



Application Notes for SIP Trunking Using AT&T IP Flexible Reach - Enhanced Features with IPv6 and Avaya IP Office Release 10.1 with Avaya Session Border Controller for Enterprise Release 7.2 – Issue 1.1

Abstract

These Application Notes describe the steps for configuring an Avaya IP Office R10.1 solution with the AT&T IP Flexible Reach - Enhanced Features service using IPv6 and AVPN or MIS/PNT transport connections. In the sample configuration, the Avaya IP Office solution consists of Avaya Session Border Controller for Enterprise Release 7.2, Avaya IP Office Server Edition Release 10.1, and Avaya SIP, H.323, digital, and analog endpoints.

These Application Notes complement previously published Application Notes by illustrating the configuration screens and Avaya testing of IP Office Release 10.1 and Avaya Session Border Controller for Enterprise Release 7.2 to support IPv6.

The AT&T IP Flexible Reach - Enhanced Features service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

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

AT&T 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.....	5
2.2.	Test Results	6
2.3.	Support	7
3.	Reference Configuration.....	7
3.1.	Call Flows	10
3.1.1.	Inbound	10
3.1.2.	Outbound.....	11
3.1.3.	Call Forward	12
3.1.4.	Coverage to Voicemail	13
4.	Equipment and Software Validated	14
5.	Avaya IP Office Primary Configuration	15
5.1.	Licensing	16
5.2.	TLS Management.....	17
5.3.	System Settings	17
5.3.1.	LAN Settings	17
5.3.2.	Voicemail Settings.....	20
5.3.3.	System Telephony Configuration.....	21
5.3.4.	System Codecs Configuration.....	22
5.3.5.	VoIP Security.....	22
5.4.	IP Route.....	23
5.5.	SIP Line.....	23
5.5.1.	Importing a SIP Line Template.....	24
5.5.2.	Creating a SIP Trunk from an XML Template.....	25
5.5.3.	SIP Line – SIP Line tab	26
5.5.4.	SIP Line – Transport tab.....	27
5.5.5.	SIP Line – SIP URI tab.....	28
5.5.6.	SIP Line – VoIP tab	29
5.5.7.	SIP Line – T38 Fax Tab.....	30
5.5.8.	SIP Line – SIP Advanced Tab	30
5.6.	IP Office Line.....	32
5.7.	Users, Extensions, and Hunt Groups.....	33
5.7.1.	H.323 User 6322	33
5.7.2.	Hunt Groups.....	35
5.8.	Short Codes	35
5.9.	Incoming Call Routes.....	37
5.10.	ARS	39
5.11.	Save Configuration.....	40
6.	Avaya IP Office Expansion Configuration.....	41
6.1.	Physical Hardware.....	41
6.2.	System Settings	42
6.2.1.	LAN Settings	42
6.3.	IP Route.....	43

6.4.	IP Office Line.....	43
6.5.	Short Codes	44
6.6.	ARS	45
6.7.	Save Configuration.....	45
7.	Configure Avaya Session Border Controller for Enterprise	46
7.1.	System Management – Status	47
7.2.	TLS Management.....	48
7.2.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	48
7.2.2.	Server Profiles.....	49
7.2.3.	Client Profiles	51
7.3.	Network Management	52
7.4.	Server Interworking Profile.....	53
7.4.1.	Server Interworking Profile – IP Office.....	53
7.4.2.	Server Interworking Profile – AT&T	54
7.5.	Signaling Manipulation	56
7.6.	Server Configuration	57
7.6.1.	Server Configuration – IP Office	57
7.6.2.	Server Configuration – AT&T.....	59
7.7.	Routing Profile	61
7.8.	Topology Hiding Profile	62
7.9.	Application Rule	63
7.10.	Media Rule	64
7.11.	Signaling Rule	66
7.12.	Endpoint Policy Groups.....	67
7.13.	Advanced Options	68
7.14.	Media Interface.....	69
7.15.	Signaling Interface.....	69
7.16.	End Point Flows - Server Flow.....	69
8.	AT&T IP Flexible Reach – Enhanced Features Configuration	71
9.	Verification Steps.....	71
9.1.	Avaya SBCE	71
9.1.1.	Incidents.....	71
9.1.2.	Server Status	72
9.1.3.	Tracing	72
9.2.	IP Office	74
9.2.1.	System Status	74
9.2.2.	Monitor	75
10.	Conclusion	77
11.	Additional References.....	77

1. Introduction

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) trunking between an Avaya IP Office solution (IPv4 address) and the AT&T IP Flexible Reach - Enhanced Features service (IPv6 address) using **AVPN** or **MIS/PNT** transport connections. In the sample configuration, the Avaya IP Office solution consists of an Avaya IP Office Server Edition Primary Server (Primary server), an IP500 V2 Expansion System, Voicemail Pro, Avaya one-X® Portal for IP Office, WebRTC gateway, Avaya Communicator for Windows, Avaya Communicator for Web, Avaya SIP, H.323, digital, and analog endpoints.

Avaya IP Office is a versatile communications solution that combines the reliability and ease of a traditional telephony system with the applications and advantages of an IP telephony solution. This converged communications solution can help businesses reduce costs, increase productivity, and improve customer service.

The Avaya Session Border Controller for Enterprise (Avaya SBCE) is the point of connection between Avaya IP Office and the AT&T IP Flexible Reach - Enhanced Features service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling and media for interoperability between IPv4 and IPv6.

The AT&T IP Flexible Reach - Enhanced Features service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach - Enhanced Features service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites. The AT&T IP Flexible Reach - Enhanced Features service utilizes AVPN¹ or MIS/PNT² transport service.

<p>Note – The AT&T IP Flexible Reach - Enhanced Features service will be referred to as IPFR-EF in the remainder of this document.</p>

2. General Test Approach and Test Results

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.

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPFR-EF and the Customer Premises Equipment (CPE) containing the Avaya SBCE, and Avaya IP Office (see **Section 3.2** for call flow examples).

¹ AVPN uses compressed RTP (cRTP).

².MIS/PNT does not support cRTP.

The test environment described in these Application Notes consisted of:

- A simulated enterprise with the Avaya SBCE, Avaya IP Office, Avaya SIP, H.323, digital and analog endpoints, as well as a fax machine emulator (Ventafax).
- An IPFR-EF production circuit, to which the simulated enterprise was connected via AVPN transport.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the AT&T Flexible Reach service did not include use of any specific encryption features as requested by AT&T.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible.

2.1. Interoperability Compliance Testing

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPFR-EF network. Calls were made to/from the PSTN across the IPFR-EF network, to/from the CPE.

The following SIP trunking VoIP features were tested with the IPFR-EF service:

- Incoming and outgoing voice calls between PSTN, the IPFR-EF service, the Avaya SBCE, and Avaya IP Office, utilizing Avaya SIP, H.323, digital, and analog endpoints.
- Inbound/Outbound fax calls using T.38 or G.711.
- Various outbound PSTN destinations were tested including, local, long distance, international, and toll-free.
- Requests for privacy (i.e., caller anonymity) for Avaya IP Office outbound calls to the PSTN, as well as privacy requests for inbound calls from the PSTN to Avaya IP Office users.
- SIP OPTIONS messages used to monitor the health of the SIP trunk from both Avaya IP Office and AT&T.
- Incoming and outgoing calls using the G.729(A & B) and G.711 ULAW codecs.
- Call redirection with Diversion Header.
- 411 and 911 calls.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful PSTN and Avaya IP Office menu navigation.

- Telephony features such as hold, transfer, and conference.
- Avaya IP Office Mobile twinning to a mobile phone when the associated Avaya IP Office extension is called, as well as Mobility features such as Mobile Callback and Mobile Call Control.
- Avaya Remote Worker configuration (Avaya Communicator SIP softphone) via Avaya SBCE.
- AT&T IPFR-EF service features such as:
 - Simultaneous Ring
 - Sequential Ring
 - Call Forward – Always
 - Call Forward – Busy
 - Call Forward – Ring No Answer
- “Blind” and Attended transfers utilizing SIP Refer messaging.

2.2. Test Results

The test objectives stated in **Section 2.1**, with limitations as noted below, were verified.

1. **Avaya IP Office only supports a packet size (ptime) of 20 msecs, and therefore does not specify a ptime value in the SIP SDP (in either requests or responses) –**
 - Although no issues were found during testing, AT&T recommends that for maximum customer bandwidth utilization, a ptime value of 30 should be specified.
2. **AT&T IPFR-EF Sequential Ringing** – When the IP Office extension number associated with the primary IPFR-EF Sequential Ringing number was answered by Voicemail Pro, no mailbox greeting was heard. It was determined the cause of this anomaly was caused by the initial INVITE from AT&T included the media attribute “sendonly” and once the call was answered a re-INVITE was sent with “sendrecv”. IP Office was unable to process this type of exchange correctly when the call was answered by Voicemail Pro.
 - This is currently being investigated by IP Office development team.
 - The recommended workaround is described in **Section 7.5**, where Avaya SBCE will convert the media attribute from “sendonly” to “sendrecv”.
3. **Video enabled endpoints and outbound SIP trunk calls** – Although AT&T does not support video calls, it is necessary to enable video in the Application Rule on Avaya SBCE to have the video connection line (c-line) properly changed to an IPv6 address toward AT&T (See **Section 7.9**).
4. **Alphanumeric characters in IPv6 address** – The Avaya SBCE Server Configuration IP address field is case sensitive. The AT&T IPv6 address needs to be entered using lowercase characters. The Avaya SBCE will not match the source address of incoming SIP packets from AT&T if the IPv6 address is entered using uppercase characters (See **Section 7.6.2**).

5. **DiffServ markings** – For IP Office Server Edition, the IP header in SIP signaling packets sent from the IP Office server do not contain the DSCP values configured in IP Office Manager for Quality of Service policies (See **Section 5.3.1**). The IP headers in RTP media packets have the correct values. Also, this only affects Server Edition systems; the IP headers in SIP signaling packets from IP 500V2 systems have the correct values.
6. **Emergency 911/E911 Services Limitations and Restrictions** – Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) documented in these Application Notes will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer’s responsibility to ensure proper operation with the equipment/software vendor.
While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at <http://new.serviceguide.att.com>. Such circumstances include, but are not limited to, relocation of the end user’s CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer’s location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

2.3. Support

For more information on the AT&T IP Flexible Reach service visit:

<http://www.business.att.com/enterprise/Service/voice-services/null/sip-trunking/>

AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

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

3. Reference Configuration

Note – Documents used to provision the test environment are listed in **Section 11**. References to these documents are indicated by the notation [x], where x is the document reference number.

The reference configuration used in these Application Notes is shown in **Figure 1** below and consists of the following components:

- Avaya IP Office provides the voice communications services for a particular enterprise site. In the reference configuration, Avaya IP Office runs on the Avaya IP Office Server Edition platform. This solution is extensible to the IP 500 V2 platform as well.
- Avaya endpoints are represented with an Avaya 9608 H.323 Deskphone, an Avaya 9508 Digital Telephone, an Avaya 6211 Analog Telephone, an Avaya 1140E SIP Deskphone, as well as Avaya Communicator for Windows, and Avaya Communicator for Web. Fax

endpoints are represented by PCs running Ventafax emulation software connected by modem to an Expansion System analog port.

- Voicemail Pro (running on the Primary server) provided the voice messaging capabilities in the reference configuration. This solution is extensible to the Avaya IP Office embedded voice mail as well.
- In the reference configuration, Primary server interface “LAN 1” is connected to the private CPE network (the “LAN 2” interface is not used).
- Avaya Session Border Controller for Enterprise running on VMware platform. This solution is extensible to other Avaya Session Border Controller for Enterprise platforms as well.
- TLS/5061 is the recommended transport protocol/port to use on the Avaya IP Office LAN1 connection to the Avaya SBCE A1 interface. However, TCP/5060 may be used for this connection if desired.
- The AT&T IPFR-EF service requires the following SIP trunk network settings between the Avaya SBCE and the IPFR-EF Border Element:
 - UDP transport using port 5060
 - RTP port ranges 16384-32767
- AT&T provided the inbound and outbound access numbers (DID and DNIS) used in the reference configuration. Note that the IPFR-EF service may deliver 10 or 7 digits in the SIP Invite R-URI depending on the circuit order provisioning. In the reference configuration, the IPFR-EF service delivered 10 digits.
- The Primary server and the Avaya SBCE used in the reference configuration were deployed using the following configuration.
 - Primary server LAN1 interface connected to the CPE private network.
 - Avaya SBCE A1 interface connected to the CPE private network.
 - Avaya SBCE B2 interface connected to the AT&T IPFR-EF network router.
- An Avaya Remote Worker endpoint (Avaya Communicator for Windows) was used in the reference configuration. The Remote Worker endpoint resides on the public side of an Avaya SBCE (via a TLS connection), and registers/communicates with Avaya IP Office as though it was an endpoint residing in the private CPE space.

<p>Note – The configuration of the Remote Worker environment is beyond the scope of this document. Refer to [5] for information on Remote Worker deployments.</p>
--

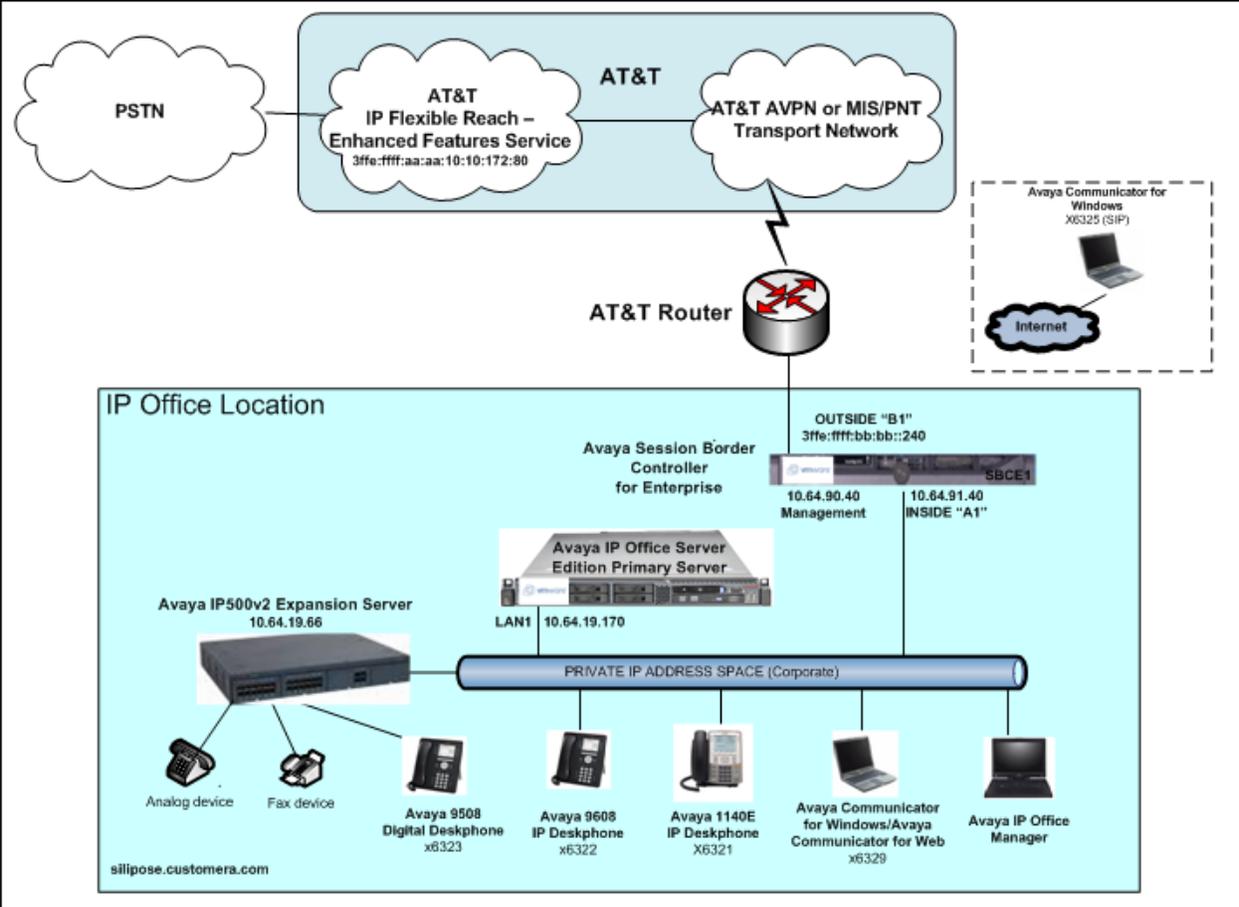


Figure 1: Avaya Interoperability Test Lab Configuration

3.1. Call Flows

To understand how inbound and outbound AT&T IPFR-EF service calls are handled by Avaya IP Office, four basic call flows are described in this section.

3.1.1. Inbound

The first call scenario illustrated in the figure below is an inbound AT&T IPFR-EF service call that arrives on Avaya IP Office, which in turn routes the call to a hunt group, phone or a fax endpoint.

1. A PSTN phone originates a call to an IPFR-EF service number.
2. The PSTN routes the call to the AT&T IPFR-EF service network.
3. The AT&T IPFR-EF service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any specified SIP header modifications, and routes the call to Avaya IP Office.
5. Avaya IP Office applies any necessary digit manipulations based upon the DID and routes the call to a hunt group, phone or a fax endpoint.

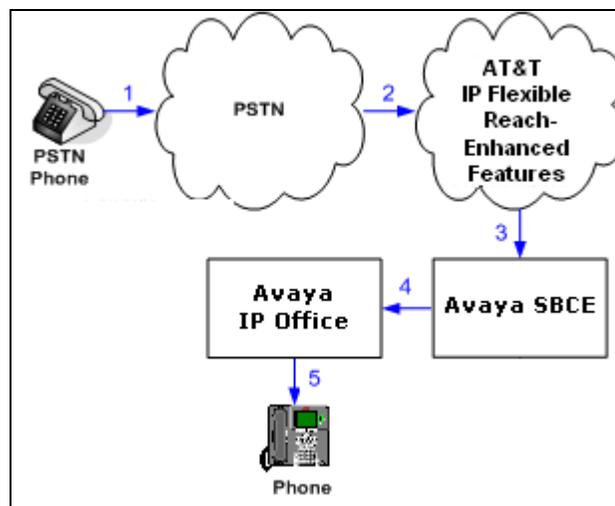


Figure 2: Inbound AT&T IPFR-EF Call

3.1.2. Outbound

The second call scenario illustrated in the figure below is an outbound call initiated on Avaya IP Office for delivery to AT&T IPFR-EF service.

1. An Avaya IP Office phone or fax endpoint originates a call to an AT&T IPFR-EF service number for delivery to PSTN.
2. Avaya IP Office applies any necessary origination treatment (verifying permissions, determining the proper route, selecting the outgoing trunk, etc.) and sends the call to the Avaya SBCE.
3. The Avaya SBCE performs SIP Network Address Translation (NAT) and any specified SIP header modifications, and routes the call to the AT&T IPFR-EF service.
4. The AT&T IPFR-EF service delivers the call to PSTN.
5. PSTN delivers the call to a phone or fax endpoint.

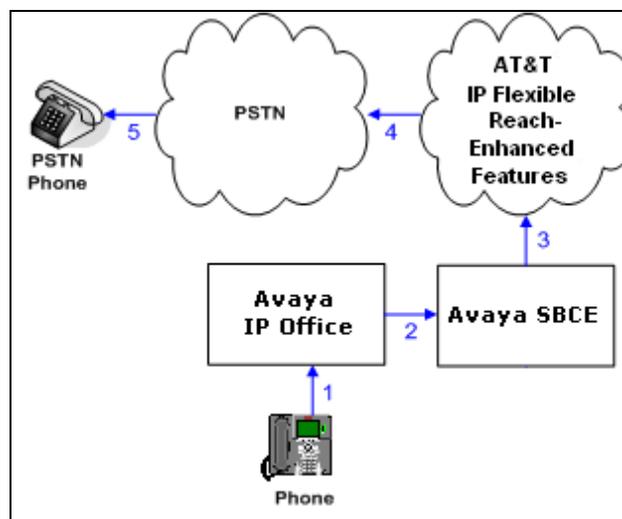


Figure 3: Outbound Call to AT&T IPFR-EF

3.1.3. Call Forward

The third call scenario illustrated in the figure below is an inbound AT&T IPFR-EF service call destined for an Avaya IP Office station that has set Call Forwarding to an alternate destination. Without answering the call, Avaya IP Office redirects the call back to the AT&T IPFR-EF service for routing to the alternate destination.

Note – AT&T requires the Diversion header be used when a call is redirected to AT&T IPFR-EF service (See **Section 5.5.5**).

1. Same as the first call scenario in **Section 3.2.1**.
2. Because the Avaya IP Office phone has set Call Forward to another AT&T IPFR-EF service number, Avaya IP Office initiates a new call back out to the AT&T IPFR-EF service network. This new SIP INVITE will contain a Diversion Header.
3. The AT&T IPFR-EF service places a call to the alternate destination and upon answer, Avaya IP Office connects the calling party (PSTN Phone) to the target party (Target Phone).

Note – The IPFR-EF service offers similar Call Forwarding features that allow users to predefine alternate call destinations based on Ring-No-Answer, Busy, Not Reachable, or Unconditional criteria.

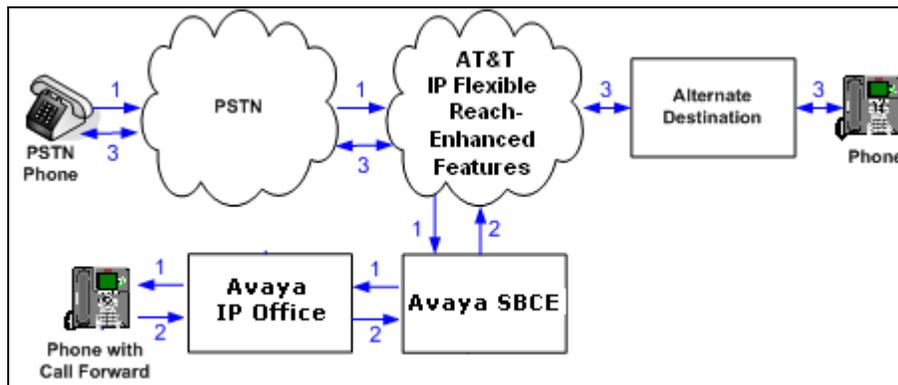


Figure 4: Call Forward

3.1.4. Coverage to Voicemail

The call scenario illustrated in the figure below is an inbound call that is covered to Voicemail. In the reference configuration, the Voicemail system used is Voicemail Pro.

1. Same as the first call scenario in **Section 3.2.1**.
2. The Avaya IP Office phone does not answer the call, and the call covers to Voicemail Pro.

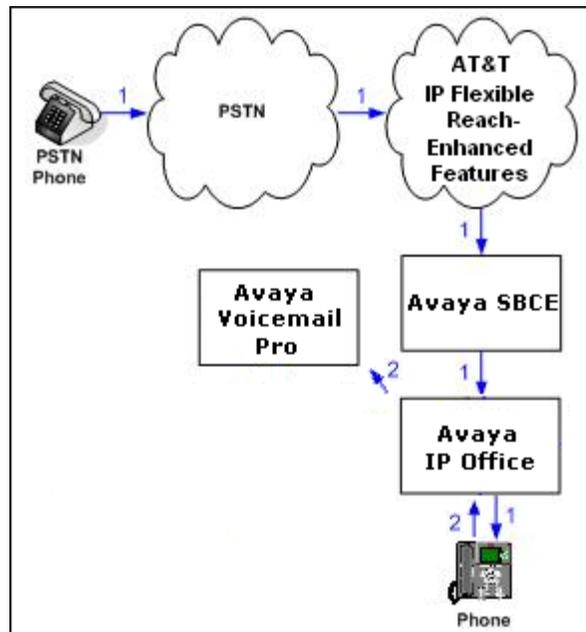


Figure 5: Coverage to Avaya IP Office Voicemail

4. Equipment and Software Validated

Table 2 shows the equipment and software used in the sample configuration.

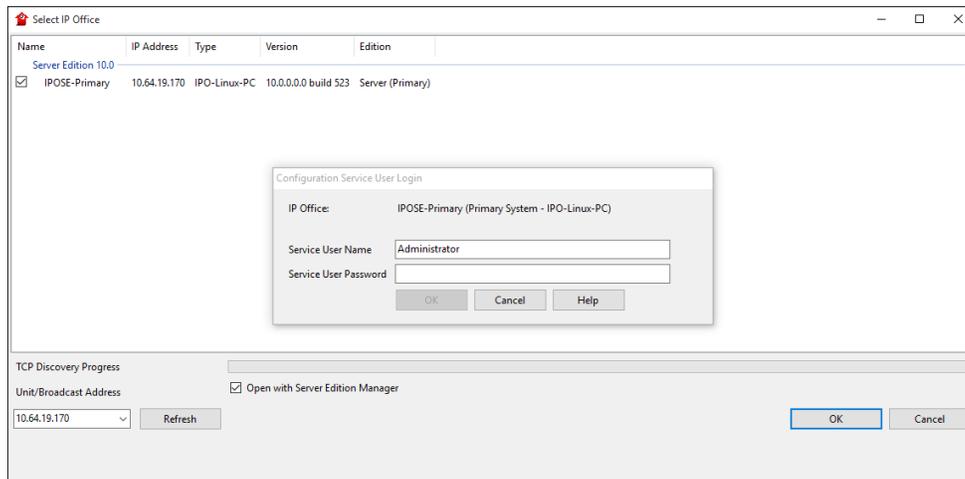
Avaya IP Telephony Solution Components	
Equipment	Software
Avaya Session Border Controller for Enterprise	Release 7.2.0.0-18-13712
Avaya IP Office Server Edition (Primary Server) <ul style="list-style-type: none"> ▪ IP Office ▪ Voicemail Pro ▪ Avaya WebRTC Gateway ▪ Avaya one-X® Portal for IP Office 	Release 10.1.0.0 build 237 Release 10.1.0.0 build 241 Release 10.1.0.0 build 13 Release 10.1.0.0 build 305
Avaya IP Office IP500 V2 (Expansion System) <ul style="list-style-type: none"> ▪ Avaya IP Office TCM 8 ▪ Avaya IP Office COMBO6210/ATM4 	Release 10.1.0.0 Build 237 Release 10.1.0.0 Build 237
Avaya IP Office Manager	Release 10.1.0.0 Build 237
Avaya 9611SW IP Deskphone (H.323)	Release 6.6401
Avaya 1140E IP Deskphone (SIP)	Release 04.04.23
Avaya 9508 Digital Telephone	Release 0.60
Avaya Communicator for Windows	Release 2.1.4.245
Avaya Communicator for Web	Release 1.0.17.1620
Analog Fax device	Ventafax 7.9

Table 1: Equipment and Software Tested

Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2, and also when deployed with all configurations of IP Office Server Edition. Note that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks.

5. Avaya IP Office Primary Configuration

IP Office is configured via the IP Office Manager program. For more information on IP Office Manager, consult reference [2]. From the IP Office Manager PC, select **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application. Navigate to **File** → **Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials.



On Server Edition systems, the Solution View screen will appear, similar to the one shown below. If the left navigation pane does not immediately appear, click on the **Configuration** link as highlighted below. In the reference configuration, IP users are registered to the Primary server and failover to the Secondary server. Digital and Analog users are configured on the Expansion System. A SIP trunk to the Avaya SBCE is configured on the Primary server. Clicking the “plus” sign next to the Primary server system name, e.g., **IPOSE-Primary**, on the left navigation pane will expand the menu on this server.



5.1. Licensing

In the sample configuration, **IPOSE-Primary** was used as the system name of the Primary Server and **IP500 Expansion** was used as the system name of the Expansion System. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane.

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

To verify that there is a SIP Trunk Channels License with sufficient capacity, click **License** in the Navigation pane. Confirm a valid **SIP Trunk Channels** license with sufficient **Instances** (trunk channels). If Avaya IP Telephones will be used as is the case in these Application Notes, verify the **Avaya IP endpoints** license.

License Type	Status
License	Remote Server
License Mode	WebLM Normal
Licensed Version	10.0

Feature	Instances	Status	Expiration Date	Source
Additional Voicemail Pro Ports	152	Valid	Never	WebLM
VMPro TTS Professional	1	Valid	Never	WebLM
Power User	6	Valid	Never	WebLM
Avaya IP endpoints	9	Valid	Never	WebLM
SIP Trunk Channels	50	Valid	Never	WebLM
CTI Link Pro	1	Valid	Never	WebLM
Server Edition R10	1	Valid	Never	WebLM
Web Collaboration	5	Valid	Never	WebLM
UMS Web Services	1	Valid	Never	WebLM
Basic User	5	Valid	Never	WebLM

License Type	Status
License	Remote Server

Remote Server Configuration

License Source: WebLM

Domain Name (URL): 10.64.19.170

Path: WebLM/LicenseServer

Port Number: 52233

WebLM client ID: 000C29140005-silipose

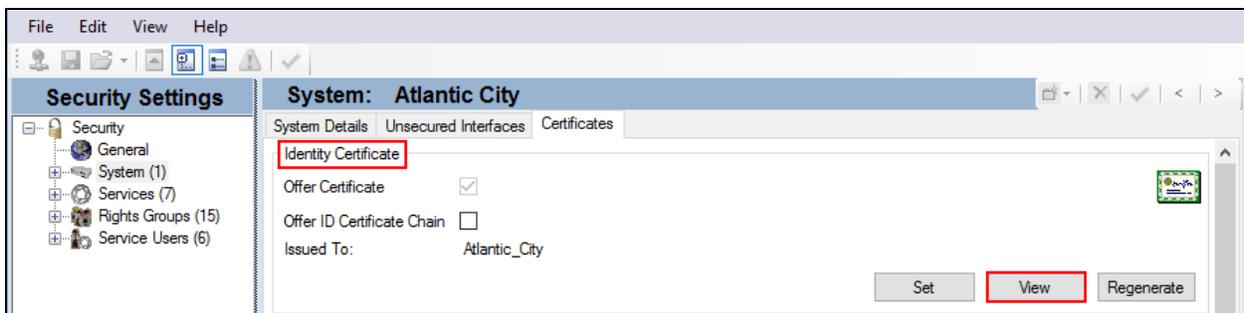
Reserved Licenses	Instances	Server Edition	Instances
SIP Trunk Sessions	50	Server Edition	1
SM Trunk Sessions	0	Avaya IP Endpoints	9
Voicemail Pro Ports	152	3rd Party IP Endpoints	0
VMPro Recordings Administrators	0	Receptionist	0
VMPro TTS Professional	1	Basic User	5
CTI Link Pro	1	Office Worker	0
UMS Web Services	1	Power User	6
Mac Softphones	0	Avaya Softphone	0
Avaya Contact Center Select	0	Web Collaboration	5
Third Party Recorder	0		

5.2. TLS Management

For the compliance test, the signaling on the SIP trunk between Avaya IP Office and the Avaya SBCE was secured using TLS. Testing was done using identity certificates signed by a local certificate authority **SystemManager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes. However, once the certificates are available they can be viewed on the Avaya IP Office in the following manner.

To view the certificates currently installed on Avaya IP Office, navigate to **File → Advanced → Security Settings**. In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

To verify the identity certificate, locate the **Identity Certificate** section and click **View** to see the details of the certificate.

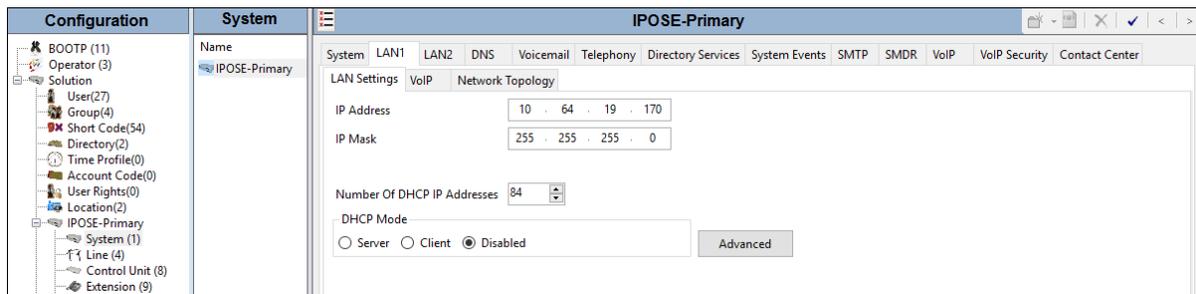


5.3. System Settings

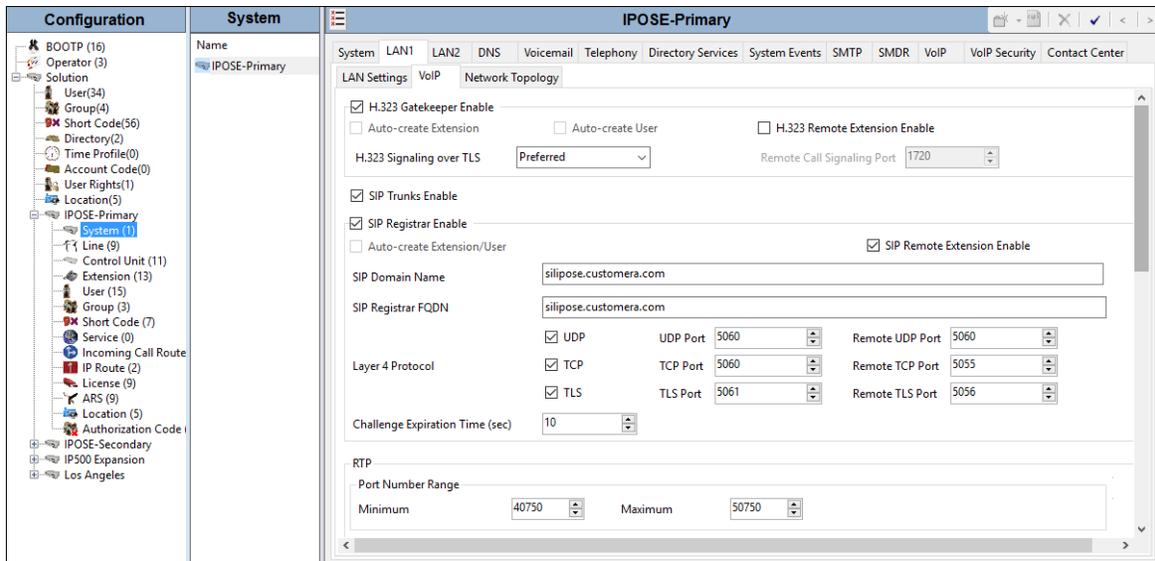
This section illustrates the configuration of system settings. Select **System** in the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings. For all of the following configuration sections, the **OK** button (not shown) must be selected in order for any changes to be saved.

5.3.1. LAN Settings

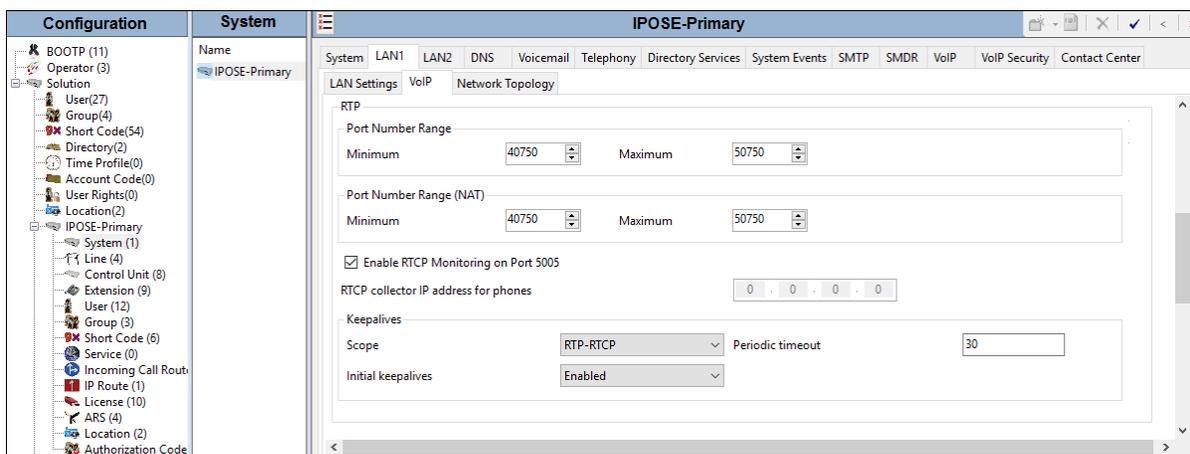
In the sample configuration, LAN1 is used to connect the Primary server to the enterprise network. To view or configure the **IP Address** of LAN1, select the **LAN1** tab followed by the **LAN Settings** tab. As shown in **Figure 1**, the IP Address of the Primary server is **10.64.19.170**. Other parameters on this screen may be set according to customer requirements.



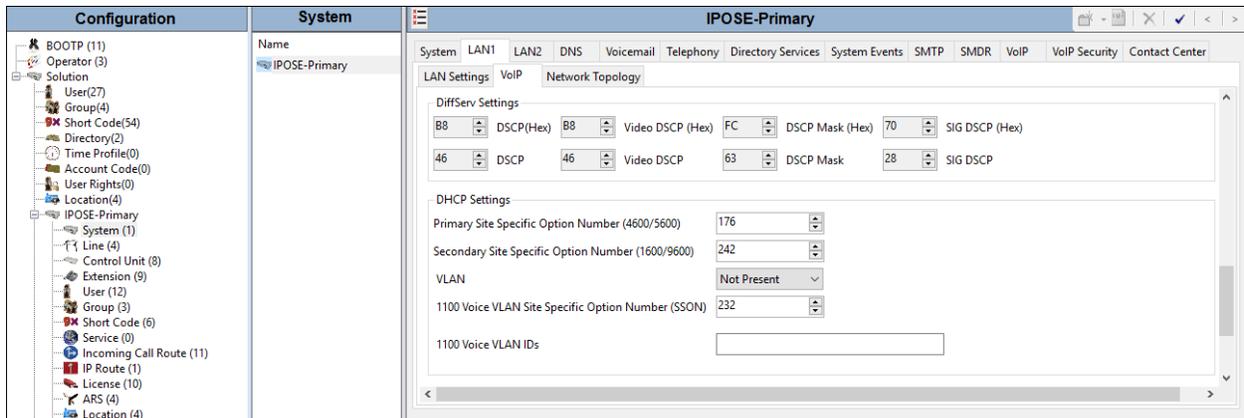
Select the **VoIP** tab as shown in the following screen. The **H323 Gatekeeper Enable** parameter is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 9808 used in the sample configuration. The **SIP Registrar Enable** parameter is checked to allow Avaya 1140E and Avaya Communicator usage. The **SIP Trunks Enable** parameter must be checked to enable the configuration of SIP trunks to AT&T. The **SIP Domain Name** and **SIP Registrar FQDN** may be set according to customer requirements. If desired, the **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media paths from Avaya SBCE to the Primary server. The defaults are used here.



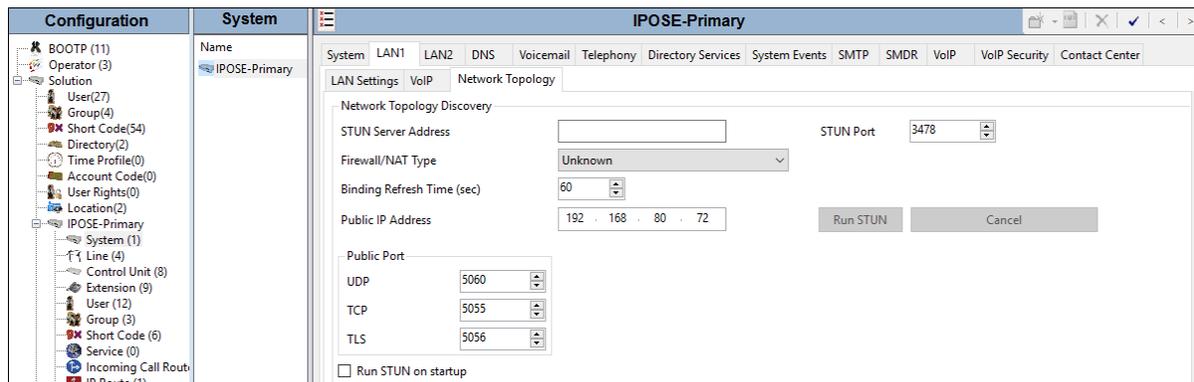
Scroll down to the **Keepalives** section, and set the **Scope** to **“RTP-RTCP”**. Set the **Periodic timeout** to **“30”** and the **Initial keepalives** parameter to **“Enabled”**. These settings will cause the Primary server to send RTP and RTCP keepalive packets starting at the time of initial connection and every 30 seconds thereafter if no other RTP or RTCP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting to see media from the other, as well as helping to keep ports open for the duration of the call.



Scrolling down, the Primary server can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies. In the sample configuration shown below, IP Office will mark SIP signaling with a value associated with “Assured Forwarding” using DSCP decimal 28 (**SIG DSCP** parameter). IP Office will mark the RTP media with a value associated with “Expedited Forwarding” using DSCP decimal 46 (**DSCP** parameter). See **Section 2.2** for limitations with IP Office Server Edition. This screen enables flexibility in IP Office DiffServ markings (RFC 2474) to allow alignment with network routing policies, which are outside the scope of these Application Notes. Other parameters on this screen may be set according to customer requirements.

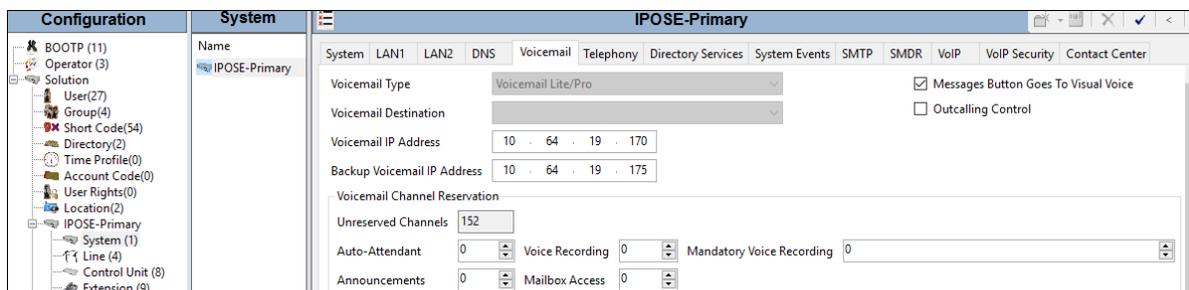


Select the **Network Topology** tab as shown in the following screen. The **Firewall/NAT Type** is set to “**Unknown**” in the sample configuration. The **Public IP Address** and **Public Port** section relates to remote workers, and is not used for the AT&T IPFR-EF SIP trunk service connection.



5.3.2. Voicemail Settings

To view or change voicemail settings, select the **Voicemail** tab as shown in the following screen. The settings presented here simply illustrate the sample configuration and are not intended to be prescriptive. The **Voicemail Type** in the sample configuration is “**Voicemail Lite/Pro**”. The **Voicemail IP Address** in the sample configuration is “**10.64.19.170**”, the IP address of the Primary server running the Voicemail Pro software. The **Backup Voicemail IP Address** is “**10.64.19.175**”, the IP address of the Secondary server.

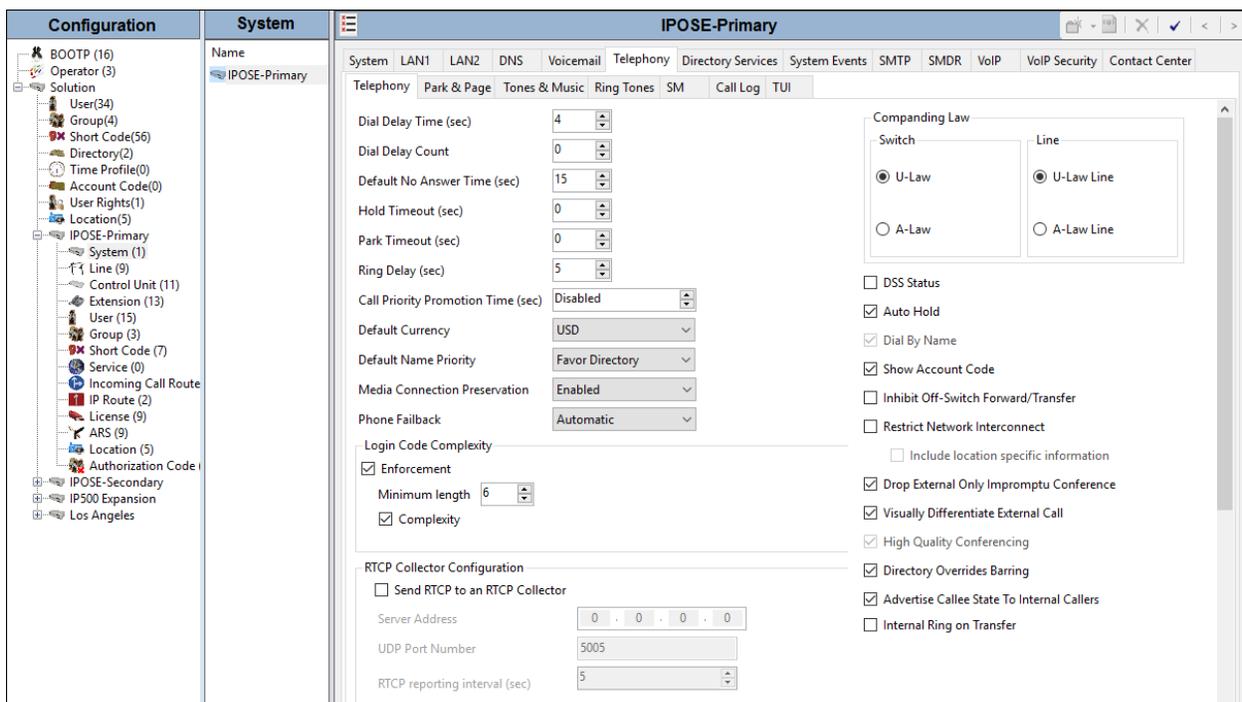


In the sample configuration, the “Callback” application of Avaya Voicemail Pro was used to allow Voicemail Pro to call out via the SIP Line to AT&T IPFR-EF when a message is left in a voice mailbox. The **SIP Settings** shown in the screen below enable the Primary server to populate the SIP headers for an outbound “callback” call from Voicemail Pro, similar to the way the fields with these same names apply to calls made from telephone users (e.g., see **Section 5.7**).



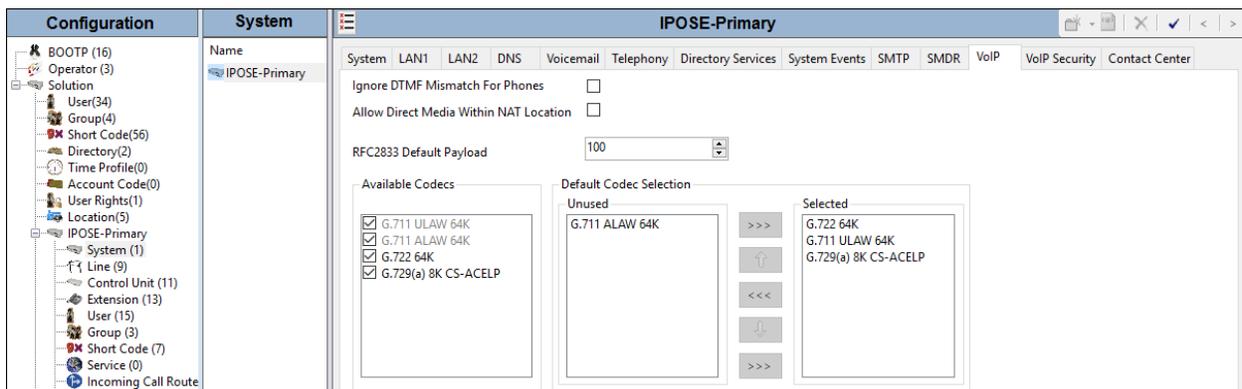
5.3.3. System Telephony Configuration

To view or change telephony settings, select the **Telephony** tab and **Telephony** sub-tab as shown in the following screen. The settings presented here simply illustrate the sample configuration and are not intended to be prescriptive. In the sample configuration, the **Inhibit Off-Switch Forward/Transfer parameter** is unchecked so that call forwarding and call transfer to PSTN destinations via the AT&T IPFR-EF service can be tested. That is, a call can arrive to IP Office via the AT&T IPFR-EF service and be forwarded or transferred back to the PSTN with the outbound leg of the call using the AT&T IPFR-EF service. The **Companding Law** parameters are set to “**U-Law**” as is typical in North American locales. In the reference configuration, **Default Name Priority** is set to **Favor Directory**. With the option set to **Favor Directory**, Avaya IP Office will prefer to display names found in a personal or system directory over those arriving from the far-end, if there is a directory match to the caller ID. This capability is also defined in the **SIP Line** tab in **Section 5.5.3**. Other parameters on this screen may be set according to customer requirements.



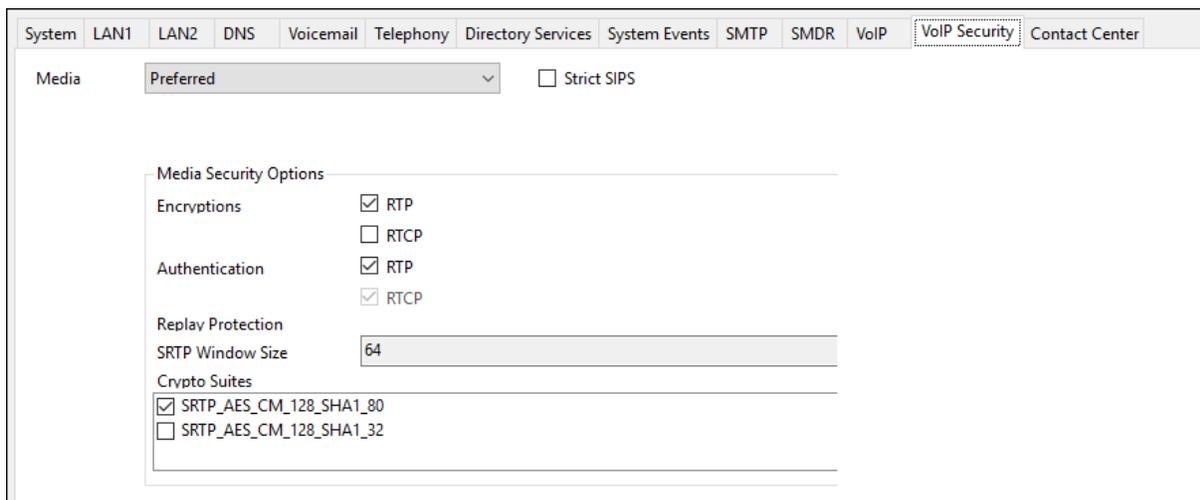
5.3.4. System Codecs Configuration

To view or change system codec settings, select the **VoIP** tab. On the left, observe the list of **Available Codecs**. In the example screen below, which is not intended to be prescriptive, the parameter next to each codec is checked, making all the codecs available in other screens where codec configuration may be performed (such as the SIP Line in **Section 5.5**). The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis, using the up, down, left, and right arrows. By default, all IP (SIP and H.323) lines and extensions will assume the system default codec selection, unless configured otherwise for the specific line or extension. The **RFC2833 Default Payload** parameter is set to “**100**”, the value preferred by AT&T.



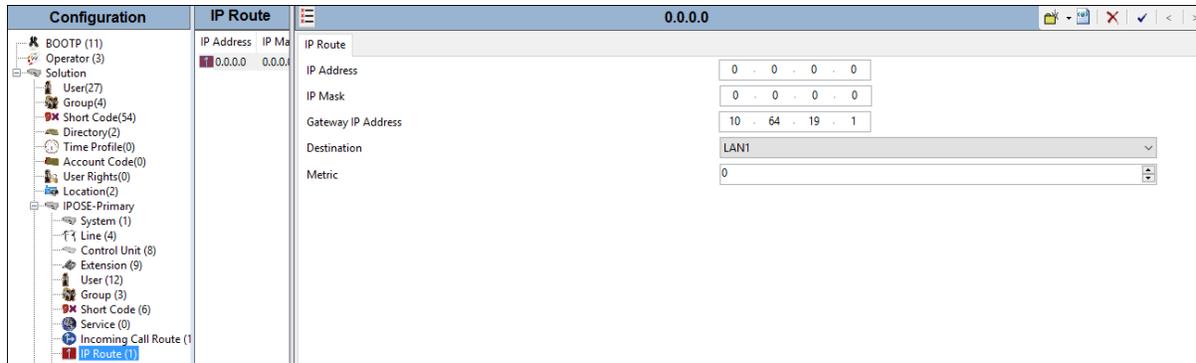
5.3.5. VoIP Security

For the compliance test, SRTP was used internal to the enterprise wherever possible. To view or configure the media encryption settings, select the **VoIP Security** tab. Set the **Media** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption. Under **Media Security Options**, select “**RTP**” for the **Encryptions** and **Authentication** fields. Under **Crypto Suites**, select “**SRTP_AES_CM_128_SHA1_80**”. Click **OK** to commit (not shown).



5.4. IP Route

In the sample configuration, the Primary server LAN1 port is physically connected to the local area network switch at the IP Office customer site. The default gateway for this network is 10.64.19.1. The Avaya SBCE resides on a different subnet and requires an IP route to allow SIP traffic between the two devices. To add an IP route in the Primary server, right-click **IP Route** from the Navigation pane, and select **New** (not shown). To view or edit an existing route, select **IP Route** from the Navigation pane, and select the appropriate route from the Group pane. The following screen shows the Details pane with the relevant route using **Destination** “LAN1”.



5.5. SIP Line

The following sections describe the configuration of a SIP Line. The SIP Line terminates the CPE end of the SIP trunk to the AT&T IPFR-EF service.

The recommended method for creating/configuring a SIP Line is to use the template associated with the provisioning described in these Application Notes. The template is an .xml file that can be used by Avaya IP Office Manager to create a new SIP Line for SIP trunking with the AT&T IPFR-EF service. Follow the steps in **Section 5.5.2** to create a SIP Trunk 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 as shown in **Sections 5.5.3 – 5.5.8**.

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

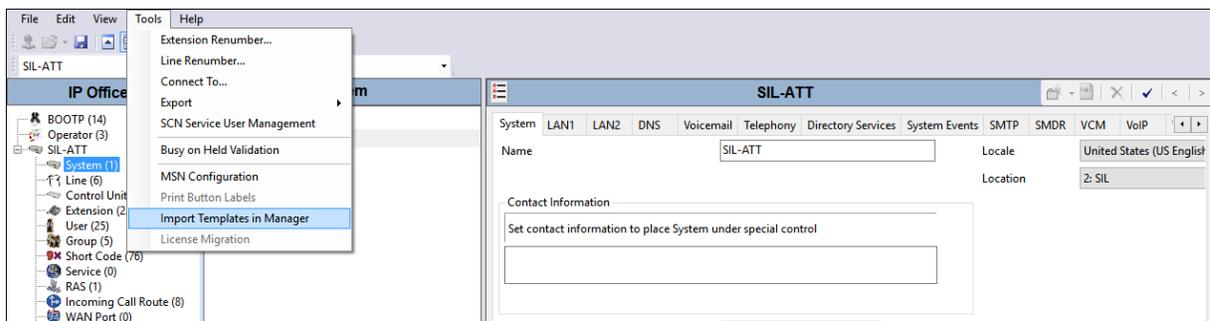
- SIL Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Requirements
- SIP Advanced Engineering

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.5.3 – 5.5.8**.

5.5.1. Importing a SIP Line Template

Note – DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (IP500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer’s environment.

1. Copy a previously created template file to a location (e.g., *\temp*) on the same computer where IP Office Manager is installed.
2. Import the template into IP Office Manager. From IP Office Manager, select **Tools → Import Templates in Manager**.

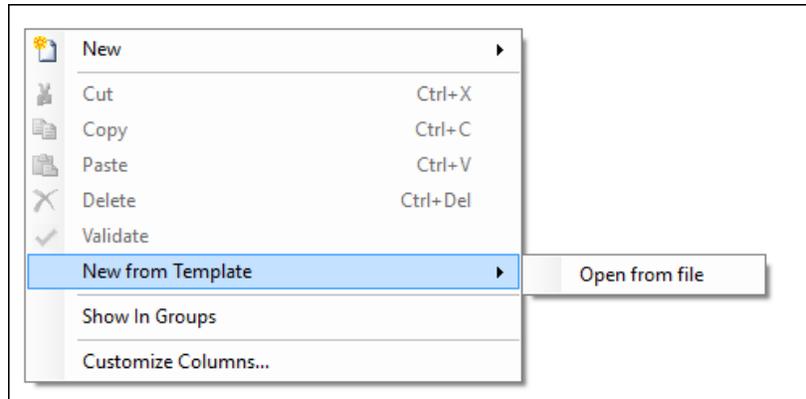


3. A folder browser will open (not shown). Select the directory used in **step 1** to store the template(s) (e.g., *\temp*). In the reference configuration, template file **IPO10SBC72IP6FR.xml** was imported. The template files are automatically copied into the IP Office default template location, **C:\Program Files\Avaya\IP Office\Manager\Templates**.
4. After the import is complete, a final import status pop-up window will open stating success or failure.

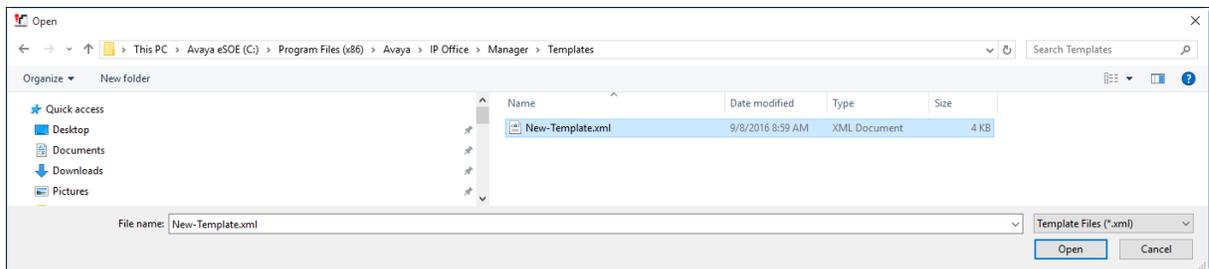


5.5.2. Creating a SIP Trunk from an XML Template

1. To create the SIP Trunk from a template, right-click on **Line** in the Navigation Pane, and hover over **New from Template**, and select **Open from file**.



2. Navigate to **C:\Program Files\Avaya\IP Office\Manager\Templates**. Select ***.xml** as the file type, find the template, and click **Open**.



The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line 2).

Line Number	Line Type	Line SubType
1	IP Office Line	WebSocket Server SCN
3	IP Office Line	WebSocket Server SCN
2	SIP Line	

Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.5.3 – 5.5.8**.

5.5.3. SIP Line – SIP Line tab

The **SIP Line** tab in the Details pane is shown below for **Line Number 4**, used for the SIP Trunk to AT&T IPFR-EF. Note, if no SIP Line exists, right click on the **Line** item in the **Navigation** pane and select **New → SIP Line** (not shown). In the reference configuration, SIP Line 4 was created. The SIP Line form is completed as follows:

- **ITSP Domain Name:** Set to the IP address of the Avaya SBCE A1 interface (e.g., **10.64.91.40**).
- **Local Domain Name:** Set to the IP address of the Avaya IP Office LAN1 SIP trunking interface (e.g., **10.64.19.170**).
- **In Service** and **Check OOS:** These boxes are checked (default).
 - Note that the Out Of Service (OOS) option is used in conjunction with SIP OPTIONS.
- **Refresh Method:** Set to **Re-Invite**, as AT&T does not support UPDATE.
- **Incoming Supervised Refer:** Set this field to **Always** to enable Avaya IP Office to accept REFER sent by the network during a transfer scenario.
- **Outgoing Supervised Refer:** Set this field to **Always** to enable Avaya IP Office to use REFER (with Replaces) for station initiated call transfer scenarios back to PSTN.
- **Outgoing Blind Refer:** Optional. Enable this option to support Refer (without Replaces) for “Blind” (unattended) transfers (e.g., transfer-to party is still ringing when the transfer operation is completed). If this feature is not enabled then Refer (with Replaces) will be used. **Note – This feature is only supported with SIP telephones.**
- Use the default values for the other fields.
- Click **OK** (not shown).

As described in **Section 5.3.3**, the **Name Priority** parameter may retain the default **System Default** setting, or can be configured to **Favor Trunk**. As shown below, the default **System Default** setting was used in the reference configuration.

Configuration	Line	SIP Line - Line 4
BOOTP (16)	Line Number	4
Operator (3)	Line Type	SIP Line
Solution	ITSP Domain Name	10.64.91.40
User (34)	Local Domain Name	10.64.19.170
Group (4)	URI Type	SIP
Short Code (56)	Location	Cloud
Directory (2)	Prefix	
Time Profile (0)	National Prefix	
Account Code (0)	International Prefix	
User Rights (1)	Country Code	
Location (5)	Name Priority	System Default
IPOSE-Primary	Description	SBCE-40 AT&T IPFR
System (1)	In Service	<input checked="" type="checkbox"/>
Line (9)	Check OOS	<input checked="" type="checkbox"/>
Control Unit (11)	Refresh Method	Re-Invite
Extension (13)	Timer (sec)	1800
User (15)	Redirect and Transfer	
Group (3)	Incoming Supervised REFER	Always
Short Code (7)	Outgoing Supervised REFER	Always
Service (0)	Send 302 Moved Temporarily	<input type="checkbox"/>
Incoming Call Rout	Outgoing Blind REFER	<input checked="" type="checkbox"/>
IP Route (2)		
License (9)		
ARS (9)		
Location (5)		
Authorization Code		
IPOSE-Secondary		
IP500 Expansion		

5.5.4. SIP Line – Transport tab

Select the **SIP Line** → **Transport** tab and configure the following:

- **ITSP Proxy Address:** Set to the Avaya SBCE A1 IP address (e.g., **10.64.91.40**).
- **Network Configuration** → **Layer 4 Protocol:** Set to **TLS**.
- **Network Configuration** → **Send Port:** Set to **5061**.
- **Network Configuration** → **Use Network Topology Info:** Set to **None**.
- **Network Configuration** → **Listen Port:** Set to **5061**.
- **Verify Calls Route via Registrar:** Enabled (default)
- **Click OK** (not shown).

The screenshot shows the 'Transport' tab of a SIP Line configuration window. The 'ITSP Proxy Address' is set to '10.64.91.40'. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'TLS', 'Send Port' is '5061', and 'Use Network Topology Info' is set to 'None'. 'Listen Port' is also '5061'. There are two 'Explicit DNS Server(s)' fields, both containing '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is checked. A 'Separate Registrar' field is empty.

5.5.5. SIP Line – SIP URI tab

Select the **SIP Line** → **SIP URI** tab. To add a new SIP URI, click the **Add...** button. At the bottom of the screen, a **New URL** area will be opened. Configure the following:

- **Local URI, Contact** and **Display Name** fields: Set these fields to **Use Internal Data**.
- **Identity:** Set to the default **None**.
- **Send Caller ID:** Set to **Diversion Header**. This is required by the AT&T IPFR-EF service for call redirection scenarios (e.g., Call Forward, Mobile Twinning).
- Verify **Diversion Header:** Set to the default **None**.
- Verify **Registration:** Set to the default **0: <None>**.
- **Incoming Group:** Set to **4** (SIP Line 4). This value references the table created with **Incoming Call Routes** in **Section 5.9**.
- **Outgoing Group:** Set to **4** (SIP Line 4). This will be used for routing outbound calls to AT&T via the **ARS** configuration (**Section 6.6**).
- **Max Sessions:** In the reference configuration this was set to **10**. This sets the maximum number of simultaneous calls that can use the URI before Avaya IP Office returns busy to any further calls.
- Click **OK**.

URI	Groups	Local URI	Contact	Display Name	Identity	Header	Originator Number	Send Caller ID	Diversion Header	Credential	Max Calls
1	4 4	<Internal>	<Internal>	<Internal>	None	PAI		Diversion	None	0: <Non...	10
2	4 24	Auto	Auto	Auto	None	PAI		None	None	0: <Non...	10

Edit URI	
Local URI	Use Internal Data
Contact	Use Internal Data
Display Name	Use Internal Data
Identity	
Identity	None
Header	P Asserted ID
Forwarding And Twinning	
Originator Number	
Send Caller ID	Diversion Header
Diversion Header	None
Registration	0: <None>
Incoming Group	4
Outgoing Group	4
Max Sessions	10

In the sample configuration, the single SIP URI shown above was sufficient to allow incoming calls for AT&T DID numbers destined for specific IP Office users or IP Office hunt groups. The calls are accepted by IP Office since the incoming number will match the SIP Name configured

for the user or group that is the destination for the call. URI 2 will match on any number not associated with users or groups, such as a DID number routed directly to voicemail or DID used for Mobile Call Control. DID numbers that IP Office should admit can be entered specifically, such as 3035559320, into the **Local URI** and **Contact** fields instead of “Use Internal Data”. To allow IP Office to admit any number, “**Auto**” can be entered into the **Local URI** and **Contact** fields as shown below. This URI entry will not be used for outbound dialing, therefore an unused number is specified for the **Outgoing Group**.

The screenshot shows the 'SIP Line Transport SIP URI VoIP SIP Credentials SIP Advanced Engineering' configuration window. At the top is a table with columns: URI, Groups, Local URI, Contact, Display Name, Identity, Header, Originator Number, Send Caller ID, Diversion Header, Credential, and Max Calls. Row 2 is selected, showing: URI 2, Groups 4 24, Local URI Auto, Contact Auto, Display Name Auto, Identity None, Header PAI, Originator Number, Send Caller ID None, Diversion Header None, Credential 0: <Non..., and Max Calls 10. Below the table is the 'Edit URI' form with fields for Local URI (Auto), Contact (Auto), Display Name (Auto), Identity (None), Header (P Asserted ID), Forwarding And Twinning (Originator Number, Send Caller ID: None), Diversion Header (None), Registration (0: <None>), Incoming Group (4), Outgoing Group (24), and Max Sessions (10). Buttons for 'Add...', 'Remove', 'Edit...', 'OK', and 'Cancel' are visible.

5.5.6. SIP Line – VoIP tab

Select the **SIP Line → VoIP** tab.

- The **Codec Selection** drop-down box → **System Default** will list all available codecs. In the reference configuration, **Custom** was selected and **G729(a) 8K CS-ACELP**, and **G.711 ULAW 64K** were specified. This causes Avaya IP Office to include these codecs in the Session Description Protocol (SDP) offer, and in the order specified. Note that in the reference configuration G.729A is set as the preferred codec on the SIP trunk to the AT&T IPFR-EF network.
- T.38 fax was used in the reference configuration. Set the **Fax Transport Support** drop-down menu to **T.38**. Note that Error Correction Mode (ECM) is enabled by default on the **T.38 Fax** tab (**Section 6.4**). ECM is supported by the AT&T IPFR-EF service. G.711 fax also worked in the reference configuration (T.38 option disabled); however, T.38 is the preferred method.
- The **DTMF Support** parameter can remain set to the default value **RFC2833/RFC4733**.

- Set the **Media Security** drop-down menu to **Same as System (Preferred)** to have IP Office use the system setting for media security set in **Section 5.3.5** to encrypted RTP toward Avaya SBCE.
- The **Re-invite Supported** parameter can be checked 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.
- Click **OK** (not shown).

SIP Line Transport SIP URI VoIP SIP Credentials SIP Advanced Engineering

Codec Selection: Custom

Unused: G.711 ALAW 64K, G.722 64K

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

Local Hold Music:

Re-invite Supported:

Codec Lockdown:

Allow Direct Media Path:

Force direct media with phones:

PRACK/100rel Supported:

Fax Transport Support: T38

DTMF Support: RFC2833/RFC4733

Media Security: Same as System (Preferred)

Advanced Media Security Options: Same As System

Encryptions: RTP, RTCP

Authentication: RTP, RTCP

Replay Protection: RTP, RTCP

SRTCP Window Size: 64

Crypto Suites: SRTP_AES_CM_128_SHA1_80, SRTP_AES_CM_128_SHA1_32

5.5.7. SIP Line – T38 Fax Tab

Note – This tab is only available when configuring a SIP line on IP Office 500 V2, and the settings on this tab are only accessible if **Re-invite Supported** and a **Fax Transport Support** option (**T38**) are selected on the **VoIP** tab (**Section 5.5.6**). See **Section 6.4** for T38 Fax settings.

5.5.8. SIP Line – SIP Advanced Tab

By default, Avaya IP Office will use the PPI (P-Preferred-Identity) header for signaling user information when privacy is invoked. However, AT&T utilizes the PAI (P-Asserted-Identity) header for privacy. Therefore, Avaya IP Office is configured to use the PAI header to pass the calling party information for authentication and billing when privacy is used (see **Sections 5.5.5** and **5.8**). IP Office can be configured to signal when a call is placed on hold by sending an INVITE with media attribute “sendonly”. AT&T in turn will respond with media attribute “recvonly”, and will stop sending RTP media for the duration the call is on hold. When the call is

taken off of hold, IP Office will send another INVITE with media attribute “sendrecv” indicating to AT&T to start sending RTP again.

- Select **Indicate HOLD**.
- Select **Emulate NOTIFY for Refer**.

Note – The AT&T IPFR-EF service does not support NOTIFY. Some Avaya endpoints (e.g., Avaya Communicator for Windows) require receipt of a NOTIFY when Refer based call transfers are performed. This option will send a NOTIFY to these endpoints.

- Select **No Refer if using Diversion**.

Note – By default, Avaya IP Office sends Refer in addition to Diversion header, for call forward scenarios. However, AT&T only requires Diversion header. Therefore, in the reference configuration the **No Refer if using Diversion** was selected.

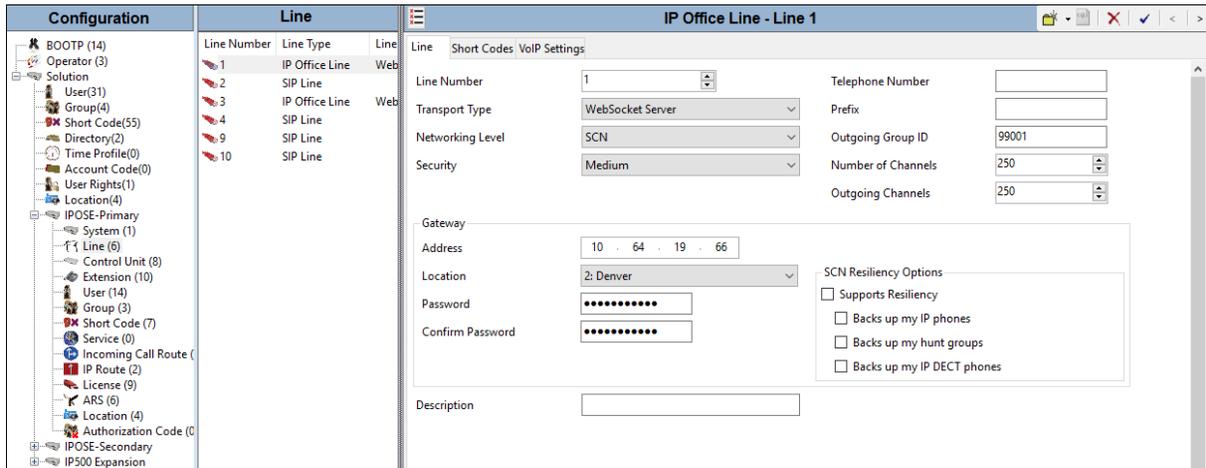
- Select the **Use PAI for Privacy** option, and click **Ok** (not shown).

The screenshot shows the 'SIP Advanced' configuration page for 'Engineering'. The page is divided into several sections:

- Addressing:** Association Method is 'By Source IP address', Call Routing Method is 'Request URI', and Suppress DNS SRV Lookups is unchecked.
- Identity:** 'Use PAI for Privacy' is checked. Other options like 'Use "phone-context"', 'Add user=phone', 'Use + for International', 'Use Domain for PAI', 'Swap From and PAI/Diversion', 'Caller ID from From header', 'Send From In Clear', 'Cache Auth Credentials', 'User-Agent and Server Headers', 'Send Location Info', 'Add UUI header', and 'Add UUI header to redirected calls' are unchecked.
- Media:** 'Indicate HOLD' is checked. Other options like 'Allow Empty INVITE', 'Send Empty re-INVITE', 'Allow To Tag Change', 'P-Early-Media Support', 'Send SilenceSupp=Off', 'Force Early Direct Media', and 'Media Connection Preservation' are either unchecked or set to 'None'/'Disabled'.
- Call Control:** 'Emulate NOTIFY for REFER' and 'No REFER if using Diversion' are checked. Other settings include 'Call Initiation Timeout (s)' at 4, 'Call Queuing Timeout (mins)' at 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', and 'Action on CAC Location Limit' set to 'Allow Voicemail'.

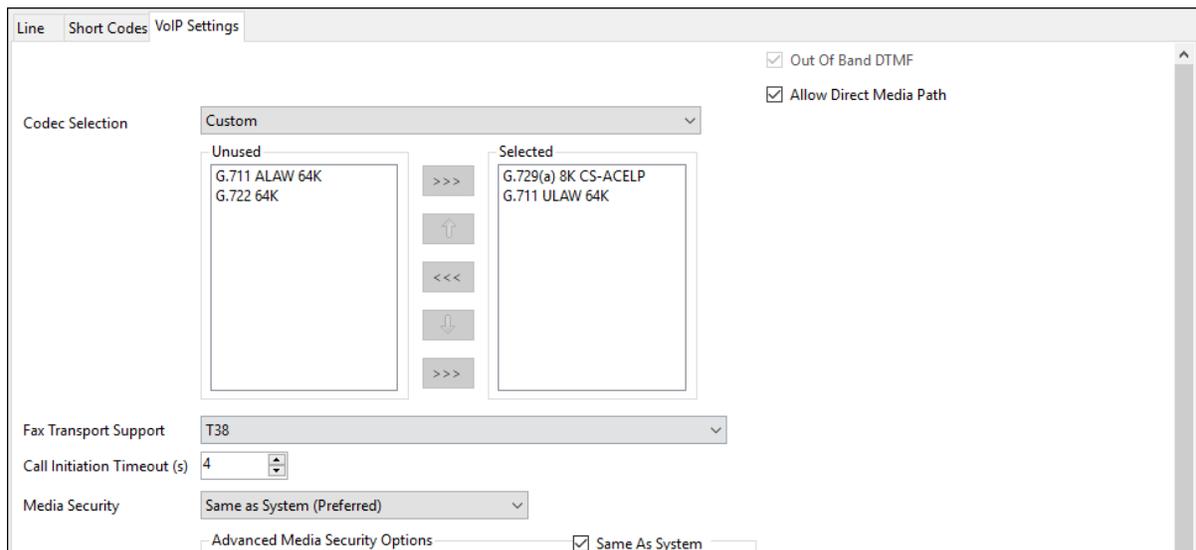
5.6. IP Office Line

IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate Line to be configured in the Group pane. Below is the IP Office Line to the Expansion System.



In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate T.38 fax, select the **VoIP Settings** tab and configure the following:

- **Fax Transport Support: T38**



5.7. Users, Extensions, and Hunt Groups

In this section, examples of an IP Office User, Extension, and Hunt Group will be illustrated. In the interests of brevity, not all users and extensions shown in **Figure 1** will be presented, since the configuration can be easily extrapolated to other users. To add a User, right click on **User** in the Navigation pane, and select **New**. To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane.

5.7.1. H.323 User 6322

The following screen shows the **User** tab for user 6322. As shown in **Figure 1**, this user corresponds to the Avaya 9608 H.323 endpoint.

User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membersh
Name	ATT-Avaya 9608											
Password											
Confirm Password											
Unique Identity												
Conference PIN											
Confirm Audio Conference PIN											
Account Status	Enabled											
Full Name	ATT-Avaya 9608											
Extension	6322											
Email Address												
Locale	United States (US English)											
Priority	5											
System Phone Rights	None											
Profile	Basic User											
	<input type="checkbox"/> Receptionist											

The following screen shows the **SIP** tab for user 6322. The **SIP Name** and **Contact** parameters are configured with the DID number of the user, “3035559322”. These parameters configure the user part of the SIP URI in the From header for outgoing SIP trunk calls, and allow matching of the SIP URI for incoming calls, without having to enter this number as an explicit SIP URI for the SIP Line. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** parameter may be checked to withhold the user’s information from the network. See **Section 5.8** for a method of using a short code (rather than static user provisioning) to place an anonymous call.

Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Menu Programming	Mobility	Group Membership	Announcements	SIP	Personal Directory
SIP Name	3035559322									
SIP Display Name (Alias)	ATT-Avaya 9608									
Contact	3035559322									
	<input type="checkbox"/> Anonymous									

The following screen shows the **Mobility** tab for user 6322. 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 mobile telephone, including the dial access code for ARS, in this case “93035552177”. Other options can be set according to customer requirements.

The screenshot displays the 'Mobility' configuration tab for user 6322. The 'Internal Twinning' section is unchecked. The 'Mobility Features' section is checked, and within it, 'Mobile Twinning' is also checked. The 'Mobile Twinning' section includes the following fields and options:

- Twinned Mobile Number (including dial access code): 93035552177
- Twinning Time Profile: <None>
- Mobile Dial Delay (sec): 0
- Mobile Answer Guard (sec): 0
- Hunt group calls eligible for mobile twinning:
- Forwarded calls eligible for mobile twinning:
- Twin When Logged Out:
- one-X Mobile Client:
- Mobile Call Control:
- Mobile Callback:

The following screen shows the Extension information for this user. To view, select **Extension** from the Navigation pane, and the appropriate extension from the Group pane.

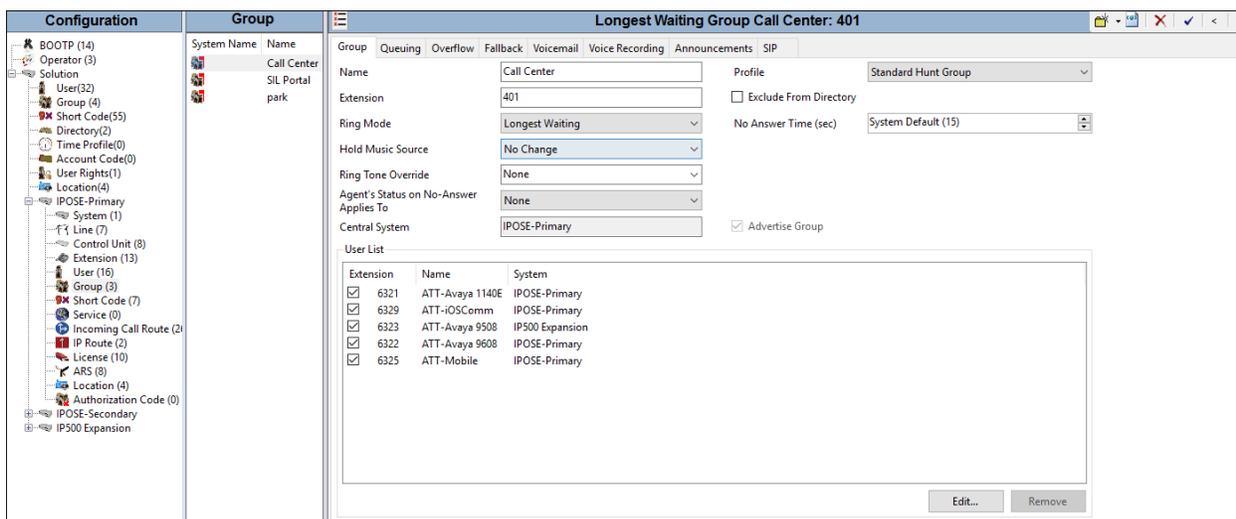
The screenshot displays the 'Extension' configuration page for H.323 Extension: 11212 6322. The left pane shows a tree view of the configuration hierarchy, with 'Extension' selected. The right pane shows the configuration details for the selected extension:

Field	Value
Extension ID	11212
Base Extension	6322
Phone Password	••••
Confirm Phone Password	••••
Caller Display Type	On
Reset Volume After Calls	<input type="checkbox"/>
Device Type	Unknown IP handset
Location	Automatic
Fallback As Remote Worker	Auto
Module	0
Port	0
Disable Speakerphone	<input type="checkbox"/>

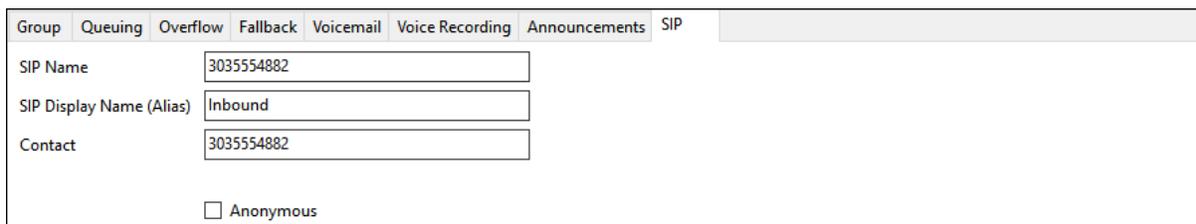
5.7.2. Hunt Groups

During the verification of these Application Notes, users could also receive incoming calls as members of a hunt group. To configure a new hunt group, right-click **Group** from the Navigation pane, and select **New**. To view or edit an existing hunt group, select **Group** from the Navigation pane, and the appropriate hunt group from the Group pane.

The following screen shows the **Group** tab for hunt group 401. The telephone extensions in the **User List** are rung based on the extension that has been unused for the longest period, due to the **Ring Mode** setting “**Longest Waiting**” (i.e., most idle user receives the next call). Click the **Edit** button to change the **User List**.



The following screen shows the **SIP** tab for hunt group 401. The **SIP Name** and **Contact** are configured with AT&T DID “**3035554882**”. Later, in **Section 5.9**, an Incoming Call Route will map 3035554882 to this hunt group based on the information entered on this tab.



5.8. Short Codes

In this section, various examples of IP Office short codes will be illustrated. To add a short code, right click on **Short Code** in the Navigation pane, and select **New**. To edit an existing short code, click **Short Code** in the Navigation pane, and the short code to be configured in the Group pane.

In the screen shown below, the Short Code **9N** is illustrated. This Short Code will allow an Avaya IP Office user to dial the digit 9 followed by any telephone number, symbolized by the

letter **N**, to reach the SIP Line to the Avaya SBCE/AT&T. However, Avaya IP Office will first consult the ARS table defined in **Section 5.10**. The variable **N** can be any number string.

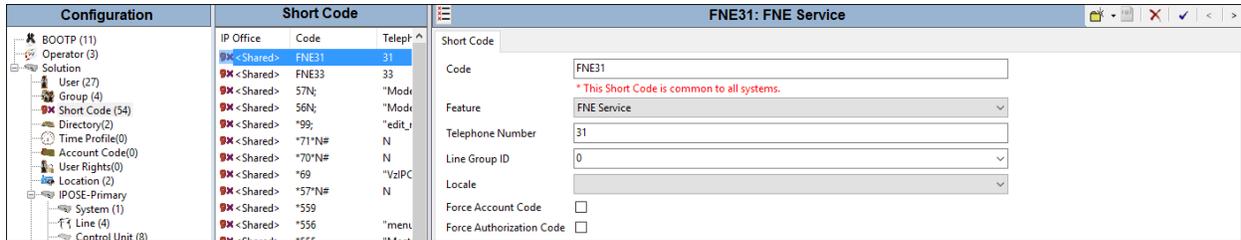
- The **Code** parameter is set to **9N**
- The **Feature** parameter is set to **Dial**
- The **Telephone Number** parameter is set to **N**
- The **Line Group ID** parameter is set to “**54: ATT-IPFR**”, which directs the call to ARS (see **Section 5.10**).
- Click the **OK** button (not shown)

Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	54: ATT-IPFR
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

Optionally, add or edit a short code that can be used to access the SIP Line anonymously. In the screen shown below, the short code ***67N** is illustrated. This short code is similar to the “**9N**” short code except that the **Telephone Number** field begins with the letter “**W**”, which means “withhold the outgoing calling line identification”. In the case of the SIP Line connecting to AT&T documented in these Application Notes, when a user dials ***67** plus any number “**N**”, IP Office will include the user’s telephone number in the P-Asserted-Identity (PAI) header (see **Section 5.5.8**) along with “Privacy: Id”. AT&T will allow the call due to the presence of a valid DID in the PAI header, but will prevent presentation of the caller id to the called PSTN destination.

Short Code	
Code	*67N
Feature	Dial
Telephone Number	WN
Line Group ID	54: ATT-IPFR
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

The following screen illustrates a solution level short code, common to all servers, that acts like a feature access code rather than a means to access a SIP Line. In this case, the **Code “FNE31”** is defined for **Feature “FNE Service”** to **Telephone Number “31”** (Mobile Call Control). This short code will be used as means to allow an AT&T DID to be programmed to route directly to this feature, via inclusion of this short code as the destination of an Incoming Call Route. See **Section 5.9**. This feature is used to provide dial tone to twinned mobile devices (e.g., cell phone) directly from IP Office; once dial tone is received the user can perform dialing actions including making calls and activating Short Codes.

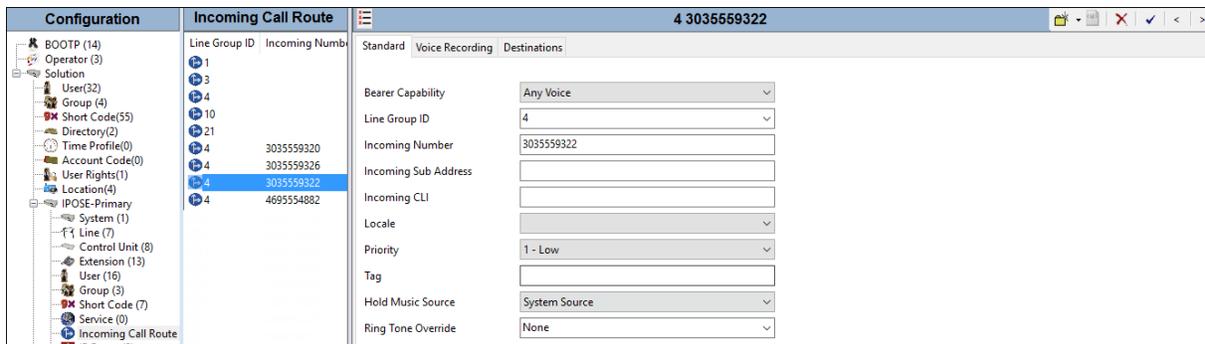


5.9. Incoming Call Routes

Each Incoming Call Route will map a specific AT&T DNIS number to a destination User, Hunt Group, or Short Code, on Avaya IP Office. To add an incoming call route, right click on **Incoming Call Route** in the Navigation pane, and select **New** (not shown). To edit an existing incoming call route, select **Incoming Call Route** in the Navigation pane, and the appropriate incoming call route to be configured in the Group pane.

Note – In the reference configuration, the AT&T IPFR-EF service delivered ten DNIS digits in the SIP Invite R-URI. Therefore, incoming calls to Avaya IP Office will match on the ten digit inbound AT&T DNIS string (e.g., **3035559322**). The AT&T IPFR-EF service can also be configured to deliver seven DNIS digits. Verify the digits being delivered by AT&T.

In the screen shown below, the incoming call route for **Incoming Number → 3035559322** is illustrated. The **Line Group ID** is set to **4**, matching the **Incoming Group** field configured in the **SIP URI** tab for the SIP Trunk to AT&T in **Section 5.5.5**.



Select the **Destinations** tab. From the **Destination** drop-down menu, select the extension to receive the call when AT&T delivers DNIS digits **3035559322**. In the reference configuration DNIS digits **3035559322** is associated with user **6322** (the 9608 H.323 telephone).

4 3035559322			
Standard Voice Recording Destinations			
TimeProfile	Destination	Fallback Extension	
▶ Default Value	6322 ATT-Avaya 9608	▼	▼

Repeat this process to route all AT&T DNIS numbers to additional telephone, as well as other Avaya IP Office destinations (Hunt Group (**4695554882**), Voicemail (**3035559320**), Short Codes (**3035559326**), etc.). For example:

4 4695554882			
Standard Voice Recording Destinations			
TimeProfile	Destination	Fallback Extension	
▶ Default Value	401 Call Center	▼	▼

4 3035559320			
Standard Voice Recording Destinations			
TimeProfile	Destination	Fallback Extension	
▶ Default Value	VoiceMail	▼	▼

4 3035559326			
Standard Voice Recording Destinations			
TimeProfile	Destination	Fallback Extension	
▶ Default Value	FNE31	▼	▼

Note - The **Destination** menu may not contain all desired destinations (e.g., Short Codes). In these cases the desired destination may be manually typed into the **Destination** field.

5.10. ARS

While detailed coverage of ARS is beyond the scope of these Application Notes, this section includes basic ARS screen illustrations and considerations. As described in **Section 5.8**, Short Code **9N** was defined for ARS access. Therefore, outbound calls via ARS are dialed as 9 plus the number. ARS will strip off the 9 and process the call based on the remaining digits.

- To add a new ARS route, right-click **ARS** in the Navigation pane, and select **New** (not shown). To view or edit an existing ARS route, select **ARS** in the Navigation pane, and select the appropriate route name in the Group pane (e.g., **54: ATT-IPFR**).
- To add a new ARS table entry, click on the **Add** button. To change an existing entry, click on the **Edit** button (note that the Edit button is grayed out until an entry is selected).

The following screen shows an example ARS configuration for the route **ATT-IPFR** (ARS Route ID 54).

- **Code = 1xxxxxxxxx** This means any dialed string starting with a 1, and 11 digits total will be routed to the specified Line Group.
- **Telephone Number = .**
- **Feature = Dial**
- **Line Group ID = 4** (SIP Line 4)

ARS

ARS Route ID: 54

Route Name: ATT-IPFR

Dial Delay Time: System Default (4)

Description: ATT IPFR

In Service: Out of Service Route: <None>

Time Profile: <None> Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
*7N;	.	Dial	4
*9N;	.	Dial	4
0N;	.	Dial	4
1xxxxxxxxx	.	Dial	4
311	.	Dial	4
411	.	Dial	4
711	.	Dial	4

Alternate Route Priority Level: 1

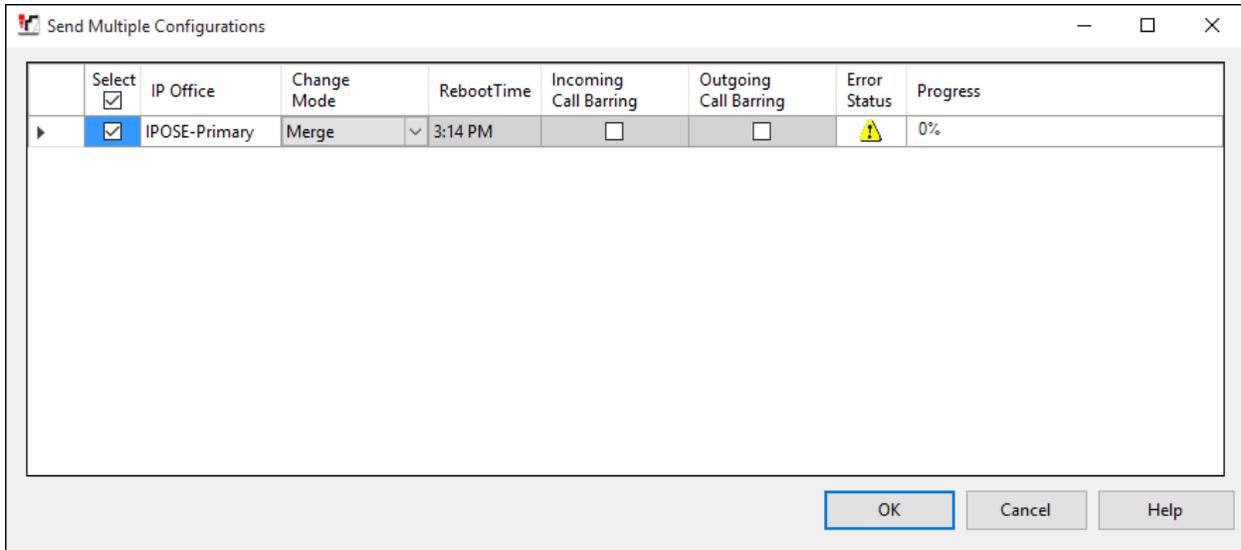
Alternate Route Wait Time: 5

Alternate Route: <None>

5.11. Save Configuration

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

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



6. Avaya IP Office Expansion Configuration

Navigate to **File** → **Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the “plus” sign next to **IP500 Expansion** on the left navigation pane will expand the menu on this server.

The screenshot shows the Avaya IP Office configuration interface. On the left is a navigation tree with 'IP500 Expansion' selected. The main area is titled 'Server Edition Expansion System' and contains the following sections:

- Hardware Installed:** Control Unit: IP 500 V2, Internal Modules: TCM8, COMBO6210/ATM4, Expansion Modules: NONE, Serial Number: 00e0070595f2
- System Settings:** IP Address: 10.64.19.66, Sub-Net Mask: 255.255.255.0, Default Gateway: 10.64.19.1, System Locale: United States (US English), System Location: 2: Denver, Device ID: NONE, Number of Extensions on System: 16
- Features Configured:** Licenses Installed: Power User(2); SIP Trunk Channels(25); Server Edition R10(1); Basic User(14), Connected Extensions: 201; 6242, Users NOT Configured for Voicemail: Fax, Users assigned as Ex-Directory: NONE, Users assigned for Twinning: NONE, Users barred from making Outgoing Calls: NONE, Music on Hold: WAV File

6.1. Physical Hardware

In the sample configuration, looking at the Expansion System IP500 V2 from left to right, the first module is a TCM 8 Digital Station Module. This module supports BCM / Norstar T-Series and M-Series telephones. The second module is a COMBO6210/ATM4 module. This module is used to add a combination of ports to an IP500 V2 control unit and is not supported by IP500 control units. The module supports 10 voice compression channels. Codec support is G.711, G729A and G.723 with 64ms echo cancellation. G.722 is supported by IP Office Release 8.0 and higher. The “Combo” card will support 6 Digital Station ports for digital stations in slots 1-6 (except 3800, 4100, 4400, 7400, M and T-Series), 2 Analog Extension ports in slots 7-8, and 4 Analog Trunk ports in slots 9-12.

The screenshot shows the 'Server Edition' configuration page. It includes a 'Hardware Installed' section, a 'System Settings' section, and a 'System Status' sidebar. At the bottom, there is a table summarizing the system components:

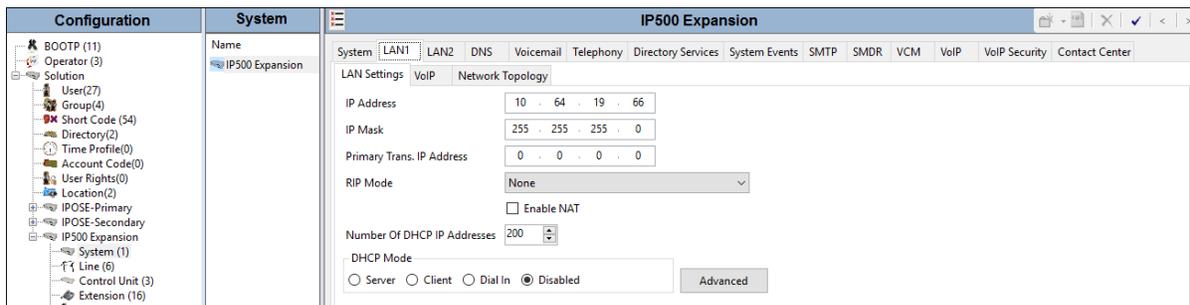
Description	Name	Address	Primary Link	Secondary Link	Users Configured	Extensions Configured
Solution					27	25
Primary Server	IPOSE-Primary	10.64.19.170		Bothway	11	9
Secondary Server	IPOSE-Secondary	10.64.19.175	Bothway		0	0
Expansion System	IP500 Expansion	10.64.19.66	Bothway	Bothway	16	16

6.2. System Settings

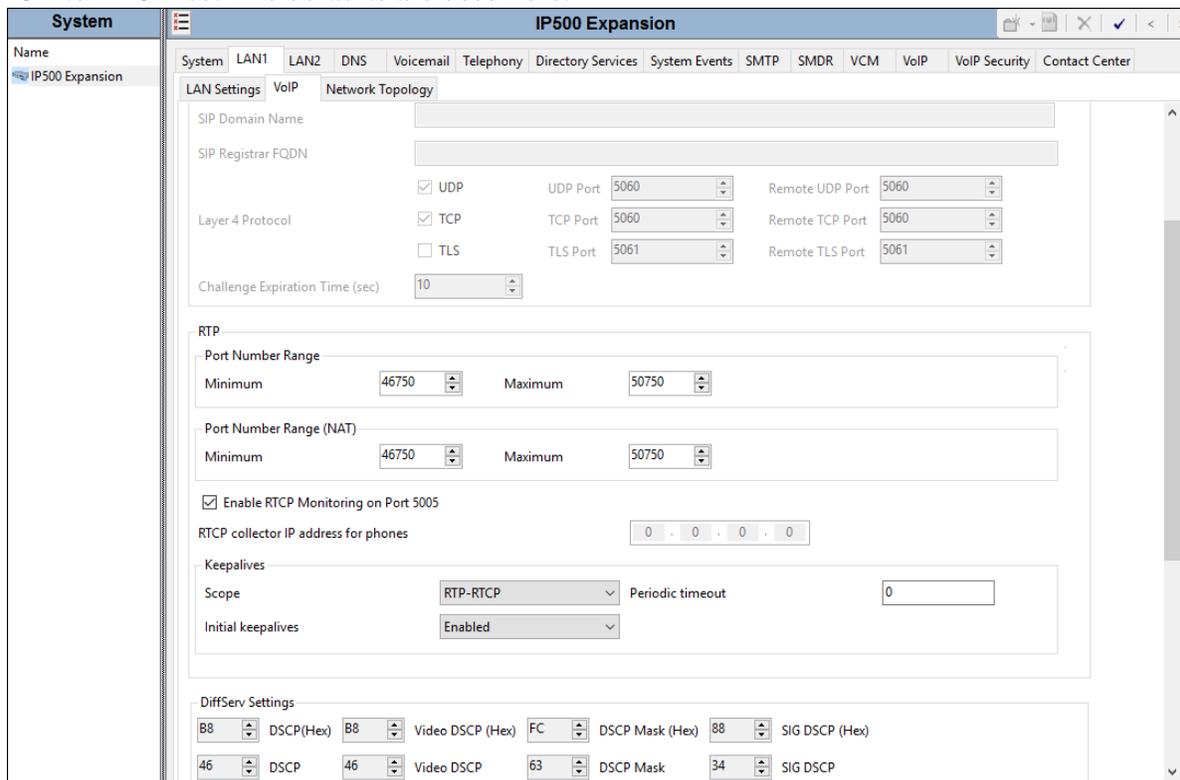
This section illustrates the configuration of system settings. Select **System** in the Navigation pane to configure these settings. The subsection order corresponds to a left to right navigation of the tabs in the Details pane for System settings. For all of the following configuration sections, the **OK** button (not shown) must be selected in order for any changes to be saved.

6.2.1. LAN Settings

In the sample configuration, LAN1 is used to connect the Expansion System to the enterprise network. To view or configure the **IP Address** of LAN1, select the **LAN1** tab followed by the **LAN Settings** tab. As shown in **Figure 1**, the IP Address of the Expansion System is **10.64.19.66**. Other parameters on this screen may be set according to customer requirements.

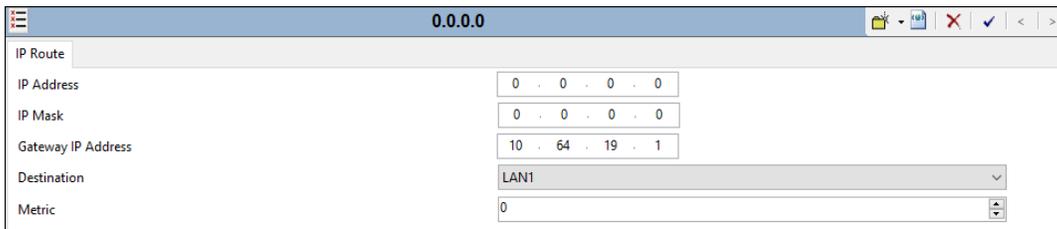


Select the **VoIP** tab as shown in the following screen. If desired, the **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media paths from Avaya SBCE to IP Office. The defaults are used here.



6.3. IP Route

Configuration is the same as the Primary server, as shown in **Section 5.4**.

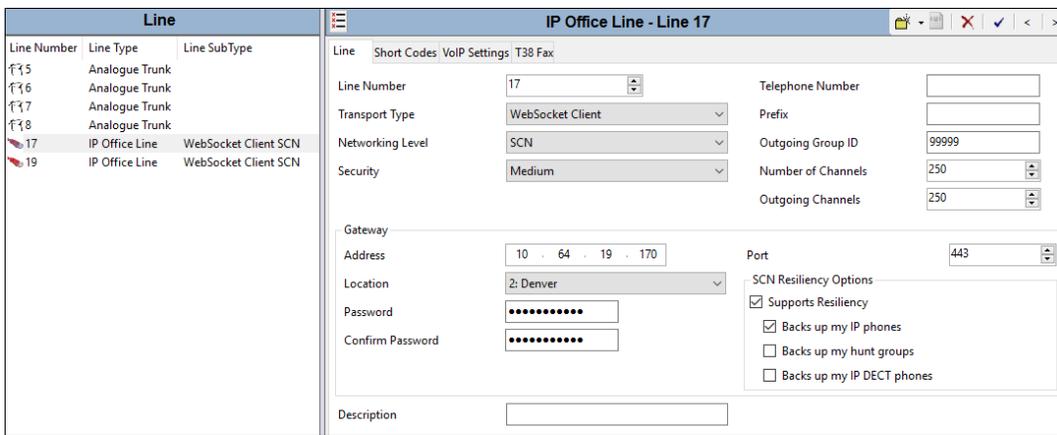


The screenshot shows the 'IP Route' configuration window. The title bar displays '0.0.0.0'. The configuration fields are as follows:

IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	10 . 64 . 19 . 1
Destination	LAN1
Metric	0

6.4. IP Office Line

The IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. Below is the IP Office Line to the Primary server.

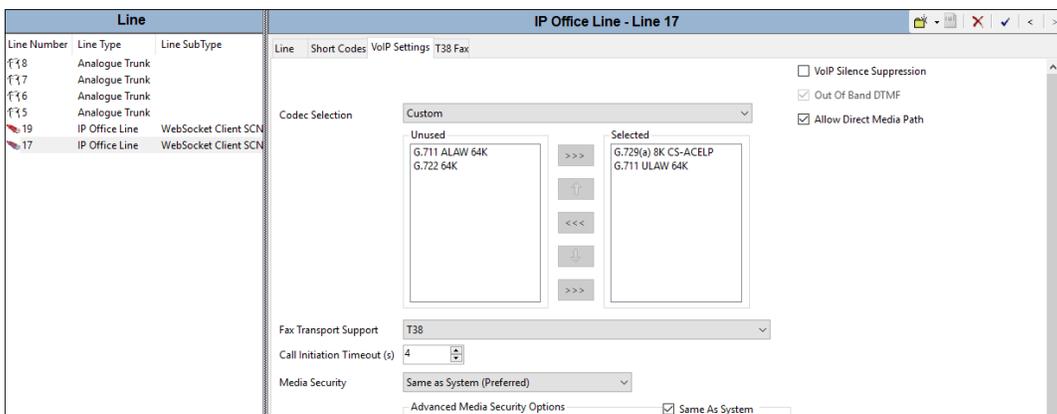


The screenshot shows the 'IP Office Line - Line 17' configuration window. The title bar displays 'IP Office Line - Line 17'. The configuration fields are as follows:

Line Number	17	Telephone Number	
Transport Type	WebSocket Client	Prefix	
Networking Level	SCN	Outgoing Group ID	99999
Security	Medium	Number of Channels	250
		Outgoing Channels	250
Gateway Address	10 . 64 . 19 . 170	Port	443
Location	2: Denver	SCN Resiliency Options	<input checked="" type="checkbox"/> Supports Resiliency
Password	*****		<input checked="" type="checkbox"/> Backs up my IP phones
Confirm Password	*****		<input type="checkbox"/> Backs up my hunt groups
			<input type="checkbox"/> Backs up my IP DECT phones
Description			

In the reference configuration, a fax machine is connected to one of the analog ports on the Expansion System. To accommodate T.38 fax, select the **VoIP Settings** tab and configure the following:

- **Fax Transport Support: T38**



The screenshot shows the 'IP Office Line - Line 17' configuration window with the 'VoIP Settings' tab selected. The configuration fields are as follows:

Codec Selection	Custom	<input type="checkbox"/> VoIP Silence Suppression
		<input checked="" type="checkbox"/> Out Of Band DTMF
		<input checked="" type="checkbox"/> Allow Direct Media Path
Fax Transport Support	T38	
Call Initiation Timeout (s)	4	
Media Security	Same as System (Preferred)	
		<input checked="" type="checkbox"/> Same As System

Select the **T38 Fax** tab. The **T38 Fax Version** is set to “0”. All other values are left at default.

Line Number	Line Type	IP Address	Line S
18	Analogue Trunk		
17	IP Office Line	10.64.19.170	WebS
19	IP Office Line	10.64.19.175	WebS

Line	Short Codes	VoIP Settings	T38 Fax
T38 Fax Version: 0			
Transport: UDPTL			
Redundancy			
Low Speed: 0			
High Speed: 0			
TCF Method: Trans TCF			
Max Bit Rate (bps): 14400			
EFlag Start Timer (ms): 2600			
EFlag Stop Timer (ms): 2300			
Tx Network Timeout (sec): 150			
<input type="checkbox"/> Use Default Values			

6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.8**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to an ARS route illustrated in the next section.

Configuration	Short Code	Telep
BOOTP (11)		
Operator (3)	*92N;	N*.2
Solution	*91N;	N*.1
User (27)	*9000*	*MA
Group(4)	*66*N#	N
Short Code (54)	*44	2
Directory(2)	*43	2
Time Profile(0)	*42	2
Account Code(0)	*41	1
User Rights(0)	*40	1
Location (4)	*39	1
IPOSE-Primary	*29	
IPOSE-Secondary		
IP500 Expansion		
System (1)	14xxx	14N
Line (6)	8N	N
Control Unit (3)	9N	N
Extension (16)		
User (17)		

Short Code
Code: 9N
Feature: Dial
Telephone Number: N
Line Group ID: 51: To-Primary
Locale:
Force Account Code: <input type="checkbox"/>
Force Authorization Code: <input type="checkbox"/>

6.6. ARS

The following screen shows an example ARS configuration for the route named “**To-Primary**” on the Expansion System. The **Line Group ID** is set to “**99999**” matching the number of the **Outgoing Group** configured on the IP Office Line 17 to the Primary server (**Section 6.4**).

The screenshot shows the ARS configuration window for the route named "To-Primary". The window title is "To-Primary". The configuration fields are as follows:

- ARS Route ID: 51
- Route Name: To-Primary
- Dial Delay Time: System Default (4)
- Description: (empty)
- In Service: (checked)
- Time Profile: <None>
- Secondary Dial tone: (checked), SystemTone
- Check User Call Barring: (checked)
- Out of Service Route: 52: To-Secondary
- Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
xN	9N	Dial	99999
911	9911	Dial Emergency	99999

Buttons: Add..., Remove, Edit...

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

Alternate Route: 52: To-Secondary

6.7. Save Configuration

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

7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, dual Avaya SBCEs are used as edge devices between the CPE and AT&T.

This section covers the configuration of the Avaya SBCE. It is assumed that the initial provisioning of the Avaya SBCE, including the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

Use a WEB browser to access the Element Management Server (EMS) web interface, and enter `https://ipaddress/sbc` in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE.

Enter the **Username** and click on **Continue**.



AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2017 Avaya Inc. All rights reserved.

Enter the password and click on **Log In**.



AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2017 Avaya Inc. All rights reserved.

The main page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is “OK”. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

The screenshot shows the Avaya SBCE Dashboard. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo. A left sidebar lists navigation options: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "Dashboard" and contains several sections:

- Information:** A table with rows for System Time (04:02:38 PM MDT), Version (7.2.0.0-18-13712), Build Date (Thu Jun 1 00:12:50 UTC 2017), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (07/17/2017 15:43:48 MDT), and Failed Login Attempts (0).
- Installed Devices:** A list showing EMS and SBCE.
- Active Alarms (past 24 hours):** None found.
- Incidents (past 24 hours):** Two incidents: "SBCE : Heartbeat Successful, Server is UP" and "SBCE : Heartbeat Failed, Server is Down".
- Notes:** No notes found.

7.1. System Management – Status

Select **System Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative. To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **SBCE** is shown. To view the configuration of this device, click **View** as highlighted below

Note – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.

The screenshot shows the Avaya SBCE System Management page. The top navigation bar is the same as the dashboard. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar is the same as the dashboard. The main content area is titled "System Management" and contains a sub-navigation bar with tabs: Devices, Updates, SSL VPN, Licensing, and Key Bundles. Below this is a table of installed devices:

Device Name	Management IP	Version	Status						
SBCE	10.64.90.40	7.2.0.0-18-13712	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. In the shared test environment, the highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to AT&T.

General Configuration Appliance Name SBCE Box Type SIP Deployment Mode Proxy		Device Configuration HA Mode No Two Bypass Mode No		License Allocation Standard Sessions Requested: 50 50 Advanced Sessions Requested: 50 50 Scopia Video Sessions Requested: 5 5 CES Sessions Requested: 0 0 Transcoding Sessions Requested: 50 50 Encryption <input checked="" type="checkbox"/>																															
Network Configuration <table border="1"> <thead> <tr> <th>IP</th> <th>Public IP</th> <th>Network Prefix or Subnet Mask</th> <th>Gateway</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td>10.64.91.40</td> <td>10.64.91.40</td> <td>255.255.255.0</td> <td>10.64.91.1</td> <td>A1</td> </tr> <tr> <td>10.64.91.40</td> <td>10.64.91.40</td> <td>255.255.255.0</td> <td>10.64.91.1</td> <td>A1</td> </tr> <tr> <td>10.64.91.40</td> <td>10.64.91.40</td> <td>255.255.255.248</td> <td>10.64.91.1</td> <td>B2</td> </tr> <tr> <td>3ffe.ffff.bb:bb::240</td> <td>3ffe.ffff.bb:bb::240</td> <td>64</td> <td>3ffe.ffff.bb:bb::1</td> <td>B1</td> </tr> <tr> <td>10.64.91.40</td> <td>10.64.91.40</td> <td>255.255.255.128</td> <td>10.64.91.1</td> <td>B1</td> </tr> </tbody> </table>						IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface	10.64.91.40	10.64.91.40	255.255.255.0	10.64.91.1	A1	10.64.91.40	10.64.91.40	255.255.255.0	10.64.91.1	A1	10.64.91.40	10.64.91.40	255.255.255.248	10.64.91.1	B2	3ffe.ffff.bb:bb::240	3ffe.ffff.bb:bb::240	64	3ffe.ffff.bb:bb::1	B1	10.64.91.40	10.64.91.40	255.255.255.128	10.64.91.1	B1
IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface																															
10.64.91.40	10.64.91.40	255.255.255.0	10.64.91.1	A1																															
10.64.91.40	10.64.91.40	255.255.255.0	10.64.91.1	A1																															
10.64.91.40	10.64.91.40	255.255.255.248	10.64.91.1	B2																															
3ffe.ffff.bb:bb::240	3ffe.ffff.bb:bb::240	64	3ffe.ffff.bb:bb::1	B1																															
10.64.91.40	10.64.91.40	255.255.255.128	10.64.91.1	B1																															
DNS Configuration Primary DNS 10.64.90.201 Secondary DNS DNS Location DMZ DNS Client IP 10.64.91.40		Management IP(s) IP #1 (IPv4) 10.64.90.40																																	

7.2. TLS Management

Note – Testing was done using identity certificates signed by a local certificate authority. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between IP Office and Avaya SBCE. The following procedures show how to view the certificates and configure the profiles to support the TLS connection.

7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

Step 1 - Select **TLS Management** → **Certificates** from the left-hand menu. Verify the following:

- The root CA certificate is present in the **Installed CA Certificates** area.
- The signed identity certificate is present in the **Installed Certificates** area.
- The private key associated with the identity certificate is present in the **Installed Keys** area.



7.2.2. Server Profiles

Step 1 - Select **TLS Management** → **Server Profiles**, and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbc40.crt**, from pull down menu.
- **Peer Verification = None.**
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

Edit Profile X

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

Profile Name

Certificate

Certificate Verification

Peer Verification

Peer Certificate Authorities

Peer Certificate Revocation Lists

Verification Depth

The following screen shows the completed TLS Server Profile form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right corner. On the left is a navigation menu with categories like Dashboard, Administration, System Management, and TLS Management. The "Server Profiles" section is active, showing a list with "sbc40-server" selected. The main content area shows the configuration for "Server Profile: sbc40-server".

Server Profiles: sbc40-server [Add] [Delete]

Click here to add a description.

TLS Profile	
Profile Name	sbc40-server
Certificate	sbc40.crt

Certificate Verification	
Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:DH:1ADH:IMD5:1aNULL:1eNULL:@STRENGTH

[Edit]

7.2.3. Client Profiles

Step 1 - Select **TLS Management** → **Client Profiles**, and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbc40.crt**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **GSSCPSMGRCA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

Edit Profile X

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

Profile Name: sbc40-client

Certificate: sbc40.crt

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities: GSSCPSMGRCA.pem

Peer Certificate Revocation Lists:

Verification Depth: 1

Extended Hostname Verification:

Custom Hostname Override:

Next

The following screen shows the completed TLS **Client Profile** form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo in the top right. A left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management (selected), Certificates, Client Profiles (selected), Server Profiles, and Device Specific Settings. The main content area is titled "Client Profiles: sbc40-client" and contains a "Delete" button. Below this is a "Client Profiles" list with "sbc40-client" selected. The "Client Profile" configuration form is shown with the following details:

Client Profile	
Click here to add a description	
TLS Profile	
Profile Name	sbc40-client
Certificate	sbc40.crt
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	GSSCPSMGRCA.pem
Peer Certificate Revocation Lists	--
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH DH ADH MD5 aNULL eNULL @STRENGTH
<input type="button" value="Edit"/>	

7.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings** → **Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the enterprise interface is assigned to **A1** and the interface towards AT&T is assigned to **B1**.

The following Avaya SBCE IP addresses and associated interfaces were used in the sample configuration:

- **B1: 3ffe:ffff:bb:bb::240** – IP address configured for the AT&T IPFR-EF service. This address is known to AT&T. See **Section 3**.
- **A1: 10.64.91.40** – IP address configured for AT&T IPFR-EF service to IP Office.

Network Management: SBCE

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Inside-A1	10.64.91.1	255.255.255.0	A1	10.64.91.40		
Outside-B2		255.255.255.248	B2		Edit	Delete
Outside-B1-IPv6	3ffe.ffff.bb.bb::1	64	B1	3ffe.ffff.bb.bb::240	Edit	Delete
Outside-B1		255.255.255.128	B1		Edit	Delete

The following screen shows interface **A1**, and **B1** are **Enabled**. To enable an interface click the corresponding **Disabled** Status link to change it to **Enabled**.

Session Border Controller for Enterprise

Network Management: SBCE

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Enabled

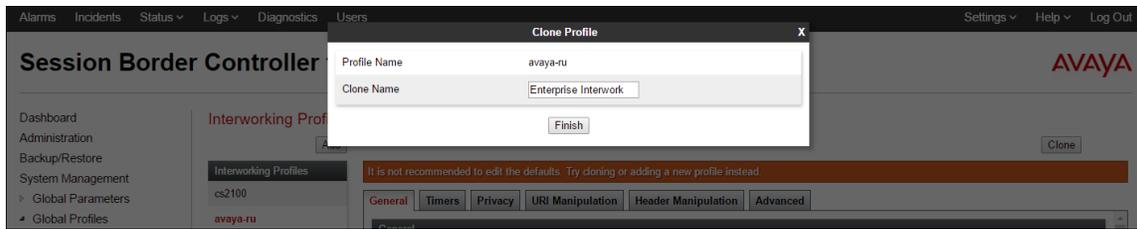
7.4. Server Interworking Profile

The Server Internetworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

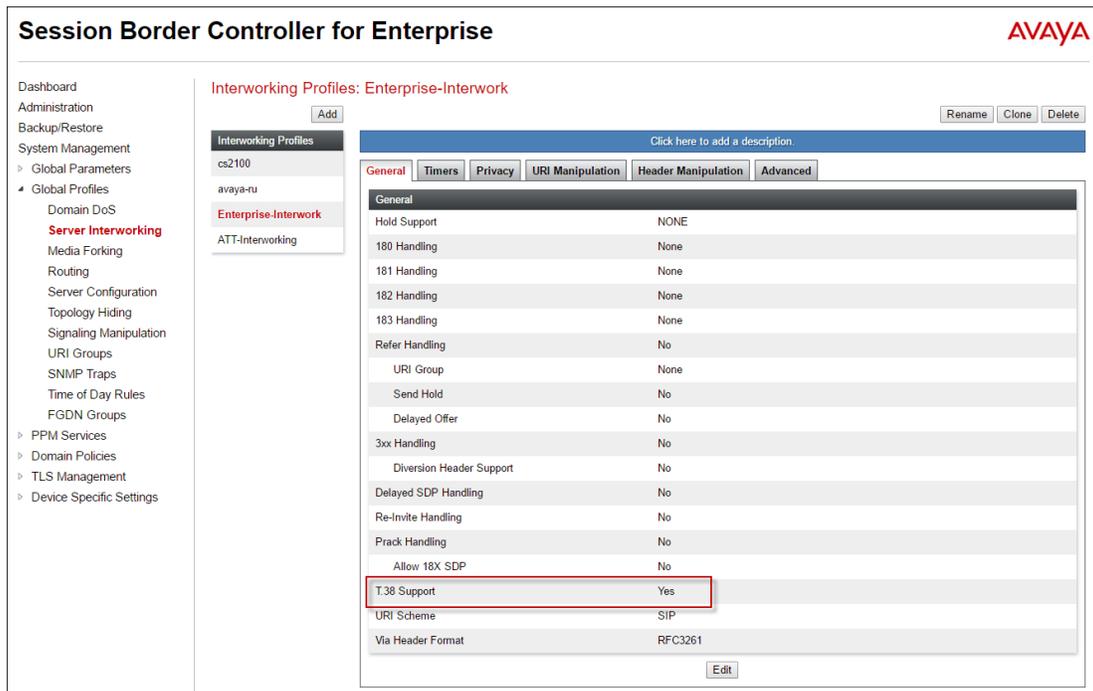
In the sample configuration, separate Server Interworking Profiles were created for IP Office and AT&T IPFR-EF service.

7.4.1. Server Interworking Profile – IP Office

In the sample configuration, the IP Office Server Interworking profile was cloned from the default **avaya-ru** profile. To clone a Server Interworking Profile for IP Office, navigate to **Global Profiles → Server Interworking**, select the **avayu-ru** profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.

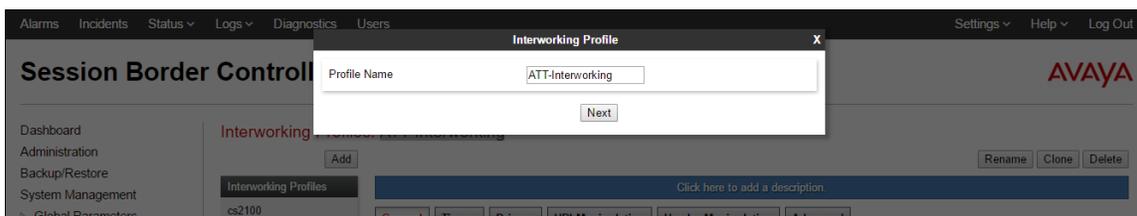


The following screen shows the “**Enterprise-Interwork**” profile used in the sample configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish** (not shown). Default values can be used for all other fields.



7.4.2. Server Interworking Profile – AT&T

To create a new Server Interworking Profile for AT&T, navigate to **Global Profiles** → **Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**.



The following screens show the “**ATT-Interworking**” profile used in the sample configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to **Yes**.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
 > Global Parameters
 Global Profiles
 Domain DoS
 Server Interworking
 Media Forking
 Routing
 Server Configuration
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SNMP Traps
 Time of Day Rules
 FGDN Groups
 PPM Services
 Domain Policies
 TLS Management
 Device Specific Settings

Interworking Profiles: ATT-Interworking

Interworking Profiles: cs2100, avaya-ru, Enterprise-Interwork, **ATT-Interworking**

Click here to add a description.

General | Timers | Privacy | URI Manipulation | Header Manipulation | Advanced

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

Edit

The **Timers** tab shows the values used for compliance testing for the **Trans Expire** field. The **Trans Expire** timer sets the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if it exists.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
 > Global Parameters
 Global Profiles
 Domain DoS
 Server Interworking
 Media Forking
 Routing
 Server Configuration
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SNMP Traps

Interworking Profiles: ATT-Interworking

Interworking Profiles: cs2100, avaya-ru, Enterprise-Interwork, **ATT-Interworking**

Click here to add a description.

General | **Timers** | Privacy | URI Manipulation | Header Manipulation | Advanced

SIP Timers	
Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	4 seconds
Invite Expire	---

Edit

Click **Next** to accept default parameters for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown) and advance to the **Advanced** area. **Record Routes** is set to **“Both Sides”**. Default values can be used for all other fields.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
PPM Services
Domain Policies

Interworking Profiles: ATT-Interworking

cs2100
avaya-ru
Enterprise-Interwork
ATT-Interworking

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation **Advanced**

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No

DTMF

DTMF Support	None
--------------	------

Edit

7.5. Signaling Manipulation

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. In the reference configuration, one signaling manipulation script is used.

Note – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Server Interworking Profiles (**Section 7.4**) or Signaling Rules (**Section 7.11**) does not meet the desired result. Refer to [7] for information on the Avaya SBCE scripting language.

Step 1 - As described in **Section 2.2, Item 2**, when an inbound call with AT&T IPFR-EF Sequential Ringing feature activated is answered by voicemail, no audio is heard. To fix this issue, the initial INVITE is manipulated to change the SDP media attribute “sendonly” to “sendrecv”.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Signaling Manipulation**.
3. Click **Add Script** (not shown) and the script editor window will open.
4. Enter a name for the script in the **Title** box (e.g., **ATT IPv6 with IPO**). The following script is defined:

Title Save

```

1 // AT&T Sequential Ringing, change a=sendonly to a=sendrecv
2 within session "ALL"
3 {
4     act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
5     {
6         %BODY[1].regex_replace("a=sendonly","a=sendrecv");
7     }
8 }

```

Step 2 - Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the IP Office Server Flow in **Section 7.16**.

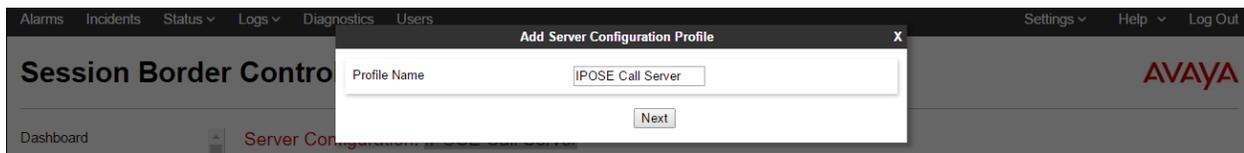
7.6. Server Configuration

The **Server Configuration** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

In the sample configuration, separate Server Configurations were created for IP Office and AT&T IPFR-EF service.

7.6.1. Server Configuration – IP Office

To add a Server Configuration Profile for IP Office, navigate to **Global Profiles** → **Server Configuration** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



The following screens illustrate the Server Configuration for the Profile name “**IPOSE Call Server**”. In the **General** parameters, the **Server Type** is set to “**Call Server**”. In the **IP Address / FQDN** field, the IP Address of the Primary server LAN 1 interface in the sample configuration is entered. This IP address is “**10.64.19.170**”. Under **Port**, “**5061**” is entered, and the **Transport** parameter is set to “**TLS**”. The TLS profile “**sbc40-client**” created in **Section 7.2.3** is selected for **TLS Client Profile**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

Edit Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Call Server

SIP Domain: [Empty]

TLS Client Profile: sbc40-client

[Add]

IP Address / FQDN	Port	Transport	
10.64.19.170	5061	TLS	Delete

[Finish]

Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeat** tab. The Avaya SBCE can be configured to source “heartbeats” in the form of PINGs or SIP OPTIONS towards IP Office. When remote workers are configured, IP Office may not respond to SIP OPTIONS from the SBCE IP address designated for remote workers; therefore PING will be used instead.

Select **PING** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source PINGs towards IP Office.

Server Configuration: IPOSE Call Server

[Add] [Rename] [Clone] [Delete]

Server Profiles: ATT-trk-svr, ATT-TollFree-trk-svr, large-site, IPO-500v2 CallServer, IPOSE Secondary, EnterpriseCallServer, ams, ATT-IPv6-trk-svr, **IPOSE Call Server**

General | **Authentication** | **Heartbeat** | Ping | Advanced

Enable Heartbeat:

Method: PING

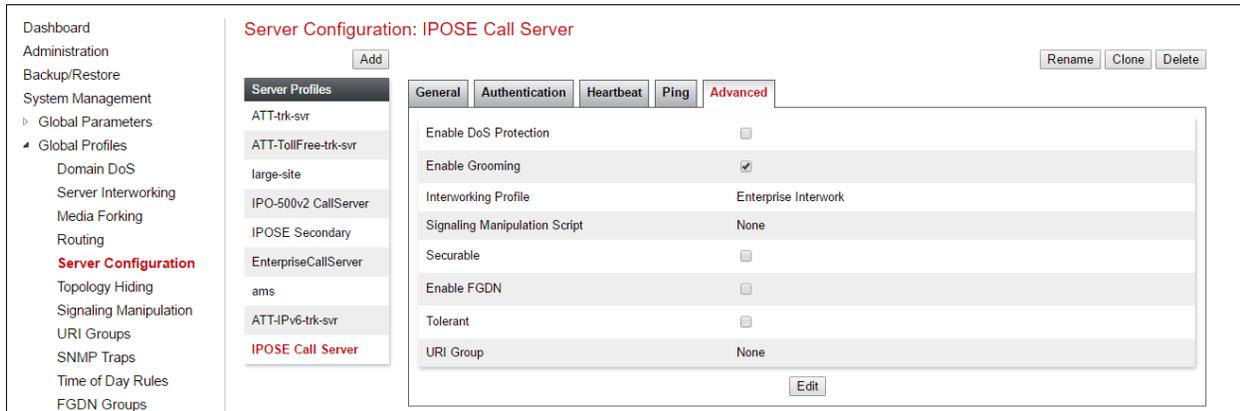
Frequency: 120 seconds

From URI: SBCE@silipose.customera.com

To URI: IPOSE@silipose.customera.com

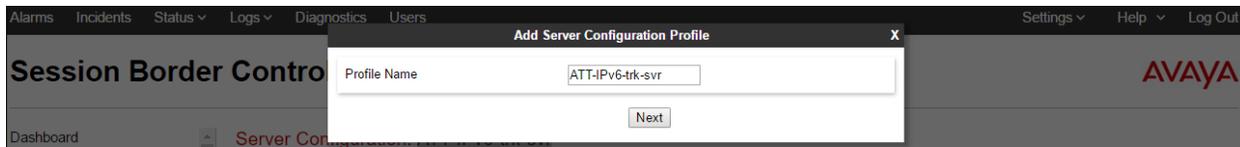
[Edit]

On the **Advanced** tab, **Enable Grooming** is checked and the **Interworking Profile** is set to “**Enterprise-Interwork**” created in **Section 7.4.1** for IP Office.

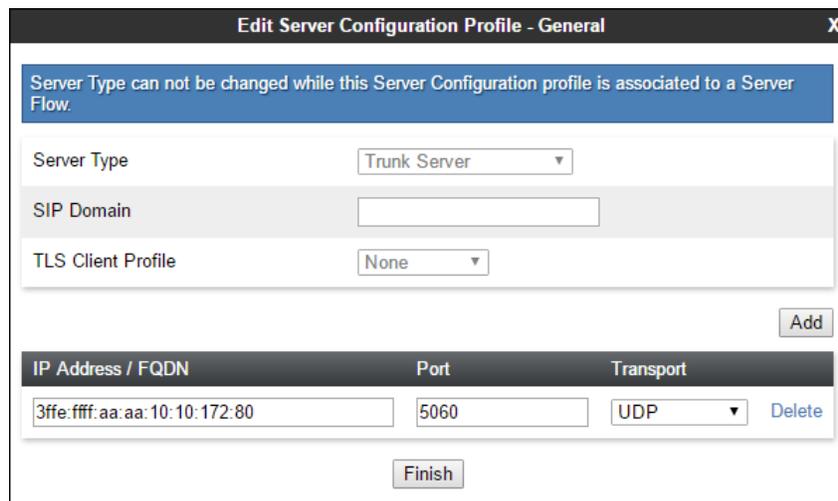


7.6.2. Server Configuration – AT&T

To add a Server Configuration Profile for AT&T, navigate to **Global Profiles** → **Server Configuration** and click **Add**. Enter a descriptive name for the new profile and click **Next**.

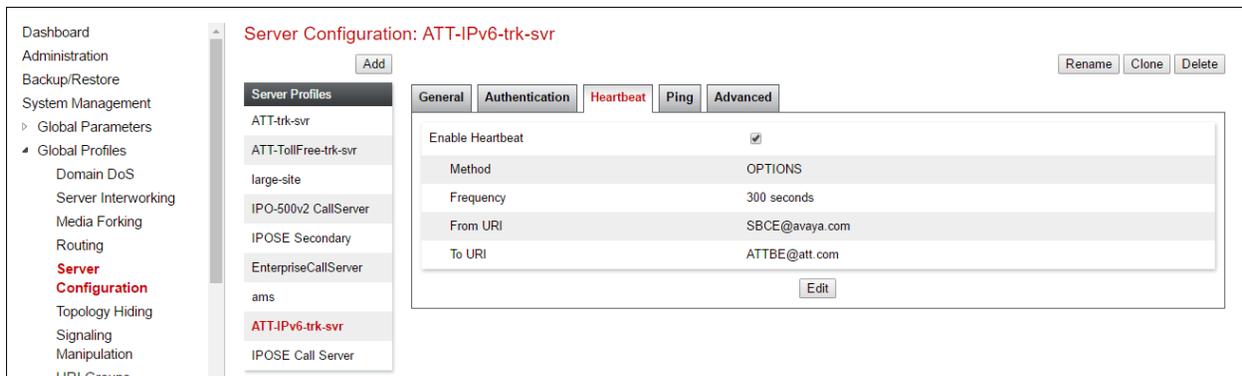


The following screens illustrate the Server Configuration for the Profile name “**ATT-IPv6-trk-svr**”. In the **General** parameters, the **Server Type** is set to “**Trunk Server**”. In the **IP Address / FQDN** field, the AT&T-provided IP address is entered. This is “**3ffe:ffff:aa:aa:10:10:172:80**”. The IPv6 address needs to be entered using lowercase characters. See **Section 2.2** for limitations in entering an IPv6 address. Under **Port**, “**5060**” is entered, and the **Transport** parameter is set to “**UDP**”. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

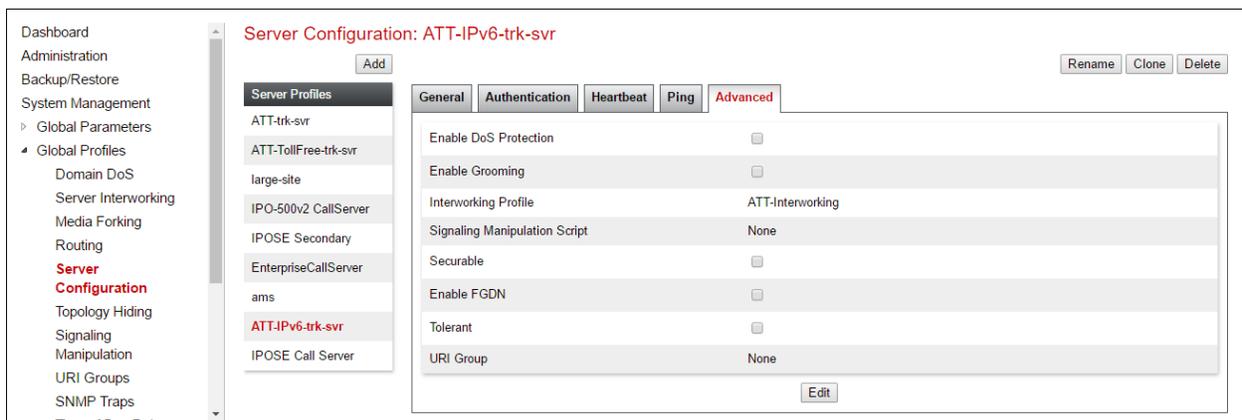


Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeats** tab. The Avaya SBCE can be configured to source “heartbeats” in the form of SIP OPTIONS towards AT&T. This configuration is optional. Independent of whether the Avaya SBCE is configured to source SIP OPTIONS towards AT&T, AT&T will receive OPTIONS from the IP Office site as a result of the **Check OOS** parameter being enabled on IP Office (see **Section 5.5.3**). When IP Office sends SIP OPTIONS to the inside private IP Address of the Avaya SBCE, the Avaya SBCE will send SIP OPTIONS to AT&T. When AT&T responds, the Avaya SBCE will pass the response to IP Office.

Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If adding a new profile, click **Next** to continuing to the **Advanced** settings.



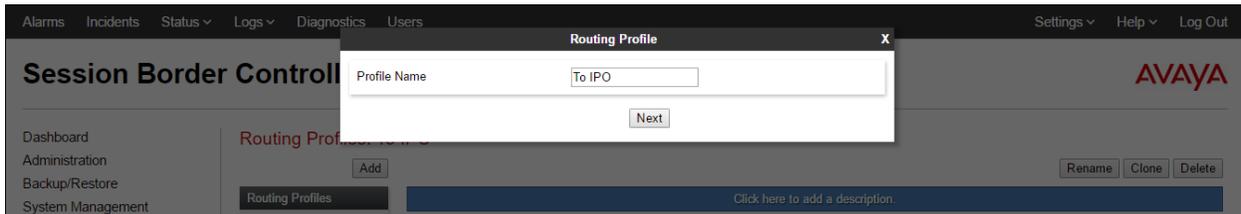
On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and is left unchecked. The **Interworking Profile** is set to “**ATT-Interworking**” created in **Section 7.4.2** for AT&T.



7.7. Routing Profile

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

Create a Routing Profile for IP Office and AT&T IPFR-EF service. To add a routing profile, navigate to **Global Profiles** → **Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.



The following screen shows the Routing Profile “**To IPO**” created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to “**1**”, and the IP Office **Server Configuration**, created in **Section 7.6.1**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with one of the values from the IP Office Server Configuration, and **Transport** becomes greyed out. Select the **TLS** entry from the drop-down menu for the **Next Hop Address**, and select **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IPOSE Call Server	10.64.19.170:5061 (TLS)	None

Similarly add a Routing Profile to AT&T. The following screen shows the Routing Profile “**To ATT IPv6**” created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to “**1**”, and the **AT&T Server Configuration**, created in **Section 7.6.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the Server Configuration, and **Transport** becomes greyed out. Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ATT-IPv6-trk-svr	[3ffe:ffff:aa:aa:10:10:172:80]:5060 (UDP)	None

7.8. Topology Hiding Profile

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the sample configuration, the “**default**” profile was cloned for AT&T, and cloned and modified for IP Office and will later be applied to the Server Flows in **Section 7.16**.

In the **Replace Action** column an action of **Auto** will replace the header field with the IP address of the Avaya SBCE interface and the **Overwrite** will use the value in the **Overwrite Value**.

In the example shown, “**SIP-Trunk-Topology**” was cloned from the default.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
PPM Services

Topology Hiding Profiles: SIP-Trunk-Topology

Topology Hiding Profiles: default, cisco_th_profile, Enterprise-Topology, **SIP-Trunk-Topology**

Click here to add a description.

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

The “**IPOSE-Topology**” was cloned from the default profile and modified to include the customer SIP domain as shown. This customer SIP domain matches the IP Office SIP Domain Name shown in **Section 5.3.1**.

Session Border Controller for Enterprise AVAYA

Global Parameters
Global Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
Reverse Proxy Policy
RADIUS
PPM Services
Domain Policies

Topology Hiding Profiles: IPOSE-Topology

Topology Hiding Profiles: default, cisco_th_profile, Enterprise-Topology, SIP-Trunk-Topology, **IPOSE-Topology**

Click here to add a description.

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

7.9. Application Rule

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

Select **Domain Policies** → **Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing application rule to edit. In the sample configuration, the “**sip-trunk**” rule was created for IP Office and AT&T. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** and **Video** applications to a value slightly larger than the licensed sessions. For example, if licensed for 150 session set the

values to “200”. The **Maximum Session Per Endpoint** should match the **Maximum Concurrent Sessions**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, and Domain Policies. Under Domain Policies, 'Application Rules' is selected. The main content area is titled 'Application Rules: sip-trunk' and includes an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. A table lists application rules with columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The 'sip-trunk' rule is highlighted, showing Audio and Video types with 200 sessions each. A 'Miscellaneous' section below the table shows 'CDR Support' set to Off and 'RTCP Keep-Alive' set to No. An 'Edit' button is at the bottom right of the configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	200
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	200

7.10. Media Rule

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

Select **Domain Policies** → **Media Rules** from the left-side menu as shown below. In the sample configuration, the default media rule **avaya-low-med-enc** was cloned for IP Office, “**enterprise med rule**”, and modified as shown below. With the **avaya-low-med-enc** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

In the sample configuration, media rule **Enterprise-med-rule** was used for IP Office as shown below.

The screenshot displays the configuration page for the 'enterprise med rule' in the Avaya Session Border Controller. The left sidebar shows a navigation menu with 'Media Rules' highlighted. The main content area shows the configuration for this rule, including tabs for Encryption, Codec Prioritization, Advanced, and QoS. The Encryption section is active, showing settings for Audio and Video Encryption, such as Preferred Formats (SRTP_AES_CM_128_HMAC_SHA1_80) and Encrypted RTCP (unchecked). The QoS section is also visible, showing Capability Negotiation (checked).

Similarly, the default media rule **default-low-med** was cloned for AT&T IPFR-EF, “**ATT-med-rule**”. The AT&T Media Rule is shown below with the DSCP values **EF** for expedited forwarding (default value) for **Media QoS**.

The screenshot displays the configuration page for the 'ATT-med-rule' in the Avaya Session Border Controller. The left sidebar shows a navigation menu with 'Media Rules' highlighted. The main content area shows the configuration for this rule, including tabs for Encryption, Codec Prioritization, Advanced, and QoS. The QoS section is active, showing settings for Media QoS Marking (Enabled), Audio QoS (Audio DSCP: EF), and Video QoS (Video DSCP: EF).

7.11. Signaling Rule

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

Clone and modify the **default** signaling rule to add the proper quality of service to the SIP signaling. To clone a signaling rule, navigate to **Domain Policies** → **Signaling Rules**. With the **default** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown). In the sample configuration, signaling rule “**enterprise sig rule**” is unchanged from the default rule.

The screenshot shows the configuration page for the 'enterprise sig rule' under 'Signaling Rules'. The left sidebar shows the navigation menu with 'Signaling Rules' selected. The main content area has tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'General' tab is active, showing 'Inbound' and 'Outbound' sections with 'Requests' set to 'Allow'. The 'Content-Type Policy' section has 'Enable Content-Type Checks' checked and 'Action' set to 'Allow'.

Signaling rule **ATT-sig-rule** was also cloned from the default rule and used for AT&T. The DSCP value **AF41** for assured forwarding (default value) was set for **Signaling QoS**.

The screenshot shows the configuration page for the 'att sig rule' under 'Signaling Rules'. The left sidebar shows the navigation menu with 'Signaling Rules' selected. The main content area has tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'Signaling QoS' tab is active, showing 'Signaling QoS' checked, 'QoS Type' set to 'DSCP', and 'DSCP' set to 'AF41'.

7.12. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.16**.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** as shown below. The following screen shows the “**enterprise policy**” created for IP Office. The details of the non-default rules chosen are shown in previous sections.

Policy Groups: enterprise policy

Policy Groups

Order	Application	Border	Media	Security	Signaling
1	sip-trunk	default	default-low-med	default-low	enterprise sig rule

The following screen shows the “**att-policy-group**” created for AT&T. The details of the non-default rules chosen are shown in previous sections.

Policy Groups: att-policy-group

Policy Groups

Order	Application	Border	Media	Security	Signaling
1	sip-trunk	default	att med rule	default-low	att sig rule

7.13. Advanced Options

In **Section 7.14**, the media UDP port ranges required by AT&T are configured (**16384 – 32767**). However, by default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE so the range required by AT&T can be defined in **Section 7.14**.

Step 1 - Select **Device Specific Settings** → **Advanced Options** from the menu on the left-hand side.

Step 2 - Select the **Port Ranges** tab.

Step 3 - In the **Signaling Port Range** row, change the range to **12000 – 16380**

Step 4 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.

Step 5 – In the **Listen Port Range** row, change the range to **6000 – 6999**.

Step 6 – In the **HTTP Port Range** row, change the range to **51001 – 62000**.

Step 7 - Select **Save**. Note that changes to these values require an application restart (see **Section 7.1**).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Device Specific Settings', with 'Advanced Options' selected. The main content area is titled 'Advanced Options: SBCE' and features several tabs: 'CDR Listing', 'Feature Control', 'SIP Options', 'Network Options', 'Port Ranges' (which is active), 'RTCP Monitoring', and 'Load Monitoring'. A warning banner at the top of the configuration area states: 'Changes to the settings below require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, the 'Port Range Configuration' section contains four rows, each with a label and two input fields for a range:

Configuration Item	Start Range	End Range
Signaling Port Range	12000	16380
Config Proxy Internal Signaling Port Range	42000	51000
Listen Port Range	6000	6999
HTTP Port Range	51001	62000

A 'Save' button is located at the bottom right of the configuration area.

7.14. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP media interface for the inside and outside IP interfaces.

To create a new Media Interface, navigate to **Device Specific Settings** → **Media Interface** and click **Add**. The following screen shows the media interfaces defined for the sample configuration.

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

Name	Media IP Network	Port Range		
Outside-B2-Media	10.64.91.40 Outside-B2 (B2, VLAN 0)	16384 - 32767	Edit	Delete
Inside-Media-Interface	10.64.91.40 Inside-A1 (A1, VLAN 0)	16384 - 32767	Edit	Delete
Outside-Media-IPv6	3ffe:ffff:bb:bb::240 Outside-B1-IPv6 (B1, VLAN 0)	16384 - 32767	Edit	Delete

7.15. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a signaling interface for the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **Device Specific Settings** → **Signaling Interface** and click **Add**. The following screen shows the signaling interfaces defined for the sample configuration.

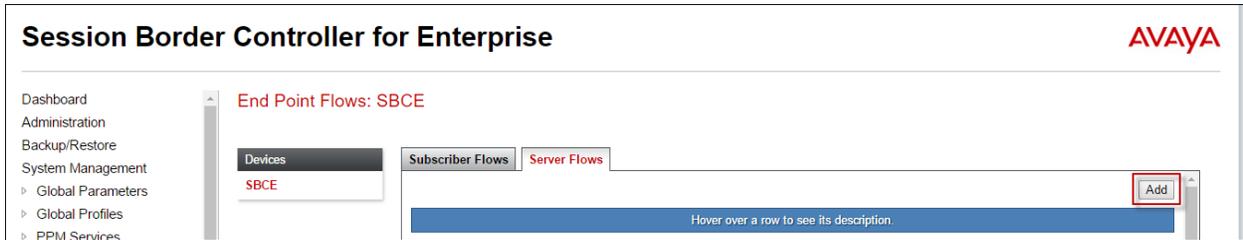
Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
Inside-Signaling-Interface	10.64.91.40 Inside-A1 (A1, VLAN 0)	---	---	5061	sbce40-server	Edit	Delete
Outside-B2-Signaling	10.64.91.40 Outside-B2 (B2, VLAN 0)	---	5060	---	None	Edit	Delete
Outside-Signaling-IPv6	3ffe:ffff:bb:bb::240 Outside-B1-IPv6 (B1, VLAN 0)	---	5060	---	None	Edit	Delete

7.16. End Point Flows - Server Flow

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

Create a Server Flow for IP Office and AT&T IPFR-EF service. To create a Server Flow, navigate to **Device Specific Settings** → **End Point Flows**. Select the **Server Flows** tab and click **Add** as highlighted below.



The following screen shows the flow named “**IPO Flow IPv6**” viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections. It also includes the **Signaling Manipulation Script** “**ATT IPv6 with IPO**” created in **Section 7.5**.

Criteria		Profile	
Flow Name	IPO Flow IPv6	Signaling Interface	Inside-Sig-40
Server Configuration	IPOSE Call Server	Media Interface	Inside-Media-Interface
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	enterprise policy
Remote Subnet	*	Routing Profile	To ATT IPv6
Received Interface	Outside-Signaling-IPv6	Topology Hiding Profile	IPOSE-Topology
		Signaling Manipulation Script	ATT IPv6 with IPO
		Remote Branch Office	Any

Once again, select the **Server Flows** tab and click **Add**. The following screen shows the flow named “**ATT-IPv6 Flow**” viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.

Criteria		Profile	
Flow Name	ATT-IPv6 Flow	Signaling Interface	Outside-Signaling-IPv6
Server Configuration	ATT-IPv6-trk-svr	Media Interface	Outside-Media-IPv6
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	att-policy-group
Remote Subnet	*	Routing Profile	To IPO
Received Interface	Inside-Sig-40	Topology Hiding Profile	SIP-Trunk-Topology
		Signaling Manipulation Script	None
		Remote Branch Office	Any

8. AT&T IP Flexible Reach – Enhanced Features Configuration

AT&T provides the IPFR-EF service border element IP address, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition, the AT&T IPFR-EF features, and their associated access numbers, are also assigned by AT&T.

9. Verification Steps

This section provides example verifications of the Avaya configuration with AT&T IPFR-EF service.

9.1. Avaya SBCE

This section provides verification steps that may be performed with the Avaya SBCE.

9.1.1. Incidents

The Incident Viewer can be accessed from the Avaya SBCE Dashboard as highlighted in the screen shot below.



Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.

Incident Viewer AVAYA

Device: All Category: All

Displaying results 1 to 15 out of 2000.

Type	ID	Date	Time	Category	Device	Cause
Server Heartbeat	732486352784939	6/3/16	10:51 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	732486352784497	6/3/16	10:51 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	732486352752785	6/3/16	10:51 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	732486352752361	6/3/16	10:51 AM	Policy	SBC1	Heartbeat Successful, Server is UP

9.1.2. Server Status

The **Server Status** can be accessed from the Avaya SBCE Dashboard by selecting the **Status** menu, and then **Server Status**.



9.1.3. Tracing

To take a call trace, navigate to **Device Specific Settings** → **Troubleshooting** → **Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.

Session Border Controller for Enterprise AVAYA

Trace: SBCE

Devices: SBCE

Packet Capture Configuration

Status: Ready

Interface: B2

Local Address (IP:Port): All

Remote Address: *

Protocol: UDP

Maximum Number of Packets to Capture: 10000

Capture Filename: protocol-trace-att.pcap

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The 'Trace: SBCE' page is active, with the 'Captures' tab selected. A blue banner at the top of the configuration area states: "A packet capture is currently in progress. This page will automatically refresh until the capture completes." Below this is the "Packet Capture Configuration" section with the following fields: Status (In Progress), Interface (B2), Local Address (All), Remote Address (*), Protocol (UDP), Maximum Number of Packets to Capture (10000), and Capture Filename (protocol-trace-att.pcap). A "Stop Capture" button is located at the bottom right of the configuration area.

Select the **Captures** tab to view the files created during the packet capture.

The screenshot shows the same Avaya Session Border Controller for Enterprise web interface, but now the "Captures" tab is selected. A "Refresh" button is visible in the top right corner of the captures area. Below it is a table listing the captured files:

File Name	File Size (bytes)	Last Modified	
protocol-trace-att_20161202095602.pcap	45,056	December 2, 2016 9:56:36 AM MST	Delete

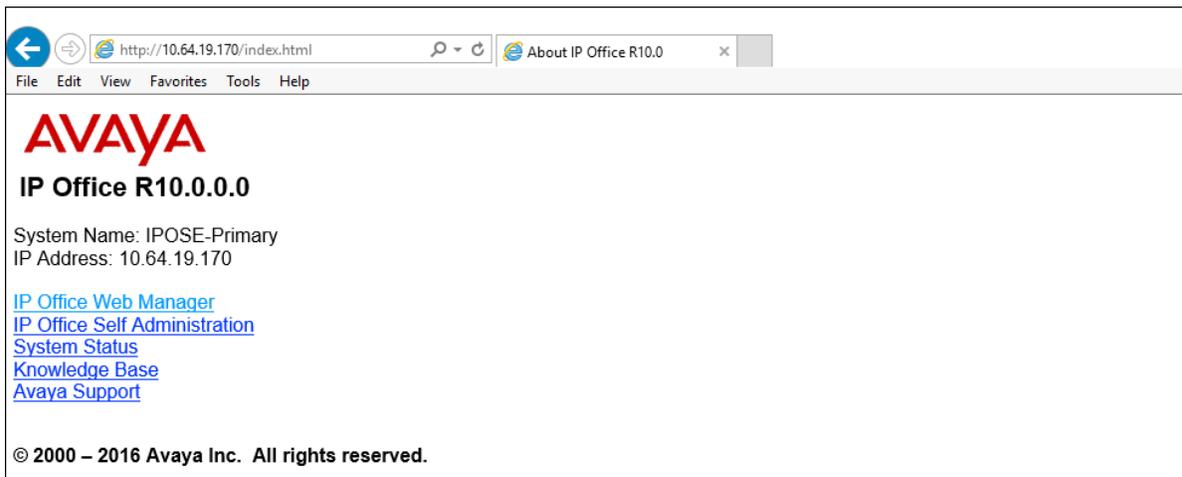
The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like Wireshark.

9.2. IP Office

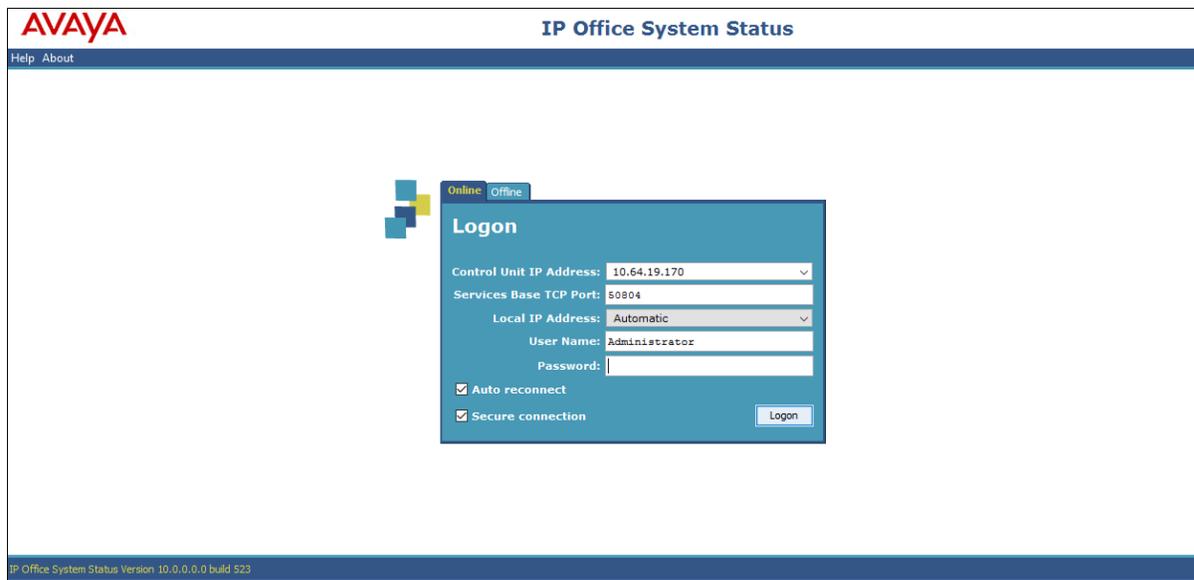
This section provides verification steps that may be performed with the IP Office.

9.2.1. System Status

The System Status application is used to monitor and troubleshoot IP Office. Use the System Status application to verify the state of the SIP trunk. System Status can be accessed from **Start → Programs → IP Office → System Status** or by opening an Internet browser and type the URL: `http://ipaddress` where *ipaddress* is the IP address of the Avaya IP Office LAN1 interface. Click on **System Status** to launch the application.



The following screen shows an example **Logon** screen. Enter the IP Office IP address in the **Control Unit IP Address** field, and enter an appropriate **User Name** and **Password**. Click **Logon**.



Select the SIP line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** is *Idle* for each channel.

The screenshot shows the AVAYA IP Office System Status interface. The left pane shows a tree view with 'Trunks (7)' expanded to 'Line: 4'. The main pane is on the 'Status' tab, displaying the 'SIP Trunk Summary' for Line 4. The summary includes fields for Line Service State (In Service), Peer Domain Name (10.64.91.40), Resolved Address (10.64.91.40), Line Number (4), Number of Administered Channels (20), Number of Channels in Use (0), Administered Compression (G729 A, G711 Mu), Enable Faststart (Off), Silence Suppression (Off), Media Stream (RTP), Layer 4 Protocol (UDP), SIP Trunk Channel Licenses (50), and SIP Trunk Channel Licenses in Use (0). A green progress indicator shows 0%. Below the summary is a table of channels:

Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media A...	Co...	Conne...	Caller ID or Dial...	Other Party on Call	Direction of Call	Round Trip D...	Receive Jitter	Receive Packe...	Transmit Jitter	Transmit Packe...
1			Idle	00:04:40											
2			Idle	20:00:57											
3			Idle	20:00:57											
4			Idle	20:00:57											
5			Idle	20:00:57											

At the bottom of the interface, there are buttons for Trace, Trace All, Pause, Ping, Call Details, Graceful Shutdown, Force Out of Service, Print..., and Save As... The status bar shows 10:00:59 AM and Online.

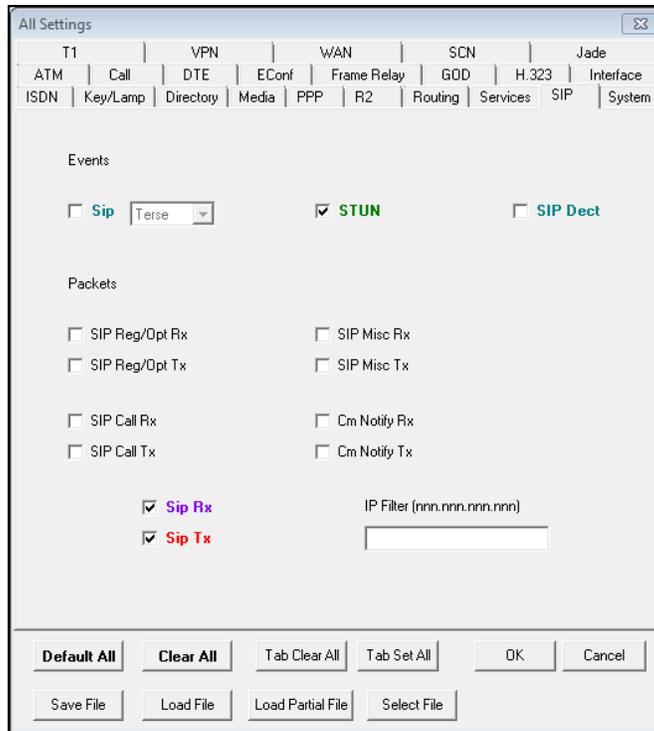
Select the **Alarms** tab and verify that no alarms are active on the SIP line.

The screenshot shows the AVAYA IP Office System Status interface with the 'Alarms' tab selected. The title is 'Alarms for Line: 4 SIP 10.64.91.40'. The main pane shows a table with columns for Last Date Of Error, Occurrences, and Error Description. The table is currently empty, indicating no active alarms.

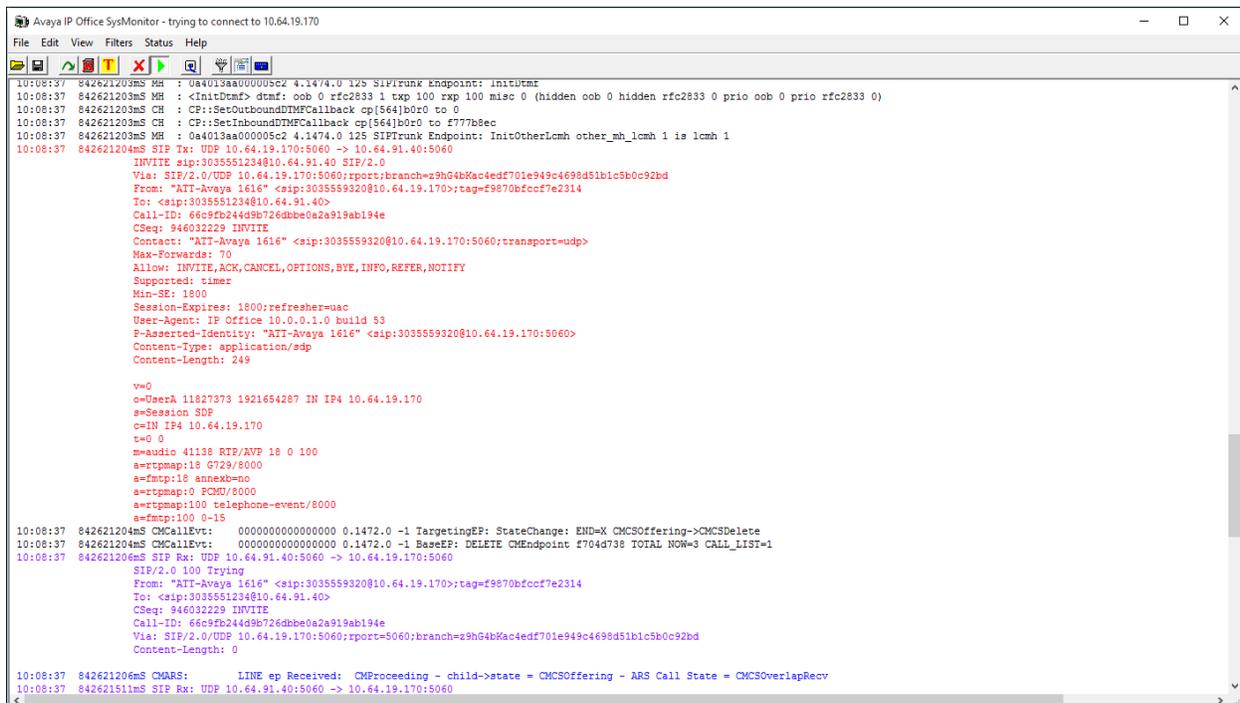
9.2.2. Monitor

The Monitor application can also be used to monitor and troubleshoot IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select **Filters → Trace Options**.

The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, the **SIP Rx** and **SIP Tx** boxes are checked. All SIP messages will appear in the trace with the color blue. To customize the color, right-click on **SIP Rx** or **SIP Tx** and select the desired color.



As an example, the following shows a portion of the monitoring window for an outbound call from extension 6320, whose DID is 303-555-9320, calling out to the PSTN via the AT&T IPFR-EF service. The telephone user dialed 9-303-555-1234.



10. Conclusion

As illustrated in these Application Notes, Avaya IP Office R10.1 and the Avaya Session Border Controller for Enterprise 7.2 can be configured to interoperate successfully with the AT&T IP Flexible Reach - Enhanced Features service using IPv6 and **AVPN** or **MIS/PNT** transport connections, within the limitations described in **Section 2.2**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

11. Additional References

This section references documentation relevant to these Application Notes. In general, Avaya product documentation is available at <http://support.avaya.com>

- [1] *IP Office™ Platform 10.1, Deploying Avaya IP Office Servers as Virtual Machines*, Document Number 15-601011, Issue 05g, July 2017
- [2] *Administering Avaya IP Office™ Platform with Manager*, Release 10.1, June 2017
- [3] *IP Office™ Platform 10.1, Deploying Avaya IP Office™ Platform IP500 V2*, Document Number 15-601042, Issue 32f, July 2017
- [4] *IP Office™ Platform 10.1, Using Avaya IP Office™ System Status*, Document Number 15-601758, Issue 12d, July 2017
- [5] *IP Office™ Platform 10.1, IP Office SIP Phones with ASBCE*, Issue 02b, July 2017
- [6] *Deploying Avaya Session Border Controller in Virtualized Environment*, June 2017
- [7] *Administering Avaya Session Border Controller for Enterprise*, June 2017
- [8] RFC 3261 *SIP: Session Initiation Protocol* <http://www.ietf.org/rfc/rfc3261.txt>

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

©2017 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.