Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

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

©2014 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the Alestra Enlace IP SIP Trunk service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya IP Office release 9.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) release 6.2 and various Avaya endpoints.

The Alestra Enlace IP SIP Trunk service referenced within these Application Notes is designed for enterprise business customers in Mexico. Customers using this service with the Avaya SIP-enabled enterprise 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.

2. General Test Approach and Test Results

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

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

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

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

©2014 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

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

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

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test
- Network Call Redirection using the REFER method is not supported by Alestra and it was not tested.
- Operator services such as dialing 0 or 0 + 10 digits are not supported.

©2014 Avaya Inc. All Rights Reserved.

2.2. Test Results

Interoperability testing of the Alestra Enlace IP SIP trunk service was completed with successful results for all test cases with the exception of the observations and limitations described below:

- **Calls to Busy Numbers:** Alestra did not send "486 Busy Here" for calls made from an enterprise extension to busy PSTN numbers. Since busy tone was heard by the caller, this observation had no direct impact to the user.
- **Caller ID on incoming calls from the U.S**.: Calls originating from PSTN telephones in the U.S. to DIDs numbers in Mexico assigned to the IP Office SIP trunk displayed "Restricted/Unavailable" on the enterprise extensions. This seems to be a PSTN restriction for all international inbound calls to Mexico from the U.S., not limited just to Alestra. This behavior is not necessarily indicative of a limitation of the combined Alestra/Avaya solution, and it is listed here simply as an observation.
- **"To" header on incoming calls**: Alestra sent in the Request-URI of incoming calls to the IP Office the last 4 digits of the DID number assigned, but in the To header it sent the complete 10 digit DID number, preceded by a constant 8 digit prefix. This issue was referred to Alestra for investigation. Since the Call Routing Method in the IP Office SIP Line was set to "Request URI", this issue had no noticeable effect to the user.
- **T.38 Fax**: When using T.38 for Fax Transport Support on the IP Office SIP line, Alestra responded with "488 Not Acceptable Here" to the re-invite sent from the IP Office to switch from voice to T.38, and the fax call dropped. This issue was sent to Alestra for investigation.
  Inbound and outbound fax calls using G.711 pass-through were successfully tested
- **Direct Media:** Direct media had to be disabled in the IP Office**,** by unchecking **Allow Direct Media Path** in the SIP Line/VoIP tab, to avoid a noticeable clipping that was observed on outbound calls at the beginning of the audio stream. This issue is currently under investigation by the IP Office team (JIRA IPOFFICE-52060).

2.3. Support

For technical support on the Alestra Enlace IP SIP Trunk service offer, visit http://www.alestra.com.mx/

©2014 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Alestra Enlace IP SIP Trunk service through a public Internet WAN connection.

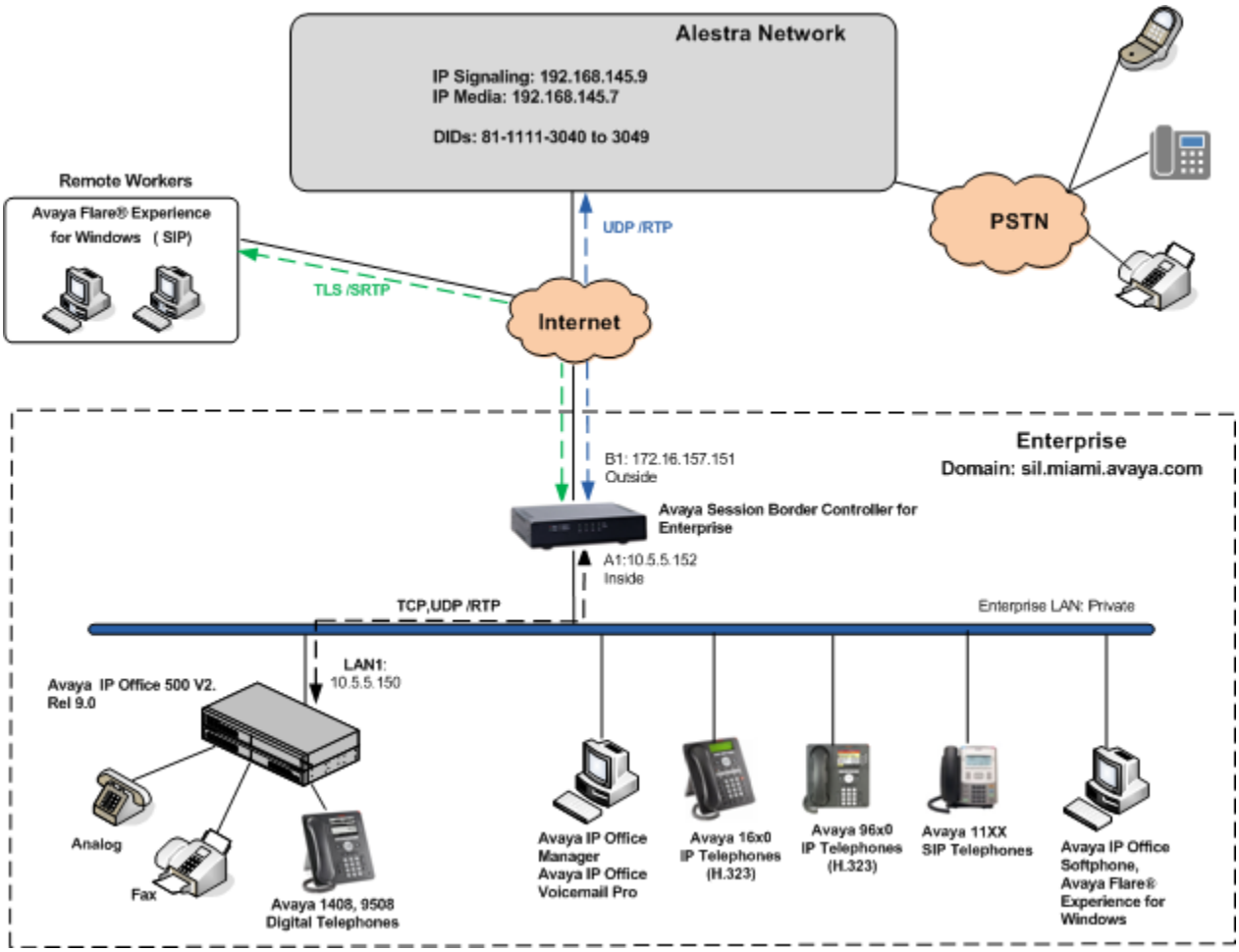


Figure 1: Test Configuration

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.

©2014 Avaya Inc. All Rights Reserved.

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

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

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

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

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

©2014 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya IP Office 500v2	9.0.0.829
Avaya IP Office Digital Expansion Module DCPx16	9.0.0.829
Avaya IP Office Manager	9.0.0.0.Build 829
Avaya IP Office Voicemail Pro	9.0.0.311
Avaya 1608 IP Telephone (H.323)	1.3 SP3
Avaya 9640 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.2
Avaya 1140E IP Telephone (SIP)	04.03.18.00
Avaya Digital Telephone 1408	32.0
Avaya Digital Phone 9508	0.45
Avaya IP Office Softphone	3.2.3.49.68975
Avaya Flare® Experience for Windows	1.1.4.23
Avaya Session Border Controller for Enterprise, on a Portwell CAD-0208 server	6.2.0.Q48
Alestra Enlace IP	
Sonus Softswitch	V07.03.06 R003
Acme Packet SBC	V6.2
Lucent 5ESS	V16.1

5. Configure Avaya IP Office

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

The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side and the Details pane on the right side. These panes will be referenced throughout the IP Office configuration.

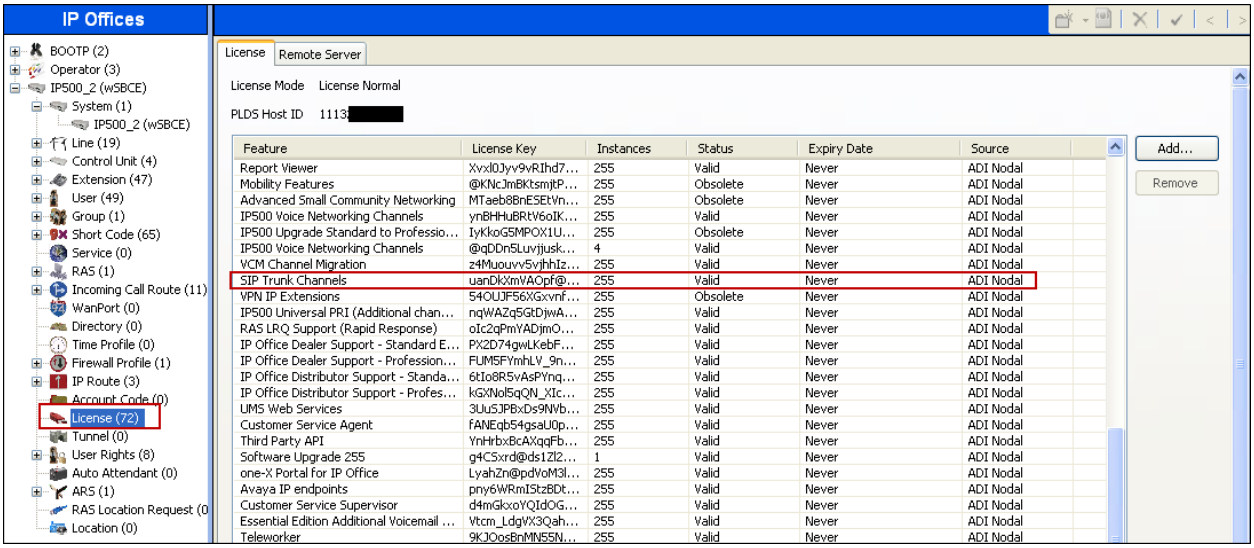
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

©2014 Avaya Inc. All Rights Reserved.

5.1. Licensing

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

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

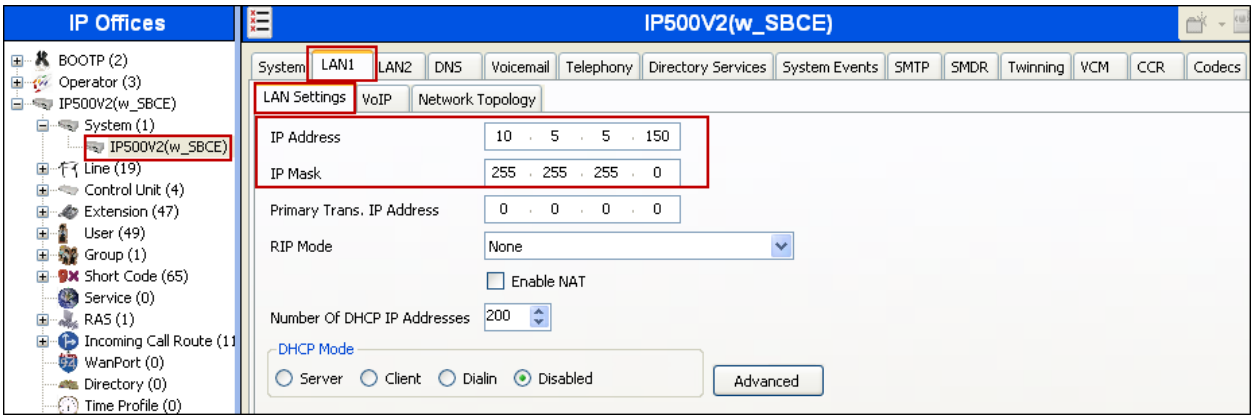


Feature	License Key	Instances	Status	Expiry Date	Source
Report Viewer	Xvxl0Jyv9vRIhd7...	255	Valid	Never	ADI Nodal
Mobility Features	@KNcJmBKtsmjtP...	255	Obsolete	Never	ADI Nodal
Advanced Small Community Networking	MTaeb8BnESEtVn...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	ynBHHuBRtV6oIK...	255	Valid	Never	ADI Nodal
IP500 Upgrade Standard to Professio...	IyKkoG5MPOX1U...	255	Obsolete	Never	ADI Nodal
IP500 Voice Networking Channels	@qDDn5Luvjjusk...	4	Valid	Never	ADI Nodal
VCM Channel Migration	z4MuouvvSvjhhIz...	255	Valid	Never	ADI Nodal
SIP Trunk Channels	uanDkXmVAOpf@...	255	Valid	Never	ADI Nodal
VPN IP Extensions	54OUJF56XGxvnf...	255	Obsolete	Never	ADI Nodal
IP500 Universal PRI (Additional chan...	nqWAZq5GtDjwA...	255	Valid	Never	ADI Nodal
RAS LRQ Support (Rapid Response)	oIc2qPmYADjmO...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Standard E...	PX2D74gwLKebF...	255	Valid	Never	ADI Nodal
IP Office Dealer Support - Profession...	FUM5FYmhLV_9n...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Standa...	6tIo8R5vAsPYnq...	255	Valid	Never	ADI Nodal
IP Office Distributor Support - Profes...	kGXNoI5qQN_XIc...	255	Valid	Never	ADI Nodal
UMS Web Services	3Uu5JPBxDs9NVb...	255	Valid	Never	ADI Nodal
Customer Service Agent	fANEqb54gsaU0p...	255	Valid	Never	ADI Nodal
Third Party API	YnHrbxBcAXqqFb...	255	Valid	Never	ADI Nodal
Software Upgrade 255	g4CSxrd@ds1Zl2...	1	Valid	Never	ADI Nodal
one-X Portal for IP Office	LyahZn@pdVoM3l...	255	Valid	Never	ADI Nodal
Avaya IP endpoints	pny6WRmISzBDt...	255	Valid	Never	ADI Nodal
Customer Service Supervisor	d4mGkxoYQIdOG...	255	Valid	Never	ADI Nodal
Essential Edition Additional Voicemail ...	Vtcm_LdgVX3Qah...	255	Valid	Never	ADI Nodal
Teleworker	9KJOosBnMN55N...	255	Valid	Never	ADI Nodal

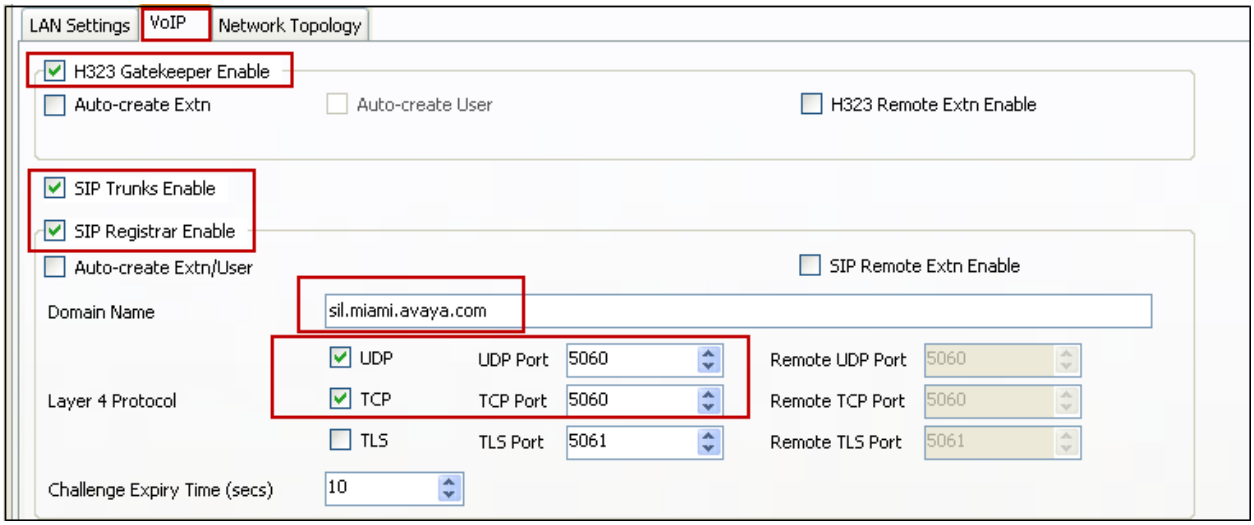
©2014 Avaya Inc. All Rights Reserved.

5.2. LAN Settings

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



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

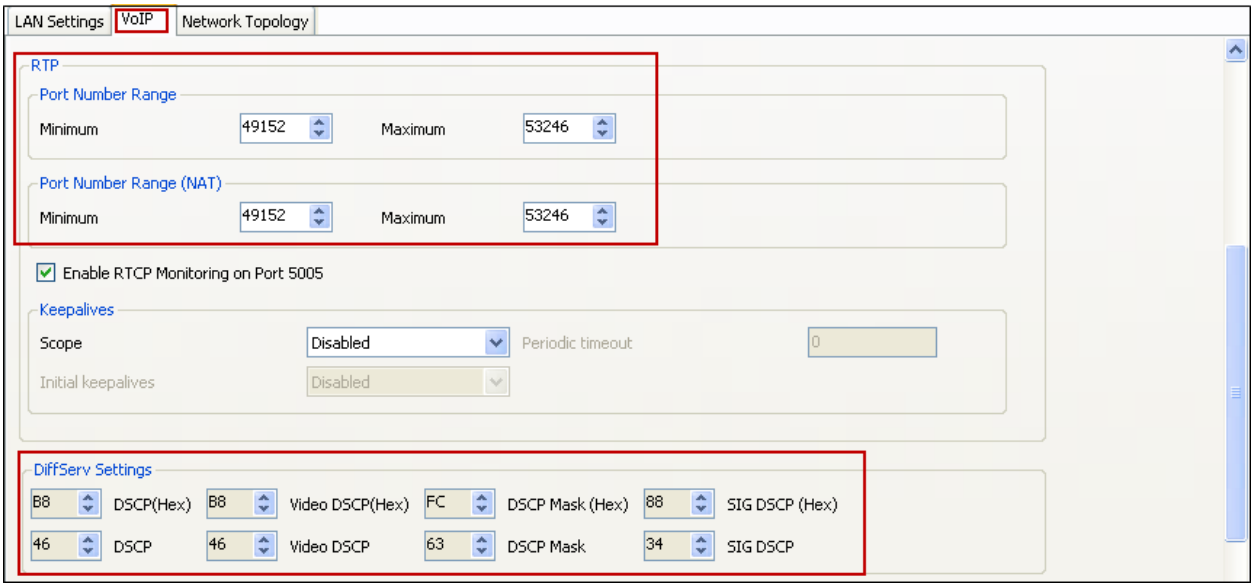


©2014 Avaya Inc. All Rights Reserved.

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

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

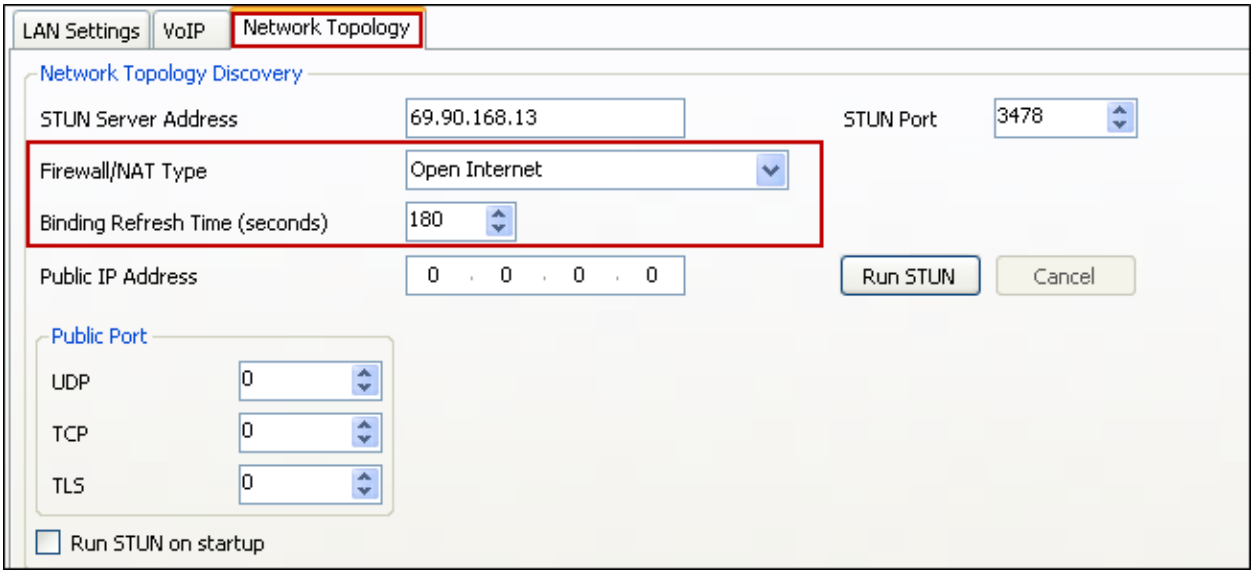
All other parameters should be set according to customer requirements.



©2014 Avaya Inc. All Rights Reserved.

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

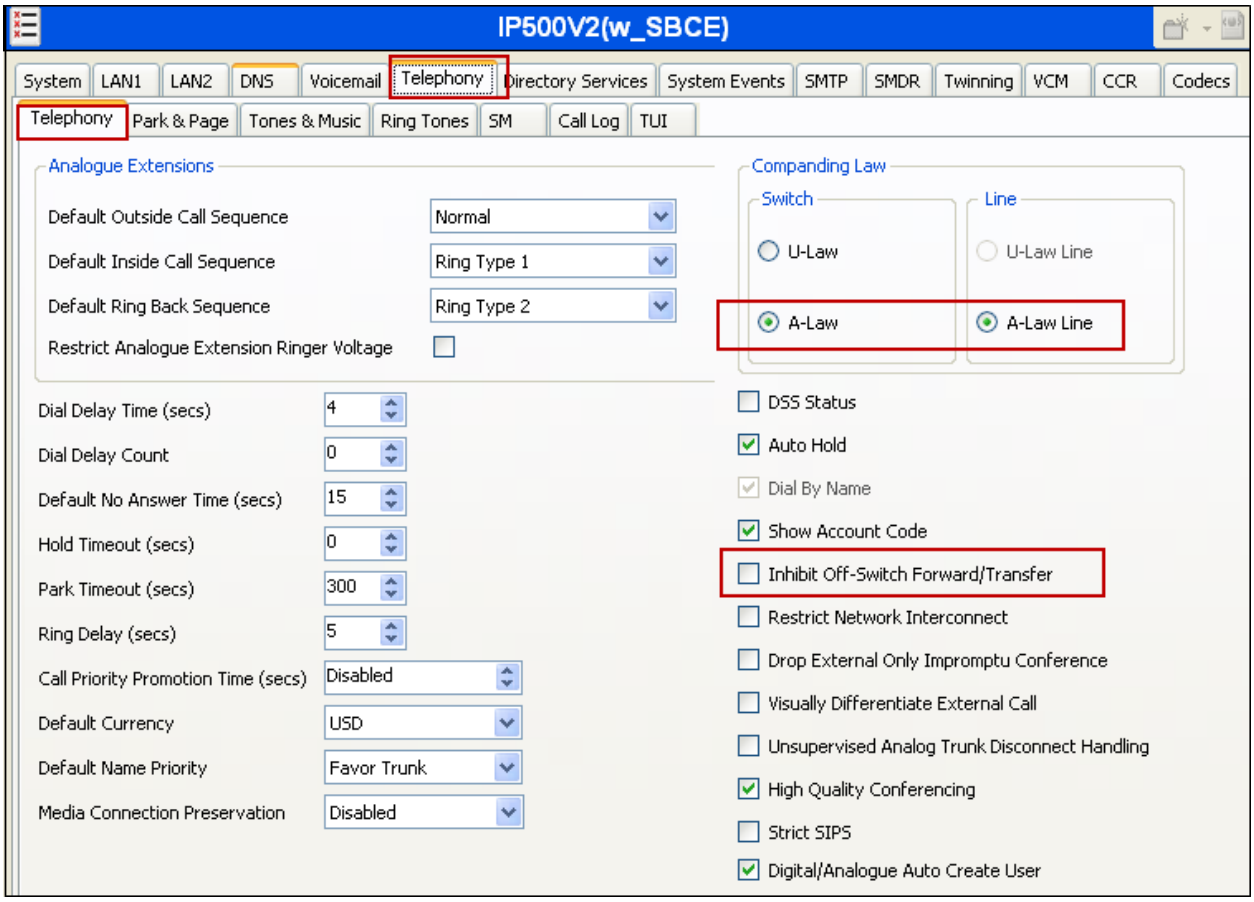
- Select the **Firewall/NAT Type** from the pull-down menu to the option that matches the network configuration. Since no network address translation (NAT) was used in the compliance test, the parameter was set to ***Open Internet***. With this configuration, settings obtained by STUN lookups are ignored.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



©2014 Avaya Inc. All Rights Reserved.

5.3. System Telephony Settings

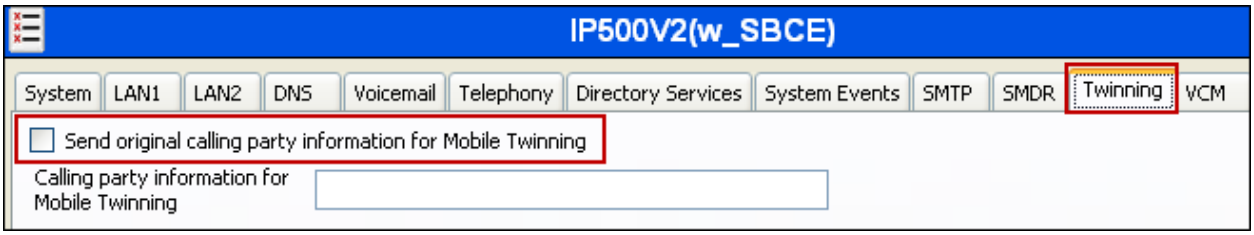
Navigate to the **Telephony → Telephony** Tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. In Mexico, ***A-Law*** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the SIP trunk to the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



©2014 Avaya Inc. All Rights Reserved.

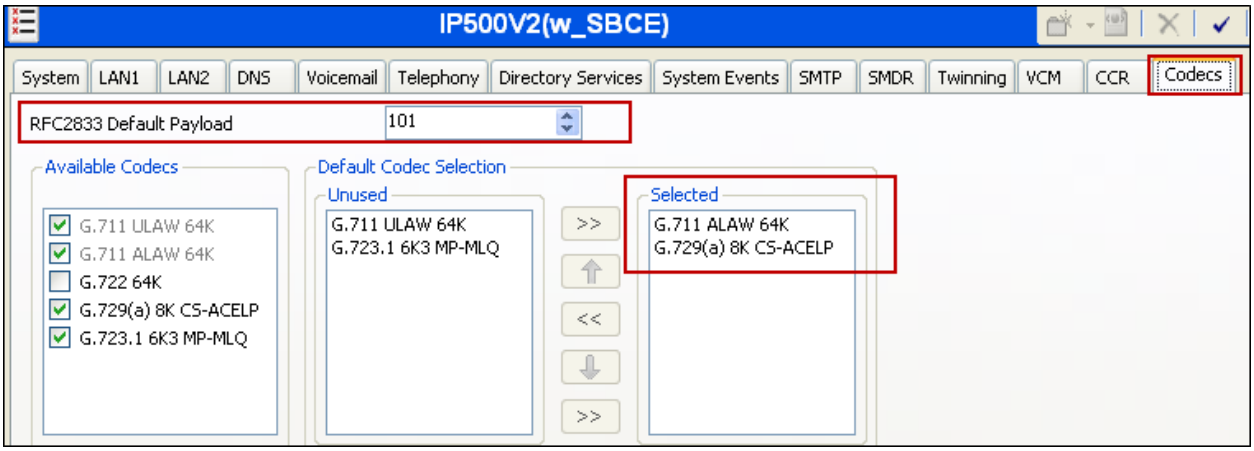
5.4. Twinning Calling Party Settings

Navigate 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.



5.5. System Codecs Settings

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



©2014 Avaya Inc. All Rights Reserved.

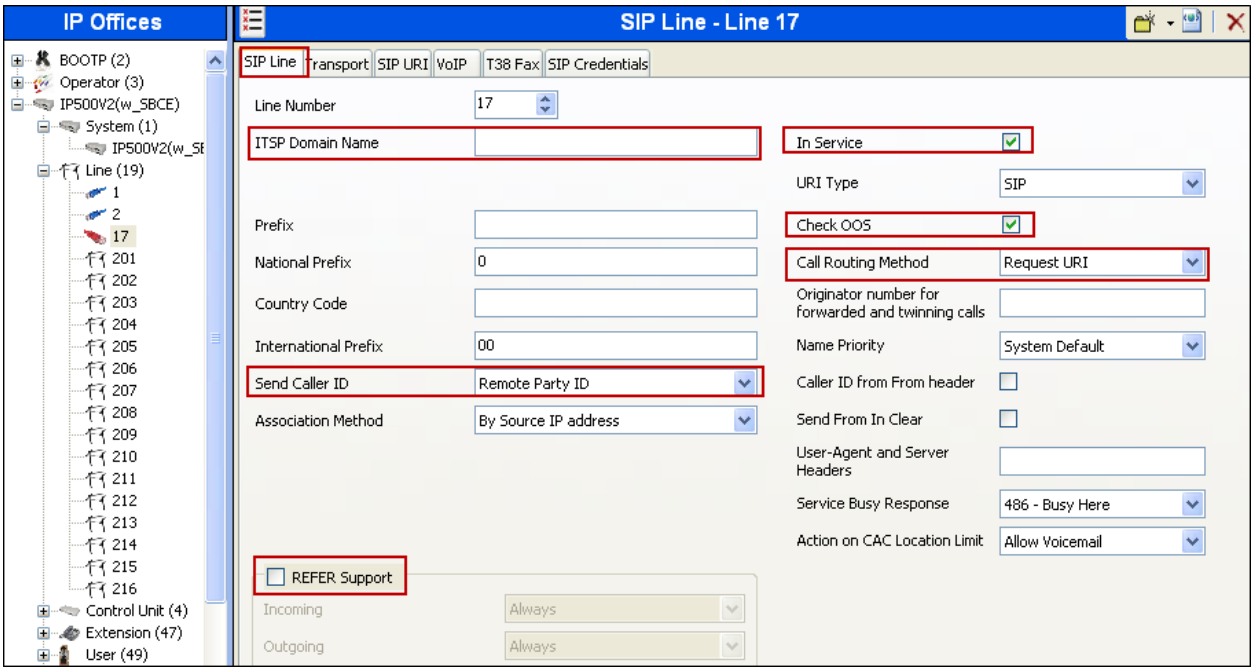
5.6. Administer SIP Line

A SIP line is created to establish the SIP connection between the IP Office and the private interface of the Avaya SBCE. This line will carry outbound and inbound traffic between to and from the service provider. 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** blank. IP Office will use the ITSP Proxy Address, defined on the Transport tab on **Section 5.6.2**, as the host portion of the SIP URI in the From headers of messages sent to the network.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will check the responses to SIP OPTIONS messages sent to the service provider to determine the operational status of the SIP Line.
- Set **Call Routing Method** to ***Request URI***.
- Set **Send Caller ID** to ***Remote Party ID.*** This was required to allow the presentation of the PSTN originator caller ID, for call forwarding of inbound calls back to the PSTN and some extension to cellular (twinning) scenarios.
- Uncheck the **REFER support** box. REFER is not supported by Alestra.
- Default values may be used for all other parameters.

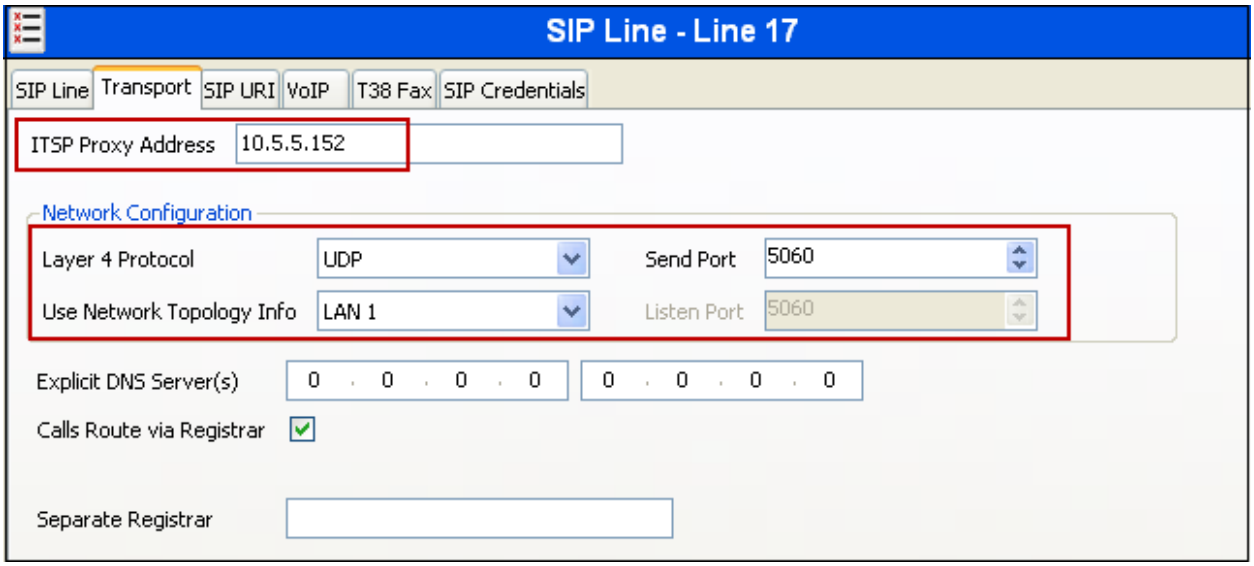


©2014 Avaya Inc. All Rights Reserved.

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.



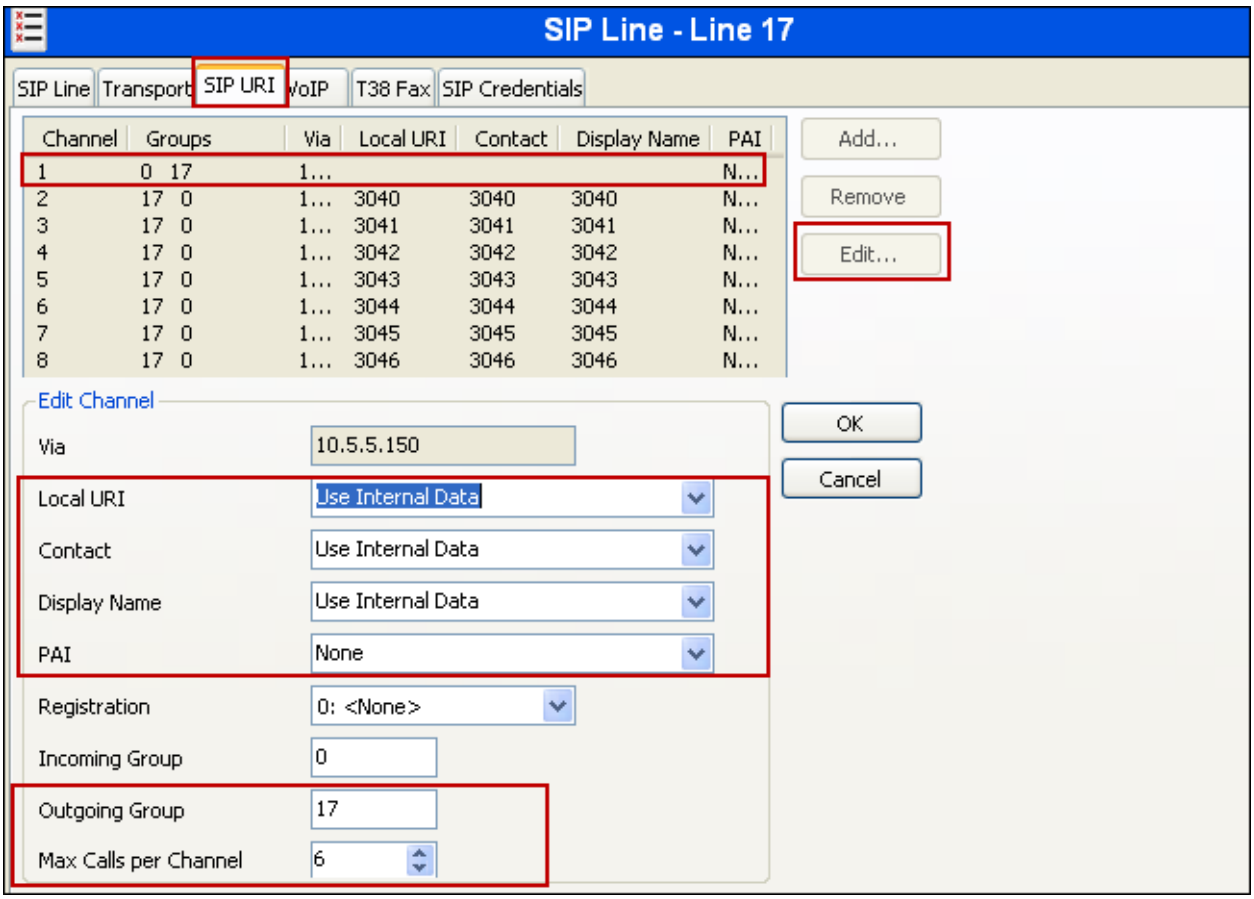
©2014 Avaya Inc. All Rights Reserved.

5.6.3. SIP URI Tab

A SIP URI entry needs to be created to match each number that the IP Office and Alestra will accept on this line. Select the **SIP URI** tab, click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit…** button. In the example screen below, a previously configured entry is edited.

For the compliance test, in the outbound direction, a single SIP URI entry was created that will populate the user part of the origination headers on outbound calls with the 10 digit DID number set in the **SIP** tab of that User, as shown in **Section 5.7.** The entry was created with the parameters shown below:

- Set **Local URI**, **Contact** and **Display Name** to ***Use Internal Data***. Set **PAI** to ***None***.
- 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 outgoing group ***17*** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

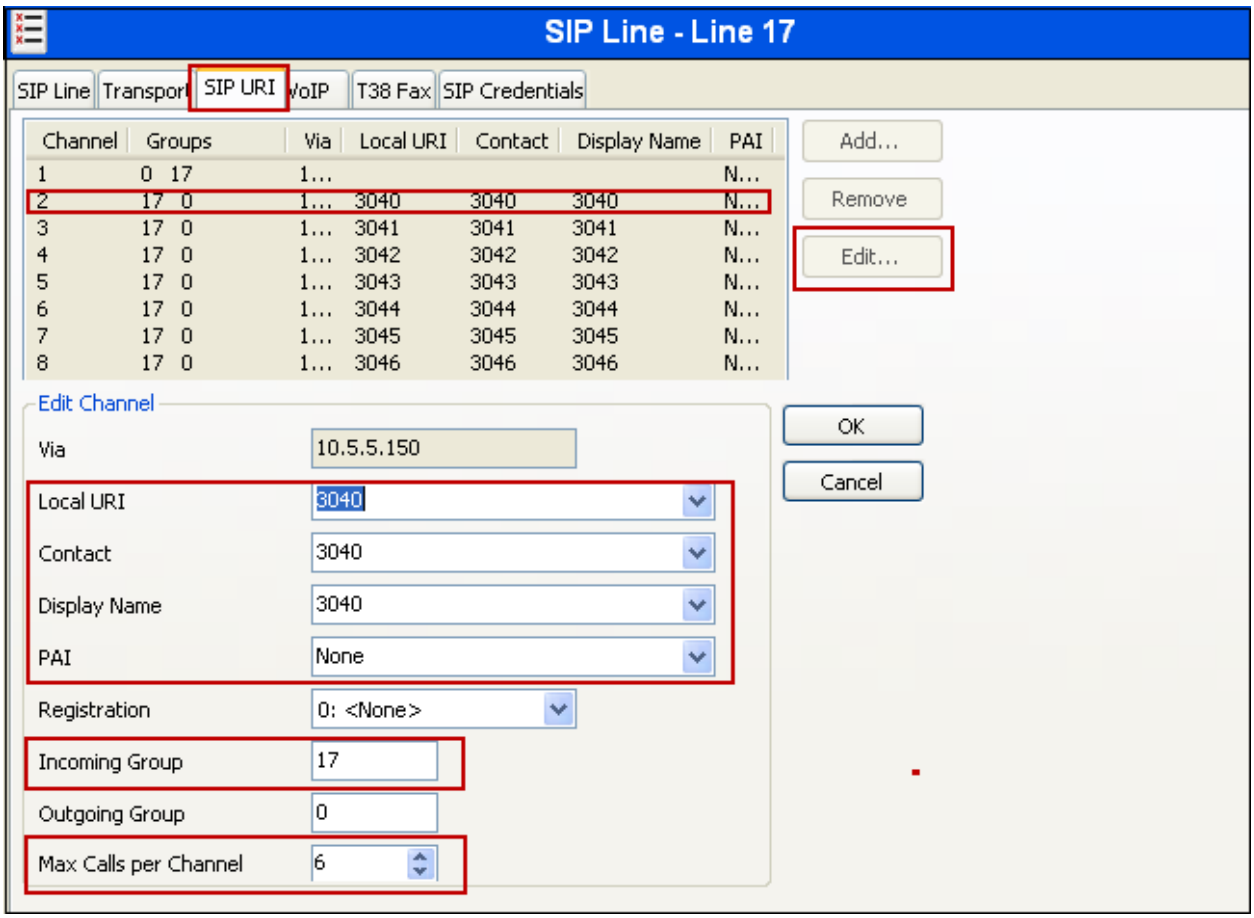


©2014 Avaya Inc. All Rights Reserved.

On inbound calls, Alestra sent in the Request-URI header to the IP Office the last 4 digits of the DID numbers assigned to the enterprise.

A SIP URI entry needs to be created to match each incoming number that the IP Office will accept on this line. The example below shows the entry for the DID number ending in digits 3040:

- Set **Local URI**, **Contact** and **Display Name** to ***3040***. Set **PAI** to ***None***.
- 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. For the compliance test, a new incoming group ***17*** was defined that only contains this line (line 17).
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

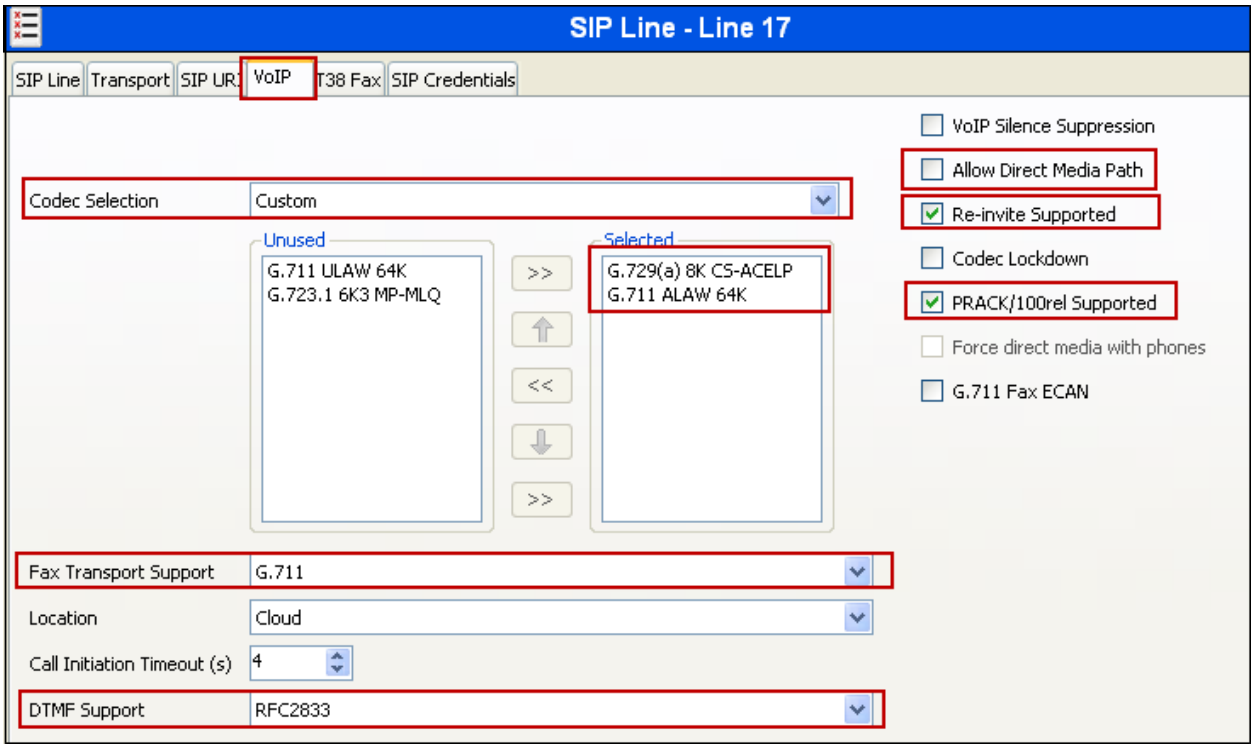


©2014 Avaya Inc. All Rights Reserved.

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 ***G.711***.
- Set the **DTMF Support f**ield to ***RFC2833.*** This directs the IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Leave **Allow Direct Media Path** unchecked. Direct media was not used during the compliance test. See **Section 2.2** for more details.
- Check th**e Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.
- Check the **PRACK/100rel Supported** box, to advertise the support for provisional responses and Early Media to Alestra.
- Default values may be used for all other parameters.

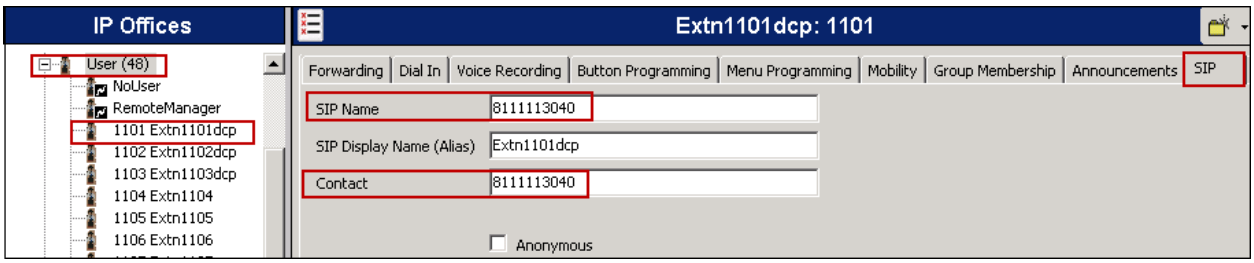


©2014 Avaya Inc. All Rights Reserved.

5.7. Users

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

The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From and Contact headers for outgoing SIP trunk calls. The example below shows the settings for user "Extn1101dcp". The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Alestra. In the example, the DID number ***8111113040*** was used. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name.



©2014 Avaya Inc. All Rights Reserved.

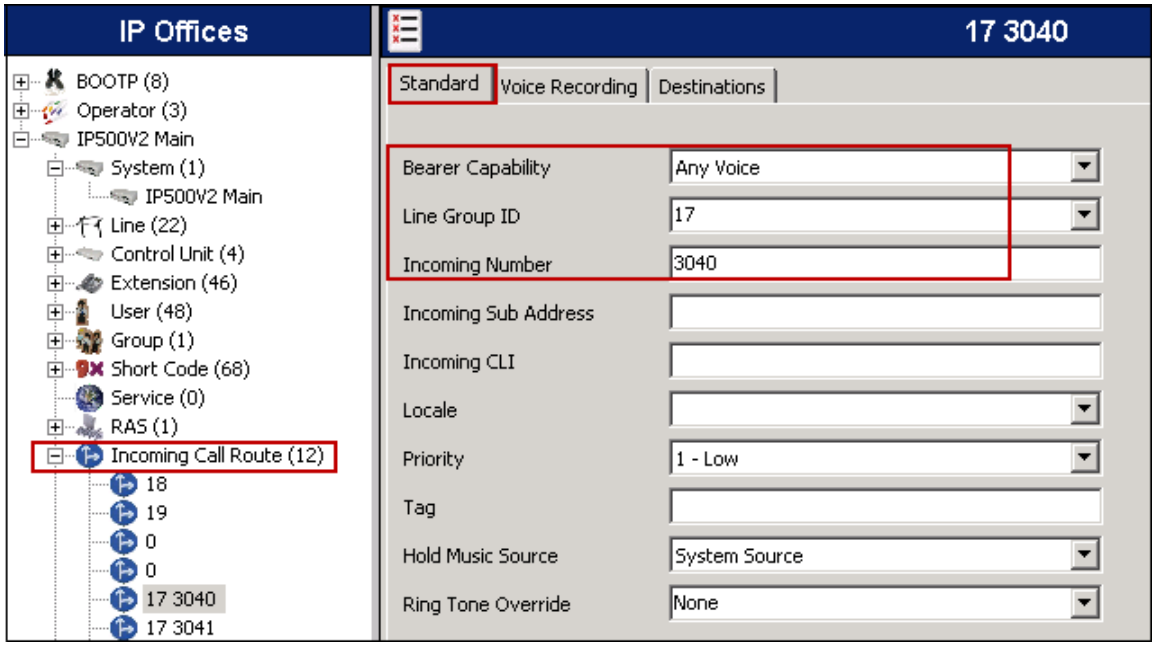
5.8. Incoming Call Route

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

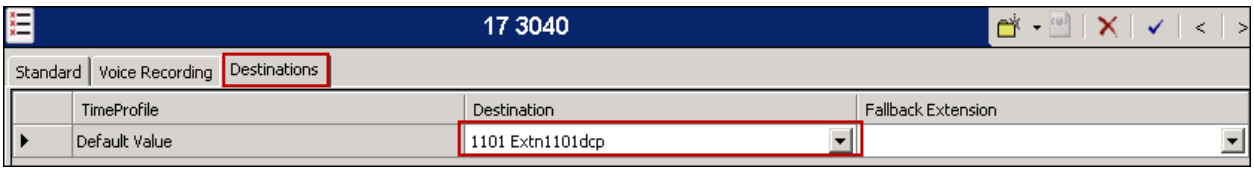
To add a new incoming call route, from the left Navigation Pane, right-click on **Incoming Call Route** and select **New** (not shown). The screen below shows the route for one of the DID numbers assigned to the enterprise by Alestra, 8111113040 in this example.

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

- Set **Bearer Capacity** to ***Any Voice***.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.6**.
- Set the **Incoming Number** to the last 4 digits of the DID number assigned by Alestra. (Alestra sent in the Request-URI to the IP Office only the last 4 digits of the DID numbers).
- Default values may be used for all other parameters.



On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. Click the **OK** button (not shown). In this example, incoming calls to 8111113040 on line 17 are routed to extension 1101.

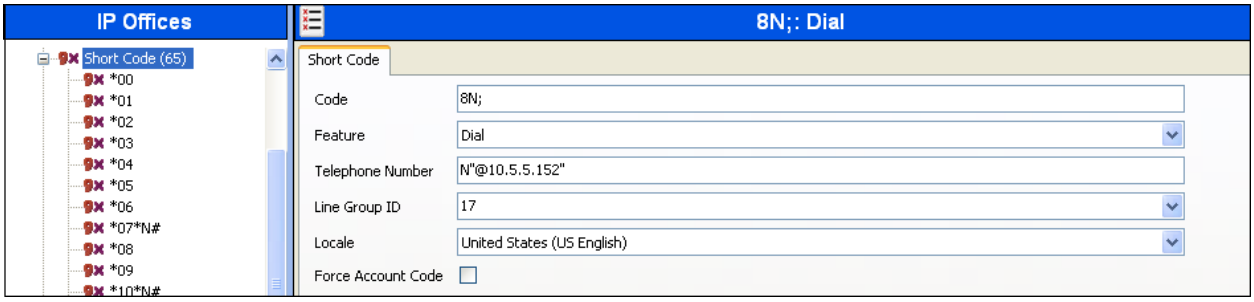


©2014 Avaya Inc. All Rights Reserved.

5.9. Short Code

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

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, ***8N;***. This short code will be invoked when the user dials 8 followed by any number.
- Set **Feature** to ***Dial***. This is the action that the short code will perform.
- Set **Telephone Number** to ***N"@10.5.5.152"***. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value ***N*** represents the number dialed by the user. The IP address 10.5.5.152 is the IP address of the private interface of the Avaya SBCE.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line** in **Section 5.6.3**. This short code will use this line group when placing outbound calls.
- Default values may be used for all other parameters.

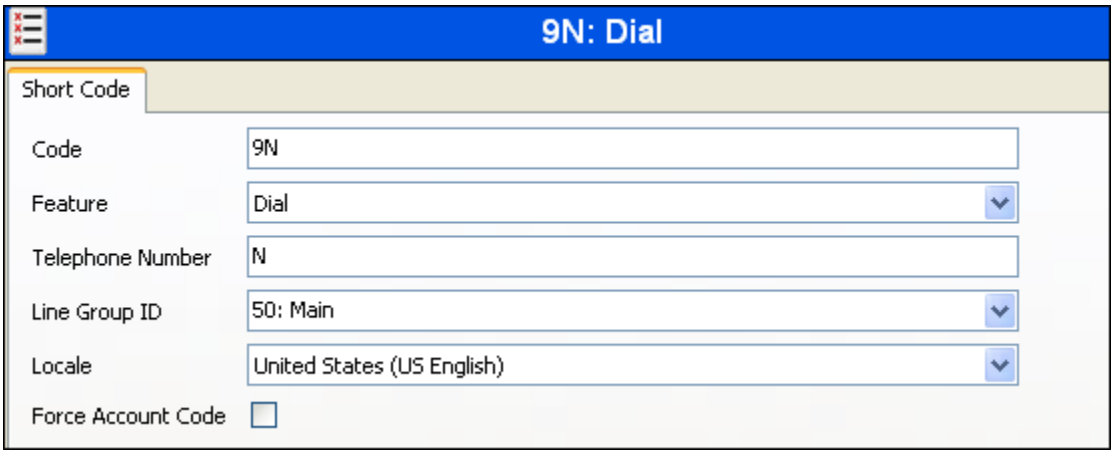


©2014 Avaya Inc. All Rights Reserved.

5.10. Automatic Route Selection

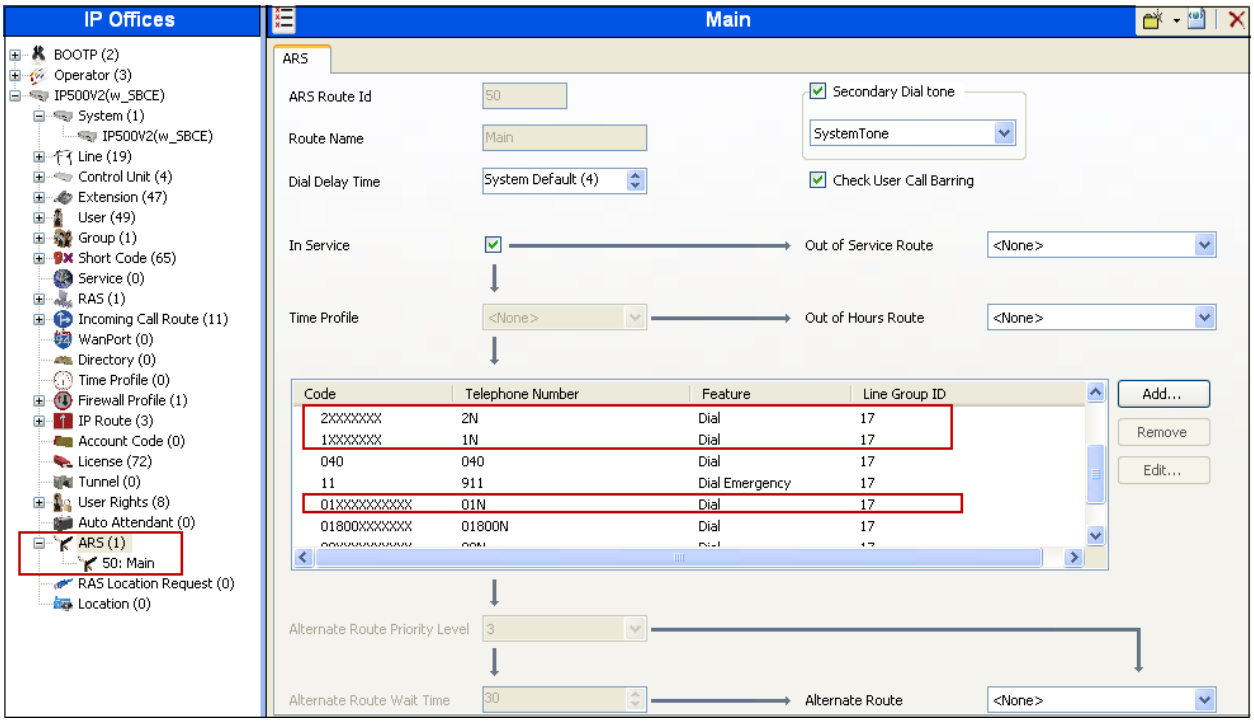
Optionally, Automatic Route Selection (ARS) can be used rather than the simple short code approach described above. With ARS, secondary dial tone can be provided after the access code. Other features like time-based routing criteria and alternate routing can be specified so that a call can re-route automatically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

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



©2014 Avaya Inc. All Rights Reserved.

The following screen shows the example ARS configuration for the route ***Main***. Note the sequence of ***X***s used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first digit on the string. This type of setting results in a much quicker response in the delivery of the call by the IP Office. For example, for local calls, the user dialed 9 plus the 8 digit local number, starting with a 1 or a 2, which was the range of local numbers used during the compliance test. For national long distance calls in Mexico, the user dialed 9, then 01, followed by 10 digit numbers.

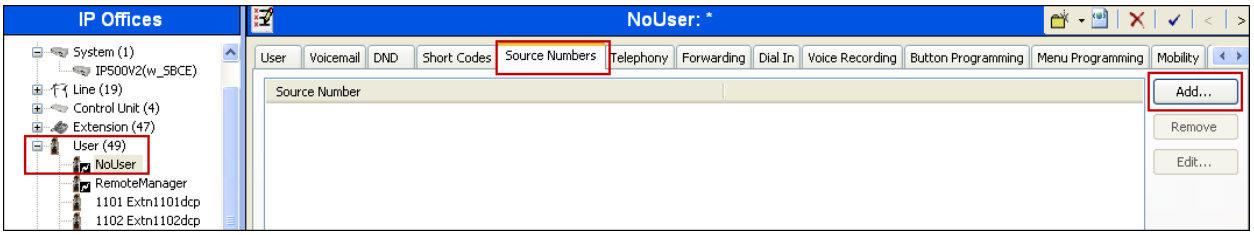


©2014 Avaya Inc. All Rights Reserved.

5.11. Privacy/Anonymous Calls

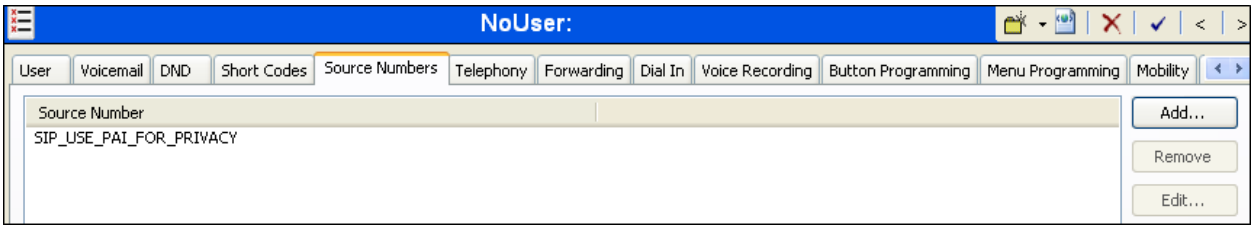
For outbound calls with privacy (anonymous) enabled, IP Office will replace the calling party number in the From and Contact headers of the SIP INVITE message with "restricted" and "anonymous" respectively. IP Office can be configured to use the P-Preferred-Identity (PPI) or P-Asserted-Identity (PAI)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

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



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

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



5.12. 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 (not shown).

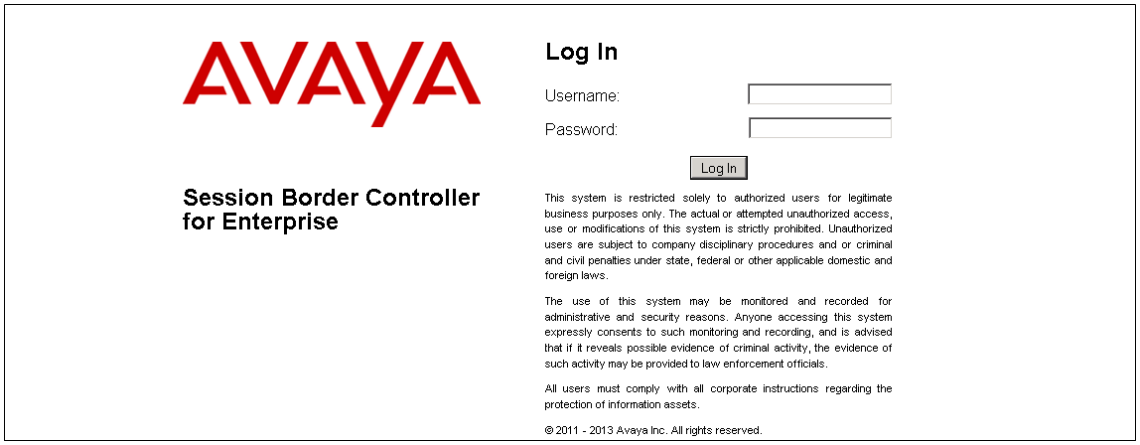
©2014 Avaya Inc. All Rights Reserved.

6. Configure Avaya Session Border Controller for Enterprise

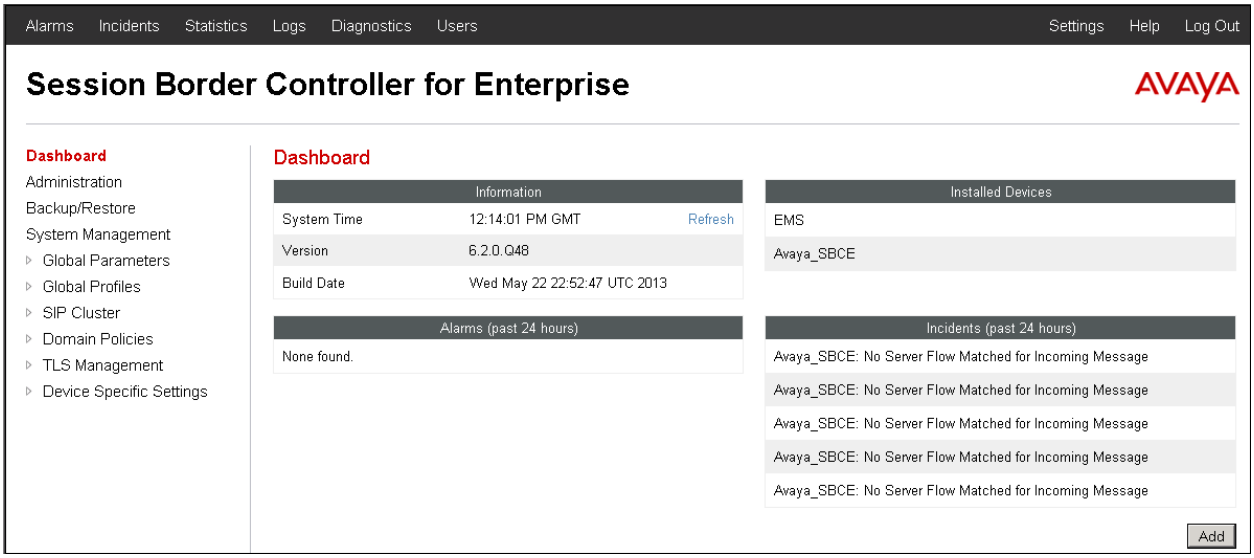
In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Alestra Enlace IP SIP Trunk service. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks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

6.1. System Access

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



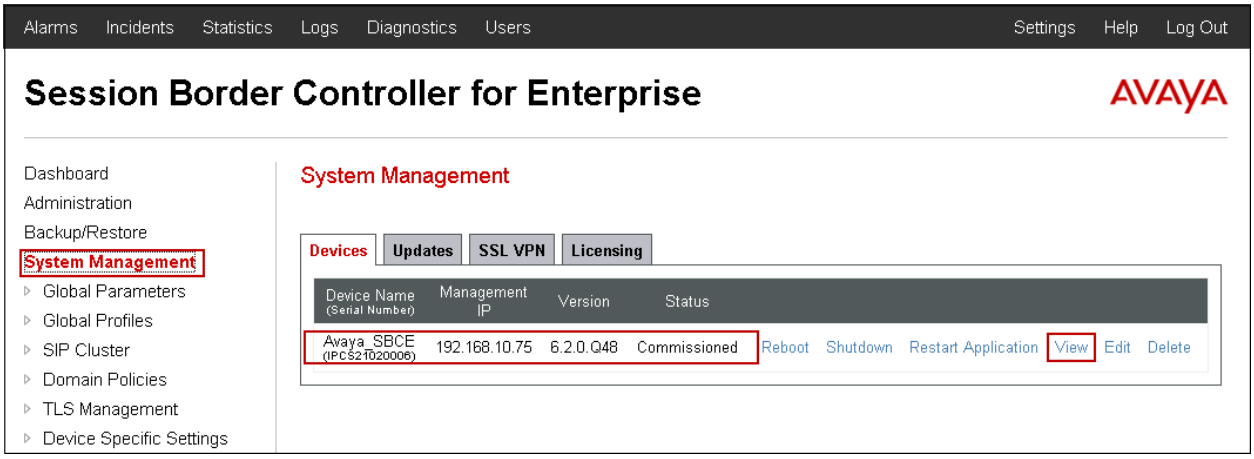
Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.



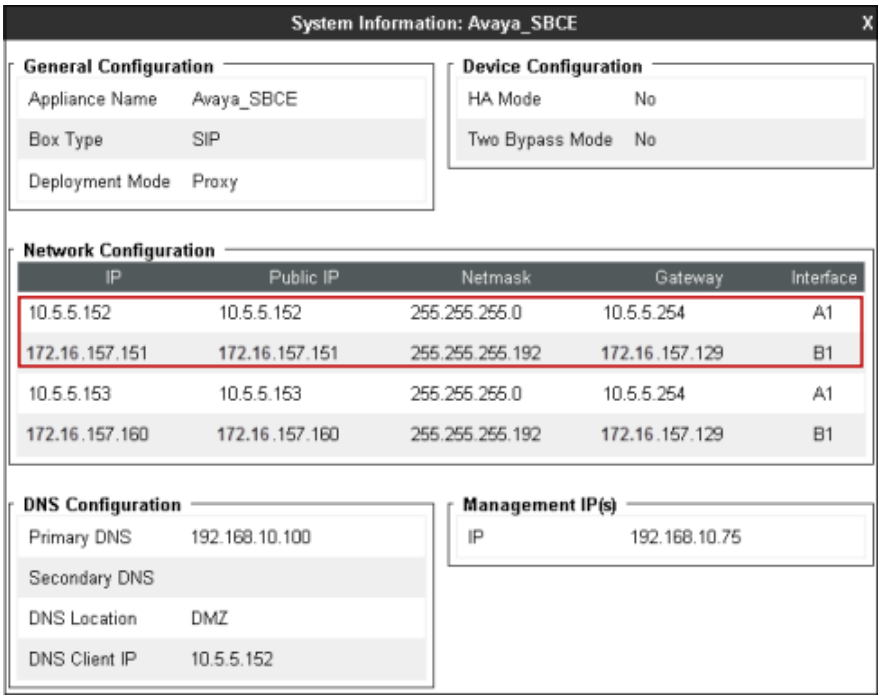
©2014 Avaya Inc. All Rights Reserved.

6.2. System Management

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



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



©2014 Avaya Inc. All Rights Reserved.

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

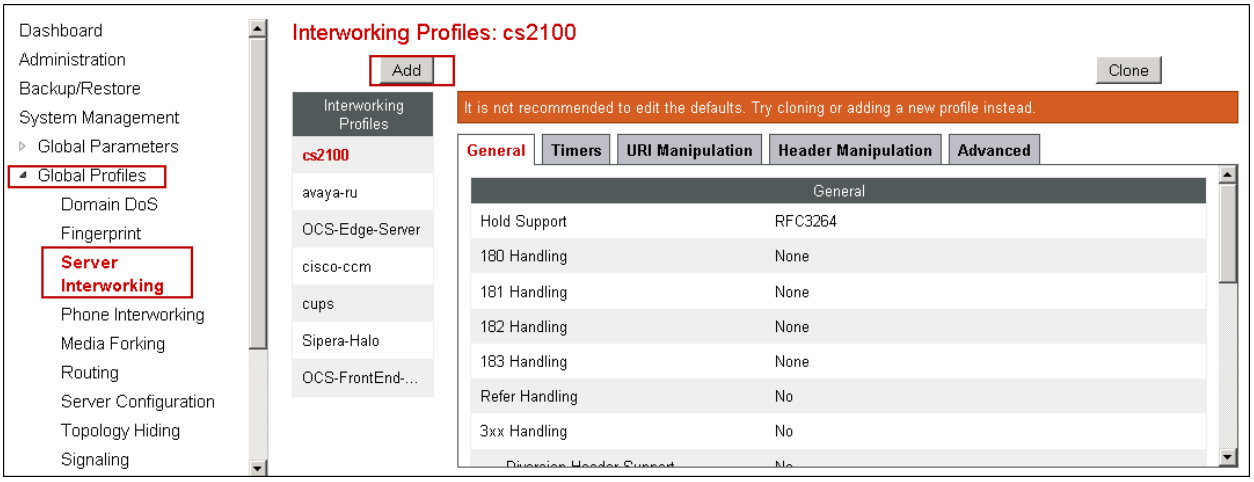
6.3. Global Profiles

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

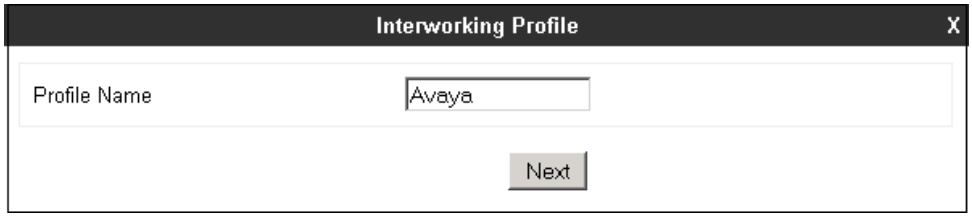
6.3.1. Server Interworking

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

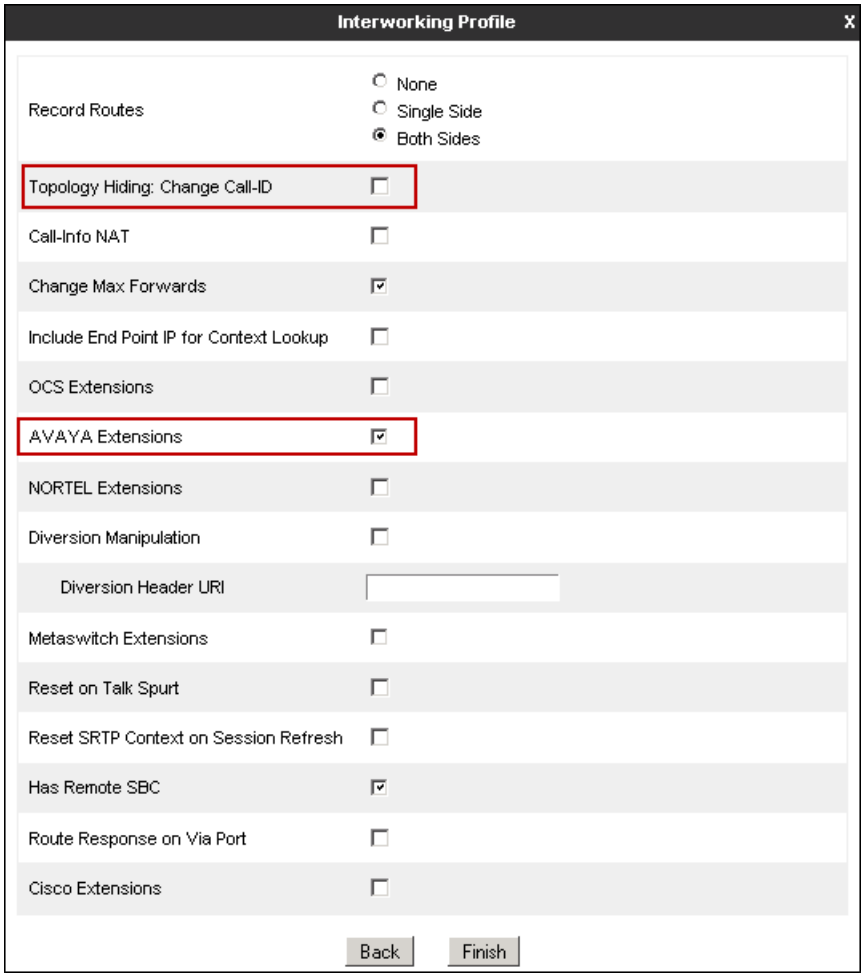


©2014 Avaya Inc. All Rights Reserved.

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

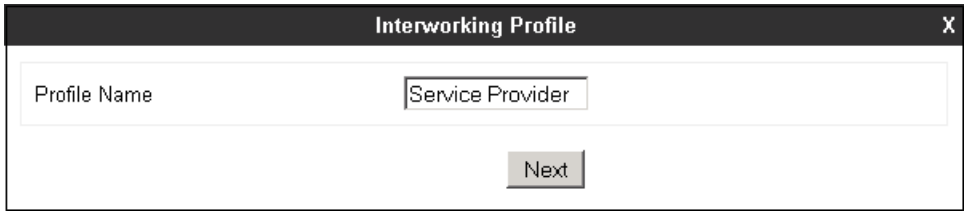
©2014 Avaya Inc. All Rights Reserved.

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



©2014 Avaya Inc. All Rights Reserved.

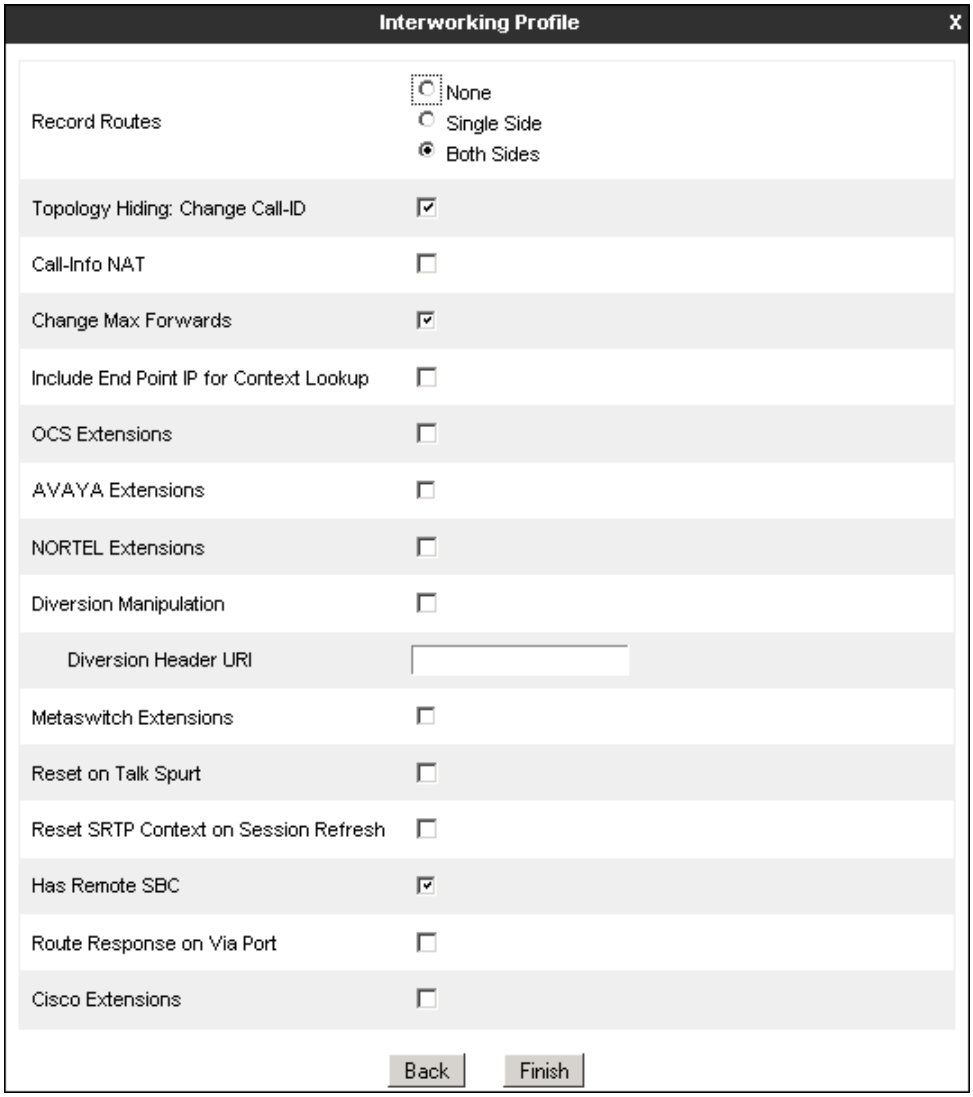
A second interworking profile named **Service Provider** in the direction of the SIP trunk to Alestra was similarly created. For this profile default values were used for all parameters.



General tab:

©2014 Avaya Inc. All Rights Reserved.

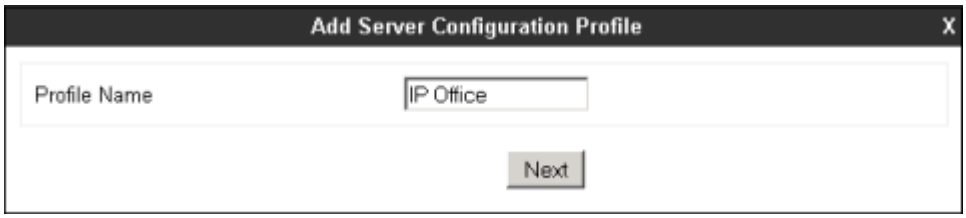
Advanced Settings tab:



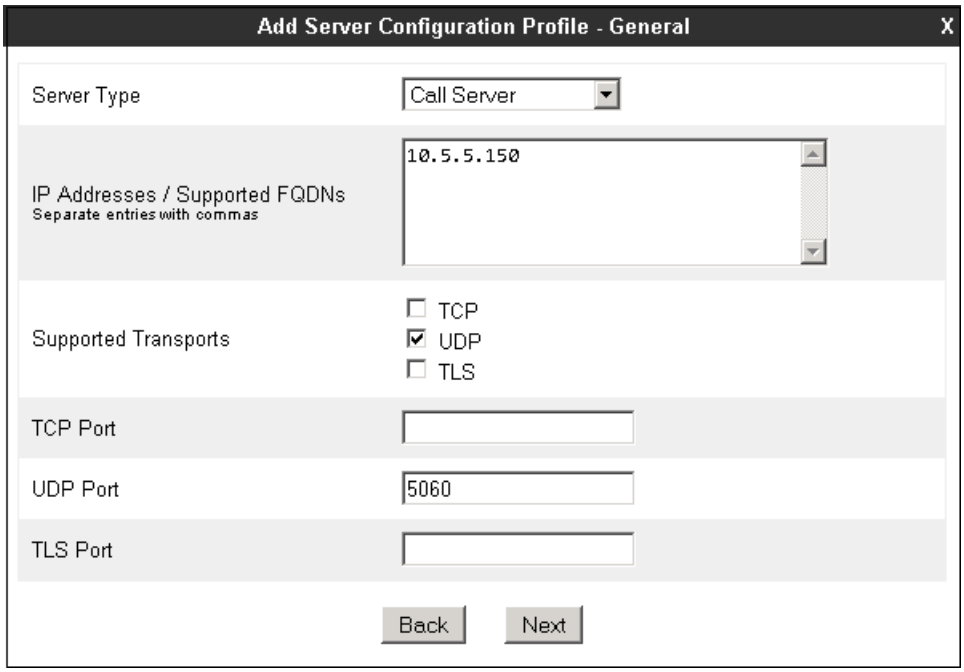
©2014 Avaya Inc. All Rights Reserved.

6.3.2. Server Configuration

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

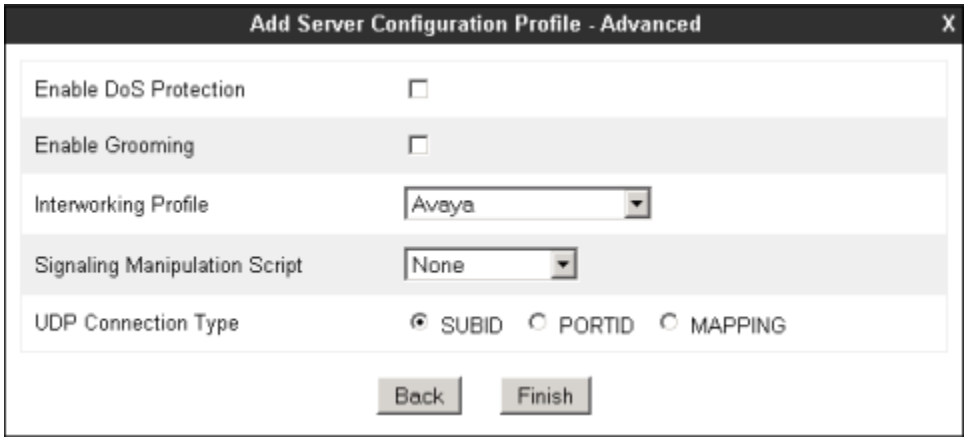


On the **Add Server Configuration Profile - General** Tab select ***Call Server*** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field**,** enter the IP address of the IP Office LAN1, as defined in **Section 5.2**. Select **UDP** for **Supported Transports**,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

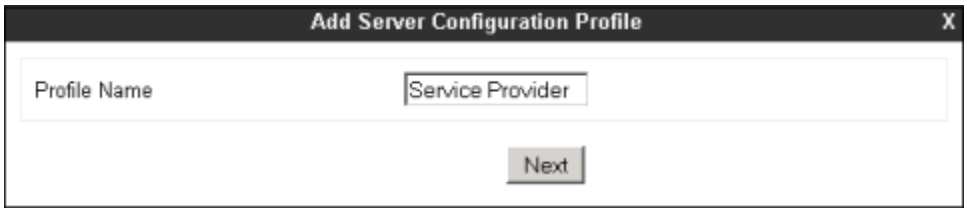


©2014 Avaya Inc. All Rights Reserved.

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

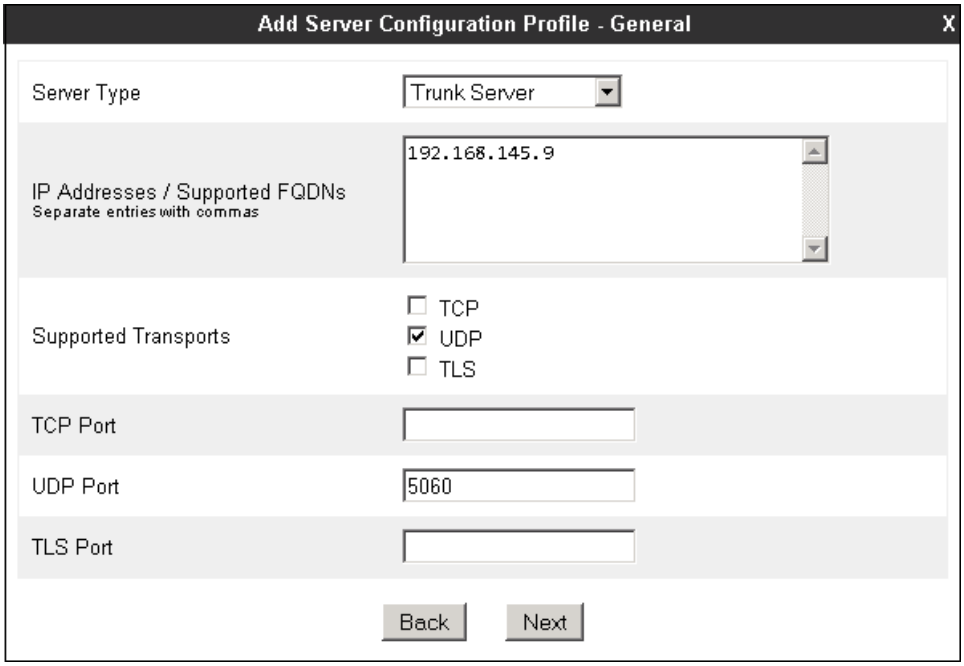


Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown). Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.

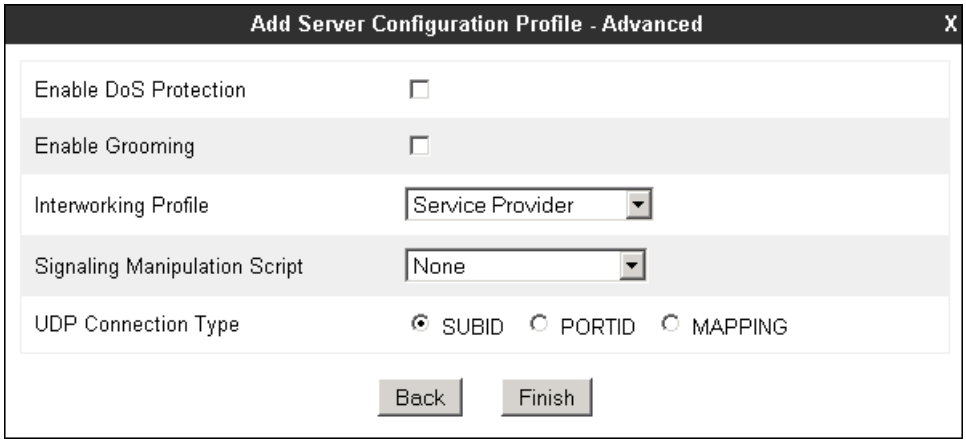


©2014 Avaya Inc. All Rights Reserved.

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 ***192.168.145.9***, the IP Address of the Alestra's SIP proxy server. Select **UDP** for **Supported Transports**, and enter ***5060*** under **UDP Port**, as specified by Alestra.



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**

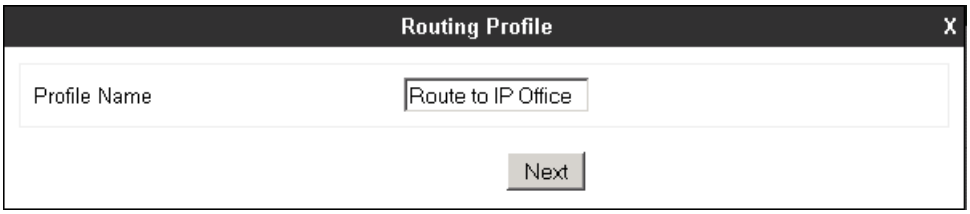


©2014 Avaya Inc. All Rights Reserved.

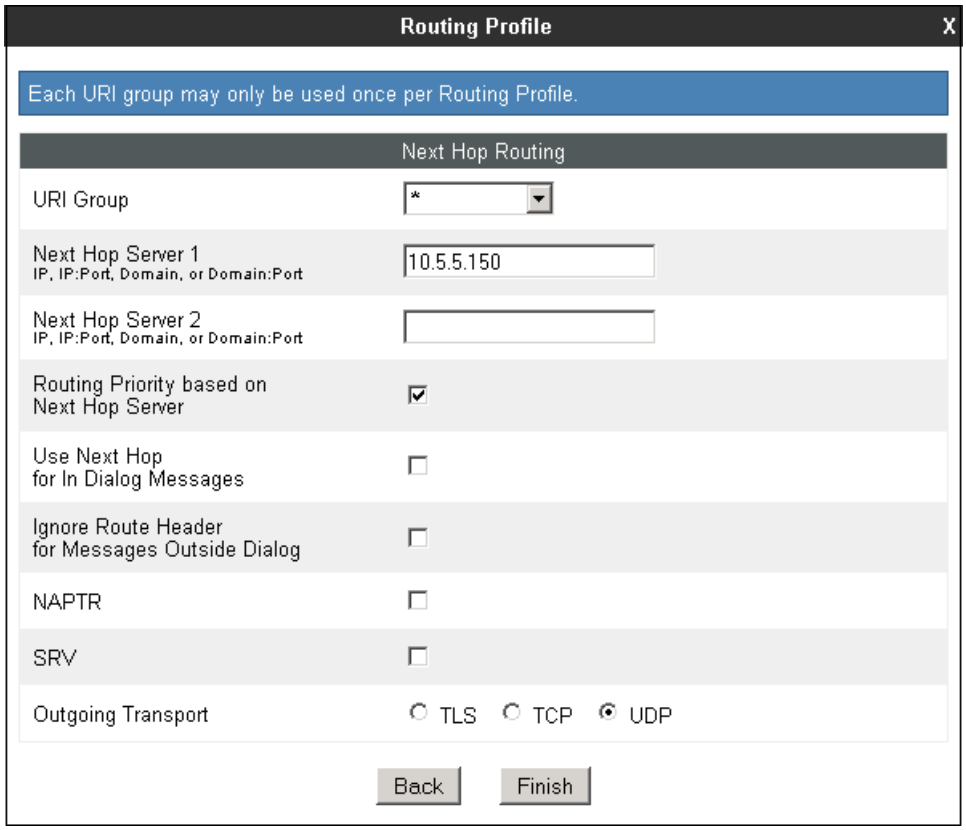
6.3.3. Routing Profiles

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 as the destination, and the second one for outbound calls, which are routed to the Alestra 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.**



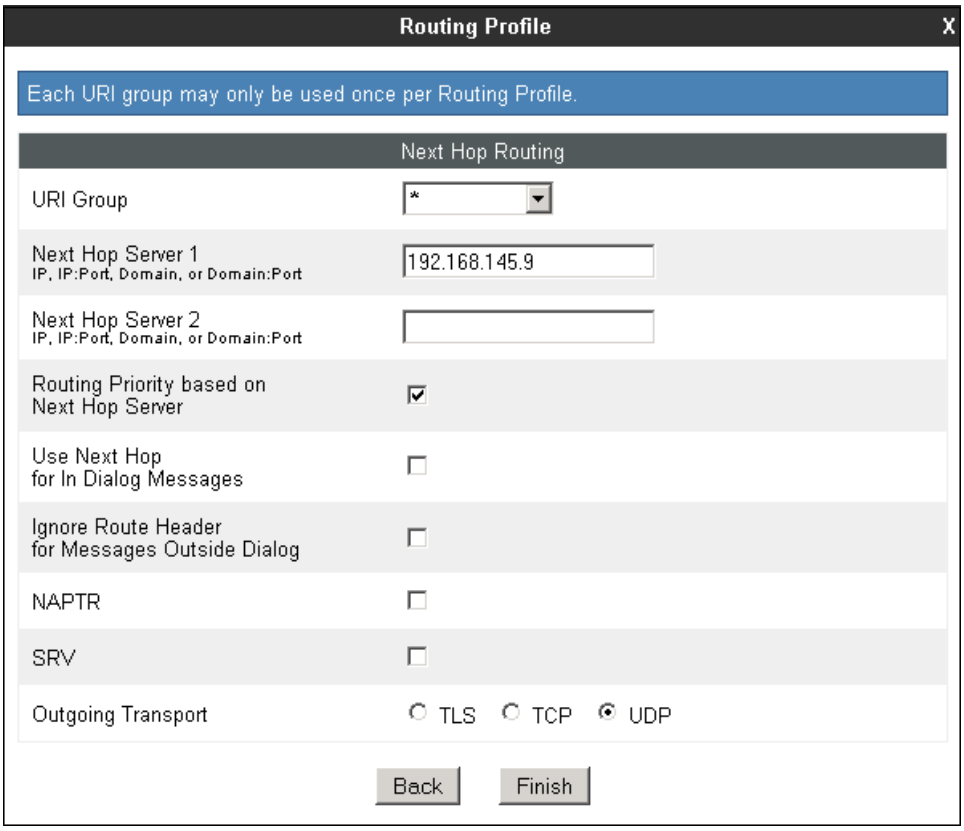
On the **Next Hop Routing** tab, enter the IP Address of the IP Office LAN1 interface as **Next Hop Server 1**. Since the default well-known port value of 5060 for UDP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **UDP** for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



©2014 Avaya Inc. All Rights Reserved.

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**. 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**.



©2014 Avaya Inc. All Rights Reserved.

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.

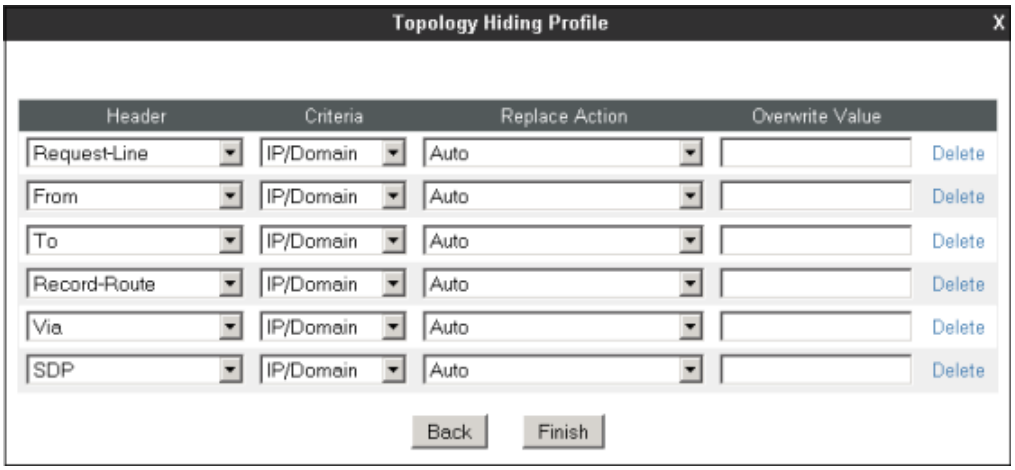
Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, only the minimum configuration required to achieve interoperability on the SIP 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.

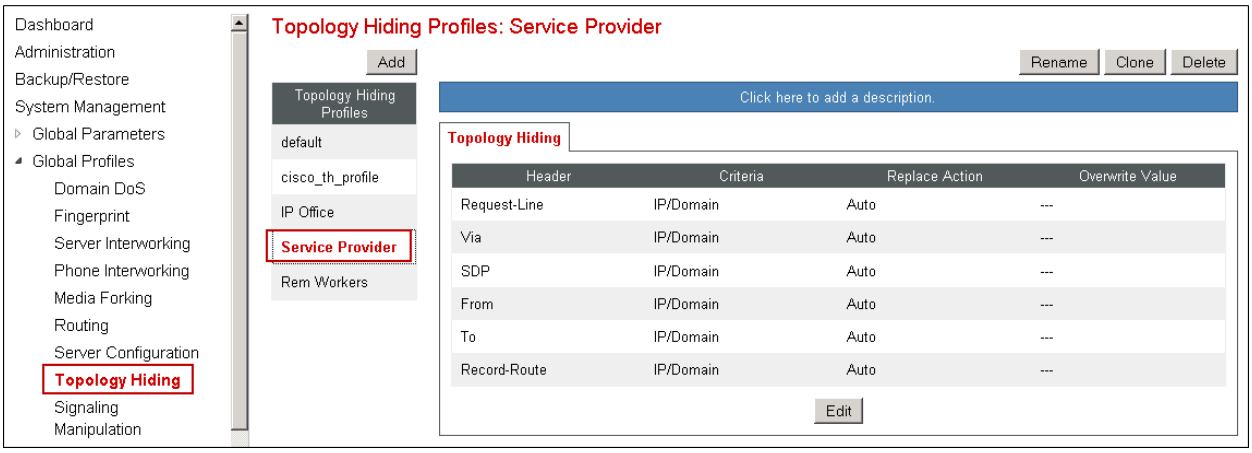
©2014 Avaya Inc. All Rights Reserved.

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



A Topology Hiding profile named **Service Provider** was similarly configured in the direction of the SIP trunk to Alestra. Since IP addresses instead of domains were used in all SIP messages between the Alestra SIP proxy server and the Avaya SBCE, the default action of ***Auto*** was also used in this profile. Even though both profiles used the same default settings, they were separately defined with the purpose of allowing possible future changes to be made to the profile in one of the directions, without affecting the settings in the other direction.

The screen below shows the **Service Provider** profile once the configuration was completed.



©2014 Avaya Inc. All Rights Reserved.

6.4. Domain Policies

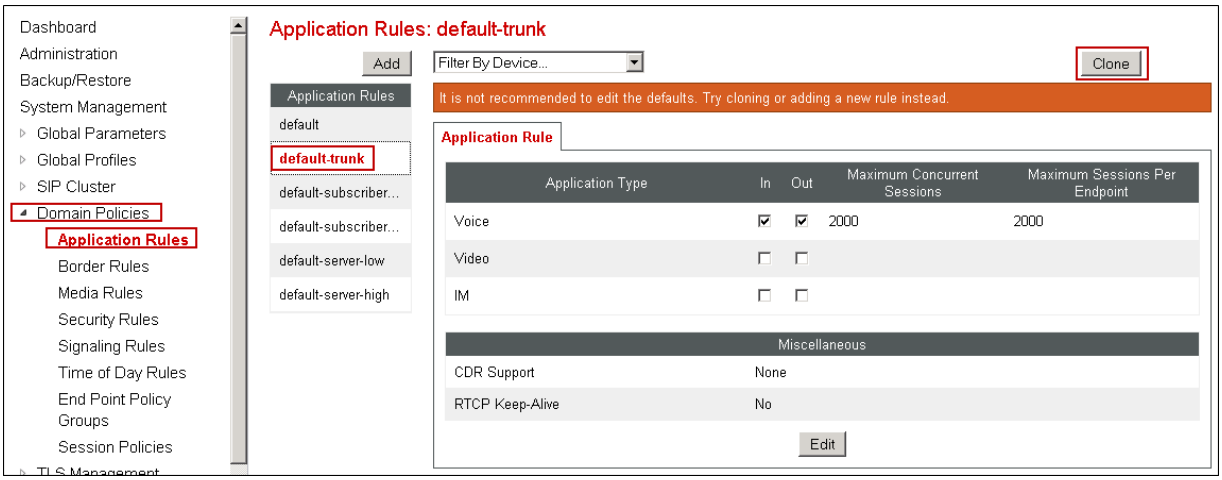
Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

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.

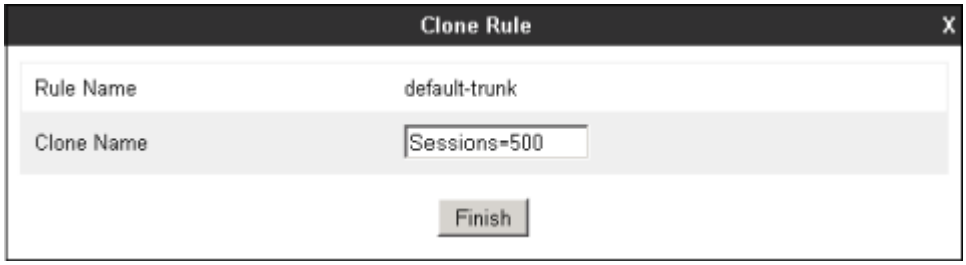
6.4.1. Application Rules

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**.

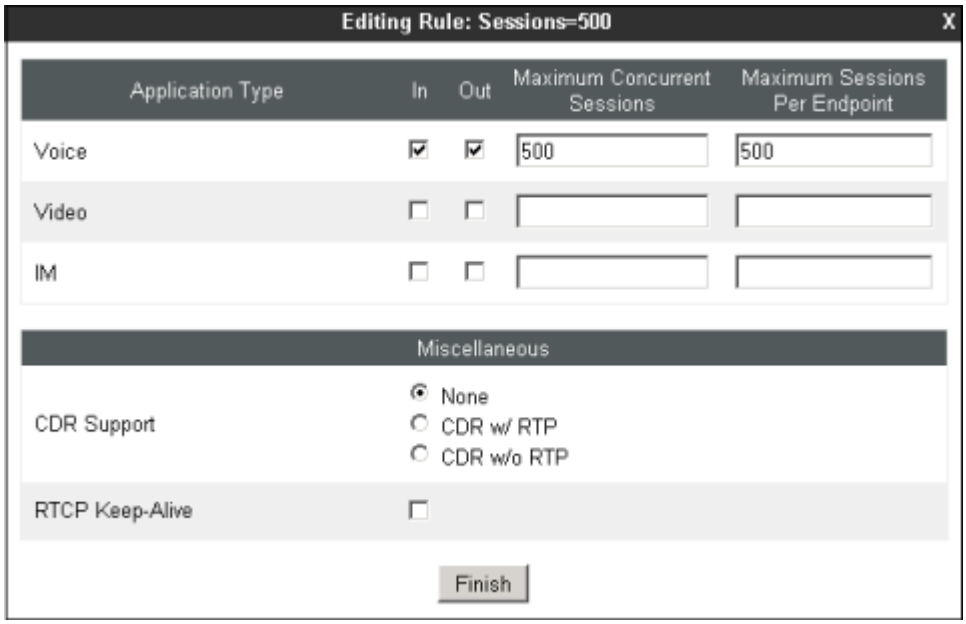


Under **Clone Name** enter the new rule name. Click **Finish** to save.



©2014 Avaya Inc. All Rights Reserved.

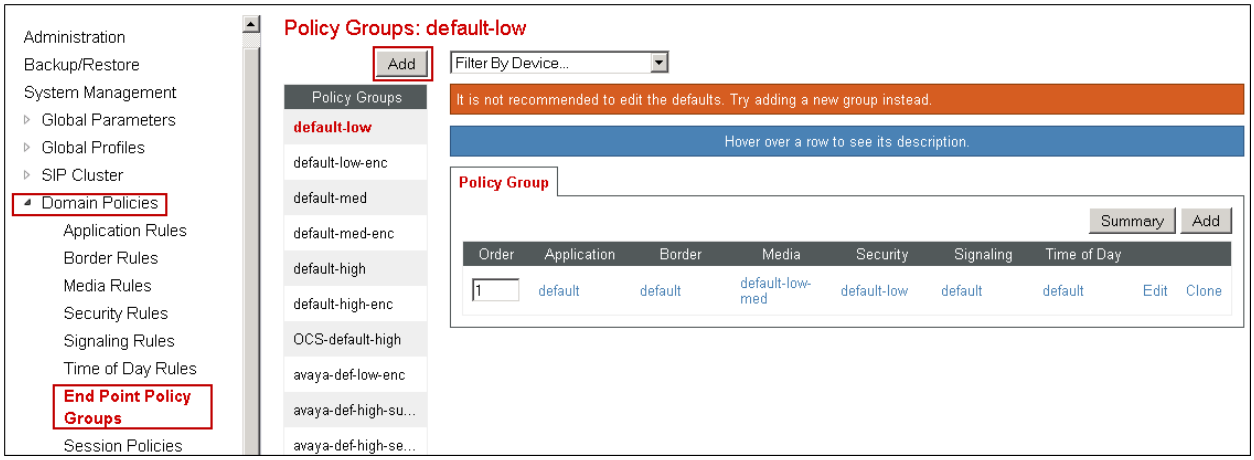
On the Application Rules screen, select the newly created rule and click **Edit** (not shown). For SIP trunking, **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** should have the same value. In the example below, they are set to ***500***, which is the number of maximum simultaneous 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.

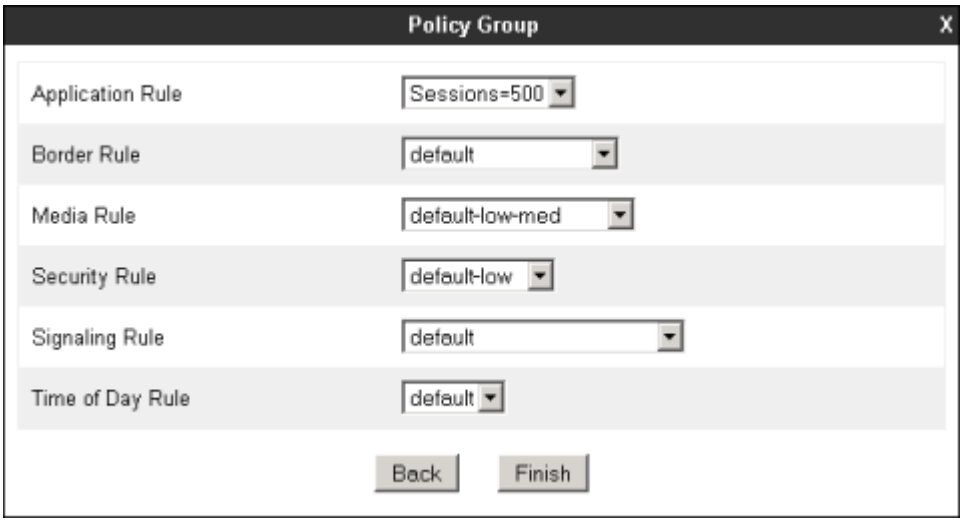
To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu. Select **Add**.



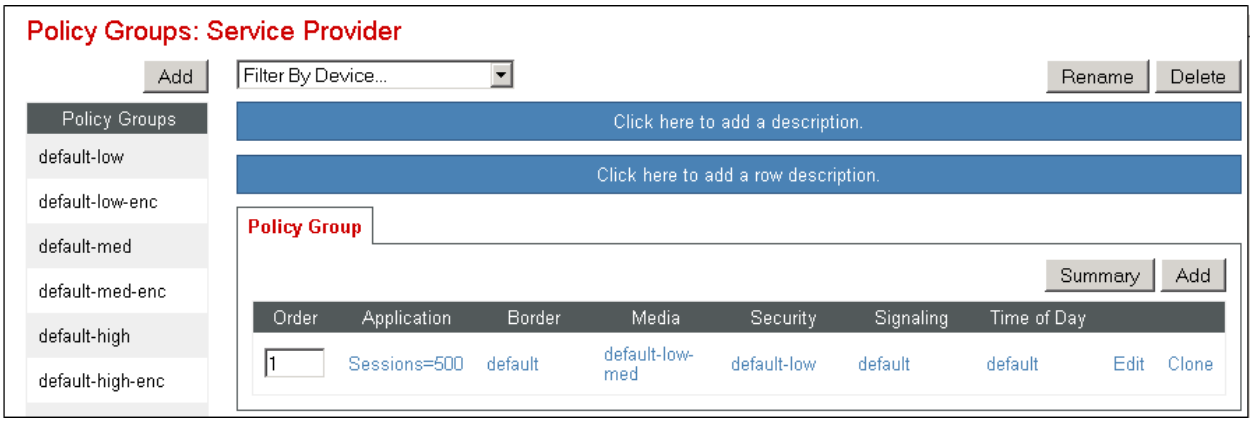
©2014 Avaya Inc. All Rights Reserved.

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.



©2014 Avaya Inc. All Rights Reserved.

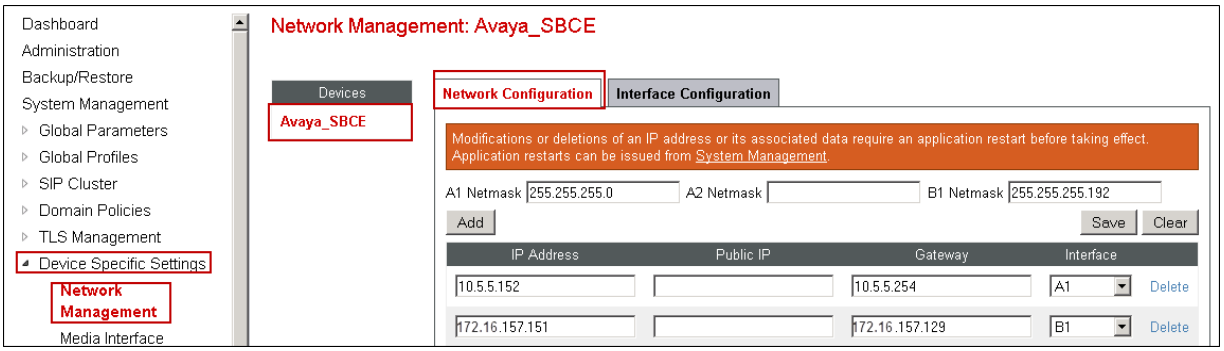
6.5. Device Specific Settings

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

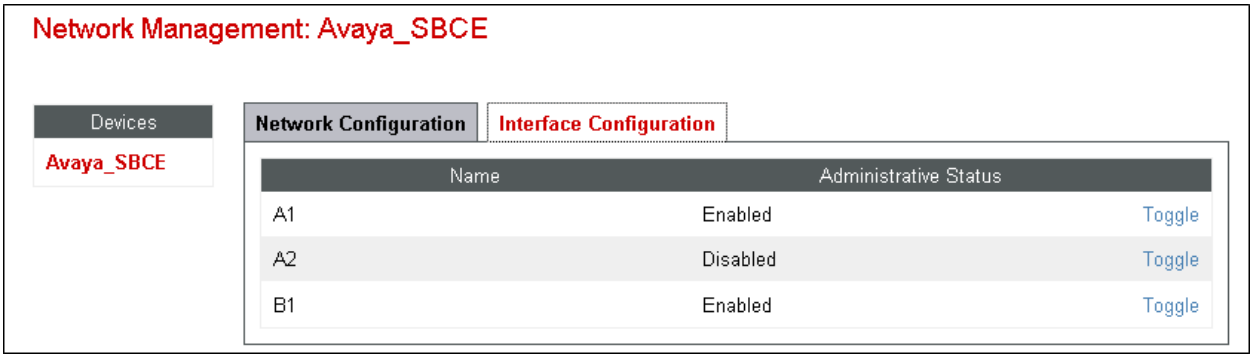
6.5.1. Network Management

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

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



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

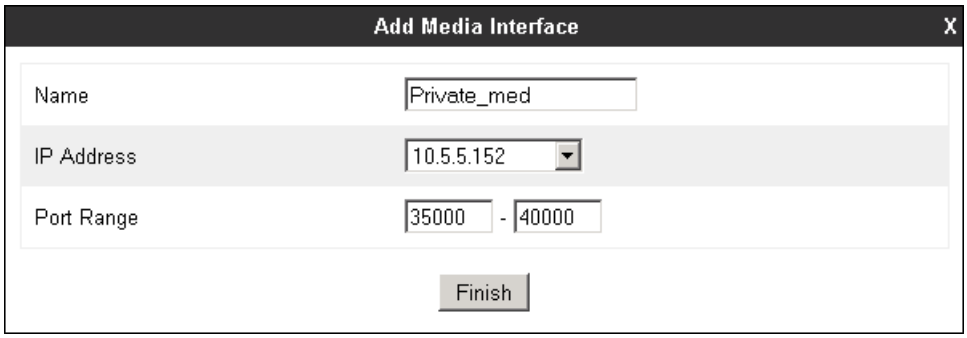


©2014 Avaya Inc. All Rights Reserved.

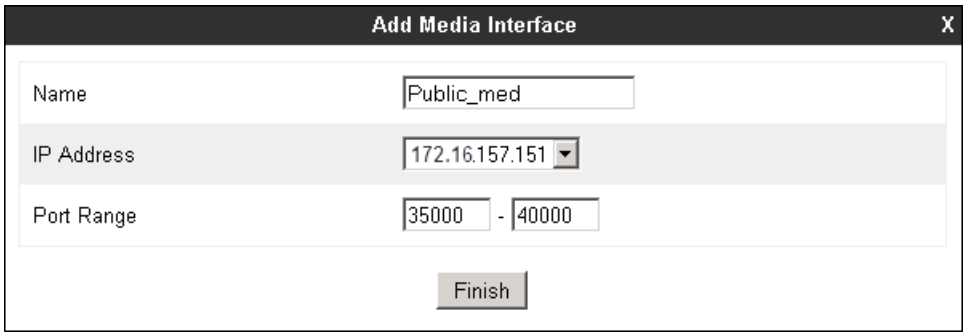
6.5.2. Media Interface

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

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

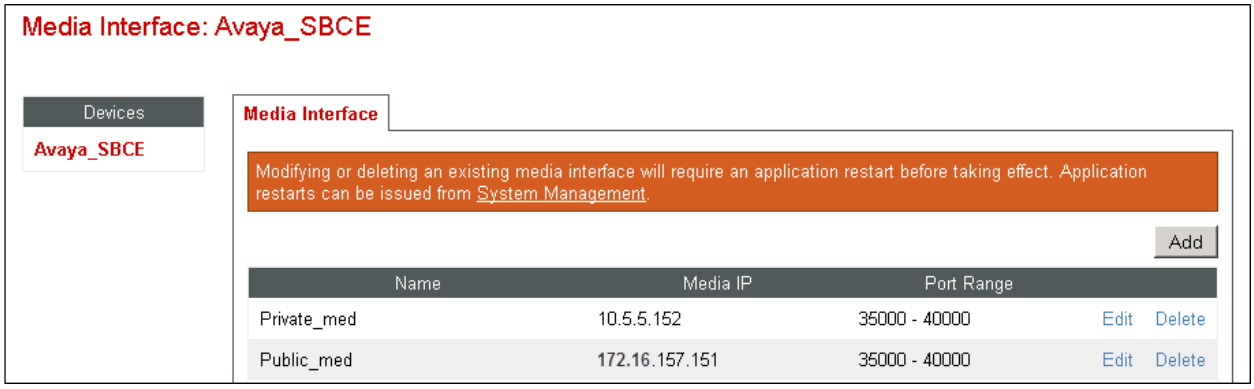


A second Media Interface facing the public network side was similarly created with the name **Public_med**, as shown below. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. The **Port Range** was left at the default values.



©2014 Avaya Inc. All Rights Reserved.

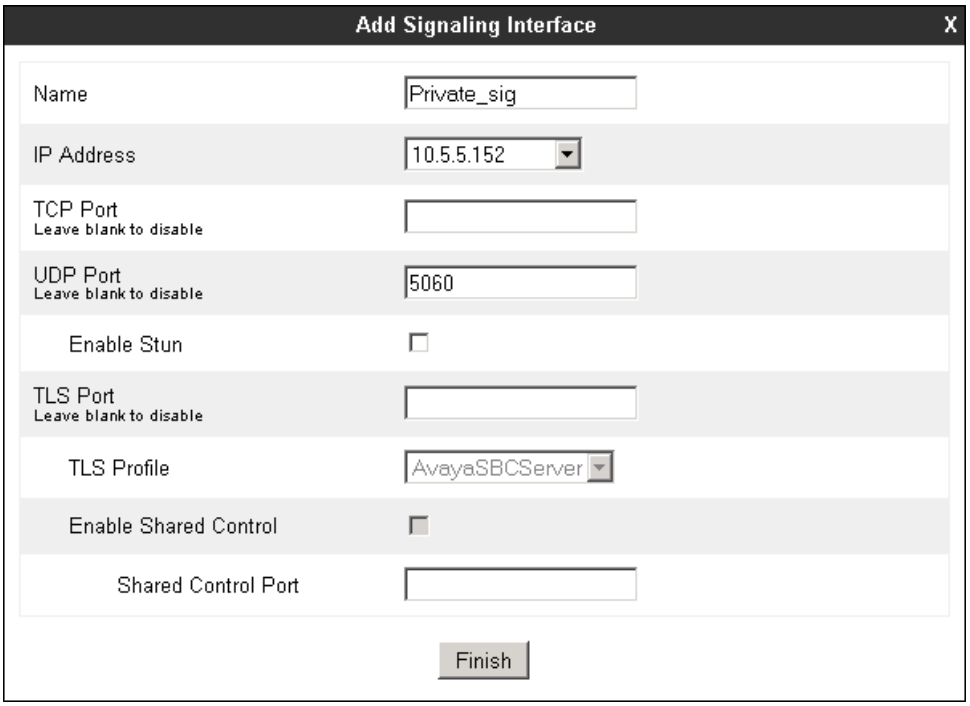
Once the configuration is complete, the **Media Interface** screen will appear as follows.



6.5.3. Signaling Interface

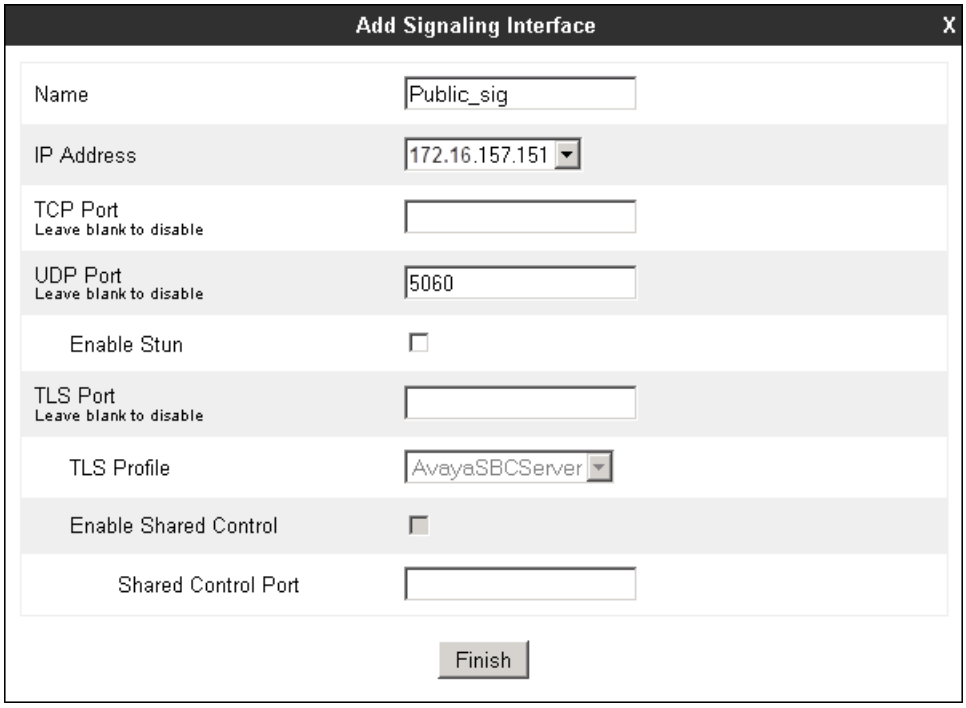
Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in both the inside and outside networks.

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 to listen for signaling traffic from the IP Office in the sample configuration. Click **Finish**.

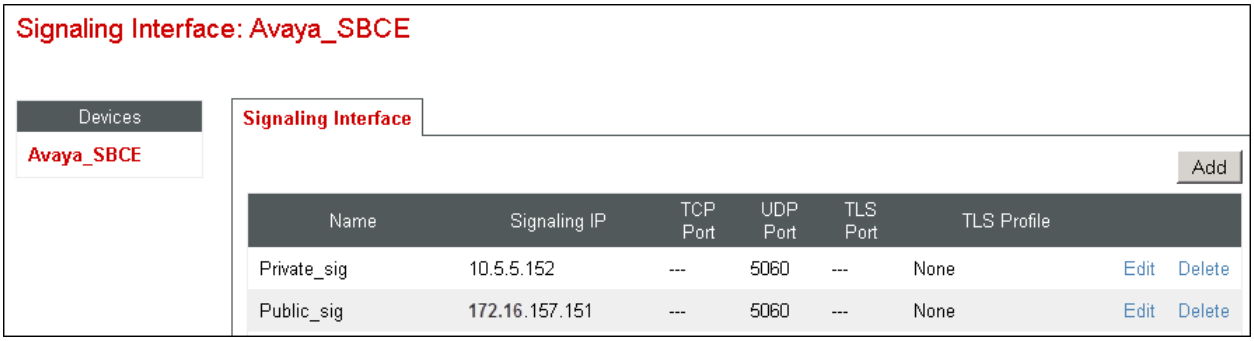


©2014 Avaya Inc. All Rights Reserved.

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



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

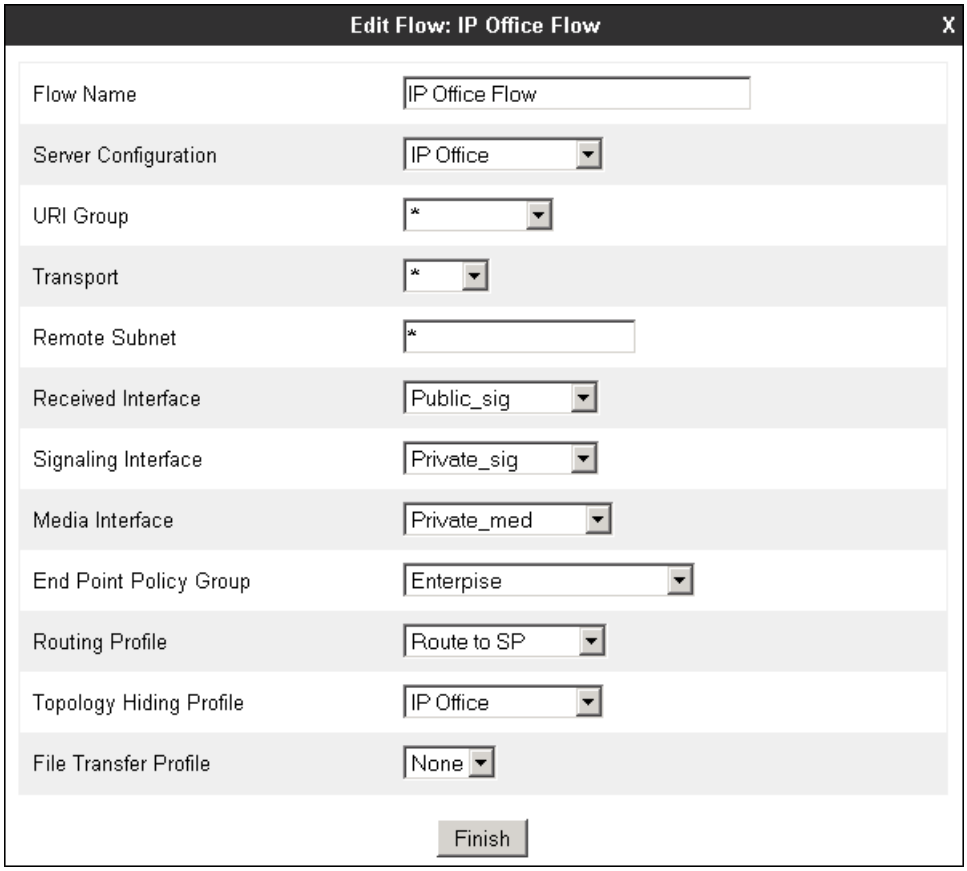


©2014 Avaya Inc. All Rights Reserved.

6.5.4. End Point Flows

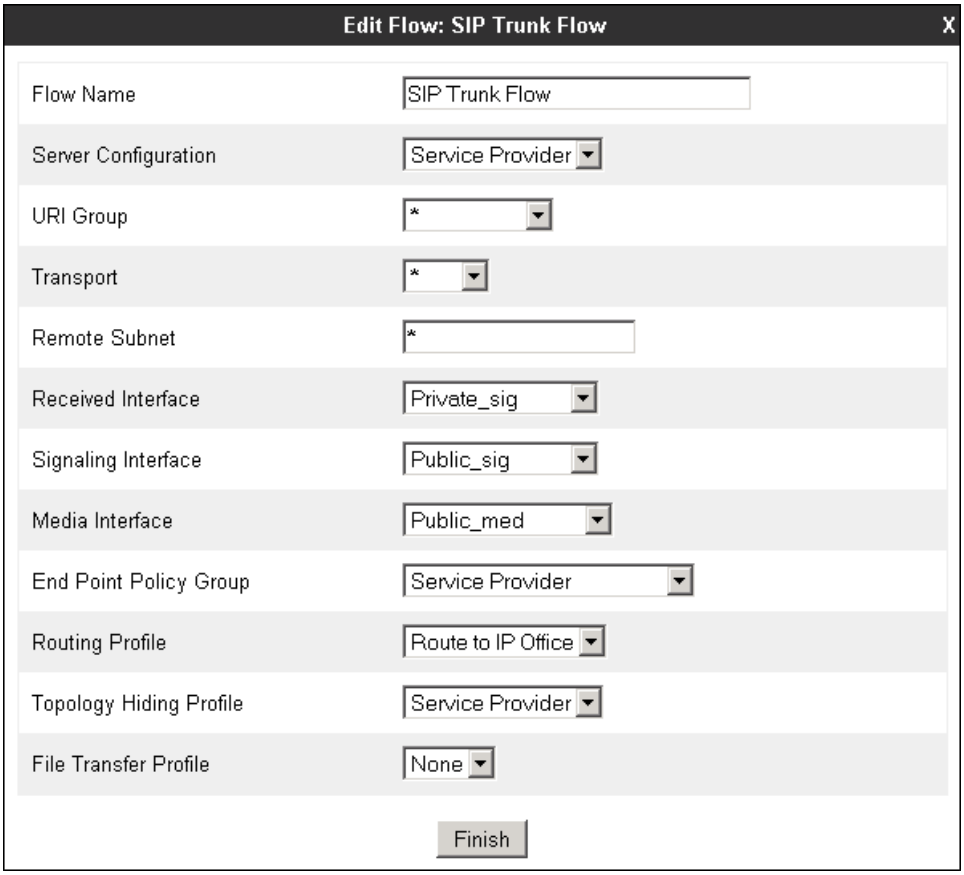
End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

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**.

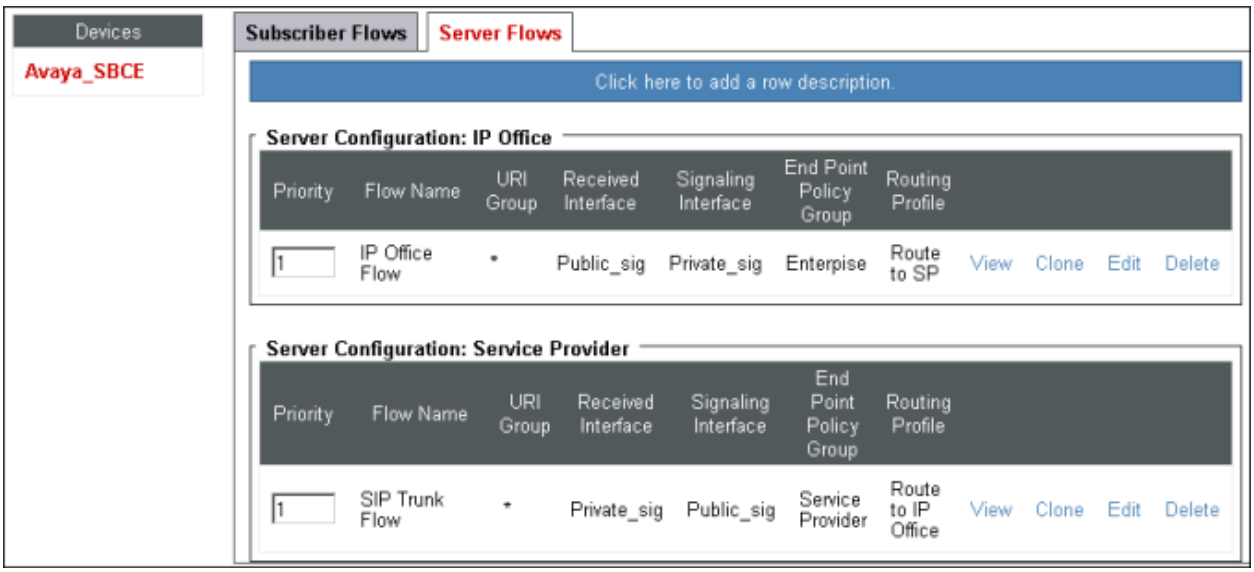


©2014 Avaya Inc. All Rights Reserved.

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.



©2014 Avaya Inc. All Rights Reserved.

7. Alestra Enlace IP SIP Trunking Configuration

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

- IP address of the Alestra 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

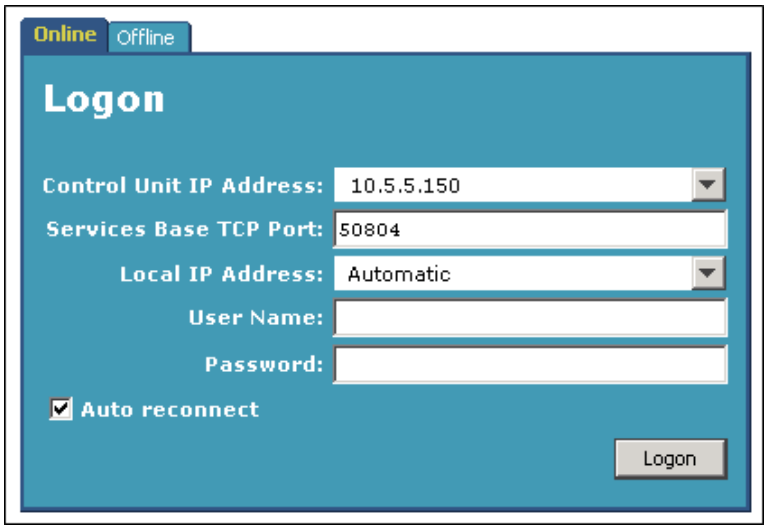
The following sections include steps that may be used to verify the configuration of the IP Office and the Avaya SBCE with the Alestra Enlace IP SIP Trunk Service.

8.1. Avaya IP Office

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

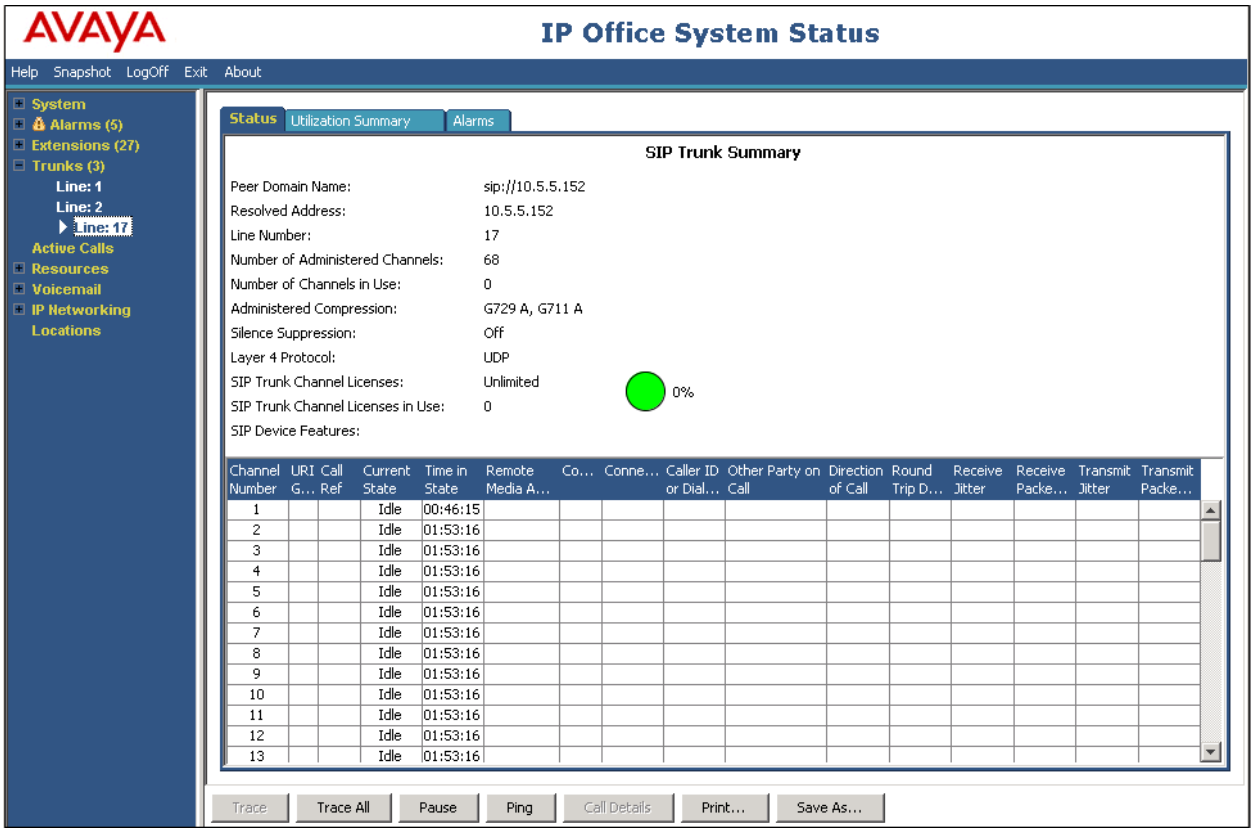
8.1.1. System Status

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

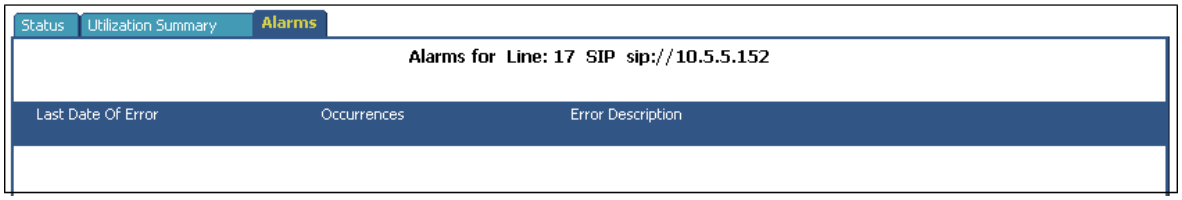


©2014 Avaya Inc. All Rights Reserved.

Select the SIP line of interest from the left pane (**Line 17** in the reference configuration). On the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).



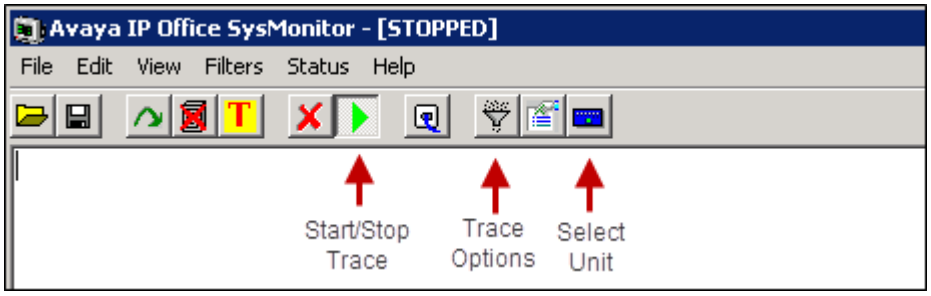
- **Select** the **Alarms** tab and verify that no alarms are active on the SIP line.



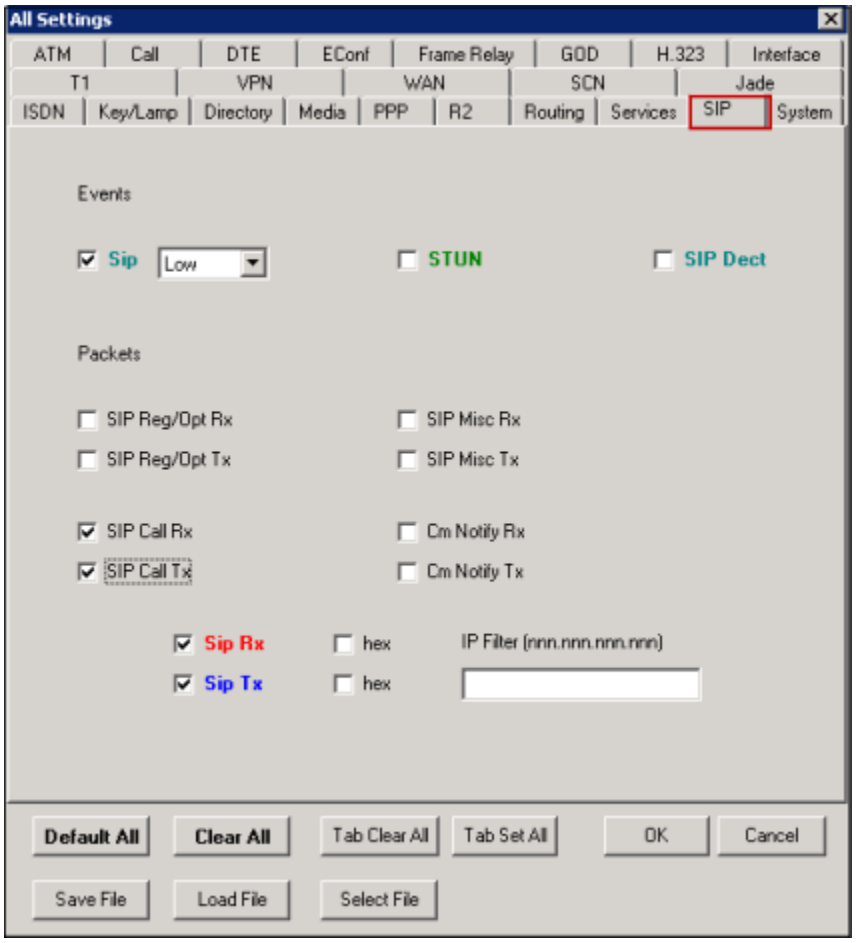
©2014 Avaya Inc. All Rights Reserved.

8.1.2. Monitor

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

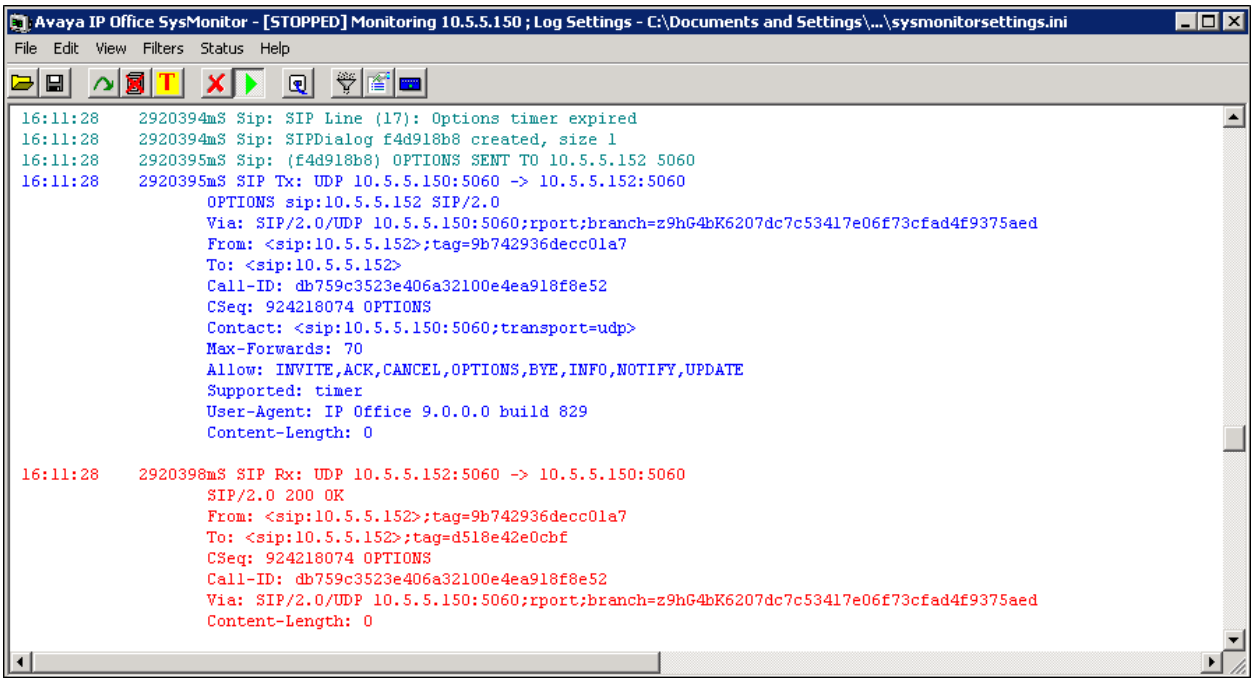


Clicking the **Trace Options** icon on the taskbar and selecting the **SIP** tab allows to modify the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type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



©2014 Avaya Inc. All Rights Reserved.

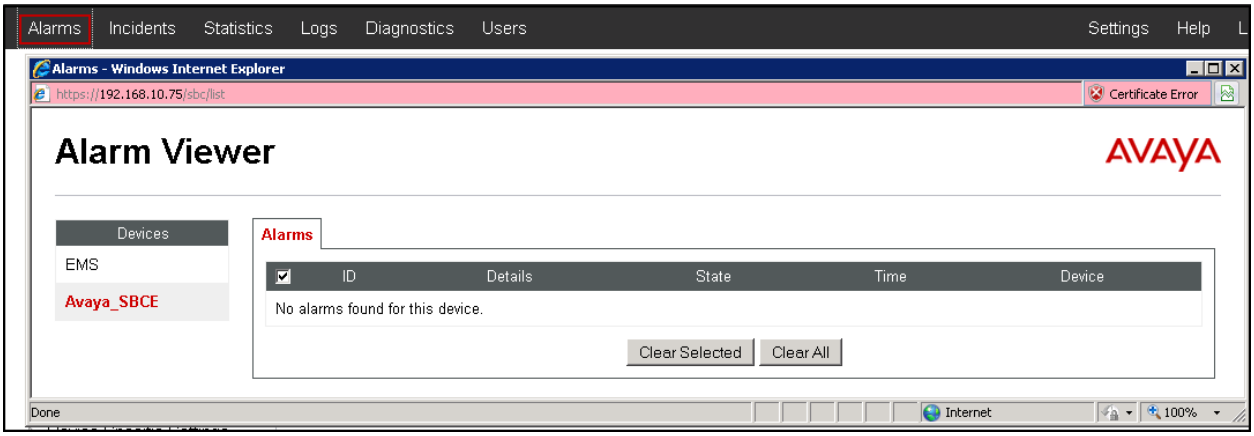
The sample screen below shows an outbound OPTIONS message and the 200 OK response from the service provider, received via the Avaya SBCE.



8.2. Avaya Session Border Controller for Enterprise

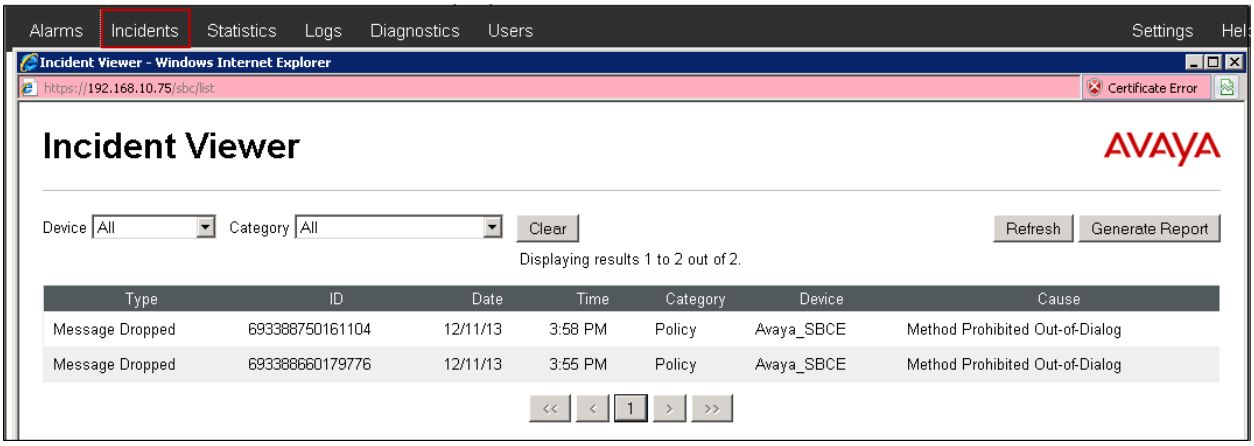
There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

Alarms: Provides information about the health of the SBC.

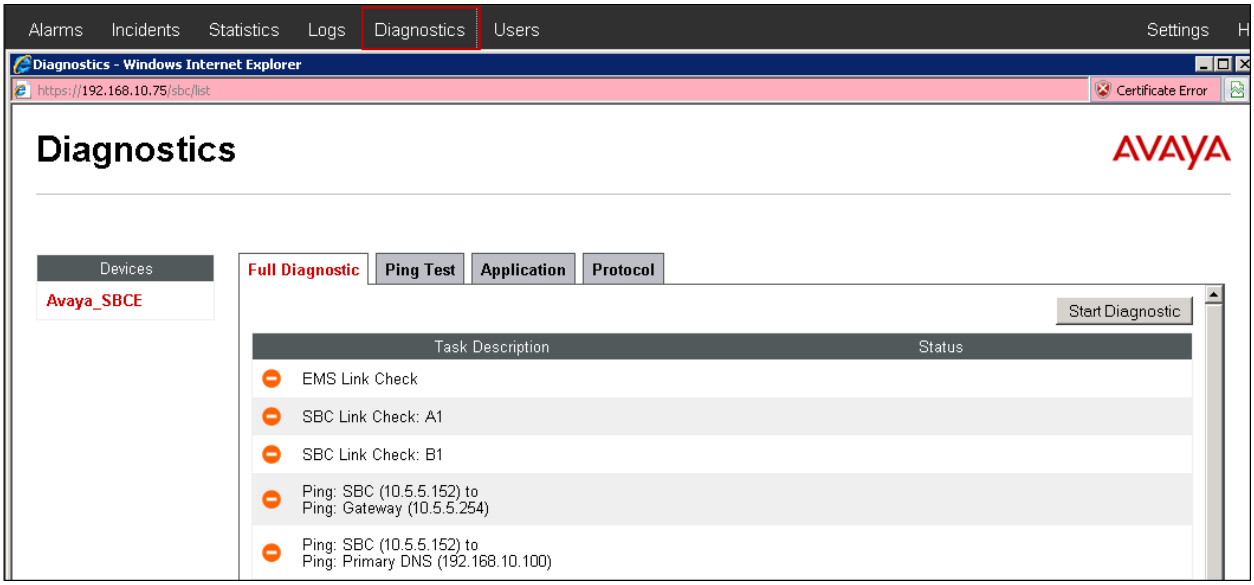


©2014 Avaya Inc. All Rights Reserved.

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

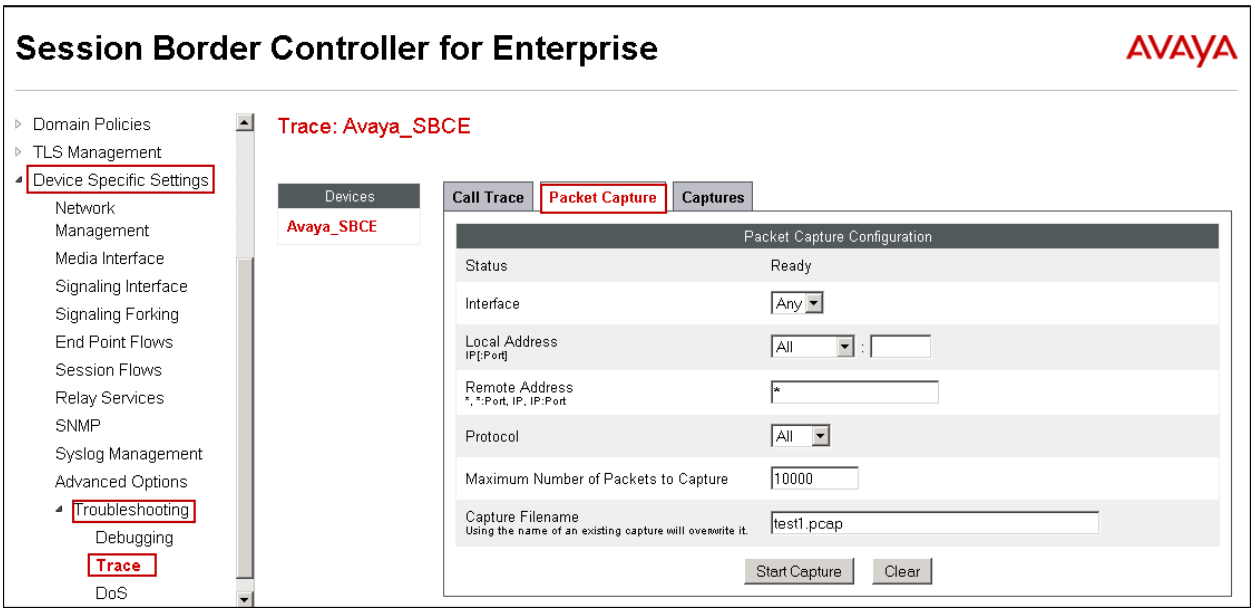


Diagnostics: This screen provides a variety of tools to test and troubleshoot the SBC network connectivity.

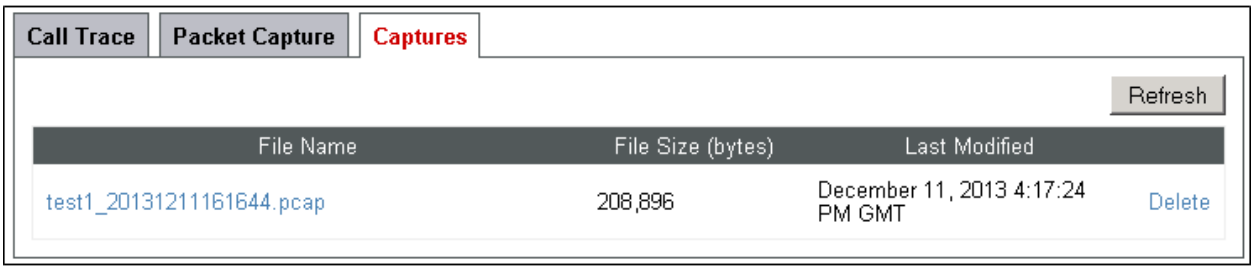


©2014 Avaya Inc. All Rights Reserved.

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.



©2014 Avaya Inc. All Rights Reserved.

9. Conclusion

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

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

10. Additional References

[1] *Avaya IP Office 9.0, Installing IP500/IP500* V2. Document 15-601042, November 2013
https://downloads.avaya.com/css/P8/documents/100174004

[2] *Avaya IP Office Manager Release 9.0,* Document 15-601011, September 2013
https://downloads.avaya.com/css/P8/documents/100174478

[3] *Administering Avaya Flare® Experience for IPad devices and Windows, Release 9.0*, September 2013
https://downloads.avaya.com/css/P8/documents/100175132

[4] *IP Office System Status Application*, Document Number 15-601758, November 2012
https://downloads.avaya.com/css/P8/documents/100150298

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

[6] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013
https://downloads.avaya.com/css/P8/documents/100168983

[7] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, May 2013
https://downloads.avaya.com/css/P8/documents/100168982

[8] *Avaya Session Border Controller for Enterprise Release Notes.* Release 6.2, June 2013
https://downloads.avaya.com/css/P8/documents/100170131

[9] *Configuring the Avaya Session Border Controller for IP Office Remote Workers*, September 2013.
https://downloads.avaya.com/css/P8/documents/100177106

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

©2014 Avaya Inc. All Rights Reserved.

Appendix: SIP Line Template

IP Office Release 9.0 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.

The SIP Line Template created from the configuration as documented in these Application Notes is as follows:


```
 <?xml version="1.0" encoding="utf-8" ?>
<Template xmlns="urn:SIPTrunk-schema">
 <TemplateType>SIPTrunk</TemplateType>
 <Version>20131212</Version>
 <SystemLocale>enu</SystemLocale>
 <DescriptiveName>Alestra (with SBCE)</DescriptiveName>
 <ITSPDomainName>10.5.5.152</ITSPDomainName>
 <SendCallerID>CallerIDRPID</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>UpdateAuto</UpdateSupport>
 <URIType>SIPURI</URIType>
 <UserAgentServerHeader />
 <CallerIDfromFromheader>false</CallerIDfromFromheader>
 <PerformUserLevelPrivacy>false</PerformUserLevelPrivacy>
 <ITSPProxy>10.5.5.152</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>
```

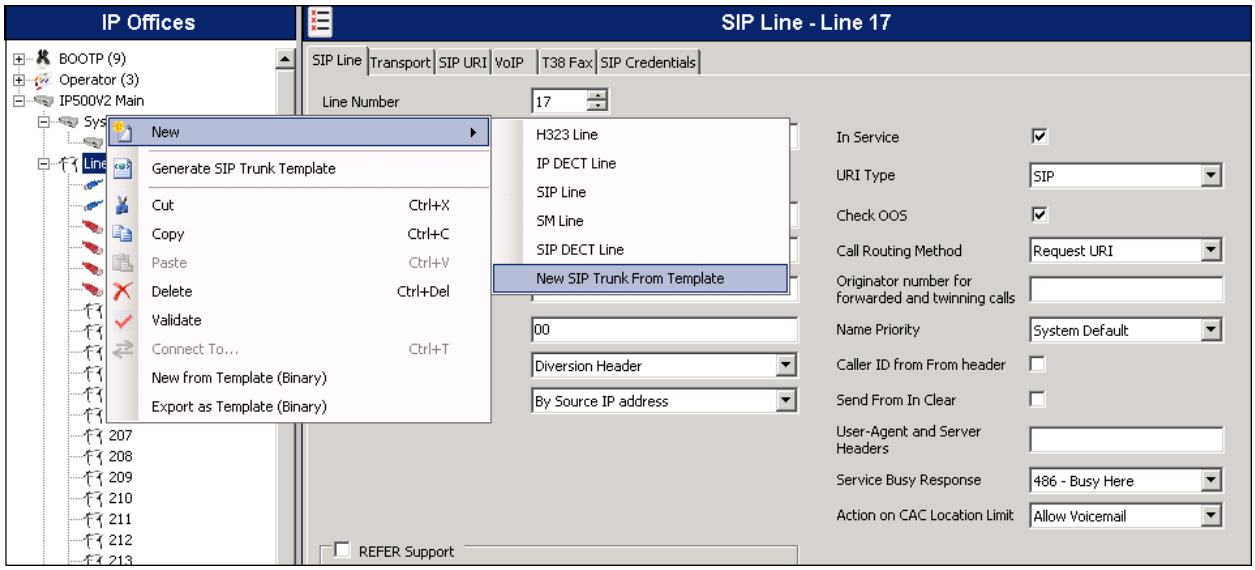

©2014 Avaya Inc. All Rights Reserved.

<AdvCodecPref>**G.729(a) 8K CS-ACELP,G.711 ALAW 64K**</AdvCodecPref>
<CallInitiationTimeout>**4**</CallInitiationTimeout>
<DTMFSupport>**DTMF_SUPPORT_RFC2833**</DTMFSupport>
<VoipSilenceSupression>**false**</VoipSilenceSupression>
<ReinviteSupported>**true**</ReinviteSupported>
<FaxTransportSupport>**FOIP_G711**</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>

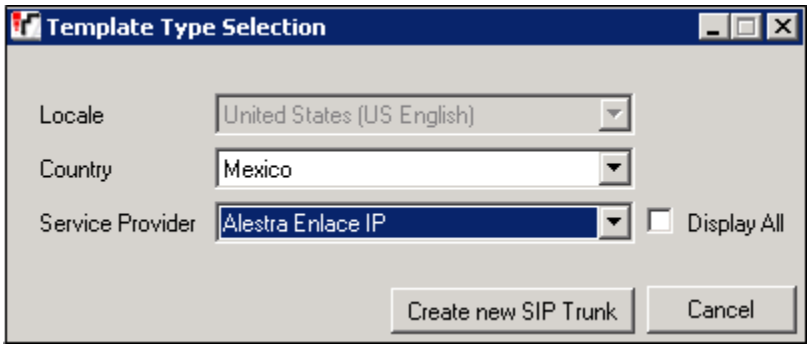
©2014 Avaya Inc. All Rights Reserved.

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

Next, import the template into the new IP Office 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.



©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 DevConnect Program at devconnect@avaya.com.