rate (bps)** to 14400, the highest fax bit rate that Avaya IP Office supports for T.38 faxing.
- Check the **Disable T30 ECM** option.
- Default values may be used for all other parameters.
- Click OK to commit (not shown).



5.8 Extension

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

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

The screenshot shows the 'IP Offices' configuration window with the 'Extn' tab selected. The left sidebar shows a tree view of the system hierarchy, with '8009 3042' highlighted under the 'Extension (36)' folder. The main configuration area displays the following fields:

- Extension Id: 8009
- Base Extension: 3042
- Phone Password: (empty)
- Caller Display Type: On
- Reset Volume After Calls:
- Device Type: Avaya 9620
- Location: Automatic
- Module: 0
- Port: 0
- Disable Speakerphone:

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

The screenshot shows the 'IP Offices' configuration window with the 'VOIP' tab selected for extension 8009 3042. The left sidebar shows a tree view of the system hierarchy, with '8009 3042' highlighted under the 'Extension (35)' folder. The main configuration area displays the following fields:

- IP Address: 0 . 0 . 0 . 0
- MAC Address: 00 00 00 00 00 00
- Codec Selection: System Default
- Reserve License: None
- TDM->IP Gain: Default
- IP->TDM Gain: Default
- Supplementary Services: None
- VoIP Silence Suppression:
- Enable Faststart for non-Avaya IP phones:
- Out Of Band DTMF:
- Local Tones:
- Allow Direct Media Path:

The codec selection area shows a list of codecs. The 'Selected' list contains G.729(a) 8K CS-ACELP and G.711 ULAW 64K. The 'Unused' list contains G.711 ALAW 64K, G.722 64K, and G.723.1 6K3 MP-MLQ.

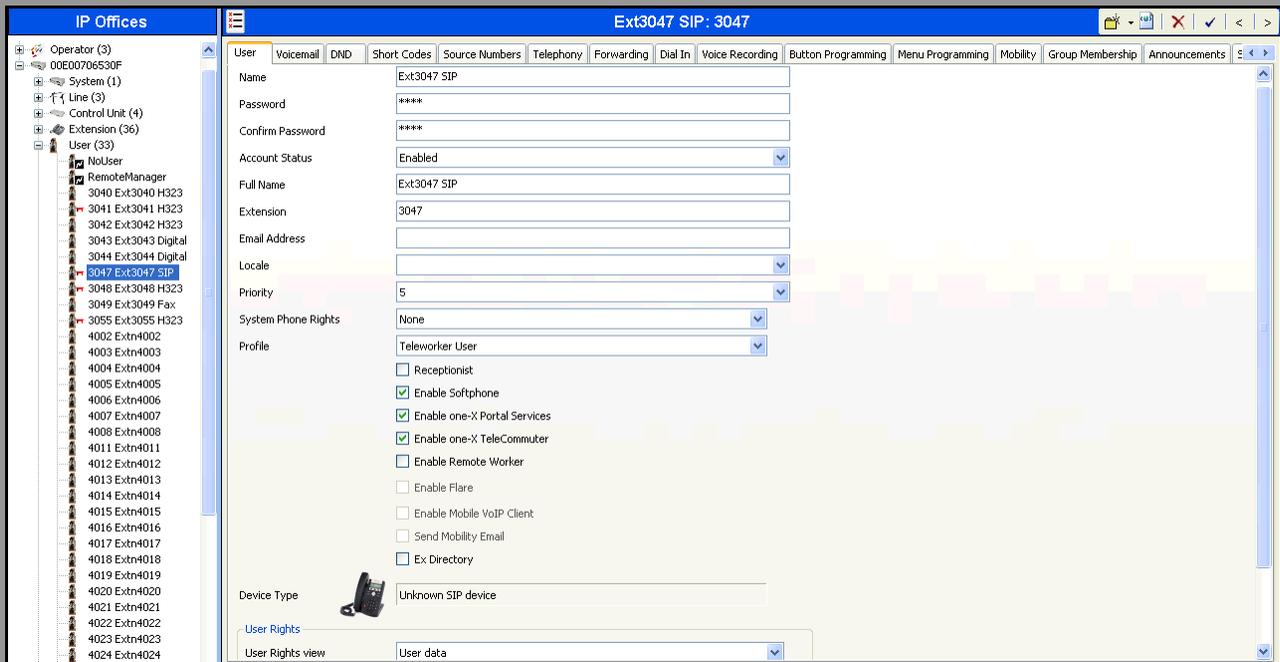
5.9 Users

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

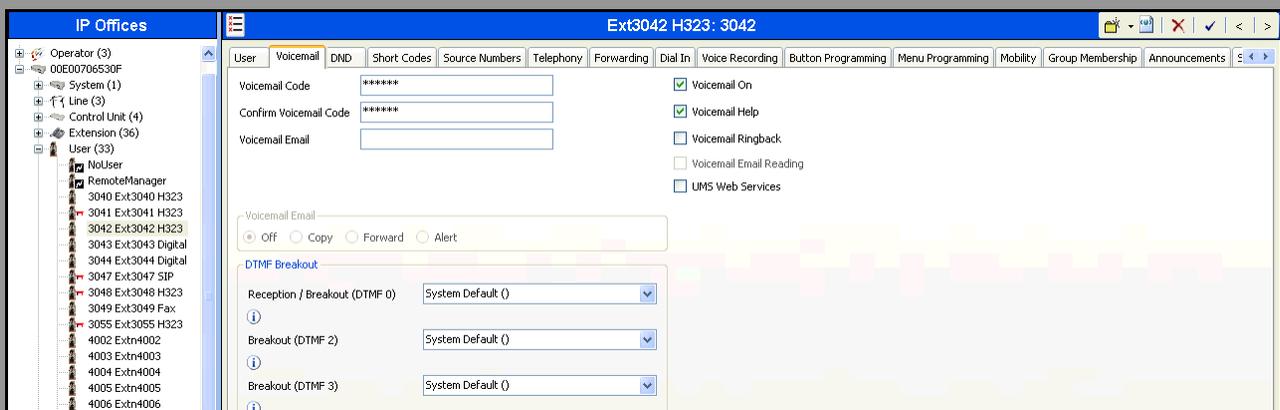
The screenshot displays the Avaya user configuration interface. On the left, the 'IP Offices' navigation pane shows a tree structure with 'User (33)' expanded, and '3042 Ext3042 H323' selected. The main area shows the configuration for this user, with the title bar indicating 'Ext3042 H323: 3042'. The configuration is organized into tabs: 'User', 'Voicemail', 'DND', 'Short Codes', 'Source Numbers', 'Telephony', 'Forwarding', 'Dial In', 'Voice Recording', 'Button Programming', 'Menu Programming', 'Mobility', 'Group Membership', and 'Announcements'. The 'User' tab is active, showing the following fields and options:

- Name: Ext3042 H323
- Password: ****
- Confirm Password: ****
- Account Status: Enabled
- Full Name: Ext3042 H323
- Extension: 3042
- Email Address: (empty)
- Locale: (empty)
- Priority: 5
- System Phone Rights: None
- Profile: Basic User
- Receptionist:
- Enable Softphone:
- Enable one-X Portal Services:
- Enable one-X TeleCommuter:
- Enable Remote Worker:
- Enable Flare:
- Enable Mobile VoIP Client:
- Send Mobility Email:
- Ex Directory:
- Device Type: Avaya 9620
- User Rights: User data

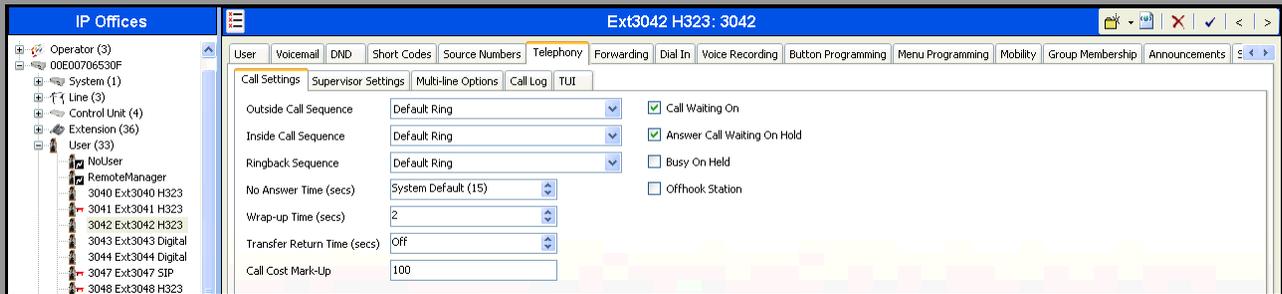
In the example below, the name of the user is “Ext3047 SIP”. This is an Avaya IP Office Softphone user, set the Profile to **Teleworker User** and check **Enable Softphone**.



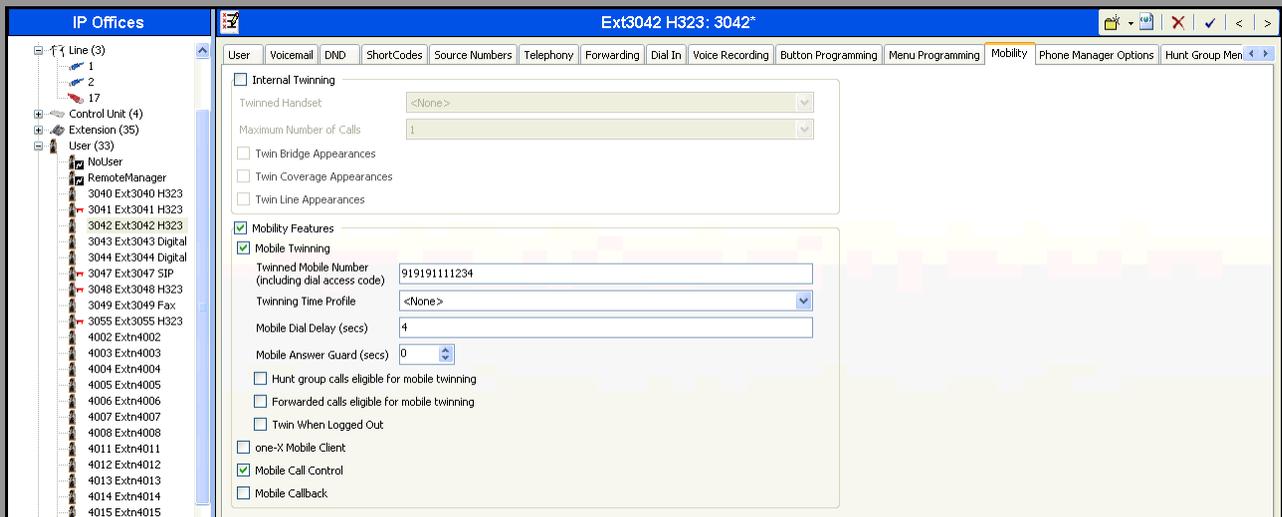
Select the **Voice Mail** tab. The following screen shows the **Voice mail** tab for the user with extension 3042. The **Voice mail On** box is checked. Voicemail password can be configured using the **Voice mail Code** and **Confirm Voice mail Code** parameters. In the verification of these Application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



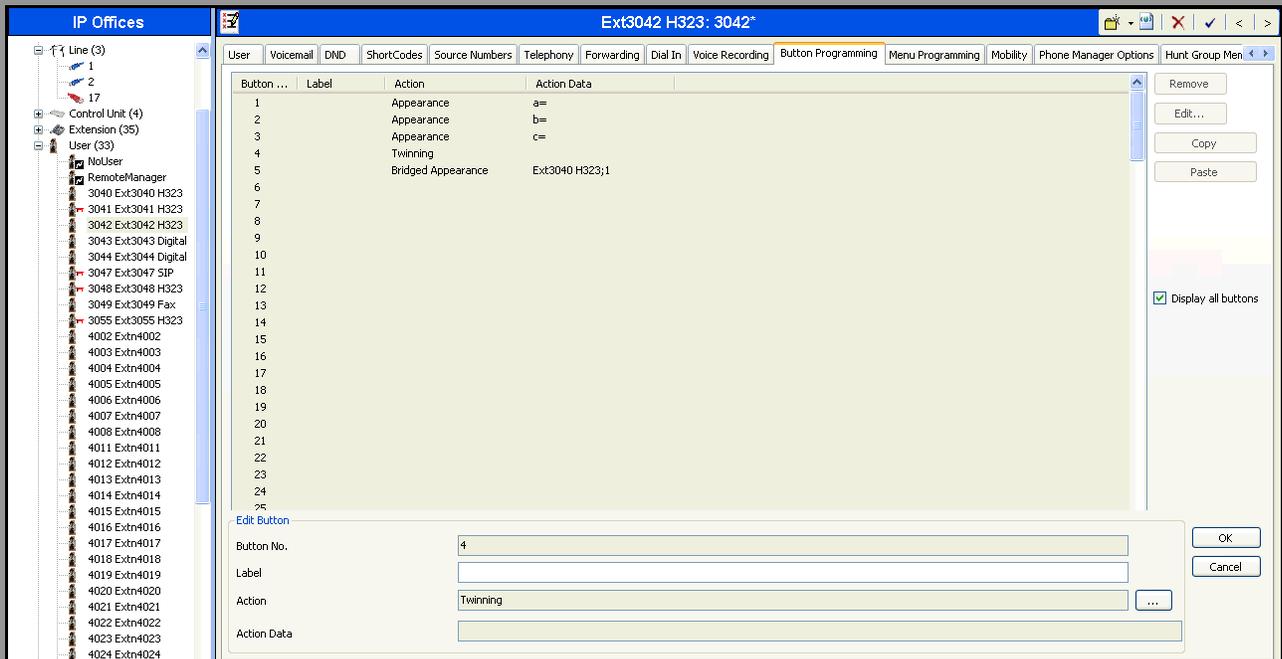
Select the **Telephony** tab, then **Call Settings** tab as shown below. Check the **Call Waiting On** box to allow an Avaya IP Office phone logged in as this extension to have multiple call appearances and for call transfers.



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



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



Select the **SIP** tab, the values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls. In addition, these settings are used to match against the SIP URI of incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.7**). The example below shows the settings for user “Ext3042 H323”. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by MTS Allstream. In the example, DID number **647776xx12** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

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



5.10 Incoming Call Route

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

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

From the left Navigation Pane, right-click on **Incoming Call Route** and select **New**. On the Details Pane (not shown), under the **Standard** tab, set the parameters as show bellow:

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

The screenshot displays the IP Office configuration interface. On the left is a navigation tree with 'Incoming Call Route (2)' selected, showing a sub-item '17'. The main pane shows the configuration for this route under the 'Standard' tab. The configuration fields are as follows:

Parameter	Value
Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

- Under the **Destinations** tab, enter “.” for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User**, which matches the number present on the user part of the incoming Request URI.
- Click OK to commit (not shown).

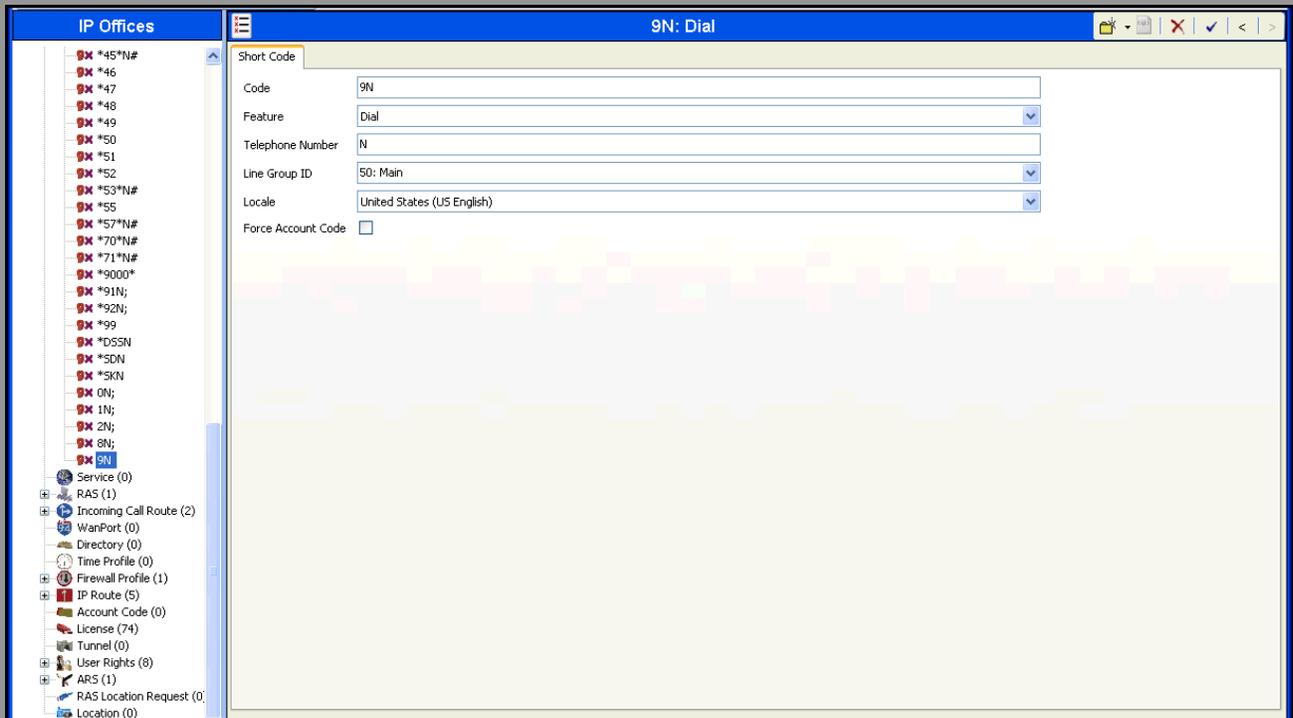


5.11 Outbound Call Routing

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

5.11.1 Short Codes and Automatic Route Selection

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



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

The screenshot displays the configuration for the ARS route 'Main'. The left sidebar shows a tree view of IP Office components, with 'ARS (1)' expanded to show '50: Main'. The main configuration area includes the following fields:

- ARS Route Id: 50
- Route Name: Main
- Dial Delay Time: System Default (3)
- In Service: (checked)
- Time Profile: <None>
- Alternate Route Priority Level: 3
- Alternate Route Wait Time: 30

Additional options include 'Secondary Dial tone' (checked), 'SystemTone' (dropdown), and 'Check User Call Barring' (checked). The 'Out of Service Route' and 'Out of Hours Route' are both set to '<None>'. A table lists the following entries:

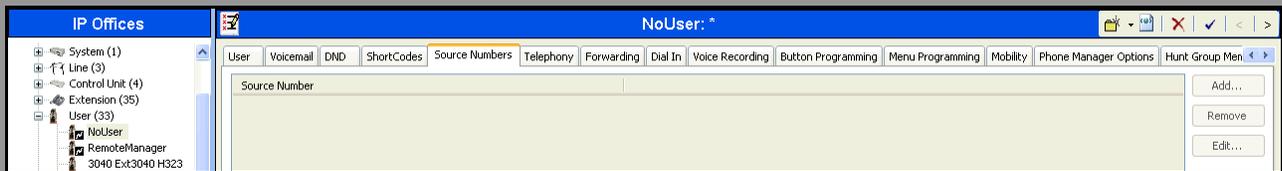
Code	Telephone Number	Feature	Line Group ID
11	911	Dial Emergency	0
911	911	Dial Emergency	0
0XXXXXXXXXXXX	0N	Dial	17
6XXXXXX	6N	Dial	17
8XXXXXXXX	8N	Dial	17
1XXXXXXXX	1N	Dial	17

Buttons for 'Add...', 'Remove', and 'Edit...' are visible to the right of the table.

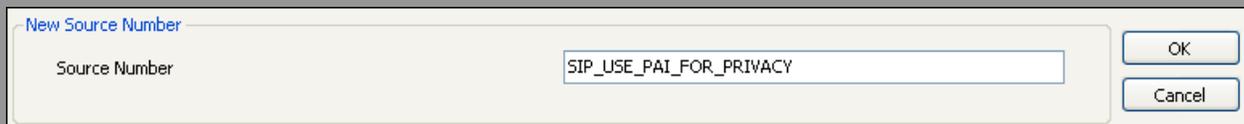
5.12 Privacy/Anonymous Calls

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

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



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



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



5.13 Save Configuration

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

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

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

The screenshot shows a 'Save Configuration' dialog box with the following fields and options:

- IP Office Settings:** 00E00706530F
- Configuration Reboot Mode:** Merge, Immediate, When Free, Timed
- Reboot Time:** 15:22
- Call Barring:** Incoming Calls, Outgoing Calls

Buttons at the bottom: OK, Cancel, Help

6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. 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 additional information on these configuration tasks, see **References Error! Reference source not found., Error! Reference source not found.** and Error! Reference source not found. in **Section 10**.

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

Note: During the next pages and for brevity in these Application Notes not every provisioning step will have a screenshot associated with it.

6.1 Log into the Avaya Session Border Controller for Enterprise

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

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



AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

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

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

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

© 2011 - 2012 Avaya Inc. All rights reserved.

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

The screenshot shows the Avaya Session Border Controller for Enterprise Dashboard. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the AVAYA logo. On the left, a sidebar menu lists various management options under 'Dashboard'. The main content area is titled 'Dashboard' and is divided into four panels: 'Information' (System Time: 10:49:51 AM GMT, Version: 6.2.0.Q48, Build Date: Wed May 22 22:52:47 UTC 2013), 'Installed Devices' (listing 'Sipera'), 'Alarms (past 24 hours)' (None found), and 'Incidents (past 24 hours)' (None found). There is also a 'Notes' section at the bottom with 'No notes found' and an 'Add' button.

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

The screenshot shows the 'System Management' page in the Avaya Session Border Controller for Enterprise. The top navigation bar is the same as in the dashboard. The main header displays 'Session Border Controller for Enterprise' and the AVAYA logo. On the left, the sidebar menu is updated to show 'System Management' as the active page. The main content area is titled 'System Management' and has tabs for 'Devices', 'Updates', 'SSL VPN', and 'Licensing'. The 'Devices' tab is active, showing a table of installed devices:

Device Name (Serial Number)	Management IP	Version	Status	
Sipera (PC931030132)	172.16.5.70	6.2.0.Q48	Commissioned	Reboot Shutdown Restart Application View Edit Delete

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

IMPORTANT! – During the Avaya SBCE installation, the Management interface, (labeled “M1”), of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to have this resolved.

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

X
System Information: Sipera

General Configuration

Appliance Name	Sipera
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
172.16.157.189	172.16.157.189	255.255.255.192	172.16.157.129	B1
172.16.157.189	172.16.157.189	255.255.255.192	172.16.157.129	B1
172.16.157.189	172.16.157.189	255.255.255.192	172.16.157.129	B1
172.16.157.189	172.16.157.189	255.255.255.192	172.16.157.129	B1
172.16.157.189	172.16.157.189	255.255.255.192	172.16.157.129	A1

DNS Configuration

Primary DNS	172.16.5.102
Secondary DNS	
DNS Location	DMZ
DNS Client IP	172.16.5.71

Management IP(s)

IP	172.16.5.70
----	-------------

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

6.2 Global Profiles

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

6.2.1 Server Interworking profile - Avaya-IPO

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

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

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

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

For the newly created **Avaya-IPO** profile, click **Edit** at the bottom of the General tab.

- Check **T.38 Support**
- Click **Next**.
- Click **Finish** on the **Privacy** tab.
- Leave other fields with their default values.

The following screen capture shows the newly added **Avaya-IPO** Profile.

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

The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Global Parameters', 'Global Profiles', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Global Profiles' section is expanded, showing various profiles, with 'Avaya-IPO' highlighted in red.

The main content area is titled 'Interworking Profiles: Avaya-IPO'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a table of interworking profiles. The 'Avaya-IPO' profile is selected, and its configuration is shown in a tabbed interface with 'General' selected. The configuration includes a 'General' section with various settings and a 'Privacy' section.

Profile Name	Hold Support	180 Handling	181 Handling	182 Handling	183 Handling	Refer Handling	3xx Handling	Diversion Header Support	Delayed SDP Handling	T.38 Support	URI Scheme	Via Header Format	Privacy Enabled	User Name
cs2100	NONE													
avaya-ru		None	None	None	None	No	No	No	No	Yes	SIP	RFC3261	No	
OCS-Edge-Server														
cisco-ccm														
cups														
Sipera-Halo														
OCS-FrontEnd-Server														
Avaya-SM														
SP-General														
Avaya-CS1000														
Avaya-IPO														
Test														

6.2.2 Server Interworking profile – SP General

A second Server Interworking profile named **SP General** was created for the Service Provider, note that the **Add** button was used to add this profile.

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

Enter the new profile name, the name of **SP General** was chosen in this example. Accept the default values for all fields by clicking **Next** and then Click **Finish**.

For the newly created **SP General** profile, click **Edit** at the bottom of the General tab.

- Check **T.38 Support**
- Click **Next**.
- Click **Finish** on the **Privacy** tab.
- Leave other fields with their default values

The following screen capture shows the newly added **SP General** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. The left navigation pane lists various configuration areas, with "Server Interworking" highlighted under "Global Profiles". The main content area shows the configuration for the "SP-General" profile, which is selected in the "Interworking Profiles" list. The profile configuration is displayed in a table with tabs for General, Timers, URI Manipulation, Header Manipulation, and Advanced. The "General" tab is active, showing the following settings:

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

Below the General tab, the "Privacy" tab is visible, showing the following settings:

Privacy	
Privacy Enabled	No
User Name	

6.2.3 Routing Profiles

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

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

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

- Select the **Routing** tab.
- Select **Add**.
- Enter Profile Name: **Route_to_IPO**.
- Click **Next**.

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.60** (IP Office IP address).
- Check **Routing Priority Based on Next Hop Server**.
- Check **Outgoing Transport: UDP**.
- Click **Finish**.

The following screen shows the newly added **Route_to_IPO** Profile.

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

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

Similarly, for the outbound route:

- Select **Add**.
- Enter Profile Name: **Route to SP**.
- Click **Next**.
- **Next Hop Server 1: 10.10.2.12** (IP address for Service Provider's SIP Proxy)
- Check **Routing Priority Based on Next Hop Server**.
- Check **Outgoing Transport: UDP**.
- Click **Finish**.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Global Profiles', 'Routing', and 'SIP Cluster'. The 'Routing' section is expanded, showing a list of routing profiles: 'default', 'Route_to_SM', 'Route_to_SP', 'Route_to_CM', 'Route_to_CS1000', and 'Route_to_IPO'. The 'Route_to_SP' profile is selected and highlighted in red. The main content area shows the configuration for 'Routing Profiles: Route_to_SP'. It includes an 'Add' button, a 'Rename' button, a 'Clone' button, and a 'Delete' button. Below these is a table with the following data:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	10.10.2.12	...	View Edit

6.2.4 Server Configuration

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

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

On the **Add Server Configuration Profile** Tab:

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

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

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

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

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. A left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Server Configuration' section is active, showing a list of profiles: 'Session Manager', 'Service Provider', 'Com Manager', 'CS1000', and 'IP Office'. An 'Add' button is visible above the list. The 'Advanced' tab is selected, displaying configuration options: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (set to 'Avaya-IPO'), 'Signaling Manipulation Script' (set to 'None'), 'TCP Connection Type' (set to 'SUBID'), and 'UDP Connection Type' (set to 'SUBID'). 'Rename', 'Clone', and 'Delete' buttons are at the top right, and an 'Edit' button is at the bottom right of the configuration area.

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

On the **Add Server Configuration Profile** Tab:

- Select Server Type: **Trunk Server**.
- **IP Address: 10.10.2.12** (IP address for Service Provider's SIP Proxy).
- **Supported Transports: Check UDP**.
- **UDP Port: 5060**.
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **SP General** from the **Interworking Profile** drop down menu. Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

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

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

Property	Value
Server Type	Trunk Server
IP Addresses / FQDNs	10.10.2.12
Supported Transports	UDP
UDP Port	5060

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface, showing the 'Advanced' tab of the 'Service Provider' configuration. The top navigation bar and header are identical to the previous screenshot. The left-hand navigation menu remains the same. The main content area is titled 'Server Configuration: Service Provider' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced', with 'Advanced' selected. The configuration table shows the following details:

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

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

6.2.5 Topology Hiding

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

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

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

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

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' expanded to show 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: IP Office' and features an 'Add' button. Below this, a list of profiles is shown, with 'IP Office' highlighted. A table titled 'Topology Hiding' displays the configuration for this profile, showing headers, criteria, replace actions, and overwrite values.

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

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

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

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

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

The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. Under 'Global Profiles', 'Topology Hiding' is selected.

The main content area is titled 'Topology Hiding Profiles: Service_Provider'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a blue bar with the text 'Click here to add a description.' and a sub-section for 'Topology Hiding' containing a table.

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

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

6.2.6 Signaling Manipulation

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

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

6.3 Domain Policies

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

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

6.3.1 Create Application Rules

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

To add a new Application Rule, from the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Select **default trunk** Rule.
- Select **Clone Rule** button.
- Enter the **Application Rule Name: 500 Sessions**
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **500** was used in the sample configuration.
- Click Finish.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise AVAYA

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

Application Rules: 500 Sessions

Add
Filter By Device...
Rename Clone Delete

[Click here to add a description.](#)

Application Rule

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

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

[Edit](#)

6.3.2 Media Rules

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

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise AVAYA

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

Media Rules: default-low-med

Add
Filter By Device...
Clone

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

Media NAT
Media Encryption
Media Anomaly
Media Silencing
Media QoS

Media NAT Learn Media IP dynamically

[Edit](#)

6.3.3 Signaling Rules

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

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

The left sidebar contains a navigation menu with categories: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies (Application Rules, Border Rules, Media Rules, Security Rules, **Signaling Rules**, Time of Day Rules, End Point Policy, Groups, Session Policies), TLS Management, and Device Specific Settings.

The main content area is titled "Signaling Rules: default" and includes an "Add" button, a "Filter By Device..." dropdown, and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, there are tabs for "General", "Requests", "Responses", "Request Headers", "Response Headers", and "Signaling QoS".

The "General" tab is active and shows the following configuration:

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks	<input checked="" type="checkbox"/>		
Action	Allow	Multipart Action	Allow
Exception List	Exception List		

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

6.3.4 End Point Policy Groups

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

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

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar contains a navigation menu with "Domain Policies" expanded to "End Point Policy Groups". The main content area is titled "Policy Groups: Enterprise" and features an "Add" button, a "Filter By Device..." dropdown, and "Rename" and "Delete" buttons. Below this is a list of policy groups, with "Enterprise" highlighted. A "Policy Group" modal window is open, displaying a table with the following data:

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	500 Sessions	default	default-low-med	default-low	default	default	Edit Clone

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

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The main content area displays the configuration for the 'Service Provider' policy group. A table lists the policy groups, and a detailed view shows the configuration for the 'Service Provider' group.

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	500 Sessions	default	default-low-med	default-low	default	default	Edit Clone

6.4 Device Specific Settings

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

6.4.1 Network Management

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Network Management' highlighted under 'Device Specific Settings'. The main content area is titled 'Network Management: Sipera' and contains two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.192), and 'B2 Netmask'. An 'Add' button is present. Below the netmask fields is a table with columns for 'IP Address', 'Public IP', 'Gateway', and 'Interface'. The table contains two rows of data:

IP Address	Public IP	Gateway	Interface	
172.16.5.71		172.16.5.254	A1	Delete
172.16.157.189		172.16.157.129	B1	Delete

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

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

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

Network Management: Sipera

Devices **Network Configuration** **Interface Configuration**

Name	Administrative Status	
A1	Enabled	Toggle
B1	Enabled	Toggle

6.4.2 Media Interface

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

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

- Select **Add**.
- **Name: Private**.
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **Port Range: 35000-40000**.
- Click **Finish**.
- Select **Add Media Interface**.
- **Name: Public**.
- Select **IP Address: 172.16.157.189** (Outside IP Address of the Avaya SBCE, toward Service Provider).
- **Port Range: 35000-40000**.
- Click **Finish**.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar contains a navigation menu with 'Device Specific Settings' expanded to show 'Media Interface' selected. The main content area is titled 'Media Interface: Sipera' and features a 'Media Interface' tab. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table with columns for Name, Media IP, and Port Range, listing 'Private' and 'Public' interfaces. An 'Add' button is located in the top right corner of the table area.

Name	Media IP	Port Range	Edit	Delete
Private	172.16.5.71	35000 - 40000	Edit	Delete
Public	172.16.157.189	35000 - 40000	Edit	Delete

6.4.3 Signaling Interface

To create the Signaling Interface toward Session Manager, from the **Device Specific** menu on the left hand side, select **Signaling Interface**.

- Select **Add Signaling Interface**:
- **Name: Private.**
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward IP Office).
- **UDP Port: 5060.**
- Click **Finish.**
- Select **Add Signaling Interface**:
- **Name: Public**
- Select **IP Address: 172.16.157.189** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish.**

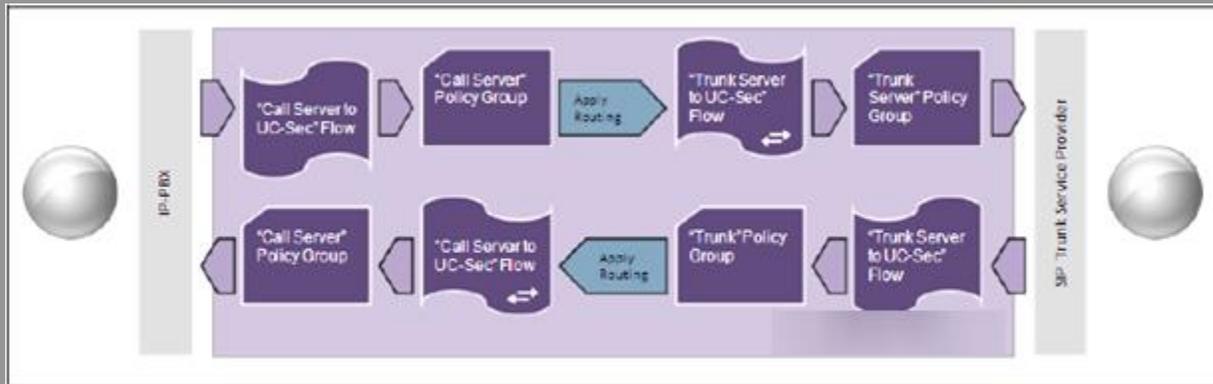
The following screen capture shows the newly added **Signaling Interfaces**.

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

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Private	172.16.5.71	---	5060	---	None	Edit	Delete
Public	172.16.157.189	---	5060	---	None	Edit	Delete

6.4.4 End Point Flows

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



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

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

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

View Flow: SIP_Trunk_Flow			
Criteria		Profile	
Flow Name	SIP_Trunk_Flow	Signaling Interface	Public
Server Configuration	Service Provider	Media Interface	Public
URI Group	*	End Point Policy Group	Service Provider
Transport	*	Routing Profile	Route_to_IPO
Remote Subnet	*	Topology Hiding Profile	Service_Provider
Received Interface	Private	File Transfer Profile	None

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

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

View Flow: IP Office Flow			
Criteria		Profile	
Flow Name	IP Office Flow	Signaling Interface	Private
Server Configuration	IP Office	Media Interface	Private
URI Group	*	End Point Policy Group	Enterprise
Transport	*	Routing Profile	Route_to_SP
Remote Subnet	*	Topology Hiding Profile	IP Office
Received Interface	Public	File Transfer Profile	None

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', and 'Device Specific Settings'. The 'End Point Flows' section is highlighted in red. The main content area is titled 'End Point Flows: Sipera' and features two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, showing a table with two configurations: 'IP Office' and 'Service Provider'. Each configuration has a table with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The 'IP Office' flow has a priority of 1, flow name 'IP Office Flow', URI Group '*', Received Interface 'Public', Signaling Interface 'Private', End Point Policy Group 'Enterprise', and Routing Profile 'Route_to_SP'. The 'Service Provider' flow has a priority of 1, flow name 'SIP_Trunk_Flow', URI Group '*', Received Interface 'Private', Signaling Interface 'Public', End Point Policy Group 'Service Provider', and Routing Profile 'Route_to_IPO'. Each row includes 'View', 'Clone', 'Edit', and 'Delete' links. An 'Add' button is located at the top right of the table area.

End Point Flows: Sipera

Devices | Subscriber Flows | **Server Flows** | Add

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	Private	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	Public	Service Provider	Route_to_IPO	View Clone Edit Delete

7. MTS Allstream SIP Trunking Configuration

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

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

8. Verification and Troubleshooting

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

8.1 Verification Steps

The following steps may be used to verify the configuration:

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

8.2 Protocol Traces

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

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

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

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

8.3 IP Office System Status

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

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

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

System
 Alarms (7)
 Extensions (24)
 Trunks (3)
 Line: 1
 Line: 2
 Line: 17
 Active Calls
 Resources
 Voicemail
 IP Networking
 Locations

Status Utilization Summary Alarms

SIP Trunk Summary

Peer Domain Name: sip://172.16.5.71
 Resolved Address: 172.16.5.71
 Line Number: 17
 Number of Administered Channels: 10
 Number of Channels in Use: 0
 Administered Compression: G729 A, G711 Mu
 Silence Suppression: Off
 Layer 4 Protocol: UDP
 SIP Trunk Channel Licenses: Unlimited 0%
 SIP Trunk Channel Licenses in Use: 0
 SIP Device Features: UPDATE (Incoming and Outgoing)

Channel Number	URI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Los...	Transmit Jitter	Transmit Packet Los...
1			Idle	5 days 17...											
2			Idle	36 days 16...											
3			Idle	36 days 16...											
4			Idle	36 days 16...											
5			Idle	36 days 16...											
6			Idle	36 days 16...											
7			Idle	36 days 16...											
8			Idle	36 days 16...											
9			Idle	36 days 16...											
10			Idle	36 days 16...											

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

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

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

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

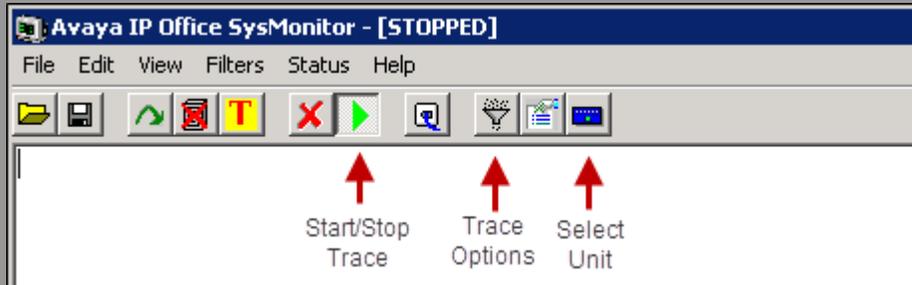
Alarms for Line: 17 SIP sip://172.16.5.92

Alarms

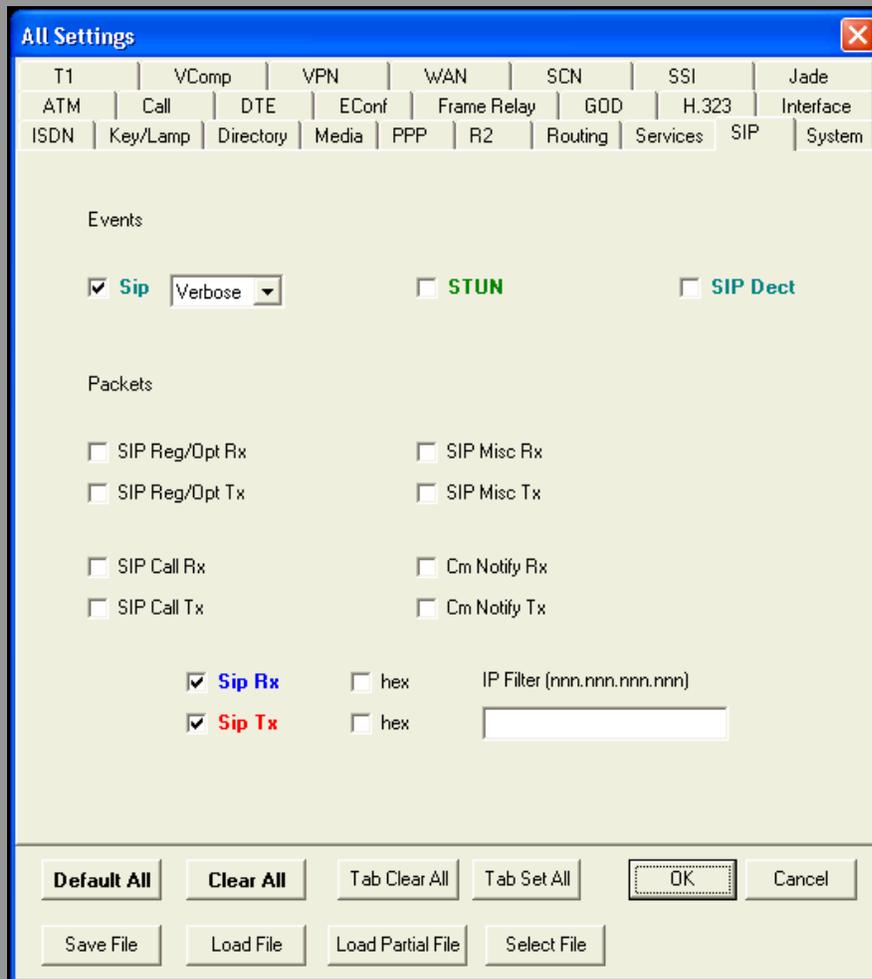
Last Date Of Error	Occurrences	Error Description
--------------------	-------------	-------------------

8.4 IP Office Monitor

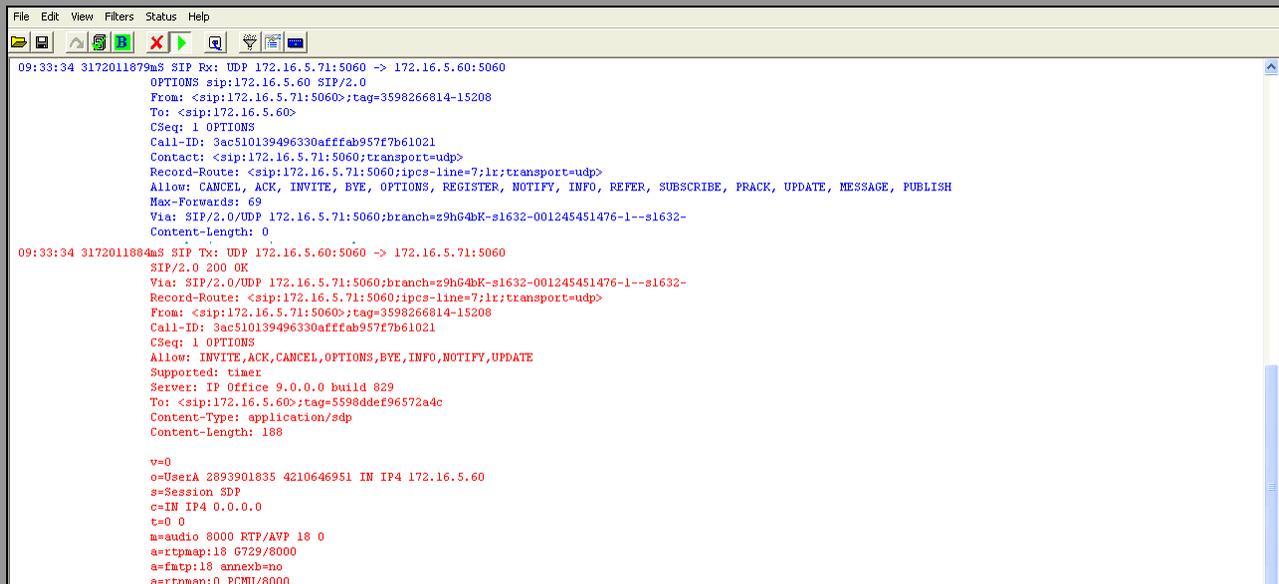
The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where Avaya IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select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



The sample screen below shows an outbound OPTIONS message and the 200 OK response received via the Avaya SBCE.



```
09:33:34 3172011879ms SIP Rx: UDP 172.16.5.71:5060 -> 172.16.5.60:5060
OPTIONS sip:172.16.5.60 SIP/2.0
From: <sip:172.16.5.71:5060>;tag=3598266814-15208
To: <sip:172.16.5.60>
CSeq: 1 OPTIONS
Call-ID: 3ac510139496330afffab957f7b61021
Contact: <sip:172.16.5.71:5060;transport=udp>
Record-Route: <sip:172.16.5.71:5060;ipcs-line=71r;transport=udp>
Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Max-Forwards: 69
Via: SIP/2.0/UDP 172.16.5.71:5060;branch=z9hG4bK-s1632-001245451476-1--s1632-
Content-Length: 0

09:33:34 3172011884ms SIP Tx: UDP 172.16.5.60:5060 -> 172.16.5.71:5060
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.5.71:5060;branch=z9hG4bK-s1632-001245451476-1--s1632-
Record-Route: <sip:172.16.5.71:5060;ipcs-line=71r;transport=udp>
From: <sip:172.16.5.71:5060>;tag=3598266814-15208
Call-ID: 3ac510139496330afffab957f7b61021
CSeq: 1 OPTIONS
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer
Server: IP Office 9.0.0.0 build 829
To: <sip:172.16.5.60>;tag=5598ddef96572a4c
Content-Type: application/sdp
Content-Length: 188

v=0
o=UserA 2893901835 4210646951 IN IP4 172.16.5.60
s=Session SDP
c=IN IP4 0.0.0.0
t=0 0
m=audio 8000 RTP/AVP 18 0
a=rtpmap:18 G729/8000
a=fmtp:18 annex=no
a=rtpmap:0 PCMU/8000
```

8.5 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.

Session Border Controller for Enterprise

Dashboard

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

Information

System Time	06:41:00 AM GMT	Refresh
Version	6.2.0.Q48	
Build Date	Wed May 22 22:52:47 UTC 2013	

Installed Devices

EMS
Sipera

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden
Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden
Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden

Add

Notes

No notes found.

The following screen shows the Alarm Viewer page.

Alarm Viewer

Devices

EMS
Sipera

Alarms

ID	Details	State	Time	Device
No alarms found for this device.				

Clear Selected Clear All

Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.

Session Border Controller for Enterprise AVAYA

Alarms **Incidents** Statistics Logs Diagnostics Users Settings Help Log Out

Dashboard

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

Information

System Time	06:41:00 AM GMT	Refresh
Version	6.2.0.Q48	
Build Date	Wed May 22 22:52:47 UTC 2013	

Installed Devices

EMS
Sipera

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden
Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden
Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden

[Add](#)

Notes

No notes found.

The following screen shows the Incident Viewer page.

Incident Viewer AVAYA

Device Category

Displaying results 1 to 15 out of 2000.

Type	ID	Date	Time	Category	Device	Cause
Routing Failure	694590900541135	1/8/14	11:50 AM	Policy	Sipera	Target is neither a server nor a subscriber, Sending 403 Forbidden
Routing Failure	694590750584190	1/8/14	11:45 AM	Policy	Sipera	Target is Click here for more details. subscriber, Sending 403 Forbidden
Routing Failure	694590690602014	1/8/14	11:43 AM	Policy	Sipera	Target is neither a server nor a subscriber, Sending 403 Forbidden

Diagnostics: This screen provides a variety of tools to test and troubleshoot the SBC network connectivity.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs **Diagnostics** Users Settings Help Log Out

Dashboard

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

Information

System Time	06:41:00 AM GMT	Refresh
Version	6.2.0.Q48	
Build Date	Wed May 22 22:52:47 UTC 2013	

Installed Devices

EMS
Sipera

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden
Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden
Sipera: Target is neither a server nor a subscriber, Sending 403 Forbidden

[Add](#)

Notes

No notes found.

The following screen shows the Diagnostics page.

Diagnostics AVAYA

https://172.16.5.70/sbc/list Certificate Error

Devices

Sipera

Full Diagnostic Ping Test Application Protocol

[Start Diagnostic](#)

Task Description	Status
EMS Link Check	
SBC Link Check: A1	
SBC Link Check: B1	
Ping: SBC (172.16.5.71) to Ping: Gateway (172.16.5.254)	
Ping: SBC (172.16.5.71) to Ping: Primary DNS (172.16.5.102)	
Ping: SBC (172.16.157.189) to Ping: Gateway (172.16.157.129)	
Ping: SBC (172.16.157.189) to Ping: Primary DNS (172.16.5.102)	

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**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top right corner features the AVAYA logo. The main header reads "Session Border Controller for Enterprise". On the left is a navigation menu with categories like Administration, System Management, and Troubleshooting. The "Trace" option under Troubleshooting is highlighted. The main content area is titled "Trace: Sipera" and contains three tabs: "Call Trace", "Packet Capture", and "Captures". The "Packet Capture" tab is active, showing a "Packet Capture Configuration" form. The form includes fields for Status (Ready), Interface (Any), Local Address (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (SIP_1.pcap). There are "Start Capture" and "Clear" buttons at the bottom of the form.

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address <small>[IP:Port]</small>	All : <input type="text"/>
Remote Address <small>*, *:Port, IP, IP:Port</small>	* <input type="text"/>
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	SIP_1.pcap

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.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Administration, System Management, and Troubleshooting. The main content area is titled "Trace: Sipera" and features three tabs: "Call Trace", "Packet Capture", and "Captures". The "Captures" tab is active, showing a table of captured files. The table has columns for "File Name", "File Size (bytes)", and "Last Modified", with a "Delete" link for each entry. Above the table are controls for sorting (Last Modified, Descending) and a Refresh button.

File Name	File Size (bytes)	Last Modified	
SIP_1_20131003115700.pcap	126,976	October 3, 2013 11:57:29 AM GMT	Delete
CL_1_20131002071526.pcap	659,456	October 2, 2013 7:16:01 AM GMT	Delete

9. Conclusion

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

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

10. References

- [1] *IP Office 9.0 Installing IP500/IP500 V2*, Document Number 15-601042.
<https://downloads.avaya.com/css/P8/documents/100174004>
- [2] *IP Office Manager Release 9.0*, Document Number 15-601011.
<https://downloads.avaya.com/css/P8/documents/100174478>
- [3] *Administering Avaya Flare® Experience for iPad devices and Windows*.
<https://downloads.avaya.com/css/P8/documents/100175132>
- [4] *IP Office System Status Application*, Document Number 15-601758.
<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*.
<https://downloads.avaya.com/css/P8/documents/100168983>
- [7] *Administering Avaya Session Border Controller for Enterprise*.
<https://downloads.avaya.com/css/P8/documents/100168982>
- [8] *Avaya Session Border Controller for Enterprise Release Notes*.
<https://downloads.avaya.com/css/P8/documents/100170131>
- [9] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*.
<https://downloads.avaya.com/css/P8/documents/100177106>

Product documentation for Avaya products may be found at <http://support.avaya.com>.
Product documentation for the Alestra Enlace IP SIP Trunk Service is available from Alestra.
Documentation for Avaya products may be found at <http://support.avaya.com>.

Product documentation for MTS Allstream SIP Trunking Service is available from MTS Allstream.

©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.