Avaya Solution & Interoperability Test Lab

Application Notes for Avaya IP Office Release 9.0 and Avaya Session Border Controller for Enterprise 6.2 with AT&T IP Flexible Reach - Enhanced Features – Issue 1.1

Abstract

These Application Notes describe the steps for configuring Avaya IP Office R9.0 and the Avaya Session Border Controller for Enterprise 6.2, with the AT&T IP Flexible Reach - Enhanced Features service using AVPN or MIS/PNT transport connections.

The Avaya Session Border Controller for Enterprise 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 for interoperability.

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.

AT&T is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

©2014 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 5
2. General Test Approach and Test Results 5
   2.1. Interoperability Compliance Testing 6
   2.2. Test Results 7
      2.2.1. Known Limitations 7
   2.3. Support 9
      2.3.1. Avaya 9
      2.3.2. AT&T 9
3. Reference Configuration 9
   3.1. Illustrative Configuration Information 11
   3.2. Call Flows 12
      3.2.1. Inbound 12
      3.2.2. Outbound 12
      3.2.3. Call Forward 13
      3.2.4. Coverage to Voicemail 14
4. Equipment and Software Validated 15
5. Avaya IP Office Configuration 16
   5.1. Platform Information 16
   5.2. Licensing 17
   5.3. System Settings 18
      5.3.1. System Tab 18
      5.3.2. LAN 1 Settings 18
      5.3.3. LAN 2 Settings 21
      5.3.4. Voicemail 21
      5.3.5. System Telephony Configuration 22
      5.3.6. System Twinning Configuration 23
      5.3.7. System Codecs Configuration 23
   5.4. SIP Line 24
      5.4.1. SIP Line from Template 25
      5.4.2. SIP Line – SIP Line tab 27
      5.4.3. SIP Line - Transport tab 28
      5.4.4. SIP Line - SIP URI tab 28
      5.4.5. SIP Line - VoIP tab 30
      5.4.6. SIP Line - T38 Fax 31
   5.5. Users, Extensions, and Hunt Groups 32
      5.5.1. Analog User Extn207 32
      5.5.2. IP Phone User Extn500 34
      5.5.3. SIP Telephone Users (Avaya 1120E and Avaya IP Office SoftPhone) 38
      5.5.4. Hunt Groups 43
   5.6. Short Codes 45
      5.6.1. Short Code Direct Dialing (no ARS access) 45
      5.6.2. Short Code Dialing via Automatic Route Selection (ARS access) 46
      5.6.3. Privacy Dialing 46
      5.6.4. Feature Dialing 47
   5.7. Incoming Call Routes 49

©2014 Avaya Inc. All Rights Reserved.

5.8. Automatic Route Selection (ARS) and Alternate Routing 50
5.9. Auto Attendant (via Avaya IP Office Voicemail Pro) 52
5.10. Privacy / Anonymous Calls 55
5.11. SIP Options Frequency 55
5.12. Saving Configuration Changes to Avaya IP Office 56
6. Configure Avaya Session Border Controller for Enterprise 57
6.1. Initial Installation/Provisioning 57
6.2. Log into the Avaya SBCE 57
6.3. Global Profiles 58
6.3.1. Server Interworking – to Avaya IP Office 58
6.3.2. Server Interworking – to AT&T 60
6.3.3. Routing – to Avaya IP Office 60
6.3.4. Routing – to AT&T 61
6.3.5. Server Configuration – Avaya IP Office 62
6.3.6. Server Configuration – AT&T 63
6.3.7. Topology Hiding – Avaya IP Office 64
6.3.8. Topology Hiding – AT&T 65
6.3.9. Signaling Manipulation 66
6.4. Domain Policies 66
6.4.1. Application Rules 66
6.4.2. Media Rules 68
6.4.3. Signaling Rules 69
6.4.4. Endpoint Policy Groups – Avaya IP Office 71
6.4.5. Endpoint Policy Groups – AT&T 71
6.5. Device Specific Settings 72
6.5.1. Network Management 72
6.5.2. Advanced Options 72
6.5.3. Media Interfaces 73
6.5.4. Signaling Interface 74
6.5.5. Endpoint Flows – Avaya IP Office 74
6.5.6. Endpoint Flows – AT&T 75
7. AT&T IPFR-EF Configuration 76
8. Verification Steps 76
8.1. AT&T IP Flexible Reach – Enhanced Features 76
8.2. Avaya IP Office 9.0 77
8.2.1. System Status Application 77
8.2.2. System Monitor Application 79
8.3. Avaya Session Border Controller for Enterprise 6.2 81
8.3.1. System Information 81
8.3.2. Avaya SBCE Protocol Traces 81
8.4. Protocol Trace Examples 83
9. Conclusion 84
10. References 85
11. Addendum 1 – Redundancy to Multiple AT&T Border Elements 86
12. Addendum 2 – Remote Worker Configuration via the Avaya SBCE 90
12.1. Provisioning the Avaya Session Border Controller for Enterprise 91

©2014 Avaya Inc. All Rights Reserved.

12.1.1. Network Management 91
12.1.2. Server Configuration – Avaya IP Office 92
12.1.3. Media Interface 93
12.1.4. Signaling Interface 93
12.1.5. Routing Profile 94
12.1.6. User Agents 95
12.1.7. Application Rules 96
12.1.8. Media Rules 96
12.1.9. End Point Policy Groups 98
12.1.10. End Point Flows 99
12.2. Remote Worker Endpoint Configuration on Avaya IP Office 102
12.2.1. Extension Configuration 102
12.2.2. User Configuration 102
12.2.3. Incoming Call Route 104
12.3. Remote Worker Avaya Flare® Experience for Windows Configuration 104
12.3.1. Settings - Server Screen 104
12.3.2. Settings - Video Screen 105

©2014 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps for configuring Avaya IP Office R9.0 (Avaya IP Office) and the Avaya Session Border Controller for Enterprise 6.2, (Avaya SBCE), with the AT&T IP Flexible Reach - Enhanced Features service using **AVPN** or **MIS/PNT** transport connections.

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 for interoperability.

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 AVPN[1] or MIS/PNT[2] transport services.

Note – The solution described in these application notes also applies to the AT&T Business in a Box service.

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

2. General Test Approach and Test Results

The test environment (see **Figure 1**) consists of:

- A simulated enterprise with Avaya IP Office, Avaya IP Office telephones and fax machines (Ventafax application), and the Avaya SBCE.
- Production IPFR-EF service, to which the simulated enterprise was connected via AVPN transport.

The test objectives were to verify the features and functionality described in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect

[1] AVPN uses compressed RTP (cRTP).
[2].MIS/PNT does not support cRTP.

©2014 Avaya Inc. All Rights Reserved.

Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 3.2**) between Avaya IP Office, the Avaya SBCE, and the IPFR-EF service.

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 AT&T network. Calls were made to/from PSTN across the IPFR-EF service network.

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

- Incoming and outgoing calls between PSTN, routed by the IPFR-EF service, and the Avaya SBCE, to Avaya IP Office. These calls are via the Avaya IP Office SIP Line and may be generated/answered by Avaya SIP telephones/Softphones, H.323 telephones, Analog telephones, Analog fax machines directly or via Hunt Groups. Coverage to Avaya IP Office Voicemail Pro, and Voicemail Pro auto-attendant applications may also be used.
- Inbound / Outbound fax using T38 or G.711.
- Proper disconnect when the caller abandoned a call before answer for both inbound and outbound calls, and when the Avaya IP Office party or the PSTN party terminated an active call.
- Proper busy tone heard when an Avaya IP Office user called a busy PSTN user, or a PSTN user called a busy Avaya IP Office user (i.e., if no redirection was configured for user busy conditions).
- Various outbound PSTN call types were tested including 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 monitoring of 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.
- Long duration calls.
- Remote Worker configuration using Avaya Flare® Experience for Windows as the remote SIP device.
- DTMF transmission (RFC 2833) for successful voice mail navigation, including navigation of a simple auto-attendant application configured on Avaya IP Office Voicemail Pro.
    - See **Section 2.2.1**, **Items 2, 4** and **5** regarding DTMF issues observed during testing.
- Telephony features such as call waiting, hold, transfer, and conference.

©2014 Avaya Inc. All Rights Reserved.

- 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.
- AT&T IPFR-EF service features such as:
    - Simultaneous Ring
    - Sequential Ring
    - Call Forward – Always
    - Call Forward – Busy
    - Call Forward – Ring No Answer

2.2. Test Results

Interoperability testing of the sample configuration and features described in **Section 2.1** were completed successfully. The following observations were noted during testing.

2.2.1. Known Limitations

1. **Avaya IP Office Softphone did not generate RFC2833 DTMF when attempting to navigate menus with an Auto Attendant system utilizing SIP 183 Session Progress signaling -** Some Auto Attendant systems send 183 Session Progress in response to an inbound call, and do not send 200 OK until a menu selection has been made. In these cases, Avaya IP Office Softphone did not generate DTMF SIP Telephone Events when menu selection was attempted (even though appropriate SIP Telephone Event SDP signaling was sent in the initial Avaya IP Office Invite and received in the network 183).
    - An MR was opened with Avaya IP Office support.
    - This issue does not occur with Avaya IP Office desk phones.
    - It should be noted that if the called Auto Attendant system answers at the onset with 200 OK (prior to a menu selection), then the Avaya IP Office Softphone does generate DTMF Telephone Events during menu selection.

2. **Avaya IP Office only supports a packet size of 20 msecs, and therefore does not specify a PTIME value in the SIP SDP (in either requests or responses) -** Network responses include MAXPTIME=20, and network requests include MAXPTIME=30.
    - Although no issues were found during testing, the AT&T IPFR-EF service recommends a value of 30ms when AVPN transport is used.

3. **Avaya IP Office and RFC2833 Telephone Event Type not applied to SIP endpoints –** Avaya IP Office R9.0 allows the RFC2833 Telephone Event Type to be specified (*System/Codecs* tab, see **Section 5.3.7**). While this parameter does apply successfully to native and H.323 endpoints, it is not applied to SIP endpoints.
    - An 1120E SIP telephone used Telephone Event Type 101
    - Avaya Flare® Experience for Windows SIP endpoint used Telephone Event Type 120.
    - No issues were found during testing as a result of this behavior.

©2014 Avaya Inc. All Rights Reserved.

4. **Avaya IP Office Direct Media feature issues -** During testing the following issues were found when the Direct Media option was enabled:
    - Initial audio clipping was observed when Direct Media is established (media stream redirected from the Avaya IP Office hardware to the Avaya IP Office endpoint).
    - It was found that when Direct Media was enabled, Avaya IP Office IP endpoints did not send RTP Events.
    - As a result of these issues, the recommended configuration is to have Direct Media disabled (see **Section 5.4.4**).
    - It should also be noted that only Direct Media *or* T.38 fax is supported on a SIP Line. The use of both features on the same SIP Line is not supported.

5. **Avaya SBCE 6.2 and T.38 fax** – In the reference configuration, Avaya SBCE 6.2 load *Q48* was used for testing. During the testing, load *Q58* was released. While executing regression testing with load Q58, it was found that T.38 fax calls failed. Therefore Avaya SBCE 6.2 load Q58 should not be used, and load Q48 used instead as shown in **Table 2**.

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) reviewed in this customer configuration guide 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 their 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://www.business.att.com/enterprise/Service/voice-services/voip/sip-trunking/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.

©2014 Avaya Inc. All Rights Reserved.

2.3. Support

2.3.1. Avaya

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

2.3.2. AT&T

For more information on the AT&T IP Flexible Reach service visit: http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/. AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

3. Reference Configuration

Note – Documents used to provision the reference configuration are listed in **Section 10**. Specific references to these documents are indicated in the following sections by the notation **reference [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 an IP 500 V2 platform. This solution is extensible to the Avaya IP Office Server Edition platform as well.
- Avaya "desk" telephones are represented with an Avaya 1608 H.323 set, an Avaya 6211 Analog set, an Avaya 1120E SIP set, Avaya IP Office SIP Softphone (in Default Mode), and Avaya Flare for Windows in a Remote Worker configuration. Fax endpoints are represented by PCs running Ventafax software connected by modem to an Avaya IP Office analog port.
- Avaya IP Office Voicemail Pro (running on a Windows 2003 server) provided the voice messaging capabilities in the reference configuration. This solution is extensible to the Avaya IP Office embedded voice mail as well.
- Avaya Session Border Controller for Enterprise running on a CAD-0208 platform. This solution is extensible to other Avaya Session Border Controller for Enterprise platforms as well.
- UDP/5060 is the recommended transport protocol/port to use on the IP Office LAN1 connection. However TCP/5060 may be used if necessary.
- Outbound and Inbound calls utilize telephone or fax User/Extensions provisioned on Avaya IP Office. Signaling is sent between Avaya IP Office and the IPFR-EF service.
- The AT&T IPFR-EF service requires the following SIP trunk network settings to 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.

©2014 Avaya Inc. All Rights Reserved.

The Avaya IP Office 500V2 platform and the Avaya SBCE CAD-0208 platform used in the reference configuration deployed using the following configuration (referred to as an IP Office **"one-wire"** configuration).

- Avaya IP Office LAN1 interface (labeled "LAN") connected to the CPE private network.
- Avaya SBCE A1 interface connected to the CPE private network.
- Avaya SBCE B1 interface connected to the AT&T IP Toll Free service IPFR-EF network router.

Note – In the reference configuration, the IP Office LAN2 interface and the Avaya SBCE M1 interface are both connected to a separate "management" subnet.

Note – The IP Office "one-wire" configuration described in this document is the preferred configuration for the IP Office/Avaya SBCE solution. However an IP Office "two-wire" configuration is also supported.

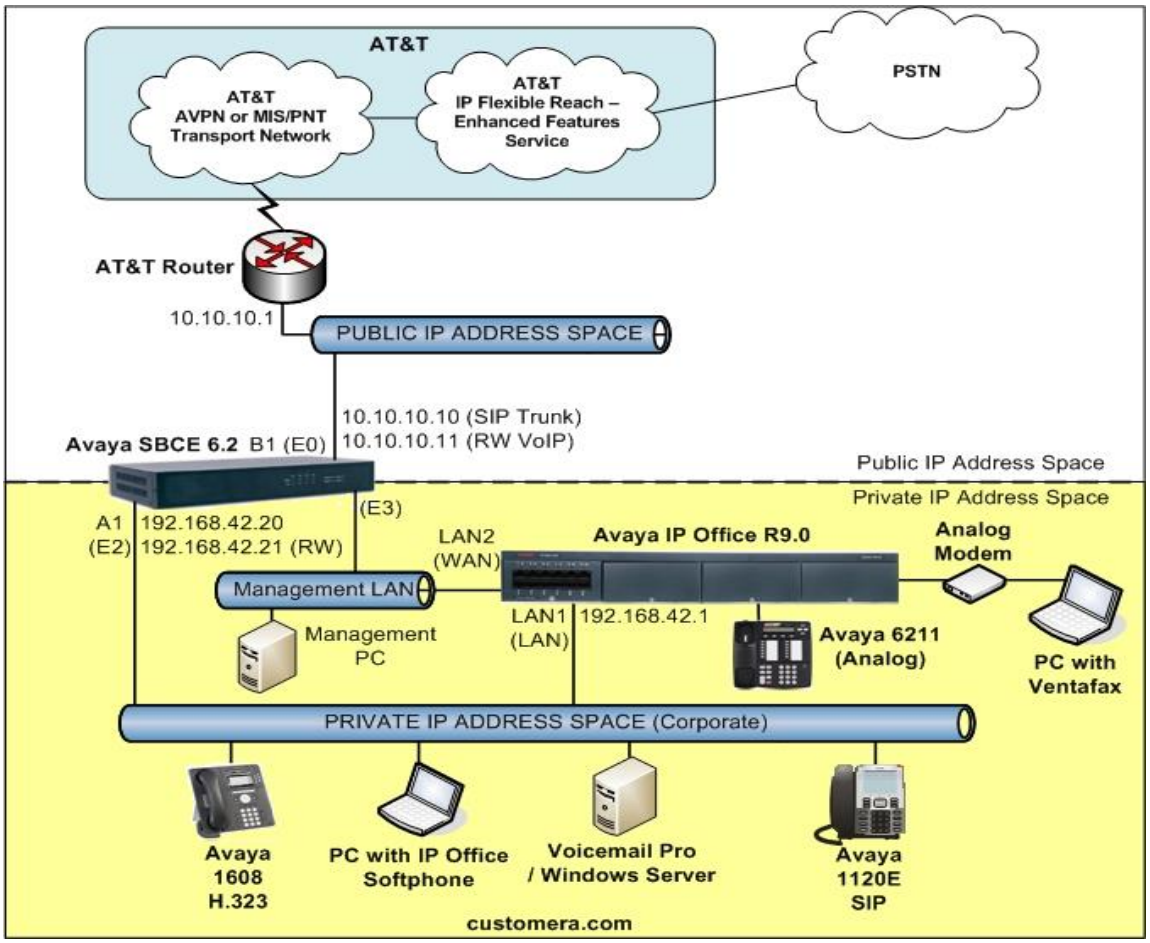


Figure 1: Reference Configuration

©2014 Avaya Inc. All Rights Reserved.

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent Sections are used in the reference configuration described in these Application Notes, and are for illustrative purposes only. Customers must obtain and use the values based on their own specific configurations.

Note - The AT&T IPFR-EF IP addressing shown in this document is an example. AT&T Customer Care will provide the actual IP addressing as part of the IPFR-EF provisioning process.

Component	Illustrative Value in these Application Notes
Avaya IP Office 500 V2 Platform	
Private network LAN1 interface, (labeled "LAN" on the chassis)	192.168.42.1
LAN2 interface, (labeled "WAN" on the chassis), for management access.	192.168.1.22
Avaya SBCE CAD-0208 Platform	
Private network SIP Trunk IP Address (A1 interface).	192.168.42.20
Private network Remote Worker IP Address (A1 interface).	192.168.42.21
Public IP SIP Trunk IP Address (B1 interface).	10.10.10.10[3]
Public IP Remote Worker IP Address (B1 interface).	10.10.10.11
Management IP address ("M1").	192.168.1.20
AT&T IPFR-EF Service	
Border Element IP Address	10.10.10.1

Table 1: Illustrative Values Used in these Application Notes

[3] The actual public addressing is not included for security purposes. The subnet 10.10.10.x is used in this document to represent the public addressing.

©2014 Avaya Inc. All Rights Reserved.

3.2. 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.

3.2.1. 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

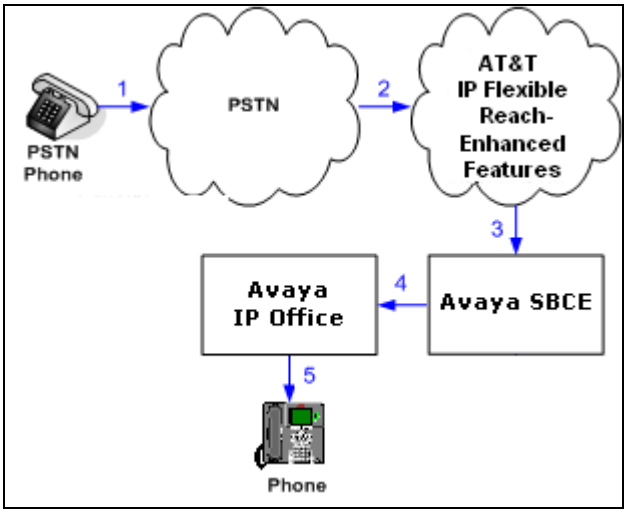


Figure 2: Inbound AT&T IPFR-EF Call

3.2.2. 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.

©2014 Avaya Inc. All Rights Reserved.

4. The AT&T IPFR-EF service delivers the call to PSTN.
5. PSTN delivers the call to a phone or fax endpoint.

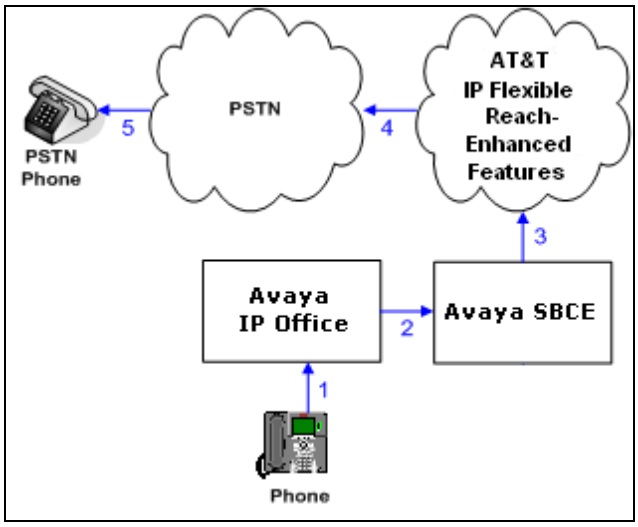


Figure 3: Outbound Call to AT&T IPFR-EF

3.2.3. Call Forward[4]

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 immediately 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 5.4.1**).

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.

[4] Note that when the redirection is completed, RTP will still flow through the Avaya SBCE and Avaya IP Office.

©2014 Avaya Inc. All Rights Reserved.

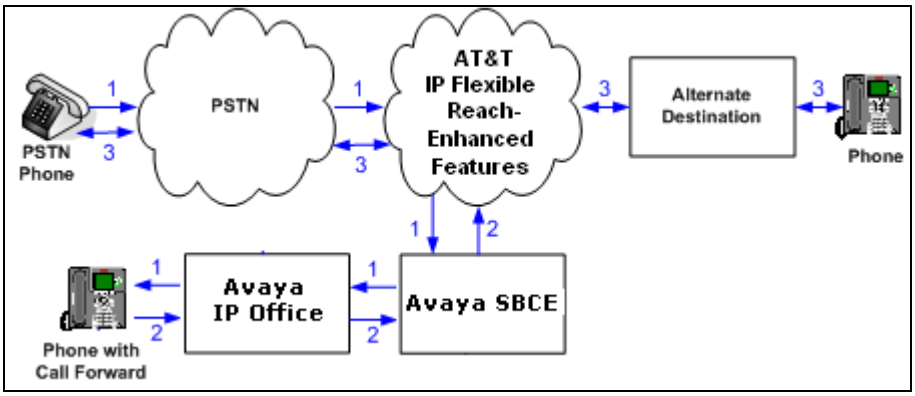


Figure 4: Re-directed (e.g. Call Forward) AT&T IPFR-EF Call

3.2.4. 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 Avaya IP Office Voicemail Pro, running on a Windows 2003 server.

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 the external application Avaya IP Office Voicemail Pro.

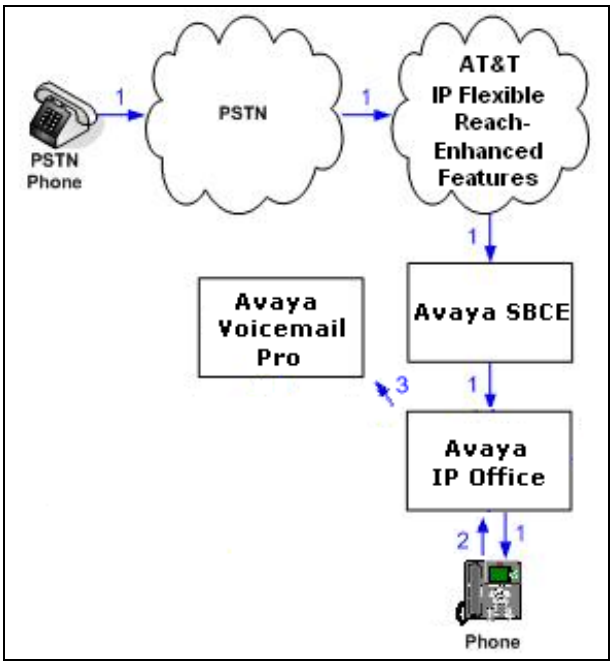


Figure 5: Coverage to Voicemail (Voicemail Pro)

©2014 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

The following equipment and software was used for the reference configuration described in these Application Notes.

Equipment/Software	Release/Version
Avaya IP Office 500 V2	R9.0 (829)
Avaya 1608 (H.323) Telephone	Ha1608ua1_330D.bin
Avaya 1120E (SIP) Telephone	04.03.18.00
Avaya IP Office Softphone (SIP)	3.2.3.20
Avaya Flare® Experience for Windows	1.1.4.23
Avaya 6211 Analog Telephone	-
Avaya Session Border Controller for Enterprise	6.2.0 Q48 (see **Section 2.2.1**)
Fax device	Ventafax 6.3

Table 2: Equipment and Software Versions

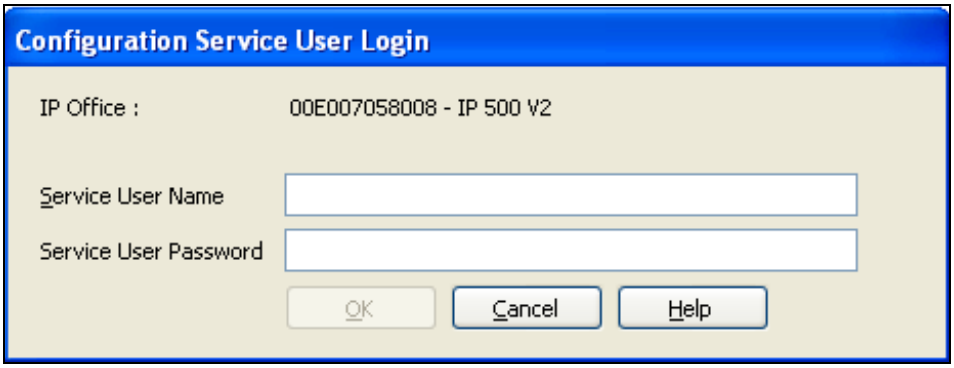
Note - Testing was performed with IP Office 500 v2 R9.0, but it also applies to IP Office Server Edition R9.0. Note that IP Office Server Edition requires an Expansion IP Office 500 v2 R9.0 to support analog or digital endpoints or trunks. IP Office Server Edition does not support TAPI Wave or Group Voicemail.

©2014 Avaya Inc. All Rights Reserved.

5. Avaya IP Office Configuration

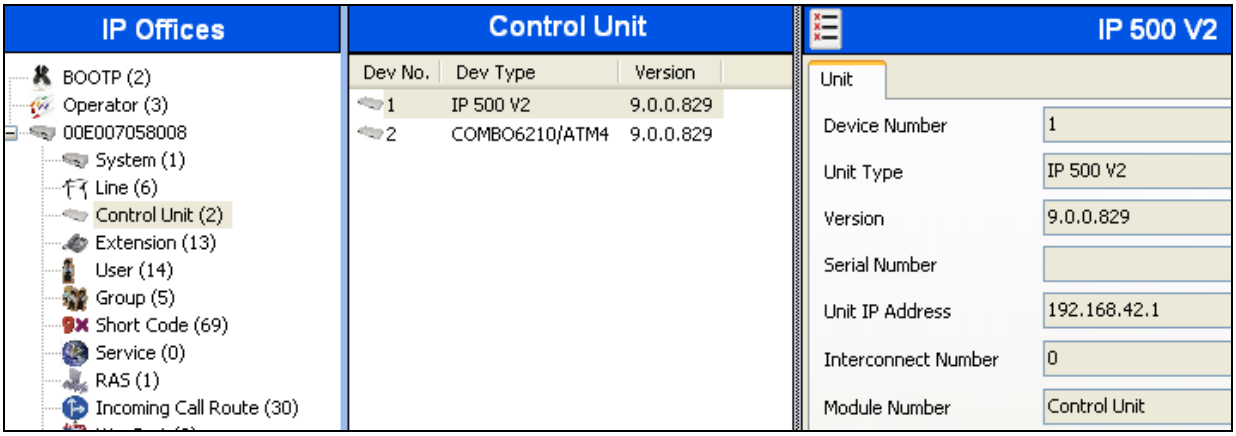
Note - This section describes attributes of the reference configuration, but is not meant to be prescriptive. In the following sections, only the parameters that are highlighted in **bold** text are applicable to this document. Other parameter values may or may not match based on local configurations. Additionally, the screen shots referenced in these sections may not be complete at times. For more information on installing Avaya IP Office consult reference **[1]**.

Avaya IP Office is configured via the Avaya IP Office Manager program. For more information on Avaya IP Office Manager, consult reference **[2]**. From the Avaya IP Office Manager PC, select **Start →Programs →Avaya IP Office →Manager** to launch the Manager application. Enter the appropriate credentials.



5.1. Platform Information

This section describes attributes of the reference configuration. The following screen shows the Avaya IP Office module configuration used in the reference configuration. In the screen below, the **IP 500 V2** platform is displayed along with the COMBO6210/ATM4 module.



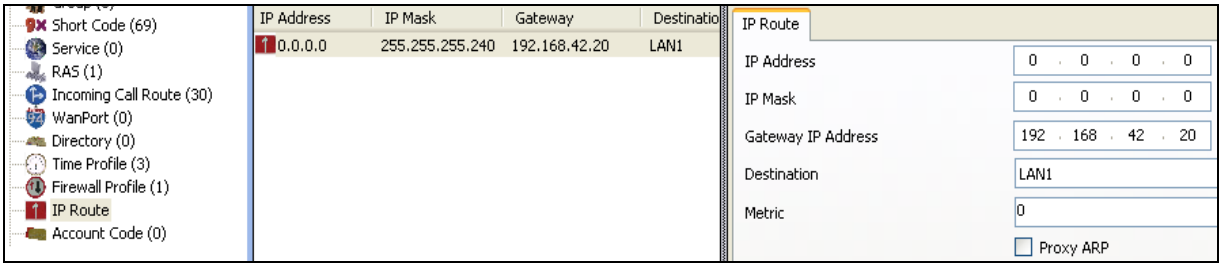
©2014 Avaya Inc. All Rights Reserved.

The Avaya IP Office 500 V2 has two Ethernet ports on the back of the chassis, labeled **WAN** and **LAN**. In the reference configuration, the LAN port (LAN1) is connected to the private CPE network, as described in **Section 3**. The Avaya H.323 and SIP telephones, and the Avaya IP Office management/Softphone PC, are also connected to the private CPE network.

The WAN port (LAN2) is connected to the CPE management subnet.

Provisioning for these interfaces is described in **Section 5.3.2** and **5.3.3**.

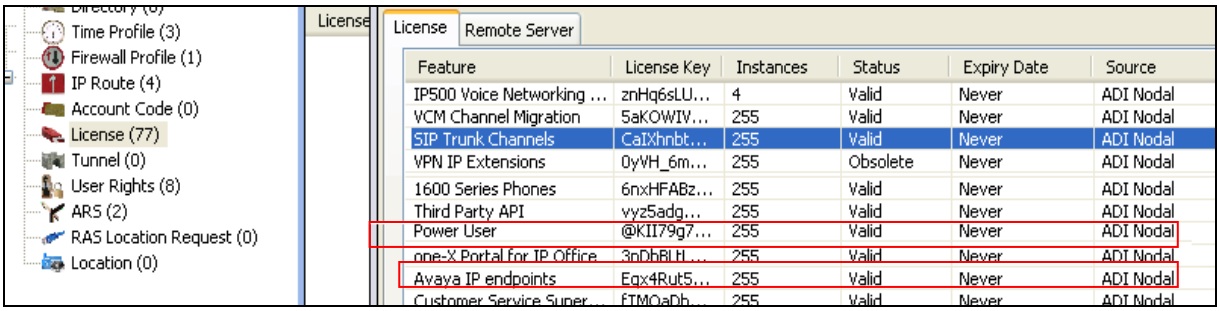
In order for the Avaya IP Office system to be able to route data to/from the AT&T network, a default route must be added specifying the Avaya SBCE "A1" interface (e.g., **192.168.42.20**). To add an IP Route in Avaya IP Office, right-click **IP Route** from the Navigation pane, and select **New** (not 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 relevant default route using **Destination → LAN1**.



5.2. Licensing

The configuration and features described in these Application Notes require the Avaya IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.
To verify that there is a SIP Trunk Channels License with sufficient capacity, click **License** in the Navigation pane and verify that **SIP Trunk Channels** has sufficient "Instances" (trunk channels).

If Avaya IP Telephones are to be used, verify the Avaya IP endpoints license. If any of those endpoints are to be defined as a "Power User", then that must be licensed as well.



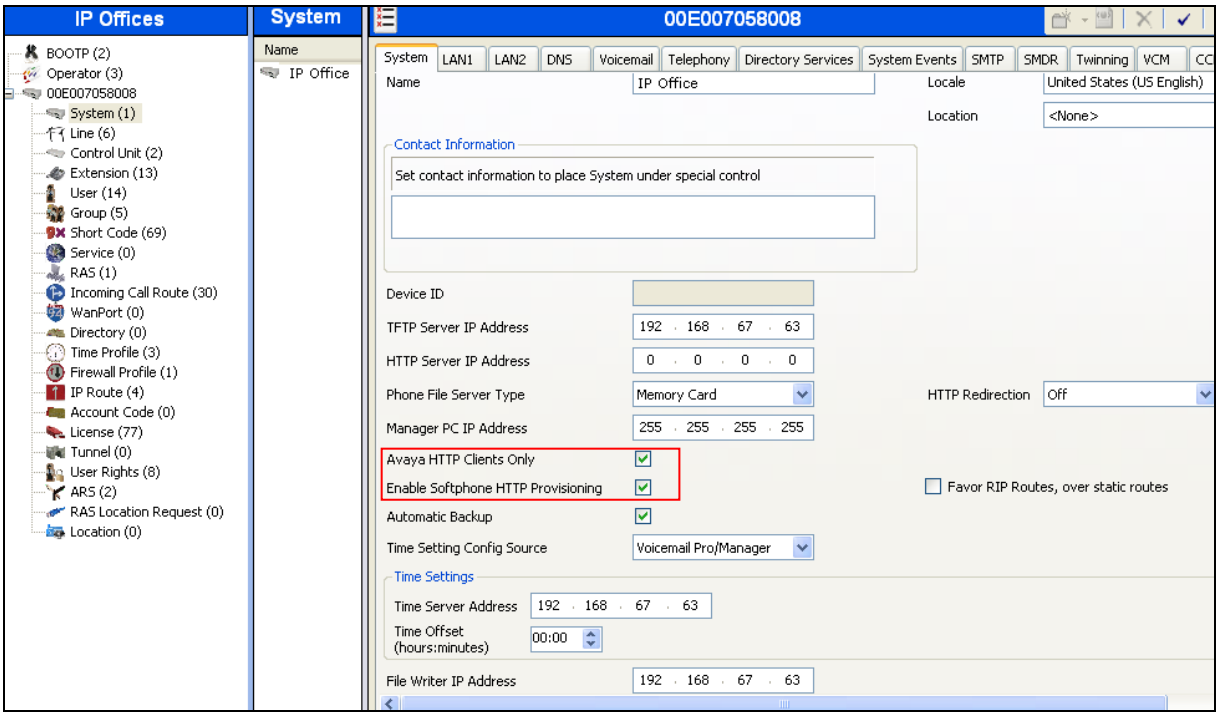
©2014 Avaya Inc. All Rights Reserved.

5.3. System Settings

This section illustrates the configuration of system settings. Select **System** in the Navigation pane to configure these settings.

5.3.1. System Tab

With the proper system name selected in the Group pane, select the **System** tab in the Details pane. The following screen shows a portion of the **System** tab. The **Name** field can be used for a descriptive name of the system. The **Avaya HTTP Clients Only** and **Enable SoftPhone HTTP Provisioning** boxes are checked to facilitate Avaya IP Office Softphone usage.

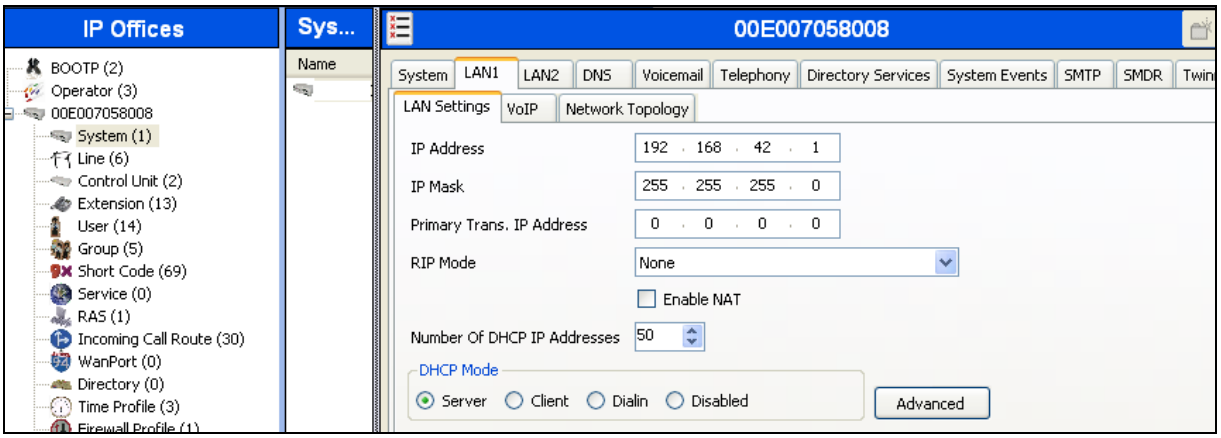


5.3.2. LAN 1 Settings

In the reference configuration, LAN1 was used to connect the Avaya IP Office to the CPE network (see **Section 3**). To view or configure the IP address, select the **LAN1** tab followed by the **LAN Settings** tab, and enter the following:

- **IP Address:** Set to **192.168.42.1** as used in the reference configuration.
- **DHCP Mode** is also set to **Server** so that IP phones will get an IP Address from the Avaya IP Office Server. Other parameters on this screen may be set according to customer requirements.
- Click the **OK** button (not shown).

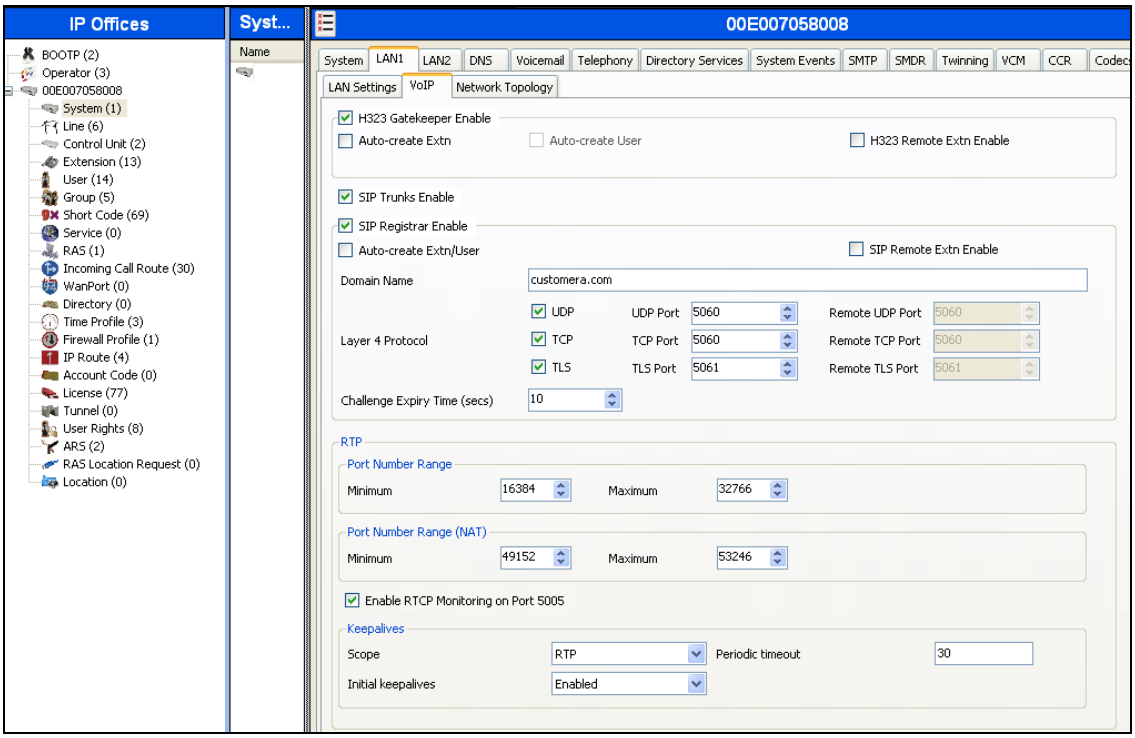
©2014 Avaya Inc. All Rights Reserved.



Select the **LAN1 → VoIP** tab as shown in the following screen. The following settings were used in the reference configuration:

- The **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the Avaya 1600-Series Telephones used in the reference configuration.
- The **SIP Trunks Enabled** box is checked to support SIP trunking.
- The **SIP Registrar Enable** box is checked to allow Avaya 11xx (SIP) and Avaya IP Office Softphone (SIP) usage.
- A **Domain Name** of **customera.com** was used in the reference configuration (see **Section 12.3.1**).
- **RTP Port Number Range:** The AT&T IPTF service requires that the RTP use the port range 16384 to 32767.
  - **16384** is entered in the **Port Range (Minimum)** field.
  - **32766** is entered in the **Port Range (Maximum)** field, as this field requires even numbers. See **Section 6.5.3** for more information on the RTP settings.
- **DiffServ Settings** (optional)**:** If desired, Avaya IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies. The default values were used in the reference configuration.
- To prevent possible issues with network firewalls closing idle RTP channels, it is recommended that **RTP Keepalives** are enabled on the **LAN1 → VoIP** tab. Scrolling down to the bottom of the form, enter the following:
  - **Scope**: Select **RTP**
  - **Periodic Timeout**: Enter **30**
  - **Initial keepalives**: Select **Enabled**
- Let all other values default.
- Click the **OK** button.

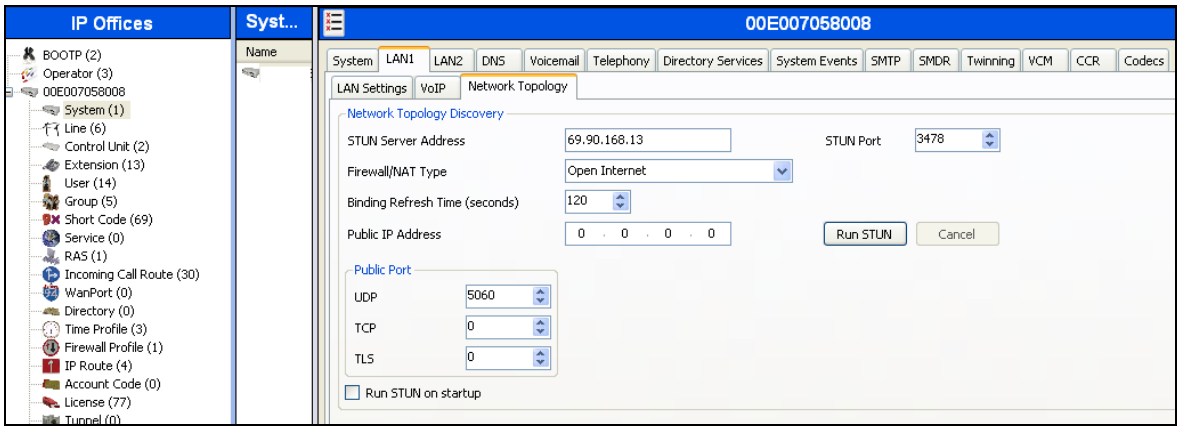
©2014 Avaya Inc. All Rights Reserved.



Select the **LAN1 → Network Topology** tab as shown in the following screen, and enter the following:

- **Public IP Address**: The **0.0.0.0** default value is used. This means Avaya IP Office will use the LAN1 IP address specified on the LAN1 **LAN Settings** tab described above (192.168.42.1).
- **Public Port** to **5060**.
- **Firewall/NAT Type** is set to **Open Internet**. With this configuration, STUN will not be used.
- Click the **OK** button (not shown).

Note: The **Firewall/NAT Type** parameter may need to be different, depending on the type of firewall or Network Address Translation device used at the customer premise.

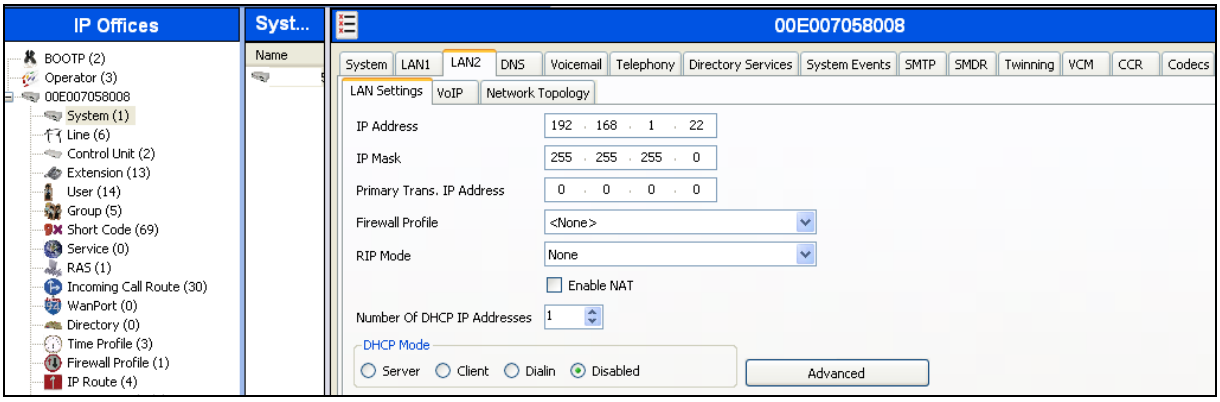


©2014 Avaya Inc. All Rights Reserved.

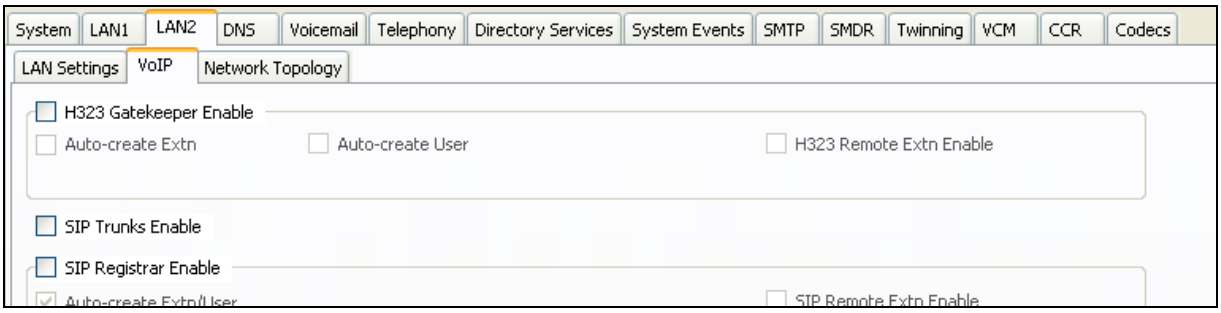
5.3.3. LAN 2 Settings

As described in **Section 3**, the LAN2 interface was not used for VoIP traffic in the "one-wire" configuration implemented in the reference configuration. However the LAN2 interface was used to manage the IP Office platform and was connected to a separate management subnet.

- **IP Address:** In the reference configuration the IP Office management address is **192.168.1.22**.
- Other parameters on this screen were set to defaults.



- On the **VoIP** tab verify that the H.323 Gatekeeper, SIP Trunks, and SIP Registrar boxes are *not* checked.



- The **Network Topology** tab uses default values.
- Click the **OK** button (not shown).

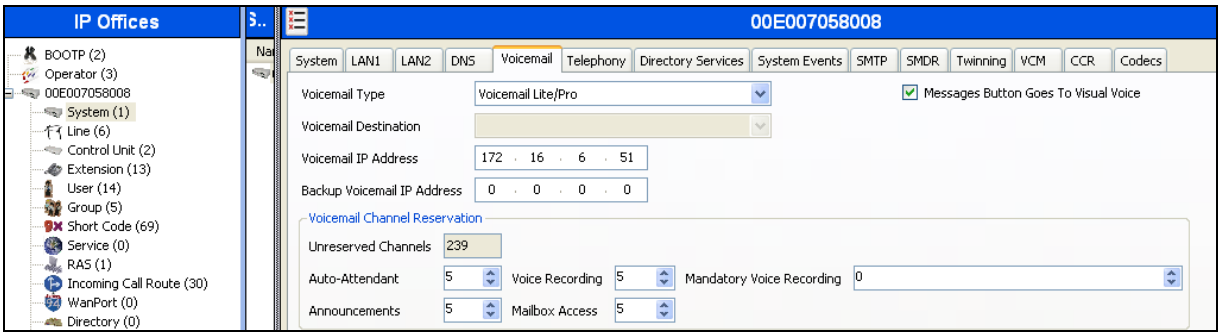
5.3.4. Voicemail

As described previously, Avaya IP Office Voicemail Pro was used in the reference configuration as the voicemail platform, running on a Windows 2003 Server. The installation and provisioning of Avaya IP Office Voicemail Pro is beyond the scope of this document. See reference **[4]** & **[5]**for more information on installing and provisioning Avaya IP Office Voicemail Pro.

To view or change Avaya IP Office Voicemail settings, select the **Voicemail** tab as shown in the following screen. The settings presented here simply illustrate the reference configuration and are not intended to be prescriptive.

©2014 Avaya Inc. All Rights Reserved.

- Set **Voicemail Type**: **Voicemail Lite/Pro**.
- Set **Voicemail IP Address**: to the IP address of the platform running Voicemail Pro.
- Other parameters on this screen may be set according to customer requirements.
- Click the **OK** button.



5.3.5. System Telephony Configuration

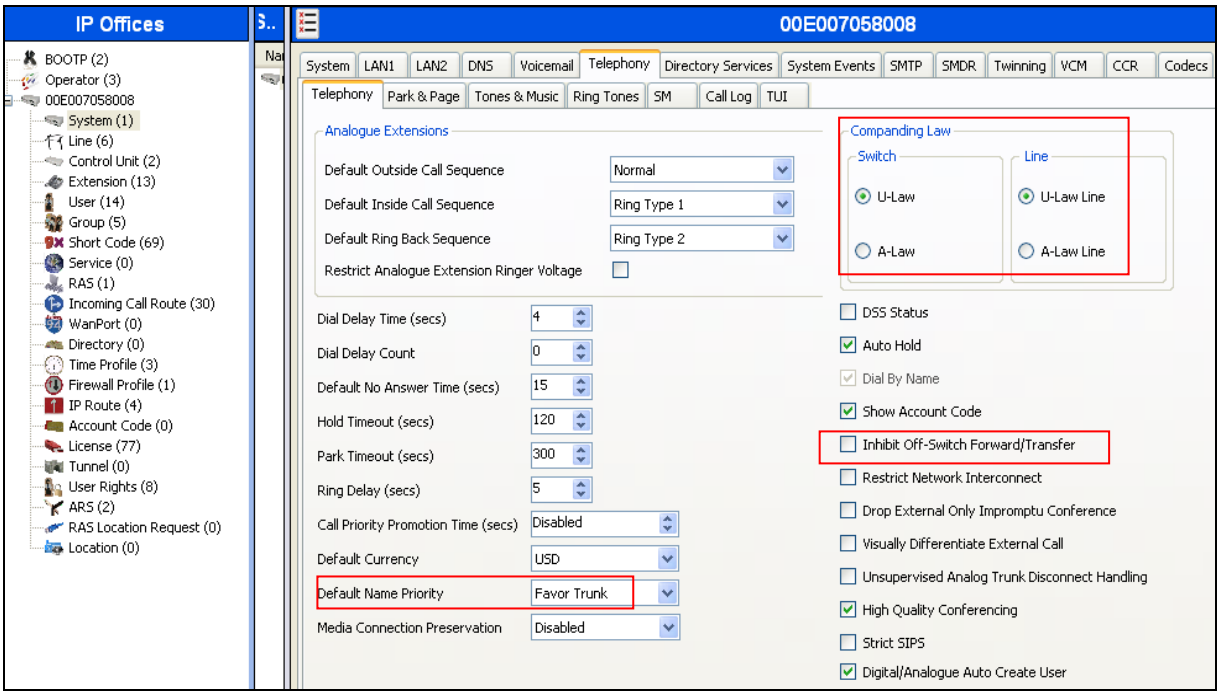
To view or change telephony settings, select the **Telephony** tab and **Telephony** sub-tab as shown in the following screen. The settings presented here simply illustrate the reference configuration and are not intended to be prescriptive.

In the reference configuration, the **Inhibit Off-Switch Forward/Transfer** box is unchecked so that call forwarding and call transfer to PSTN destinations via the AT&T IPFR-EF service can be tested.

The **Companding Law** parameters are set to **U-LAW** as is typical in North America. Other parameters on this screen may be set according to customer requirements.

OPTIONAL: The **Default Name Priority** can be relevant to SIP Trunking. The option to **Favor Trunk** or **Favor Directory** can be set system-wide using the screen below, or set uniquely for each line. **Favor Trunk** was used in the reference configuration. 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 5.4.1**. A user's personal directory example is shown in **Section 5.5.2**.

©2014 Avaya Inc. All Rights Reserved.

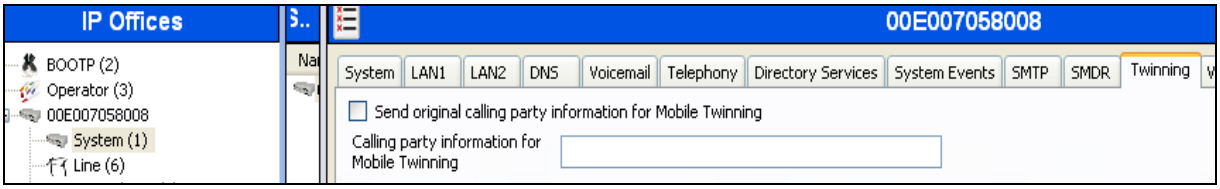


5.3.6. System Twinning Configuration

To view or change Twinning settings, select the **Twinning** tab as shown in the following screen.

The **Send original calling party information for Mobile Twinning** box is not checked, and the **Calling party information for Mobile Twinning** is left blank, in the reference configuration.

With this configuration, and related configuration of Diversion Header on the SIP Line (**Section 5.4.1**), the true identity of a PSTN caller can be presented to the twinning destination (e.g., a user's mobile phone) when a call is twinned out via the AT&T IPFR-EF service.



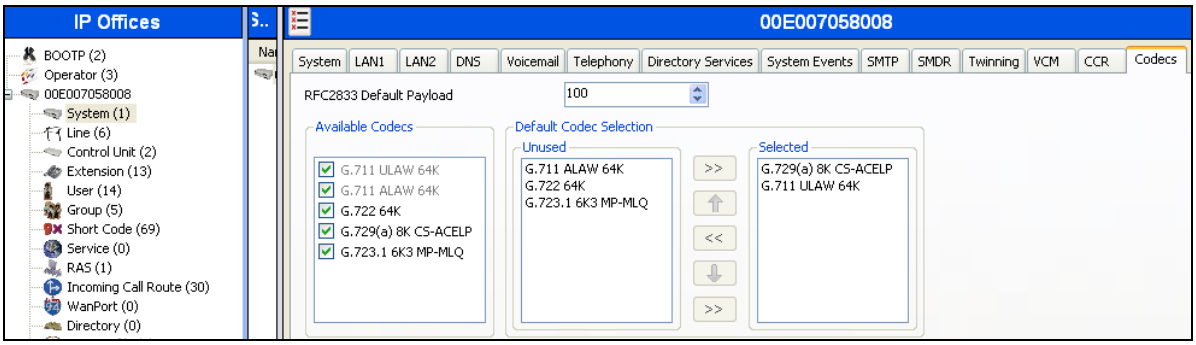
5.3.7. System Codecs Configuration

Navigate to the **System → Codecs** tab. On the left, observe the list of **Available Codecs**. By selecting codecs in this column, they will appear in the **Default Codec Selection → Unused** column. Codecs may be selected from the **Unused** list and moved to the **Selected** column by use of the >> button, thereby making the selected codecs available in other screens where codec configuration may be performed (e.g., Sip Lines and Extensions).

©2014 Avaya Inc. All Rights Reserved.

The up and down arrow buttons are used to order the selected codecs. By default, all IP (SIP and H.323) lines and extensions will assume the system default **Selected** codec list, unless configured otherwise for the specific line or extension. When completed, click on **OK** (not shown).

Note - In the reference configuration, an Extension (see **Section 5.5.2**) codec list specifies G.711mu and G.729A (in that order), and the SIP Line (see **Section 5.4.3)** offers G.729A and G.711MU (in that order). In this manner local Avaya IP Office calls will offer G.711MU first, and SIP trunk calls will offer G.729A first.



5.4. 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 IP Office Manager to create a new SIP Line for SIP trunking with the AT&T IPFR-EF service. Follow the steps in **Section 5.4.1** to create a SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary, after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.4.2 – 5.4.6**.

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

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

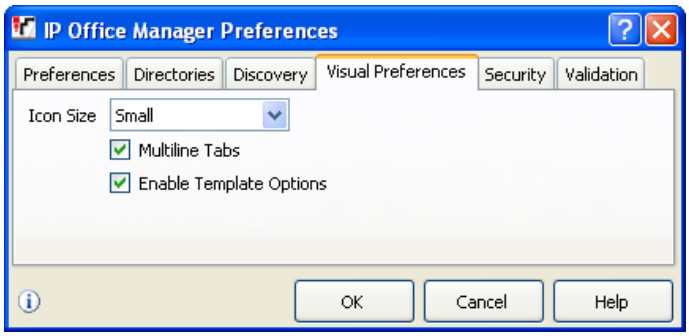
©2014 Avaya Inc. All Rights Reserved.

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 5.4.2 – 5.4.5**.

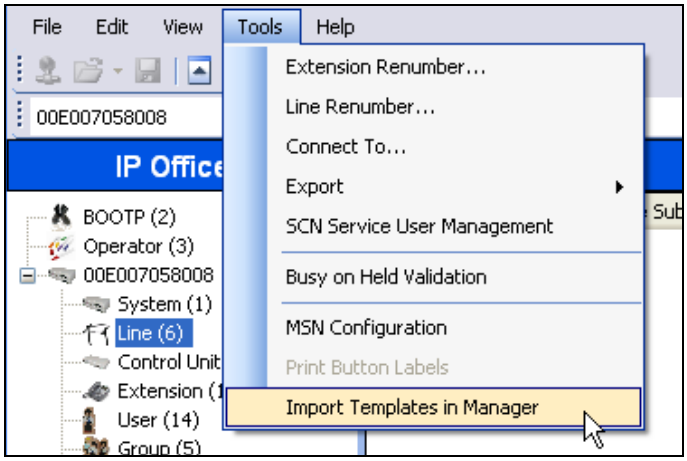
5.4.1. SIP Line from Template

1. Copy the template file to the computer where IP Office Manager is installed. Rename the template file to **US_AT&T_SIPTrunk.xml**. The file name is important in locating the proper template file in **Step 5**.

2. Verify that template options are enabled in IP Office Manager. In IP Office Manager, navigate to **File → Preferences**. In the IP Office Manager Preferences window that appears, select the Visual Preferences tab. Verify that the box is checked next to **Enable Template Options**. Click **OK**.



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

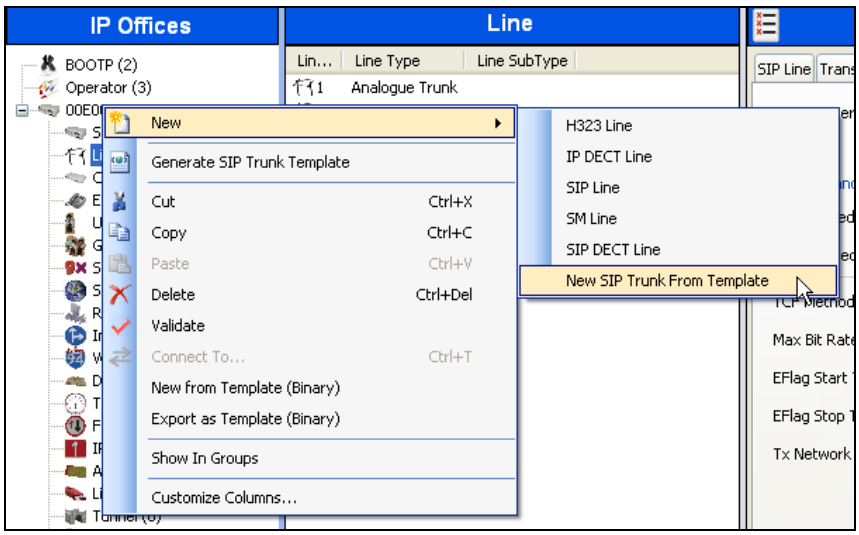


In the pop-up window (not shown) that appears, select the directory where the template file was copied in **Step 1**. After the import is complete, a final import status

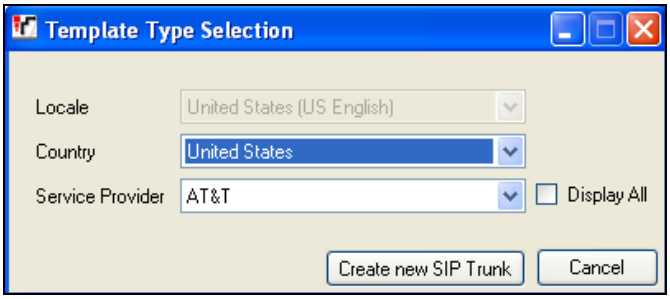
©2014 Avaya Inc. All Rights Reserved.

pop-up window (not shown) will appear stating success or failure. Click **OK** (not shown) to continue. If preferred, this step may be skipped if the template file is copied directly to the IP Office template directory.

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



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



The newly created SIP Line will appear in the Navigation pane.

6. Once the SIP Line is created, verify the configuration of the SIP Line with the configuration shown in **Sections 5.4.2 – 5.4.5.**

7. Save the configuration as shown in **Section 5.12.**

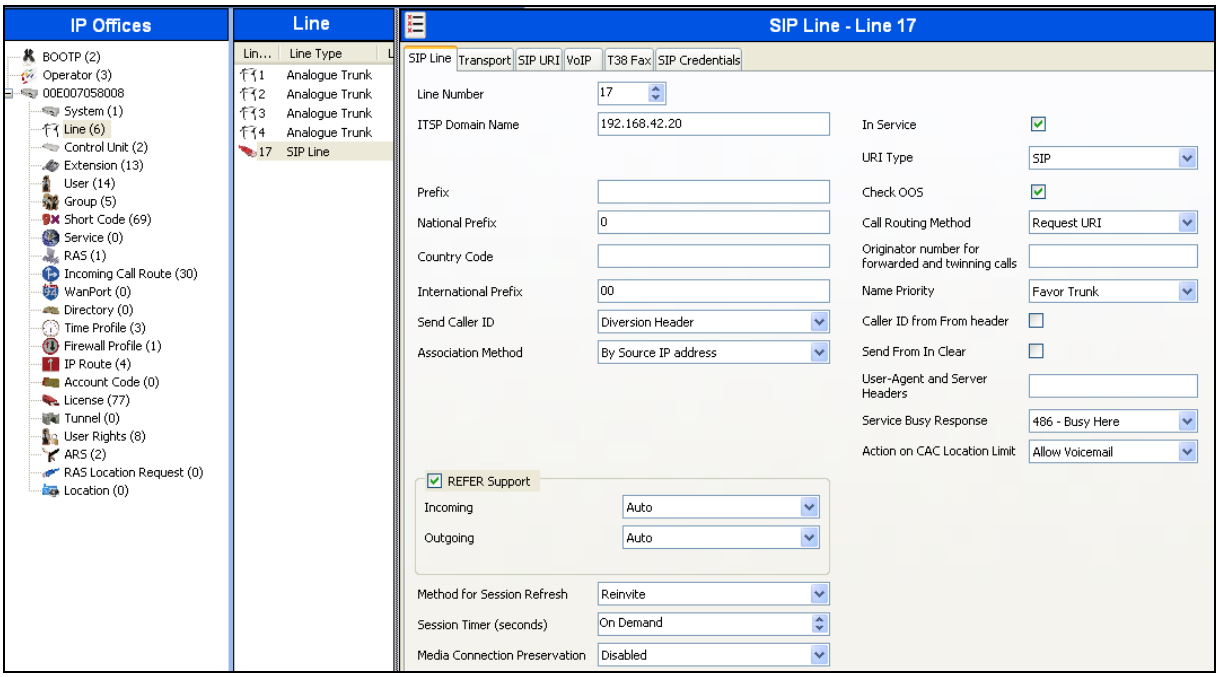
©2014 Avaya Inc. All Rights Reserved.

5.4.2. SIP Line – SIP Line tab

The **SIP Line** tab in the Details pane is shown below for **Line Number 17**, used for the SIP Trunk to the Avaya SBCE, and ultimately AT&T. 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 17 was created. The SIP Line form is completed as follows:

- **ITSP Domain Name**: Set to the IP address of the "inside" (A1) SIP trunking interface of the Avaya SBCE (e.g., **192.168.42.20**).
- **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 (see **Section 5.11**).
- **Call Routing Method**: Matched values based on the **Request URI**, or **To Header** contents, may be selected. In the reference configuration, the default **Request URI** setting was used.
- **Country Code**: Use the default <blank>.
- **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).
- **REFER Support**: Check this box to enable Avaya IP Office to use REFER for call transfer scenarios back to PSTN (attended & unattended).
- Use the default values for the other fields.
- Click **OK** (not shown).

As described in **Section 5.3.5**, the **Name Priority** parameter may retain the default **Favor Trunk** setting, or can be configured to **Favor Directory**. As shown below, the default **Favor Trunk** setting was used in the reference configuration.

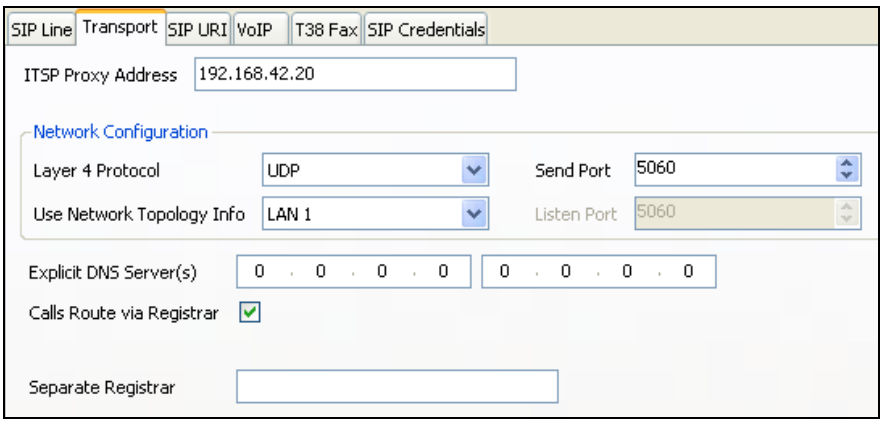


©2014 Avaya Inc. All Rights Reserved.

5.4.3. SIP Line - Transport tab

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

- **ITSP Proxy Address:** Set to the Avaya SBCE "inside" A1 SIP Trunk interface IP address **192.168.42.20**.
- **Network Configuration → Layer 4 Protocol**: Set to **UDP**.
- **Network Configuration → Send Port**: Set to **5060** (default).
- **Network Configuration → Use Network Topology Info**: Set to **LAN 1**.
- **Calls Route via Registrar:** Enabled (default).
- **Click OK** (not shown).



5.4.4. SIP Line - SIP URI tab

Select the **SIP Line → SIP URI** tab. On this form a list of the DNIS digits delivered by AT&T is created.

Note – In the reference configuration the AT&T IPFR-E service delivered seven DNIS digits in the R-URI. The entries below match on these DNIS digits, not the dialed DID number.

To add a new SIP URI, click the **Add…** button. At the bottom of the screen, a **New Channel** area will be opened. Entries may be specified in two ways:

1. A "wild-card" entry that will use the contents of SIP headers containing "called party info" information.

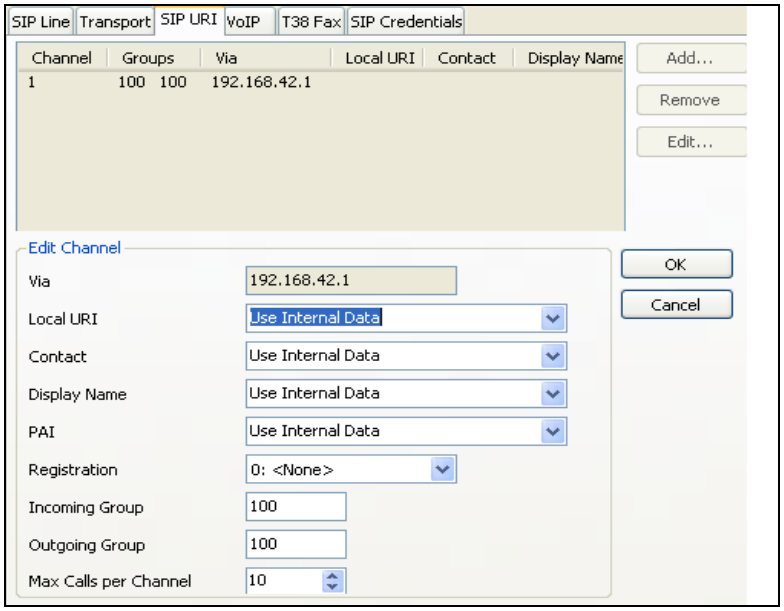
   Note - When this method is used, the inbound AT&T DNIS digits must be specified for an Avaya IP Office User or Hunt Group, on its corresponding **SIP** tab (see **Section 5.5**). Otherwise, the call will be denied.

   In this method the following information is specified:

   - The **Via** field will automatically be populated with the IP address of the system LAN interface (LAN 1) with which the SIP trunk is associated (see **Sections 5.3.2** and **5.4.1)**.
   - **Local URI**, **Contact**, **Display Name**, **and PAI**: Set to **Use Internal Data**.

©2014 Avaya Inc. All Rights Reserved.

- **Registration:** Set to the default **0: <None>**.
- **Incoming Group:** Set to **100** (SIP Line 17). This value references the table created with **Incoming Call Routes** in **Section 5.7**.
- **Outgoing Group:** Set to **100** (SIP Line 17). This will be used for routing outbound calls to AT&T via the **Short Codes** (**Section 5.6**) or **ARS** configuration (**Section 5.8**).
- **Max Calls per Channel:** 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** to save the information.



2. Specific entry(s) that will match inbound DNIS digits from AT&T.

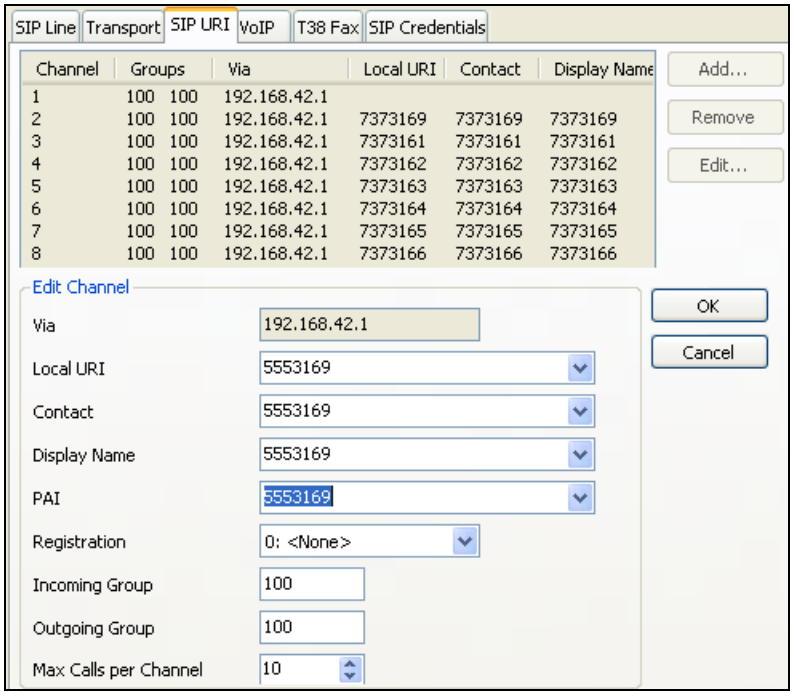
> **Note** – This method must be used for Avaya IP Office call destinations other than Users or Hunt Groups. This may be Auto Attendant and Meet-Me conference Short Codes, calls to Voicemail Pro, (or other inbound calls not defined on a User or Hunt Group SIP tab).

In this method the following information is specified:

- **Local URI**, **Contact**, PAI, and **Display Name**: Set to an AT&T DNIS number (e.g., **5555386).**
- **Registration:** Set to the default **0: <None>**.
- **Incoming Group:** Set here to **100** (SIP Line 17). This value references the **Incoming Call Routes** in **Section 5.7**.
- **Outgoing Group:** Set to **100**(SIP Line 17). This will be used for routing outbound calls to AT&T via the **Short Codes** (**Section 5.6**) or **ARS** configuration (**Section 5.8**).

©2014 Avaya Inc. All Rights Reserved.

- **Max Calls per Channel:** 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.
- Repeat for every required AT&T DNIS string.
- Click **OK** to save the information.



- To edit an existing entry, click an entry in the list (e.g., **Channel 2 →5553169**), and click the **Edit…** button. On the bottom of the screen, the **Edit Channel** area will be opened.
- When all SIP URI entries have been added/edited, click **OK** at the bottom of the screen (not shown).

5.4.5. SIP Line - VoIP tab

Note – When **T.38** is specified for **Fax Transport Support** below, the Direct Media parameters **Allow Direct Media Path** and **Force direct media with phones** cannot be selected. In addition, as mentioned in **Section 2.2.1**, **Item 4**, issues were found when Direct Media was enabled. Therefore even if T.38 is not specified, the use of Direct Media is not recommended at this time.

Select the **SIP Line → VoIP** tab.

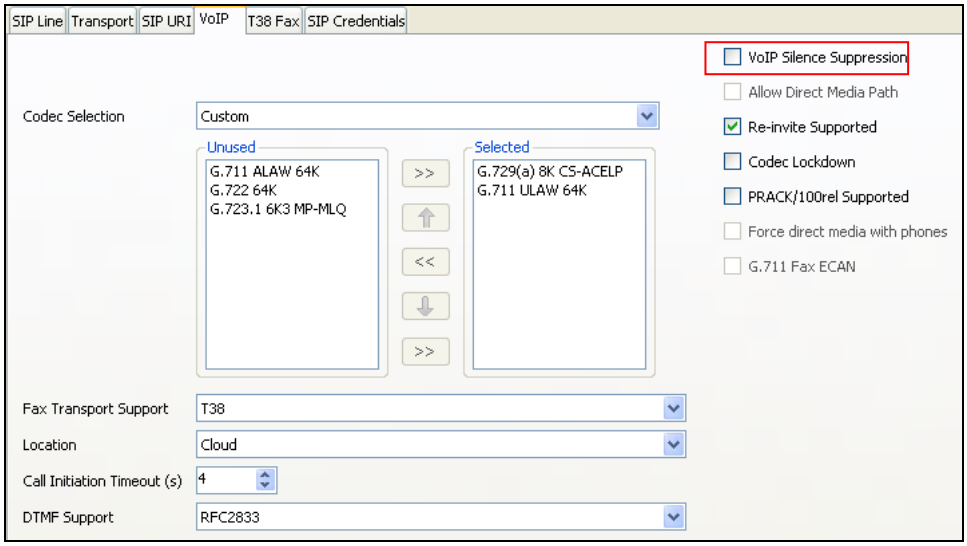
- The **Codec Selection** drop-down box → **System Default** will list all available codecs. In the reference configuration, **Custom** was selected and **G729(a) 8K CS-ACELP,** and **G.711 ULAW 64K** were specified. This causes Avaya IP Office to include these codecs in the Session Description Protocol (SDP) offer, and in the order specified. Note that in the reference configuration G.729A is set as the preferred codec on the connection to the AT&T IPFR-EF network.

©2014 Avaya Inc. All Rights Reserved.

- T.38 fax was used in the reference configuration. Set the **Fax Transport Support** drop-down menu to **T38**. Note that Error Correction Mode (ECM) is enabled by default on the **T.38 Fax** tab (**Section 5.4.5**). 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**.
- 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).

Since the AT&T IPFR-EF service does not require registration, the **SIP Credentials** tab need not be visited.

Note - By default the VoIP Silence Suppression box is not checked. This disables the use of the G.729B codec. If silence suppression is desired, check this box, and enable the **VoIP Silence Suppression** option on the **Extension** form **VoIP** tab (see **Section 5.5.2**).

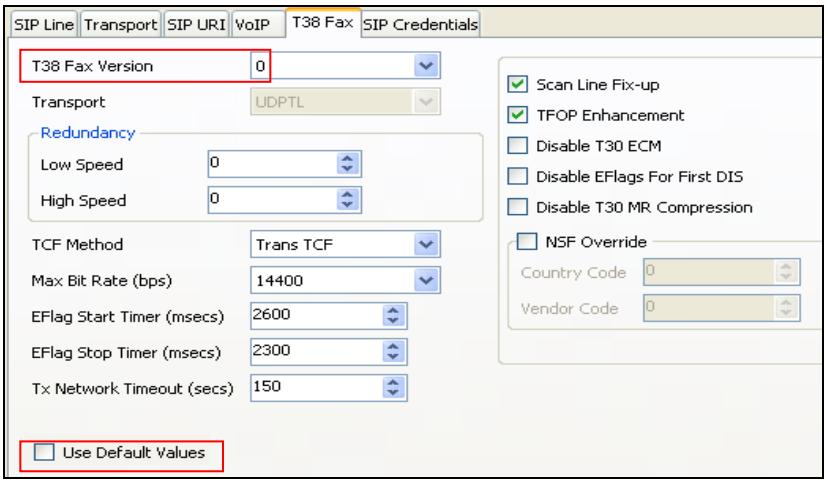


5.4.6. SIP Line - T38 Fax

Note - 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 5.4.4**).

- Unselect the **Use Default Values** option.
- Set the **T38 Fax Version** option to **0** (zero).
- Verify that **Disable T30 ECM** is *not* checked.
- Use all other default values.
- Select **Ok** (not shown).

©2014 Avaya Inc. All Rights Reserved.



5.5. Users, Extensions, and Hunt Groups

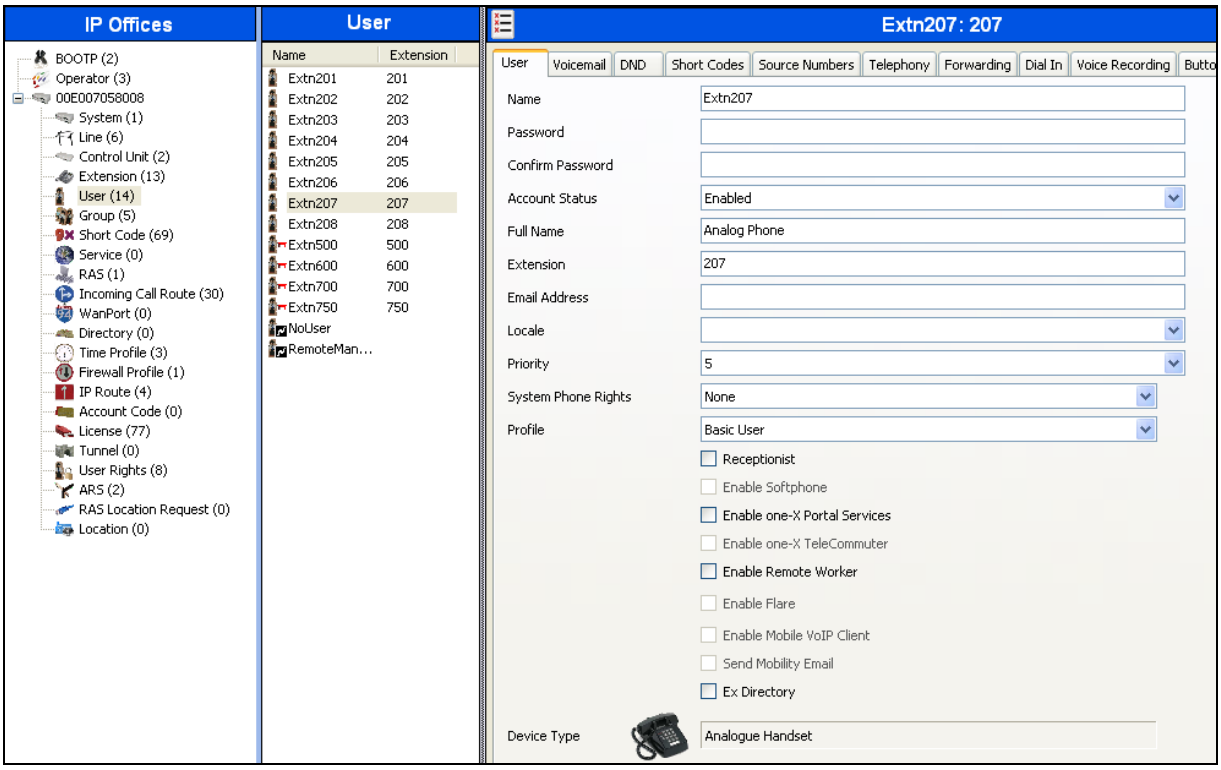
In this section, examples of Avaya IP Office Users, Extensions, and Hunt Groups are illustrated.

5.5.1. Analog User Extn207

The following screen shows the **User** tab for analog phone User **Extn207**. This user corresponds to the Avaya Analog 6211 set.

To add a User, right click on **User** in the Navigation pane, and select **New** (not shown). To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the Group pane.

©2014 Avaya Inc. All Rights Reserved.



The following screen shows the **SIP** tab for User **Extn207** (use the arrow buttons in the upper right corner to navigate to the SIP tab).

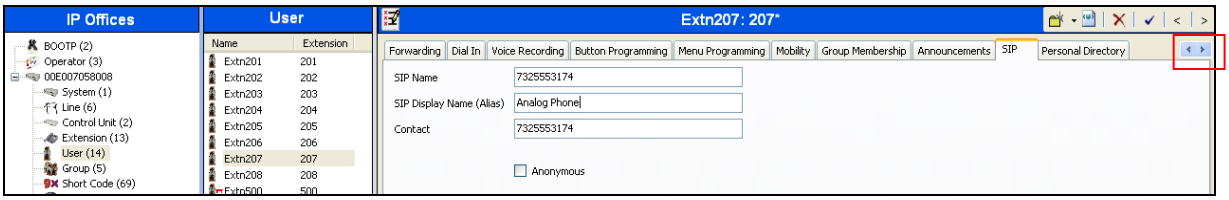
- The **SIP Name** and **Contact** parameters are configured with the associated AT&T DNIS number of the user, (e.g., **7325553174**). These parameters configure the user part of the SIP URI in the From header for outgoing SIP trunk calls, and allow matching of the SIP URI for incoming calls, without having to enter this number as an explicit SIP URI for the SIP Line (see **Section 5.4.3**).

> **Note** – For incoming calls Avaya IP Office will match these fields from *right to left*, therefore matching on the seven digit inbound AT&T DNIS string (e.g., ***5553174***). However for outbound calls Avaya IP Office will populate the calling fields (e.g., From header) with the full ten digit AT&T DID number (e.g., **7325*553174***).

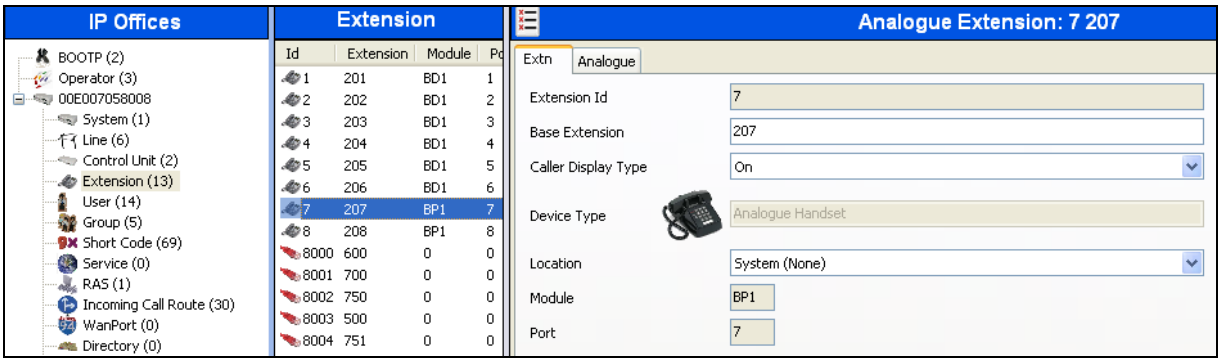
The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.

If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network (see **Section 5.10**). See **Section 5.6.3** for a method of using a Short Code (rather than static user provisioning) to place an anonymous call.

©2014 Avaya Inc. All Rights Reserved.



Select **Extension** from the Navigation pane, and select New (not shown). Enter the appropriate extension (**207**) information (note that the Extension ID is automatically generated).

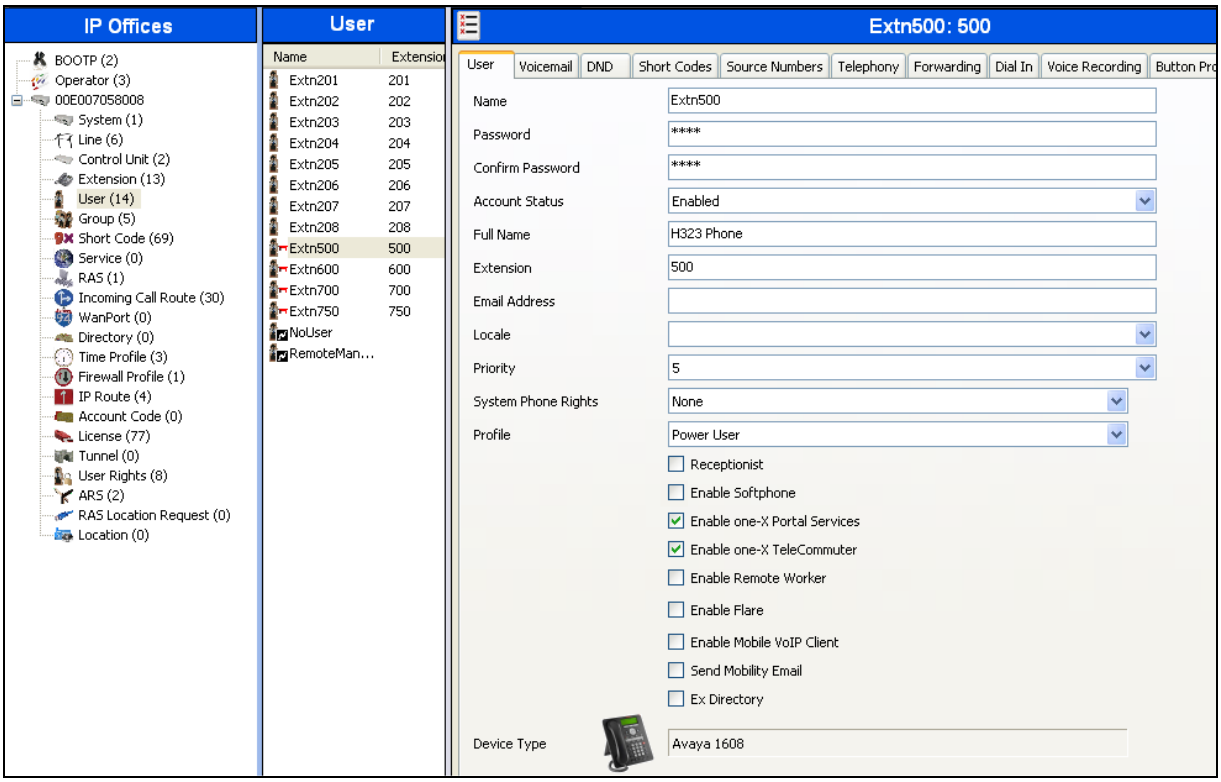


5.5.2. IP Phone User Extn500

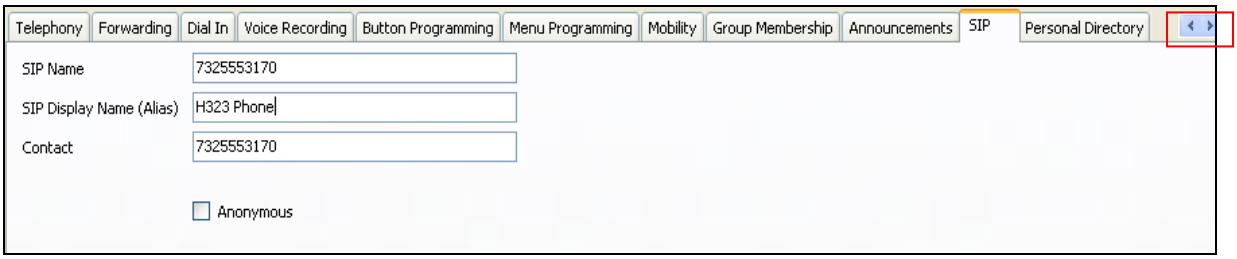
Following the steps shown in **Section 5.5.1**, create a H.323 IP phone user (e.g., **Extn500**). The following screen shows a 1608 IP Telephone provisioned in the **User** tab for User Extn500. In the reference configuration, this user will be granted "Power User" features.

- **Password**: This password is used by user applications such as SoftConsole, Phone Manager and TAPI. It is also used for users with Dial In access. Note that this is ***not*** the user's phone log in code (see the information on the **Telephony → Supervisor Settings** tab below), or their Voicemail mailbox password (see information on the **Voicemail** tab below).
- The **Profile** parameter is set to **Power User**. This gives this user access to additional Avaya P Office features. See **[1]** for more information.
- Add additional options as required.

©2014 Avaya Inc. All Rights Reserved.



Like the Analog Extn207 user, the **SIP** tab (use the arrow buttons in the upper right corner to navigate to the **SIP** tab) for User Extn500 is configured with a **SIP Name** and **Contact** specifying the user's associated AT&T number (e.g., **7325553170**). Optionally a user can be set to use privacy for all calls by selecting the **Anonymous** option.



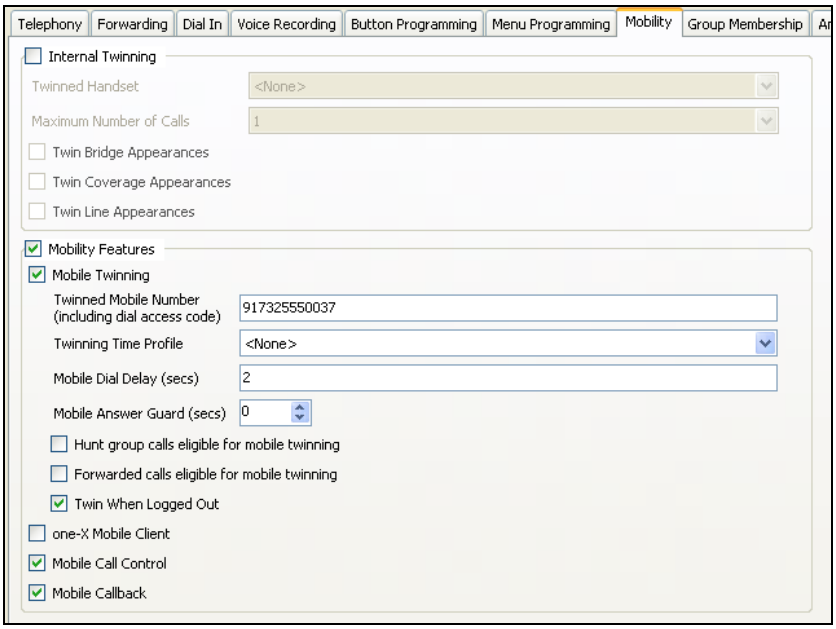
User **Extn500** will use the Mobile Twinning feature. The following screen shows the **Mobility** tab for User Extn500.

The **Mobility Features**, **Mobile Twinning**, **Mobile Call Control**, and **Mobile Callback** boxes are checked**.**

The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone, in this case **917325550037** (note that the outbound call access code **9** is specified, as described for the Short Code **9N;** access to ARS, in **Section 5.6.1**).

©2014 Avaya Inc. All Rights Reserved.

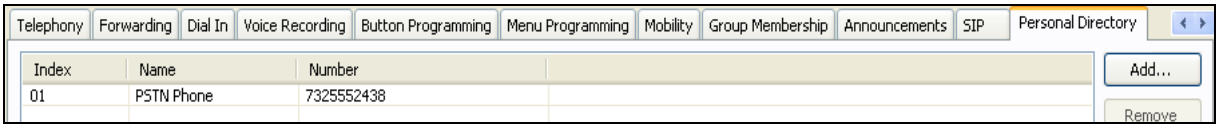
The **Mobile Call Control** and **Mobile Callback** features are accessed via Short Codes (as shown in **Section 5.6.4**), and Incoming Call Routes (as shown in **Section 5.7**).



Avaya IP Office offers a feature where users can define names in a Personal Directory, and display these names, based on the inbound calling number.

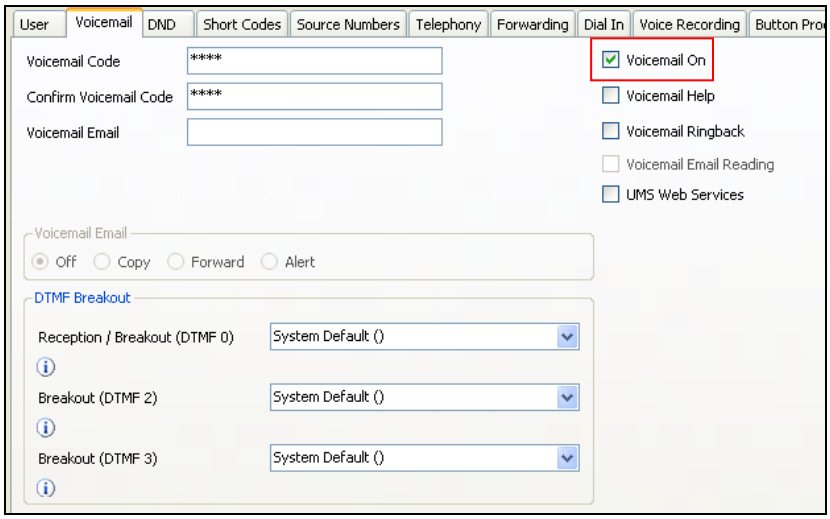
The following screen shows the **Personal Directory** tab for User **Extn500**. With the configuration shown below, if Extn500 receives an inbound AT&T call from the telephone number **7325552438**, the phone will display the name "PSTN Phone" (along with the number), even if AT&T provided a different name in the SIP INVITE message sent to Avaya IP Office.

Note – In the reference configuration, the SIP Line is configured with **Name Priority → Favor Trunk** (see **Section 5.4**). This setting needs to be changed to **Name Priority → Favor Directory**, to enable this feature.

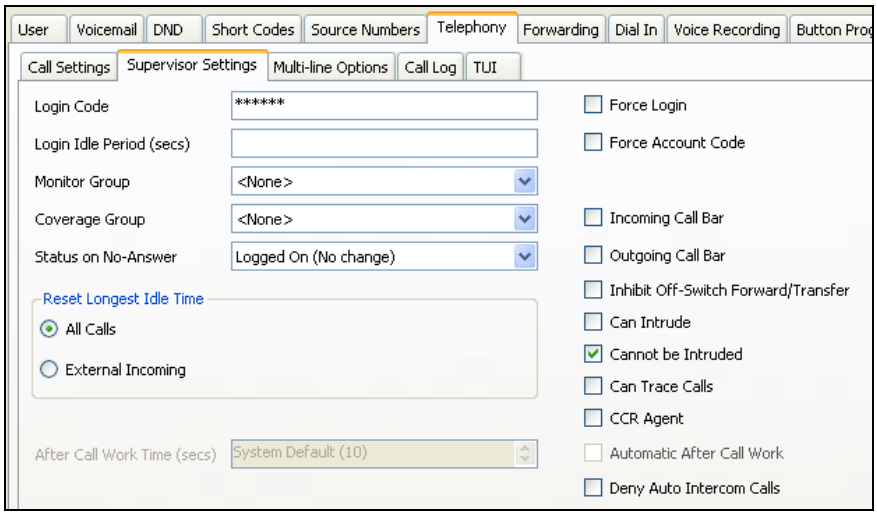


The following screen shows the **Voicemail** tab for User Extn500. The **Voicemail On** box is checked, and a Voicemail password can be configured using the **Voicemail Code** and **Confirm Voicemail Code** parameters.

©2014 Avaya Inc. All Rights Reserved.

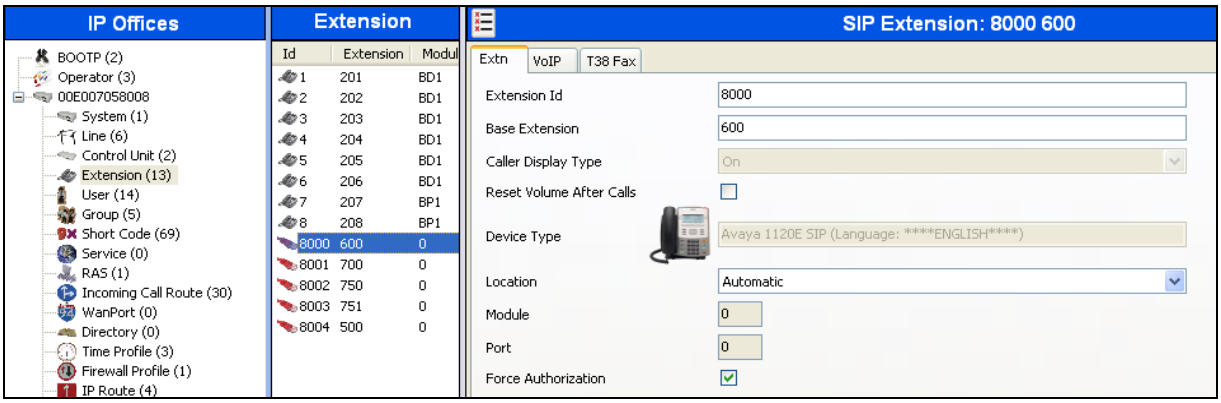


Select the **Telephony → Supervisor Settings** tab as shown below. The **Login Code** will be used by the telephone user as the phone login password.



Select **Extension** from the Navigation pane, and select New (not shown). Enter the appropriate extension (**500**) information (note that the Extension ID is automatically generated).

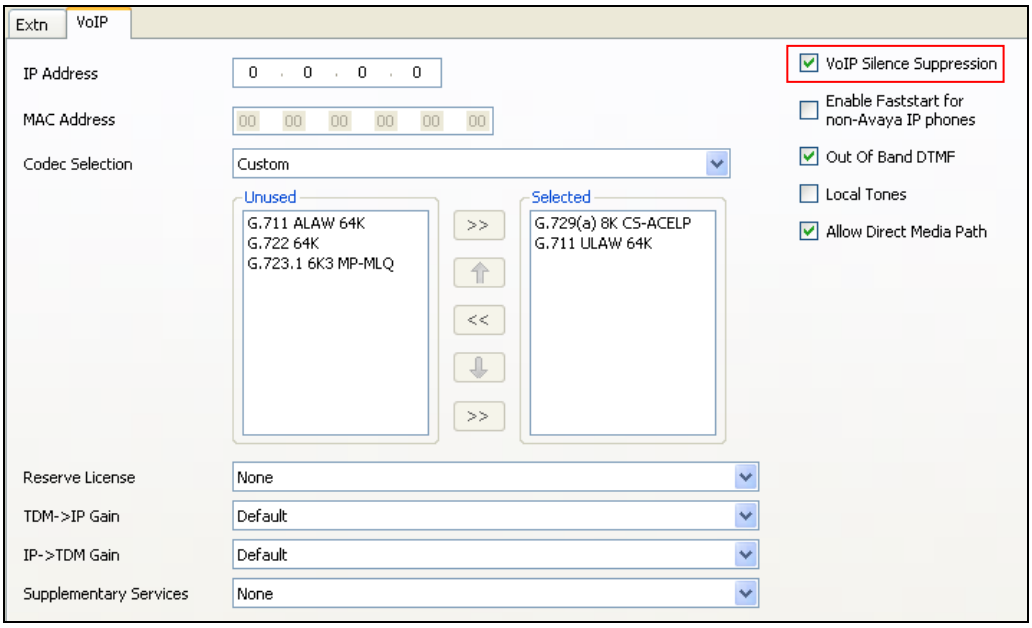
©2014 Avaya Inc. All Rights Reserved.



Select the **VoIP** tab in the Details pane.

- Use the **IP Address** field default value (**0.0.0.0**).
- Use defaults for the remaining fields.

Note that this station has Silence Suppression (G.729B) selected.



5.5.3. SIP Telephone Users (Avaya 1120E and Avaya IP Office SoftPhone)

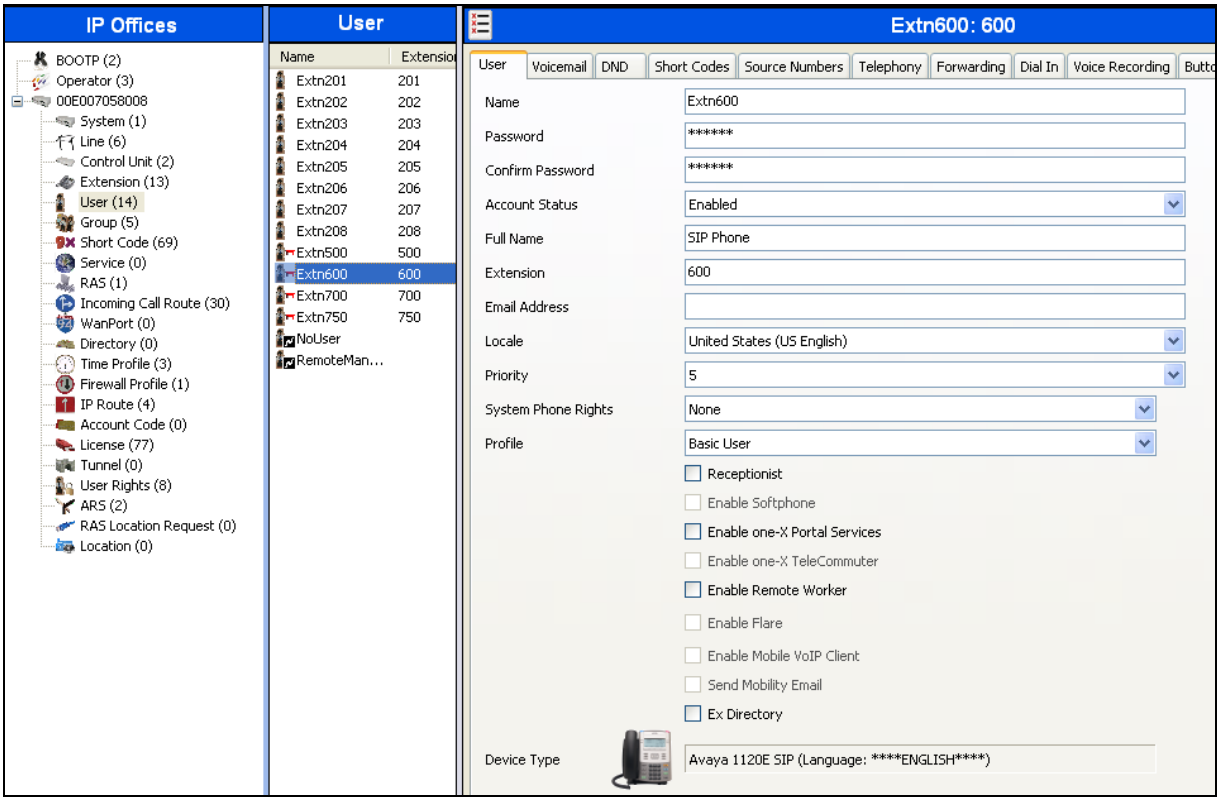
In the reference configuration, an Avaya 1120E SIP telephone and Avaya IP Office SoftPhone were provisioned as SIP users.

©2014 Avaya Inc. All Rights Reserved.

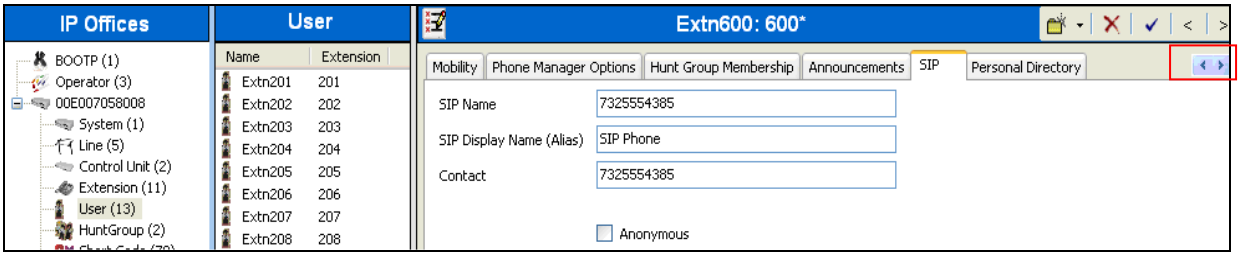
5.5.3.1 SIP Avaya 1120E

The following screen shows an 1120E Telephone provisioned in the **User** tab for User **Extn600**. The provisioning of this User is the same as for the H.323 station in **Section 5.5.2**.

Note that this station is set as a Basic User.

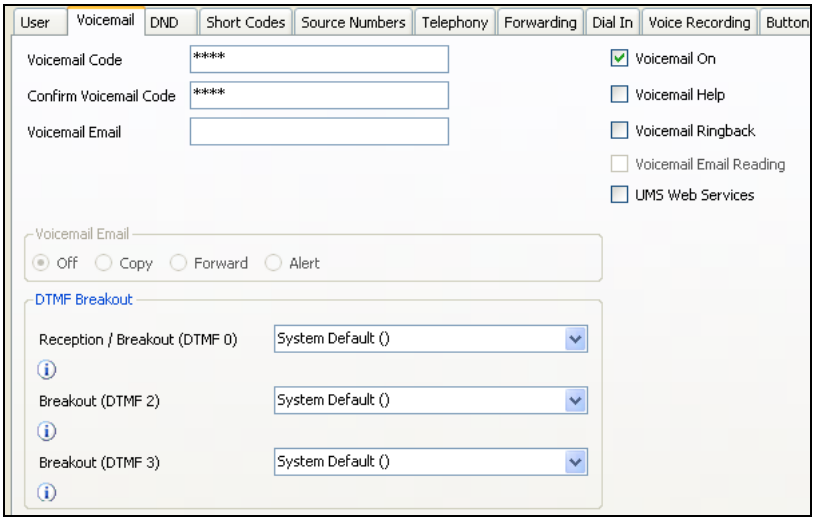


Like the H.323 Extn500 user, the **SIP** tab for User Extn600 is configured with a **SIP Name** and **Contact** specifying the user's associated AT&T number (e.g., **7325554385**).

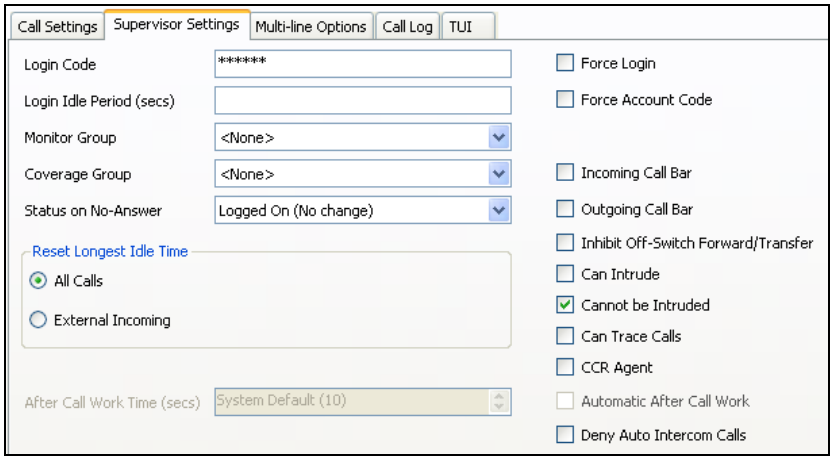


©2014 Avaya Inc. All Rights Reserved.

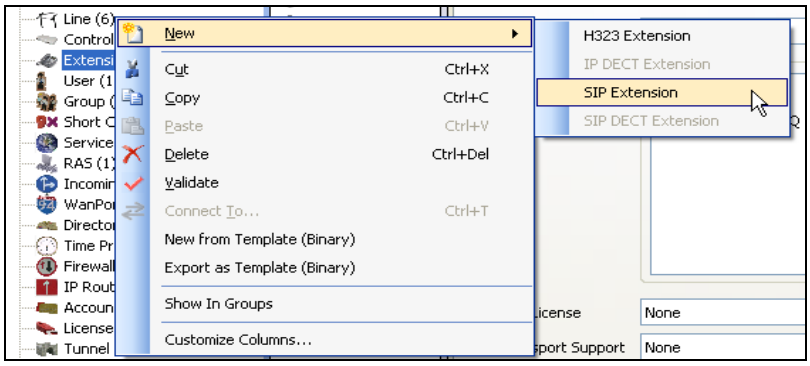
As with the H.323 Extn500 user, Extn600 also utilized the external Voicemail Pro server.



Similarly, the **Login Code** will be used by the telephone user as the phone login password.

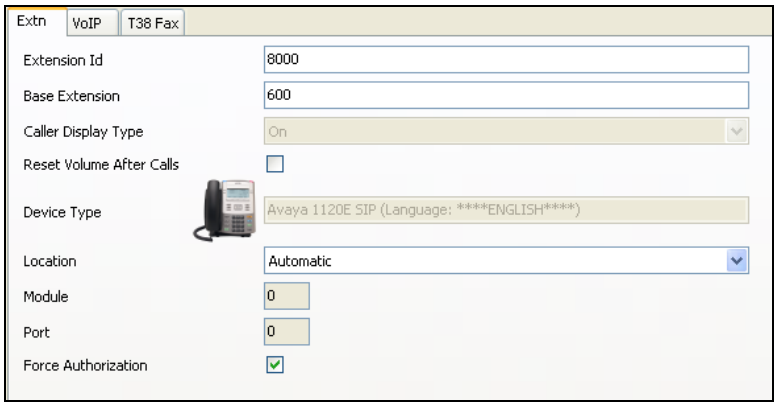


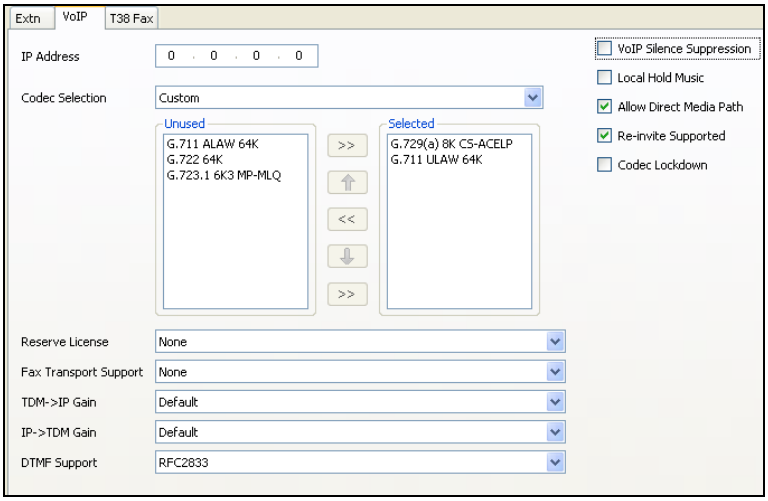
A new Extension is also created for the 1120E SIP telephone. Right Click on **Extension**, then select either a new SIP extension (or H.323) to add (e.g., a new **SIP Extension**).



©2014 Avaya Inc. All Rights Reserved.

The following screen shows the **Extn** tab for the extension corresponding to an Avaya 1120E set. Note that this station does not have Silence Suppression selected.





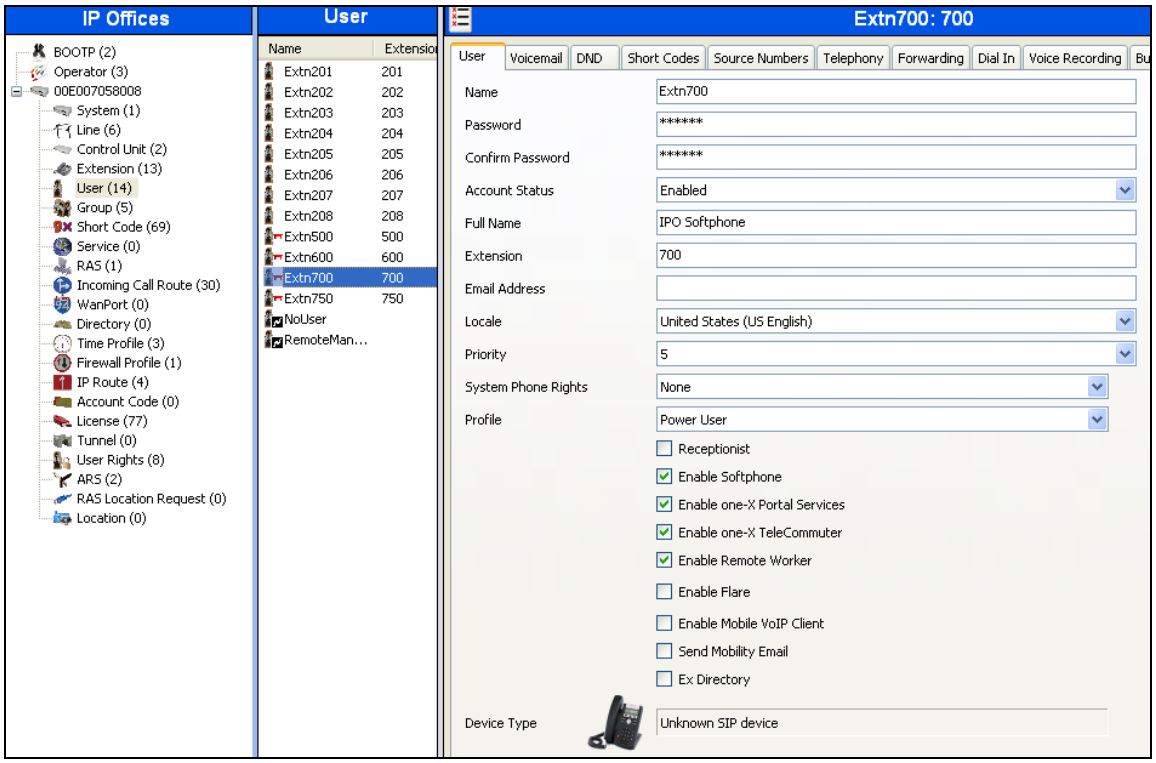
5.5.3.2 SIP Avaya IP Office Softphone

Repeat the steps shown in **Section 5.5.3.1** with the following settings.

1. Defining a **User**
   - **User** tab (shown below)
     - The **Enable Softphone** box is checked, the other enabled advanced capabilities shown, are optional.
   - **SIP** tab (not shown)
     - **SIP Name** and **Contact** specifying the user's associated AT&T DNIS number (e.g., **7325554386**).
   - **Voicemail** tab (not shown)
     - User Extn700 also utilized the embedded Voicemail. The **Voicemail On** box is checked.
   - **Telephony→ Call Settings** tab (not shown)
     - Check the **Call Waiting On** box to allow multiple call appearances and transfer operations.

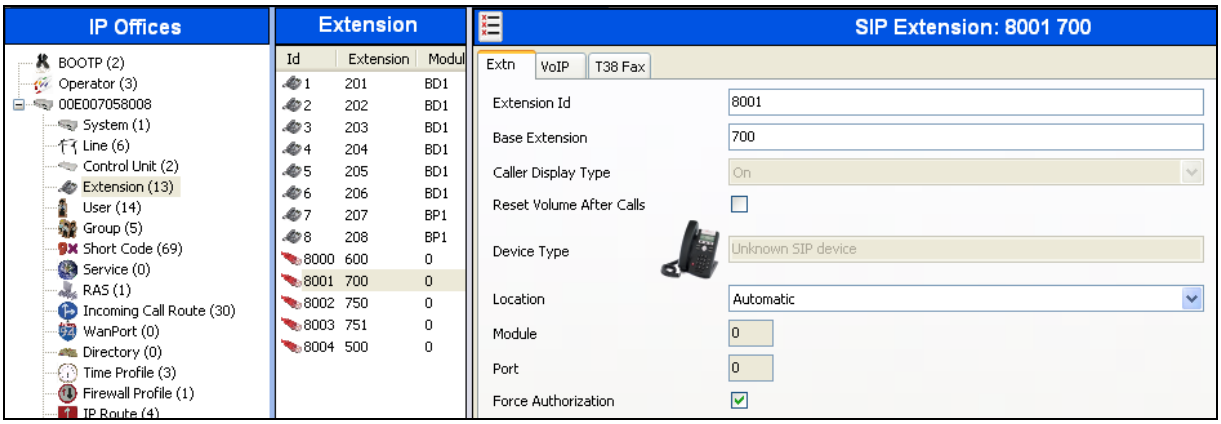
©2014 Avaya Inc. All Rights Reserved.

- **Telephony→ Supervisor Settings** tab (not shown)
    - The **Login Code** is the softphone login password.



2. Define an **Extension** for the Avaya IP Office Softphone.
    - **SIP Extension** tab (shown below)
        - The **Extension ID** is automatically assigned by Avaya IP Office (e.g., **8001**). The **Base Extension** field is manually populated with the desired extension (e.g., **700**).
    - **SIP Extension → VoIP** tab for extension 700 (not shown)
        - The **IP Address** default value is used (**0.0.0.0**).
        - In the reference configuration the **Codec Selection** parameter is set to **Custom**, and the same codec list used in **Section 5.5.3.1** is used.
        - Other fields may retain default values.

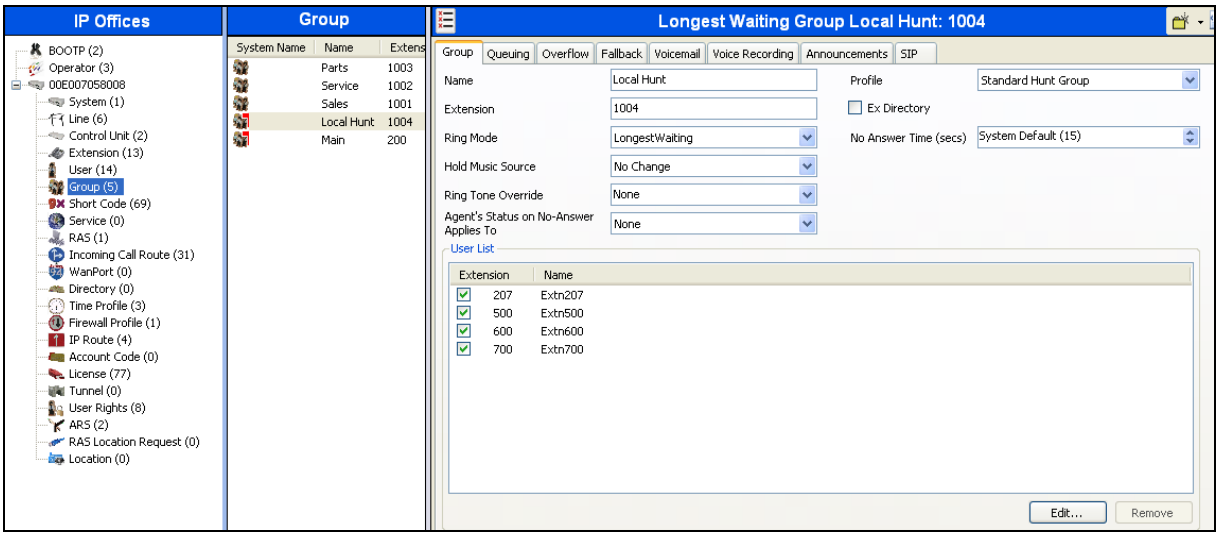
©2014 Avaya Inc. All Rights Reserved.



5.5.4. Hunt Groups

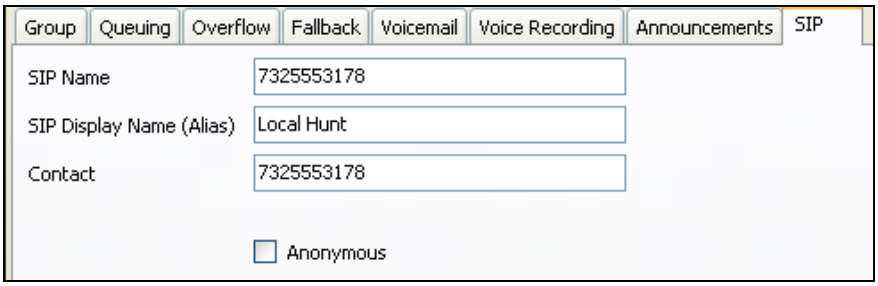
Users may also receive incoming calls as members of a hunt group. To configure a new hunt group, right-click **Group** from the Navigation pane and select **New** (not shown). To view or edit an existing hunt group, select **Group** from the Navigation pane, and the appropriate hunt group from the Group pane.

The following screen shows the **Group** tab for hunt group **1004**. This hunt group was configured to contain the Analog telephone (Extn207), the H.323 telephone (Extn500), SIP telephone (Extn600), and the SIP Softphone (Extn700). In the reference configuration, these telephone extensions are rung based on idle time, due to the **Ring Mode** setting **LongestWaiting**. Click the **Edit** button to change the **User List** included in the Hunt Group from the list of available users.



The following screen shows the **SIP** tab for hunt group **1004**. The **SIP Name** and **Contact** are configured with the AT&T DNIS number **7325553178**. In **Section 5.7**, an **Incoming Call Route** will map **5553178** to this hunt group (see the note in **Section 5.5.1** regarding incoming AT&T digits).

©2014 Avaya Inc. All Rights Reserved.



©2014 Avaya Inc. All Rights Reserved.

5.6. Short Codes

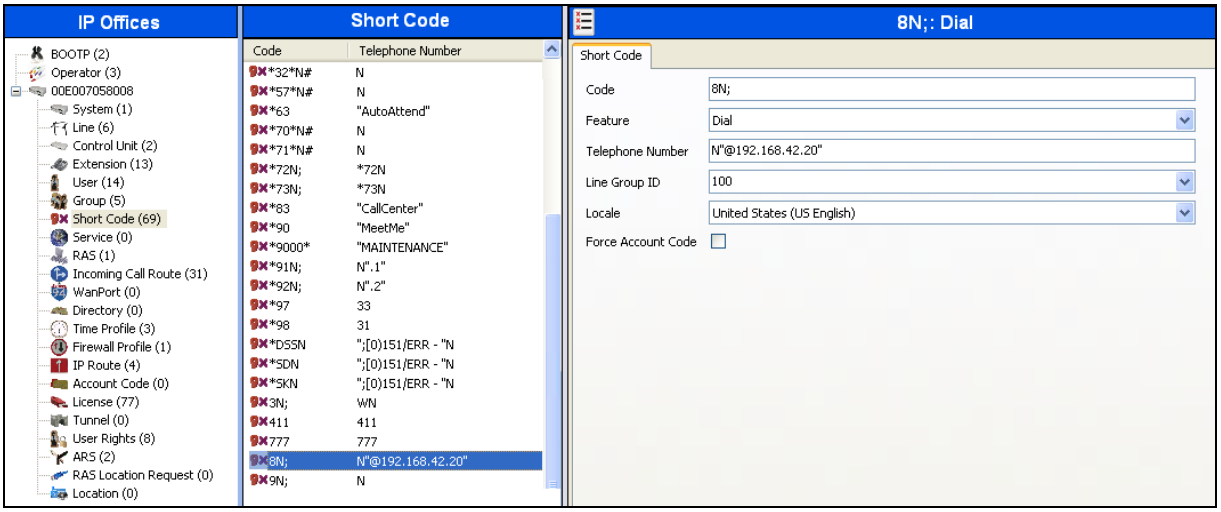
Avaya IP Office provides predefined Short Codes, however new Short Codes may be defined to match number strings to an action. To add a Short Code, right click on **Short Code** in the Navigation pane, and select **New** (not shown). To edit an existing Short Code, click **Short Code** in the Navigation pane, and the Short Code to be configured in the Group pane.

5.6.1. Short Code Direct Dialing (no ARS access)

In the screen shown below, the Short Code **8N;** is illustrated (note the semicolon at the end of the string). This Short Code will allow an Avaya IP Office user to dial the digit 8 followed by any telephone number, symbolized by the letter **N**, to reach the SIP Line to AT&T. The variable **N** can be any number such as a 10-digit number, a 1+10 digit number, a toll free number, directory assistance (e.g., 411), etc.

This Short Code does ***not*** use the ARS table. When users dial 8 plus the number, Avaya IP Office will wait for an end of dialing timeout then send a SIP INVITE.

- The **Code** parameter is set to **8N;**
- The **Feature** parameter is set to **Dial**
- The **Telephone Number** parameter is set to **N"@192.168.42.20"** with the text string beginning with @ in quotes. Address 192.168.42.20 is the "inside" SIP trunk interface (A1) IP address of the Avaya SBCE**.**
- The **Line Group ID** parameter is set to **100**, matching the number of the **Outgoing Group** configured on the **SIP URI** tab of **SIP Line 17** (see **Section 5.4.3**).
- Click the **OK** button (not shown).

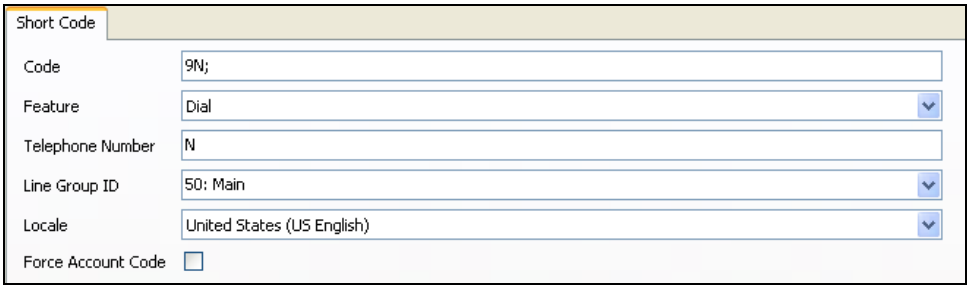


©2014 Avaya Inc. All Rights Reserved.

5.6.2. Short Code Dialing via Automatic Route Selection (ARS access)

In the screen shown below, the Short Code **9N;** is illustrated (note the semicolon at the end of the string). This simple 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 5.8**. The variable **N** can be any number such as a 10-digit number, a 1+10 digit number, a toll free number, directory assistance (e.g., 411), etc.

- 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 **50:Main** (default value provided by Avaya IP Office), which directs the call to ARS.
- Click the **OK** button (not shown).



Other short codes were also defined in the reference configuration:

- **3N;** = Outbound dialing with privacy (see **Section 5.6.3**).
- ***17** = Access VoiceMail Pro (see **Section 5.6.4.1**).
- ***63** = Access to the Auto Attendant provisioned on Voicemail Pro (see **Section 5.6.4.2**).
- ***97** = Mobile Call Back (see **Section 5.6.4.3.1**).
- ***98** = Mobile Call Control (see **Section 5.6.4.3.2**).

5.6.3. Privacy Dialing

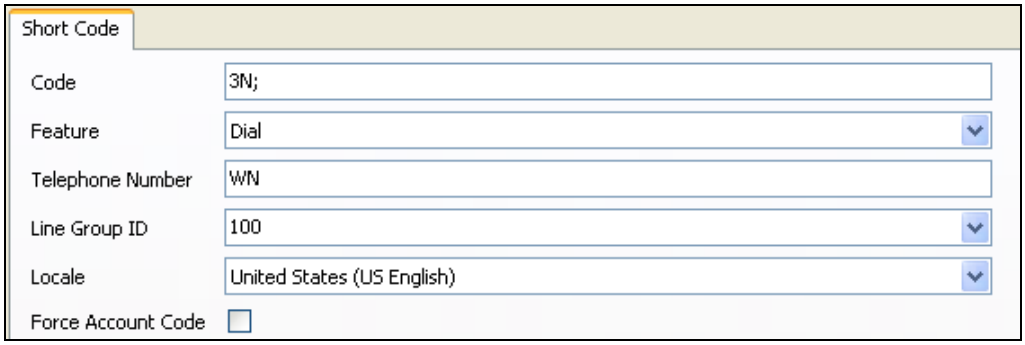
Optionally, add a Short Code that can be used to access the SIP Line anonymously. In the screen shown below, the Short Code **3N;** is illustrated. This code is similar to the **9N;** code. The **Telephone Number** field begins with the letter **W,** which means "withhold the outgoing calling line identification".

Note - When a user dials 3 plus the number, Avaya IP Office will include the user's telephone number in the **P-Asserted-Identity** (PAI) header along with a **Privacy** header of **Id**. The **From** and **Contact** headers will contain **Anonymous**.

- The **Code** parameter is set to **3N;**
- The **Feature** parameter is set to **Dial**
- The **Telephone Number** parameter is set to **WN"@192.168.42.20"**.

©2014 Avaya Inc. All Rights Reserved.

- The **Line Group ID** parameter is set to **100**, matching the number of the **Outgoing Group** configured on the **SIP URI** tab of **SIP Line 17** (see **Section 5.4.3**).
- Click the **OK** button (not shown).



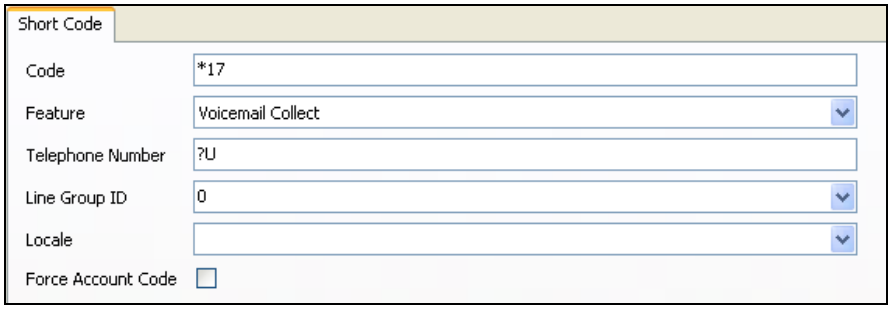
5.6.4. Feature Dialing

Optionally, add a Short Code that can be used to access Avaya IP Office features directly.

5.6.4.1 Voicemail Access

- To access the VoiceMail Pro system directly, the code ***17** is defined. This Short Code will be used as one means to allow an AT&T DNIS number to be programmed to route directly to voice messaging (via inclusion of this Short Code as the destination of an **Incoming Call Route** in **Section 5.7**).

- **Feature** = **Voicemail Collect**
- **Telephone Number** = **?U**
- **Line Group** = **0**

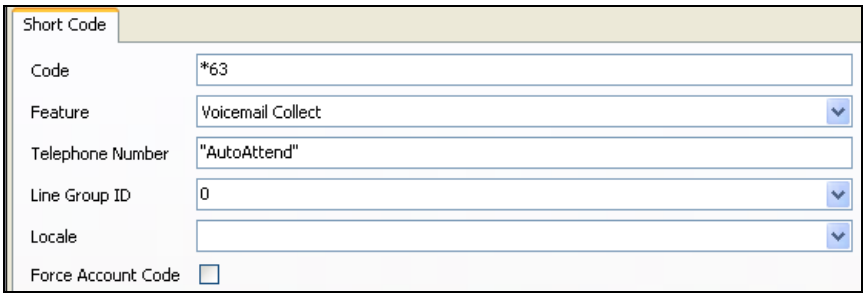


5.6.4.2 Auto Attendant Access

In the reference configuration an Auto Attendant was defined on VoiceMail Pro (see **Section 5.9**). This Auto Attendant is accessed via code *63.

- **Feature** = **Voicemail Collect**
- **Telephone Number** = **"AutoAttend"**
- **Line Group** = **0**

©2014 Avaya Inc. All Rights Reserved.



5.6.4.3 Feature Name Extension (FNE) Access

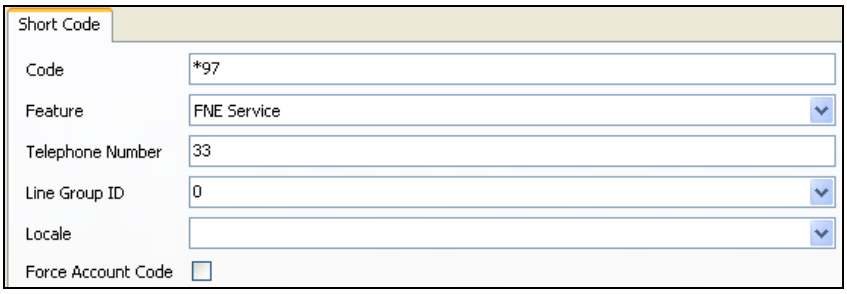
Two Avaya IP Office Mobility features, **Mobile Call Control** and **Mobile Callback**, are shown as examples of Feature Name Extension (FNE) Access.

5.6.4.3.1 Mobile Callback

The following screen illustrates the **Code *97** which is defined for **Feature** = **FNE Service** and **Telephone Number** = **33** for the Avaya IP Office Mobility feature **Mobile Callback** (note that 33 is predefined in Avaya IP Office for this feature). Code, ***97** was used as the destination of an Incoming Call Route for an AT&T DNIS number. This enabled DID calls from a configured twinning destination to be dialed, and then hung up by the caller while hearing ring back. Avaya IP Office will then call the caller back using the number defined in the **User → Mobility → Twinned Mobile Number** field (see **Section 5.5.2**), via AT&T IPFR-EF service.

Note that for this feature to work, the inbound calling number information must match the number provisioned in the associated **User → Mobility → Twinned Mobile Number**. For example, in **Section 5.5.2** the number **91*7325550037*** was defined as the Twinning number for the H.323 set. Therefore, the inbound calling number must match ***7325550037*.**

- **Feature** = **FNE Service**
- **Telephone Number** = **33**
- **Line Group** = **0**

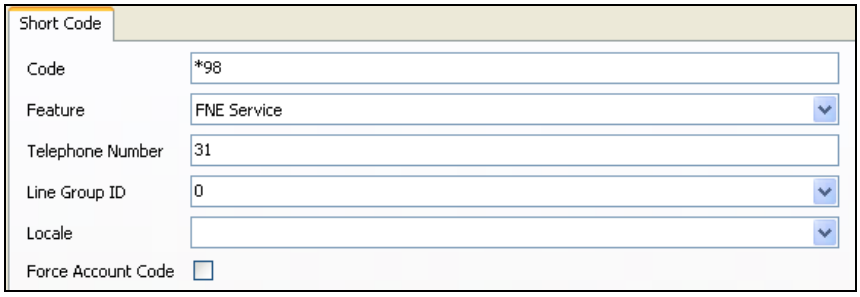


©2014 Avaya Inc. All Rights Reserved.

5.6.4.3.2 Mobile Call Control

The following screen illustrates another Mobility Short Code. In this case, the **Code *98** is defined for **Feature** = **FNE Service** and **Telephone Number** = **31** for the Avaya IP Office Mobility feature **Mobile Call Control** (note that 31 is predefined in Avaya IP Office for this feature). Code ***98** was used as the destination of an Incoming Call Route for an AT&T DNIS number. This enabled DID access to Mobile Call Control from configured twinning destinations, allowing the mobile user to make calls as if the calls were made from the user's Avaya IP Office extension in the office.

- **Feature** = **FNE Service**
- **Telephone Number** = **31**
- **Line Group** = **0**



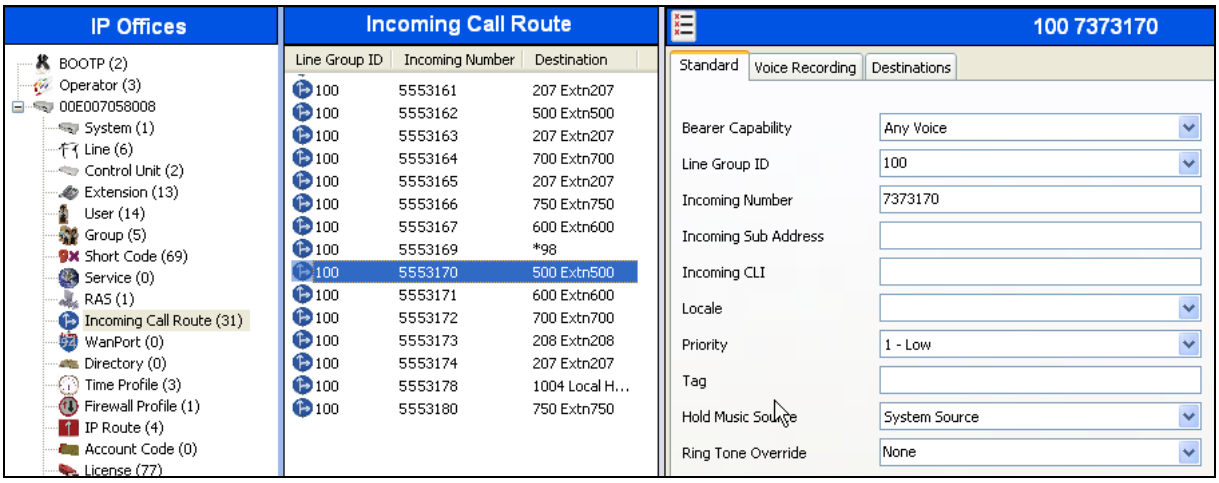
5.7. Incoming Call Routes

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.

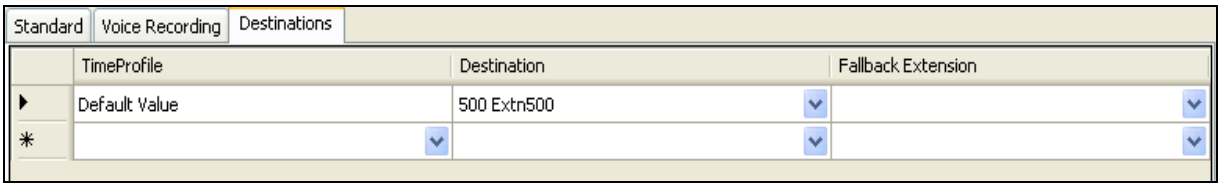
Note – In the reference configuration, although a ten digit AT&T access number is dialed in the PSTN, the AT&T IPFR-E service delivered seven DNIS digits in the R-URI. Therefore incoming calls to Avaya IP Office will match on the seven digit inbound AT&T DNIS string (e.g., **5553170**).

In the screen shown below, the incoming call route for **Incoming Number → 5553170** is illustrated. The **Line Group ID** is set to **100**, matching the **Incoming Group** field configured in the **SIP URI** tab for the SIP Line to the Avaya SBCE/AT&T in **Section 5.4.3**.

©2014 Avaya Inc. All Rights Reserved.



Select the **Destinations** tab. From the **Destination** drop-down, select the extension to receive the call when AT&T delivers DNIS digits **5553170**. In the reference configuration DNIS digits **5553170** is associated with Avaya IP Office User **Extn500** (the 1608 H.323 telephone).



Repeat this process to route all AT&T DNIS numbers to their associated Avaya IP Office destinations (phones, Hunt Groups, Short Codes, etc).

Note - The **Destination** drop down menu may not contain all desired destinations (e.g., Short Codes for feature access as described in **Section 5.6**). In these cases the desired destination may be manually typed into the **Destination** field.

5.8. Automatic Route Selection (ARS) and Alternate Routing

While detailed coverage of ARS is beyond the scope of these Application Notes, this section includes basic ARS screen illustrations and considerations, including alternate routing should the SIP Line be out of service or temporarily not responding.

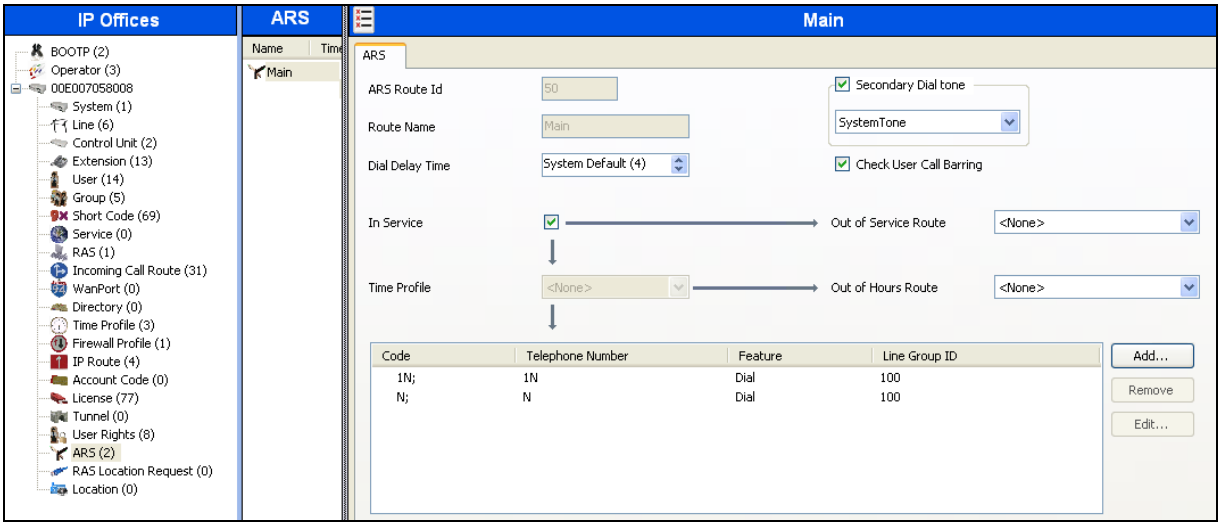
With ARS, secondary dial tone can be provided after the access code, time-based routing criteria can be introduced, and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not available. Although not shown in this section, ARS also facilitates more specific dialed telephone number matching, enabling immediate routing and alternate treatment for different types of numbers following the access code.

©2014 Avaya Inc. All Rights Reserved.

As described in **Section 5.6.2**, 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.

The following screen shows an example ARS configuration for the route **Main** (ARS Route ID 50). The **In Service** parameter refers to the ARS form itself, not the SIP Line Group(s) that may be referenced in the form. If the **In Service** box is un-checked, calls are routed to the ARS route specified in the **Out of Service Route** parameter.

- Entry **1N;** means that any dialed string beginning with 1 (e.g. 1xxxyyyxxxx) will be routed to Line Group 100 (SIP Line 17).
- Entry **N;** means that any dialed string will be routed to Line Group 100 (SIP Line 17).



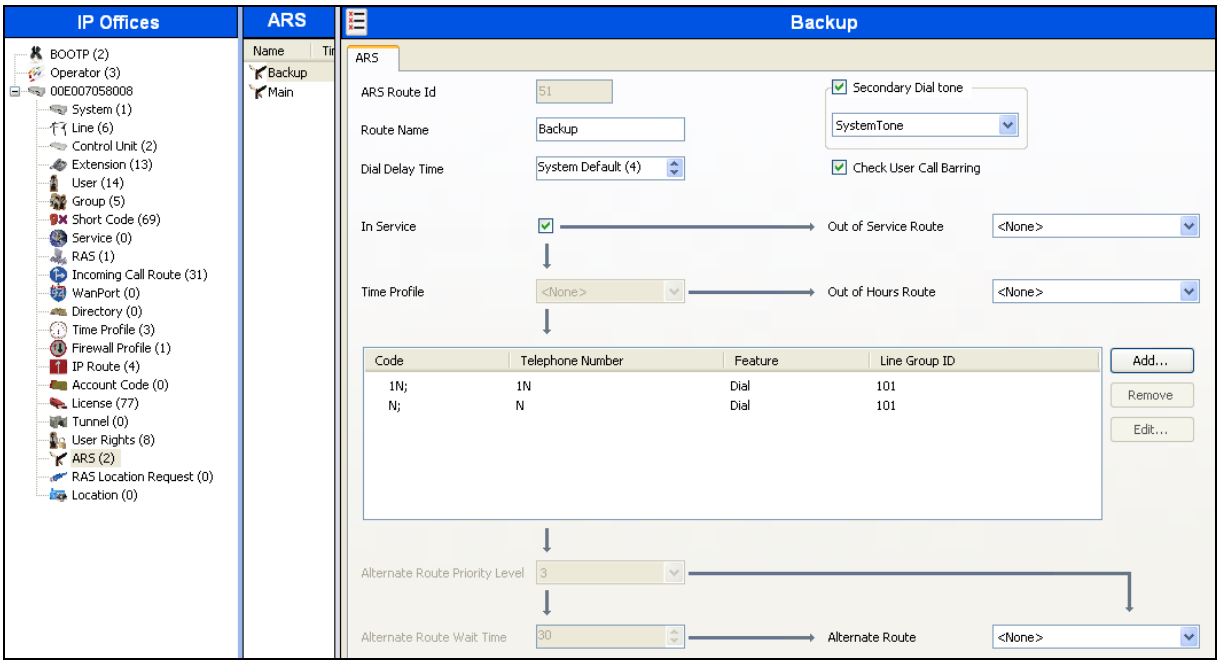
Since alternate routing can be considered a privilege not available to all callers, Avaya IP Office can control access to the alternate route by comparing the calling user's priority to the value in the **Alternate Route Priority Level** field.

Assuming the primary route is in-service, the number passed from the Short Code used to access ARS (e.g., **9N;** in **Section 5.6.2**) can be further analyzed to direct the call to a specific Line Group ID. Per the example screen above, if the user dialed 9-1-732-555-1212, the call would be directed to Line Group 100. If Line Group 100 cannot be used, the call can automatically route to the route name configured in the **Alternate Route** parameter in the lower right of the screen (**Backup**).

The following screen shows an example ARS configuration for the route named **Backup** (ARS **Route ID 51**). If the user dialed 9-1-732-555-1212, and the call could not be routed via the primary route **Main** described above, the call will be delivered to this **Backup** route. Per

©2014 Avaya Inc. All Rights Reserved.

the configuration shown below, the call would be delivered to Line Group **101** (e.g., an additional SIP Line used for backup purposes, not shown). The configuration of the **Code**, **Telephone Number**, **Feature**, and **Line Group ID** for an ARS route is similar to the configuration already shown for Short Codes in **Section 5.6**.



If a primary route experiences a network outage such that no response is received to an outbound INVITE, Avaya IP Office routes the call via the alternate route. The user receives an audible tone when the re-routing occurs and may briefly see "Waiting for Line" on the display. The redirection will occur if a call is made right after a failure of the primary route, as Avaya IP Office has not yet marked the SIP Line out of service as a result of no response to SIP OPTIONS. Alternatively calls can be delivered via the alternate route when the primary route is manually marked out-of-service, or known to be out-of-service due to prior failure of SIP OPTIONS.

5.9. Auto Attendant (via Avaya IP Office Voicemail Pro)

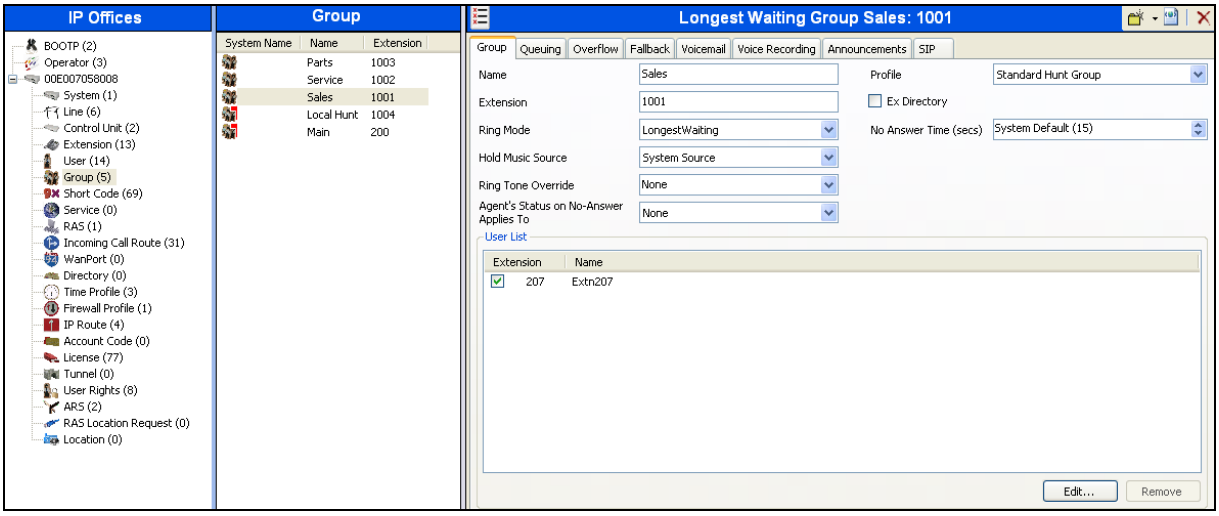
In the reference configuration, Avaya IP Office Voicemail Pro (running on a Windows 2003 server), is used for Voicemail processing. The Avaya IP Office Voicemail Pro provides for basic Auto Attendant functionality.

Note - While Avaya IP Office Voicemail Pro provisioning and programming is beyond the scope of this document, a sample Auto Attendant basic configuration is shown below.

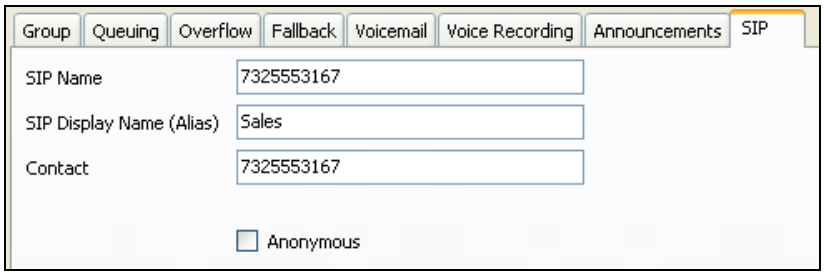
In the reference configuration an Auto Attendant was provisioned to prompt callers to select a numeric option (1, 2, or 3), that would forward the call to an associated Avaya IP Office extension (207, 500, and 600). This is accomplished via the following steps:

©2014 Avaya Inc. All Rights Reserved.

1. Via Avaya IP Office Manager interface, follow the steps in **Section 5.5.4**, and create hunt groups for "Sales", "Service", and "Parts".
    - In the **Hunt Group** tab, enter:
        i. **Name** = **Sales**
        ii. **Extension** = **1001**
        iii. **Ring Mode** = **Sequential**
        iv. **User List** = Extension **207**
        v. Let all other values default.



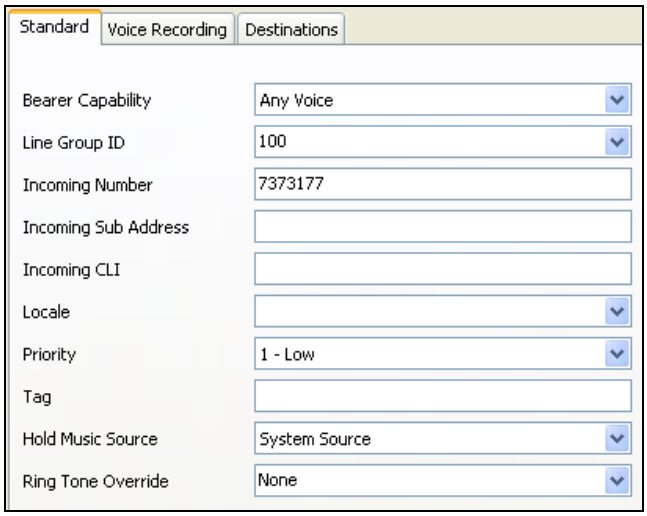
    - In the SIP tab, enter:
        i. **SIP Name** = **7325553167**
        ii. **SIP Display Name** = **Sales**
        iii. **Contact** = **7325553167**

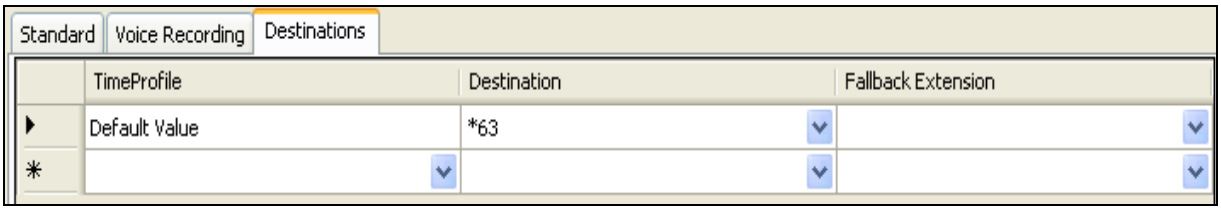


    - Repeat the above steps to create the **Service** hunt group (group extension **1002** and associated with phone extension **500**) and the **Parts** hunt group (group extension **1003** and associated with phone extension **600**).

2. Following the steps shown in **Section 5.6.4.2**, create a Short Code for the Auto Attendant.
3. Following the steps shown in **Section 5.7**, create an Incoming Call Route that maps an AT&T DID to Short Code *63 (e.g., the AT&T DID 7373177).

©2014 Avaya Inc. All Rights Reserved.

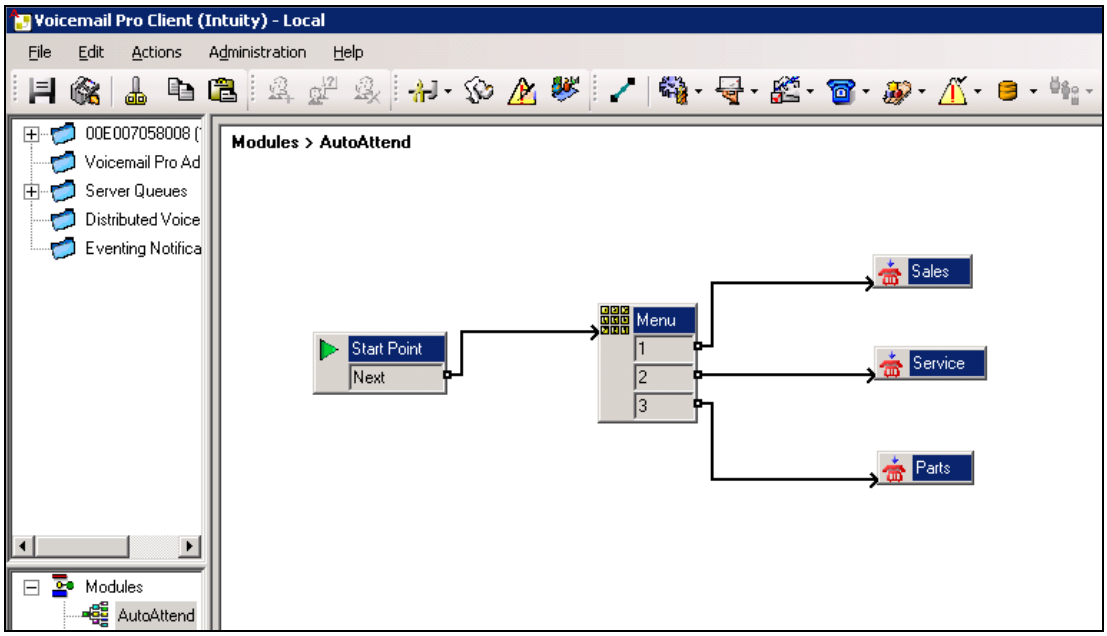




4. Via the Voicemail Pro GUI interface:
   - Create **Start Point** (**Modules → Add**), **Menu** , and **Transfer** objects.
     i. **Start Point** object properties (let all other fields default)
        1. **General** tab, **Token Name** = **Start Point**
     ii. **Menu** object properties (let all other fields default)
        1. **General** tab, **Token Name** = **Menu**
        2. **Entry Prompt** tab, Create an **Entry Prompt** that will tell the caller what digits to press to reach Sales, Service, and Parts (e.g., **attendant.wav**). To modify an existing recording, double click on the .wav file and rerecord. If no .wav files exist, double click on the to open the .wav editor.
        3. **Touch Tone** tab, Select **1, 2,** and **3** as the possible entry digits.
     iii. **Transfer** Object "**Sales**" properties
        1. **General** tab, **Token Name** = **Sales**
        2. **Specific** tab, **Destination → Mailbox → Sales**
     iv. **Transfer** Object **"Service**" properties
        1. **General** tab, **Token Name** = **Service**
        2. **Specific** tab, **Destination → Mailbox → Service**
     v. **Transfer** Object "**Parts**" properties
        1. **General** tab, **Token Name** = **Parts**
        2. **Specific** tab, **Destination → Mailbox → Parts**
   - Select the Connector icon and:

©2014 Avaya Inc. All Rights Reserved.

i. Drag a connecting flow line from the **Start Point** box to the **Menu** box (see screen shot below).
ii. Drag connecting flow lines from each of the **Menu** options to their associated **Transfer** boxes (see screen shot below).



5. From the top menu select **File → Save & Make Live**, or select the icon.

When the associated AT&T IPFR-EF number is called from PSTN (e.g., 3145555304 from step **3**), the caller will be prompted to enter 1, 2, or 3 to access Sales, Service, or Parts. The associated Avaya IP Office extension (e.g., 207, 500, or 600) will then ring.

5.10. Privacy / Anonymous Calls

As described in **Section 5.6**, an Avaya IP Office user can request privacy by dialing the Short Code **3N;** to access the SIP Line. The Avaya 1600-Series IP Telephones can also request privacy for a specific call, without dialing a unique Short Code, using **Features → Call Settings → Withhold Number**, on the phone itself. Specific users may be configured to always withhold calling line identification by checking the **Anonymous** field in the **SIP** tab for the user.

5.11. SIP Options Frequency

Avaya IP Office periodically checks the health of the SIP Line by sending a SIP OPTIONS message, based on the Binding Refresh Time. In the reference configuration, the **Binding Refresh Time** (see **Section 5.3.2**) is set to 120 (sec). In **Section 5.4**, the SIP Line to the Avaya SBCE/AT&T has the **Check OOS** box checked. As a result Avaya IP Office will send OPTIONS to AT&T, via the Avaya SBCE, every two minutes. If there is no response, Avaya IP Office can mark the trunk out of service. Although ARS (as shown in **Section 5.8**) can include alternate routes to complete calls even if the far-end is not responding, Avaya IP

©2014 Avaya Inc. All Rights Reserved.

Office must wait for the outbound INVITE to timeout before route advance. Once the SIP OPTIONS maintenance recognizes that the SIP Line is out-of-service, new calls will no longer be delayed before route advance. Also, once the problem with the SIP Line is resolved, the SIP OPTIONS maintenance will automatically bring the link back to the in-service state. In addition, for secure networks, the periodic sending of OPTIONS by Avaya IP Office *may* serve to keep network Firewall "pinholes" open preventing the blockage of inbound traffic to Avaya IP Office.

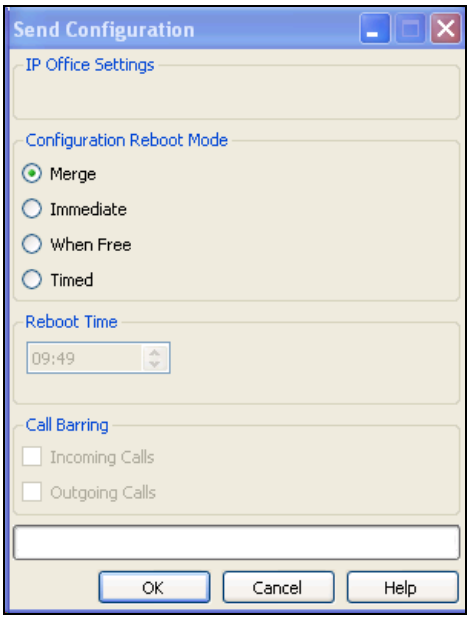
Note - In the reference configuration, the AT&T IPFR-EF service sends OPTIONS to Avaya IP Office, via the Avaya SBCE, every 60 seconds. The receipt of these OPTIONS has the effect of resetting the **Binding Refresh Time** interval (the receipt confirms that the SIP Trunk is working). Therefore Avaya IP Office never sends the OPTIONS to AT&T.

5.12. Saving Configuration Changes to Avaya IP Office

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. At the top of the Avaya IP Office Manager page click **File → Save Configuration** (if that option is grayed out, no changes are pending).

A screen similar to the following will appear, with either **Merge** or **Immediate** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Immediate** option will save the configuration and cause the Avaya IP Office server to reboot.

Click **OK** to execute the save.



The active configuration may be saved to a file at any time by selecting **File → Save Configuration As**.

©2014 Avaya Inc. All Rights Reserved.

6. Configure Avaya Session Border Controller for Enterprise

Note - Only the Avaya SBCE provisioning required for the reference configuration is described in these Application Notes.

6.1. Initial Installation/Provisioning

Note - The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to reference **[7]** and **[8]** for additional information.

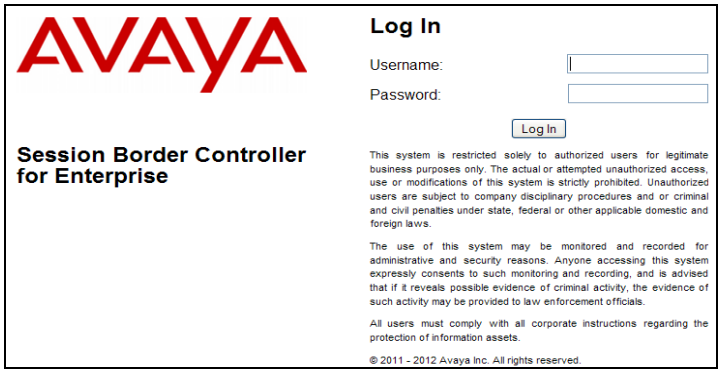
IMPORTANT! – During the Avaya SBCE installation, the Management interface, (labeled "M1"), of the Avaya SBCE <u>must</u> be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative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

The Avaya SBCE installation typically defines public and private networks. As described in **Section 3**, the reference configuration defines the Avaya SBCE private interface A1 (IP address 192.168.42.20) on the same CPE network as the IP Office LAN1 interface (IP address 192.168.42.1). The connection to AT&T used the Avaya SBCE public interface B1 (IP address 10.10.10.10[5]).

6.2. Log into the Avaya SBCE

The follow provisioning is performed via the Avaya SBCE GUI interface, using the "M1" management LAN connection on the chassis.

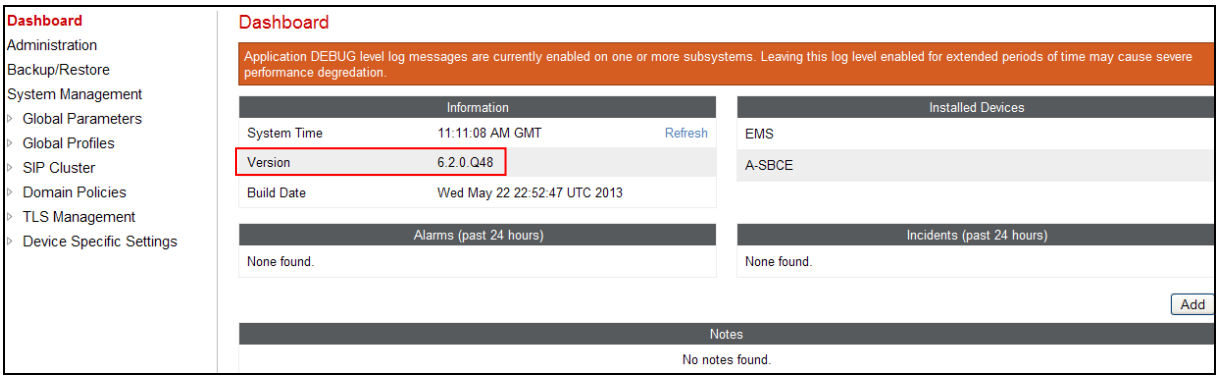
1. Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the **Username** and **Password**.



3. The main menu window will open. Note that the installed software version is displayed.

[5] See footnote 1 in **Section 3.2.1**

©2014 Avaya Inc. All Rights Reserved.



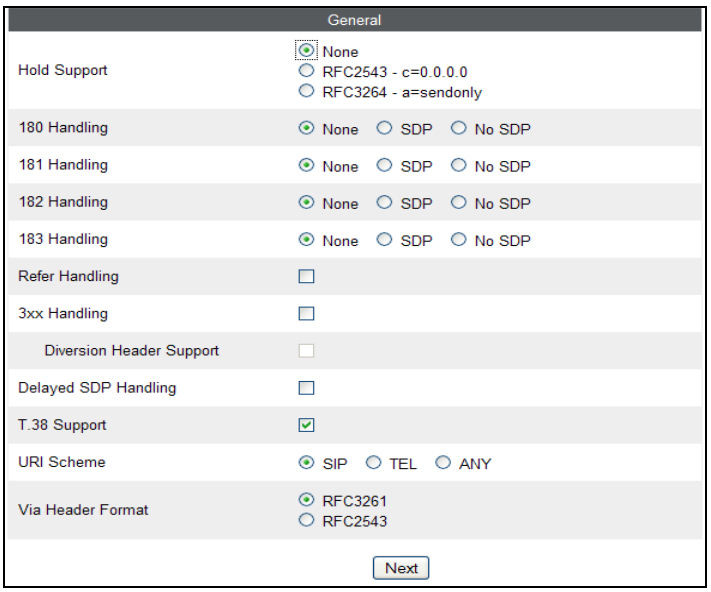
6.3. Global Profiles

Global Profiles allow for configuration of parameters across the Avaya SBCE appliances.

6.3.1. Server Interworking – to Avaya IP Office

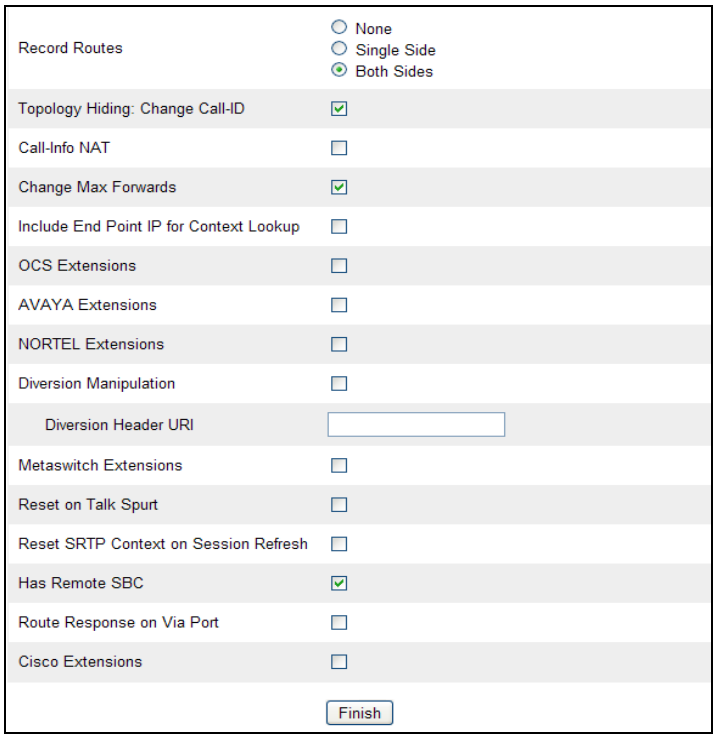
Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the connection to Avaya IP Office via the "DMZ" network.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Interworking** (not shown).
3. Select the **Add** button (not shown) and the **Profile** name window will open (not shown).
4. Enter profile name: (e.g., **Avaya_SI**), and click **Next**.
5. The **General** screen will open.
    a. Check **T38 Support**.
    b. All other options can be left with default values
    c. Click **Next**

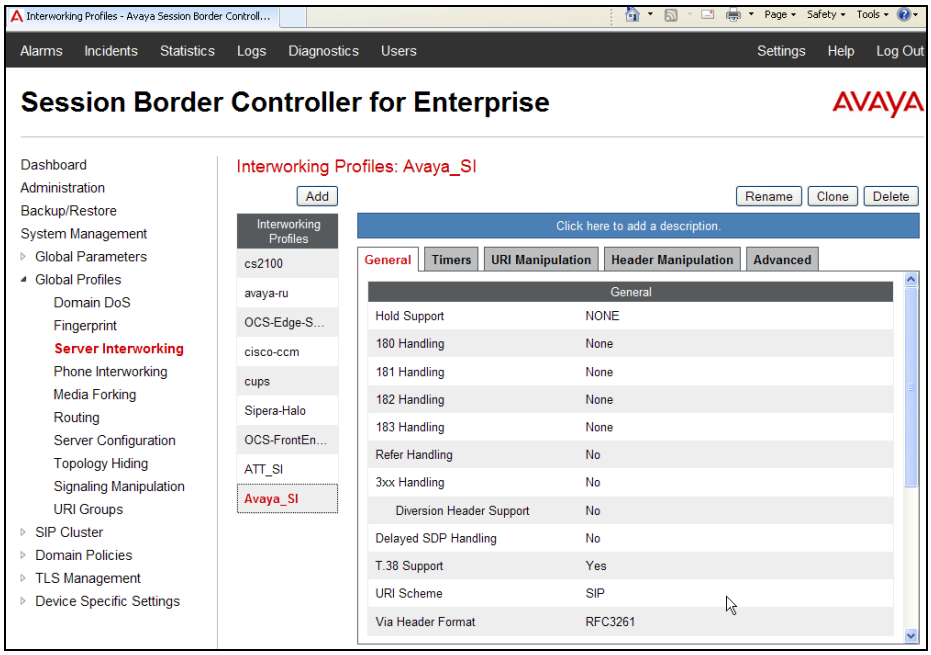


©2014 Avaya Inc. All Rights Reserved.

6. On the **Privacy/DTMF** window (not shown), select **Next** to accept default values.
7. On the **SIP Timers/Transport Timers** window (not shown), select **Next** to accept default values.
8. On the **Advanced** tab, accept the default values, and click **Finish**.



The following screenshot shows the completed **General** tab form.



©2014 Avaya Inc. All Rights Reserved.

6.3.2. Server Interworking – to AT&T

Repeat the steps shown in **Section 6.3.1** to add an Interworking Profile for the connection to AT&T via the public network.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Interworking**.
3. Select **Add Profile**.
4. On the **General** Tab (not shown):
    a. Enter a profile name**:** (e.g., **ATT_SI**)
    b. Check **T38 Support**
    c. All other options can be left as default.
    d. Click **Next**
5. At the **Privacy** tab (not shown), select **Next** to accept default values.
6. At the **Interworking Profile** tab (not shown), select **Next** to accept default values.
7. On the last screen (**Advanced** options, not shown), accept the default values, and click **Finish**.

6.3.3. Routing – to Avaya IP Office

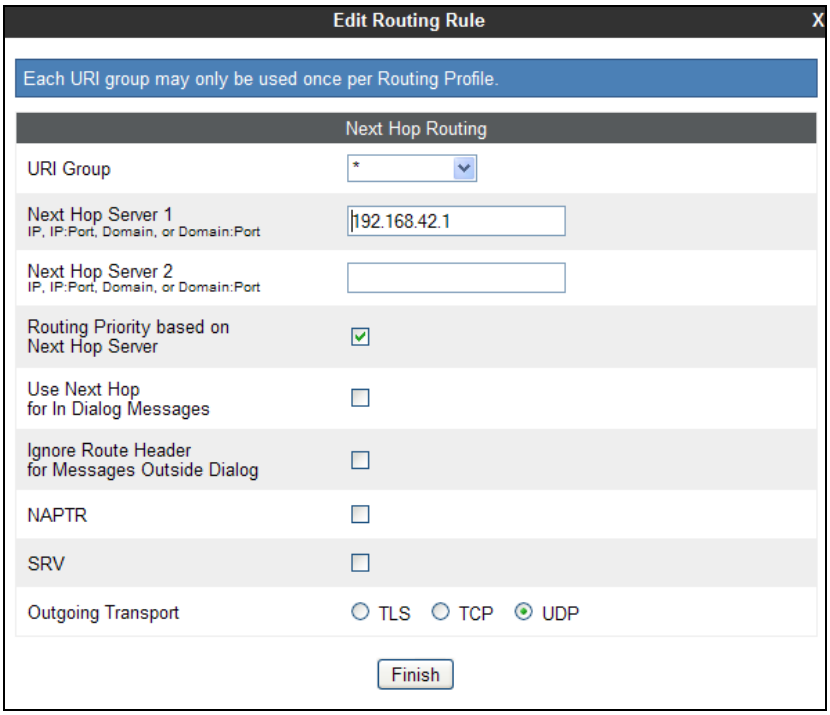
The Routing Profile allows users to manage parameters related to routing SIP signaling messages. This provisioning defines the Routing Profile for the connection to Avaya IP Office.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select the **Routing** tab (not shown).
3. Select **Add Profile** (not shown).
4. Enter **Profile Name**: (e.g., **Avaya_RP)**.
5. Click **Next** and enter:
    a. **Next Hop Server 1**: **192.168.42.1** (Avaya IP Office LAN1 IP address)
    b. Verify **Routing Priority Based on Next Hop Server** is selected (default).
    c. **Outgoing Transport**: **UDP**

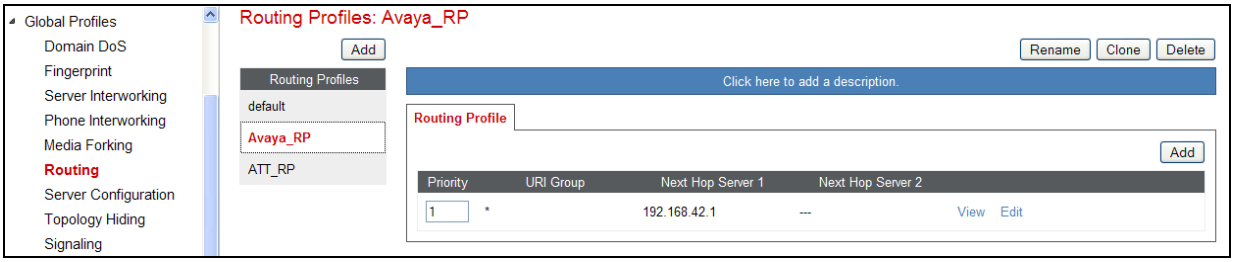
    > **Note** – UDP is the recommended protocol to use on the connection between the Avaya SBCE and IP Office. However TCP may be used if necessary.

    d. Accept remaining default values
6. Click **Finish**.

©2014 Avaya Inc. All Rights Reserved.



The following screenshot shows the completed **Routing Profiles** form.



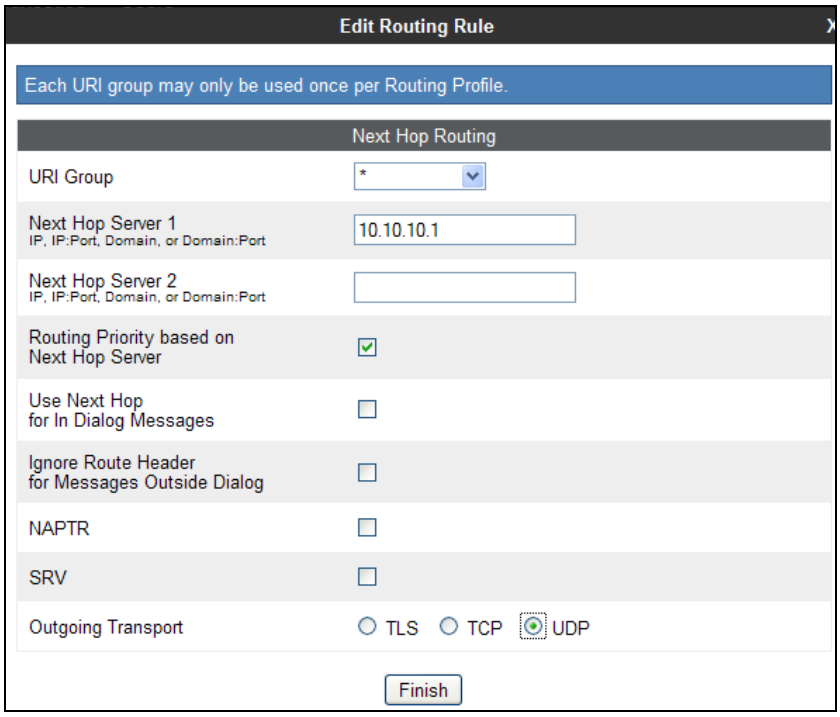
6.3.4. Routing – to AT&T

Repeat the steps in **Section 6.3.3**, with the following changes, to add a Routing Profile for the connection to AT&T.

1. Enter Profile Name: (e.g., **ATT_RP)**.
2. Click **Next**, then enter the following:
   a. **Next Hop Server 1: 10.10.10.1** (Primary AT&T Border Element IP address[6])
   b. Verify **Routing Priority Based on Next Hop Server** is selected (default).
   c. **Outgoing Transport**: **UDP**
3. Click **Finish**.

[6] See footnote 1 in **Section 3.2.1**

©2014 Avaya Inc. All Rights Reserved.



6.3.5. Server Configuration – Avaya IP Office

This section defines the Server Configuration for the connection to Avaya IP Office. The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow users to configure and manage various SIP server-specific parameters such port assignments, IP Server type, heartbeat signaling parameters and some advanced options.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**.
3. Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **Avaya_SC**) and click **Next**.
4. The **Add Server Configuration Profile - General** window will open (not shown).
   a. Select **Server Type**: **Call Server**
   b. **IP Address**: **192.168.42.1** (Avaya IP Office LAN1 IP Address)
   c. **Supported Transports**: Check **UDP**
   d. **UDP Port**: **5060**

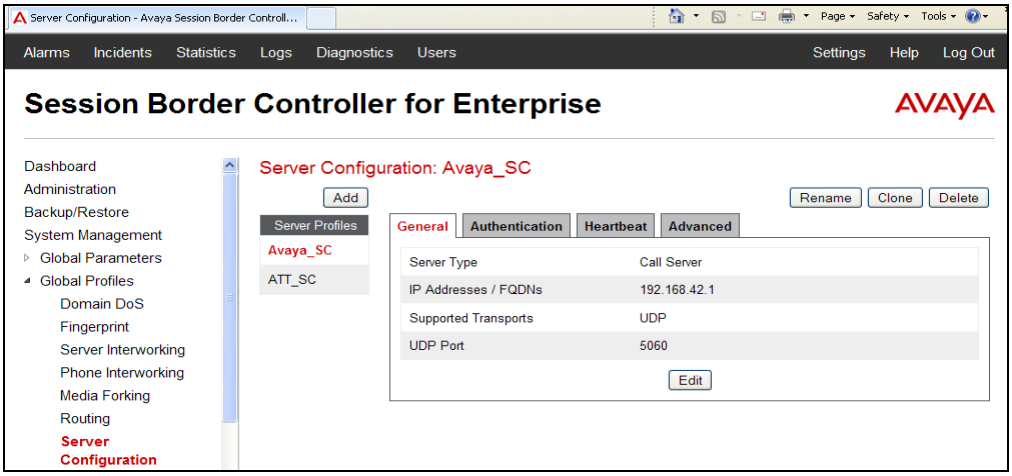
   > **Note** – UDP is the recommended protocol to use on the connection between the Avaya SBCE and Avaya IP Office for SIP Trunking. However TCP may be used if necessary.

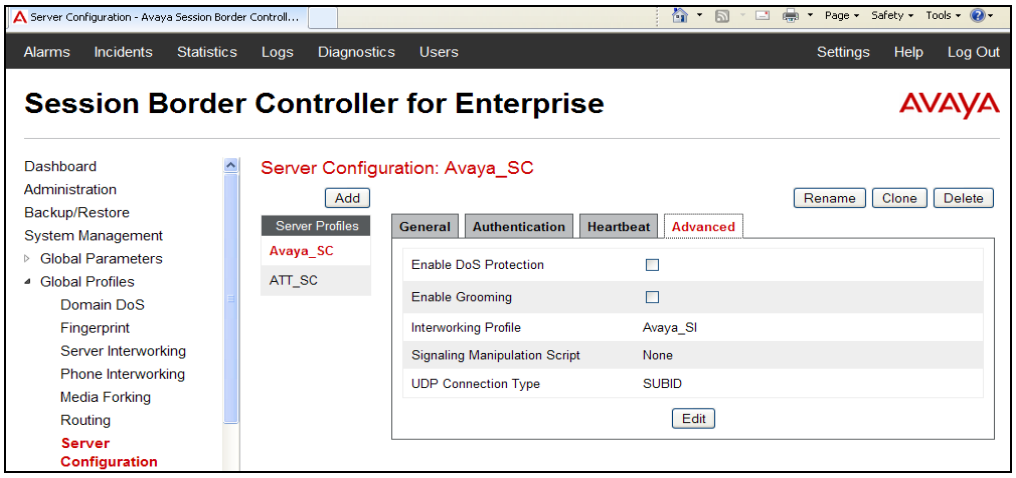
   e. Select **Next**
5. The **Add Server Configuration Profile - Authentication** window will open (not shown).
   a. Select **Next** to accept default values.
6. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
   a. Select **Next** to accept the default values.
7. The **Add Server Configuration Profile - Advanced** window will open.

©2014 Avaya Inc. All Rights Reserved.

a. Select **Avaya_SI** (created in **Section 6.3.1**), for **Interworking Profile**.
b. In the **Signaling Manipulation Script** field select **none.**
c. Select **Finish**.

The following screen shots show the completed **General** and **Advanced** tabs, that are displayed after **Finish** has been selected for each.





6.3.6. Server Configuration – AT&T

Repeat the steps in **Section 6.3.5**, with the following changes, to create a Server Configuration for the connection to AT&T.

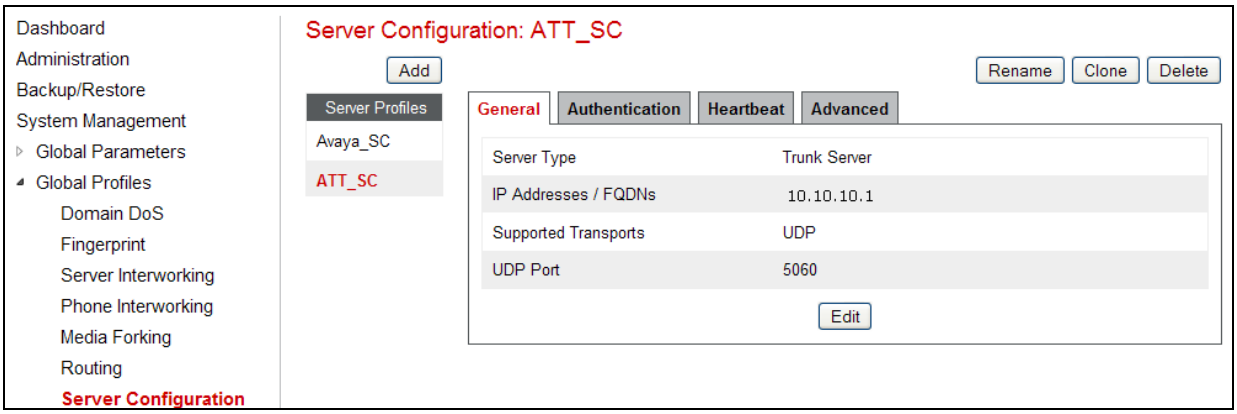
1. Select **Server Configuration**.
2. Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **ATT_SC**) and select **Next**.
3. The **Add Server Configuration Profile - General** window will open (not shown).
   a. Select Server Type**: Trunk Server**

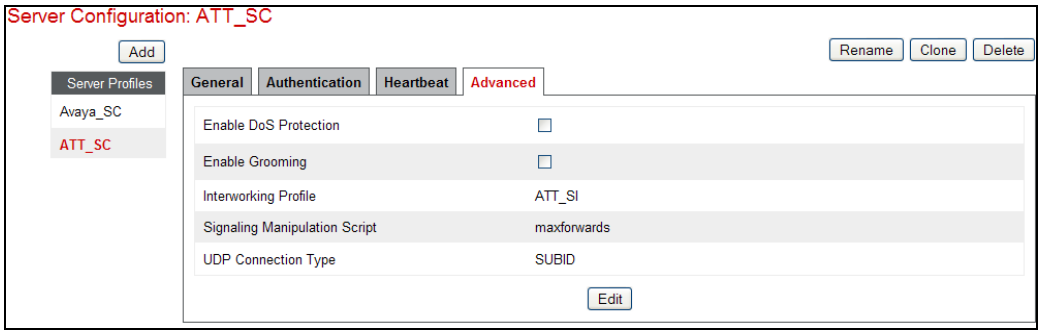
©2014 Avaya Inc. All Rights Reserved.

b. **IP Address: 10.10.10.1** (AT&T Border Element IP address[7])
c. **Supported Transports**: Check **UDP**
d. **UDP Port: 5060**
e. Select **Next**.

4. The **Add Server Configuration Profile - Advanced** window will open.
   d. Select **ATT_SI** (created in **Section 6.3.2**), for **Interworking Profile**.
   e. In the **Signaling Manipulation Script** field select **maxforwards** (see **Section 6.3.9**).
   a. Select **Finish**.

The following screen shots show the completed **General** and **Advanced** tabs, that are displayed after **Finish** has been selected for each.





6.3.7. Topology Hiding – Avaya IP Office

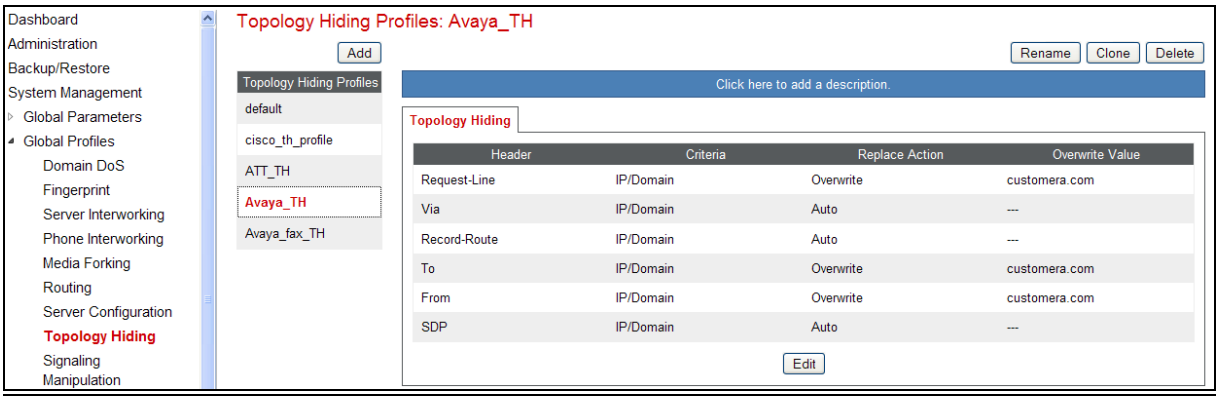
The **Topology Hiding** screen allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Topology Hiding**.

[7] See footnote 1 in **Section 3.2.1**

©2014 Avaya Inc. All Rights Reserved.

3. Click **default** profile and select **Clone Profile** (not shown).
4. Enter Profile Name: (e.g., **Avaya_TH**)
5. For the Header **To**,
    a. In the **Criteria** column select **IP/Domain**
    b. In the **Replace Action** column select **Overwrite**
    c. In the **Overwrite Value** column enter **customera.com**
6. For the Header **Request Line**,
    a. In the **Criteria** column select **IP/Domain**
    b. In the **Replace Action** column select **Overwrite**
    c. In the **Overwrite Value** column enter **customera.com**
7. For the Header **From**,
    a. In the **Criteria** column select **IP/Domain**
    b. In the **Replace Action** column select **Overwrite**
    c. In the **Overwrite Value** column enter **customera.com**
8. Use default values for rest of the fields.
9. Click **Finish**.



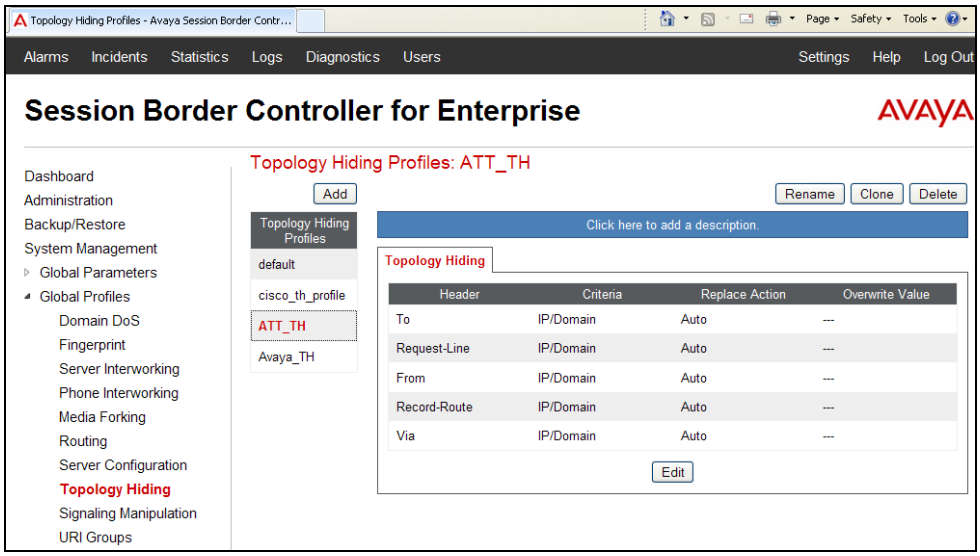
6.3.8. Topology Hiding – AT&T

Repeat the steps in **Section 6.3.7,** with the following changes, to create a Topology Hiding Profile for the connection to AT&T.

1. Enter Profile Name: (e.g., **ATT_TH**).
2. Set all **Replace Action** fields to **Auto** (**Overwrite Values** will be blank).
3. Click **Finish**.

The following screen shot shows the completed **Topology Hiding Profile** form, displayed after **Finish** has been selected.

©2014 Avaya Inc. All Rights Reserved.



6.3.9. Signaling Manipulation

The AT&T IPFR-E network sends OPTIONS with the parameter maxforwards: 0. The Avaya SBCE logs these as "Max Forwards Exceeded" in the platform incident log. To alleviate this, a Signaling Manipulation script was written to modify the maxforwards value to 45.

1. Navigate to **Global Profiles → Signaling Manipulation**, and click on the **Add** button (not shown).
2. Enter a name for the script (e.g., **maxforwards**).
3. Enter the following script, and click on **Save**.

Title maxforwards Save

```
within session "OPTIONS"

{
    act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
    {
        if (exists(%HEADERS["Max-Forwards"][1])) then
        {
            %HEADERS["Max-Forwards"][1] = "45";
        }
    }
}
```

This script is applied to the **ATT_SC** Server Configuration (see **Section 6.3.6**).

6.4. Domain Policies

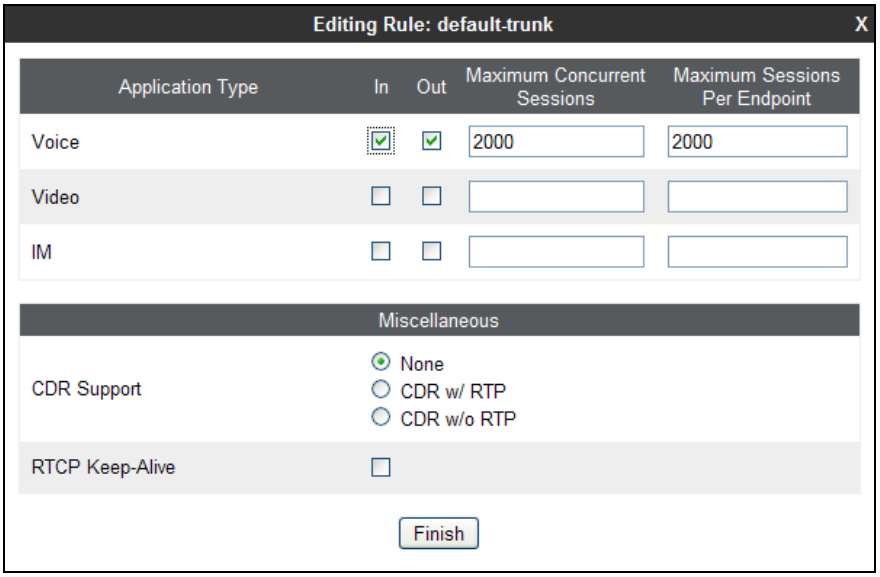
The Domain Policies feature allows users to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

6.4.1. Application Rules

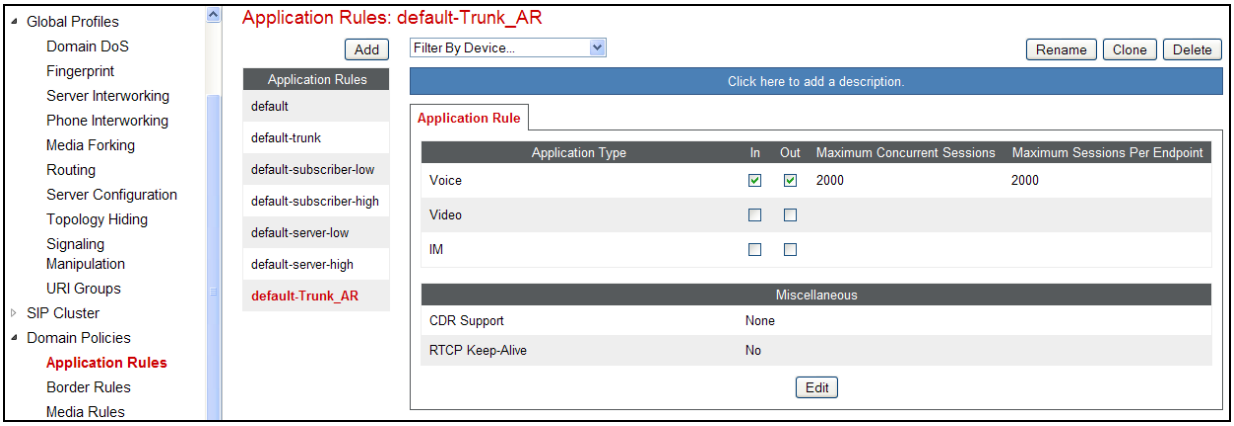
1. Select **Domain Policies** from the menu on the left-hand side (not shown).
2. Select the **Application Rules** (not shown).
3. Select the **default** Rule (not shown).

©2014 Avaya Inc. All Rights Reserved.

4. Select the **Clone** button (not shown), and the **Clone Rule** window will open.
    a. In the **Clone Name** field enter **default-trunk_AR**
    b. Click **Finish.** The newly created rule will be displayed.
5. Select the **default-trunk** rule just created (not shown).
    a. Click the **Edit** button. The **Editing Rule** screen will be displayed.
    b. In the **Voice** row:
        i. Change the **Maximum Concurrent Sessions** to **2000**
        ii. Change the **Maximum Sessions per Endpoint** to **2000**



    c. Click on **Finish.** The completed **Application Rules** screen is shown below.

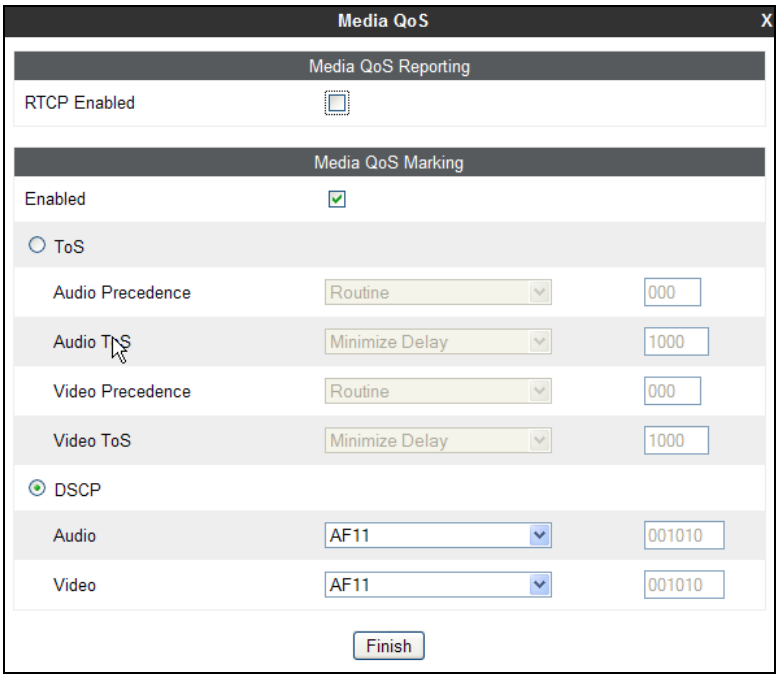


©2014 Avaya Inc. All Rights Reserved.

6.4.2. Media Rules

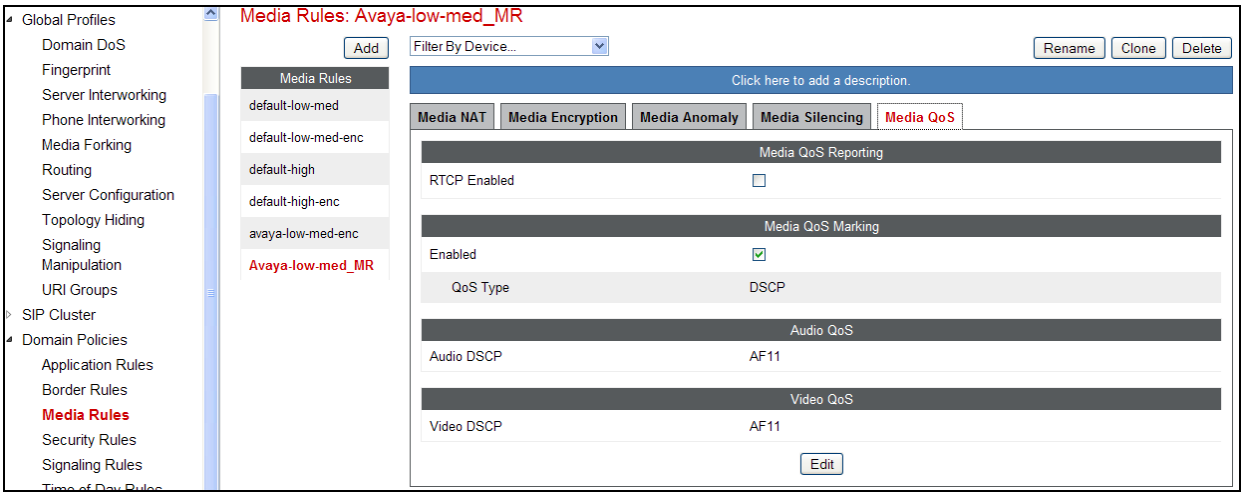
This Media Rule will be applied to both directions and therefore, only one rule is needed.

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Media Rules** (not shown).
3. The Media Rules window will open (not shown). From the Media Rules menu, select the **default-low-med** rule
4. Select **Clone** button (not shown), and the **Clone Rule** window will open.
    a. In the **Clone Name** field enter **Avaya-low-med_MR**
    b. Click **Finish.** The newly created rule will be displayed.
5. Highlight the **Avaya-low-med_MR** rule just created (not shown):
    a. Select the **Media QOS** tab (not shown).
    b. Click the **Edit** button and the **Media QOS** window will open.
    c. Check the **Media QOS Marking** field is **Enabled.**
    d. Select the **DSCP** box.
    e. **Audio**: Select **AF11** from the drop-down.
    f. **Video**: Select **AF11** from the drop-down.



6. Click **Finish.** The completed **Media Rules** screen is shown below.

©2014 Avaya Inc. All Rights Reserved.

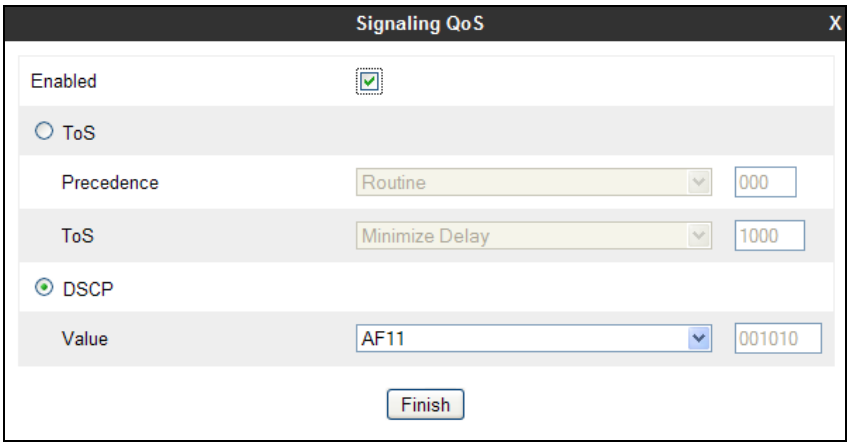


6.4.3. Signaling Rules

In the reference configuration, Signaling Rules are used to define QOS parameters. In addition, they may be used to remove or block various SIP headers.

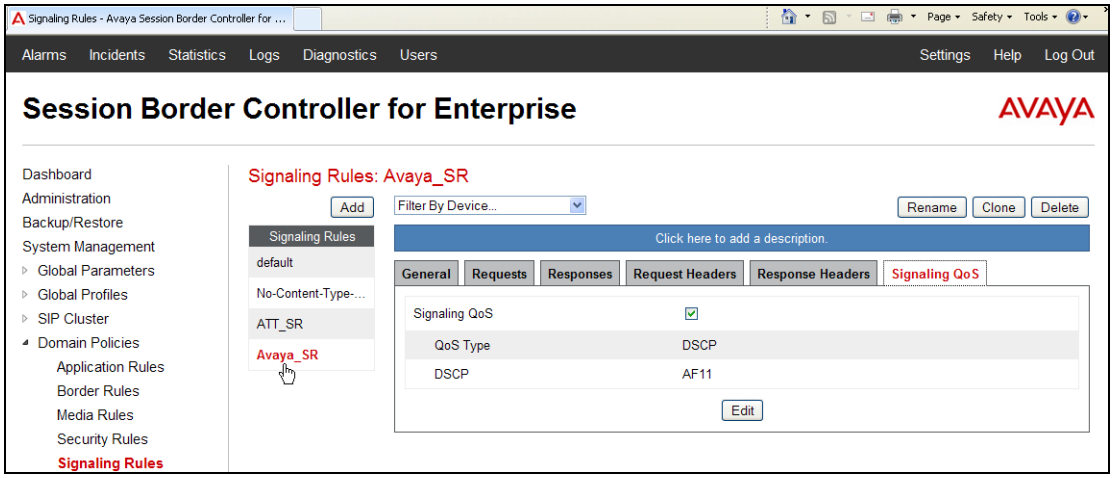
6.4.3.1 Avaya – Signaling QOS

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Signaling Rules** (not shown).
3. The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
4. Select the **Clone** button and the **Clone Rule** window will open (not shown).
   - In the **Rule Name** field enter **Avaya_SR**
   - Click **Finish.** The newly created rule will be displayed.
5. Highlight the **Avaya_SR** rule created in step **4** and enter the following:
   - Select the **Signaling QOS** tab.
   - Click the **Edit** button and the **Signaling QOS** window will open.
   - Verify that **Signaling QOS** is selected.
   - Select **DCSP**.
   - Select **Value** = **AF11**.



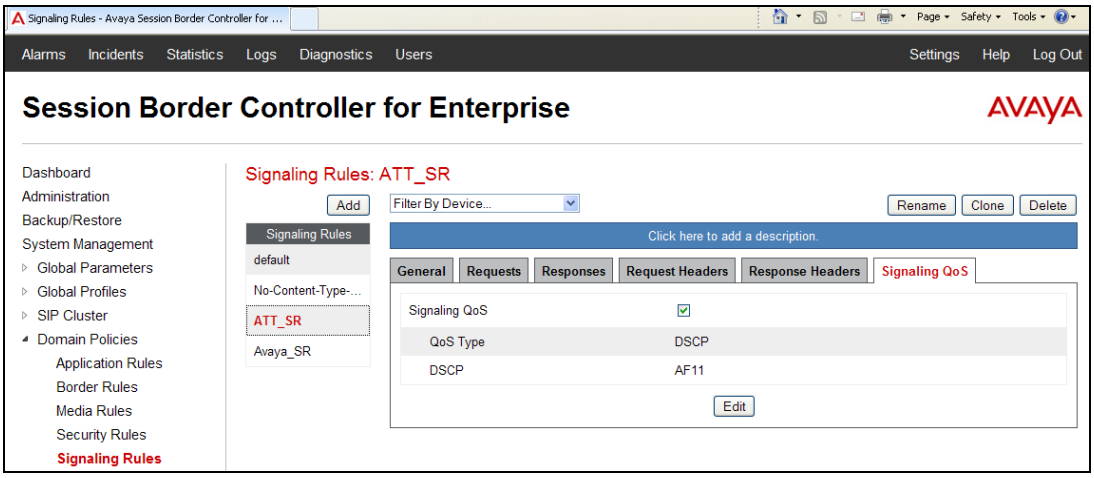
©2014 Avaya Inc. All Rights Reserved.

6. Click **Finish.** The completed **Signaling Rules** screen is shown below.



6.4.3.2 AT&T – Signaling QOS

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Signaling Rules** (not shown).
3. The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
4. Select the **Clone** button and the **Clone Rule** window will open (not shown).
   - In the **Rule Name** field enter**: ATT_SR**
   - Click **Finish.** The newly created rule will be displayed.
5. Highlight the **ATT_SR** rule created in step **4** and repeat steps **5** and **6** from **Section 6.4.3.1**.

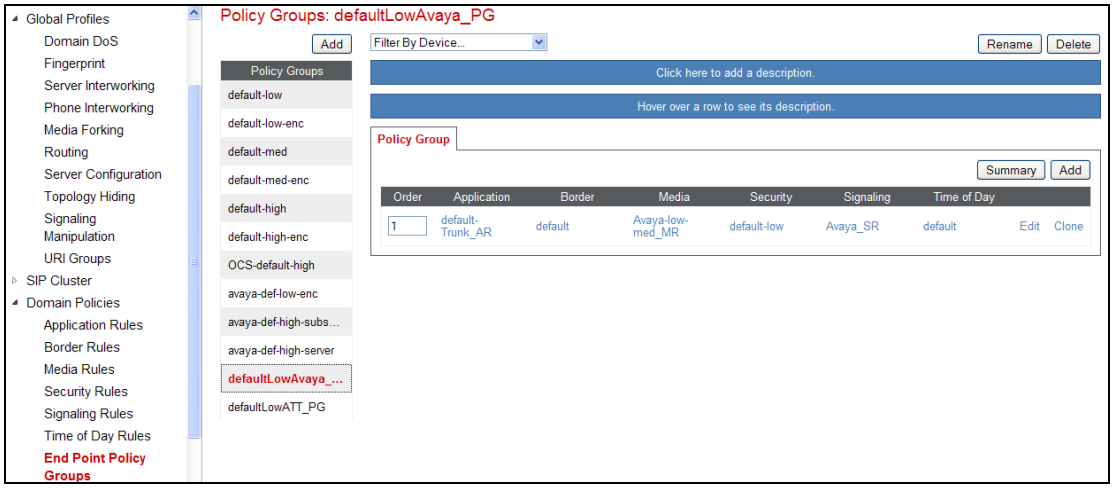


©2014 Avaya Inc. All Rights Reserved.

6.4.4. Endpoint Policy Groups – Avaya IP Office

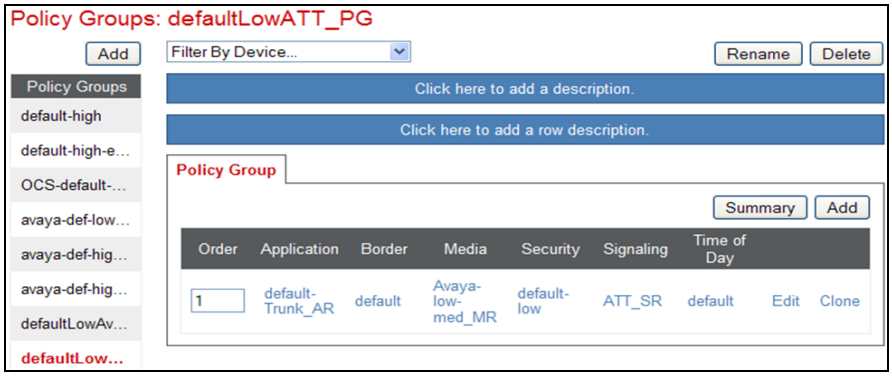
1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
   a) **Name**: **defaultLowAvaya_PG**
   b) **Application Rule**: **default-Trunk_AR** (created in **Section 6.4.1**)
   c) **Border Rule**: **default**
   d) **Media Rule**: **Avaya-low-med_MR** (created in **Section 6.4.2**)
   e) **Security Rule**: **default-low**
   f) **Signaling Rule**: **Avaya_SR** (created in **Section 6.4.3**)
   g) **Time of Day**: **default**
4. Select **Finish** (not shown)

The completed **Policy Groups** screen is shown below.



6.4.5. Endpoint Policy Groups – AT&T

1. Repeat steps **1** through **4** from **Section 6.4.4** with the following changes:
   a. **Group Name**: **defaultLowATT_PG**
   b. **Signaling Rule**: **ATT_SR** (created in **Section 6.4.3**
2. **Select Finish** (not shown)



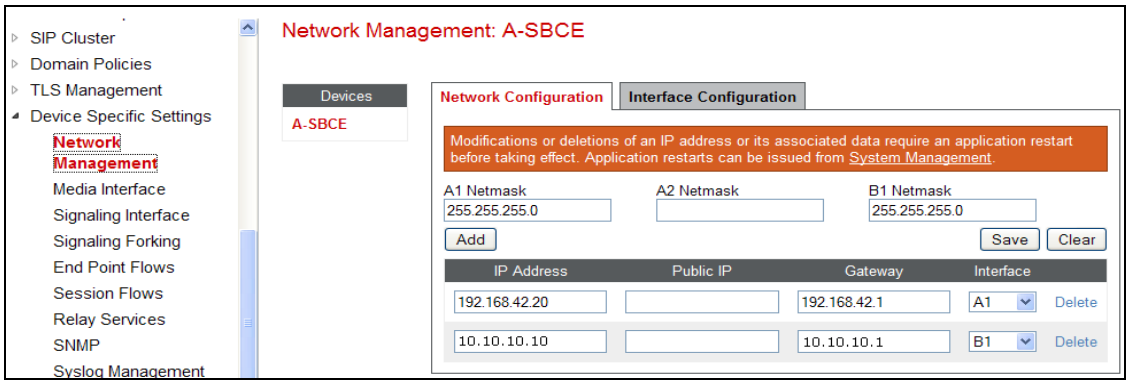
©2014 Avaya Inc. All Rights Reserved.

6.5. Device Specific Settings

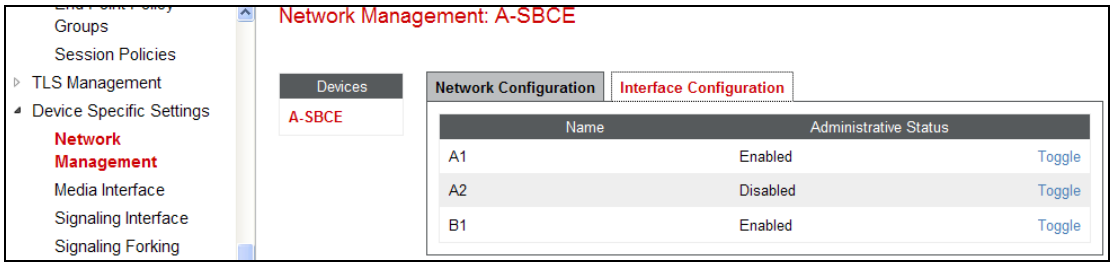
The **Device Specific Settings** feature for SIP allows users to view system information, and manage various device-specific network parameters such as port ranges.

6.5.1. Network Management

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Network Management**
   a) The network interfaces are defined during installation. However if these values need to be modified, do so via this tab.



3. In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration** tab.

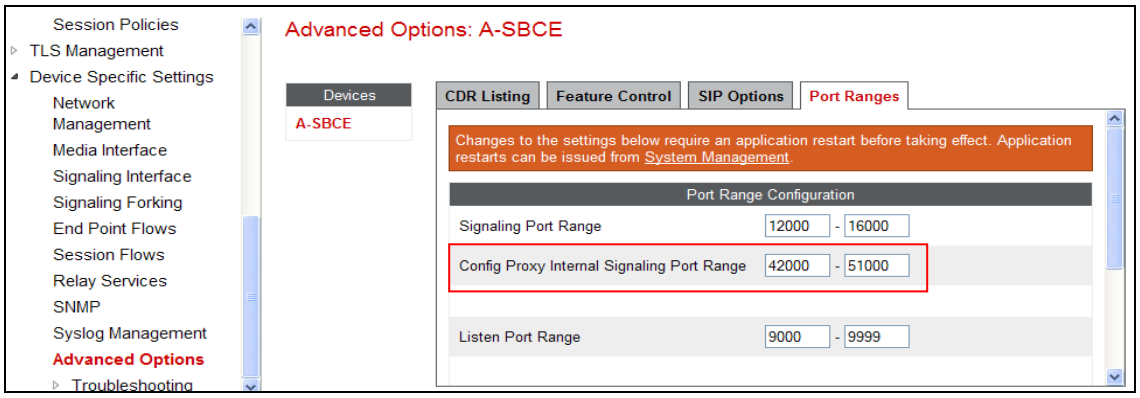


6.5.2. Advanced Options

In **Section 6.5.3**, the media UDP port ranges required by AT&T are set (**16384 – 32767**). 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 used.

1. Select **Device Specific Settings → Advanced Options** from the menu on the left-hand side.
2. Select the **Port Ranges** tab.
3. In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.
4. Scroll to the bottom of the window and select **Save** (not shown).

©2014 Avaya Inc. All Rights Reserved.

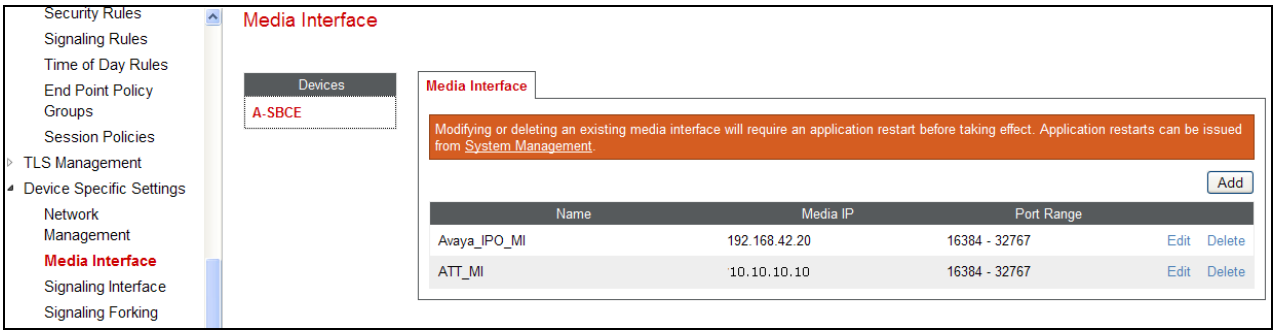


6.5.3. Media Interfaces

The AT&T IPFR-EF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, but only the outside is required by the AT&T IPFR-EF service.

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface** (not shown).
3. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
   a) **Name**: **Avaya_IPO_MI**
   b) **IP Address**: **192.168.42.20** (Avaya SBCE A1 address to IP Office)
   c) **Port Range**: **16384 - 32767**
4. Click **Finish** (not shown).
5. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
   a) **Name**: **ATT_MI**
   b) **IP Address**: **10.10.10.10** (Avaya SBCE B1 address toward AT&T[8])
   c) **Port Range**: **16384 - 32767**
6. Click **Finish** (not shown).

The completed **Media Interface** screen is shown below.



[8] See footnote 1 in **Section 3.2.1**

©2014 Avaya Inc. All Rights Reserved.

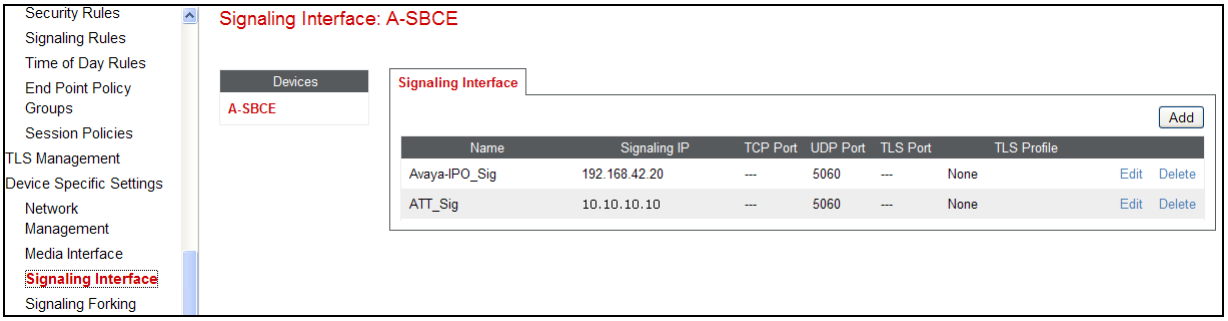
6.5.4. Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface** (not shown).
3. Select **Add** (not shown) and enter the following:
   a) **Name**: **Avaya-IPO_Sig**
   b) **IP Address**: **192.168.42.20** (Avaya SBCE A1 address to IP Office)
   c) **UDP Port**: **5060**

Note – UDP is the recommended protocol to use on the connection between the Avaya SBCE and IP Office. However TCP may be used if necessary.

4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
   a) **Name**: **ATT_Sig**
   d) **IP Address**: **10.10.10.10** (Avaya SBCE B1 address toward AT&T[9])
   b) **UDP Port**: **5060**
6. Click **Finish** (not shown).

The completed **Signaling Interface** screen is shown below.



6.5.5. Endpoint Flows – Avaya IP Office

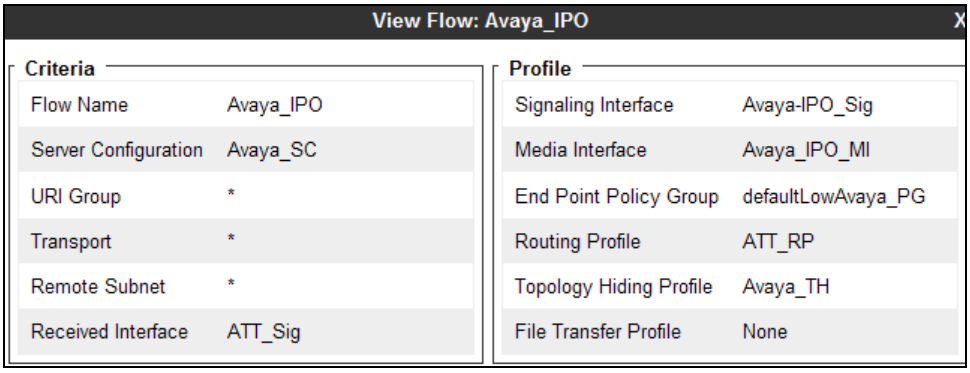
1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Endpoint Flows** (not shown).
3. Select the **Server Flows** tab (not shown).
4. Select **Add**, (not shown) and enter the following:
   a) **Name**: **Avaya_IPO**
   b) **Server Configuration**: **Avaya_SC** (**Section 6.3.5**)
   c) **URI Group**: *****
   d) **Transport**: *****
   e) **Remote Subnet**: *****
   f) **Received Interface**: **ATT_Sig**
   g) **Signaling Interface**: **Avaya-IPO_Sig** (**Section 6.5.4**)
   h) **Media Interface**: **Avaya_IPO_MI** (**Section 6.5.3**)
   i) **End Point Policy Group**: **defaultLowAvaya_PG** (**Section 6.4.4**)
   j) **Routing Profile**: **ATT_RP** (**Section 6.3.4**)

[9] See footnote 1 in **Section 3.2.1**

©2014 Avaya Inc. All Rights Reserved.

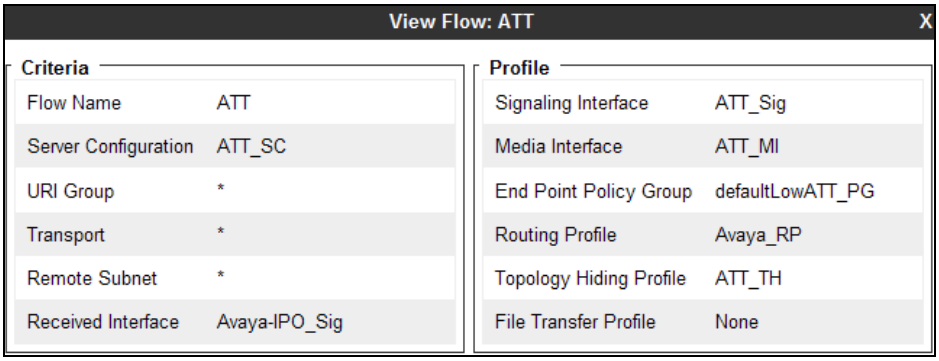
k) **Topology Hiding Profile**: **Avaya_TH** (**Section 6.3.7**)
l) **File Transfer Profile**: **None**

5. Click **Finish**.



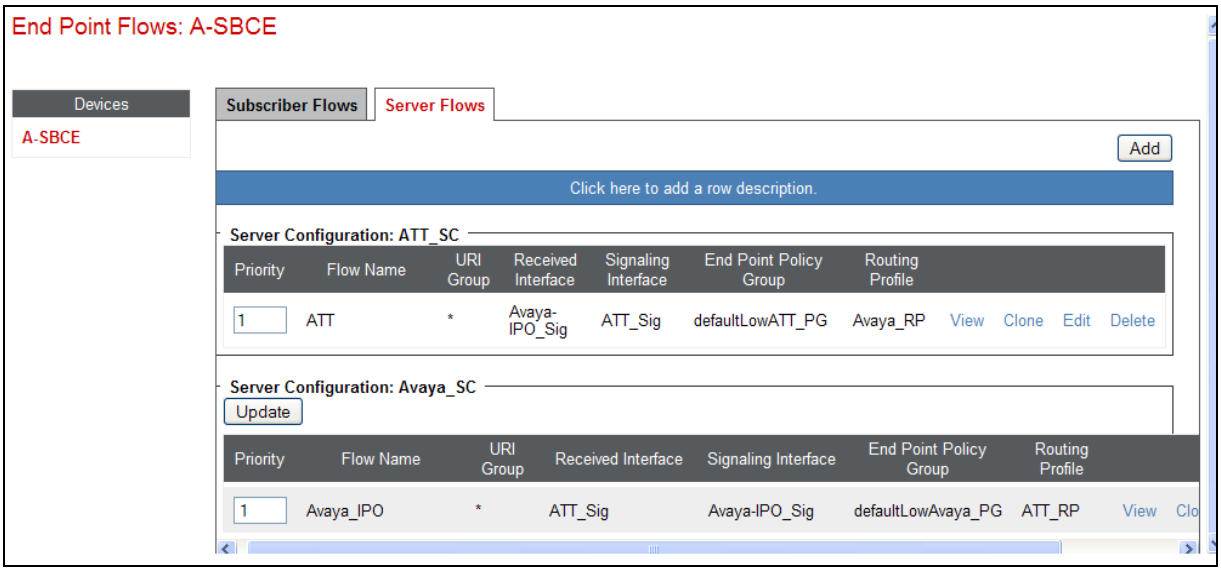
6.5.6. Endpoint Flows – AT&T

1. Repeat steps **1** through **4** from **Section 6.5.5**, with the following changes:
   a) **Name**: **ATT**
   b) **Server Configuration**: **ATT_SC** (**Section 6.3.6**).
   c) **URI Group**: *****
   d) **Transport**: *****
   e) **Remote Subnet**: *****
   f) **Received Interface**: **Avaya-IPO_Sig** (**Section 6.5.4**).
   g) **Signaling Interface**: **ATT_Sig (Section 6.5.4**).
   h) **Media Interface**: **ATT_MI** (**Section 6.5.3**).
   i) **End Point Policy Group**: **defaultLowATT_PG** (**Section 6.4.5**).
   j) **Routing Profile**: **Avaya_RP (Section 6.3.3**).
   k) **Topology Hiding Profile**: **ATT_TH** (**Section 6.3.8**).
   l) **File Transfer Profile**: **None**
2. Click **Finish**.



The completed **End Point Flows** screen is shown below.

©2014 Avaya Inc. All Rights Reserved.



7. AT&T IPFR-EF 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 EIPFR features, and their associated access numbers, are also assigned by AT&T. AT&T required that the Avaya SBCE public (B1) IP address be provided to the IPFR-EF service, as part of the provisioning process.

8. Verification Steps

The following procedures may be used to verify the Avaya IP Office R8.1 and the Avaya Session Border Controller for Enterprise 6.2, with the AT&T IP Flexible Reach - Enhanced Features service configuration.

8.1. AT&T IP Flexible Reach – Enhanced Features

The following scenarios may be executed to verify Avaya IP Office and the Avaya Session Border Controller for Enterprise 6.2, functionality with the AT&T IPFR-EF service:

- Place inbound and outbound calls, answer the calls, and verify that two-way talk path exists. Verify that the calls remain stable for several minutes and disconnects properly.
- Verify basic call functions such as hold, transfer, and conference.
- Verify the use of DTMF signaling.
- Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to Avaya Aura® Messaging voicemail. Retrieve the message from Avaya Aura® Messaging either locally or from PSTN.
- Using the appropriate IPFR-EF access numbers and codes, verify that the following features are successful:
    - Network based Simultaneous Ring – The “primary” and “secondary” endpoints ring, and either may be answered.

©2014 Avaya Inc. All Rights Reserved.

- Network based Sequential Ring (Locate Me) – Verify that after the "primary" endpoint rings for the designated time, the "secondary" endpoint rings and may be answered.
- Network based Call Forwarding Always (CFA/CFU), Network based Call Forwarding Ring No Answer (CF-RNA), Network based Call Forwarding Busy (CF-Busy), Network based Call Forwarding Not Reachable (CF-NR) – Verify that based on each feature criteria, calls are successfully redirected and may be answered.

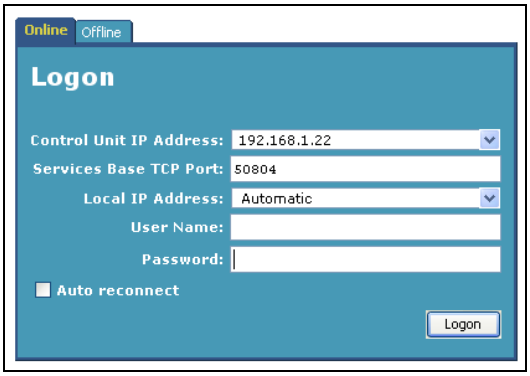
- Inbound / Outbound fax using T38 or G.711.
- SIP OPTIONS monitoring of the health of the SIP trunk. In the reference configuration Avaya IP Office sent OPTIONS to the AT&T IPFR-EF service Border Element, (via the Avaya SBCE), and AT&T responded with *405 Method Not Allowed* (which is the expected response). That response is sufficient for Avaya IP Office to consider the connection up. The AT&T IPFR-EF service Border Element does ***not*** send OPTIONS to Avaya IP Office.
- Incoming and outgoing calls using the G.729 (A or B) and G.711 ULAW codecs.
- 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 may also be verified.

8.2. Avaya IP Office 9.0

The following items may be used to analyze/troubleshoot Avaya IP Office operations.

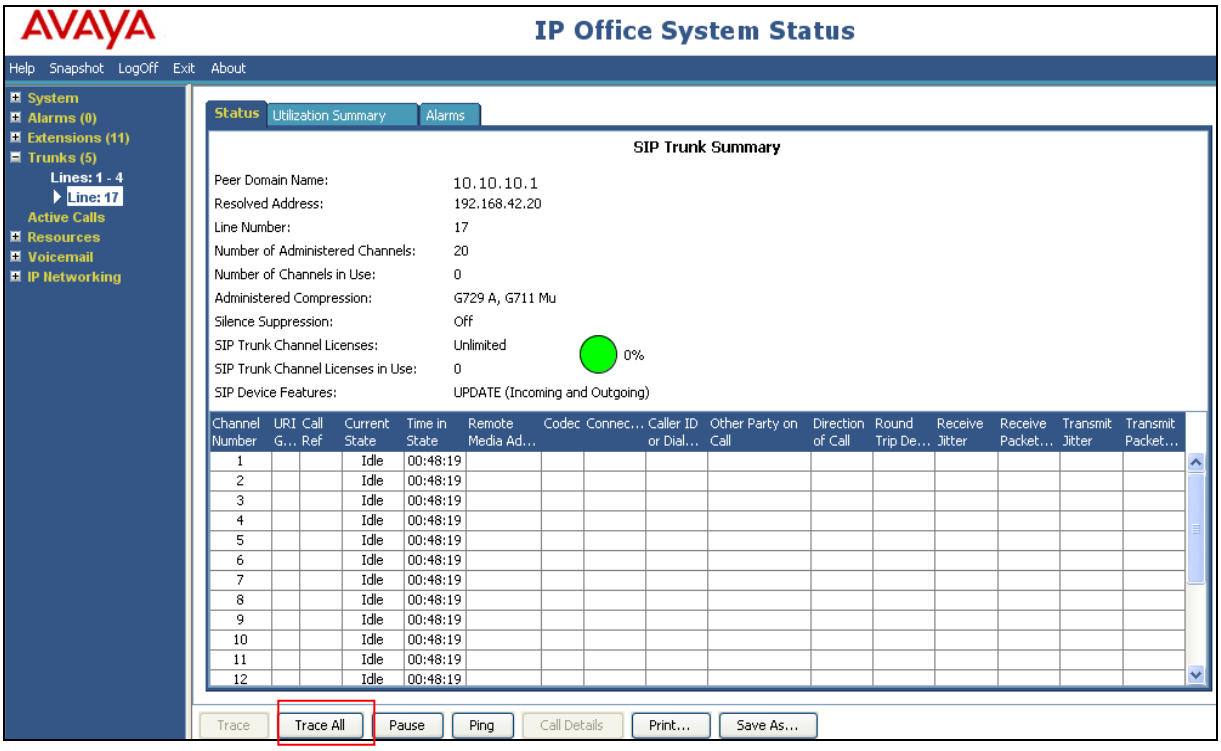
8.2.1. System Status Application

The System Status application can be used to monitor or troubleshoot Avaya IP Office. The System Status application can typically be accessed from **Start → Programs → Avaya IP Office → System Status**. The following screen shows an example **Logon** screen. Enter the Avaya IP Office IP address in the **Control Unit IP Address** field, and enter an appropriate **User Name** and **Password**. Click **Logon**.

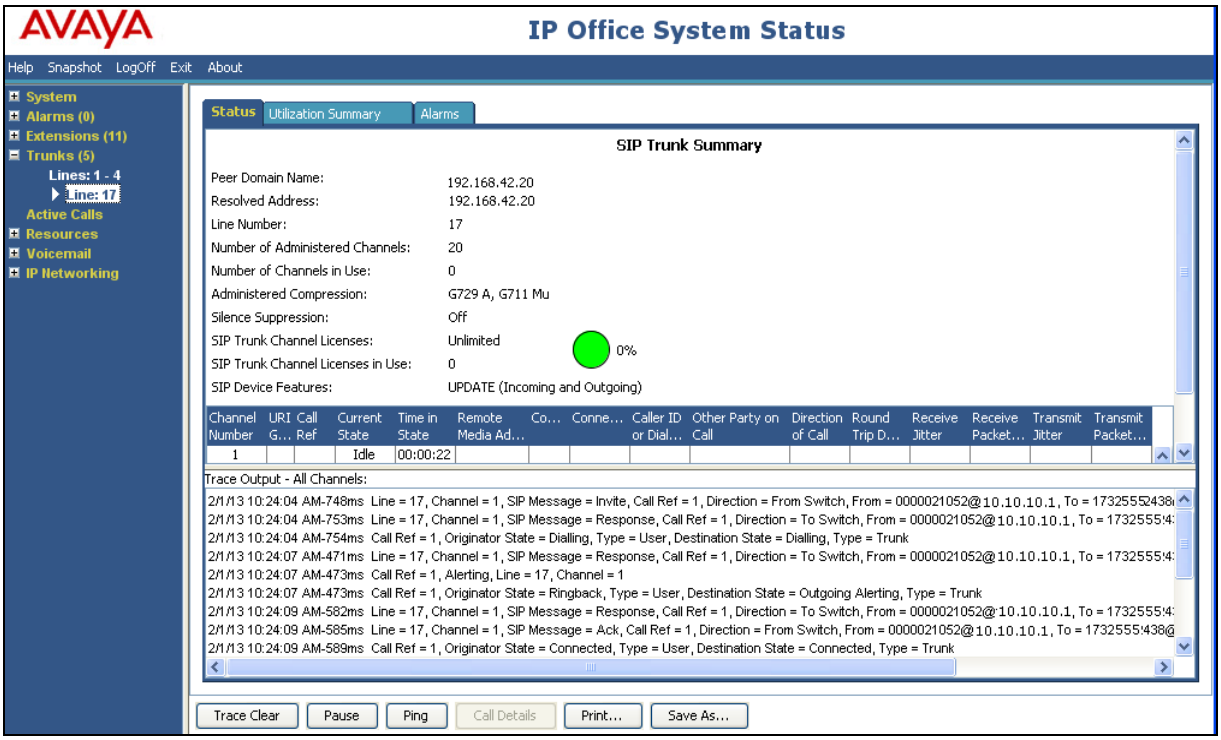


After logging in, select **Trunks → Line: 17** from the left navigation menu. (SIP Line 17 is configured in **Section 5.4**). A screen such as the one shown below is displayed. In the lower left, the **Trace All** button may be pressed to display tracing information as calls are made using this SIP Line.

©2014 Avaya Inc. All Rights Reserved.



The following screen shows an example outbound call where Avaya IP Office H.323 phone Extn500 called the PSTN.



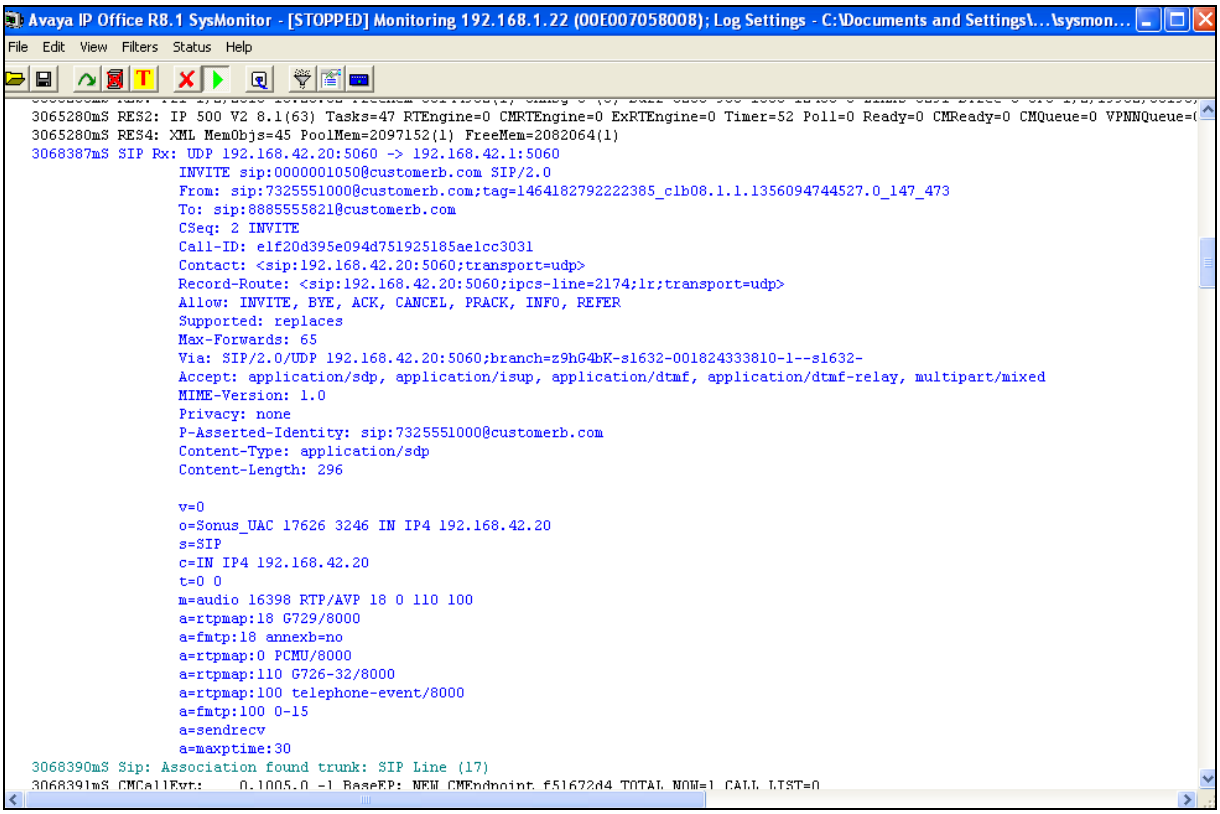
©2014 Avaya Inc. All Rights Reserved.

8.2.2. System Monitor Application

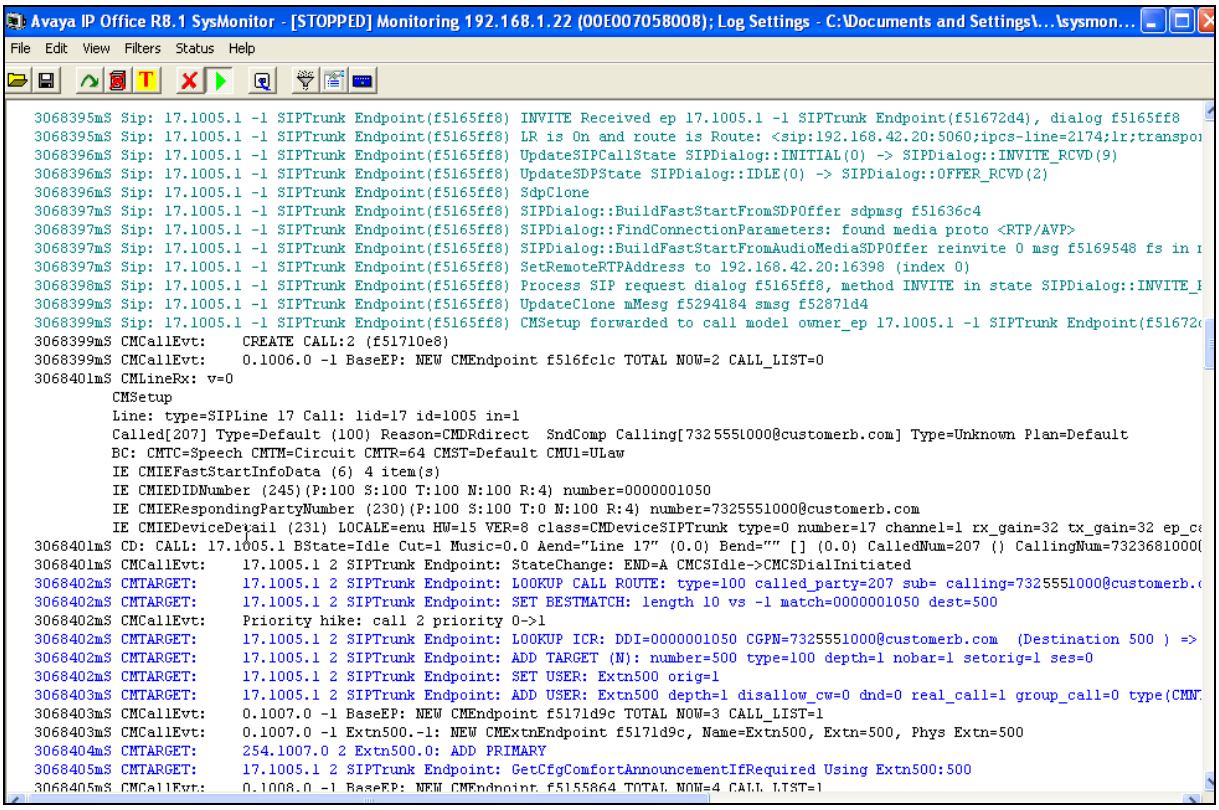
The System Monitor application can also be used to monitor or troubleshoot Avaya IP Office functionality (see reference **[3]**. The System Monitor application can typically be accessed from **Start → Programs → Avaya IP Office → Monitor**.

The Monitor will be active at startup. To pause the Monitor press the Pause button. The pause button will be replaced with the Start button. Press this button to resume the monitoring. To clear the Monitor display, press the Clear button.

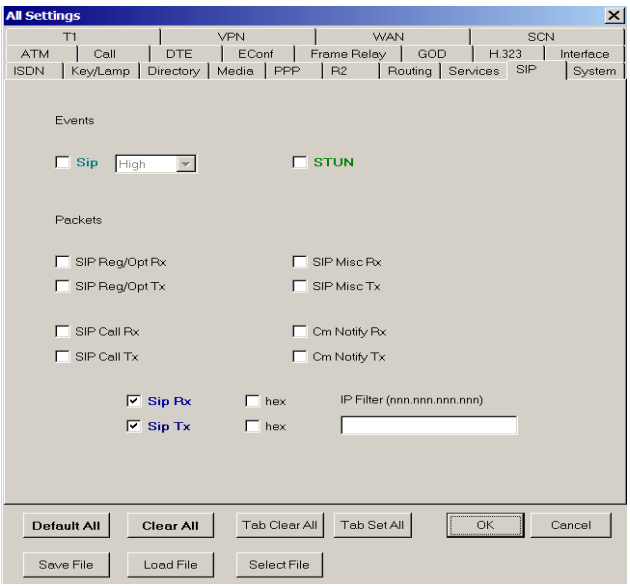
Below are samples of a monitored inbound call to Avaya IP Office SIP telephone Extn500. The Monitor will display SIP protocol (first image) as well as internal Avaya IP Office processing (second image).



©2014 Avaya Inc. All Rights Reserved.



The Monitor application allows the monitored information to be customized. To customize, from the screen at the beginning of this section, select the Options button that is third from the right, or 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.



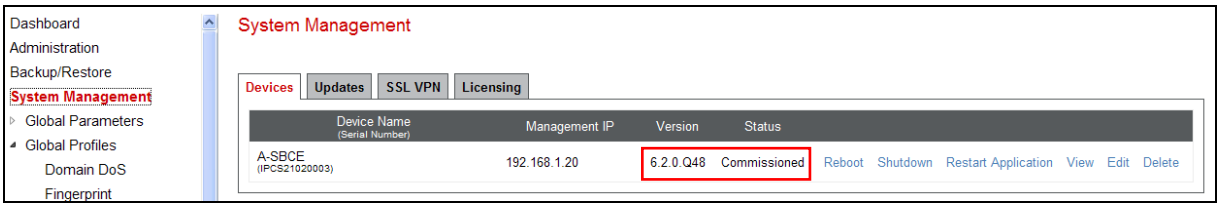
©2014 Avaya Inc. All Rights Reserved.

8.3. Avaya Session Border Controller for Enterprise 6.2

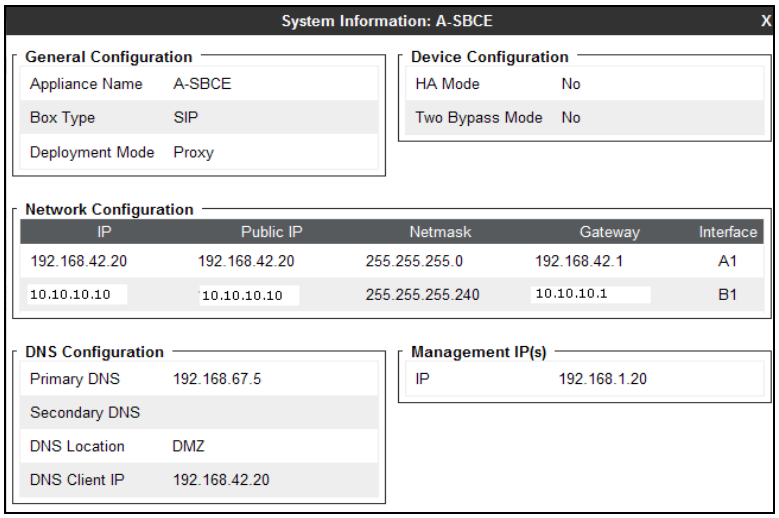
The following items may be used to analyze/troubleshoot Avaya SBCE operations.

8.3.1. System Information

1. Navigate to **System Management → Devices** tab.
   - The software version is shown in the **Version** column.
   - Also verify that the **Status** column says **Commissioned**.



2. Click on **View** (shown above) to display more system information.



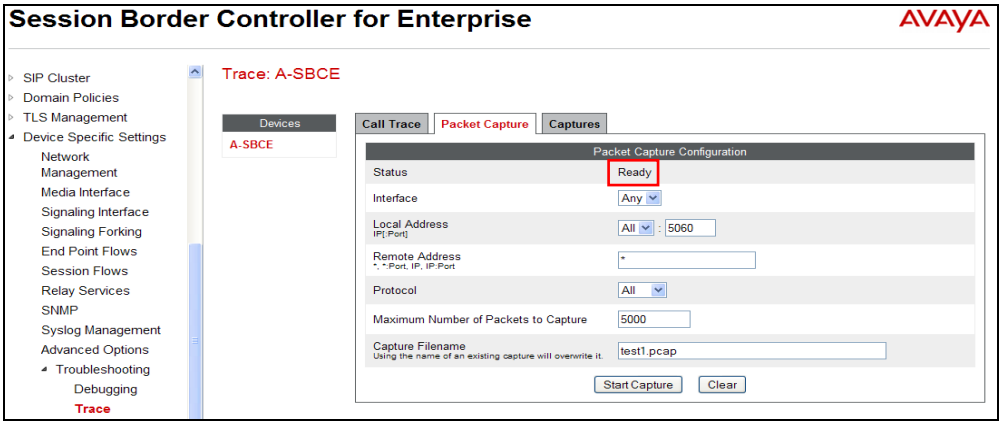
8.3.2. Avaya SBCE Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces. In the example below both SIP signaling crossing interfaces A1 and B1 are captured.

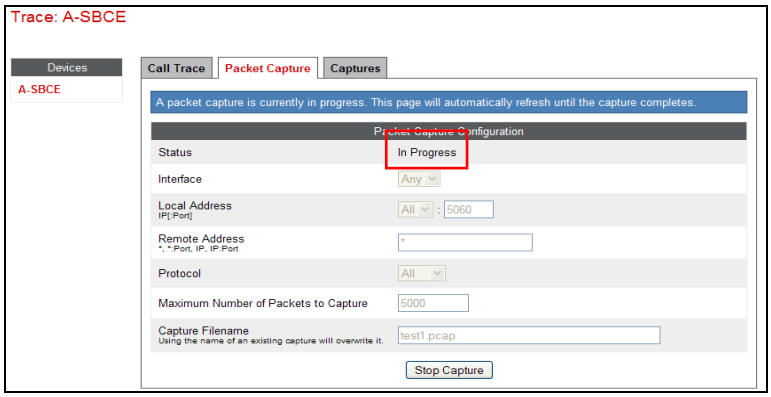
1. Navigate to **Device Specific Settings → Troubleshooting → Trace**
2. Select the **Packet Capture** tab and select the following:
   - **Interface** : Select **A1**, **B1**, or **Any** from the drop down menu. Note that specifying the option **Any** will capture packets from both the A1 and B1 interfaces.
   - **Local Address**: Select **All** and **5060** from the dropdown menus. This will capture any packets using port 5060 (e.g., SIP signaling).
   - **Remote Address**: Enter *****
   - **Protocol**: Select **All** from the dropdown menu.
   - **Maximum Number of Packets to Capture**: Specify a number that will include all the messaging required for the trace (e.g., **5000**).

©2014 Avaya Inc. All Rights Reserved.

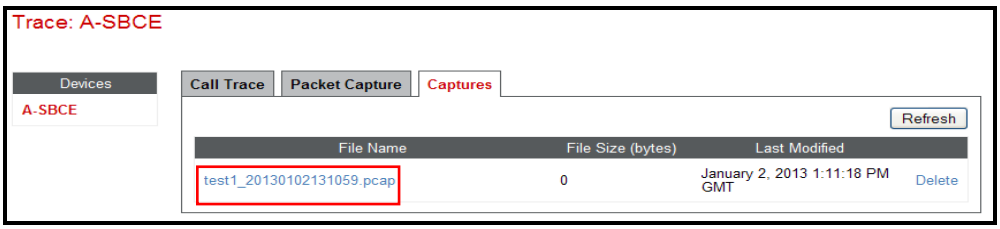
- **Capture Filename**: Specify a name for the trace file. Include a **.pcap** extension to open the file with Wireshark.
- Click **Start Capture** to begin the trace.



The capture process will initialize and then display the following status window:



3. Run the test.
4. Select **Stop Capture** button shown above.
5. Click on the Captures tab and the packet capture is listed as a .pcap file with the date and time added to filename specified in Step 2 (e.g., test1).



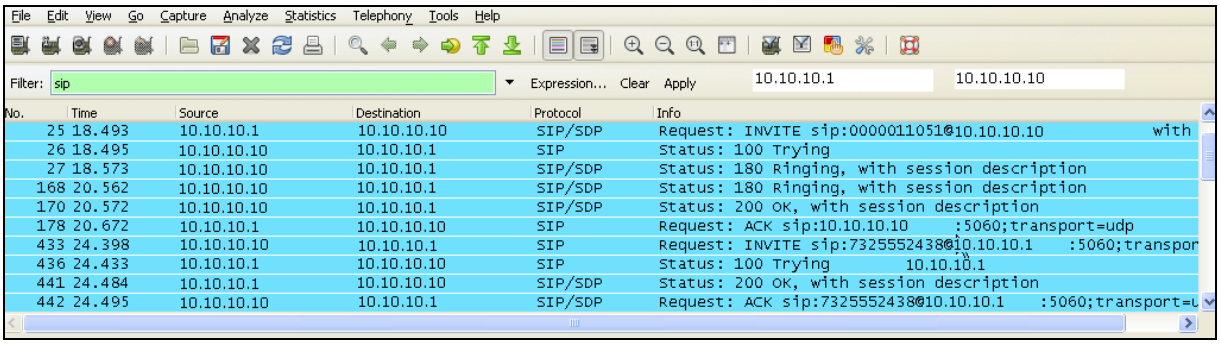
6. Click on the **File Name** to download the file and use an application such as Wireshark to open the trace.

©2014 Avaya Inc. All Rights Reserved.

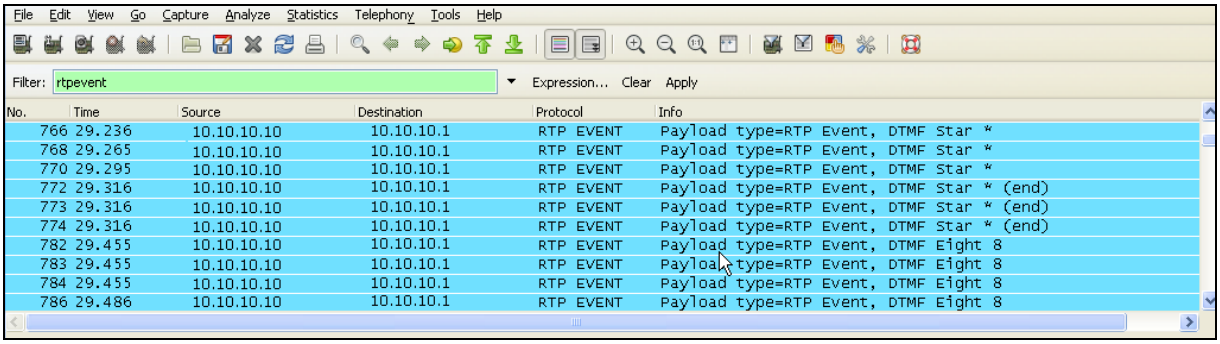
8.4. Protocol Trace Examples

This section shows examples of protocol traces taken at the Avaya SBCE B1 interface (to AT&T).

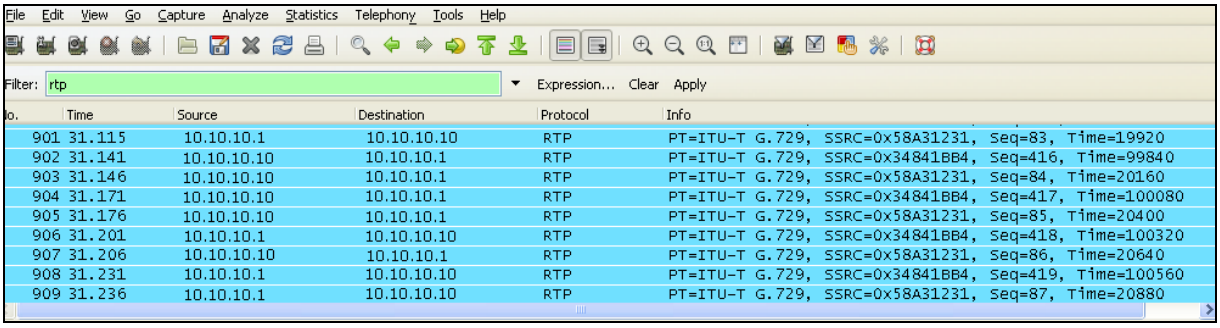
The following is an example of an inbound call from AT&T, filtering on the SIP protocol.



The following is an example of a call filtering on DTMF events.



The following is an example of a call filtering on RTP.



©2014 Avaya Inc. All Rights Reserved.

9. Conclusion

As illustrated in these Application Notes, Avaya IP Office R9.0and the Avaya Session Border Controller for Enterprise 6.2, can be configured to interoperate successfully with the AT&T IP Flexible Reach - Enhanced Features service using **AVPN** or **MIS/PNT** transport connections, within the limitations described in **Section 2.2.1**.

This solution provides users of Avaya IP Office R9.0 the ability to support inbound and outbound calls utilizing an AT&T IPFR-EF SIP trunk service connection, via AVPN or MIS/PNT transport, using the platform and service features listed in **Section 2.1**.

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.

©2014 Avaya Inc. All Rights Reserved.

10. References

Avaya:
Avaya product documentation is available at http://support.avaya.com

[1] IP Office Manager Release 9.0, 15-601011 Issue 9.01 (Monday, September 09, 2013)

[2] IP Office 9.0, Using System Status, 15-601758 Issue 09c - (15 August 2013)

[3] IP Office Voicemail Pro Example Exercises, 15-601138 Issue 07c - (06 July 2009)

[4] Configuring the Avaya Session Border Controller for IP Office Remote Workers, Release 9.0, Issue , September 2013

[5] IP Office 9.0 Using IP Office System Monitor 15-601019 Issue 05c - (19 August 2013)

[6] Additional Avaya IP Office documentation can be found at:
http://marketingtools.avaya.com/knowledgebase/

[7] Installing Avaya Session Border Controller for Enterprise, Release Release 6.2, Issue 3, June 2013

[8] Administering Avaya Session Border Controller for Enterprise, Issue 2, May 2013

[9] Administering Avaya Flare® Experience for Windows, Release 1.1, 18-604156, Issue 4, September 2013

AT&T IPFR-EF Service:

[10] http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/

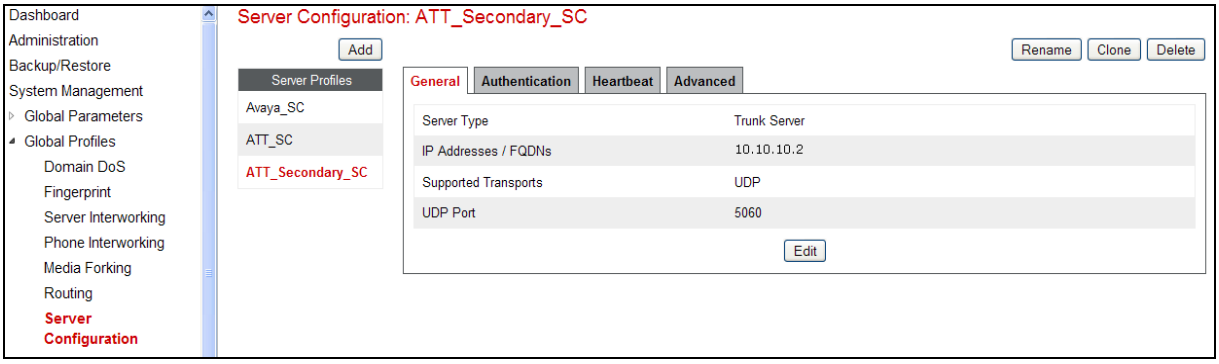
©2014 Avaya Inc. All Rights Reserved.

11. Addendum 1 – Redundancy to Multiple AT&T Border Elements

AT&T may provide two network border elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration.

Given two AT&T border elements **10.10.10.1**[10] (Primary) and **10.10.10.2** (Secondary), the Avaya SBCE is provisioned as follows to include the backup trunk connection.

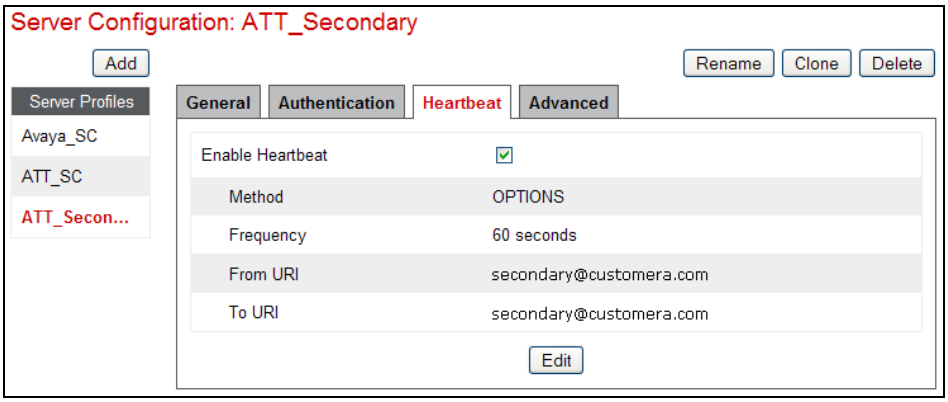
1. **Secondary Location in Server Configuration**
    1. Select **Global Profiles** from the menu on the left-hand side
    2. Select the **Server Configuration**
    3. Select **Add Profile**
        - **Name: ATT_Secondary_SC**
    4. On the **Add Server Configuration Profile – General** tab:
        - Select **Server Type: Trunk Server**
        - **IP Address: 10.10.10.2** (Address for a secondary location)
        - **Supported Transports**: Check **UDP**
        - **UDP Port: 5060**
        - Select **Next** (not shown)



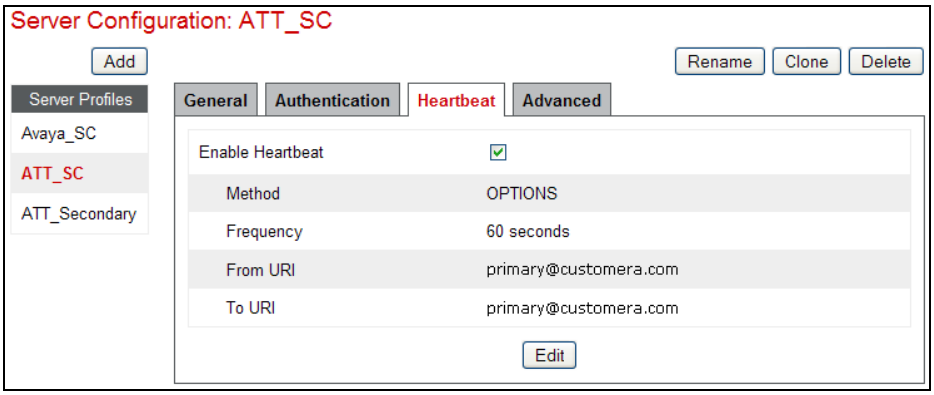
    5. On the **Authentication** tab
        - Select **Next** to accept defaults (not shown).
    6. On the **Heartbeat** tab:
        - Check **Enable Heartbeat**
        - **Method: OPTIONS**
        - **Frequency: 60 seconds**
        - **From URI: secondary@customera.com**
        - **To URI: secondary@customera.com**
        - Select **Next** (not shown)

[10] See footnote 3 in **Section 3.1**

©2014 Avaya Inc. All Rights Reserved.

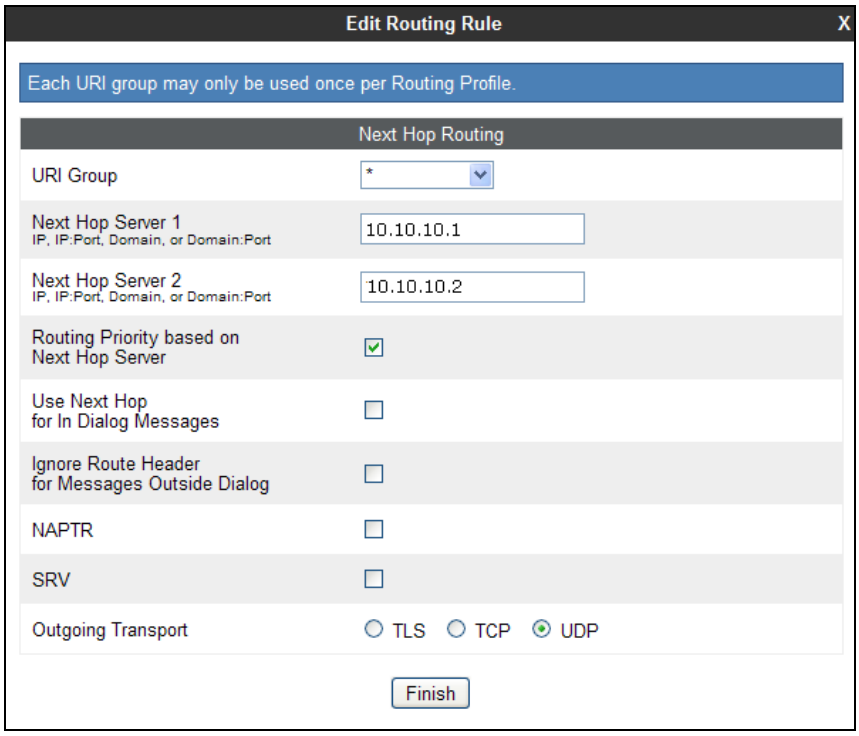


7. On the **Advanced** Tab
   Click **Finish** to accept defaults (not shown).
8. Select the **Server Configuration** created in **Section 6.3.6** (e.g., **ATT_SC**)
9. Select the **Heartbeat Tab**
10. Select **Edit**
11. Repeat **Steps 6 – 7**, but with information for the Primary Trunk as shown below.



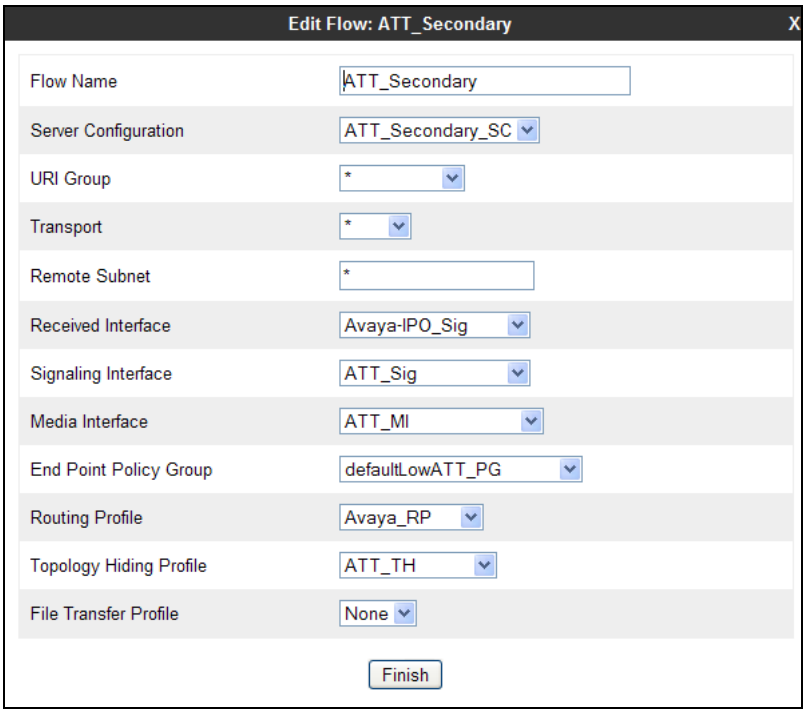
2. Add Secondary IP Address to Routing
   1. Select **Global Profiles** from the menu on the left-hand side
   2. Select the **Routing**
   3. Select the **Routing Profile** created in **Section 6.3.4** (e.g., **ATT_RP**)
   4. Click **Edit** (not shown)
      a) Enter the IP Address of the secondary location in the **Next Hop Server 2** (e.g., **10.10.10.2**)
   5. Click **Finish**

©2014 Avaya Inc. All Rights Reserved.



3. Configure End Point Flows – ATT_Secondary
   1. Select **Device Specific Settings** from the menu on the left-hand side
   2. Select **Endpoint Flows**
   3. Select the **Server Flows** Tab
   4. Select **Add Flow**
      a) **Name: ATT_Secondary**
      b) **Server Configuration: ATT_Secondary_SC**
      c) **URI Group: ***
      d) **Transport: ***
      e) **Remote Subnet: ***
      f) **Received Interface: Avaya-IPO_Sig**
      g) **Signaling Interface: ATT_Sig**
      h) **Media Interface: ATT_MI**
      i) **End Point Policy Group**: **defaultLowATT_PG**
      j) **Routing Profile: Avaya_RP**
      k) **Topology Hiding Profile: ATT_TH**
      l) **File Transfer Profile: None**
   5. Click **Finish**

©2014 Avaya Inc. All Rights Reserved.



When completed the Avaya SBCE will issue OPTIONS messages to the primary (10.10.10.1) and secondary (10.10.10.2) border elements. If the SBCE fails to get a response to the OPTIONS sent to 10.10.10.1, the SBCE will direct outbound calls to 10.10.10.2.

©2014 Avaya Inc. All Rights Reserved.

12. Addendum 2 – Remote Worker Configuration via the Avaya SBCE

This section describes the process for connecting select remote Avaya SIP endpoints on the public Internet, and access Avaya IP Office on a private enterprise, via the Avaya SBCE. The provisioning builds on the reference configuration described in previous sections of this document.

Note – This Remote Worker configuration is based on provisioning via the Avaya SBCE. It is not to be confused with "native" Avaya IP Office Remote Worker configurations.

Supported Remote Worker endpoints are:

- Flare® Experience for iPad
- Flare® Experience for Windows
- one-X® Mobile Preferred VoIP client for iOS
- one-X® Mobile Preferred VoIP client for Android

In the reference configuration Avaya Flare® Experience for Windows was used as the Remote Worker SIP endpoint.

For Avaya IP Office R9.0, the following table summarizes encryption support for these remote worker endpoints (see **Section 12.1.7**):

Client type	Uses to the external interface of the SBCE		
	TLS	SRTP Audio	SRTP Video
Flare Experience for iPad R1.1.1	Y*	Y*	N
Flare Experience for Windows R1.1.1	Y*	Y*	N
one-X Mobile Preferred VoIP client for iOS	Y	N	N
one-X Mobile Preferred VoIP client for Android	N	N	N
* If the client is used inside and outside of the IP Office core, the signalling type must be changed. IP Office 9.0 does not support TLS or SRTP connections to these clients on the inside of the SBCE.			

The reference configuration, including the Remote Worker endpoint, is shown in **Figure 6** below. Internet access is simulated by a D-Link Router/NAT/Firewall/Default Gateway located between the Remote Worker private LAN and the public Internet interface (B1) of the Avaya SBCE. The D-Link router also provides DHCP functionality in the private space. Note that the use of the D-Link router is for functionality testing only and is not prescriptive.

Provisioning of the D-Link is beyond the scope of this document.

©2014 Avaya Inc. All Rights Reserved.

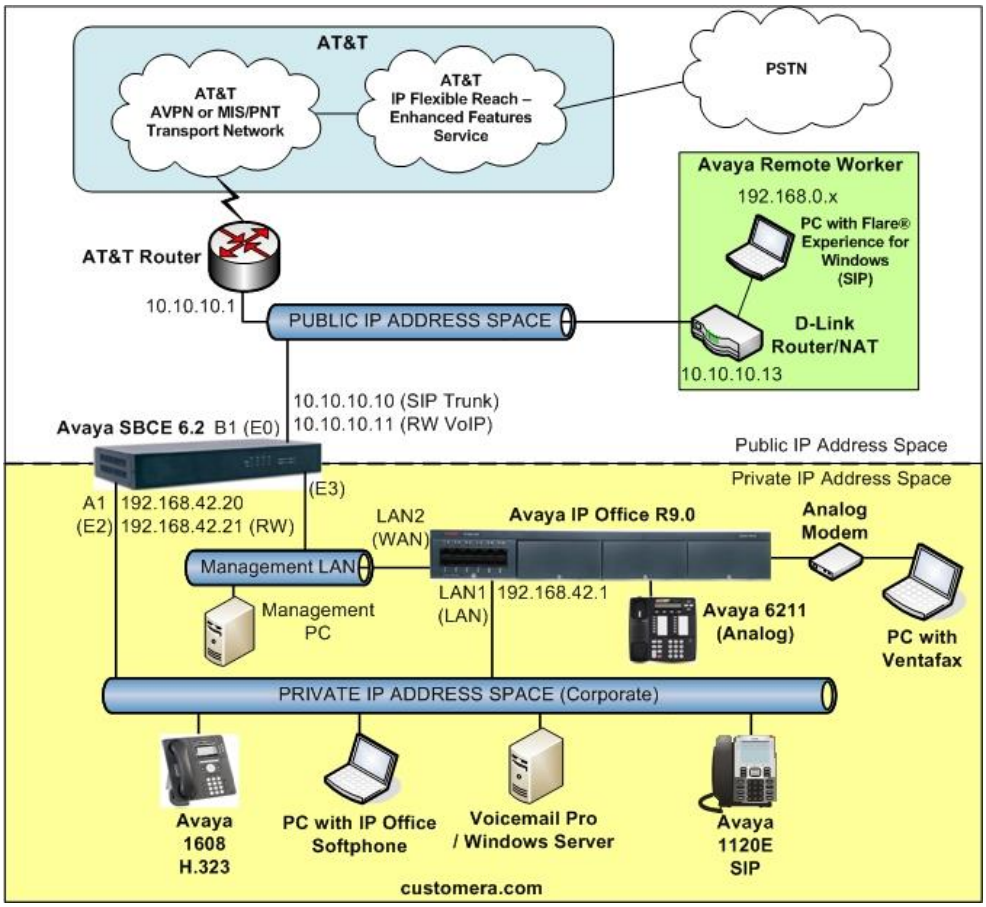


Figure 6

12.1. Provisioning the Avaya Session Border Controller for Enterprise

Provisioning of the Avaya SBCE to support Avaya IP Office SIP Trunking to the AT&T IPFR-EF service is described in **Section 6**. The following sections build on that provisioning.

12.1.1. Network Management

This section shows the **Network Management** configuration of the Avaya SBCE to support Remote Worker. The Avaya SBCE is configured with a second "outside" IP address assigned to physical interface B1, and an additional "inside" address assigned to physical interface A1.

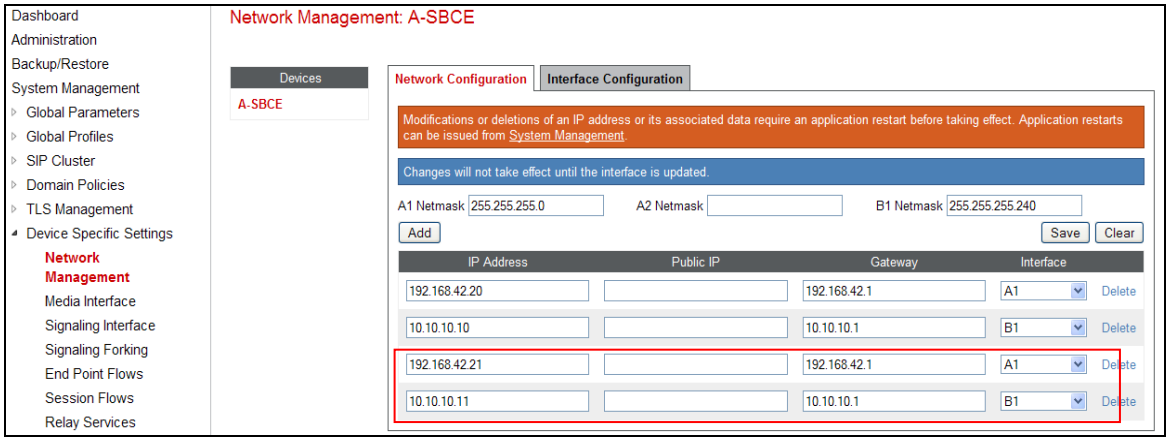
These are the Avaya SBCE IP addresses used in the reference configuration:

- **192.168.42.20** is the SBCE "inside" address previously provisioned for SIP Trunking with AT&T (see **Section 6.1**).
- **192.168.42.21** is the new SBCE "inside" address for Remote Worker access to IP Office.

©2014 Avaya Inc. All Rights Reserved.

- **10.10.10.10**[11] is the SBCE "outside" address previously provisioned for SIP Trunking with AT&T (see **Section 6.1**).
- **10.10.10.11** is the new SBCE "outside" address for Remote Worker access to IP Office.

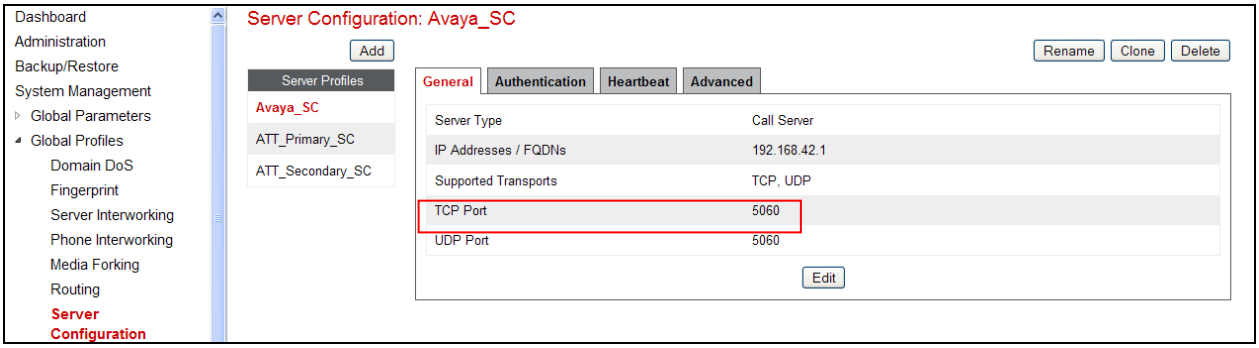
1. On the **Network Configuration** tab, using the values shown below, select **Add** to create an entry for **192.168.42.21** on interface **A1**, then select **Save**.
2. Repeat step **1** for an entry for **10.10.10.11** on interface **B1**.



12.1.2. Server Configuration – Avaya IP Office

In this section TCP transport protocol (which is required for the Remote Worker connection between the Avaya SBCE and Avaya IP Office), is added to the existing **Avaya_SC** Server Configuration (see **Section 6.3.5**).

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**.
3. Select the existing **Avaya_SC** profile and click on **Edit**.
4. The **Add Server Configuration Profile - General** window will open (not shown).
   a. **Supported Transports**: Check **TCP**
   b. **TCP Port**: **5060**
   c. Select **Finish**.



[11] See footnote 1 in **Section 3.2.1**

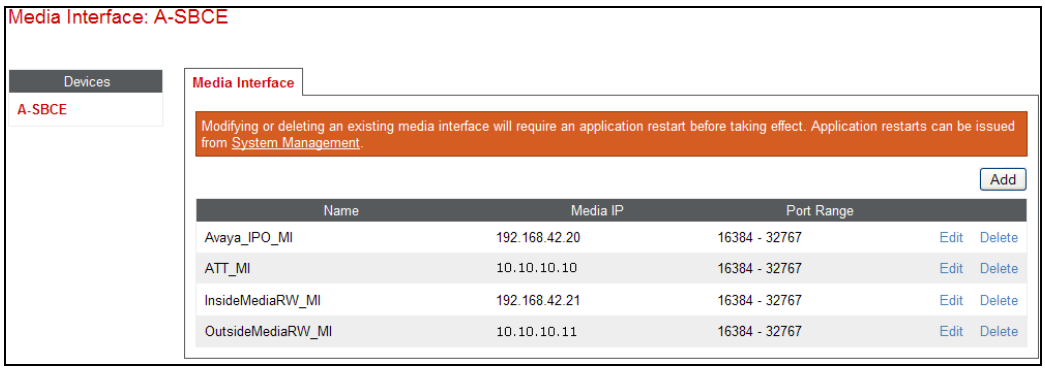
©2014 Avaya Inc. All Rights Reserved.

12.1.3. Media Interface

Note - The AT&T network services require the use of port range 16384-32767. Therefore this range is required on the 192.168.67.120 and 10.10.10.10 SIP Trunking interfaces (see **Section 6.5.2).** However for consistency, this range is used on the Remote Worker interfaces as well.

Note – Media Interfaces **Inside_Trunk_MI** and **Outside_Trunk_MI** were previously defined for SIP Trunking with AT&T (see **Section 6.5.3**).

1. Click on the **Add** button and create Media Interface **InsideMediaRW_MI** using the parameters shown below. Click on the **Finish** button (not shown).
2. Repeat step **1** to create Media Interface **OutsideMediaRW_MI**.



Media Interface **OutsideMediaRW_MI** is used in the **RW_Flare** Subscriber Flow (**Section 12.1.9.1**). Media Interface **InsideMediaRW_MI** is used in the **IPO_Remote_Worker** Server Flow (**Section 12.1.9.2**).

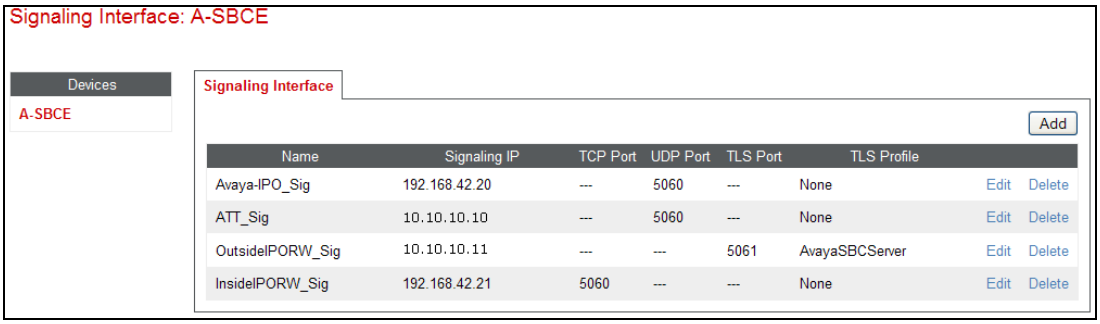
12.1.4. Signaling Interface

The following screen shows the **Signaling Interface** settings. Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic. Interface **OutsideIPORW_SI** supports TLS, while interface **InsideIPORW_SI** supports TCP.

1. Select the **Add** button to create Signaling Interface **OutsideIPORW_SI**
   a. Signaling IP = **10.10.10.11**
   b. TLS Port = **5061**
   c. Select TLS Profile **AvayaSBCServer** from the drop down menu.
   d. Click on **Finish** (not shown).
2. Repeat step **1** to create Signaling Interface **InsideIPORW_SI**
   a. Signaling IP = **192.168.42.21**
   b. TCP Port = **5060**
   c. Click on **Finish** (not shown).

©2014 Avaya Inc. All Rights Reserved.

Signaling Interface **OutsideIPORW_SI** is used in the **RW_Flare** Subscriber Flow (**Section 12.1.9.1**), and in the **IPO_Remote_Worker** Server Flow (**Section 12.1.9.2**).

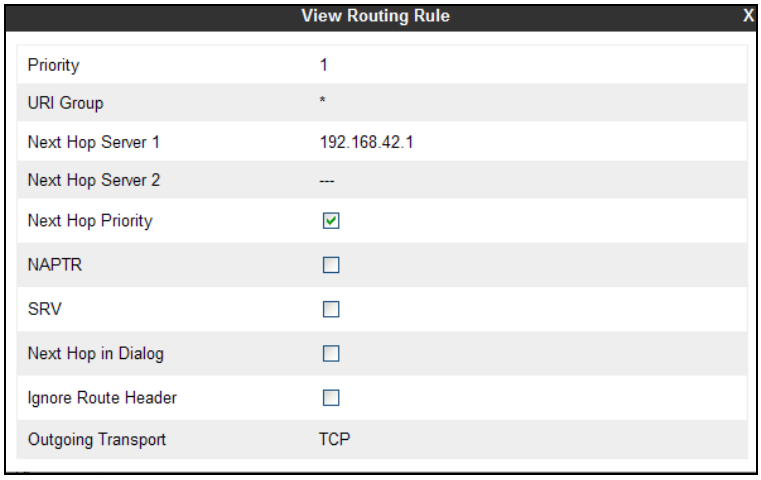


Signaling Interface **InsideIPORW_SI** is used in the **IPO_Remote_Worker** Server Flow (**Section 12.1.9.2**).

12.1.5. Routing Profile

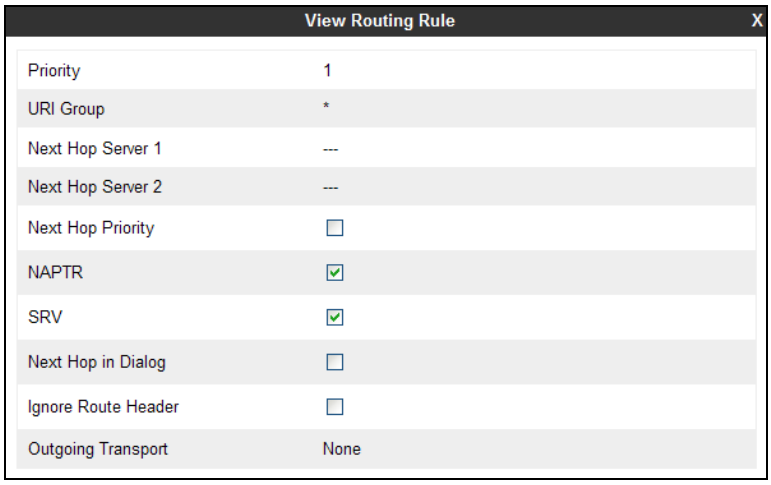
Two new Routing Profiles are required to support the Remote Worker.

1. Select the **Add** button to create Routing Profile **RW_RP**, the select Next (not shown).
2. Enter the following:
   a. **URI Group** = ***** (default)
   b. **Next Hop Server 1** = **192.168.42.1** (IP Office LAN1 interface defined in **Section 5.3.2**).
   c. Verify **Routing Priority based on Next Hop Server** is checked.
   d. Select **TCP**.
   e. Click on **Finish** (not shown).

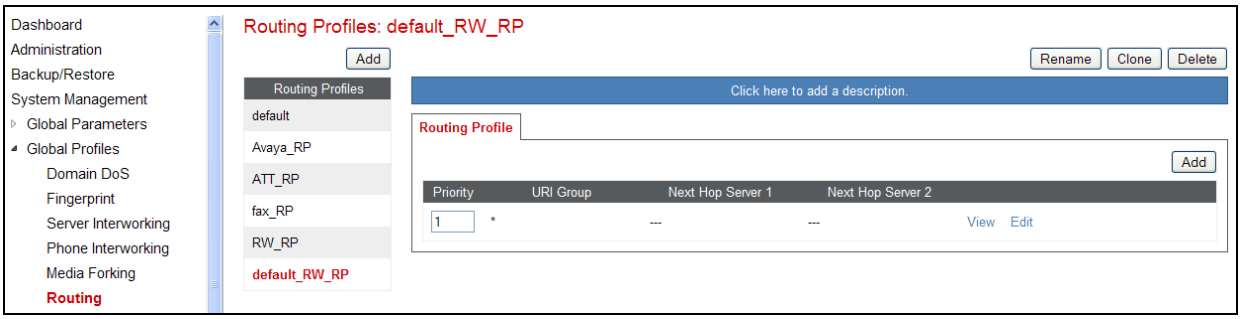


3. Select the existing **default** Routing Profile and click on the **Clone** button, and name it **default_RW_RP**, then select **Next** (not shown).
4. Keep all the default values and click on **Finish** (not shown).

©2014 Avaya Inc. All Rights Reserved.



Below is the completed Routing Profile screen.



The Routing Profile **RW_RP** is used in the Remote Worker Subscriber Flow (**Section 12.1.9.1** and in the Remote Worker Server Flow (**Section 12.1.9.2**).

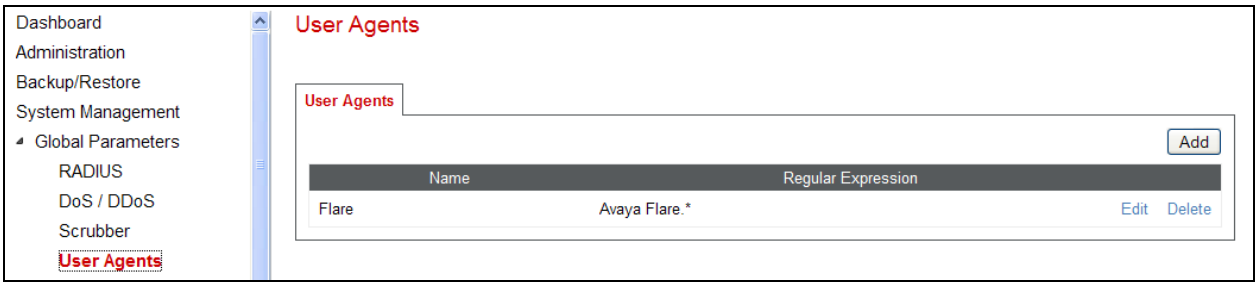
12.1.6. User Agents

User Agents are created for each type of Remote Worker endpoint used. In the reference configuration the Avaya Flare® Experience for Windows SIP softphone was used, and its configuration is shown below.

1. Select the **Add** button to create a new User Agent.
2. Enter the following:
    a. **User Agent** = **Flare**
    b. **Regular expression = Avaya Flare ***
    c. Click on **Finish** (not shown).

In this expression, "Avaya Flare.*" will match any software version listed after the user agent name.

©2014 Avaya Inc. All Rights Reserved.

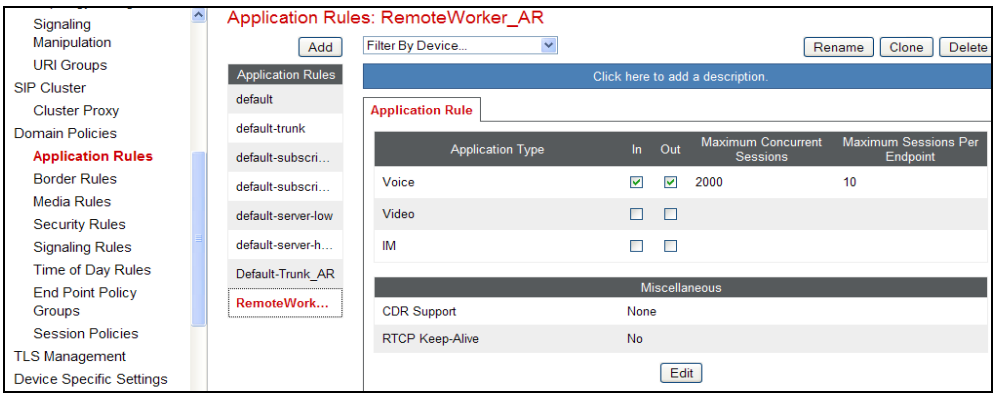


The **Flare** User Agent is defined in the Remote Worker Subscriber Flow (**Section 12.1.9.1**).

12.1.7. Application Rules

In this section Application Rule **RemoteWorker_AR** is created.

1. To create the **RemoteWorker_AR** rule, select **Add**. Enter the following:
    a. Enter a name (e.g., **RemoteWorker_AR**), and click on **Next** (not shown).
    b. In the **Voice** field:
        i. Check **In** and **Out**.
        ii. Enter an appropriate value in the **Maximum Concurrent Sessions** field, (e.g., **2000**).
        iii. Enter **10** in the **Maximum Session per Endpoint** field.
    c. Leave the **CDR** field at **None** and the **RTCP Keep-Alive** field unchecked (**No**).
    d. Click on **Finish** (not shown).



The rule **RemoteWorker_AR** is assigned to the End Point Policy Groups (**Section 12.1.8**).

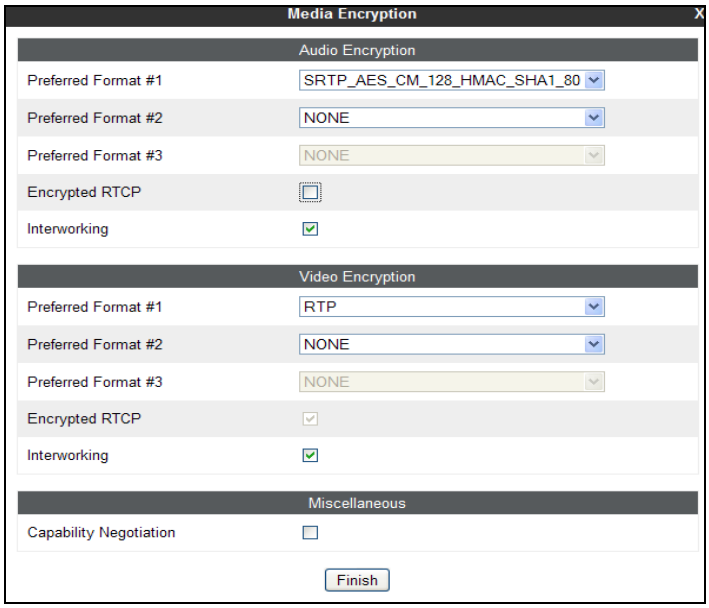
12.1.8. Media Rules

Two Media Rules are defined. Rule **RW_SRTP_MR** is defined to enable the use of SRTP between the Avaya Flare® Experience for Windows Remote Worker, (which also uses TLS for transport; see **Section 12.3.1**), and the Avaya SBCE. Rule **RW_RTP_MR** is created for the Remote Worker connection from the Avaya SBCE to Avaya IP Office.

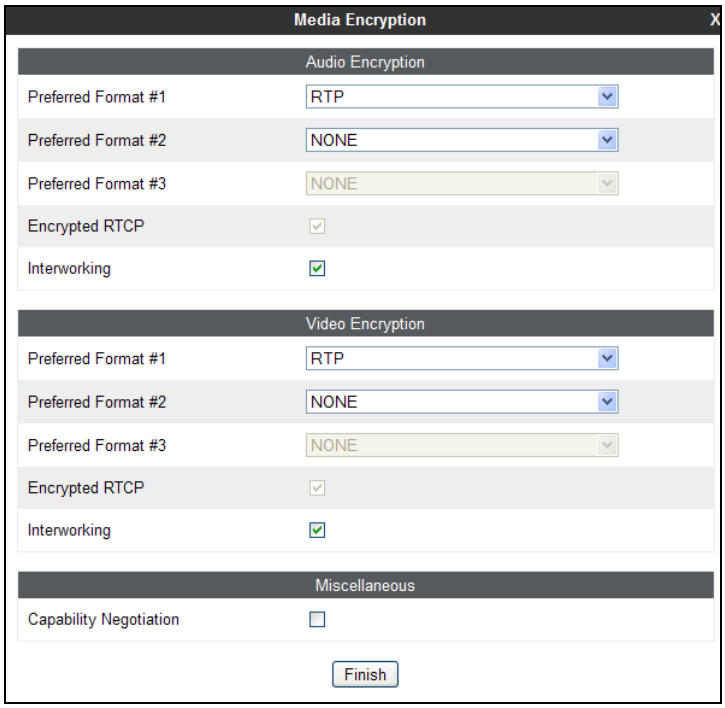
1. To create the **RW_SRTP_MR** rule, select the **Avaya-low-med_MR** rule created in **Section 6.4.2**, and click on the **Clone** button.

©2014 Avaya Inc. All Rights Reserved.

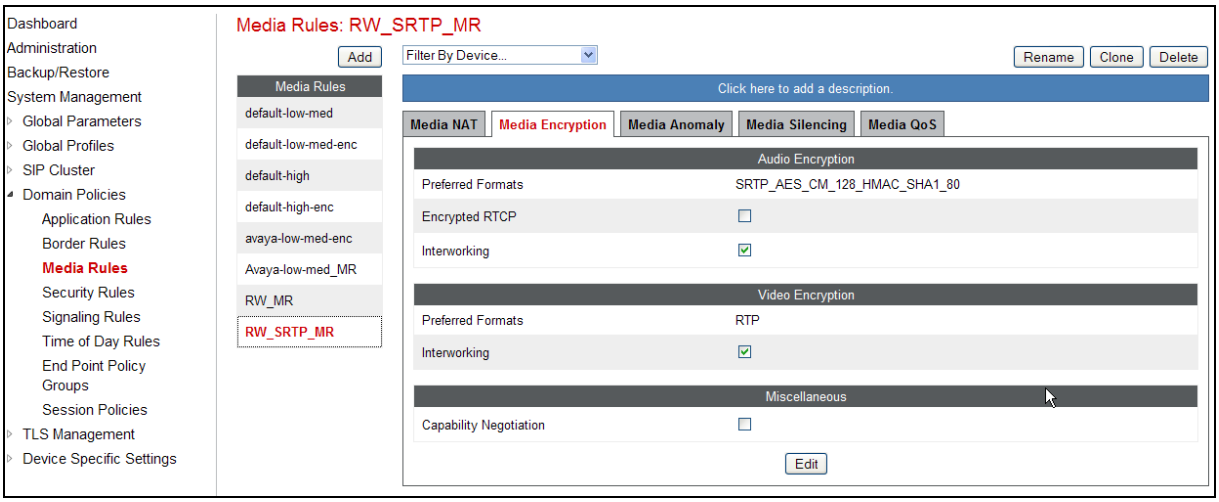
2. Enter a name (e.g., **RW_SRTP_MR**) and click **Next** (not shown).
3. Populate the fields as shown below, then click on **Finish**.



4. To create the **RW_RTP_MR** rule, select the **Avaya-low-med_MR** rule created in **Section 6.4.2**, and click on the **Clone** button (the existing **Avaya-low-med_MR** rule could have been specified here instead, however a distinct Remote Worker rule was use to illustrate the provisioning).
5. Leave all values as they were.



©2014 Avaya Inc. All Rights Reserved.

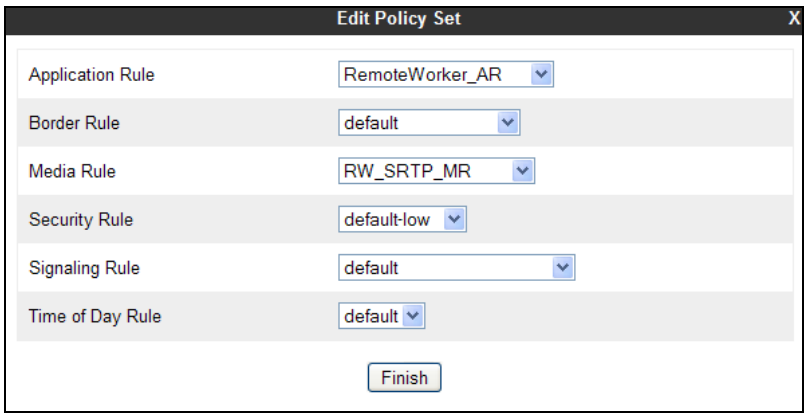


Media Rule **RW_SRTP_MR** is assigned to the End Point Policy Group **RW_SRTP_PG** (**Section 12.1.8**). Media Rule **RW_RTP_MR** is assigned to the End Point Policy Group **RW_RTP_PG** (**Section 12.1.8**).

12.1.9. End Point Policy Groups

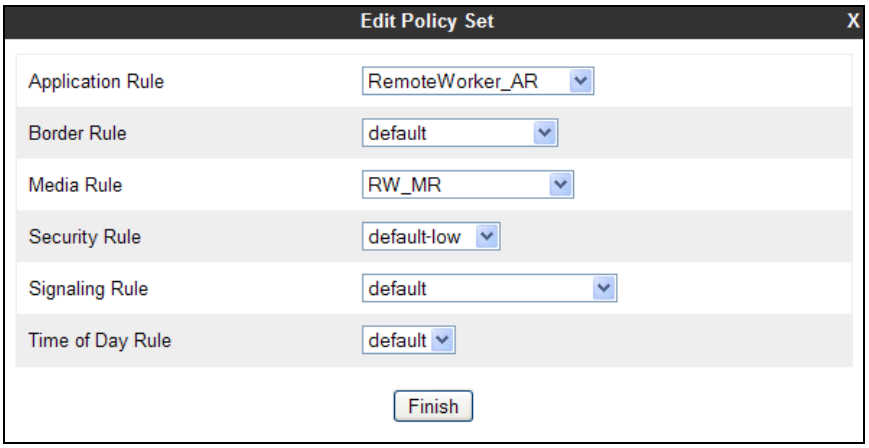
Two new End Point Policy Groups are defined for Remote Worker. Group **RW_SRTP_PG** is defined for the SRTP connection and **RW_PG** is defined for the RTP connection.

1. To create the new **RW_SRTP_PG** group, click on **Add**. Enter the following:
    a. Enter a name (e.g., **RW_SRTP_PG**), and click on **Next** (not shown).
    b. The **Policy Group** window will open. Enter the following:
        i. **Application Rule** = **RemoteWorker_AR** (**Section 12.1.6**)
        ii. **Border Rule** = **default**
        iii. **Media Rule** = **RW_SRTP_MR** (**Section 12.1.7**)
        iv. **Security Rule** = **default-low**
        v. **Signaling Rule** = **default**
        vi. **Time of Day Rule** = **default**
    c. Click on **Finish**.



©2014 Avaya Inc. All Rights Reserved.

2. To create the new **RW_PG** group, click on **Add**. Enter the following:
    d. Enter a name (e.g., **RW_PG**), and click on **Next** (not shown).
    e. The **Policy Group** window will open. Enter the following:
        i. **Application Rule** = **RemoteWorker_AR** (**Section 12.1.6**)
        ii. **Border Rule** = **default**
        iii. **Media Rule** = **RW_MR** (**Section 12.1.7**)
        iv. **Security Rule** = **default-low**
        v. **Signaling Rule** = **default**
        vi. **Time of Day Rule** = **default**
    f. Click on **Finish** (not shown).



End Point Policy Group **RW_SRTP_PG** is used in the Subscriber Flow **IPO_Remote_Worker** (**Section 12.1.9.1**). End Point Policy Group **RW_PG** is used in the Server Flow **IPO_Remote_Worker** (**Section 12.1.9.2**).

12.1.10. End Point Flows

A **Subscriber Flow** and an **Endpoint Flow** are created for Remote Worker.

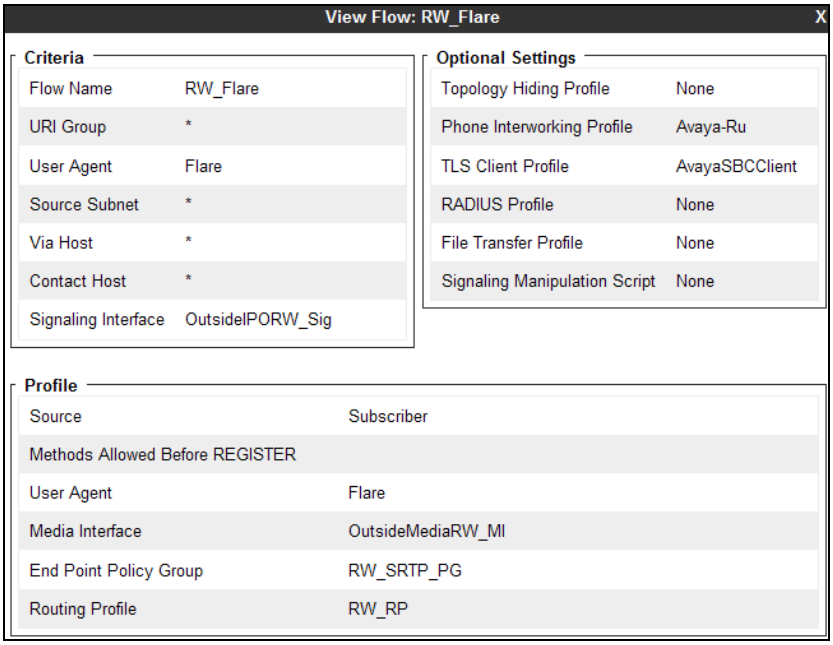
12.1.10.1 Subscriber Flow

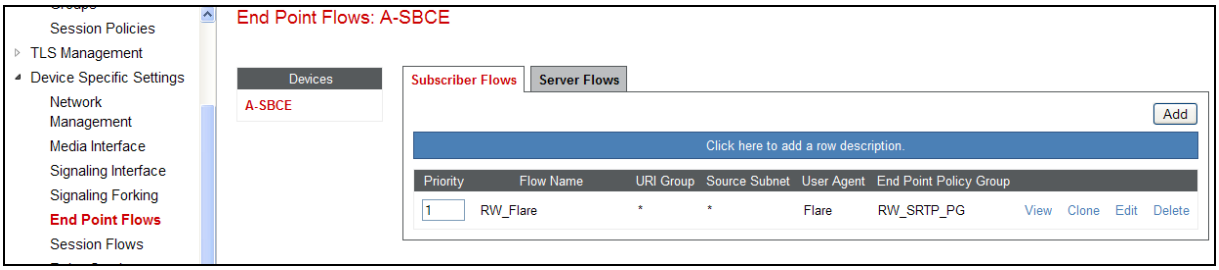
A **Subscriber Flow** is defined for the Avaya Flare® Experience for Windows softphone used in the reference configuration.

1. To create the Subscriber Flow, click on **Add** and the Criteria window will open (not shown). Enter the following:
    a. Enter a name (e.g., **RW_Flare**)
    b. **URI Group** = ***** (default)
    c. **User Agent** = **Flare**
    d. **Source Subnet** = ***** (default)
    e. **Via Host** = ***** (default)
    f. **Contact Host** = ***** (default)
    g. **Signaling Interface** = **OutsideIPORW_Sig** (**Section 12.1.3**)

©2014 Avaya Inc. All Rights Reserved.

2. Click on **Next** (not shown) and the Profile window will open (not shown). Enter the following:
    a. **Source** = **Subscriber**
    b. **Methods Allowed Before REGISTER =** Leave as default
    c. **Media Interface** = **OutsideMediaRW_MI** (**Section 12.1.2**).
    d. **End Point Policy Group = RW_SRTP_PG** (**Section 12.1.8**).
    e. **SIP Cluster Flow** = unchecked
    f. **Routing Profile = RW_RP** (**Section 12.1.4**)
    g. **Topology Hiding Profile** = **None**
    h. **Phone Interworking Profile** = **Avaya-RU**
    i. **TLS Client Profile** = **AvayaSBCClient**
    j. **Radius Profile = None**
    k. **File Transfer Profile** = **None**
    l. **Signaling Manipulation Script** = **None**
3. Click on **Finish** (not shown).



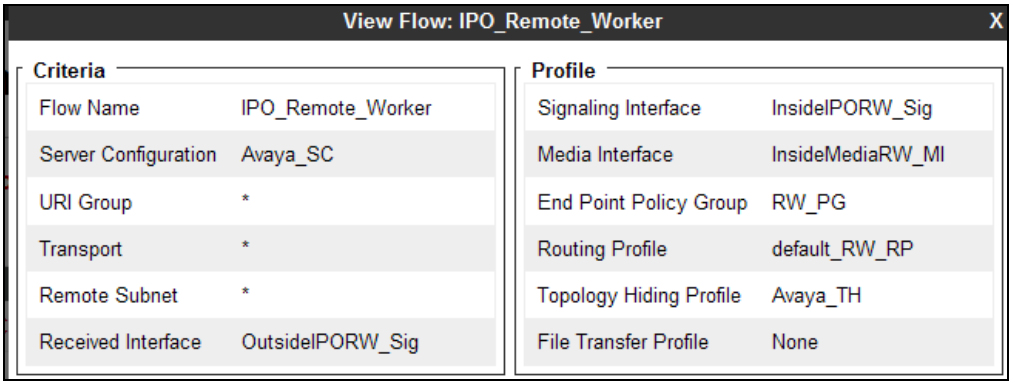


©2014 Avaya Inc. All Rights Reserved.

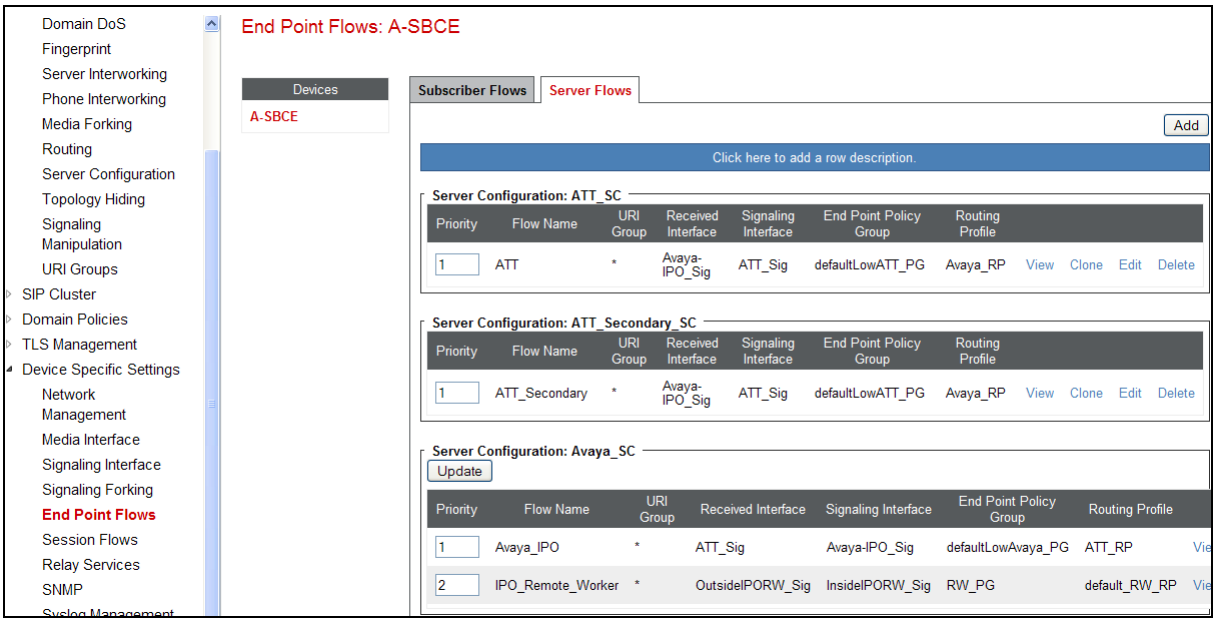
12.1.10.2 Server Flow

The following section shows the new **Server Flow** settings for Remote Worker access to IP Office. The new flow is defined as part of the **Avaya_SC** Server Configuration created in **Section 6.3.5**.

1. Select **Device Specific Settings** from the menu on the left-hand side.
2. Select **Endpoint Flows**
3. Select the **Server Flows** tab
4. Select **Add** (not shown), and enter the following:
   m) **Name = IPO_Remote_Worker**
   n) **Server Configuration** = **Avaya_SC** (**Section 6.3.5**)
   o) **URI Group** = ***** (default)
   p) **Transport** = ***** (default)
   q) **Remote Subnet** = ***** (default)
   r) **Received Interface** = **OutsideIPORW_Sig** (**Section 12.1.3**)
   s) **Signaling Interface** = **InsideIPORW_Sig** (**Section 12.1.3**)
   t) **Media Interface** = **InsideMediaRW_MI** (**Section 12.1.2**)
   u) **End Point Policy Group** = **RW_PG** (**Section 12.1.8**)
   v) **Routing Profile** = **default_RW_RP (Section 12.1.4)**
   w) **Topology Hiding Profile** = **Avaya_TH** (**Section 6.3.7**)
   x) **File Transfer Profile** = **None** (default)
5. Click **Finish** (not shown).



©2014 Avaya Inc. All Rights Reserved.

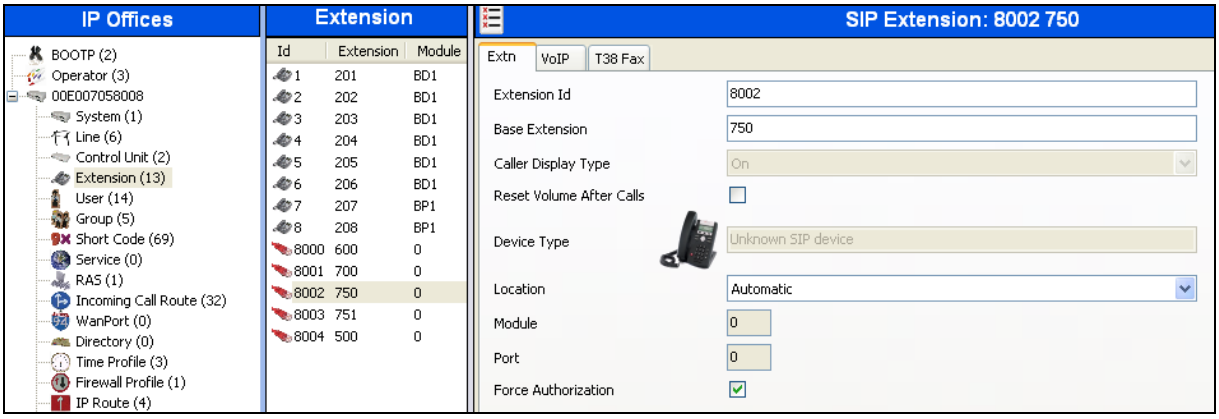


12.2. Remote Worker Endpoint Configuration on Avaya IP Office

The Remote Worker Avaya Flare® Experience for Windows endpoint is added to the Avaya IP Office **User** and **Extension** configuration, as well an **Incoming Call Route**.

12.2.1. Extension Configuration

No special procedures are required to create the Remote Worker Extension. Following the procedures shown in **Section 5.5.3**, Extension 750 was created for the Avaya Flare® Experience for Windows Remote Worker.



12.2.2. User Configuration

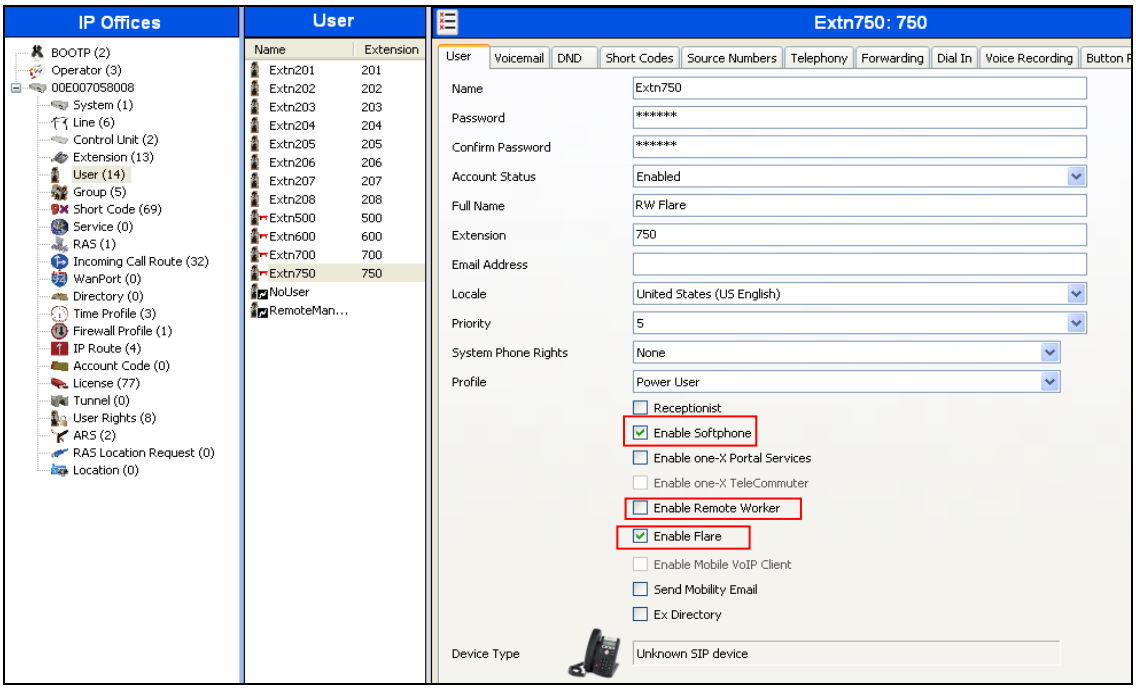
Following the procedures shown in **Section 5.5.3**, create a user for the Remote Worker. Provisioning specific to the Avaya Flare® Experience for Windows Remote Worker used in the reference configuration, is shown below.

©2014 Avaya Inc. All Rights Reserved.

12.2.2.1 User Tab

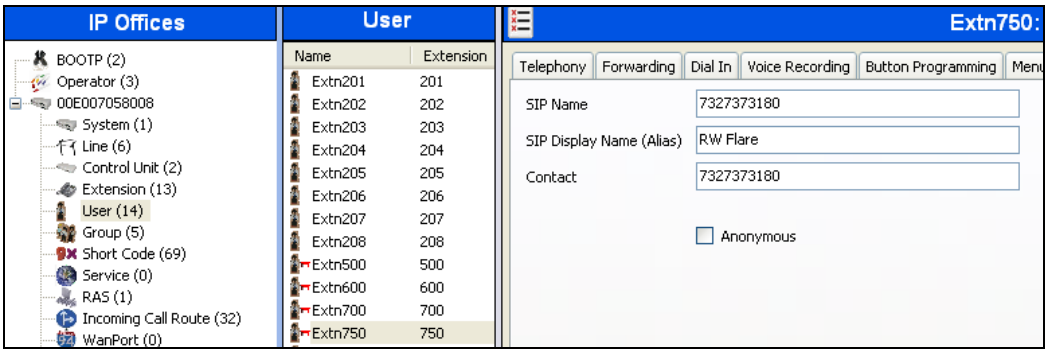
The Remote Worker is provisioned as shown below. Note that since the Remote Worker endpoint used in the reference configuration is Avaya Flare® Experience for Windows, the **Enable Softphone** and **Enable Flare** options are selected.

Note – *Do not* check the **Enable Remote Worker** option. This is only enabled for Avaya IP Office "native" Remote Worker configurations. Not for Remote Worker configurations utilizing the SBCE.



12.2.2.2 SIP Tab

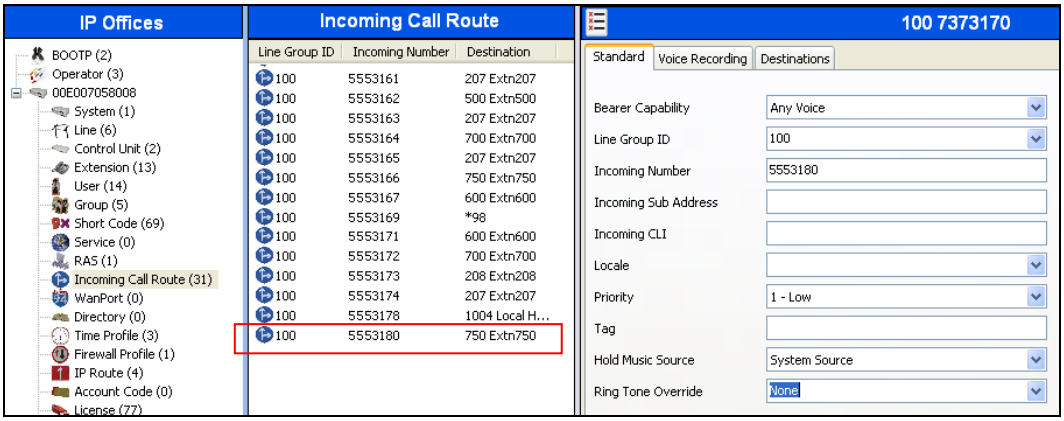
The Remote User is configured with a **SIP Name** and **Contact** specifying the user's associated AT&T number (e.g., **7325553180**).



©2014 Avaya Inc. All Rights Reserved.

12.2.3. Incoming Call Route

Following the procedures described in **Section 5.7**, an Incoming Call Route is defined for calls to the Remote Worker.



12.3. Remote Worker Avaya Flare® Experience for Windows Configuration

The following screens illustrate Avaya Flare® Experience for Windows administration settings for the Remote Worker, used in the reference configuration.

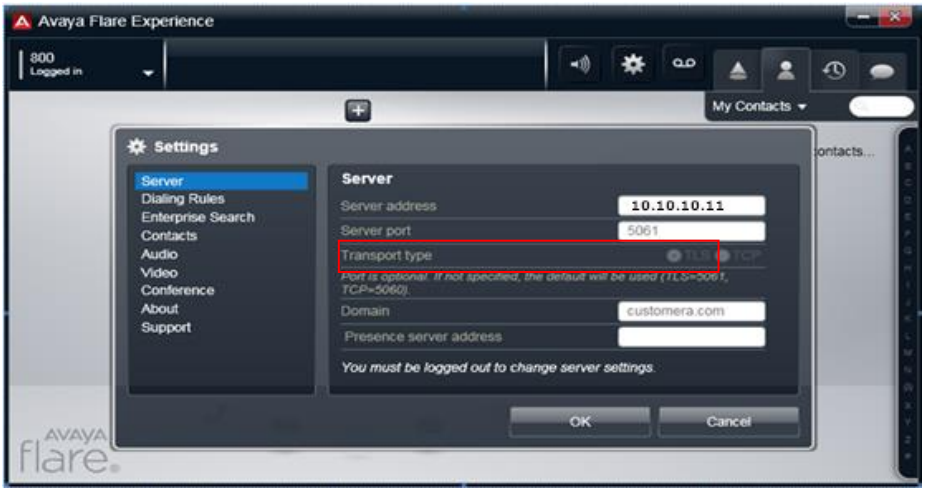
12.3.1. Settings - Server Screen

After opening the Avaya Flare® Experience for Windows application, select the Settings icon , select **Server** from the menu, and enter the following:

- **Server address** = **10.10.10.11**[12] (the IP address of RW virtual interface (B1) of the Avaya SBCE (see **Section 6.1**).
- **Server port = 5061** (note that the Tr**ansport type** will automatically change to TLS).
- **Domain = customera.com** (see the IP Office configuration in **Section 5.3.2**).
- Click on **OK**.

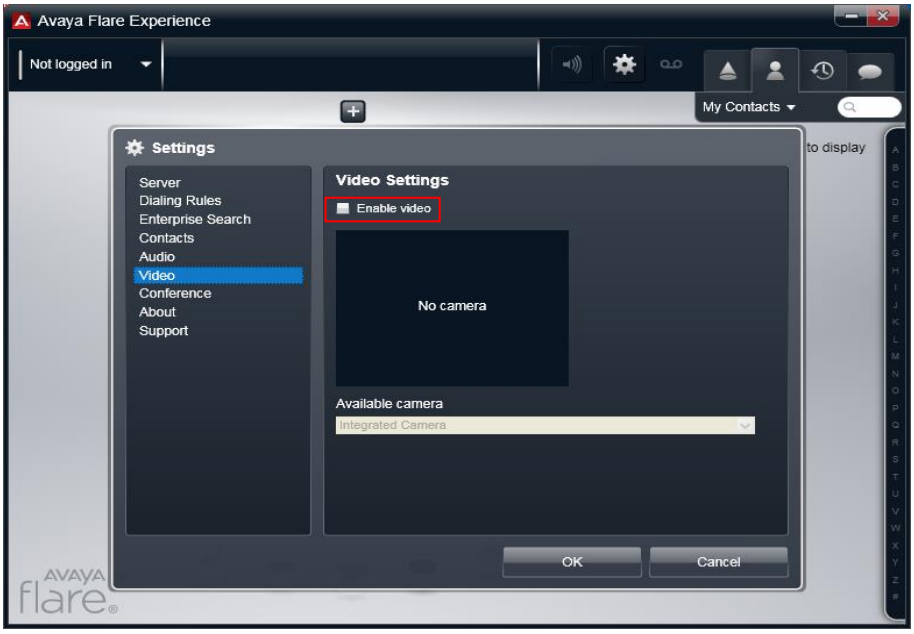
[12] See footnote 1 in **Section 3.2.1**

©2014 Avaya Inc. All Rights Reserved.



12.3.2. Settings - Video Screen

Select **Video** from the menu, then *unselect* the **Enable Video** option. This will enable the Avaya Flare® Experience for Windows to use SRTP (see **Section 12.1.7**).



©2014 Avaya Inc. All Rights Reserved.

©2014 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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