Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office 8.1 Server Edition Solution and Avaya Session Border Controller for Enterprise 6.2 with Wind Telecom SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking in the Avaya IP Office 8.1 Server Edition Solution and Avaya Session Border Controller for Enterprise 6.2 to connect to the Wind Telecom SIP Trunk Service.

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

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking in the Avaya IP Office 8.1 Server Edition Solution and Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2 to connect to the Wind Telecom SIP Trunk Service.

The Avaya IP Office Server Edition solution can be deployed in a pure IP environment, supporting IP endpoints and SIP trunking, or in a hybrid scenario, which provides additional support for TDM stations and trunks. In the sample configuration, a hybrid deployment is used, consisting of the Primary Server running the Avaya IP Office Server Edition Linux software, and an Avaya IP Office Expansion System (V2), on an IP500V2 chassis.

The Avaya SBCE provides UC security for the Avaya IP Office Server Edition solution, as well as interoperability features for the SIP trunk.

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

2. General Test Approach and Test Results

A simulated enterprise site was configured in the test lab using the Avaya IP Office Server Edition Solution and the Avaya SBCE, connected to the Wind Telecom SIP Trunk Service via a SIP trunk over the public Internet. This scenario may differ from a real customer environment, in which a dedicated private network connection could be provided by Wind Telecom to the actual customer site.

The configuration shown in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

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

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types. Phone types included SIP, H.323, digital and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types. Phone types included SIP, H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from soft clients.
- Various call types including: local, long distance, international, outbound toll-free, etc.
- Codecs G729A and G.711MU.
- Direct Media Path for SIP trunks. This feature is currently only supported in Server Edition systems. It enables the redirection of RTP streams on routes other than through the IP Office system, allowing the conservation of VoIP resources.
- G.711 Fax.
- Caller ID presentation and Caller ID restriction.
- DTMF transmission using RFC 2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and twinning.

2.2. Test Results

Interoperability testing with Wind Telecom was completed with successful results with the exception of the observations/limitations described below:

- **OPTIONS** - Wind Telecom was not configured to send OPTIONS messages to the enterprise during the compliance test. The Avaya SBCE will still forward to the network the OPTIONS messages sent periodically by the IP Office to monitor the status of the SIP trunk, to which Wind Telecom responded sending back “200 OK” messages.
- **SIP REFER -** On PSTN calls to or from the enterprise that are transferred back to the PSTN on the SIP trunk, Wind Telecom responds with a “202 Accepted” to the REFER message sent from the enterprise, but the call between the two PSTN endpoints drops. **REFER Support** needs to be disabled in the SIP Line tab in the IP Office for the call transfer to complete, otherwise the call transfer fails. The implication is that the IP Office is not released after the call is transferred, and two trunks remain busy for the duration of the call.

- **Call Forward Unconditional to the PSTN-** On inbound calls that are unconditionally forwarded back to the PSTN, the receiving party in the PSTN will see as the Caller ID the DID number assigned to the forwarding extension in the IP Office, not the number of the originating party. IP Office will not send the originator's number in any of the source headers on the outbound leg of the call, sending the number of the forwarding party in the IP Office instead. This behavior is different to other call forward scenarios, such as "Call Forward/No Answer" or "Call Forward/Busy", where the actual number of the originating party is sent in the From header of the outbound INVITE from the IP Office. A ticket was created for investigation.
- **Fax –** T.38 fax was not tested during the compliance test. There is a known issue with DTMF recognition on inbound voice (non-fax) calls with the SDP format used by Wind Telecom when the IP Office is set to T.38 or T.38 Fallback modes. A fix is expected in a future software load. G711 fax was tested instead, and even though outbound fax calls were consistently successful, inbound fax calls to the enterprise were not reliable.
  For the reasons above, it is recommended not to use fax with this solution at this time.

Note: During the compliance test, the SIP trunk to Wind Telecom was configured to terminate on the Primary Server. On IP Office Server Edition systems, the fax mode supported by the media server on the Primary Server is G.711 fax. T.38 Fax relay is supported across a single IP500 V2 Expansion System or in other scenarios where the Primary Server is not involved (for example, between Expansion Systems (V2) over SIP/Analogue trunks where direct media is used). For this reason, if T.38 were to be used with Wind Telecom in a future software release, the service provider's SIP trunk should be terminated in an Expansion System (V2) and not on the Primary Server. See section "Telephony Operation Configuration" in [**3**] in **Additional References** for considerations and details regarding changes to the routing configuration.

2.3. Support

For technical support on the Wind Telecom SIP Trunk Service offer, visit www.windtelecom.com.do

3. Reference Configuration

Figure 1 below illustrates the test configuration. It shows the enterprise site connected to the Wind Telecom SIP Trunk Service through the public IP network.

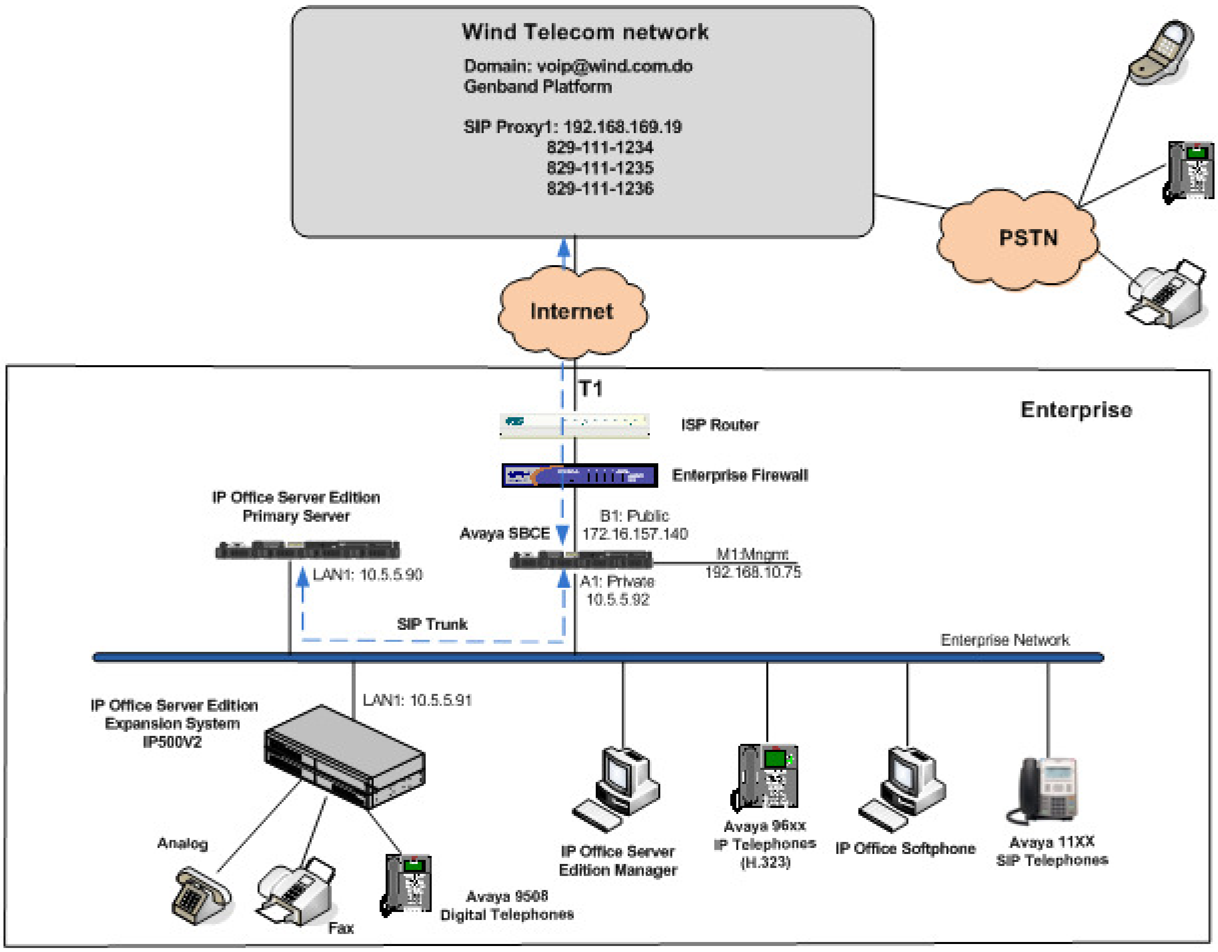


Figure 1: Test Configuration

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

In the sample configuration, the Avaya IP Office Server Edition solution consists of the following main components:

- IP Office Server Edition Primary Server.
- IP Office Server Edition Expansion System (V2)

The Primary Server consists of a HP Proliant DL360 server, running the Avaya IP Office Server Edition Linux software. The server is the only mandatory component required to support SIP trunking and IP endpoints. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of the Primary Server (Eth0) is connected to the enterprise LAN. The LAN2 port (Eth1) was not used during the compliance test. Note that Avaya one-X® Portal for IP Office is installed by default in the Primary Server, but since this application was not used during the compliance test, the configuration of this service is not covered in these Application Notes.

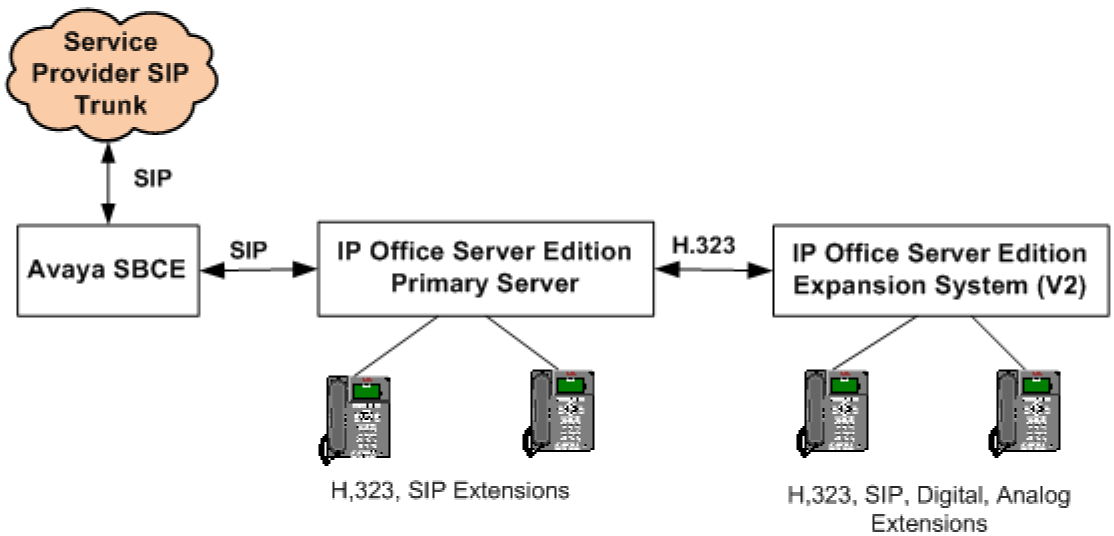
The optional Expansion System (V2) is used for the support of digital, analog and additional IP stations. It consists of an Avaya IP Office 500v2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module). The LAN1 port of the Avaya IP Office IP500V2 is connected to the enterprise LAN. LAN2 was not used.

The Avaya SBCE constitutes the single point of connection between the public network and the Local Area Network in the enterprise. It provides comprehensive security for all SIP and RTP traffic entering the private network, as well as network address translation (NAT) at both the IP and SIP layers. The Avaya SBCE also serves as an interoperability tool between the enterprise and the service provider networks, by allowing the manipulation and adjustment of the SIP headers in the traffic flowing through its interfaces.

IP endpoints at the enterprise include Avaya 96x0 and 96x1 Series IP Telephones (with H.323 firmware), Avaya 1140E IP Telephones (with SIP firmware) and Avaya IP Office Softphones. Some IP endpoints were registered to the Primary Server while others were registered to the Expansion System. Avaya 9508D Digital Telephones and analog telephones are connected to media modules on the Expansion System. The site also has a Windows XP PC running Avaya IP Office Server Edition Manager to configure and administer the system. Mobile Twinning is configured for some of the IP Office users so that calls to these users' extensions will also ring and can be answered at the configured mobile phones.

Even though the IP Office Server Edition solution allows SIP trunks to the service provider to be hosted by any of the servers in the solution, the default call routing settings in the configuration send all potential external calls to the IP Office Server Edition Primary Server, where it is assumed those calls will be routed to SIP trunks hosted in this server. This was the scenario used during the compliance test. Consult [**3**] in **Additional References** for more information and configuration changes needed in other configuration scenarios.

Inbound calls from the service provider SIP trunk first arrive to the Avaya SBCE, where the necessary security checks and interworking manipulation are performed. The call is then sent via SIP trunk to the Server Edition Primary Server, where Incoming Call Routes are checked to determine the call destination. In the event that the destination of the incoming call is an endpoint in the Expansion System (V2), the call is sent via the Small Community Network (SCN) H.323 trunk to the expansion IP500V2 for routing to the final endpoint. This SCN H.323 trunk is automatically created during the initial process of addition of the Expansion System to the IP Office Server Edition solution.



Similarly, outbound calls from the enterprise to the PSTN are routed via the SIP trunk to the Avaya SBCE for interworking treatment before egress to the Wind Telecom network. Calls originated from extensions registered to the Primary Server are routed directly to the Avaya SBCE, while calls originated from extensions on the Expansion System are sent to the Primary Server via SCN H.323 trunk, before being routed to the SIP trunk to the Avaya SBCE.

During the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Wind Telecom. The short code 9 was stripped off by the Avaya IP Office but the remaining N digits were sent unaltered to the network. Since the Dominican Republic is a country member of the North American Numbering Plan (NANP), the users dialed 10 digits for local calls, including the area code, and 11 (1 + 10) digits for other calls between the NANP.

4. Equipment and Software Validated

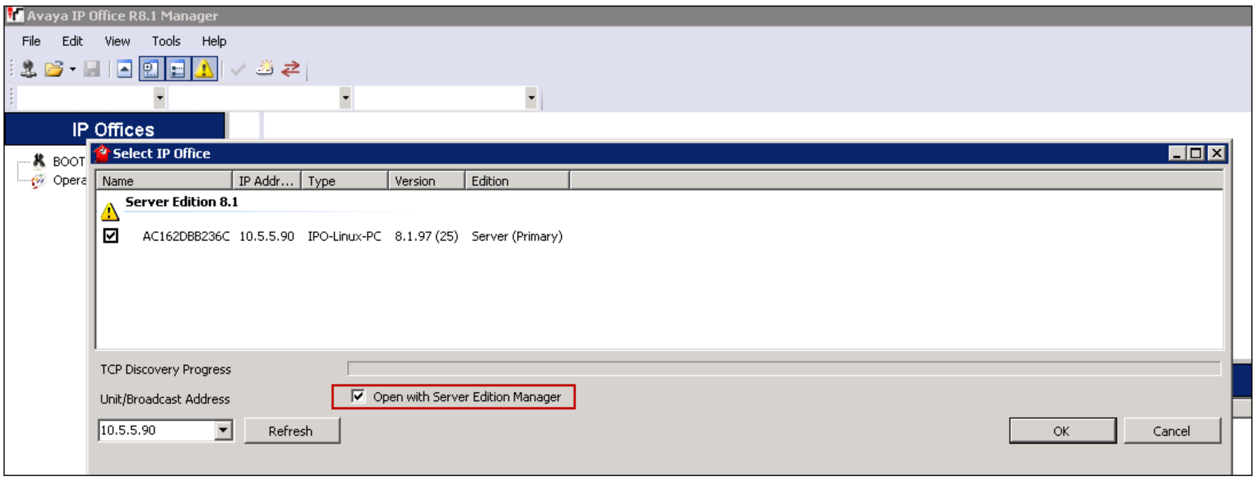
The following equipment and software were used for the sample configuration provided:

Component	Version
Avaya	
Avaya IP Office Server Edition solution • Primary Server HP Proliant DL360 G7 • Voicemail Pro • Expansion System (V2) IP500V2 • Avaya IP Office Analogue Phone 8 Card • Avaya IP Office VCM64/PRID U Card • Avaya IP Office Digital Expansion Module DCPx16	8.1.97(25) 8.1.97-25.el6 8.1.9102.0 8.1 (67) 8.1 (67) 8.1 (67) 10.1 (67)
Avaya IP Office Server Edition Manager	10.1 (67)
Avaya 9620 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.2
Avaya 9611 IP Telephone (H.323)	Avaya one-X Deskphone 6.2
Avaya 1140E IP Telephone (SIP)	04.03.12.00
Avaya Digital Phone 9508	0.45
Avaya IP Office Video Softphone	3.2.3.48.67009
Avaya Session Border Controller for Enterprise, on a Portwell CAD-0208 server	6.2.0.Q36
Wind Telecom SIP Trunk Service	
Genband Softswitch	C20 CVM 14

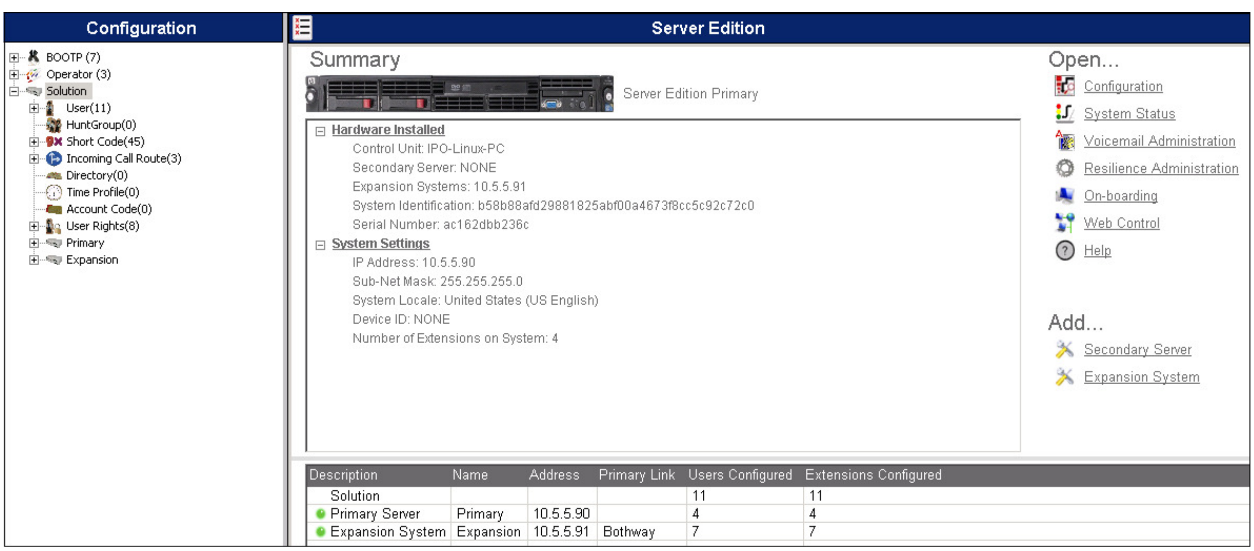
5. Configure Avaya IP Office Server Edition Solution

This section describes the Avaya IP Office Server Edition solution configuration necessary to support connectivity to the Wind Telecom SIP Trunk Service. It is assumed that the initial installation and provisioning of the Server Edition Primary Server and Expansion System has been previously completed and therefore is not covered in these Application Notes. For information on these installation tasks refer to [**1**] in the **Additional References** section.

The solution is configured through the Avaya IP Office Server Edition Manager PC application. From the PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office Server Edition system, making sure the box for **Open with Server Edition Manager** is checked. Log in using the appropriate credentials.



The Solution View screen will appear, similar to the one shown below. This screen includes the system inventory of the servers and links for administration and configuration tasks.



In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center and the Details pane on the right side. These panes will be referenced throughout the rest of this section.

Note that the Navigation pane includes solution settings, under the Solution menu, which apply to all the systems in the Server Edition solution, and individual system settings, each grouped under the Primary Server and the Expansion System menus.

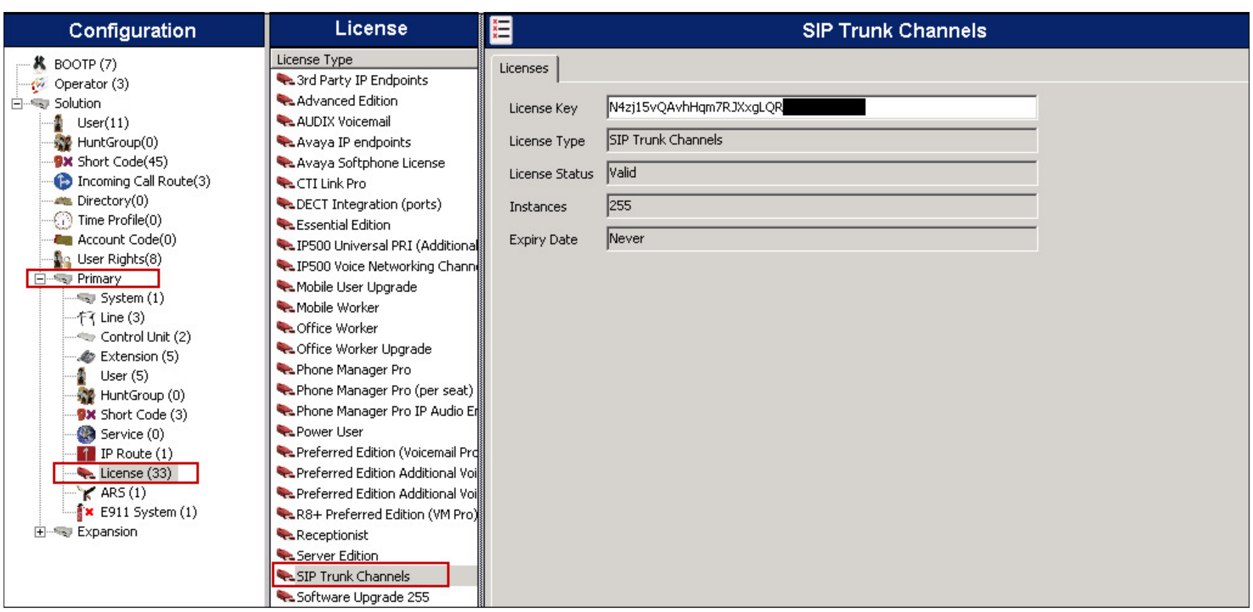
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

5.1. Licensing

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

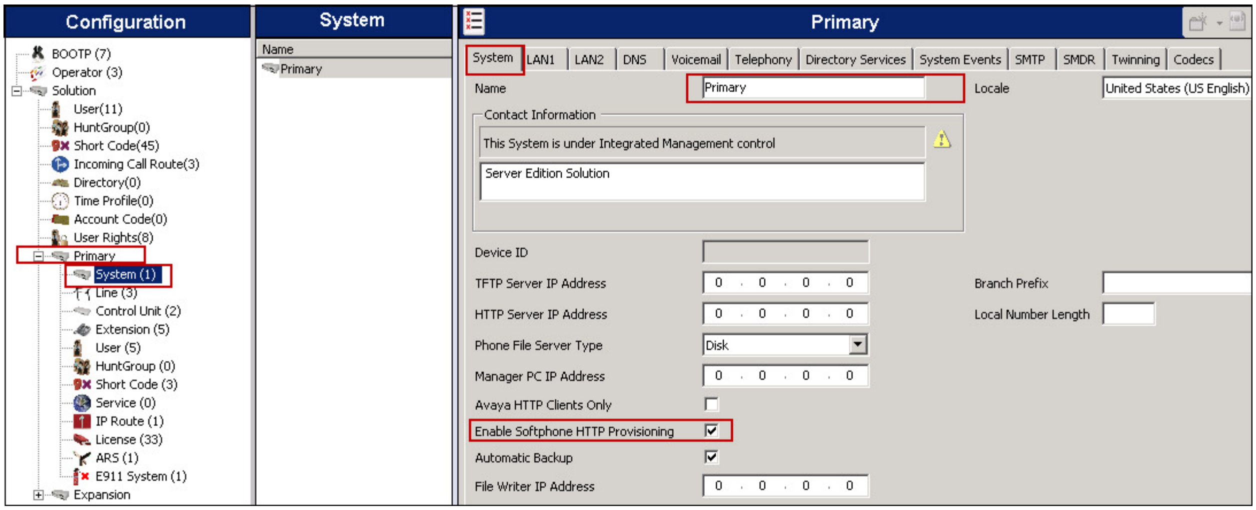
Licenses for an IP Office Server Edition solution are based on a combination of centralized licensing done through the IP Office Server Edition Primary Server, and server specific licenses that are entered into the configuration of the system requiring the feature. SIP Trunk Channels are centralized licenses, and they are entered into the configuration of the Primary Server. Note that when centralized licenses are used to enable features on other systems, such as SIP trunk channels, the Primary Server allocates those licenses to the other systems only after it has met its own license needs.

To verify that there is a SIP Trunk Channels license with sufficient capacity, select **License** under **Primary** on the Navigation pane and **SIP Trunk Channels** in the Group pane. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the Details pane. Note that the actual License Key in the screen below was edited for security purposes.

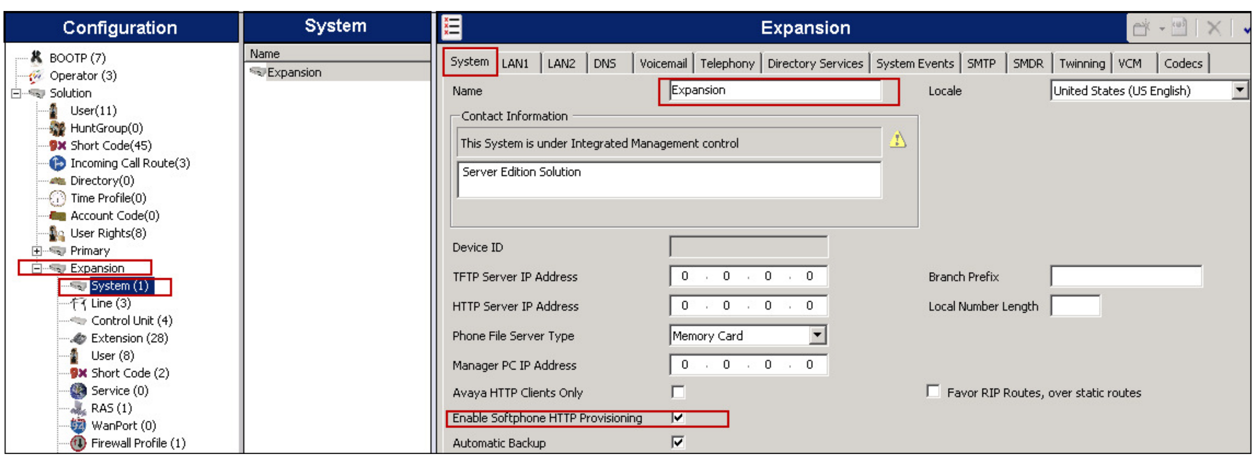


5.2. System Tab

Navigate to **System(1)** under the Primary Server on the left pane and select the **System** tab in the Details pane. The Name field can be used to enter a descriptive name for the system. In the reference configuration, **Primary** was used as the name in the Primary Server. Make sure to check the **Enable SoftPhone HTTP Provisioning** box to enable the support of Avaya IP Office Video Softphone.



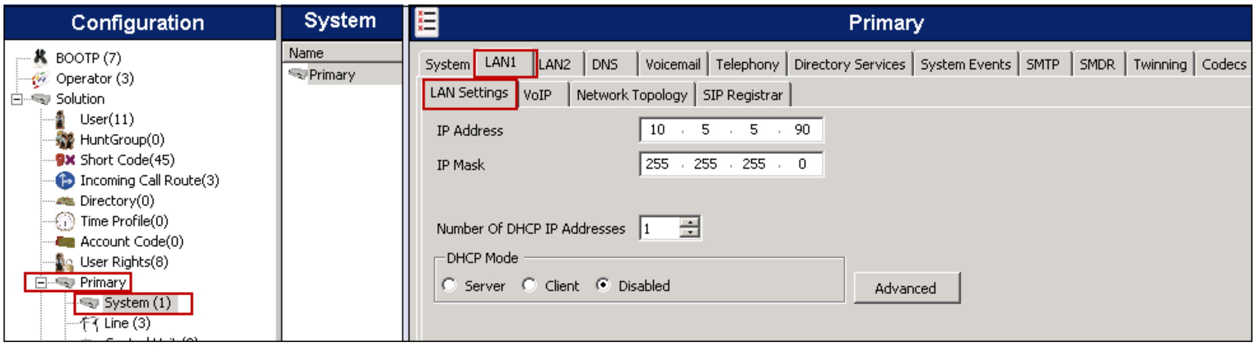
Repeat the steps above, selecting in this case **System(1)** under the Expansion System on the navigation pane to select the settings for the Expansion System. In this case, **Expansion** was used as the system name.



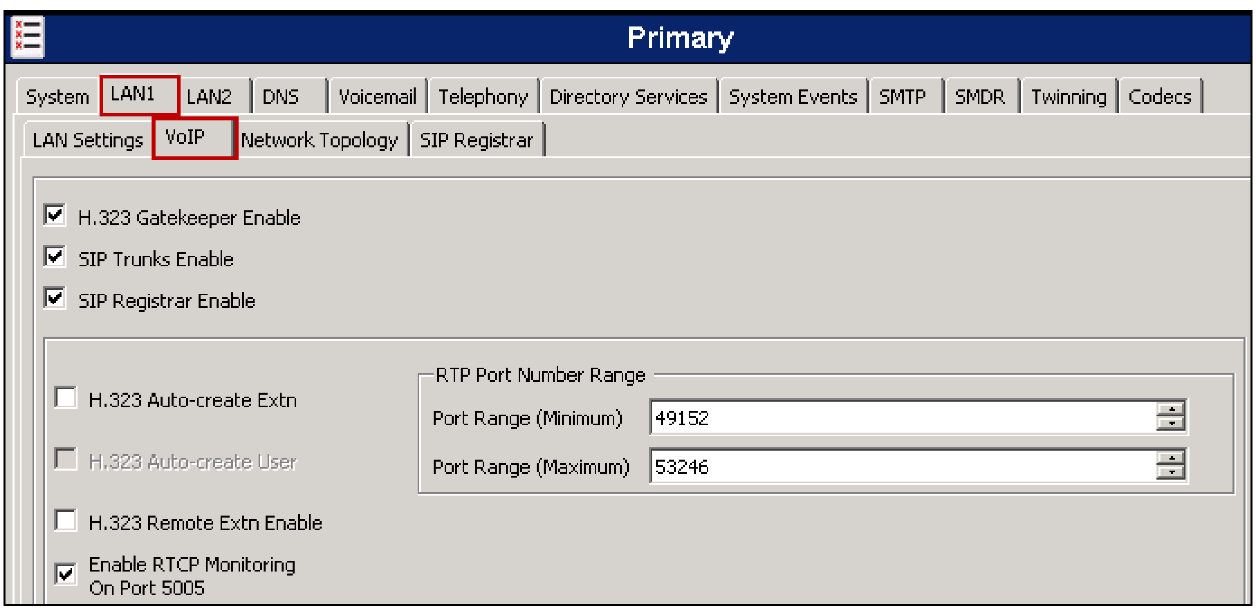
5.3. LAN1 Settings

In the sample configuration, LAN1 is used to connect both the Primary Server and the Expansion System to the enterprise network.

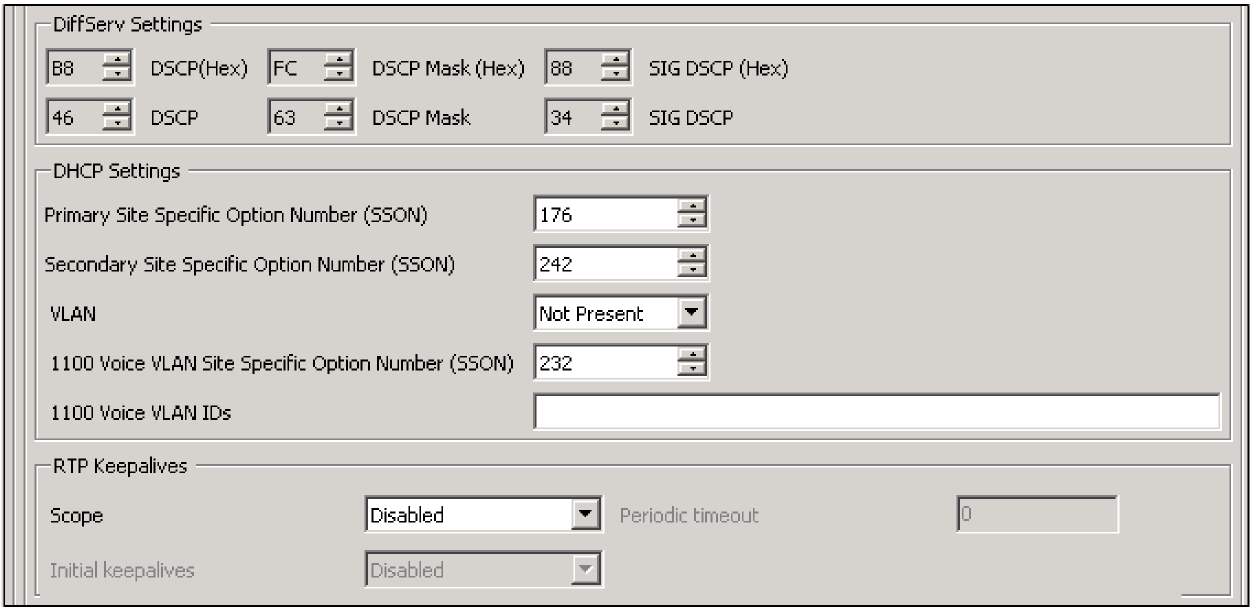
To configure the LAN1 settings on the Primary Server, complete the following steps. Navigate to **Primary → System (1)** in the Navigation pane and then to the **LAN1 → LAN Settings** tab in the Details pane. The **IP Address** and **IP Mask** fields should be populated with the values assigned during the Primary Server initial installation process. Verify the configuration or modify the values if needed. While DHCP was disabled during the compliance test, this parameter should be set according to customer requirements.



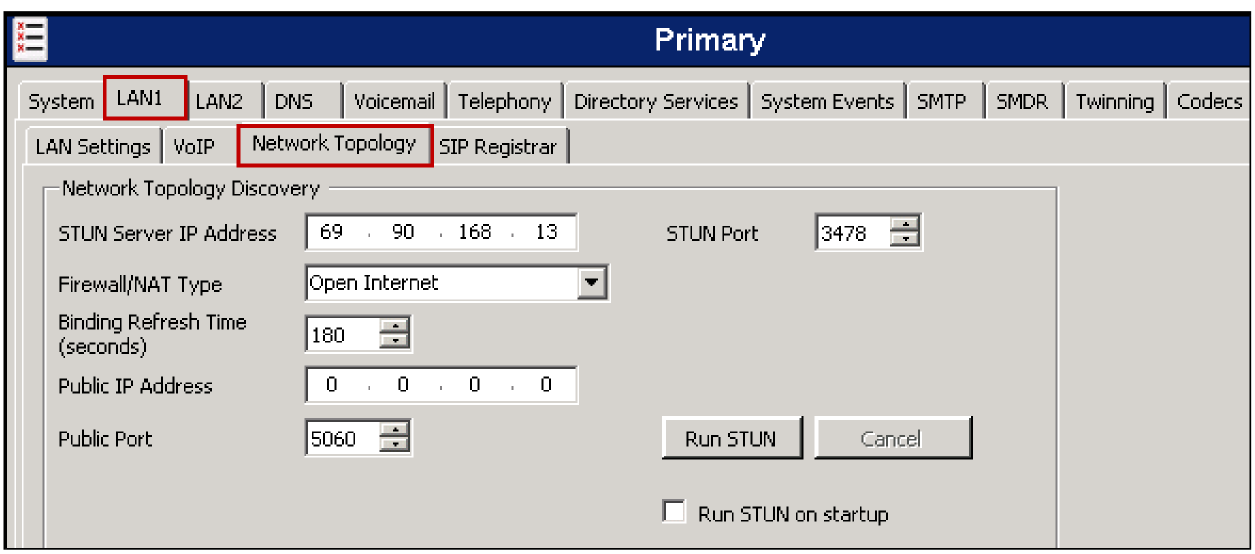
On the **VoIP** tab in the Details pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol. The **SIP Trunks Enabled** box is checked to support SIP trunking. The **SIP Registrar Enable** box is checked to allow Avaya 11xx (SIP) and Avaya IP Office Softphone (SIP) usage. The **RTP Port Number Range** can be customized to a specific range of listening ports for the RTP media. Based on this setting, Avaya IP Office would request RTP media be sent to a UDP port in the configurable range.



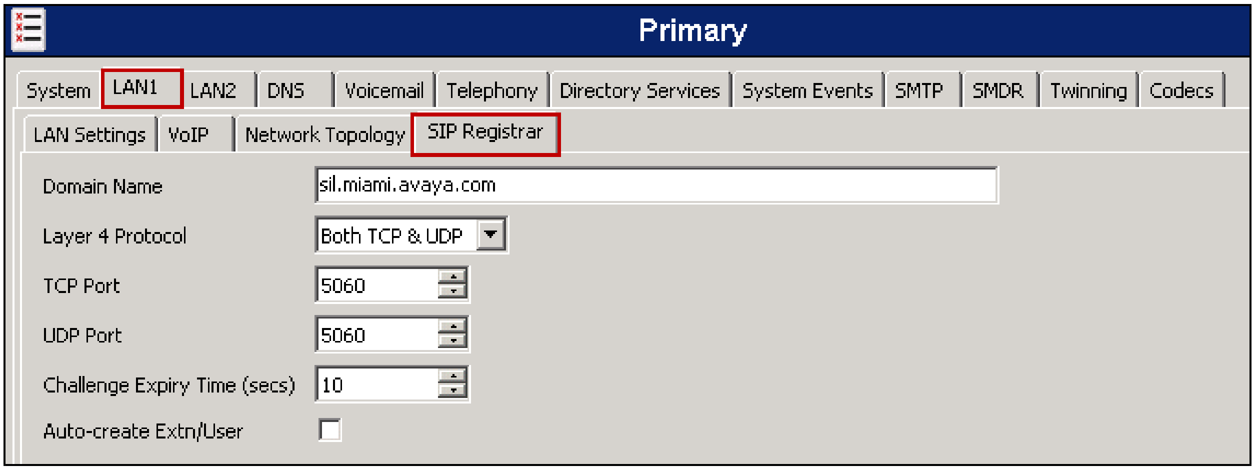
Differentiated Services Code Point (DSCP) can be used to mark the IP header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements.



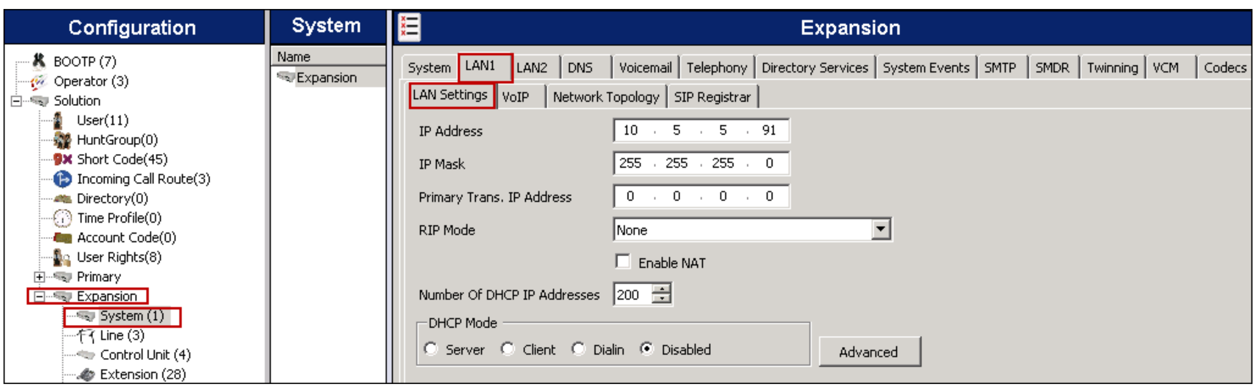
On the **Network Topology** tab in the Details pane, select the **Firewall/NAT Type** from the pull-down menu to ***Open Internet***. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used. Set **Binding Refresh Time (seconds)** to ***180.*** This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. Set **Public Port** to ***5060***. Default values were used for all other parameters.



On the **SIP Registrar** tab in the Details pane, enter the settings to be used for SIP endpoints registering to the system. The **Domain Name** used in the compliance test is shown on the screen below. Default values were used for all other parameters.



To configure the LAN1 settings for the Expansion System, navigate to **Expansion → System (1)** on the Navigation pane and then navigate to the **LAN1 → LAN Settings** tab in the Details pane. The **IP Address** and **IP Mask** fields should be populated with the values assigned during the Expansion System initial installation process. Verify the configuration or modify the values if needed. While DHCP was disabled during the compliance test, this parameter should be set according to customer requirements. Other settings were left at their default values.

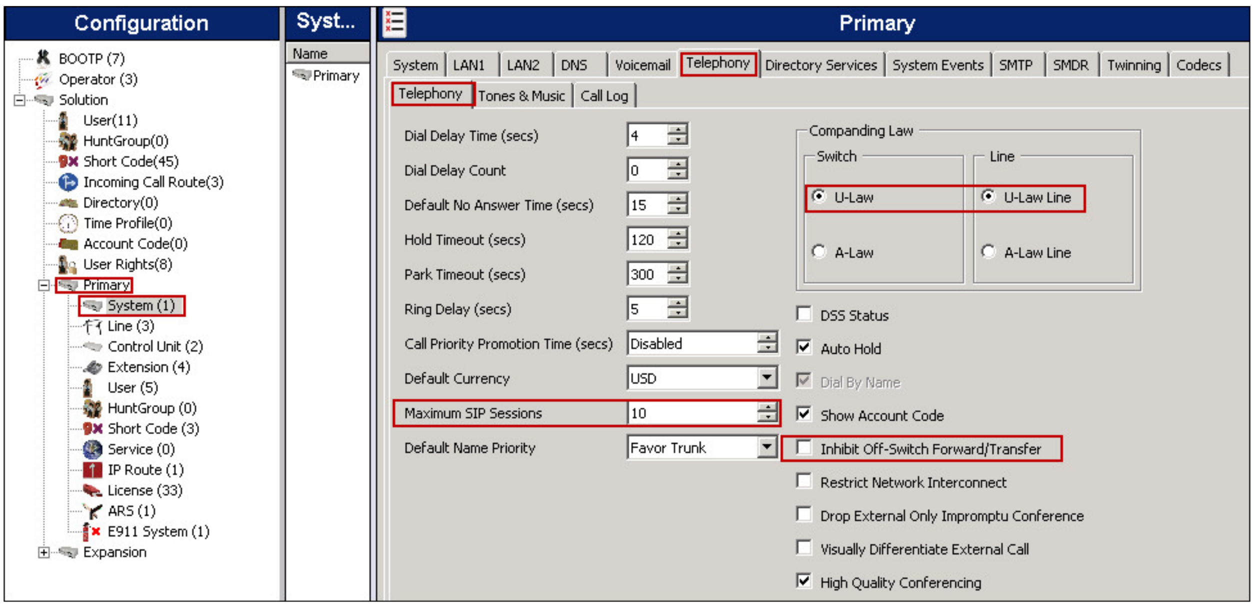


The remaining parameters in the **VoIP**, **Network Topology** and **SIP Registrar** tabs for LAN1 in the Expansion System can be configured using the same values previously described for the LAN1 settings in the Primary Server. Use the configuration steps and screens for these tabs previously shown in this section to complete the configuration of the LAN1 settings in the Expansion System.

5.4. System Telephony Settings

Navigate to **System(1)** under **Primary** on the Navigation pane and then to **Telephony → Telephony** tab in the Details Pane to configure the Telephony settings for the Primary Server. Choose the **Companding Law** typical for the enterprise location. ***U-Law*** was used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the service provider.

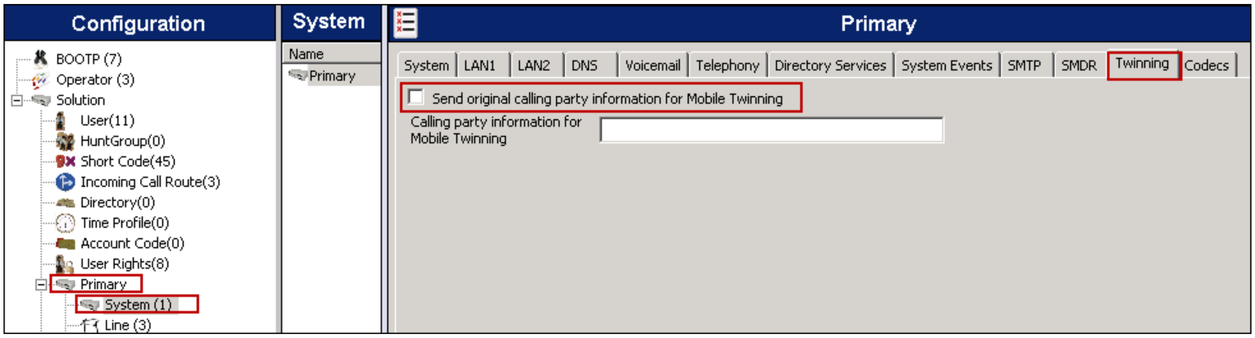
The **Maximum SIP Sessions** field appears only in Server Edition systems. This value determines the number of SIP Trunk Channel licenses reserved for concurrent sessions on SIP trunks provided by this server. These licenses are reserved from the pool of SIP Trunk Channel licenses shown on **Section 5.1**. In the compliance test, **10** sessions were reserved on the Primary Server. Defaults were used for all other settings.



Navigate to **Expansion → System(1)** and repeat the steps above to configure the Telephony settings for the Expansion System. Since the SIP trunk will be terminated on the Primary Server, it was not necessary to enter a value in the **Maximum SIP Sessions** field in this case, and the default value of **0** was used (not shown).

5.5. Twinning Calling Party Settings

Navigate to **Primary → System(1)** on the Navigation pane and to the **Twinning** tab on the Details Pane. Uncheck the **Send original calling party information for Mobile Twinning** box. This will allow the Caller ID for Twinning to be controlled by the setting on the SIP Line (**Section 5.6**). This setting also impacts the Caller ID for call forwarding.



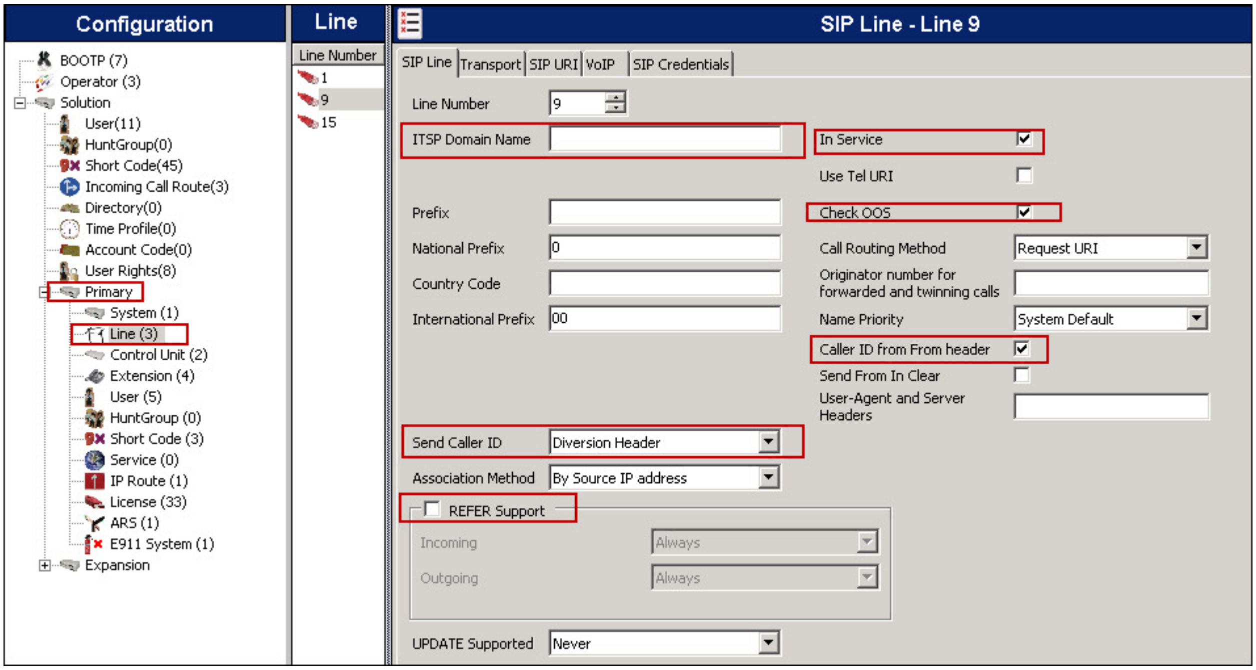
5.6. Administer SIP Line

A SIP line is created to establish the SIP connection between the Server Edition Primary Server and the private interface of the Avaya SBCE. This line will carry all inbound and outbound traffic between the service provider and the enterprise. To create the SIP line, navigate to **Primary → Line** in the Navigation pane. Right-click and select **New→ SIP Line** (not shown).

5.6.1. SIP Line Tab

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

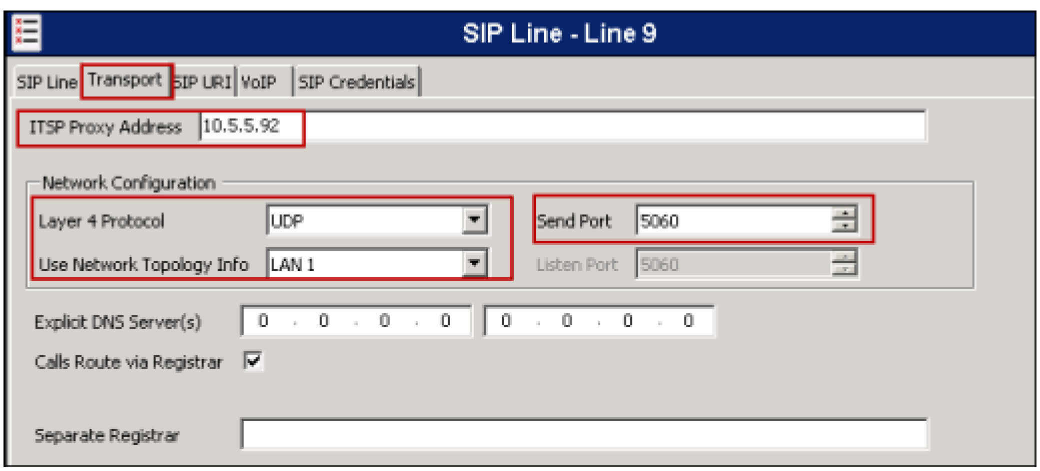
- Leave the **ITSP Domain Name** field blank. With this setting, the IP address of LAN1 in the Primary Server is automatically used in the domain part of the SIP URIs sent to the Avaya SBCE.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, the SIP OPTIONS method will be used to periodically check the SIP Line.
- Check the **Caller ID from From header** box.
- Set **Send Caller ID** to ***Diversion Header.***
- Uncheck the **REFER support** box. IP Office will not send REFER headers for calls that are transferred back to the PSTN. See **Section 2.2** for more information.
- Default values may be used for all other parameters.



5.6.2. Transport Tab

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

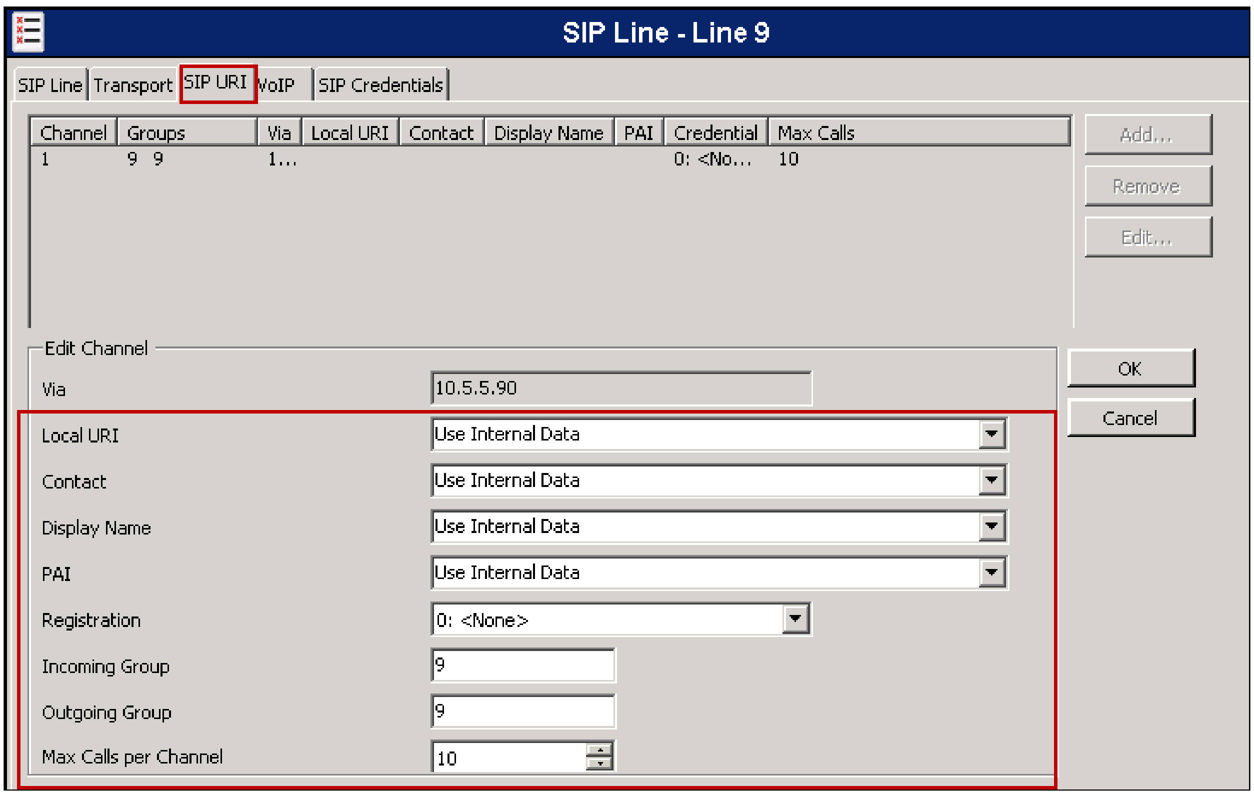
- Set the **ITSP Proxy Address** to the IP address of the private interface of the Avaya SBCE.
- Set the **Layer 4 Protocol** to ***UDP***.
- Set **Use Network Topology Info** to ***LAN1*** as configured in **Section 5.2**.
- Set the **Send Port** to ***5060***.
- Default values may be used for all other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



5.6.3. SIP URI Tab

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

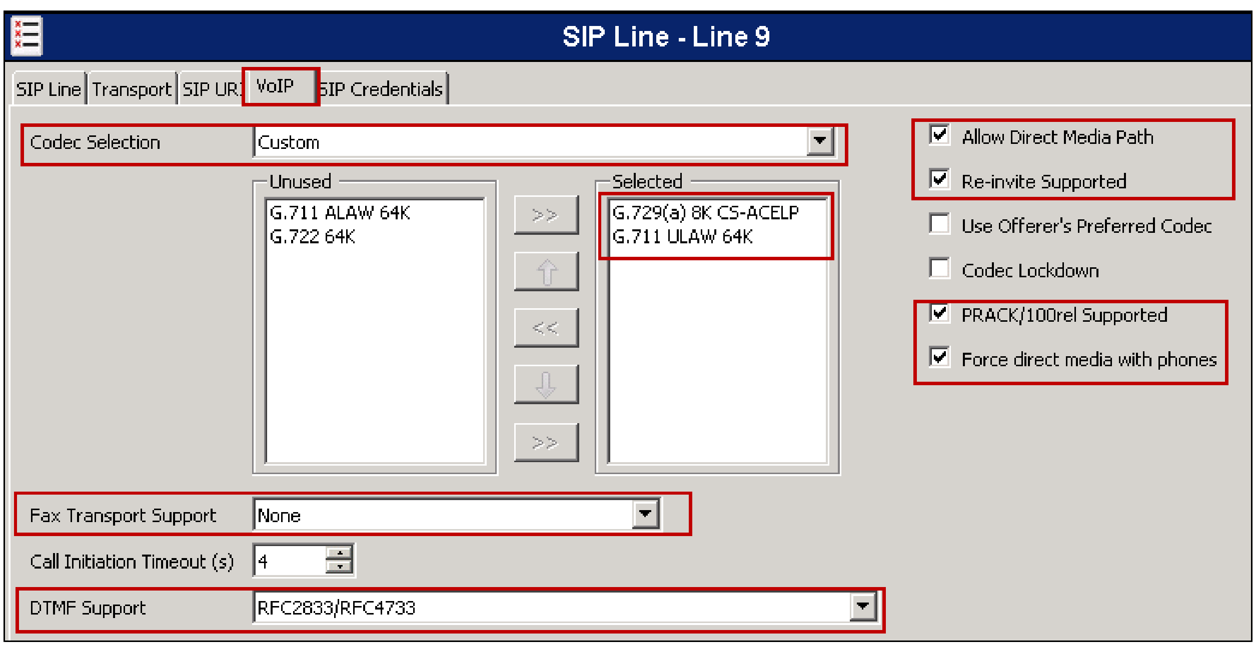
- Set **Local URI**, **Contact**, **Display Name** and **PAI** to ***Use Internal Data***. This setting allows calls on this line whose SIP URI match the number set in the **SIP** tab of any user as shown in **Section 5.7**.
- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group ***9*** was defined that only contains this line (line 9).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.



5.6.4. VoIP Tab

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

- In the sample configuration, the **Codec Selection** was configured using the ***Custom*** option, allowing an explicit ordered list of codecs to be specified. The buttons allow setting the specific order of preference for the codecs to be used on the line, as shown.
- Set **Fax Transport Support** to *None*. See **Section 2.2** for limitations in the use of fax.
- Set the **DTMF Support** field to ***RFC2833/RFC4733.*** With this setting, DTMF tones using RTP events messages will be used.
- Check the **Re-invite Supported** box. This is necessary to allow the use of re-invites used for codec and direct media path re-negotiation.
- Check the **Allow Direct Media Path** box to enable the RTP streams to be re-routed directly between the inside interface of the Avaya SBCE and IP endpoints on the enterprise network, allowing the conservation of VoIP resources in the Primary Server and Expansion System. This box is initially grayed out, and it becomes active only after **Re-invite Supported** is enabled.
- Check the **PRACK/100rel Supported** box, to advertise the support for provisional responses and Early Media to Wind Telecom.
- Check **Force direct media with phones**. This feature applies to H.323 extensions involved in direct media path calls. It allows digits pressed on the extension to be detected, changing to an indirect media call so that DTMF can be sent using RFC2833. The call will remain as an indirect media call for 15 seconds after the last digit press, before reverting back to being a direct media call.
- Default values may be used for all other parameters.

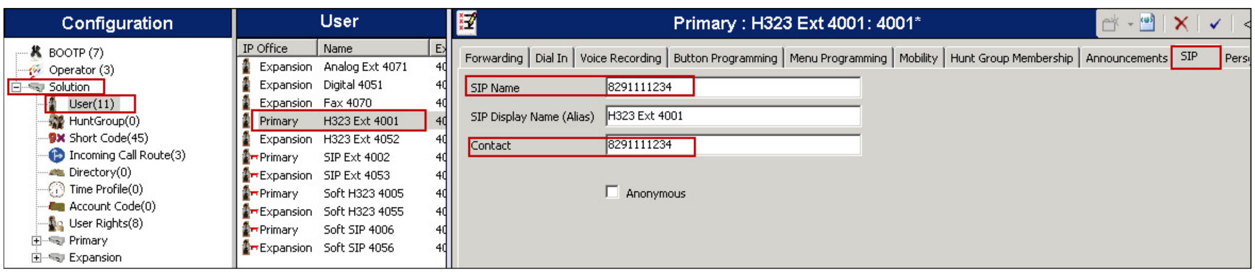


5.7. Users

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.6**, selecting **User** under the corresponding individual system. User settings are additionally grouped under the Solution menu to allow for easy configuration access, as shown on the screen below.

Navigate to **Solution → User** in the left Navigation Pane and then select the name of the user to be modified in the center Group Pane. Select the **SIP** tab in the Details Pane.

The values entered for the **SIP Name** and **Contact** fields will populate the user part of the SIP URI in the From and Contact headers for outbound SIP trunk calls. In addition, the value in the **SIP Name** field is used to match against the SIP URI of incoming calls without having to enter this number as an explicit SIP URI for the SIP line or as a separate Incoming Call Route. The example below shows the settings for user "H323 Ext 4001", a H.323 extension registered to the Primary Server. The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Wind Telecom. In the example, the DID number ***8291111234*** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.



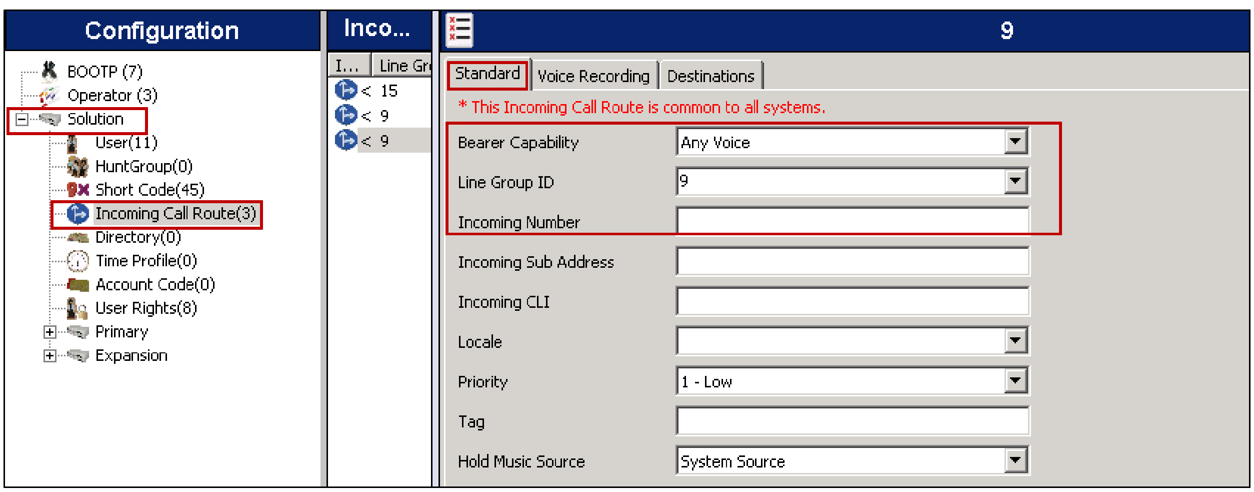
5.8. Incoming Call Route

An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc, within the IP Office Server Edition solution. Note that in Server Edition systems, Incoming Call Routes are solution settings, shared by all the systems in the solution.

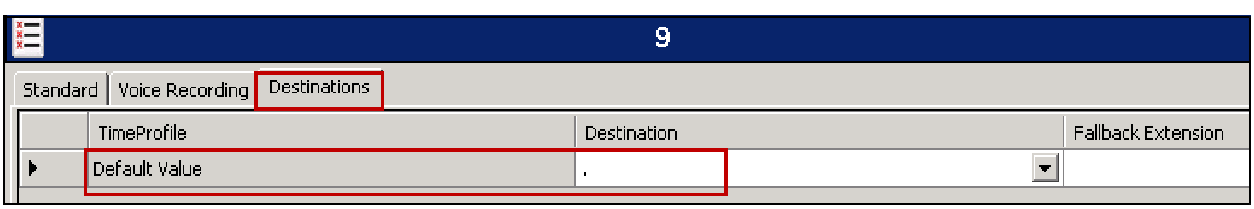
Incoming call routes could be defined for each DID number assigned by the service provider. In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in the IP Office Primary Server or Expansion System. The routing decision for the call is based on the parameters previously configured for the users **SIP Name**, already populated with the assigned Wind Telecom DID numbers **(Section 5.7)**

On the left Navigation Pane, navigate to **Solution**. Right-click on **Incoming Call Route** and select **New.** On the Details Pane, under the **Standard** tab, set the parameters as show bellow:

- Set **Bearer Capacity** to ***Any Voice***.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.6**.
- Leave the **Incoming Number** field blank
- Default values may be used for all other parameters.



- Under the **Destinations** tab, enter "**.**" for **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of that **User,** matching the number present on the user part of the Request URI on the incoming call.

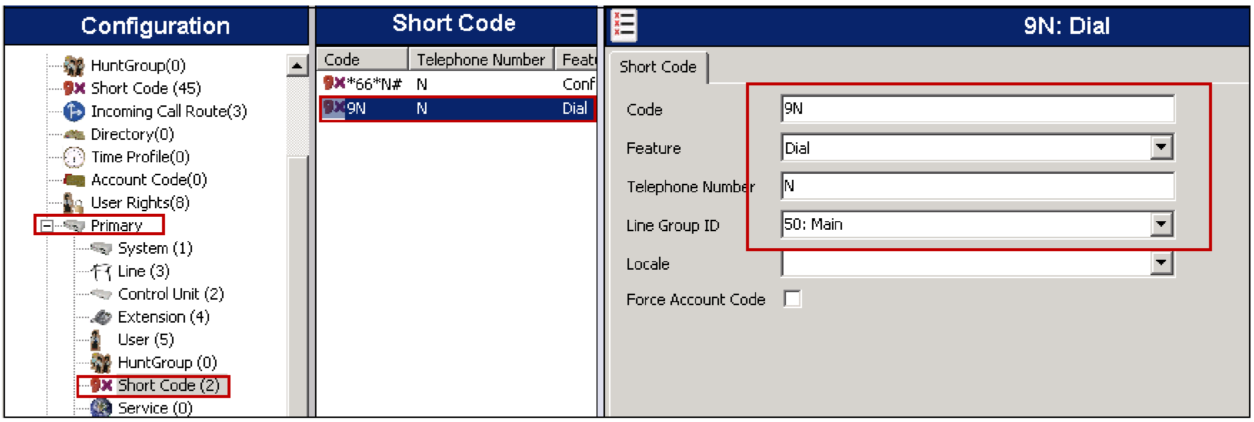


5.9. Outbound Call Routing

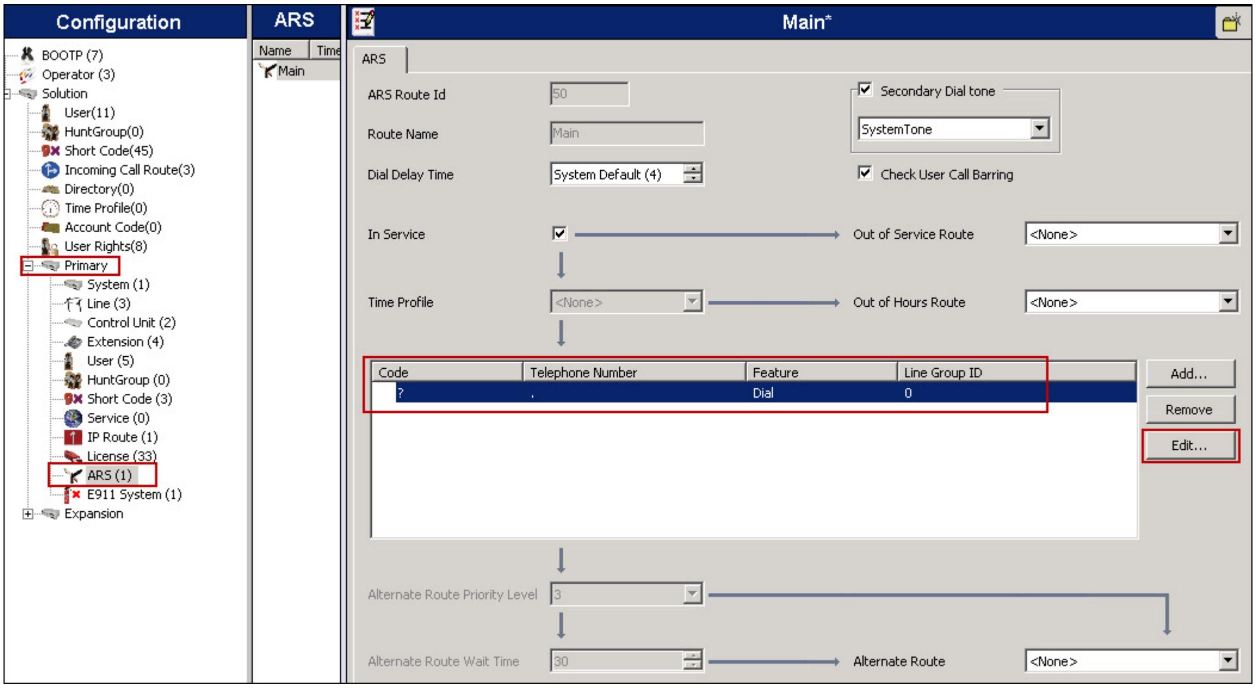
For outbound call routing, a combination of system short codes and Automatic Route Selection (ARS) entries are used. With ARS, features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically if the primary route or outgoing line group is not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

5.9.1. Short Codes and ARS in the Primary Server

On the left Navigation pane, select **Primary → Short Code**. The screen below shows the default short code ***9N***, used in the Primary Server to route the digits ***N*** to **Line Group ID *50: Main***, which is configurable via ARS. No changes were made to the default values on this screen.

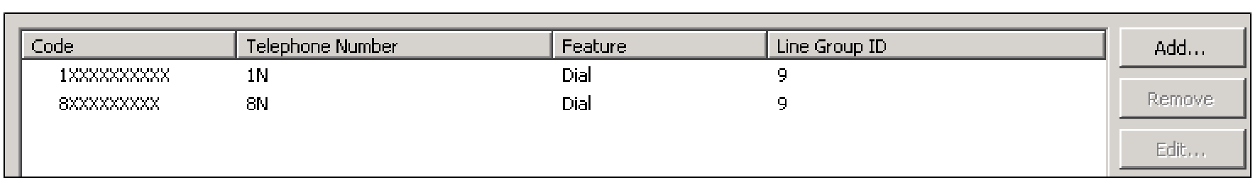


Navigate to **Primary → ARS** on the left pane. The following screen shows the default ARS entry in the Primary Server. Select and edit the existing "***?***" short code to change its **Line Group ID** from the default ***0*** to **Line Group ID *9***, as defined in **Section 5.6**.



This entry can be further edited, or new entries can be defined, to allow for a more granular treatment for different types of calls, and to permit a more specific matching of the telephone number dialed following the access code.

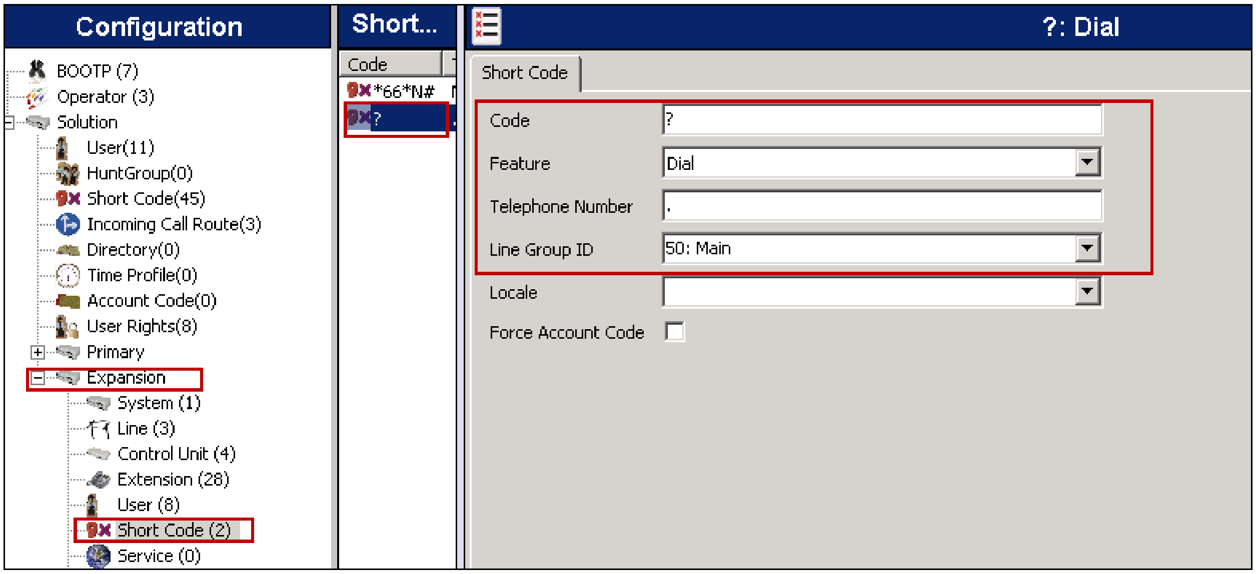
The screen below shows the actual ARS entries created in the test configuration for the route ***Main*** in the Primary Server. The example shows that for local calls, after dialing 9, the user dialed 10 digit numbers starting with an 8. For calls to other area codes in the North American Numbering Plan, the user dialed 9, followed by 11 digits, starting with a 1. In both cases the call is delivered to **Line Group ID *9***. Note the sequence of ***X***s used in the short codes, under the **Code** column, to specify the exact number of digits to be expected, following the access code and the first digit on the string. This type of setting results in a quicker response in the delivery of the call.



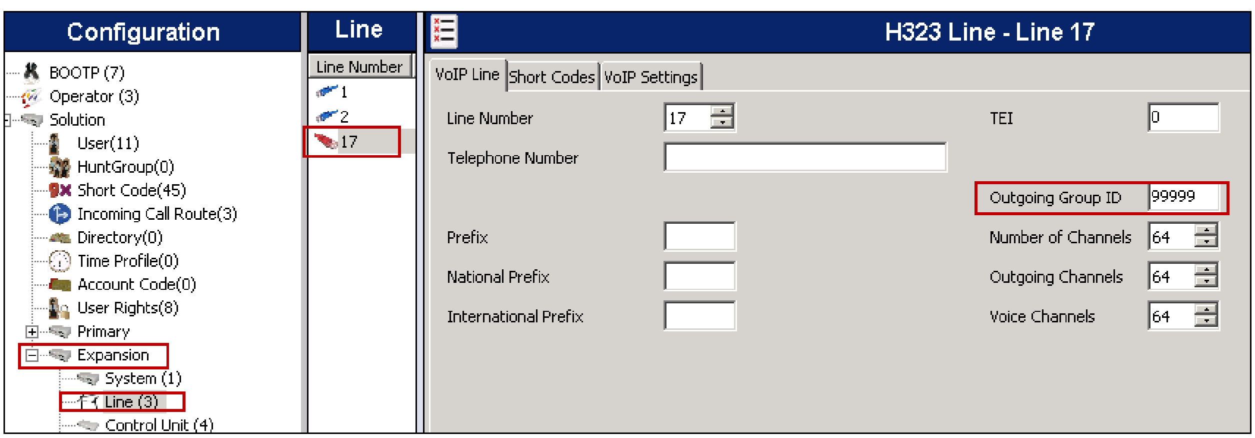
Code	Telephone Number	Feature	Line Group ID
1XXXXXXXXXX	1N	Dial	9
8XXXXXXXXX	8N	Dial	9

5.9.2. Short Codes and ARS in the Expansion System

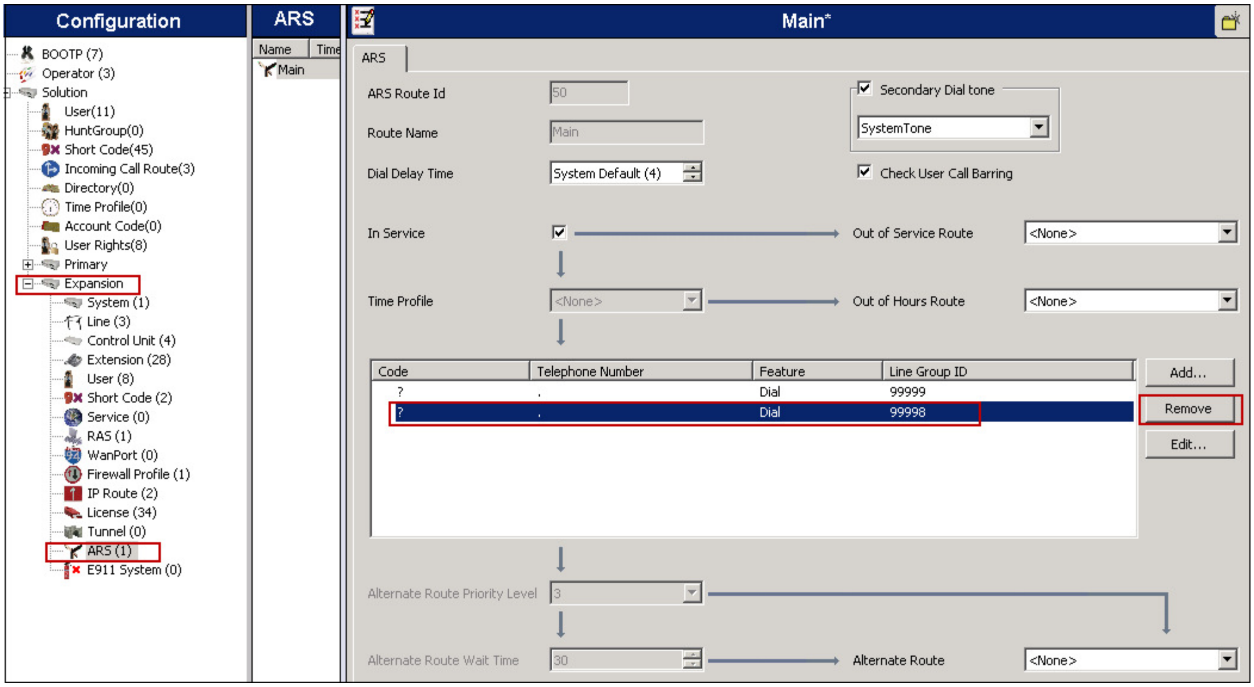
On the left Navigation pane, select **Expansion → Short Code**. The screen below shows the default "**?**" short code present in the Expansion System configuration. This short code routes any dialed number that has no other match to the ARS record ***50:Main*** of this system. No changes were made to the default values on this screen.



Verify the ID of the H.323 line connecting the Expansion System to the Primary Server. To do this, select **Expansion → Line** on the navigation pane and select the H.323 line on the Group pane (line ***17*** on the screen below). Make note of the **Outgoing Group ID** on the Details pane (***99999*** below).



Navigate to **Expansion → ARS** on the left pane. The following screen shows the default ARS entries in the Expansion System. A default "***?***" short code in the ARS entry with **Line Group ID *99999*** is used to route all calls to line 17 (as seen on the previous screen) to the IP Office Server Edition Primary Server. The second entry with **Line Group ID *99998*** would correspond to a H.323 line to a Secondary Server, if available. A Secondary Server was not used in the reference configuration, and this entry was removed by selecting it and clicking the **Remove** button.

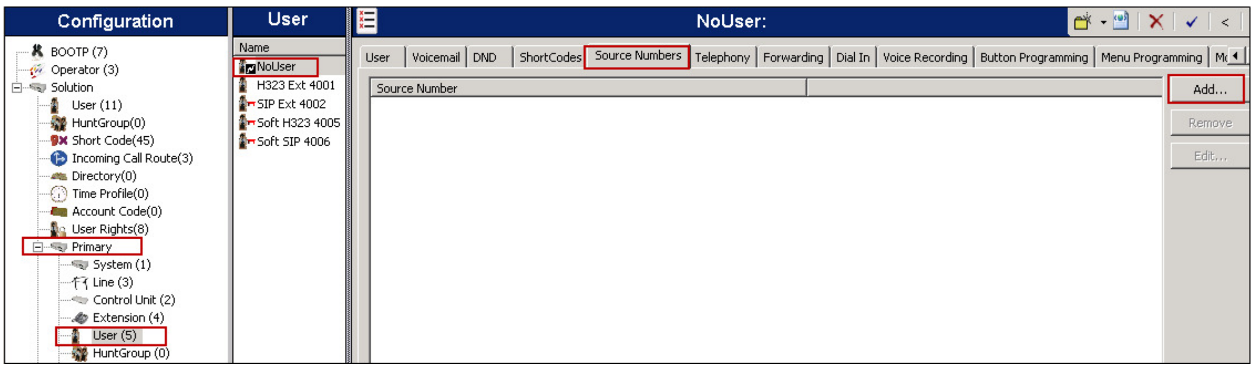


The following example summarizes the settings shown on the previous screens. When a user on the Expansion System dials 9 followed by the number called, the digits are matched to the local ***?/Dial/./Main*** short code, which sends the call to the local ARS ***50:Main***. The ARS routes the call to **Line Group ID *99999***, the H.323 line to the Primary Server, sending the digits unaltered, including the 9 prefix. The digits received at the Primary Server are matched to the ***9N/Dial/N/Main*** system short code. This routes the call to ARS ***50:Main*** on the Primary Server, having removed the 9 prefix. The ARS then routes the call to **Line Group ID *9*,** the external SIP trunk to the Avaya SBCE.

5.10. Privacy/Anonymous Calls

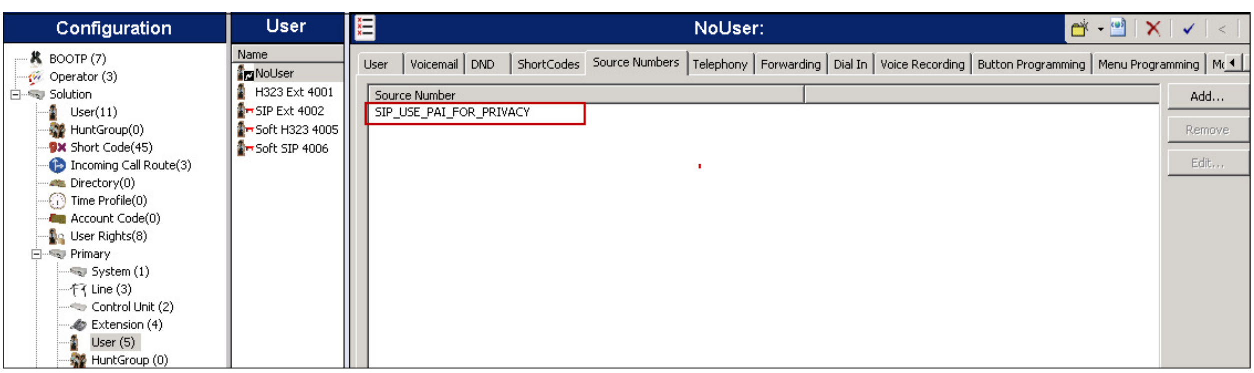
For outbound calls with privacy (anonymous) enabled, Avaya IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with “restricted” and “anonymous” respectively. Avaya IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity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

To configure Avaya IP Office to use PAI for privacy calls, navigate to **Primary → User** on the left navigation pane and select **NoUser** in the Group pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button.



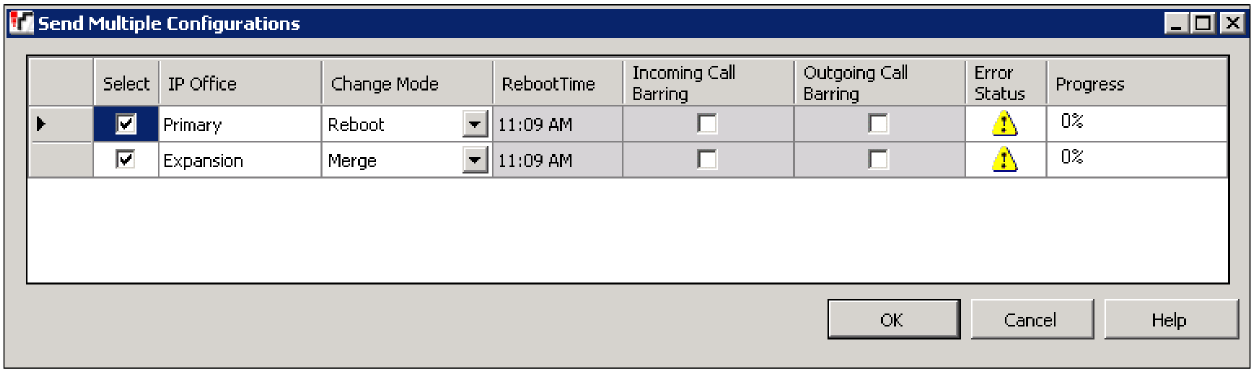
At the bottom of the Details Pane, the **Source Number** field will appear. Enter ***SIP_USE_PAI_FOR_PRIVACY***. Click **OK**.

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



5.11. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top left of the screen to save the configuration performed in the preceding sections. A screen like the one shown below is displayed, showing details for those systems where the system configuration has been changed and needs to be sent back to the system. **Reboot** or **Merge** is shown for each system under the **Change Mode** column, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration.

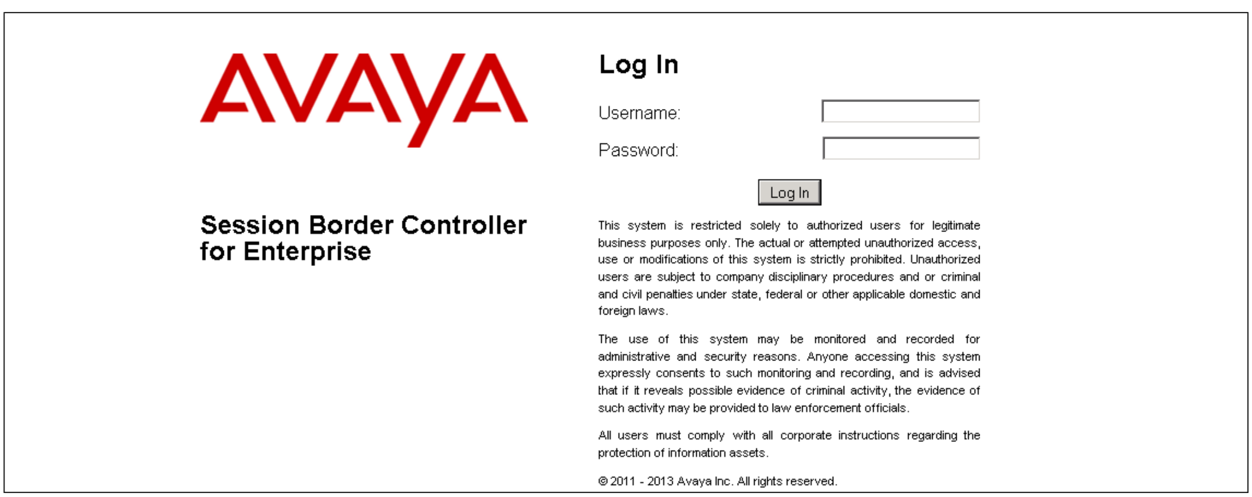


6. Configure Avaya Session Border Controller for Enterprise

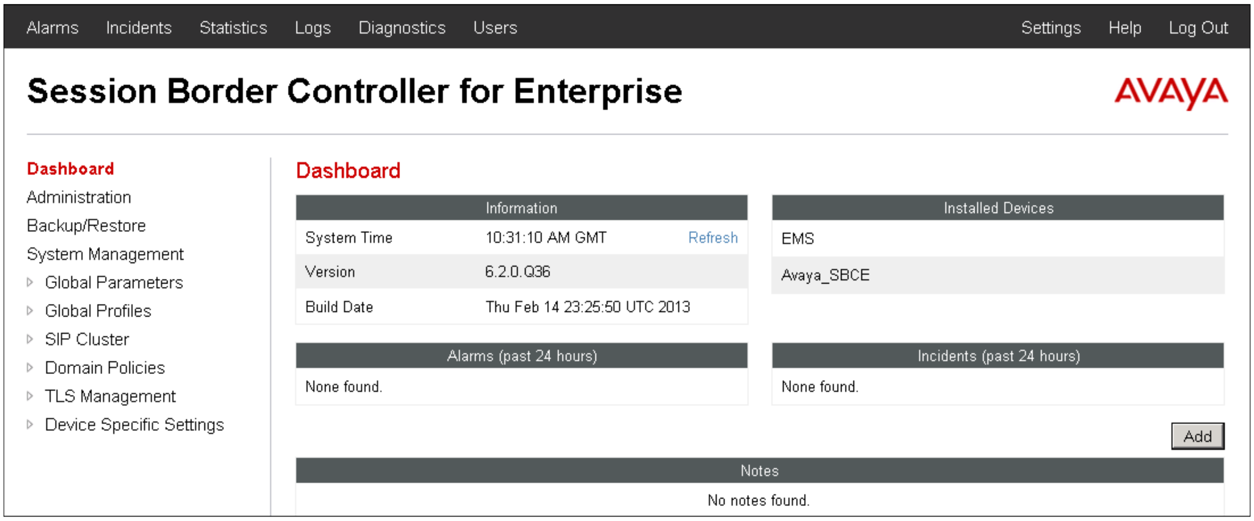
In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Wind Telecom SIP Trunking Service. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult [**5**] and [**6**] in the **Additional References** section.

6.1. System Access

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

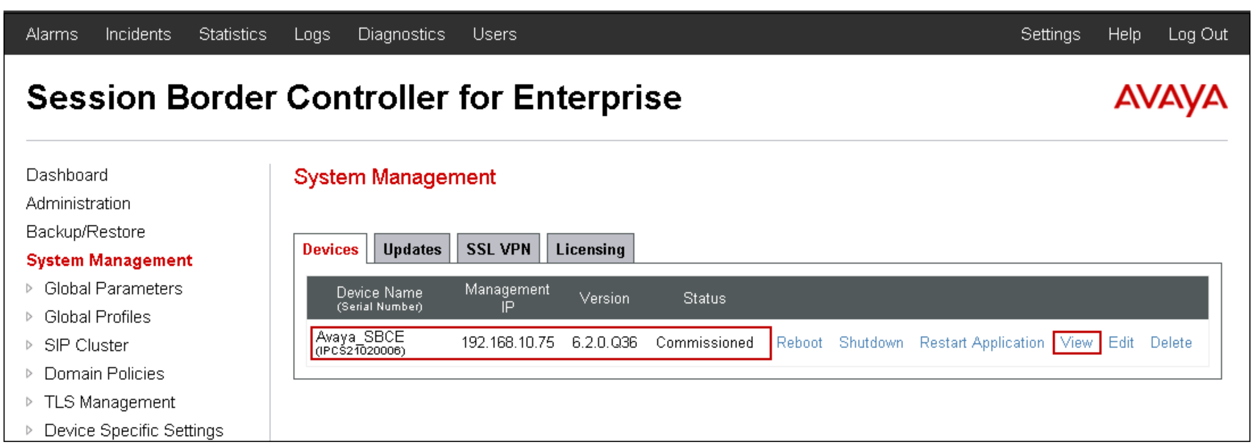


Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.

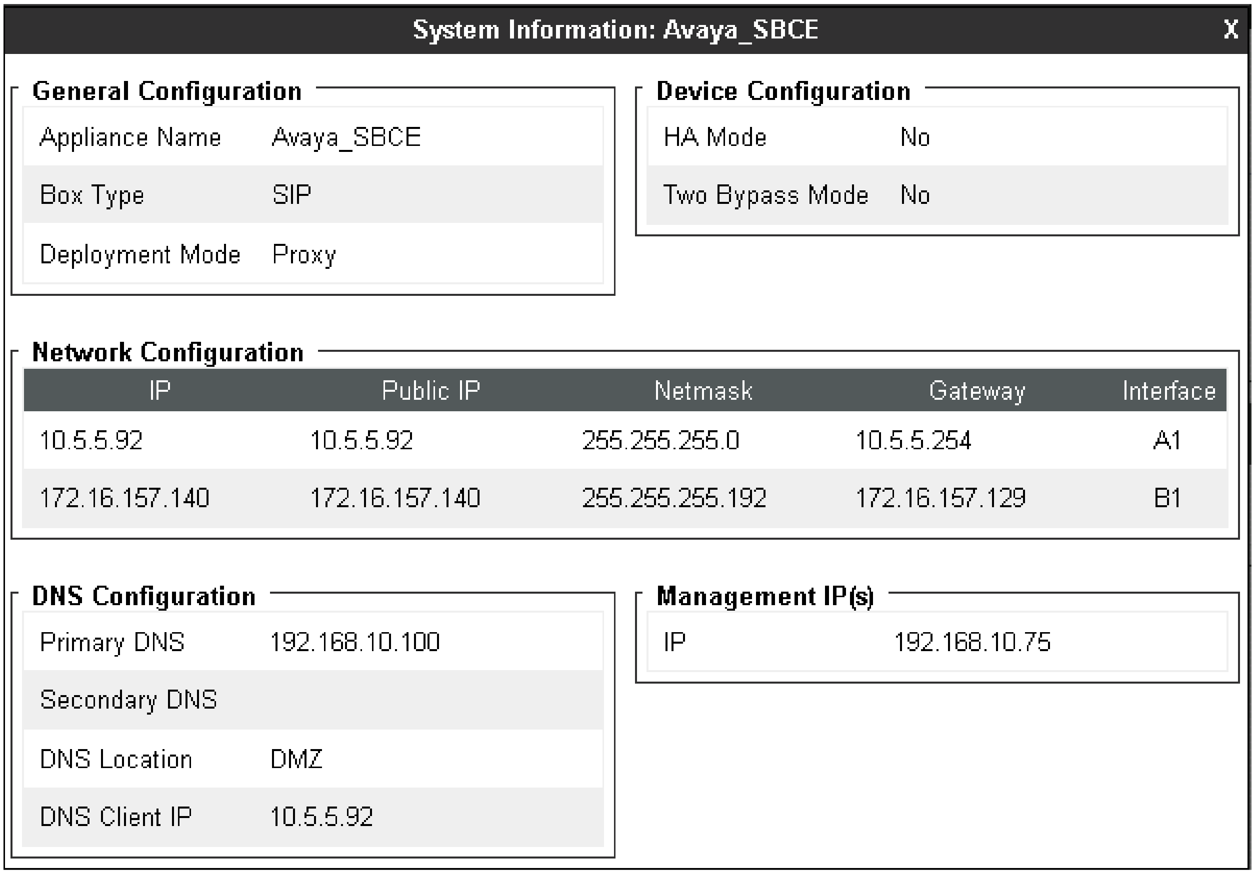


6.2. System Management

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



To view the network information assigned to the Avaya SBCE, click **View** on the previous screen. The **System Information** window is displayed as shown below.



The **System Information** screen shows the current device and the network settings**.** Note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces for the Avaya SBCE, as shown in **Figure 1** in **Section 3**.

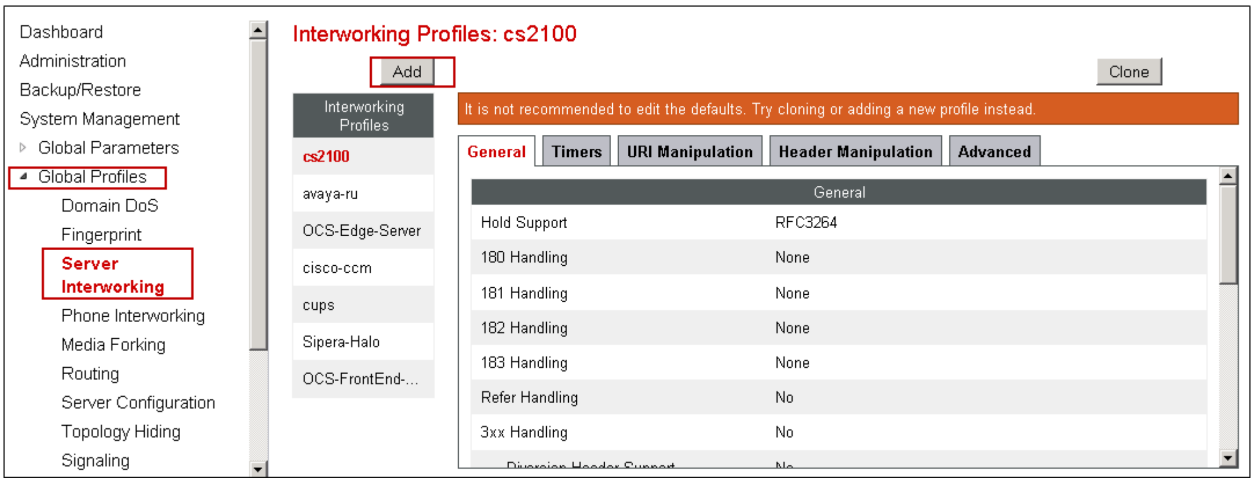
6.3. Global Profiles

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

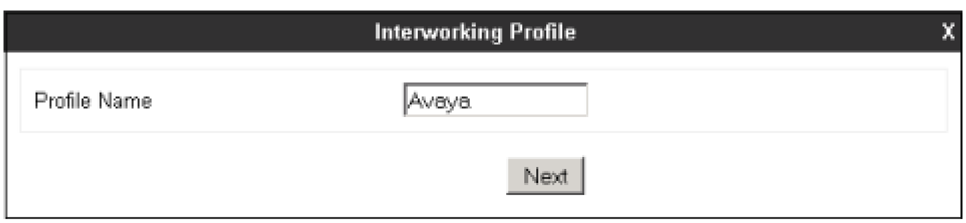
6.3.1. Server Interworking

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

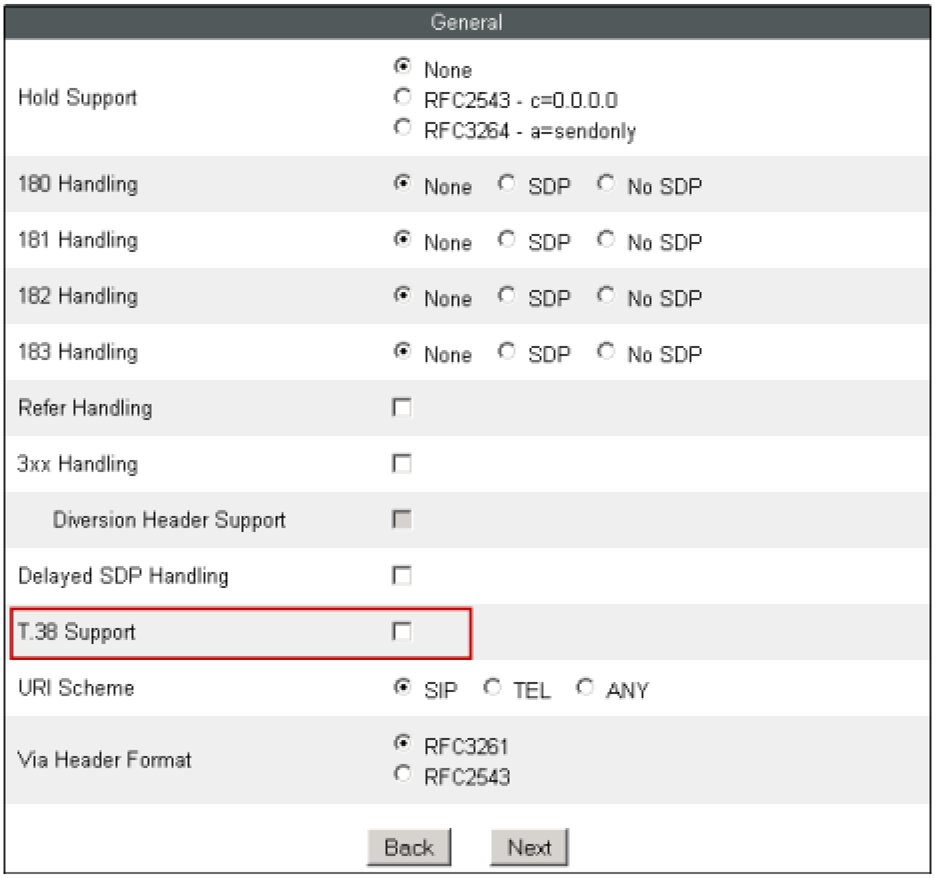
To configure the interworking profile in the enterprise direction, select **Global Profiles → Server Interworking** on the left navigation pane. Click **Add**.



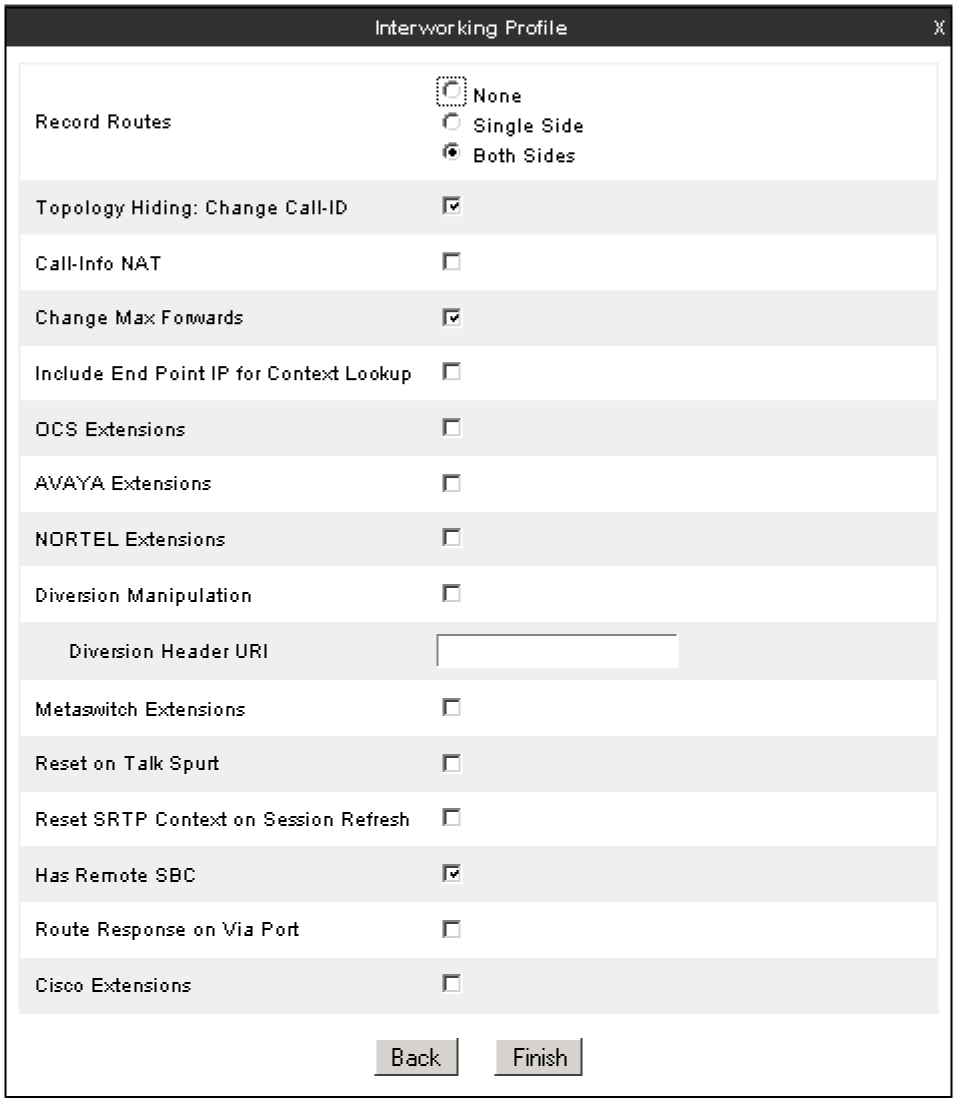
Enter a descriptive name for the new profile. Click **Next**.



On the **General** screen, leave the **T.38 Support box** unchecked, since T.38 fax should not be used with this solution. All other parameters retain their default values. Click **Next**.

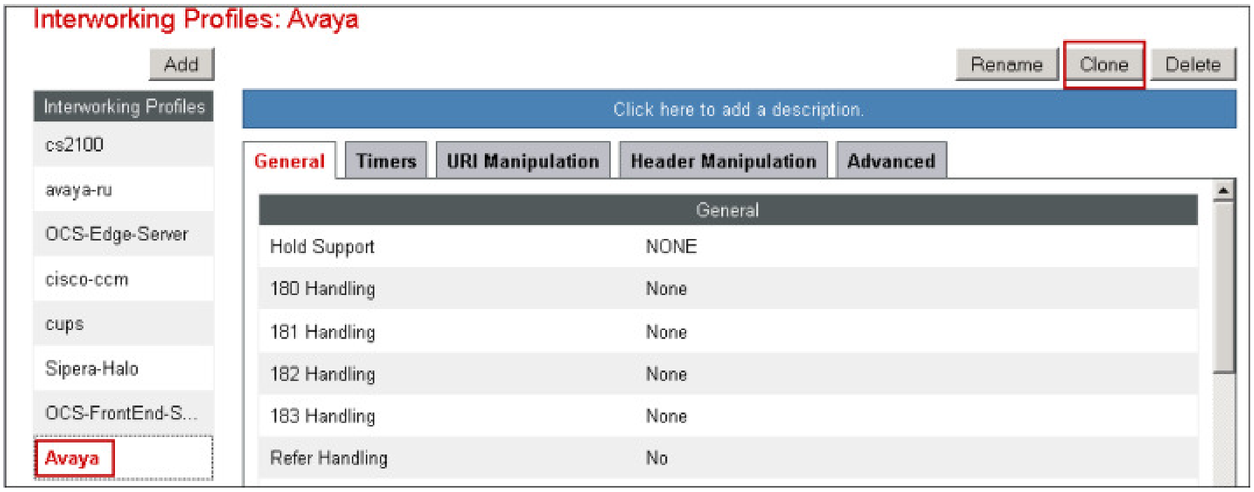


Click **Next** on the **Privacy/DTMF** and **SIP Timers/Transport Timers** tabs (not shown). On the **Advanced Settings** tab, accept the default values and click **Finish** to save and exit.

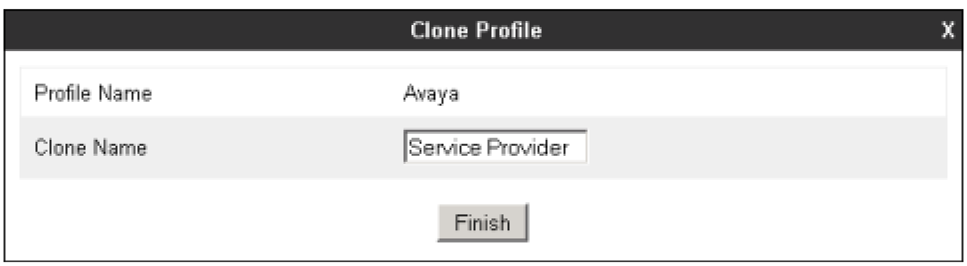


A second interworking profile named ***Service Provider*** in the direction of the SIP trunk to Wind Telecom was created, using the same settings specified previously for the profile in the enterprise direction. This is done with the purpose of allowing changes to be made to one of the profiles in the future if needed, without affecting the settings in the profile for the other direction.

On the Interworking Profiles screen, select the ***Avaya*** profile previously created and click **Clone**.

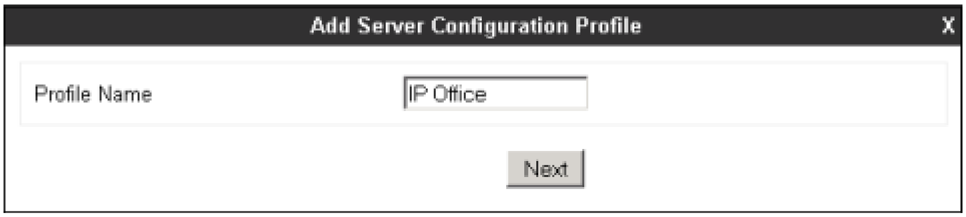


Under **Clone Name** enter the new profile name. Click **Finish** to save and exit.

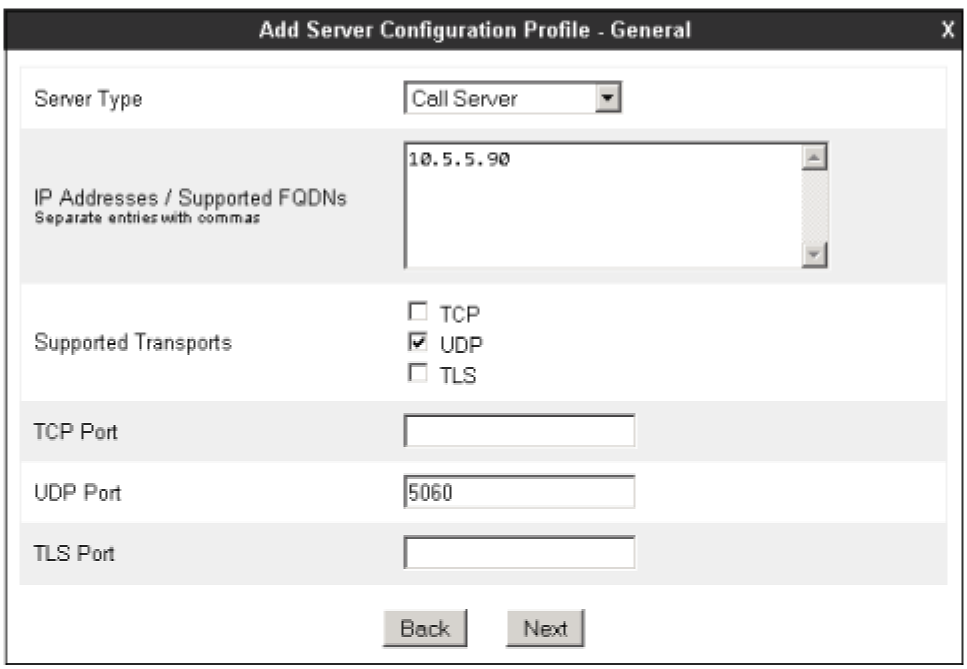


6.3.2. Server Configuration

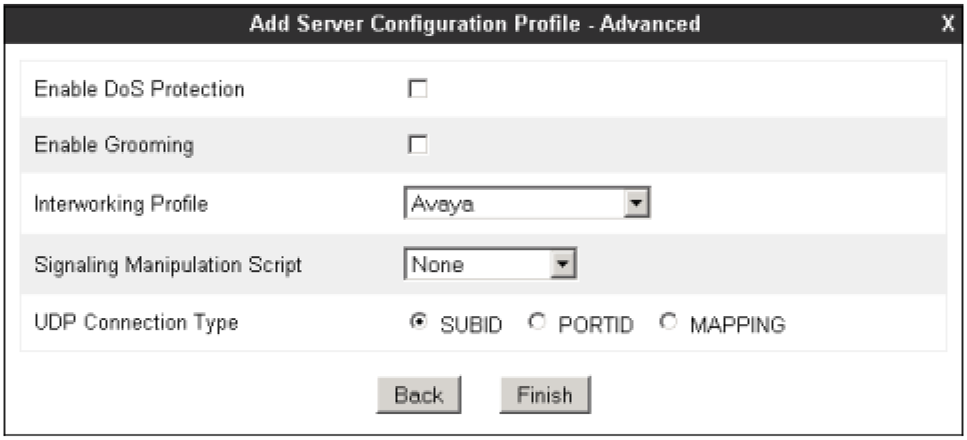
Server Profiles are created to define the parameters for the Avaya SBCE two peers, i.e., the IP Office Primary Server (Call Server) and the SIP Proxy at the service provider's network (Trunk Server). From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and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



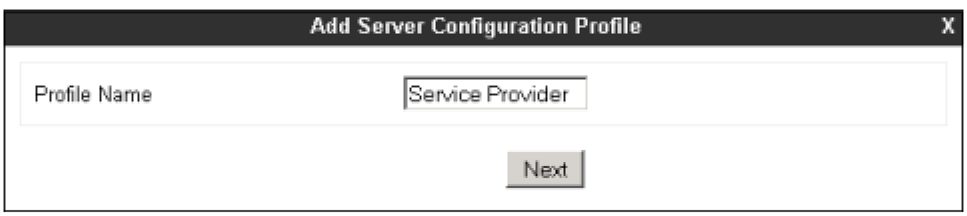
On the **Add Server Configuration Profile - General** Tab select ***Call Server*** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field**,** enter the IP address of the IP Office Primary Server LAN1, as defined in **Section 5.3**. Select **UDP** for **Supported Transports**, and enter ***5060*** under **UDP Port**. The transport protocol and port selected here must match the values used on the IP Office SIP line on **Section 5.6**. Click **Next**.



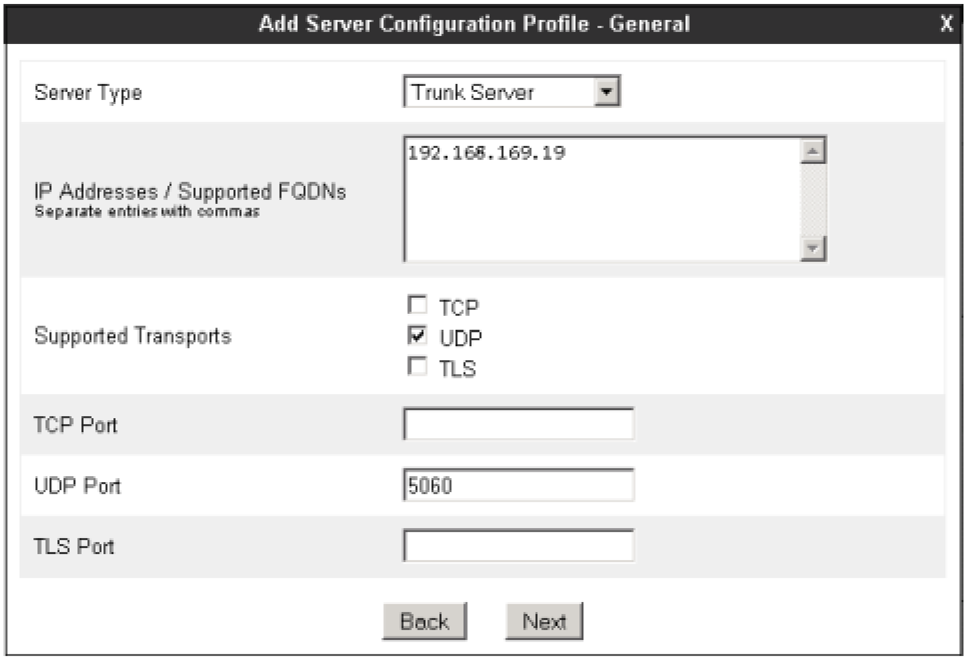
Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, select ***Avaya*** from the **Interworking Profile** drop down menu. Leave **Signaling Manipulation Script** set to the default ***None*** at this time. This screen will be re-visited later in the configuration process. Click **Finish**.



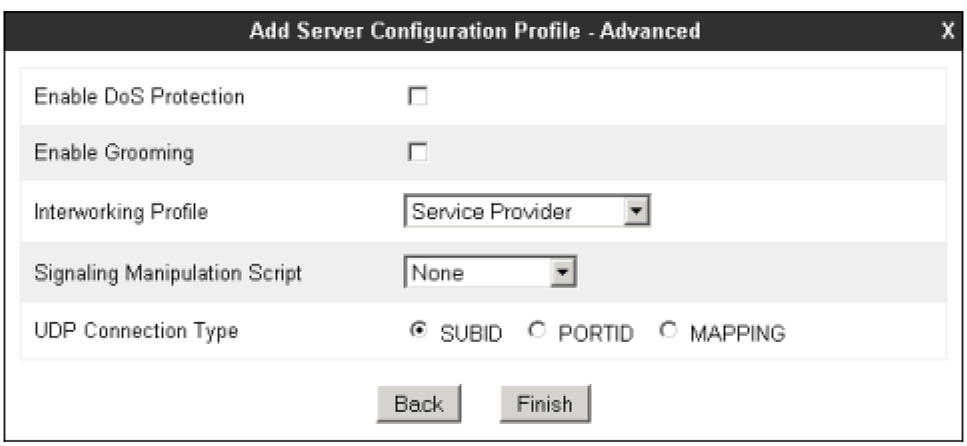
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown). Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



On the **Add Server Configuration Profile - General** Tab select ***Trunk Server*** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field**,** enter ***192.168.169.19***, the IP Address of Wind Telecom's SIP proxy server. Select **UDP** for **Supported Transports**, and enter ***5060*** under **UDP Port**, as specified by Wind Telecom.



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

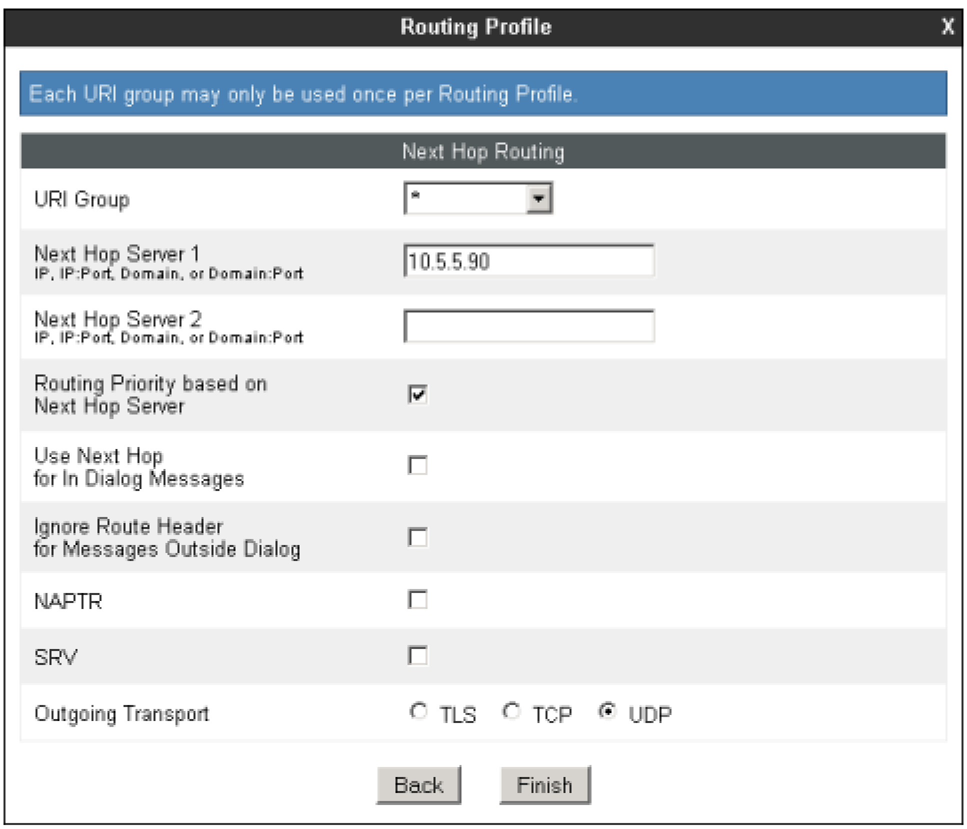


6.3.3. Routing Profiles

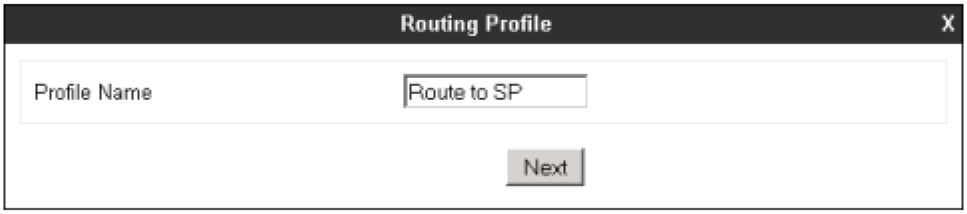
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces.

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

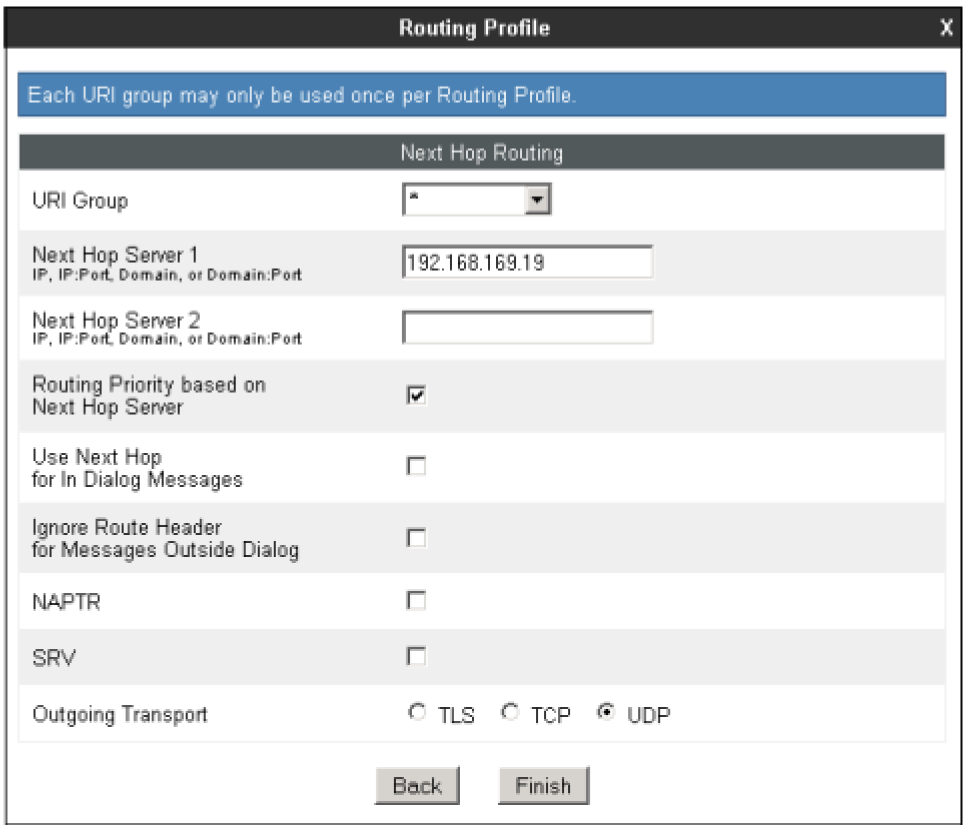
On the **Next Hop Routing** tab, enter the IP Address of the IP Office Primary Server LAN1 as **Next Hop Server 1**. Since the default well-known port value of 5060 for UDP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **UDP**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



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



On the Next Hop Routing tab, enter the IP Address of the service provider SIP proxy server as **Next Hop Server 1**. The port number would need to be also specified here if different than the default well-known value of 5060 for UDP. Check **Routing Priority based on Next Hop Server**. Choose **UDP** for **Outgoing Transport**. Click **Finish**.

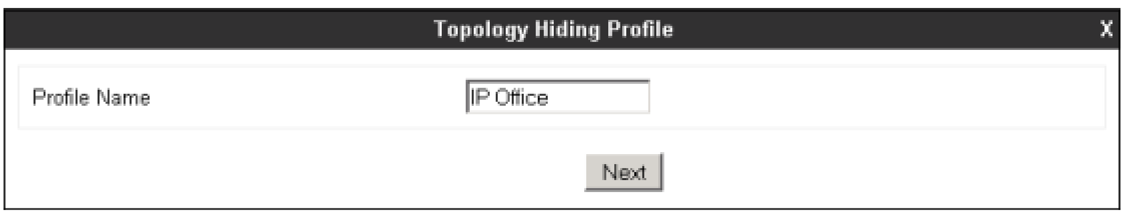


6.3.4. Topology Hiding

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

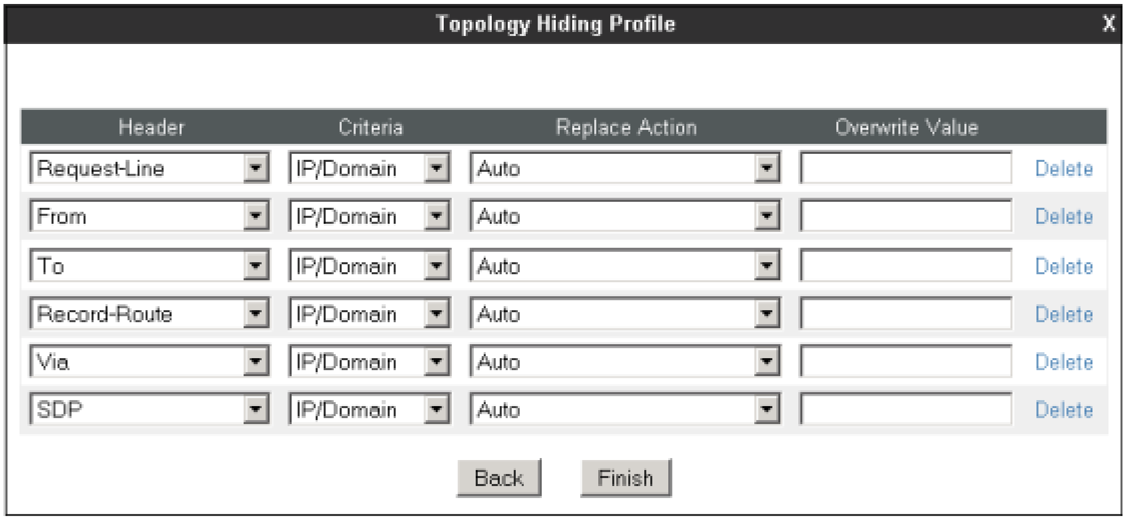
Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, only the minimum configuration required to achieve interoperability on the SIP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

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

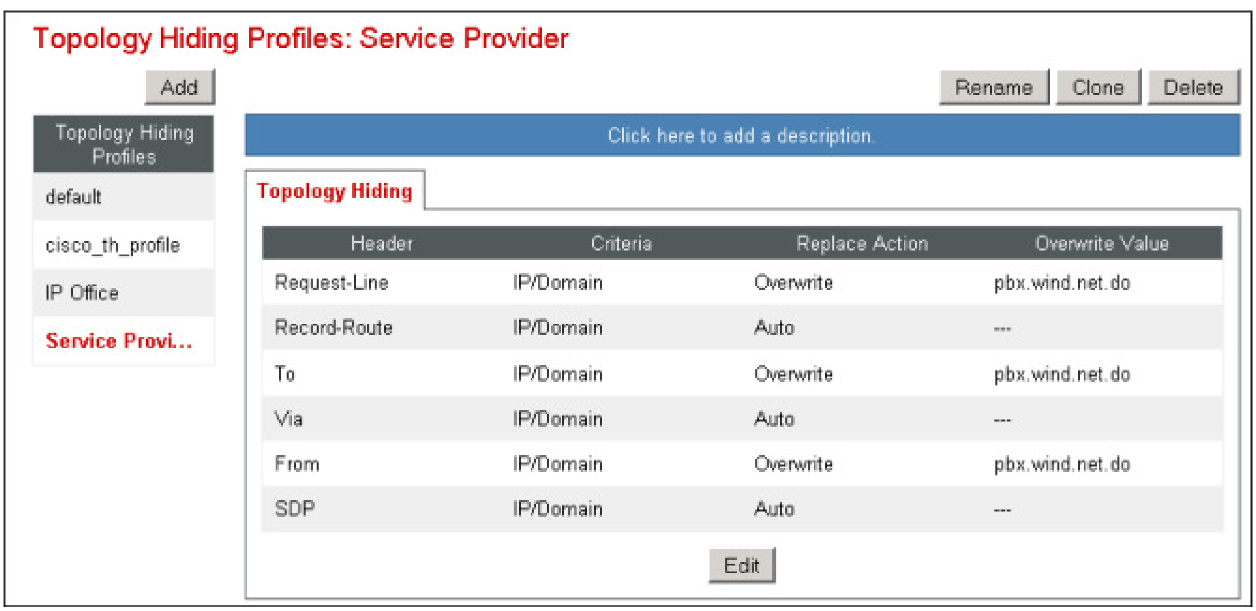


On the **Topology Hiding Profile** screen, click the **Add Header** button repeatedly to show the rest of the headers in the profile.

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



A Topology Hiding profile named ***Service Provider*** was similarly configured in the direction of the SIP trunk to Wind Telecom. In this case, for the **Request-Line**, **From** and **To** headers, ***Overwrite*** was selected in the **Replace Action** column and the SIP domain expected by the service provider, ***pbx.wind.net.do***, was entered in the **Overwrite Value** column of these headers, as shown below. Default values were used for all other fields.



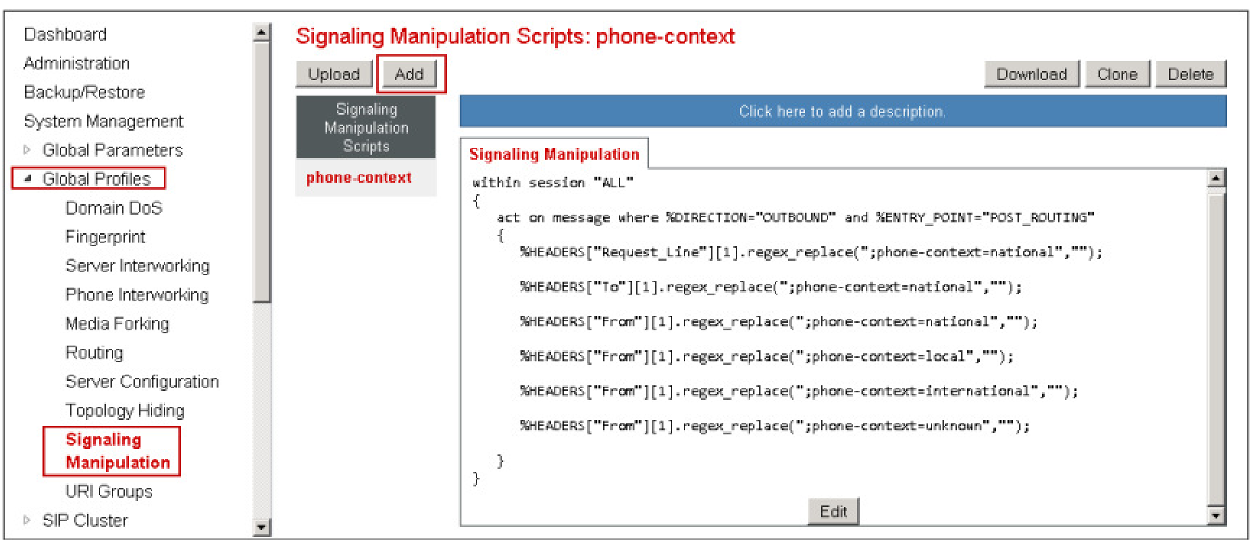
6.3.5. Signaling Manipulation

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

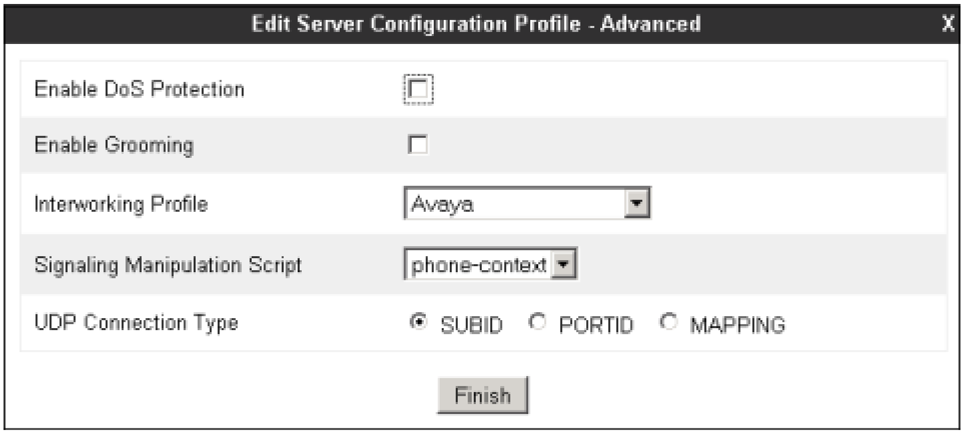
During the compliance test, it was observed that Wind Telecom inserted a “phone-context” parameter as part of the user part of the SIP URIs on incoming calls to the enterprise. This parameter was being displayed on the system telephones, appended to the caller ID of the originating party. Since the “phone-context” parameter has no local significance for the enterprise, a Sigma script was created to remove this character string present on the SIP headers of incoming calls. The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For the test configuration, the Editor was used to create the script needed to handle the header manipulation described above. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. See **[6]** on the **Additional References** section for more information on this topic.

From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click **Add** to open the SigMa Editor screen, where the text of the script can be entered.

The screen below shows the finished Signaling Manipulation script named **phone-context**. The details of the script can be found in **Appendix A**.



After the Signaling Manipulation Script is created, it should be applied to the **IP Office** Server Profile previously created in **Section 6.3.2.** To do this, navigate to **Global Profiles → Server Configuration → IP Office → Advanced** tab **→ Edit** (not shown). Select ***phone-context*** from the drop down menu on the **Signaling Manipulation Script** field as shown below. Click **Finish** to save and exit.



6.4. Domain Policies

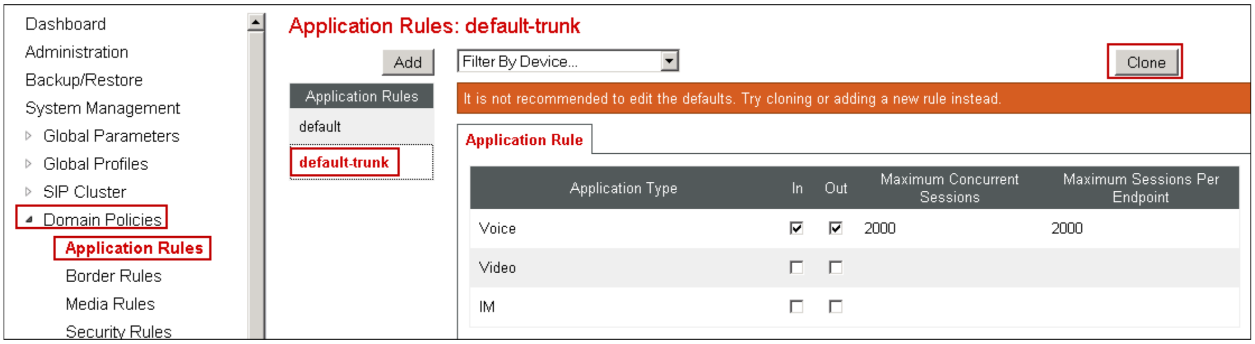
Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

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

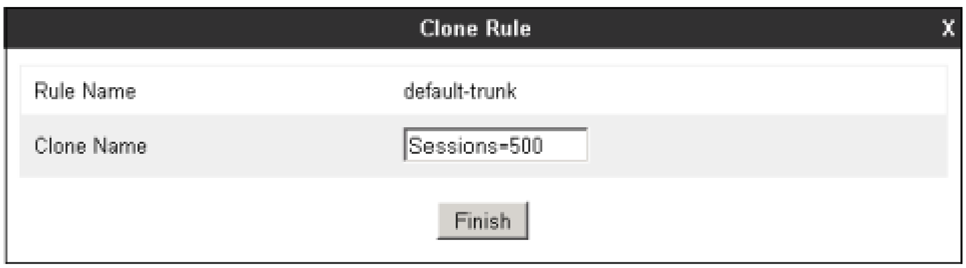
6.4.1. Application Rules

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

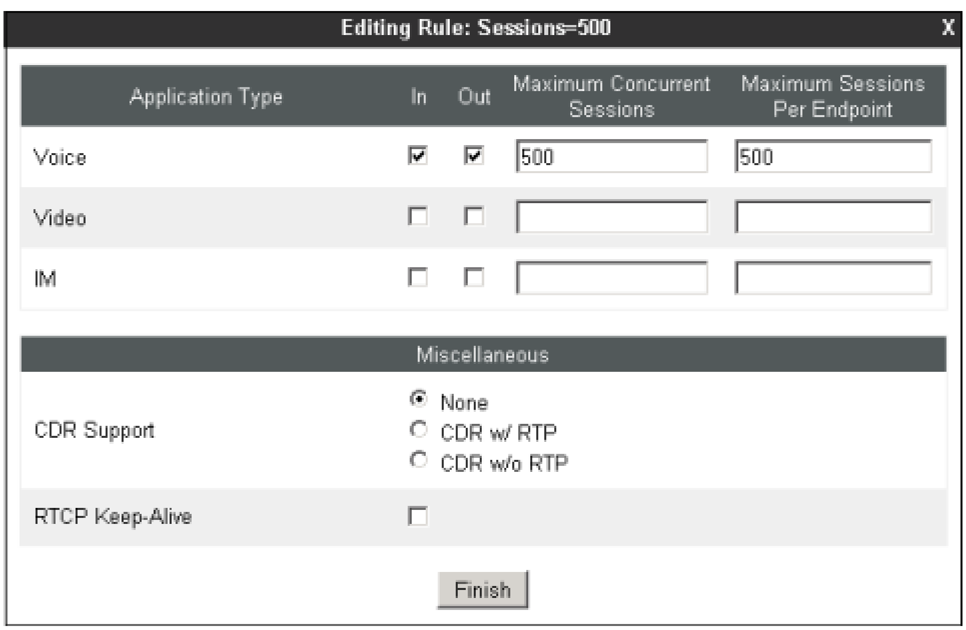
Select **Application Rules** under the **Domain Policies** menu on the left hand side, select the **default-trunk** Application Rule and click **Clone**.



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



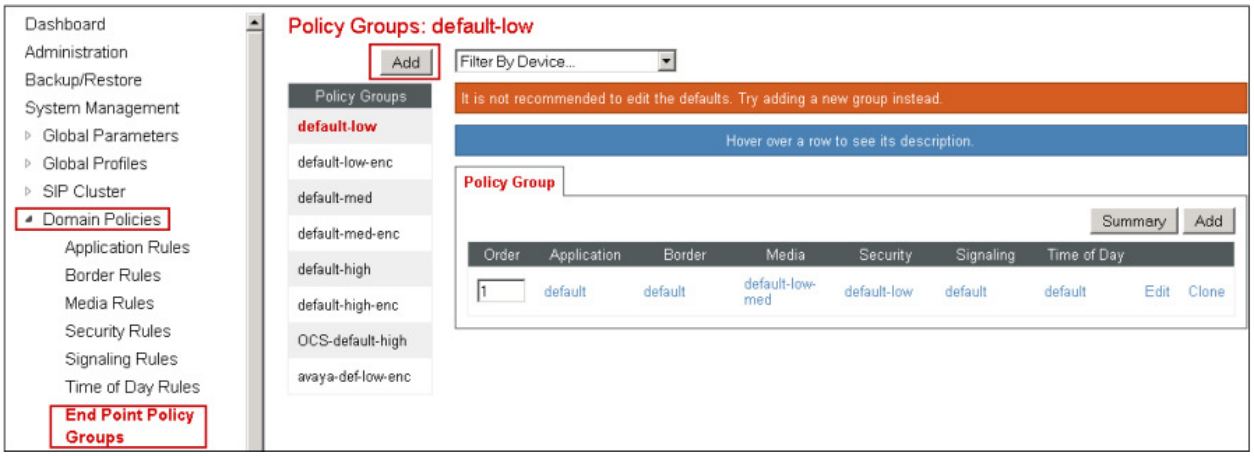
On the Application Rules screen, select the newly created rule and click **Edit** (not shown). For SIP trunking, **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** should have the same value. In the example below, they are set to ***500***, which is the number of maximum simultaneous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



6.4.2. End Point Policy Groups

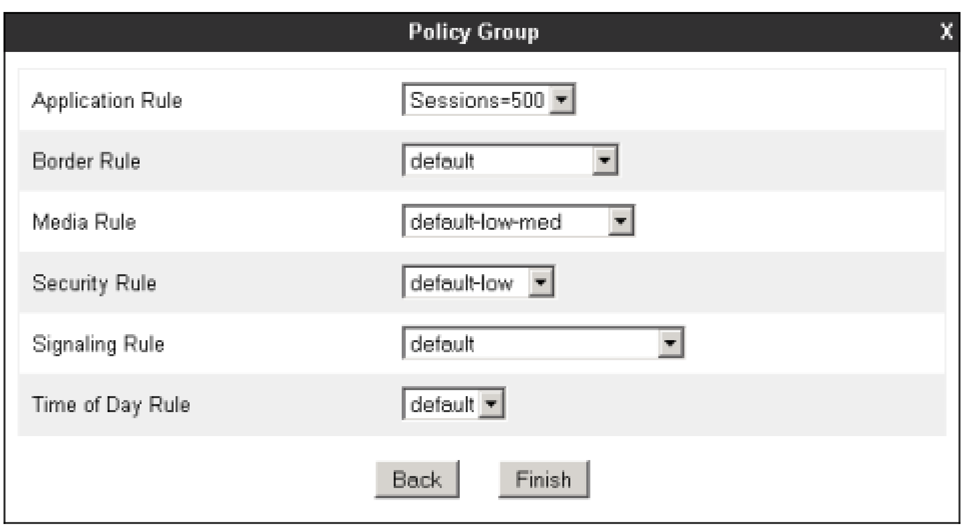
End Point Policy Groups associate the different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE.

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

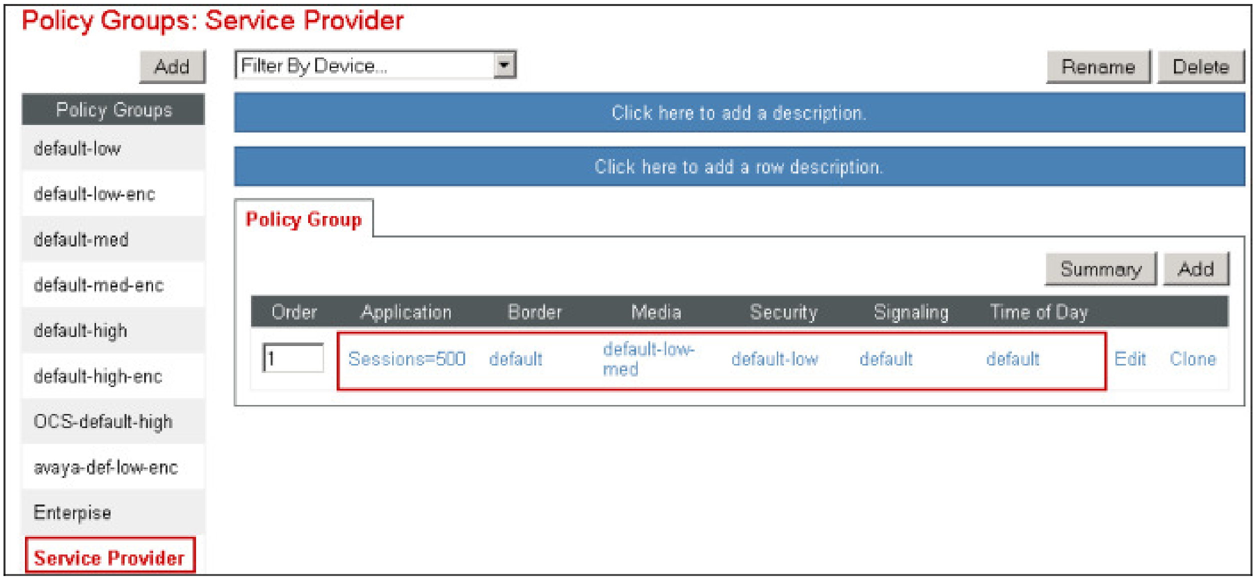


Enter an appropriate name in the **Group Name** field. Click **Next**.

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



A second End Point Policy Group was created for the service provider, repeating the steps described above. This is done with the purpose of allowing changes to be made to one of the groups in the future if needed, without affecting the settings in the other group. The screen below shows the ***Service Provider*** End Point Policy Group after the configuration was completed.



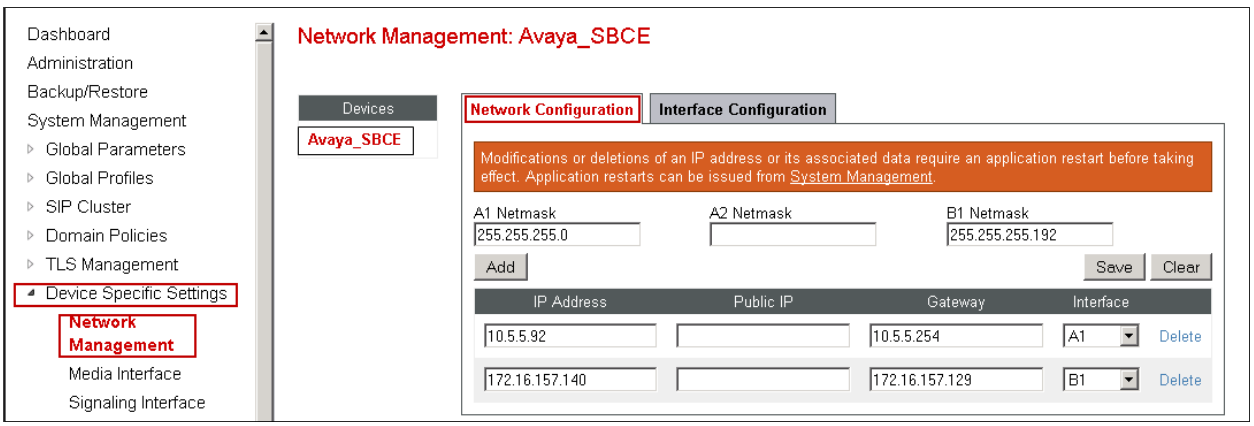
6.5. Device Specific Settings

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

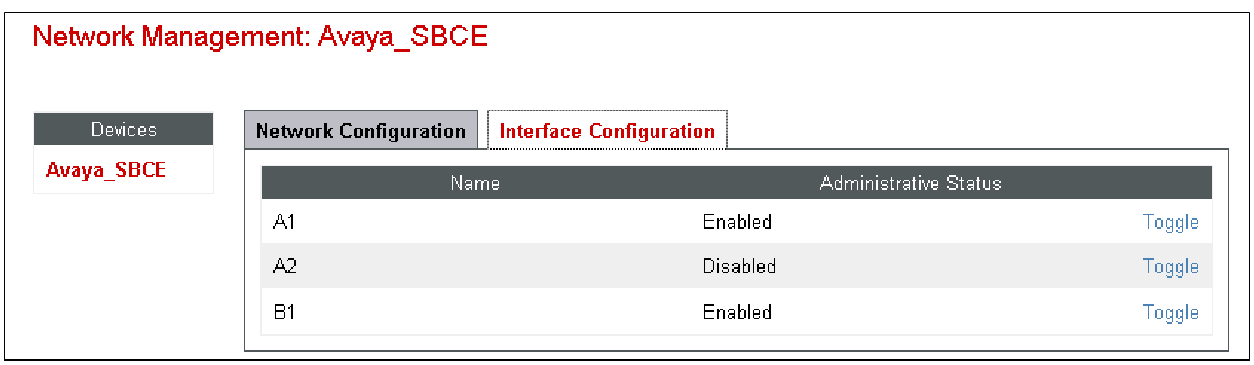
6.5.1. Network Management

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

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



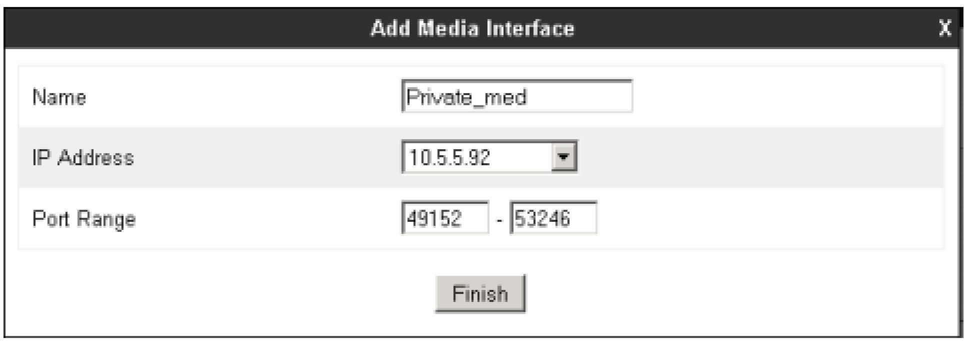
On the **Interface Configuration** tab, click the **Toggle State** control for interfaces **A1** and **B1** to change the status to **Enabled**. Since the default state for all interfaces is **Disabled**, it is important to perform this step, or the SBC will not be able to communicate on any of its interfaces.



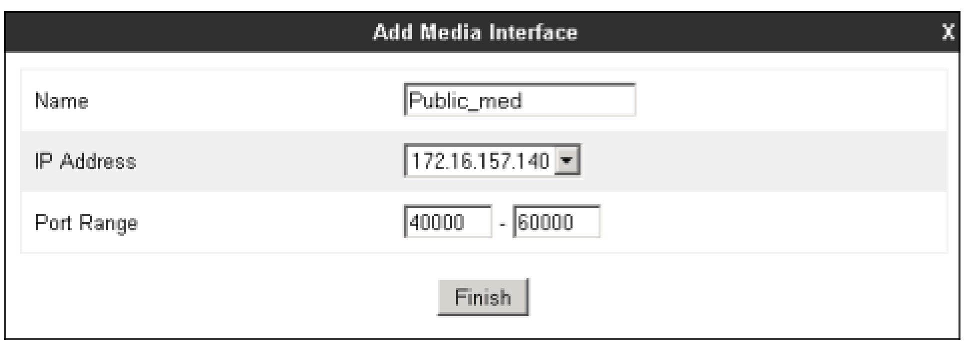
6.5.2. Media Interface

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

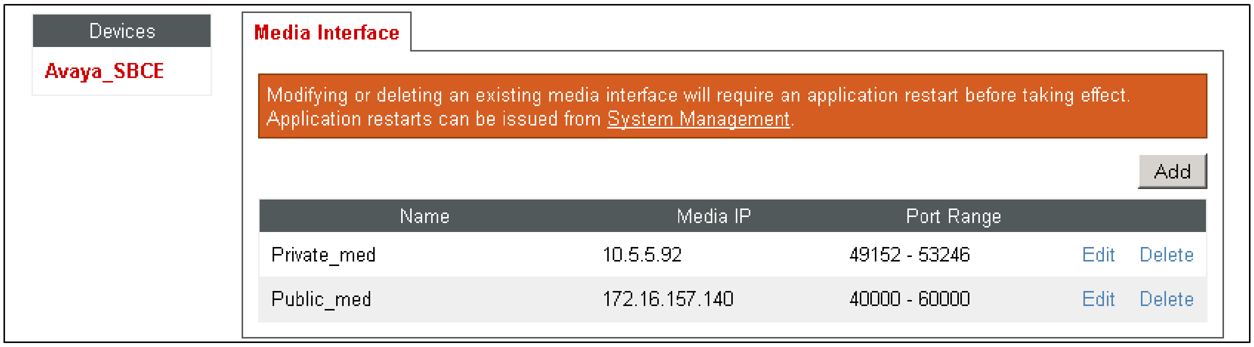
To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. The **Port Range** was set to match the default RTP port range of ***49152*** to ***53246*** specified in the IP Office Primary Server LAN1. Click **Finish**.



A second Media Interface facing the public network side was similarly created with the name ***Public_med***. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. The **Port Range** was set to the values of ***40000*** to ***60000*** specified by Wind Telecom, as shown below.



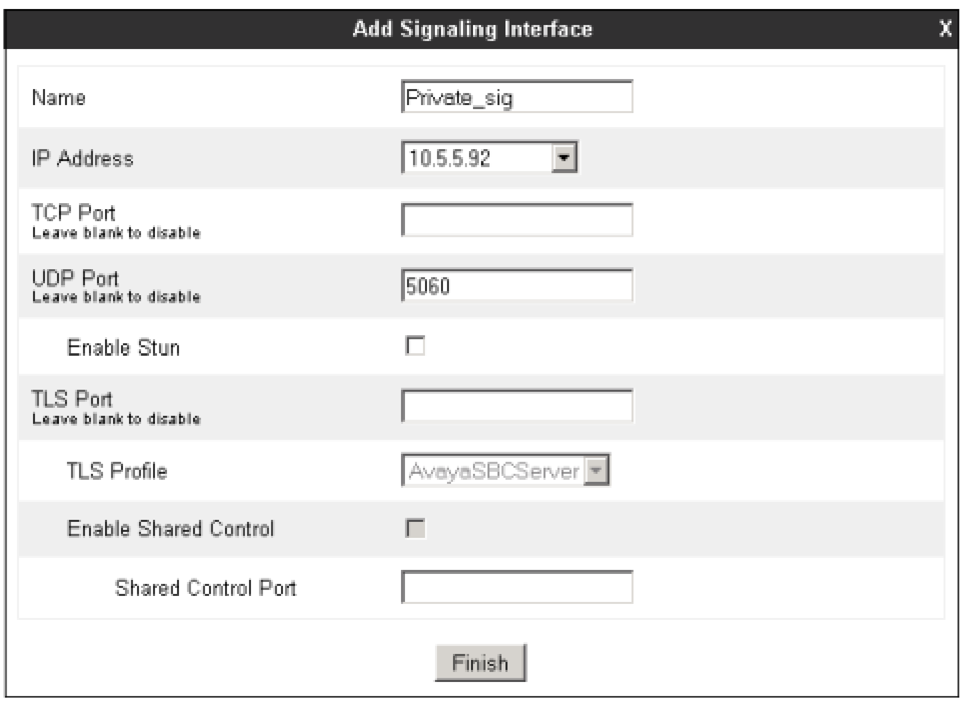
Once the configuration is complete, the **Media Interface** screen will appear as follows.



6.5.3. Signaling Interface

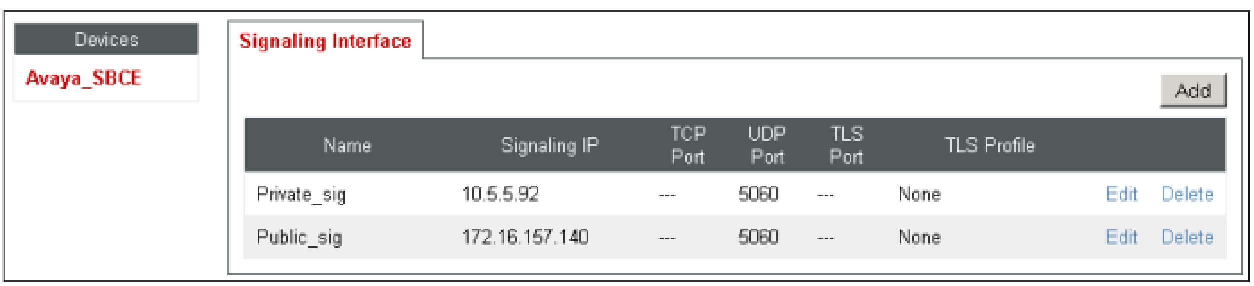
Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in both the inside and outside networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya_SBCE** device and click the **Add** button (not shown).On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. Enter ***5060*** for **UDP Port**, since UDP port 5060 is used between the IP Office Primary Server LAN1 and the Avaya SBCE in the sample configuration. Click **Finish**.



A second Signaling Interface with the name ***Public_sig*** was similarly created in the network direction. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. **UDP Port *5060*** was selected since this is the protocol and port used between the Avaya SBCE and the service provider.

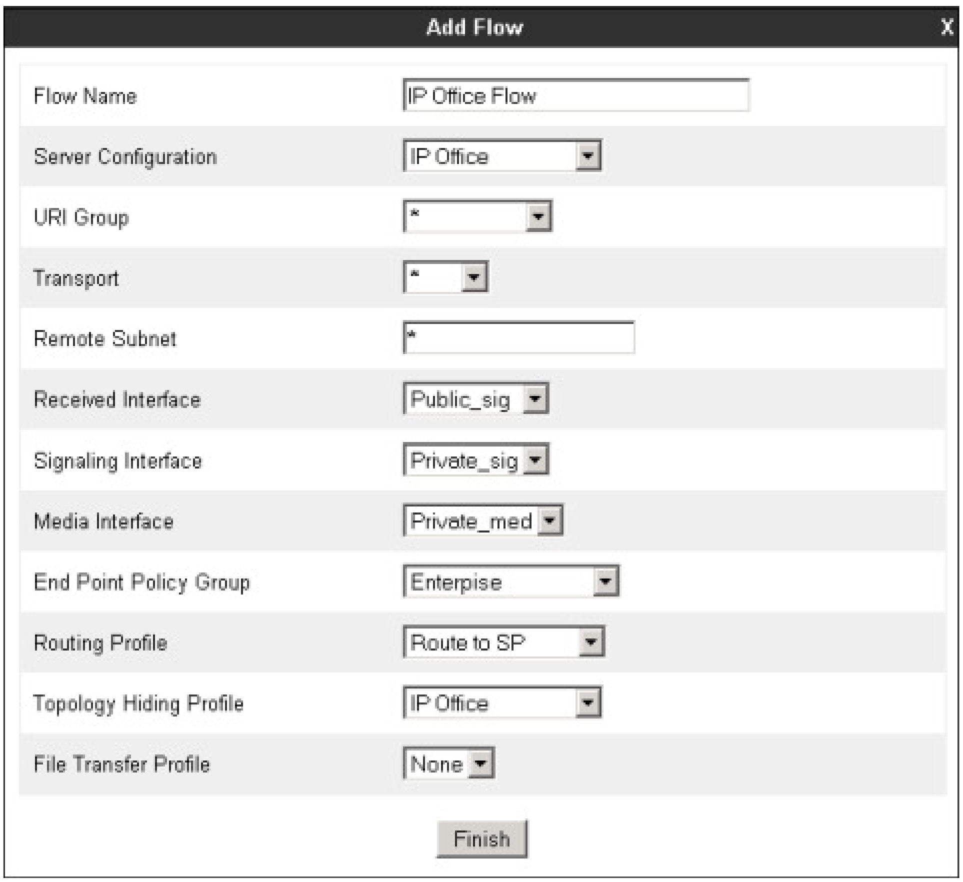
Once the configuration is complete, the **Signaling Interface** screen will appear as follows.



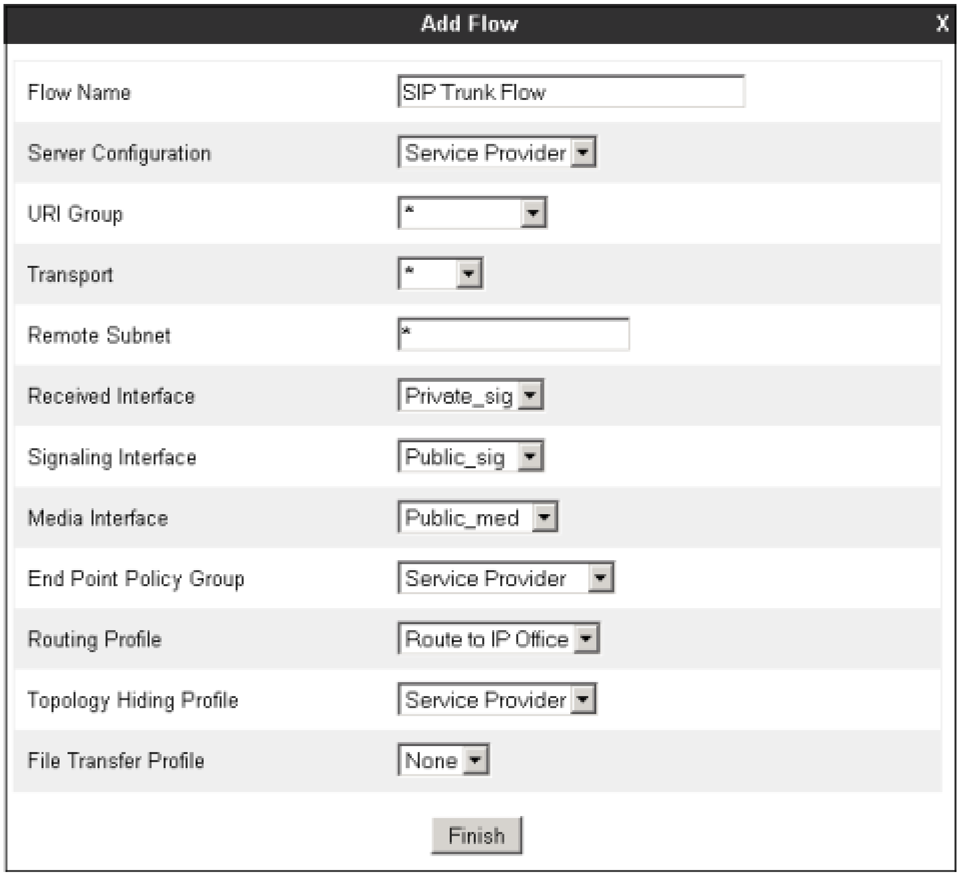
6.5.4. End Point Flows

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

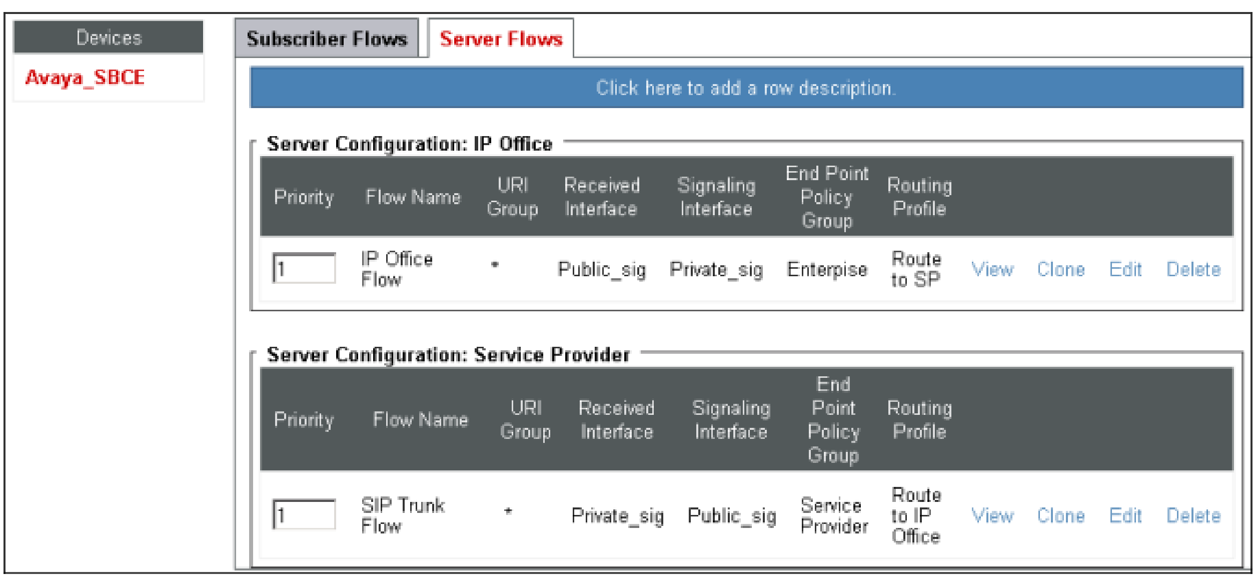
To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named ***IP Office Flow*** created in the sample configuration. The flow uses the interfaces,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



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



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



7. Wind Telecom SIP Trunking Configuration

Wind Telecom is responsible for the configuration of the Wind Telecom SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Wind Telecom will provide the customer the necessary information to configure the Avaya IP Office Server Edition solution and Avaya SBCE SIP trunk connection, including:

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

8. Verification Steps

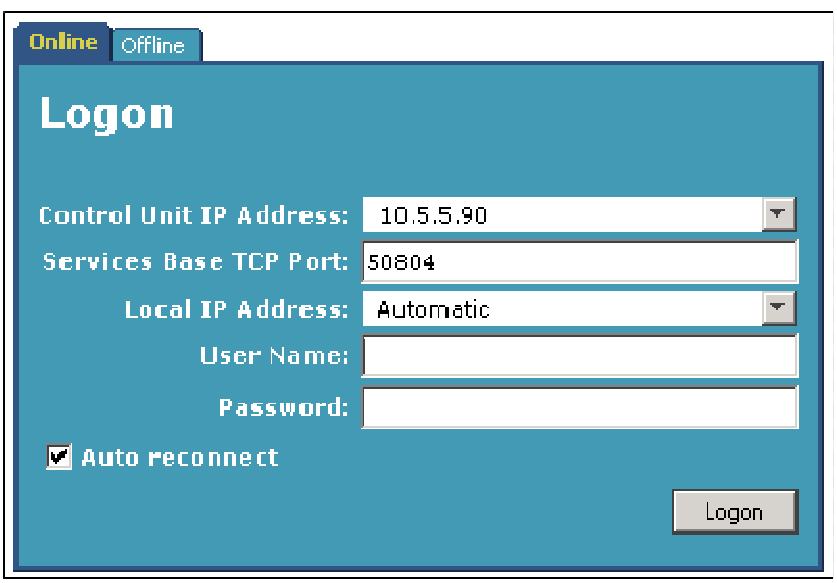
The following sections include steps that may be used to verify the configuration of the Avaya IP Office Server Edition solution and the Avaya SBCE with the Wind Telecom SIP Trunk Service.

8.1. Avaya IP Office Server Edition Solution

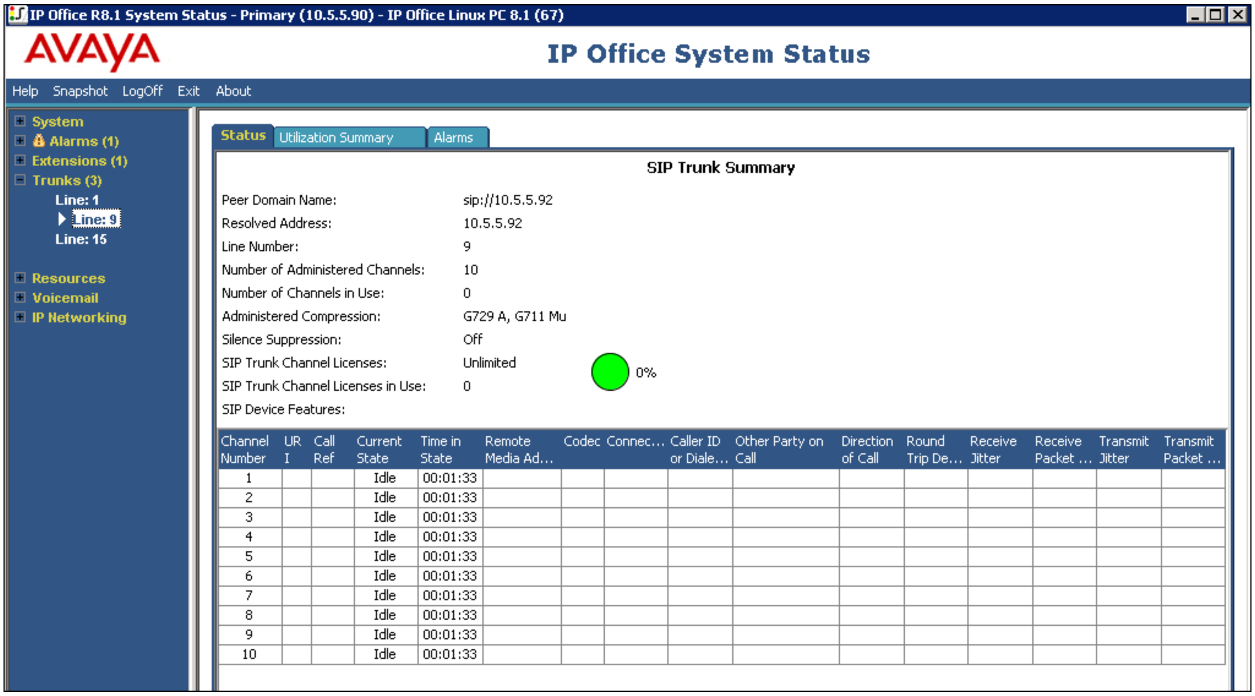
The Avaya IP Office System Status and Monitor applications are useful tools used for the verification and troubleshooting of the SIP connection to the service provider via the Avaya SBCE.

8.1.1. System Status

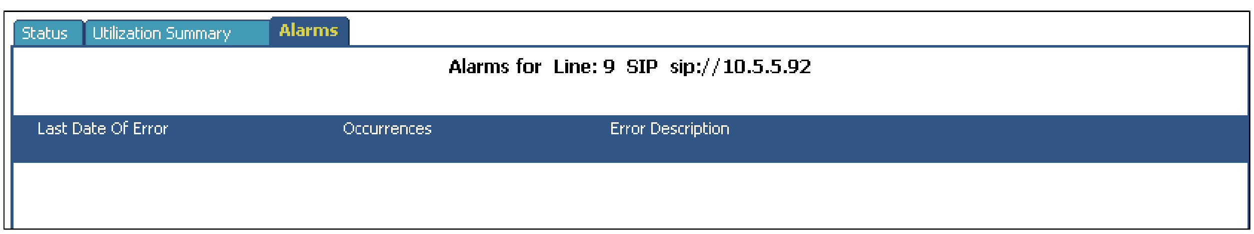
The Avaya IP Office System Status application can be used to verify the service state of the SIP line. Launch the application from **Start → Programs → IP Office → System Status** on the PC where Avaya IP Office Server Edition Manager was installed. Under **Control Unit IP Address** select the IP address of the system hosting the SIP trunk to the Avaya SBCE (Primary Server in the reference configuration). Log in using the appropriate credentials



Select the SIP line of interest from the left pane (**Line 9** in the reference configuration). On the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).

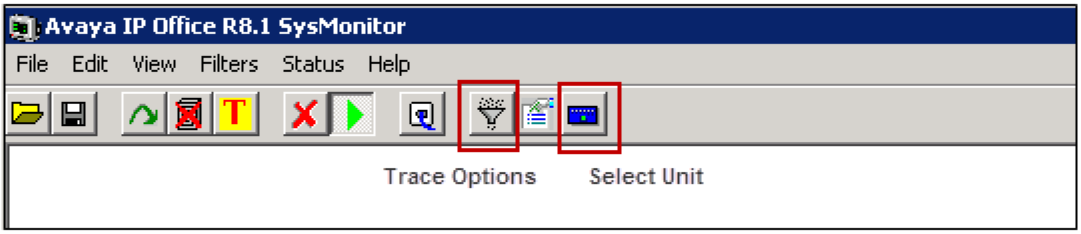


Select the **Alarms** tab and verify that no alarms are active on the SIP line.

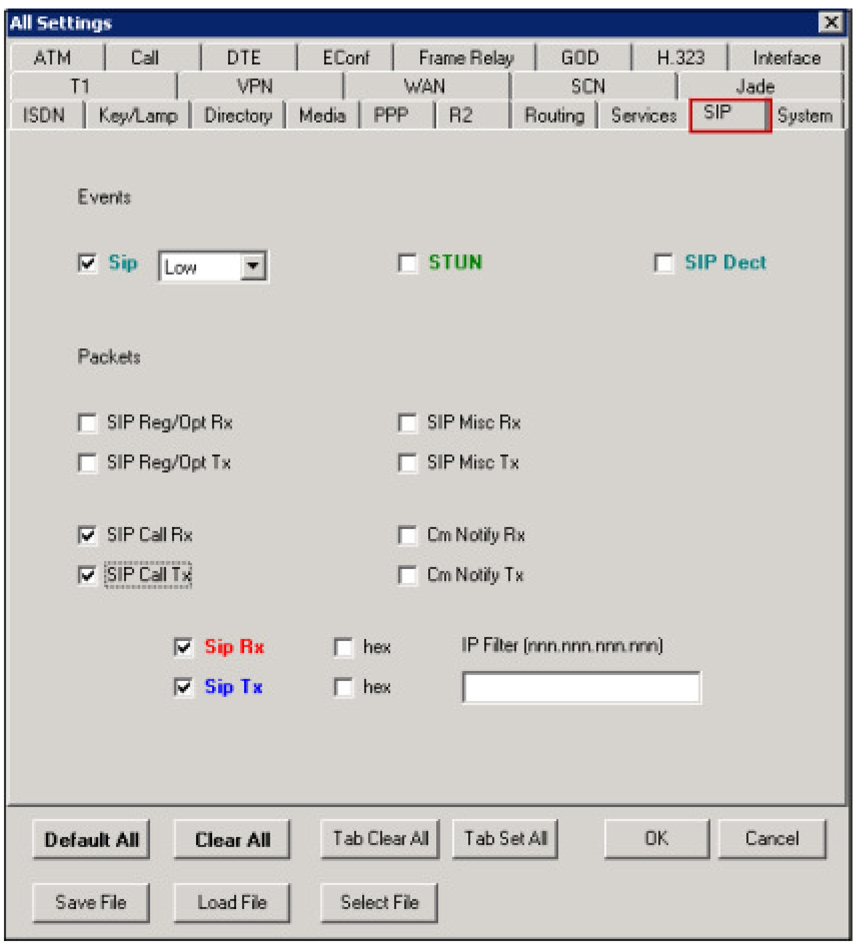


8.1.2. Monitor

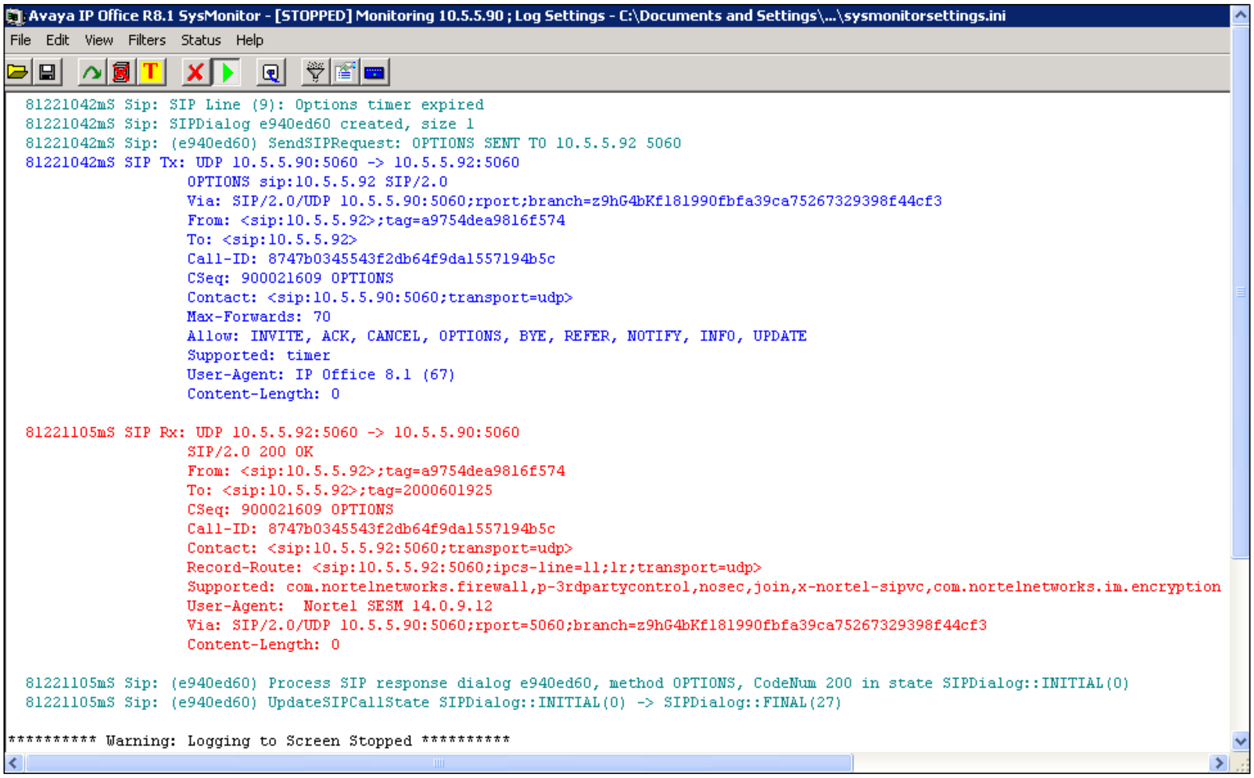
The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP trunk. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where Avaya IP Office Server Edition Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the LAN1 interface of the Primary Server.



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



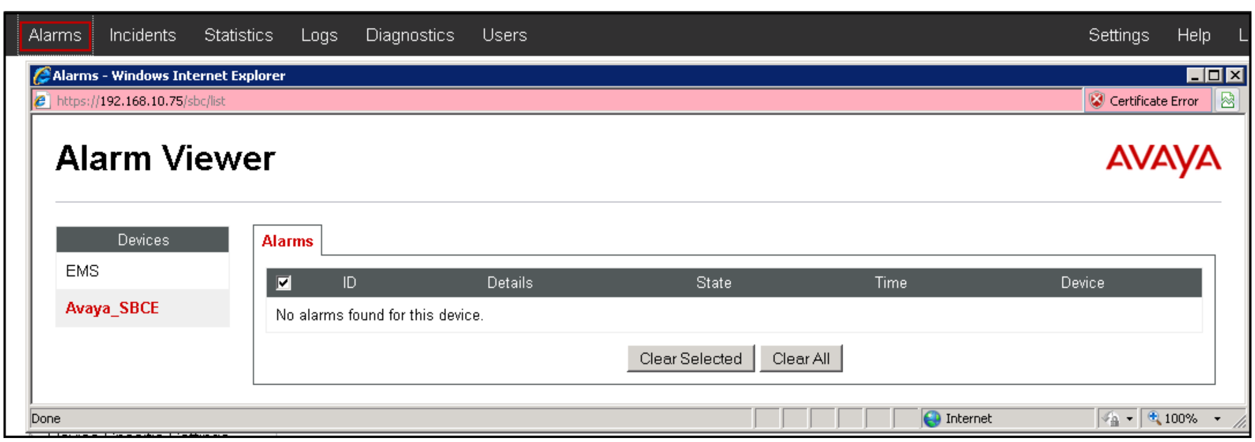
The sample screen below shows an outbound OPTIONS message and the 200 OK response from the service provider, received via the Avaya SBCE.



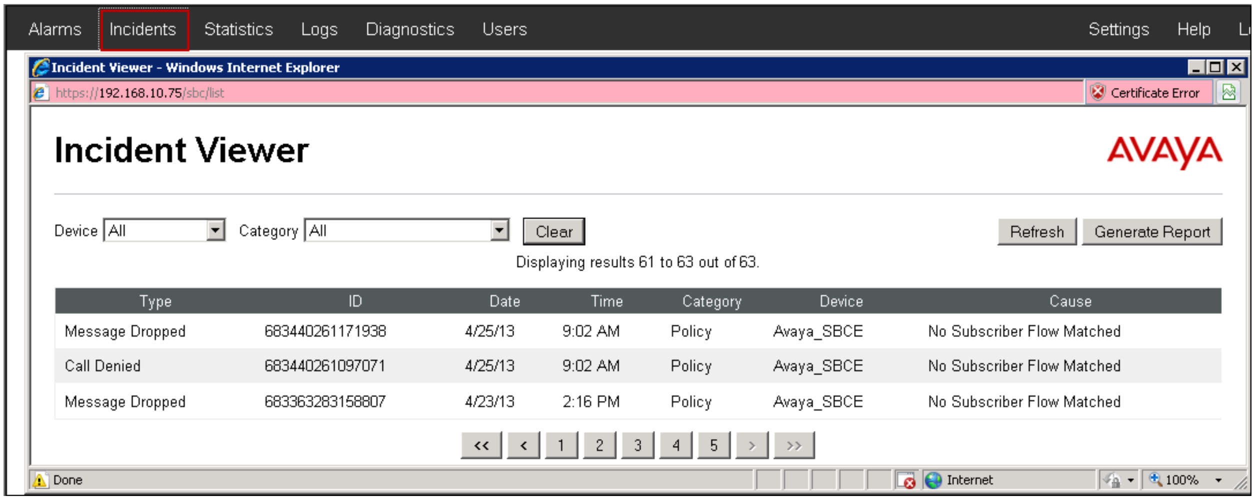
8.2. Avaya Session Border Controller for Enterprise

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

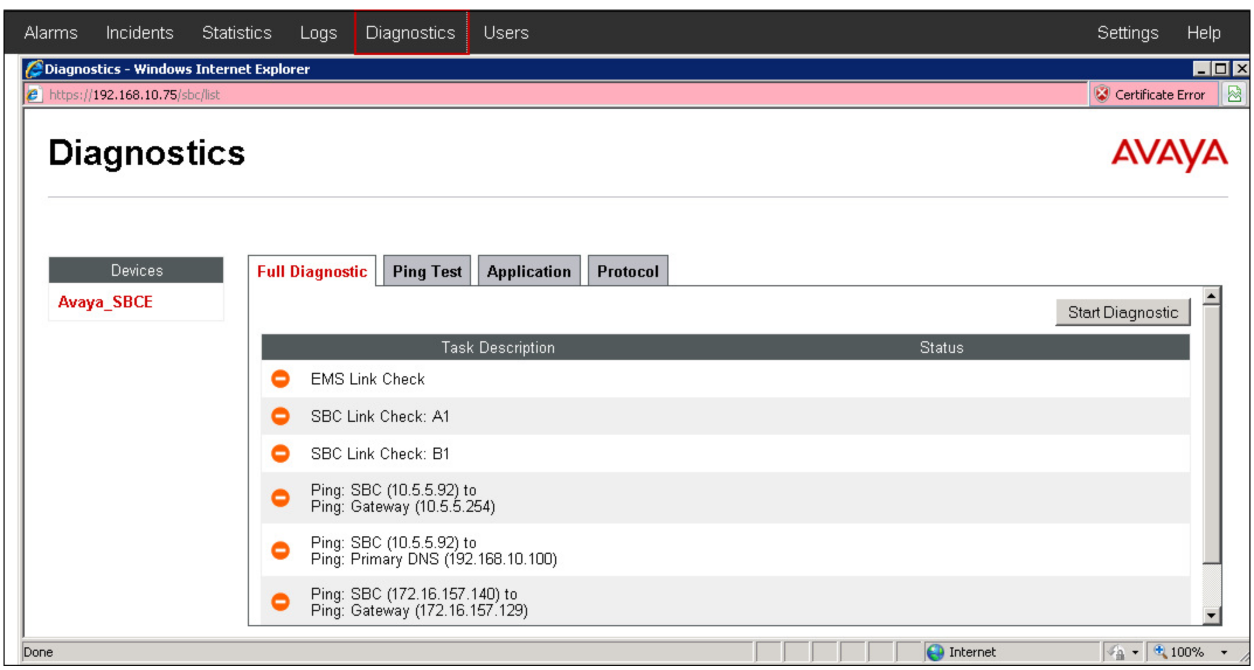
Alarms: Provides information about the health of the SBC.



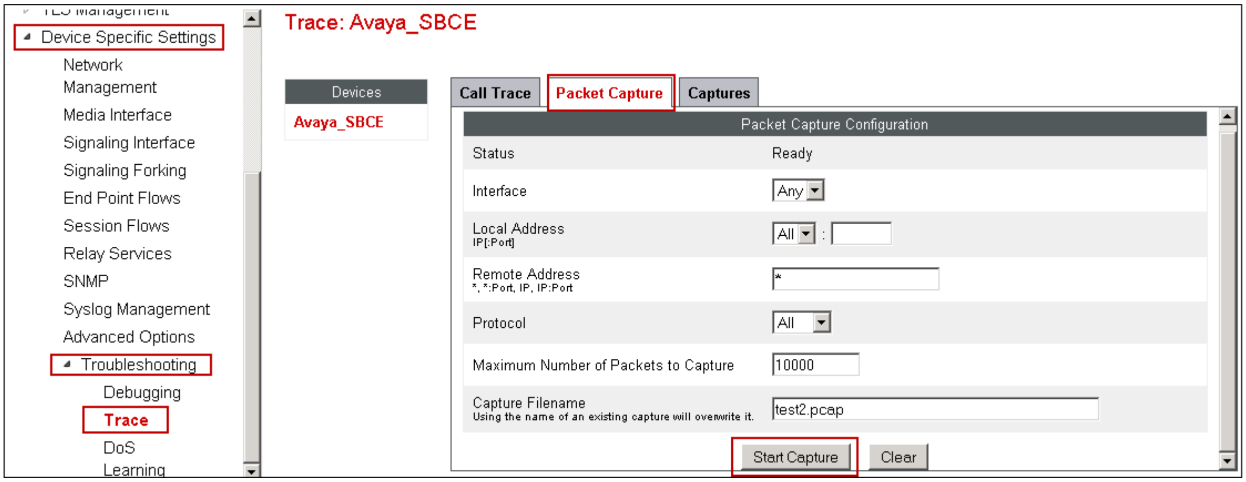
Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.



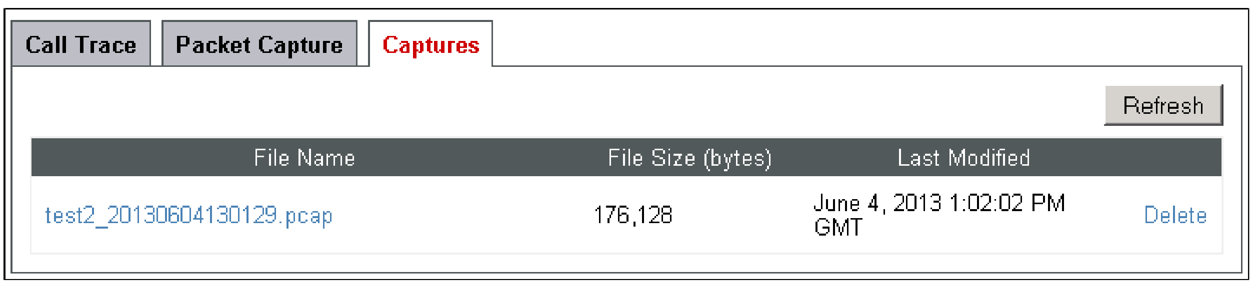
Diagnostics: This screen provides a variety of tools to test and troubleshoot the SBC network connectivity.



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



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



9. Conclusion

These Application Notes describe the procedures required to configure an Avaya IP Office 8.1 Server Edition solution and Avaya Session Border Controller for Enterprise 6.2, to connect to the service provider Wind Telecom using Session Initiation Protocol (SIP) Trunking, as shown in **Figure 1**.

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

10. Additional References

[1] *Deploying IP Office Server Edition Solution IP Office 8.1*, Document 15-604134, December 2012

[2] *IP Office Server Edition Reference Configuration IP Office 8.1*, Document 15-604135, December 2012

[3] *IP Office R8.1 FP1, Manager 10.1*, Document Number 15-601011, April 2013

[4] *Avaya IP Office Knowledgebase,* http://marketingtools.avaya.com/knowledgebase

[5] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, March 2013

[6] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, March 2013

Product documentation for Avaya products may be found at http://support.avaya.com.
Product documentation for the Wind Telecom SIP Trunk Service is available from Wind Telecom.

Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE, **Section 6.3.5**:

```
// Script to remove the phone-context parameter

within session "ALL"

{

   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"

   {

     %HEADERS["Request_Line"][1].regex_replace(";phone-context=national","");

     %HEADERS["To"][1].regex_replace(";phone-context=national","");

     %HEADERS["From"][1].regex_replace(";phone-context=national","");

     %HEADERS["From"][1].regex_replace(";phone-context=local","");

     %HEADERS["From"][1].regex_replace(";phone-context=international","");

     %HEADERS["From"][1].regex_replace(";phone-context=unknown","");

    }

}
```

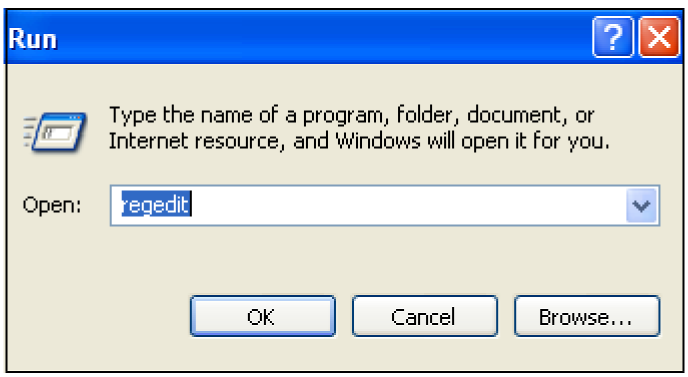
Appendix B: SIP Line Template

Avaya IP Office Server Edition Release 8.1 supports a SIP Line Template (in xml format) that can be created from an existing configuration and imported into a new installation to simplify configuration procedures as well as to reduce potential configuration errors.

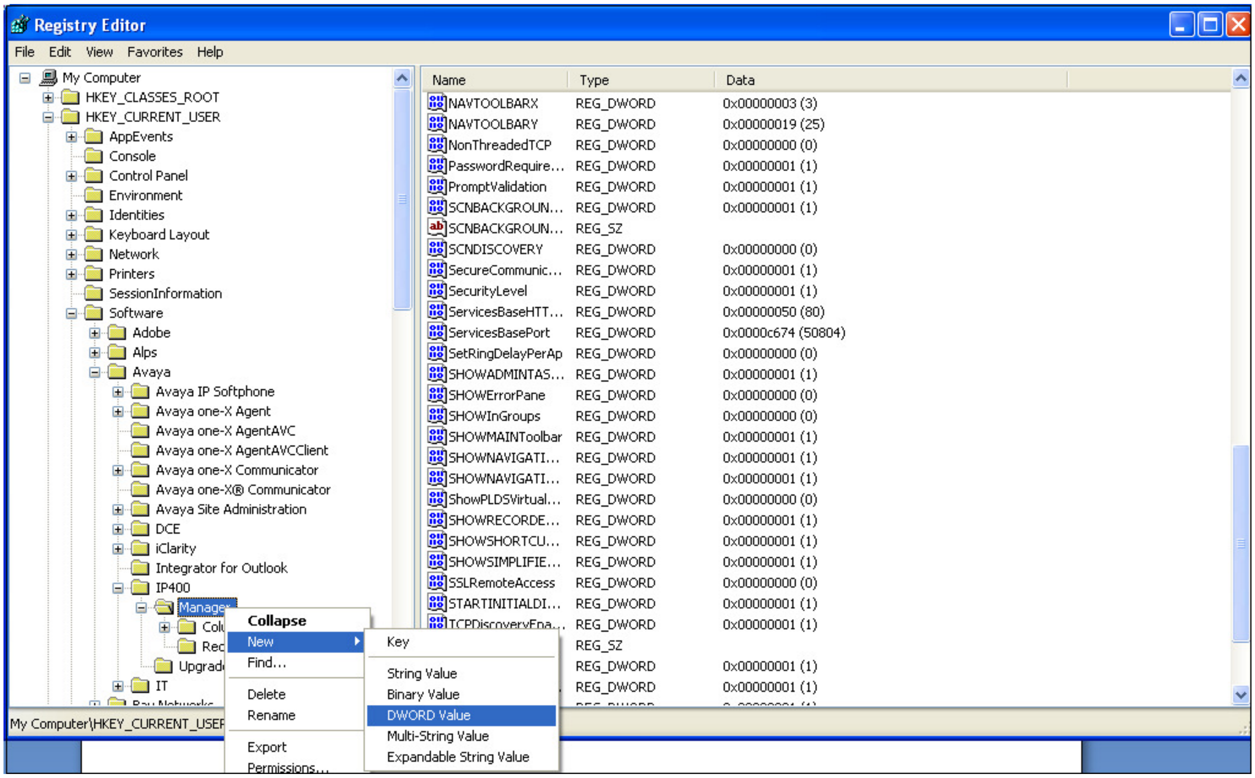
Not all of the configuration information is included in the SIP Line Template, therefore, it is critical that the SIP Line configuration be verified/updated after a template has been imported, and additional configuration be supplemented using **Section 5.6** in these Application Notes as a reference.

To create a SIP Line Template from the configuration described in these Application Notes, configure the parameters as described below.

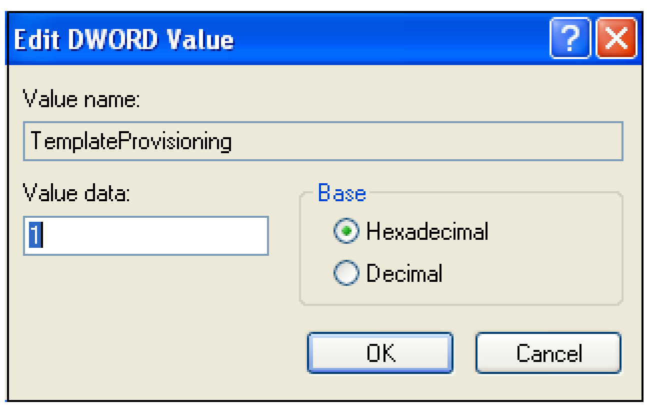
Use the Windows Registry Editor on the PC where Avaya IP Office Server Edition Manager is installed to add a new ***TemplateProvisioning*** registry entry. This procedure is only required the first time the PC is used to create the template. Select **Start → Run**. Enter ***regedit*** in the **Open** box.



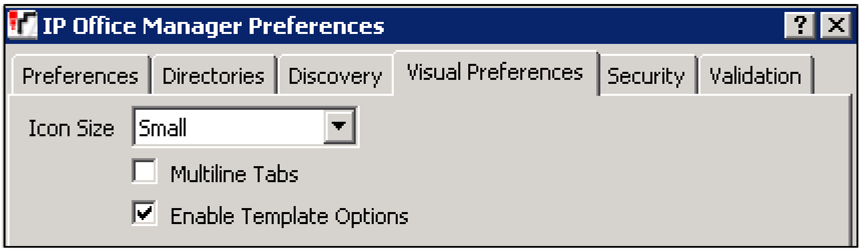
On the Registry Editor, navigate to **HKEY_CURRENT_USER → Software → Avaya →IP400**. Right click on **Manager** and select **New → DWORD Value**.



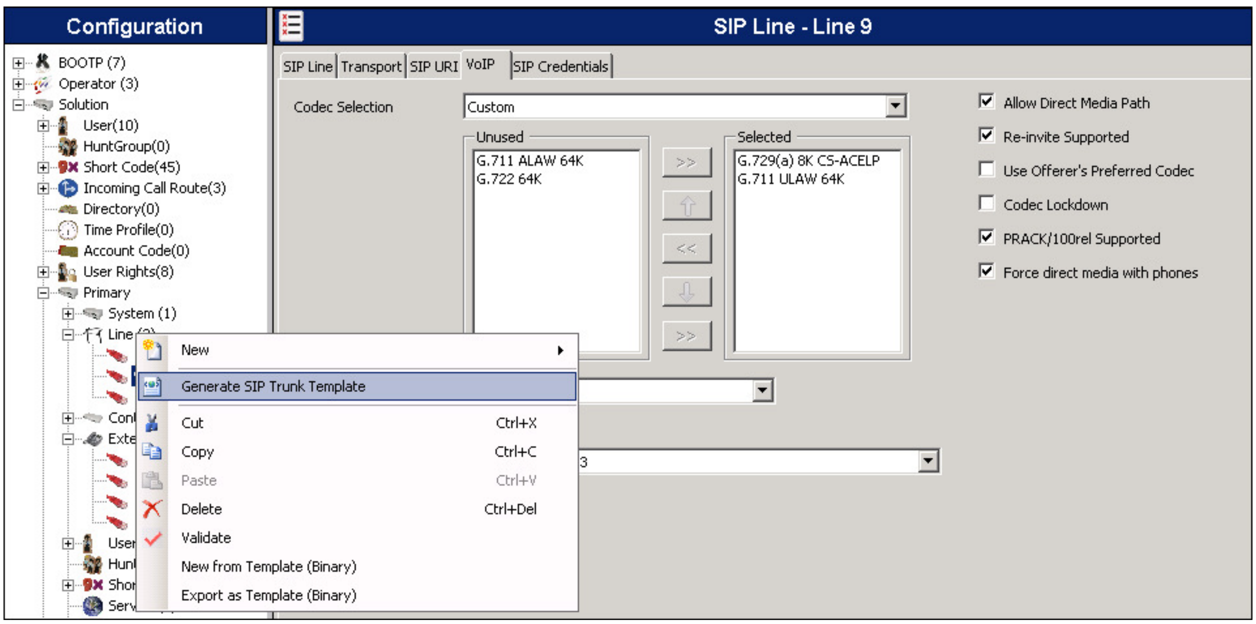
Right click the newly created entry and rename it to ***TemplateProvisioning***. Double click the entry and change the value under **Value Data** from "***0***" to "***1***". Restart the PC.



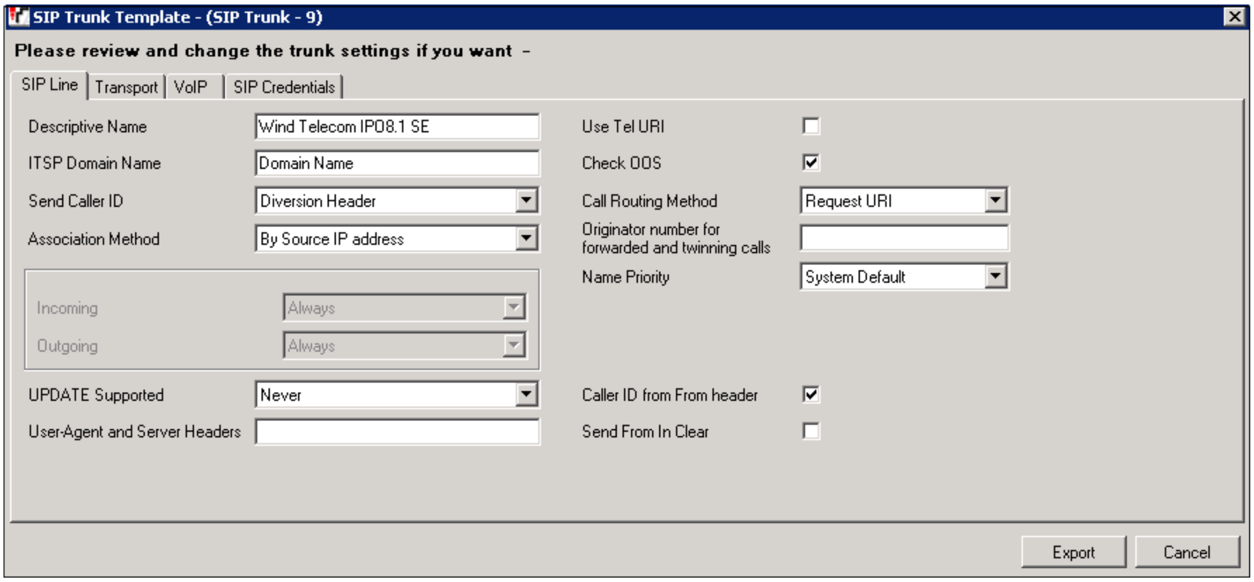
To enable template support in the IP Office Server Edition Manager, select **File**, then **Preferences**. On the **Visual Preferences** tab, check the **Enable Template Options** box.



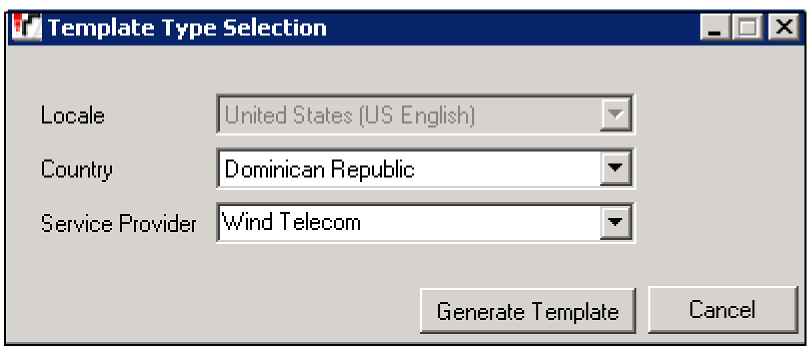
To create a SIP Line Template from the configuration, on the left Navigation pane, right click the Sip Line (**9**), and select **Generate SIP Trunk Template**.



The trunk's settings are displayed as configured in **Section 5.6.** Enter a descriptive name for the template and adjust the settings if required. Even though the **ITSP Domain Name** was left blank in the configuration, a phantom value (***Domain Name*** in the example below) needs to be entered in this field in order to be accepted by the template. Note that this value will need to be removed from the configuration of the target system where the template is to be imported. Click **Export**.



On the next screen, **Template Type Selection**, select the **Country,** enter the name for the **Service Provider**, and click **Generate Template**.



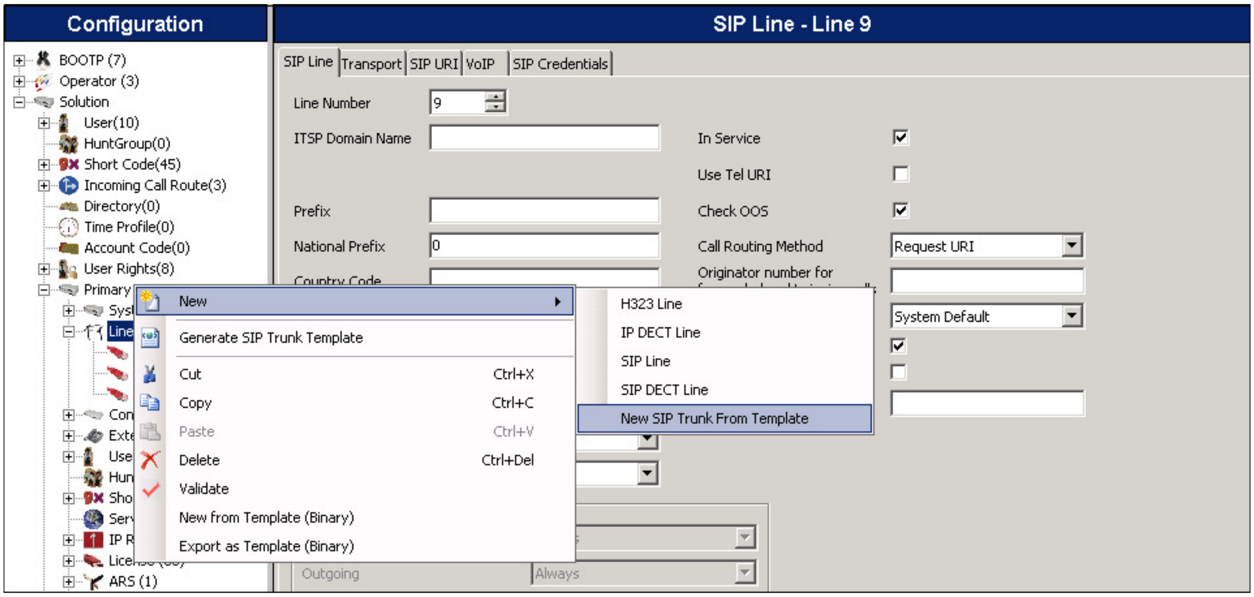
The following is the exported SIP Line Template file **DO_Wind Telecom_SIPTrunk.xml**:


```
<?xml version="1.0" encoding="utf-8" ?>
- <Template xmlns="urn:SIPTrunk-schema">
  <TemplateType>SIPTrunk</TemplateType>
  <Version>20130605</Version>
  <SystemLocale>enu</SystemLocale>
  <DescriptiveName>Wind Telecom IPO8.1 SE</DescriptiveName>
  <ITSPDomainName>Domain Name</ITSPDomainName>
  <SendCallerID>CallerIDDIV</SendCallerID>
  <ReferSupport>false</ReferSupport>
  <ReferSupportIncoming>1</ReferSupportIncoming>
```

<ReferSupportOutgoing>**1**</ReferSupportOutgoing>
<RegistrationRequired>**false**</RegistrationRequired>
<UseTelURI>**false**</UseTelURI>
<CheckOOS>**true**</CheckOOS>
<CallRoutingMethod>**1**</CallRoutingMethod>
<OriginatorNumber />
<AssociationMethod>**SourceIP**</AssociationMethod>
<LineNamePriority>**SystemDefault**</LineNamePriority>
<UpdateSupport>**UpdateNever**</UpdateSupport>
<UserAgentServerHeader />
<CallerIDfromFromheader>**true**</CallerIDfromFromheader>
<PerformUserLevelPrivacy>**false**</PerformUserLevelPrivacy>
<ITSPProxy>**10.5.5.92**</ITSPProxy>
<LayerFourProtocol>**SipUDP**</LayerFourProtocol>
<SendPort>**5060**</SendPort>
<ListenPort>**5060**</ListenPort>
<DNSServerOne>**0.0.0.0**</DNSServerOne>
<DNSServerTwo>**0.0.0.0**</DNSServerTwo>
<CallsRouteViaRegistrar>**true**</CallsRouteViaRegistrar>
<SeparateRegistrar />
<CompressionMode>**AUTOSELECT**</CompressionMode>
<UseAdvVoiceCodecPrefs>**true**</UseAdvVoiceCodecPrefs>
<AdvCodecPref>**G.729(a) 8K CS-ACELP,G.711 ULAW 64K**</AdvCodecPref>
<CallInitiationTimeout>**4**</CallInitiationTimeout>
<DTMFSupport>**DTMF_SUPPORT_RFC2833**</DTMFSupport>
<VoipSilenceSupression>**false**</VoipSilenceSupression>
<ReinviteSupported>**true**</ReinviteSupported>
<FaxTransportSupport>**FOIP_NONE**</FaxTransportSupport>
<UseOffererPrefferedCodec>**false**</UseOffererPrefferedCodec>
<CodecLockdown>**false**</CodecLockdown>
<Rel100Supported>**true**</Rel100Supported>
<T38FaxVersion>**3**</T38FaxVersion>
<Transport>**UDPTL**</Transport>
<LowSpeed>**0**</LowSpeed>
<HighSpeed>**0**</HighSpeed>
<TCFMethod>**Trans_TCF**</TCFMethod>
<MaxBitRate>**FaxRate_14400**</MaxBitRate>
<EflagStartTimer>**2600**</EflagStartTimer>
<EflagStopTimer>**2300**</EflagStopTimer>
<UseDefaultValues>**true**</UseDefaultValues>
<ScanLineFixup>**true**</ScanLineFixup>
<TFOPEnhancement>**true**</TFOPEnhancement>
<DisableT30ECM>**false**</DisableT30ECM>
<DisableEflagsForFirstDIS>**false**</DisableEflagsForFirstDIS>
<DisableT30MRCompression>**false**</DisableT30MRCompression>
<NSFOverride>**false**</NSFOverride>
</Template>

To import the template into a new IP Office system, copy the exported xml template file into the Templates directory (C:\Program Files\Avaya\IP Office\Manager\Templates) on the PC where IP Office Server Edition Manager for the new system is running.

Next, import the template into the new system by creating a new SIP Line as shown in the screenshot below. In the Navigation Pane on the left, right-click on **Line** then navigate to **New, New SIP Trunk From Template**.



On the next screen, **Template Type Selection**, verify that the information in the **Country** and **Service Provider** fields is correct. If more than one template is present, use the drop-down menus to select the required template. Click **Create new SIP Trunk** to finish the process.