Avaya Solution & Interoperability Test Lab

Application Notes for ThinkTel SIP Trunking Service with Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring ThinkTel Session Initiation Protocol (SIP) Trunking Service with Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise Release 6.2.

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

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

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between service provider ThinkTel and Avaya IP Office solution. In the sample configuration, Avaya IP Office solution consists of Avaya IP Office (IP Office) Release 8.1, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2 and various Avaya endpoints.

ThinkTel SIP Trunking Service (ThinkTel) referenced within these Application Notes is designed for business customers. This service enables PSTN calling via a broadband WAN connection using SIP protocol. This converged network solution is a cost effective alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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

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

2.1 Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types including H.323, SIP, digital and analog telephones at the enterprise. All incoming calls from PSTN were routed to the enterprise across the SIP Trunk from service provider.
- Outgoing PSTN calls from various phone types including SIP, H.323, digital and analog telephone at the enterprise. All outgoing calls to PSTN were routed from the enterprise across the SIP Trunk to service provider.
- Incoming and outgoing PSTN calls to/from Avaya IP Office softphone using both SIP and H.323 protocols.
- Dialing plans including local, long distance, outgoing and incoming toll-free calls, local directory assistance (411), etc.
- Calling Party Name presentation and Calling Party Name restriction (using the "P-Preferred-Identity" header).
- Proper codec negotiation with G.711MU and G.729 codecs.
- Proper early media transmissions G.711MU and G.729 codecs.
- Proper media transmission using G.711MU and G.729 codecs.
- Incoming and outgoing fax over IP using G.711MU codec.
- DTMF tone transmissions as out-of-band RTP event per RFC 2833.
- Voicemail navigation for incoming and outgoing calls.

- Telephony features such as hold and resume, call transfer, call forward and conferencing.
- Off-net call transfer using re-INVITE method.
- Off-net call forward using Diversion method.
- Mobility Twinning incoming calls to mobile phones using Diversion method.
- Dynamic SIP Trunk registration using REGISTER method.
- Response to OPTIONS heartbeat.
- Session Timer refresh per RFC 4028.
- Response to incomplete call attempts and trunk errors.

Items that are not supported by ThinkTel or not part of the compliance testing because ThinkTel has not provided the necessary configuration, are listed as follows:

- Outgoing emergency (E911), operator and operator assisted calls are not supported.
- T.38 fax is not supported.
- Off-net call transfer using REFER method is not supported.
- Off-net call forward using History-Info method is not supported.

2.2 Test Results

Interoperability testing of ThinkTel with Avaya IP Office solution was successfully completed with the exception of the observations/limitations described below.

1. **For outgoing calls**, **ThinkTel is now blocking Calling Party Name**. Configuring an IP Office station with any Calling Party Name for outgoing calls, ThinkTel transmitted original Calling Party Name to the called PSTN party without any modification. This is not expected because display information from the enterprise is not trusted and it should be examined by service provider. This issue has been fixed by ThinkTel to restrict Calling Party Name from being sent to PSTN.

2. **For outgoing calls**, **ThinkTel is now overriding Calling Party Number by a pilot number if original Calling Party Number is not a subscribed DID number**. Configuring an IP Office station with any Calling Party Number different than the subscribed DID numbers for outgoing calls, ThinkTel transmitted original Calling Party Number to the called PSTN party without any modification. This is not expected because display information from the enterprise is not trusted and it should be examined by service provider. This issue has been fixed by ThinkTel to override Calling Party Number by a pilot number if original Calling Party Number is not a subscribed DID number. **Note**: If outgoing calls from a subscribed DID number, original Calling Party Number will be sent to PSTN.

3. **Calling Party Name and Number are not updated if IP Office off-net redirects (by transferring or forwarding) an incoming or outgoing call back to PSTN**. Before and after completing the off-net redirection, IP Office did not send UPDATE or re-INVITE signaling to update the call display on PSTN parties. This is a known behavior of IP Office with no available resolution at this time. This issue has low user impact, and it is listed here simply as an observation.

4. **Calling Party Name and Number are not updated if IP Office off-net redirects (by transferring or forwarding) an incoming or outgoing call to internal station**. Before and

after completing the local redirection to internal station, IP Office did not send UPDATE or re-INVITE signaling to update the call display on PSTN party. This is a known behavior of IP Office with no available resolution at this time. This issue has low user impact, and it is listed here simply as an observation.

5. **For off-net call forward or Mobility Twinning calls**, **Calling Party Number is now corrected**. In order to perform off-net call forward, IP Office sent initial INVITE on the 2nd leg with the "Diversion" containing a subscribed DID number to support call authentication done by service provider. The same DID number has also been sent in the "P-Asserted-Identity" header, this caused the forwarded PSTN party to unexpectedly display DID number of IP Office station instead of displaying Calling Party Number of the originating PSTN party in the "From" header. This issue has been corrected by removing support for the "P-Asserted-Identity" header on IP Office. As a result, IP Office does not send the "P-Asserted-Identity" header in the signaling to service provider. This workaround assists service provider to transmit proper display info which is presented in the "From" header. For more information, refer to **Section** Error! Reference source not found.. This is a known behavior of IP Office with no available resolution at this time. This issue has low user impact, it is listed here simply as an observation. **Note**: Disabling the "P-Asserted-Identity" header on the SIP Trunk, IP Office will use the "P-Preferred-Identity" header for outgoing private calls to provide necessary information for call authentication done by service provider and the calls appeared to work well.

6. **G.711MU codec is preferred for fax over IP because T.38 fax is not fully working**. For incoming and outgoing fax calls using T.38, sometimes ThinkTel sent re-INVITE(T.38) to change the media from voice to fax for the successful fax calls. But at the other times, it did not. The issue seemed to depend on the type of PSTN fax terminal and POTS line. Thus, G.711MU codec was recommended for fax calls because T.38 fax appeared not to function fully. During the compliance testing, incoming and outgoing faxes using G.711MU codec were successfully transmitted with acceptable quality. This is a known behavior on ThinkTel SIP Trunking Service with no available resolution at this time. For detailed configuration, refer to **Section 5.5.4**.

2.3 Support

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

For technical support on ThinkTel SIP Trunking Service, contact ThinkTel technical support at:

- Phone: 1 (866) 928-4465
- Email: support@thinktel.ca
- Website: http://support.thinktel.ca/

3. Reference Configuration

Figure 1 on the next page illustrates the test configuration. It shows an enterprise site connected to the ThinkTel networks through the Internet.

For confidentiality and privacy purposes, actual public IP address and PSTN routable phone number used in the certification testing have been replaced with fictitious parameters throughout the Application Notes.

The Avaya components used to create the simulated customer site including:

- Avaya IP Office v500v2
- Avaya Session Border Controller for Enterprise
- Avaya Voicemail Pro for IP Office
- Avaya 9600 Series H.323 IP Telephones
- Avaya 11x0 Series SIP IP Telephones
- Avaya IP Office Softphones (SIP and H.323 modes)
- Avaya 1408D Digital Telephones
- Avaya Symphony 2000 Analog Telephones

Located at the enterprise site is Avaya IP Office 500v2 with the MOD DGTL STA16 expansion to provide connection for 16 digital stations, the PHONE 8 module to provide connection for 8 analog stations and the 64-channel Voice Compression Module (VCM) for supporting VoIP codec. The IP Office LAN port connects to internal interface of Avaya SBCE across the enterprise network. On public side, external interface of Avaya SBCE connects to ThinkTel networks via the internet.

Mobility Twinning was configured for some IP Office users so that incoming calls to these user phones can also be delivered to configured mobile phones.

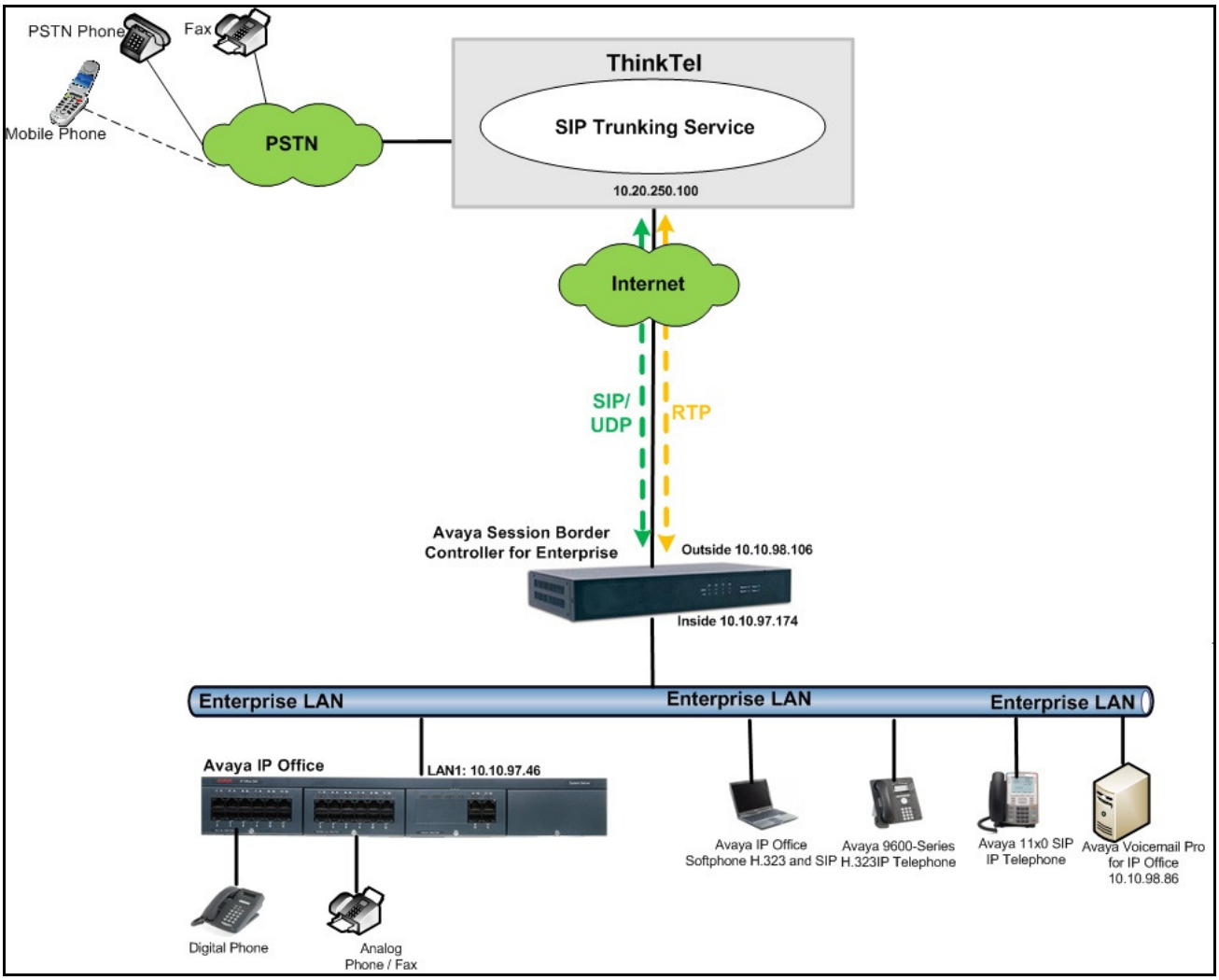


Figure 1: Avaya IP Telephony Network Connecting to ThinkTel SIP Trunking Service.

For the compliance testing, ThinkTel provided the service provider public SIP domain as its Application Server (AS) IP address **10.20.161.101** and the enterprise public SIP domain as the Avaya SBCE external IP address **10.10.98.106**. These public SIP domains will be used for public SIP traffic between ThinkTel and Avaya SBCE using transport protocol UDP. **Note**: The service provider public SIP domain **10.20.161.101** was obtained from ThinkTel per SIP Trunk basis and it is different fromservice provider Session Border IP address **10.20.250.100** as shown in Figure 1.

For outgoing calls, IP Office sent either 10 or 11 digits in destination headers, e.g., "Request-URI" and "To", and sent 10 digits in source headers, e.g., "From", "Contact", and "P-Preferred-Identity". For incoming calls, ThinkTel sent 10 digits in both destination headers.

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

4. Equipment and Software Validated

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

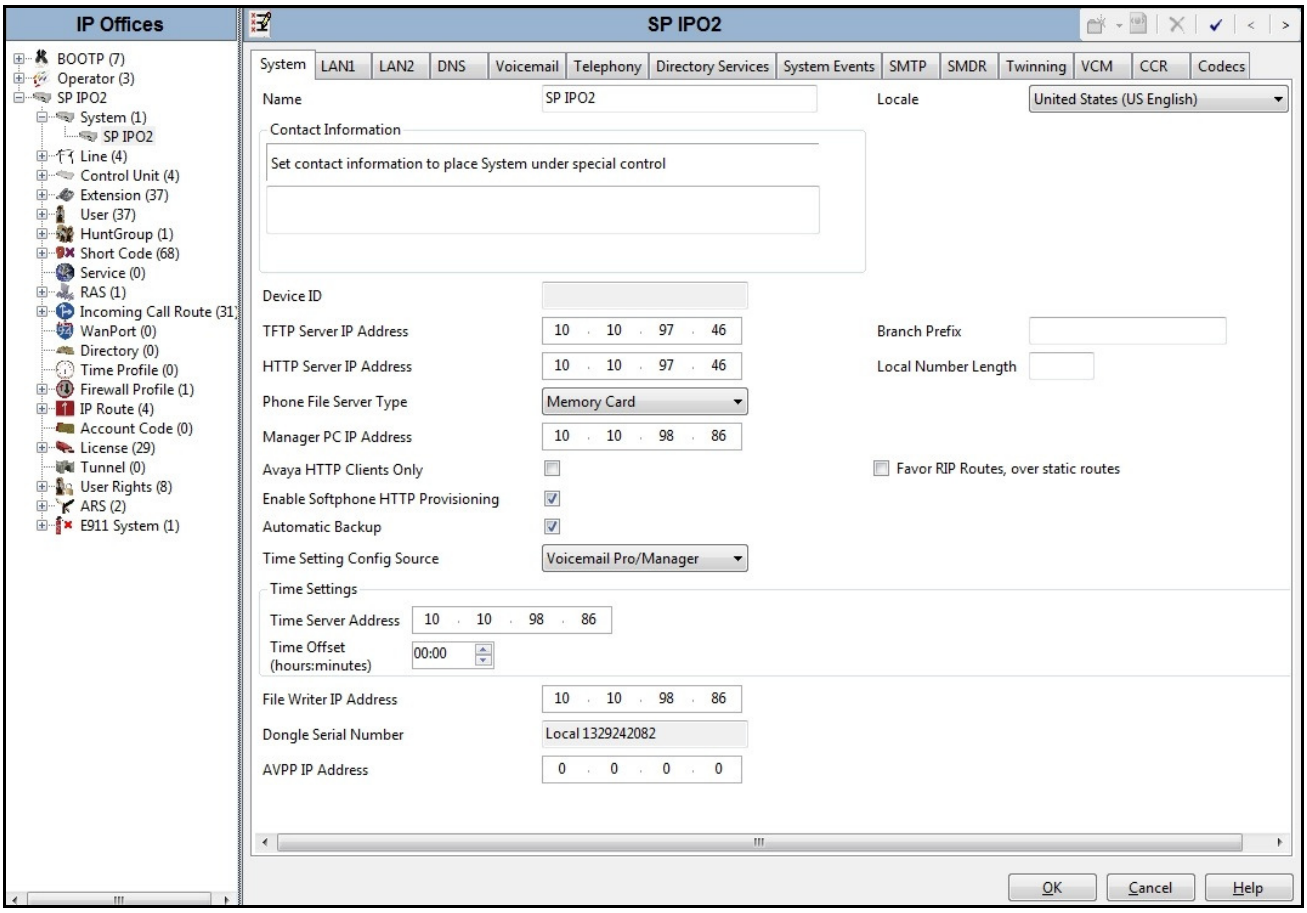
Avaya Telephony Components	
Equipment/Software	**Release/Version**
Avaya IP Office 500v2	8.1 (69)
Avaya IP Office DIG DCP*16 V2	8.1 (69)
Avaya IP Office Ext Card Phone 8	8.1
Avaya IP Office Manager	10.1 (69)
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2 (6.2.0 Q30)
Avaya Voicemail Pro for IP Office	8.1.9203.0
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.0.1
Avaya 11x0 IP Telephone (SIP)	SIP11x0e04.03.12.00
Avaya IP Office Softphone	3.2.3.48 67009
Avaya Digital Telephones (1408D)	N/A
Avaya Symphony 2000 Analog Telephone	N/A

ThinkTel SIP Trunking Service Components	
Equipment/Software	**Release/Version**
Metaswitch	7.4
Opensips Session Border Controller	1.6.2

Testing was performed with IP Office 500v2 R8.1, but it also applies to IP Office Server Edition R8.1. Note that IP Office Server Edition requires an Expansion IP Office 500 v2 R8.1 to support analog or digital endpoints or trunks.

5. Configure IP Office

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

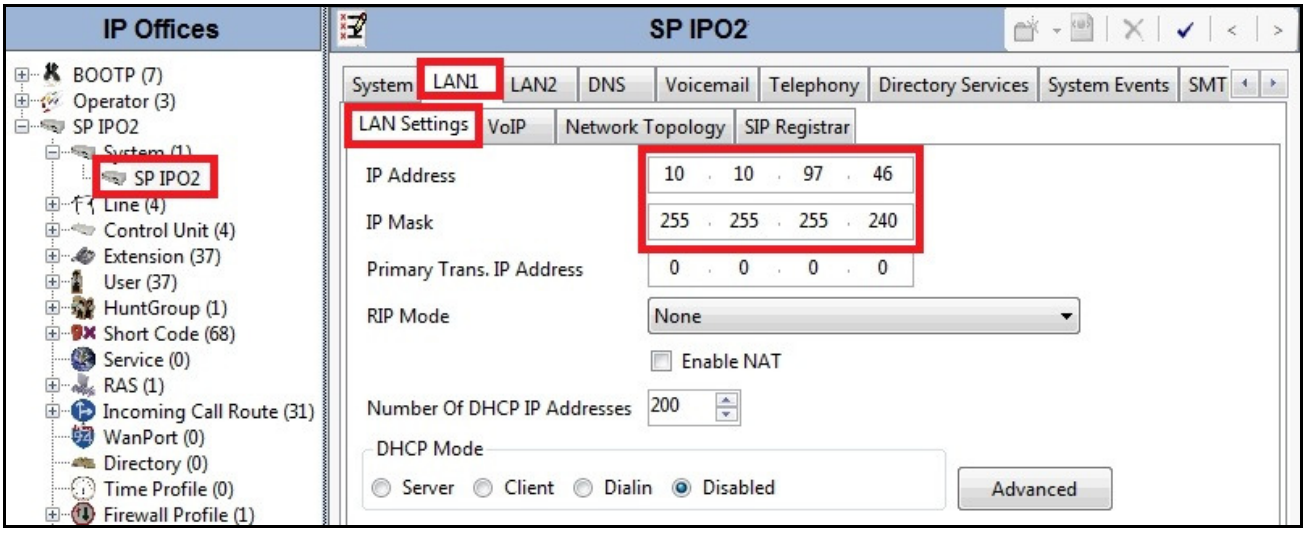


These Application Notes assume the basic installation and configuration have already been completed and are not discussed here. For further information on IP Office, please consult **References** in **Section 10**.

5.1 LAN

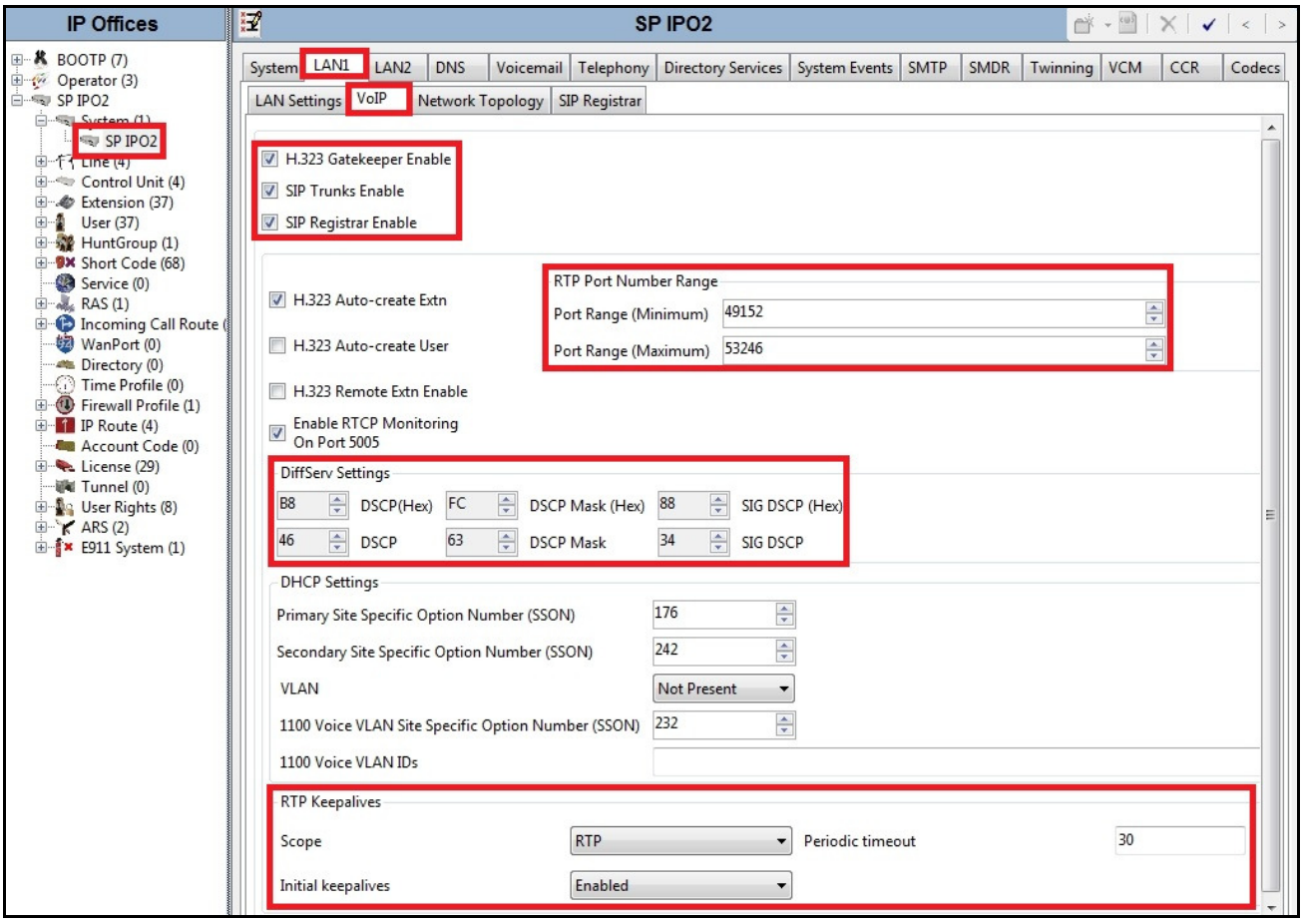
In the sample configuration, IP Office was configured with system name **SP IPO2** and the LAN port was used to connect to ThinkTel networks via Avaya SBCE. To access to **LAN1** settings that correspond to the LAN port on IP Office, navigate to **System (1) → SP IPO2** in the Navigation Pane then in the Details Pane navigate to **LAN1→ LAN Settings** tab. **LAN1** settings for the compliance testing were configured with following parameters.

- Set **IP Address** field to LAN IP address, e.g., **10.10.97.46**.
- Set **IP Mask** field to subnet mask of public network, e.g., **255.255.255.240**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.



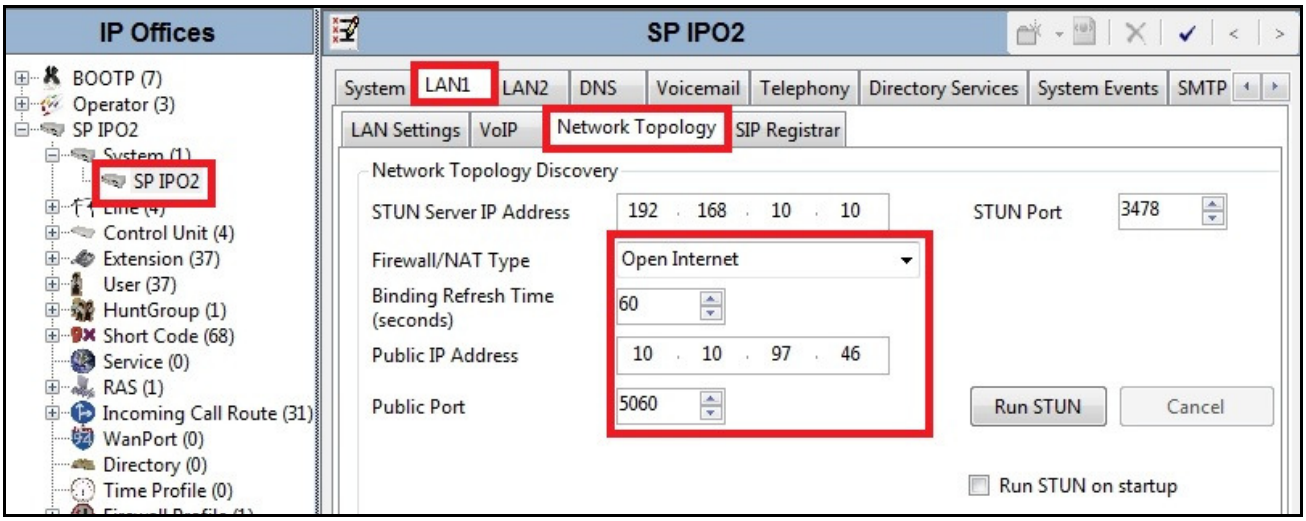
On **VoIP** tab as shown in the screenshot below, configure with following settings.

- Check **H323 Gatekeeper Enable** to allow Avaya IP telephones/ softphones using H.323 protocol to register.
- Check **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to ThinkTel.
- Check **SIP Registrar Enable** to allow Avaya IP telephones/ softphones to register using SIP protocol.
- Verify **RTP Port Number Range** settings for a specific range for RTP. **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- Verify **DiffServ Settings** were kept as default for Differentiated Services Code Point (DSCP) parameter in IP packet headers to support Quality of Services policies for both signaling and media. **DSCP** and **SIG DSCP** fields are the values defined for media and signaling appropriately.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.



Under **Network Topology** tab in the Details Pane, configure following parameters:

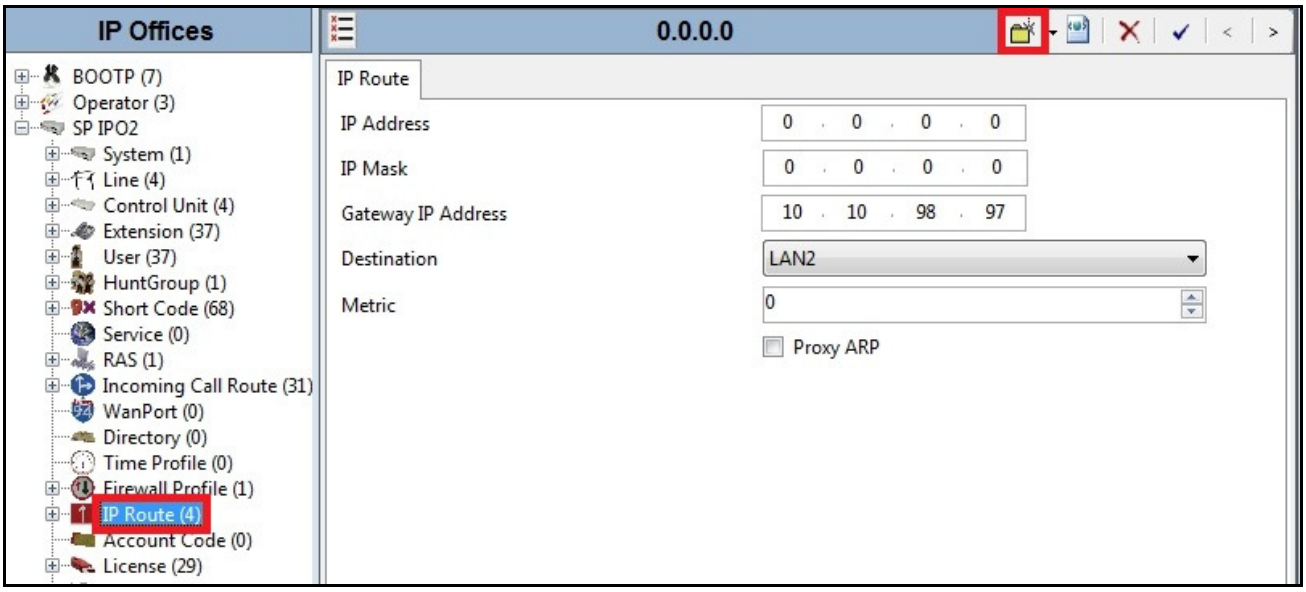
- Select **Firewall/NAT Type** from the pull-down menu that matches network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even the default STUN settings are populated but they will not be used.
- Set **Binding Refresh Time (seconds)** to **60**. This value is used to determine the frequency that IP Office will send OPTIONS heartbeat to service provider.
- Set **Public IP Address** to IP Office LAN IP address, e.g., **10.10.97.46**.
- Set **Public Port** was set to **5060**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.



5.2 IP Route

IP Route settings include IP Route **10.10.0.0** on LAN1 connecting to Avaya SBCE for SIP and RTP traffic to ThinkTel, and a second IP Route **10.33.0.0** on the same LAN1 connecting to private enterprise networks.

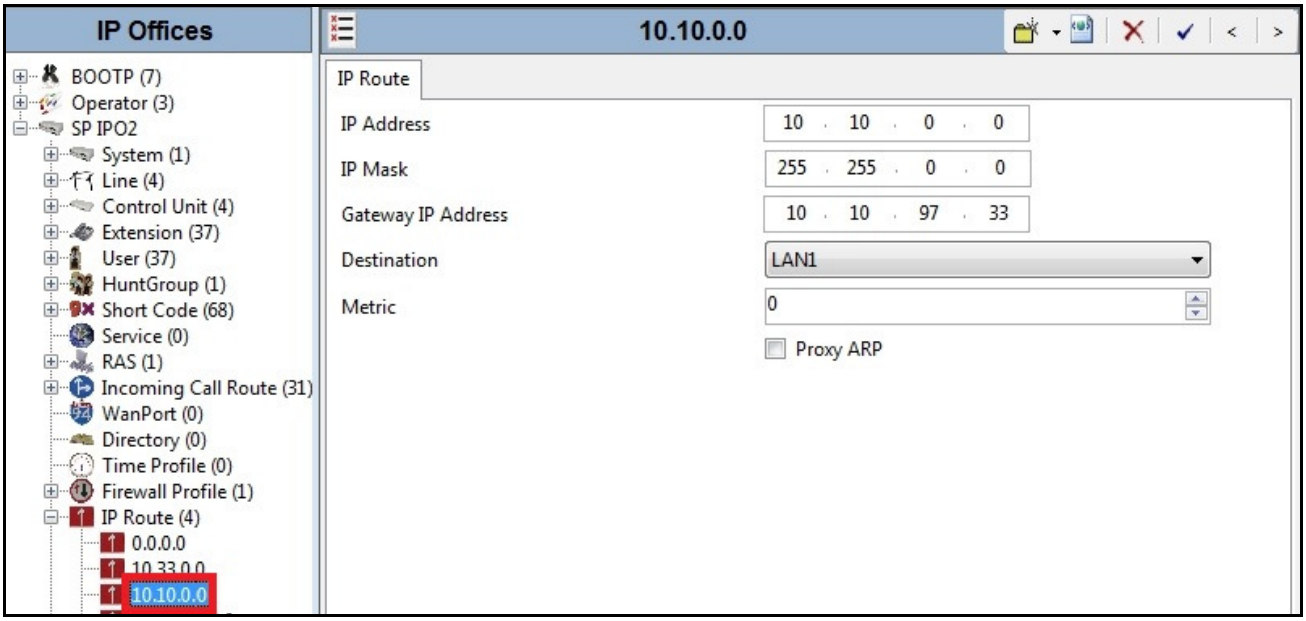
To create IP Route, select **IP Route** in the Navigation Pane then click "**Create a New Record**" icon as shown in the screenshot below.



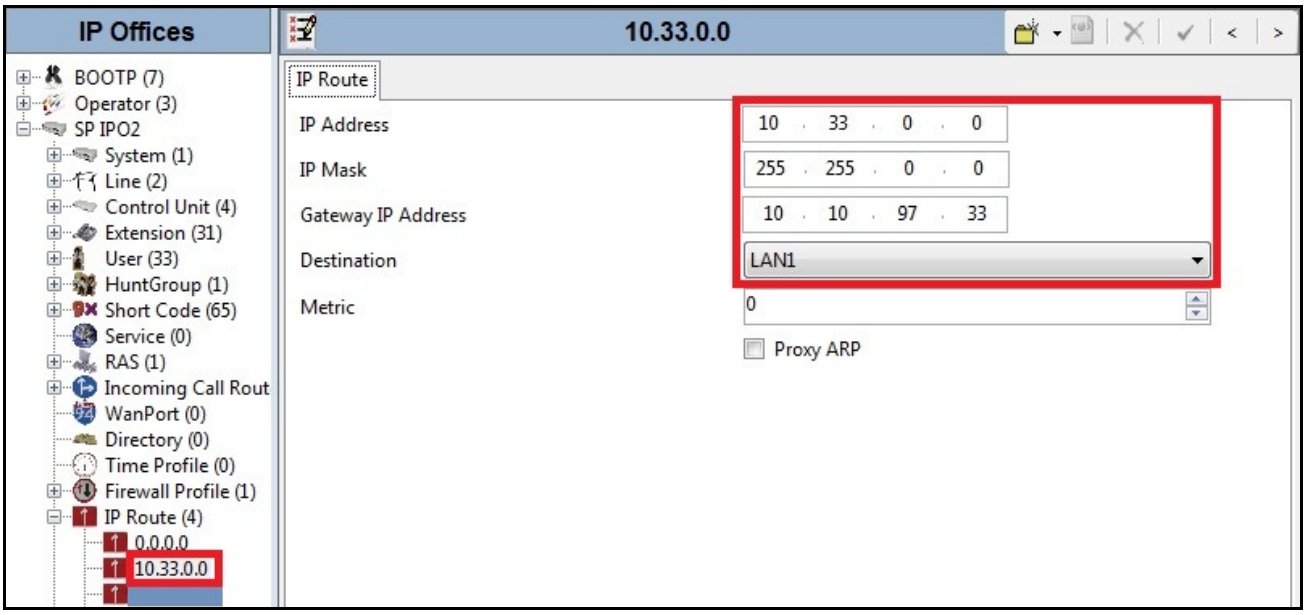
The IP Routes were configured using the following settings.

- Set **IP Address** to the address of destination network.
- Set **IP Mask** to the subnet mask of destination network.
- Set **Gateway IP Address** to the IP address of enterprise gateway that routes traffic to destination network.
- Set **Destination** to interface **LAN1**.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.

The following screenshot shows IP Route **10.10.0.0** that was created on **LAN1** for SIP and RTP traffic to ThinkTel via Avaya SBCE. **LAN1** was assigned to network address **10.10.0.0** and default subnet mask **255.255.0.0**. The default gateway was set to IP address **10.10.97.33** which is an internal gateway on enterprise network that connects to **LAN1**.



Similarly, IP Route **10.33.0.0** was created on **LAN1** for IP phone connections across enterprise network. **LAN1** was assigned to network address **10.33.0.0** and default subnet mask **255.255.0.0**. The default gateway was set to IP address **10.10.97.33** which is an internal gateway on enterprise network that connects to **LAN1**.

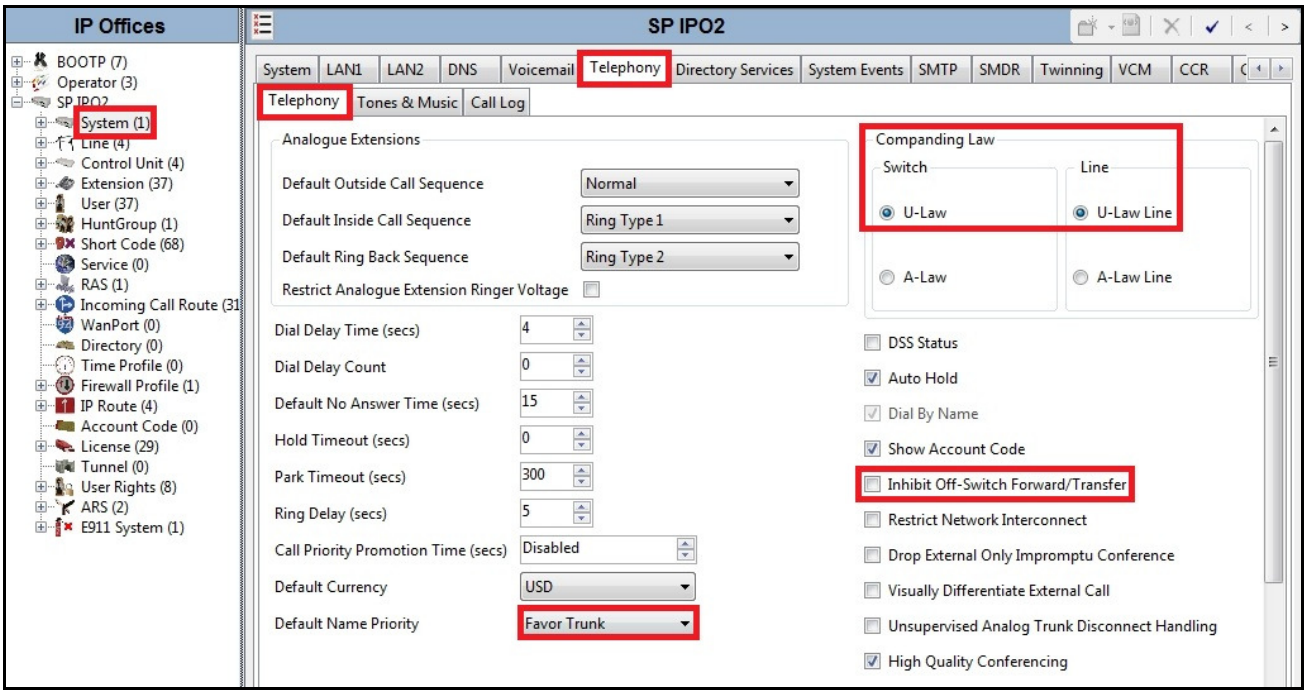


5.3 System Telephony and Codecs

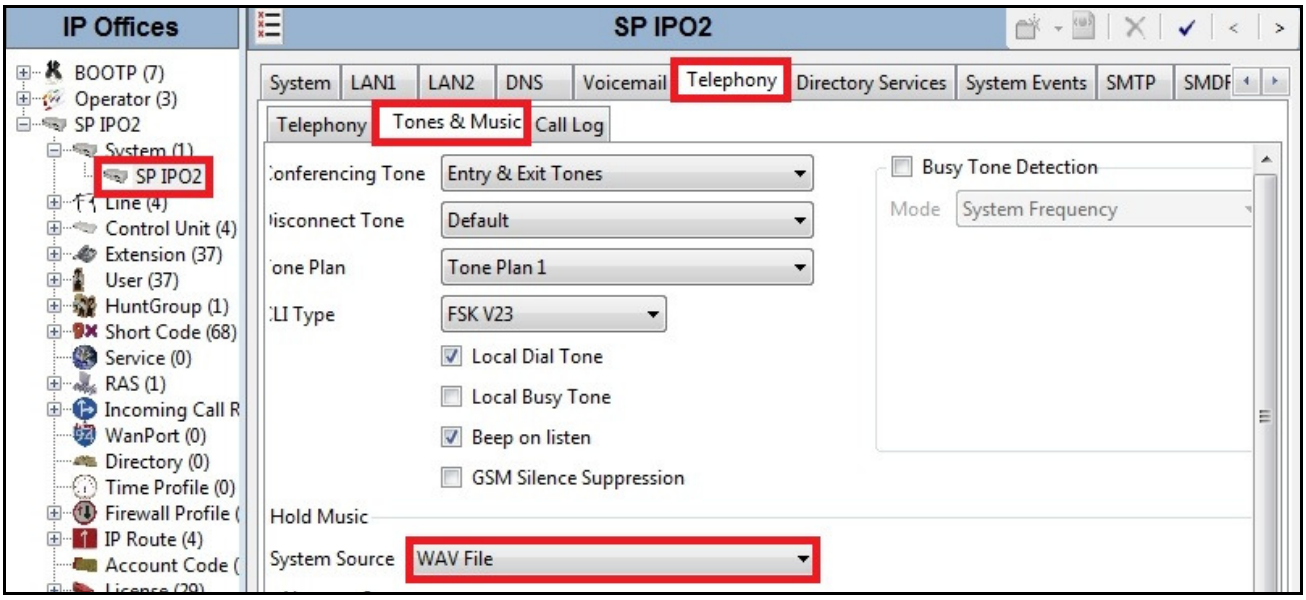
Navigate to **System (1)** → **SP IPO2** in the Navigation Pane then select **Telephony** → **Telephony** tab in the Details Pane.

The System Telephony settings are shown in the screenshot below with following configurations.

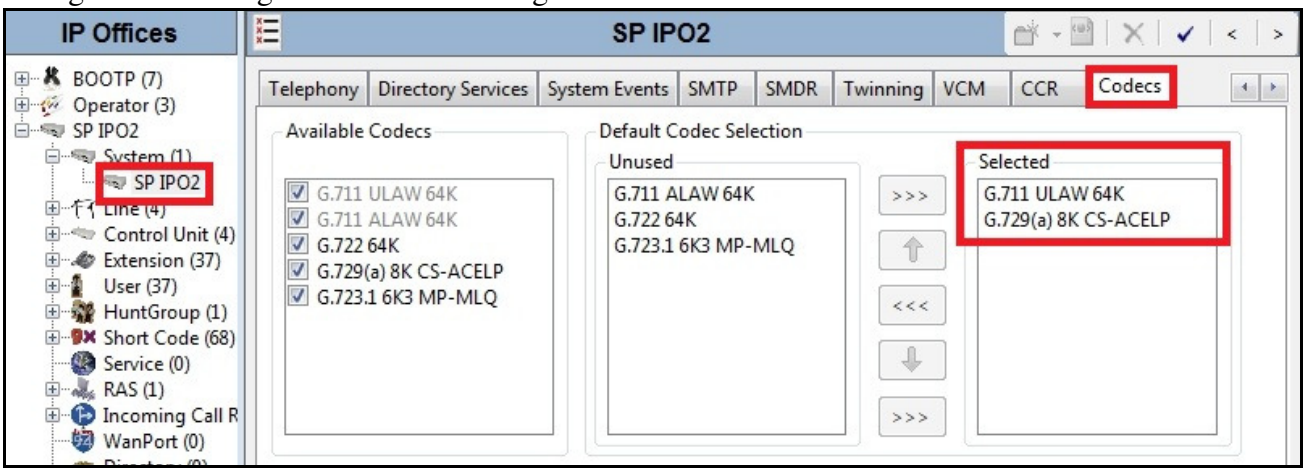
- Set **Companding Law** to **U-Law** for both **Switch** and **Line**. For North America, **U-Law** is used.
- Set **Default Name Priority** to **Favor Trunk**. This allows IP Office to use information received from the SIP Trunk for call display rather than overriding it with pre-defined internal settings.
- Uncheck **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to PSTN via the service provider SIP Trunk.
- Click OK to commit (not shown) then press Ctrl + S to save.



Under **Tones & Music** tab as shown below, **Hold Music** was configured with **System Source** to use **WAV File** which is an uploaded media to provide Music on Hold on the SIP Trunk.



For **Codecs** settings, navigate to **System (1) → SP IPO2** in the Navigation Pane and then select **Codecs**. **Codecs** settings are shown in the screenshot below with G.729 and G.711MU selected in prioritized order. In the compliance testing, even ThinkTel supported G.729 as the first choice and G.711MU as the second choice for RTP, G.711MU should be set as higher priority on IP Office to support fax over IP. Otherwise, the fax calls would fail because both ThinkTel and IP Office cannot re-negotiate to change the RTP from using other codec to G.711MU for fax.



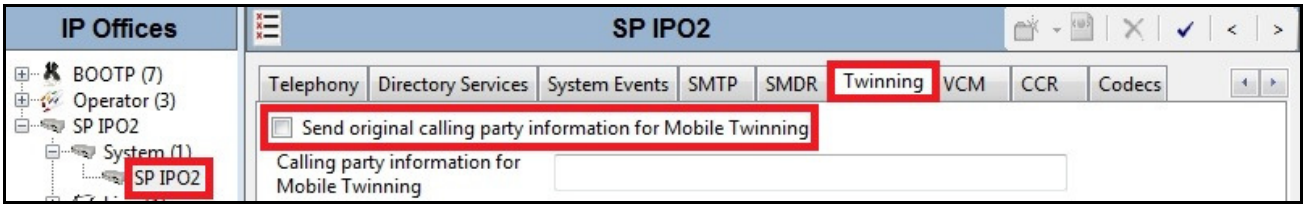
Click OK to commit (not shown) then press Ctrl + S to save.

5.4 Twinning Calling Party Information

When using Twinning, Calling Party Number displayed on the twinned phone is controlled by two parameters. The first parameter is **Send original calling party information for Mobile Twinning** box on **System (1) → SP IPO2 →Twinning** tab. The second parameter is **Send Caller ID** parameter on **SIP Line** form shown in **Section 5.5.1**.

For the compliance testing, **Send original calling party information for Mobile Twinning** as shown below was unchecked. This setting allows **Send Caller ID** parameter that was set to **Diversion Header** in **Section 5.5.1**, to be used. IP Office will send following in the "From" header:

- On calls from internal extension to the twinned phone, IP Office sends Calling Party Number of the originating extension.
- On calls from PSTN to the twinned phone, IP Office sends Calling Party Number of the originating PSTN party.



5.5 Administer SIP Line

SIP Line was needed to establish the SIP Trunk between IP Office and ThinkTel via Avaya SBCE.

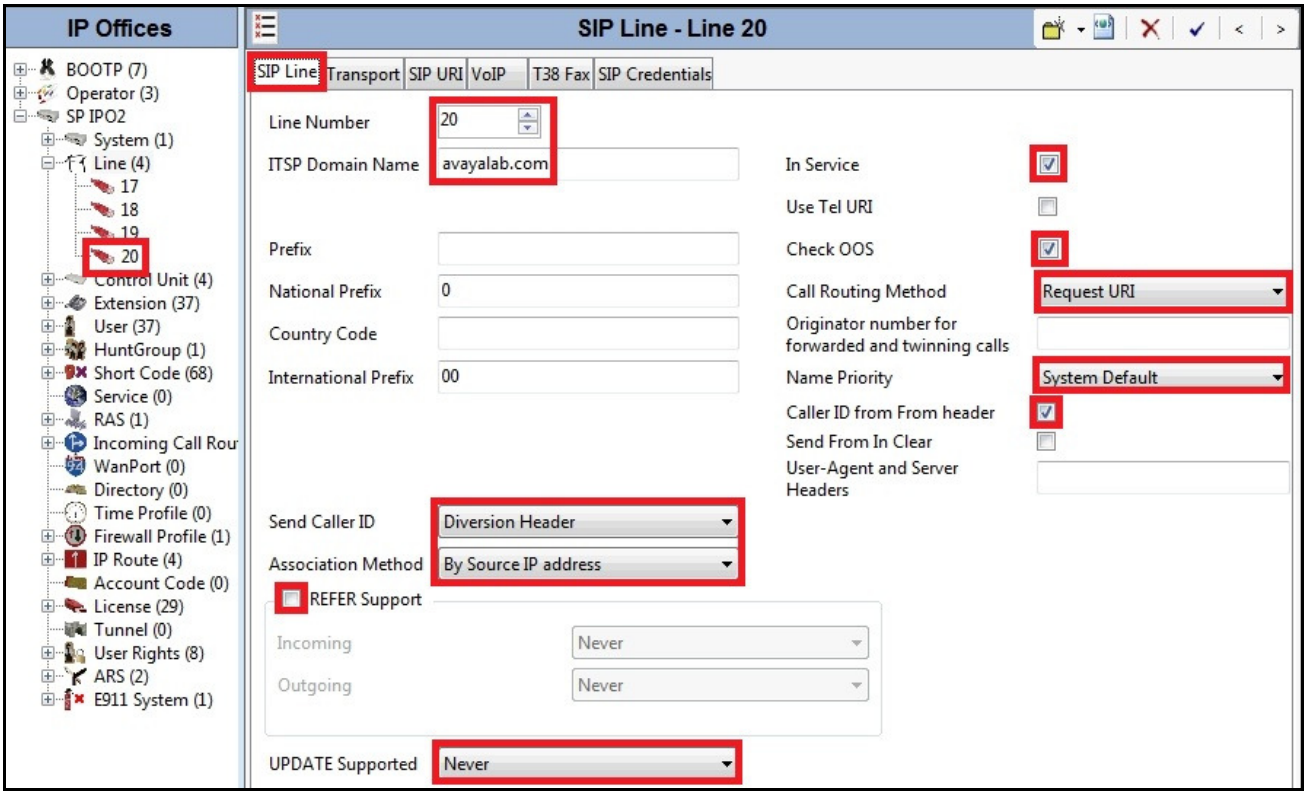
To create SIP Line, navigate to **Line** in the left Navigation Pane then select **New → SIP Line** (not shown).

5.5.1 Administer SIP Line Settings

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

- Set **Line Number** to an unassigned number, e.g., **20**.
- Set **ITSP Domain Name** to the FQDN or IP address that will be used as the enterprise SIP domain so that IP Office uses this domain as the URI-Host of the "From", "P-Asserted-Identity" and "Diversion" headers. In the compliance testing, the enterprise SIP domain was defined as **avayalab.com** for internal traffic between IP Office and Avaya SBCE. This domain will be changed by Topology-Hiding configured on Avaya SBCE (see **Section 6.2.3**) to the public IP address of Avaya SBCE **10.10.98.106** to meet the requirements from ThinkTel.
- Set **Send Caller ID** to **Diversion Header**. For the compliance testing, this parameter was used for Caller ID since **Send original calling party information for Mobile Twinning** was unchecked in **Section 5.4**.
- Set **Association Method** to **By Source IP address**. This setting allows IP Office to apply the configuration for the public SIP Trunk to incoming calls from ThinkTel, if the traffic was originated from **ITSP Proxy Address** that was defined in **Section 5.5.2**.
- Uncheck **REFER Support** and set **UPDATE Supported** to **Never** because they were not supported by ThinkTel in this certification testing.
- Check **In Service** box.
- Check **Check OOS** box. With this option selected, IP Office will send the OPTIONS heartbeat to check status of the SIP Trunk.
- Set **Call Routing Method** field to **Request URI**.
- Set **Name Priority** field to **System Default**.
- Check **Call ID from From header** box.

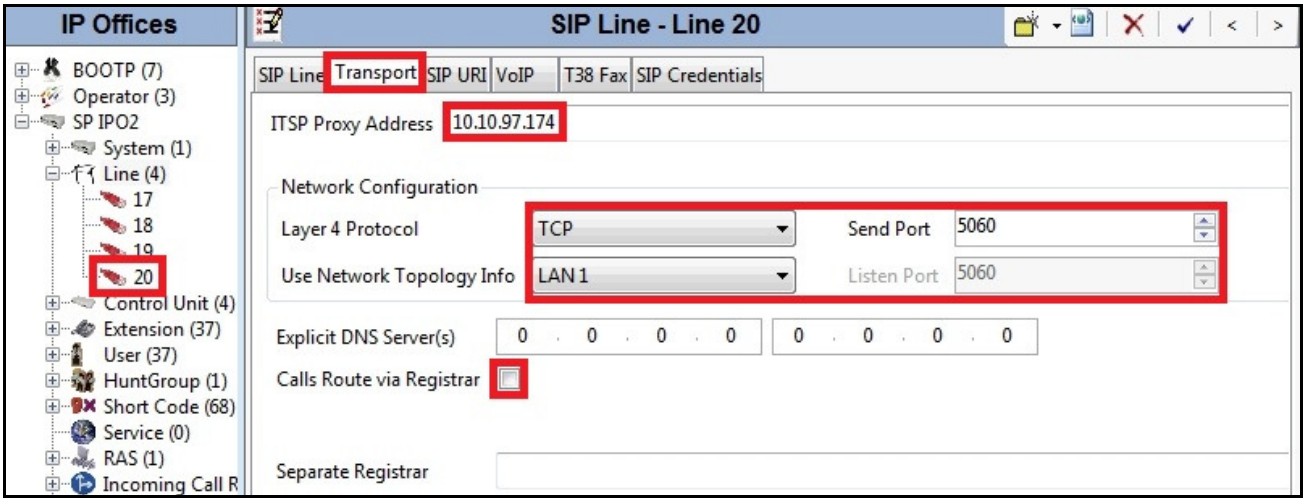
- Default values may be used for all other parameters.
- Click OK to commit (not shown) then press Ctrl + S to save.



5.5.2 Administer Transport Settings

Select **Transport** tab then configure following parameters as shown in the screenshot below.

- The **ITSP Proxy Address** was set to internal IP Address of Avaya SBCE **10.10.97.174** as shown in **Figure 1**.
- In **Network Configuration** area, **TCP** was selected for **Layer 4 Protocol** and **Send Port** was set to well-known port number **5060** which is the port that Avaya SBCE listens for SIP traffic.
- **Use Network Topology Info** parameter was set to **LAN 1**. This associates SIP Line 20 to the parameters defined in **System → LAN1 → Network Topology** tab.
- **Calls Route via Registrar** was unchecked. **Note**: In this certification testing, dynamic Registration on the SIP Trunk was implemented on Avaya SBCE as shown in **Section 6.2.5.2**.
- Other parameters retain default values.
- Click OK to commit (not shown) then press Ctrl + S to save.

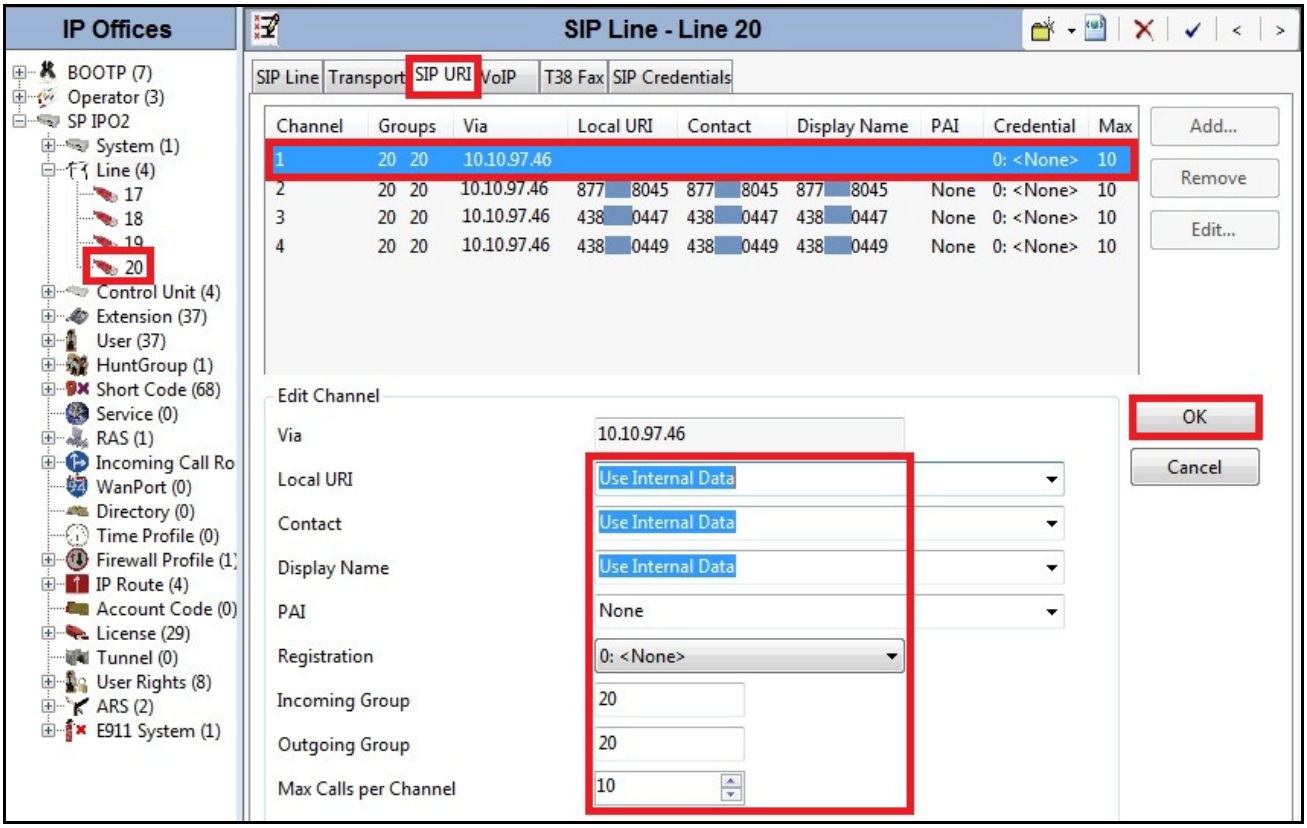


5.5.3 Administer SIP URI Settings

SIP URI entries must be created to match Calling Party Number for incoming calls or to present Calling Party Number for outgoing calls on the SIP Line. Select **SIP URI** tab, click **Add** button to display **New Channel** area at the bottom of the pane (not shown). To edit an existing entry, click an entry in the list at the top and click **Edit…** button (not shown).

For the compliance testing, SIP URI entry with **Channel 1** was created for incoming and outgoing calls with parameters as shown below:

- Set **Local URI**, **Contact** and **Display Name** to **Internal Data**. This setting uses Calling Party Name and Number defined under **SIP** tab of **User** as shown in **Section 5.7**.
- Set **PAI** field to **None** to disable PAI on the SIP Trunk. For more information, refer to **Section** Error! Reference source not found., observation **5**.
- For **Registration** field, select **0:<None>** to disable the Registration.
- Associate SIP Line **20** to **Incoming Group** and **Outgoing Group**. The line group number will be used in defining incoming or outgoing call routes for this SIP Line.
- Set **Max Calls per Channel** to **10** which is the number of simultaneous SIP calls that are allowed using this SIP URI pattern.



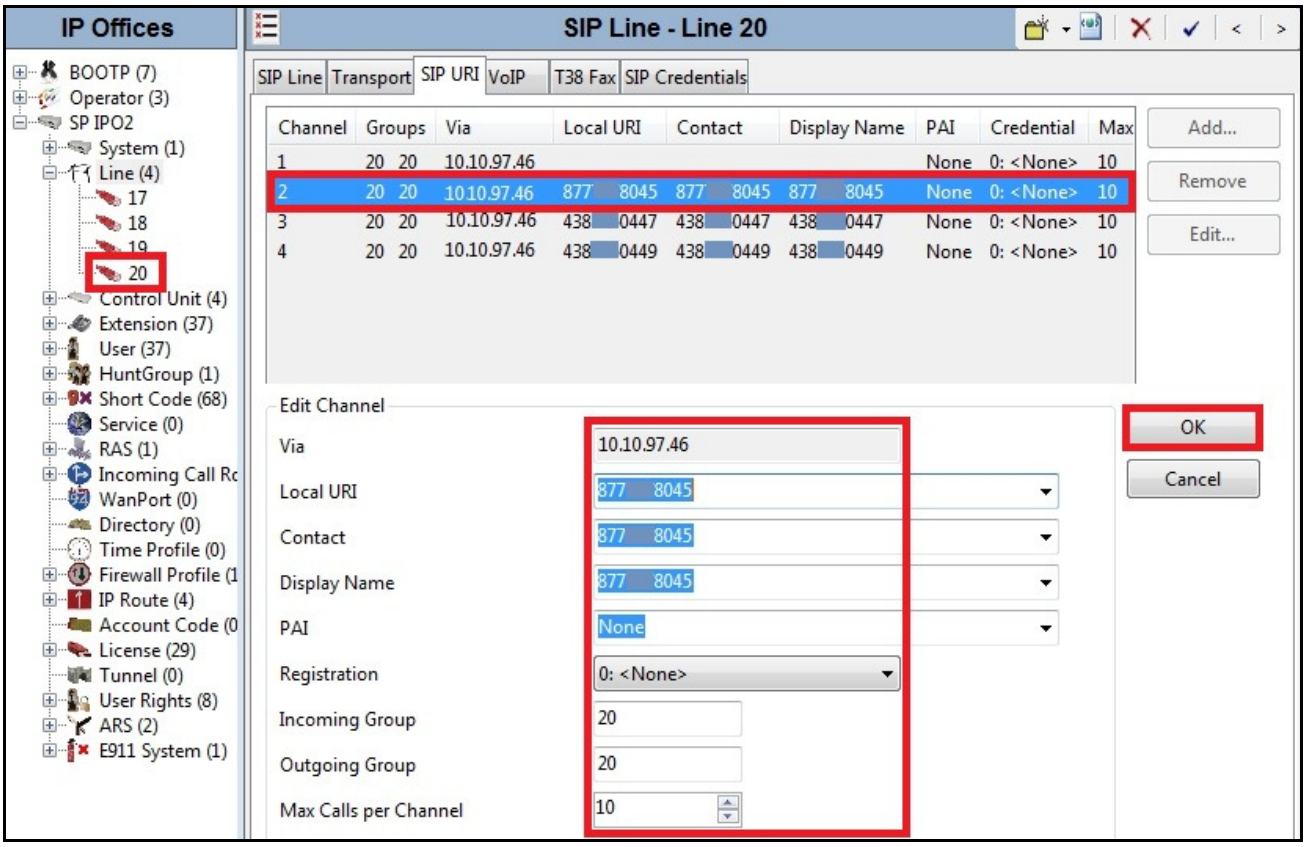
SIP URI entries with **Channel 2**, **Channel 3** and **Channel 4** were similarly created for incoming calls appropriately to pre-define DID numbers **877XXX8045**, **438XXX0447** and **438XXX0449** for access to toll free VoiceMail access, Feature Name Extension 00 (FNE00) and Feature Name. The

Short Codes for FNE00 and FNE33 were defined in **Section 5.6** to provide Dial Tone and Mobile Callback for mobility extension.

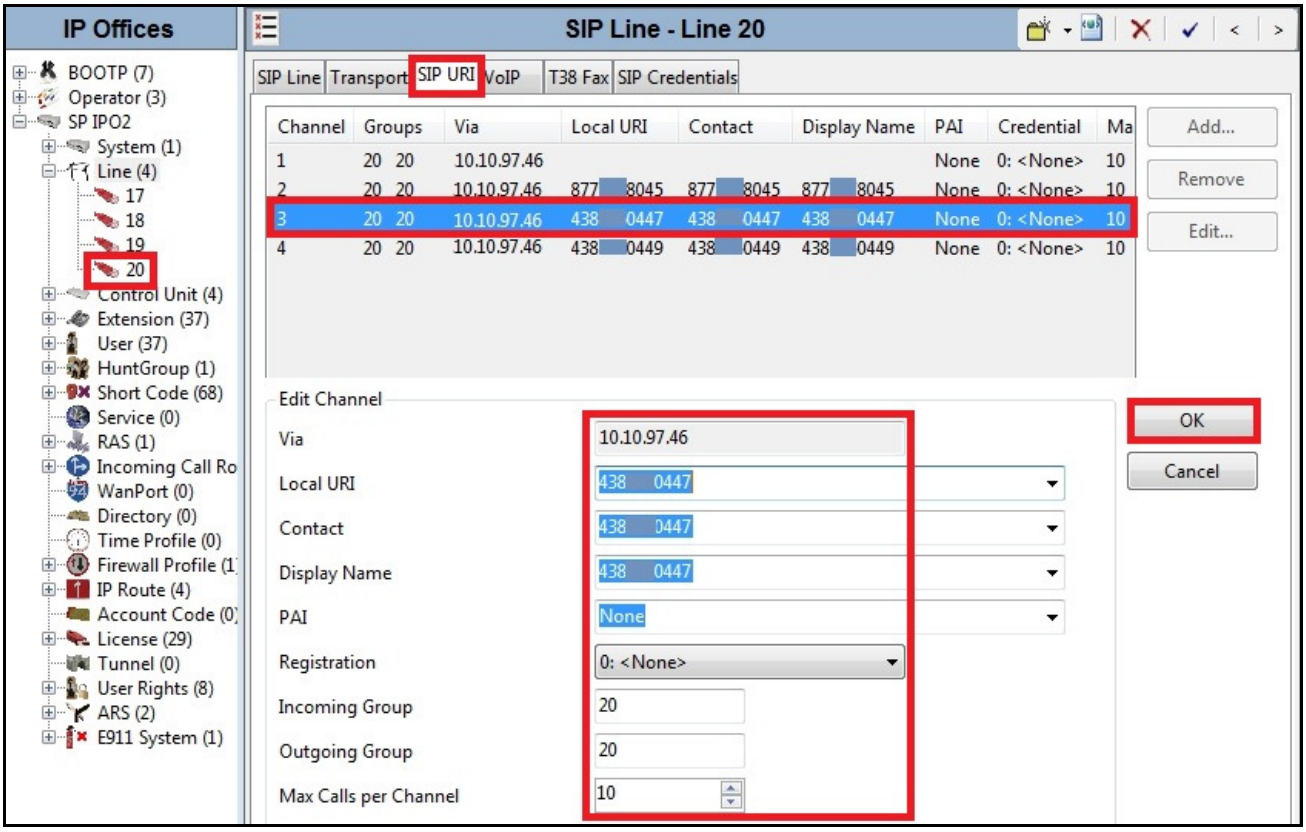
The **Channel 2**, **Channel 3** and **Channel 4** as shown in the screenshot below, were configured with following parameters.

- Set **Local URI** and **Contact** fields to pre-define DID number **877XXX8045**, **438XXX0447** and **438XXX0449** appropriately for **Channel 2**, **Channel 3** and **Channel 4**.
- Associate **Incoming Group** and **Outgoing Group** to SIP Line **20**.
- Set **Max Calls per Channel** field to **10**.
- Other parameters retain default values.
- Click OK to commit.

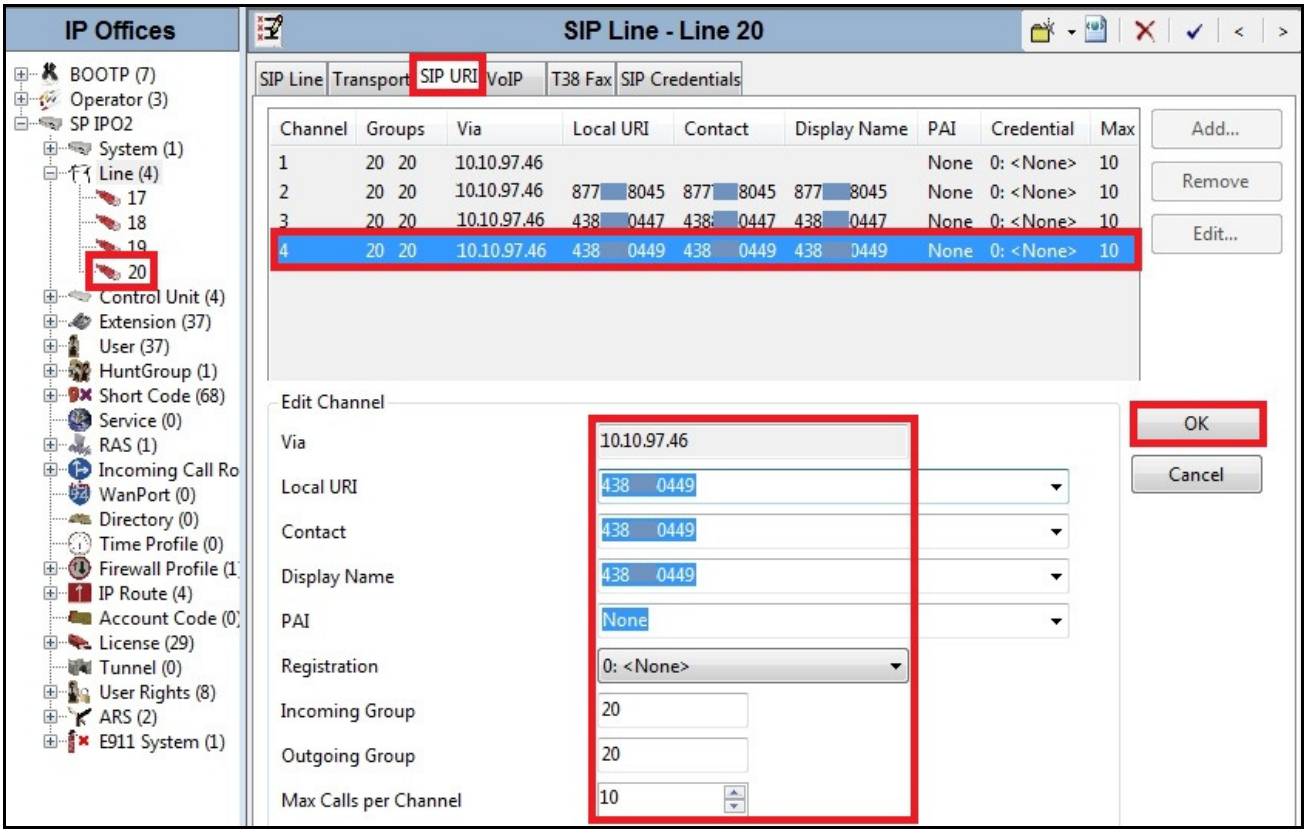
SIP URI entry for **Channel 2**:



SIP URI entry for **Channel 3**:



SIP URI entry for **Channel 4**:

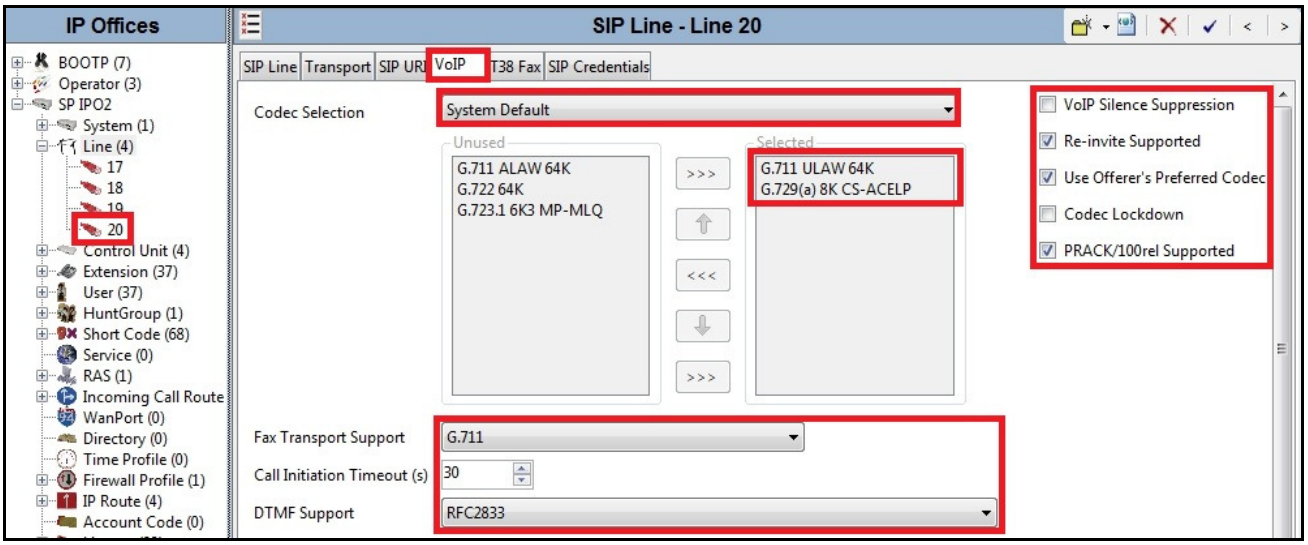


Click OK to commit (not shown) then press Ctrl + S to save.

5.5.4 Administer VoIP Settings

Select **VoIP** tab, then set parameters of the SIP Line as following:

- **Codec Selection** can be selected to **System Default** from the pull-down menu to use System Codecs as defined in **Section 5.3**.
- Set **Fax Transport Support** to **G.711**, see **Section 2.2**, observation **6** for more detail.
- Set **Call Initiation Timeout (s)** to **30** seconds to allow a long enough duration for a public call to be established over the SIP Trunk.
- Set **DTMF Support** to **RFC2833**. This directs IP Office to send out-of-band DTMF tones using RTP events per RFC 2833.
- Uncheck **VoIP Silence Suppression** box. By unchecking **VoIP Silence Suppression** box, calls can be established with the G.729 codec but without silence suppression.
- Check **Re-invite Supported** box.
- Check **Use Offerer's Preferred Codec** box.
- Uncheck **Codec Lockdown** box.
- Check **PRACK/100rel** because ThinkTel supports the "100rel" signaling as described in RFC 3262.
- Default values may be used for all other parameters.
- Click OK to commit (not shown) then press Ctrl + S to save.

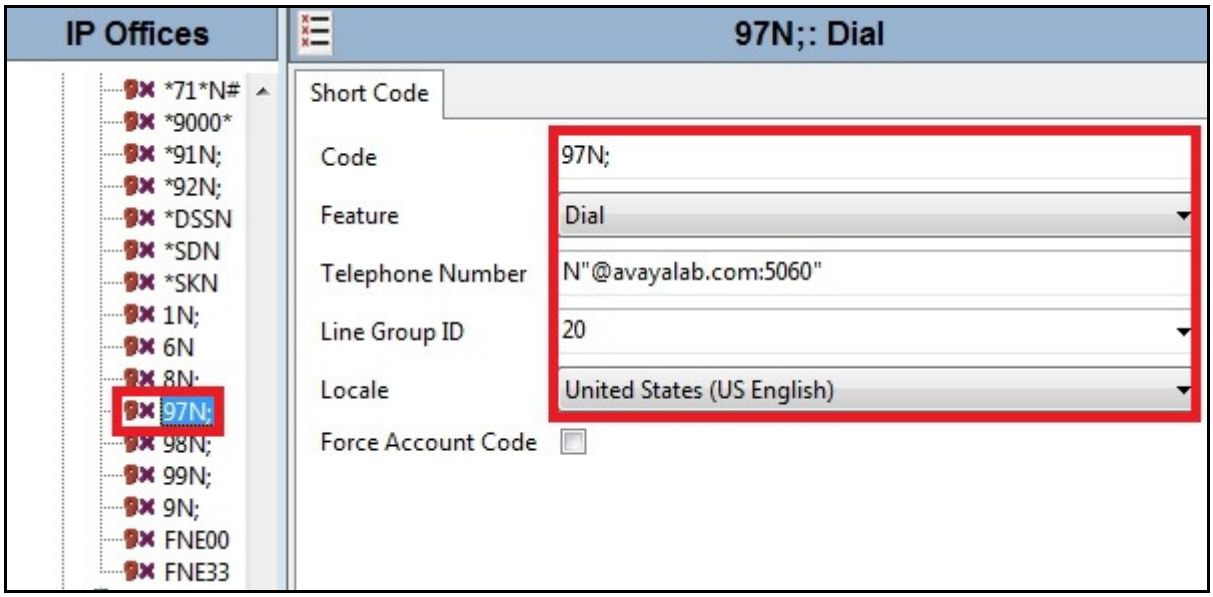


5.6 Short Code

Short Codes are defined to route general outgoing calls and private outgoing calls to PSTN over the SIP Line. In addition, Short Codes are also defined for incoming calls from mobility extensions to access Feature Name Extensions (FNE) hosted on IP Office, or to retrieve voice message on IP Office VoiceMail Pro.

To create short code, select **Short Code** in the left Navigation Pane then right-click and select **New** (not shown). On **Short Code** tab in the Details Pane, configure parameters for the new short code to be created. The screenshot below shows details of Short Code **97N;** that was created for outgoing calls in the test configuration.

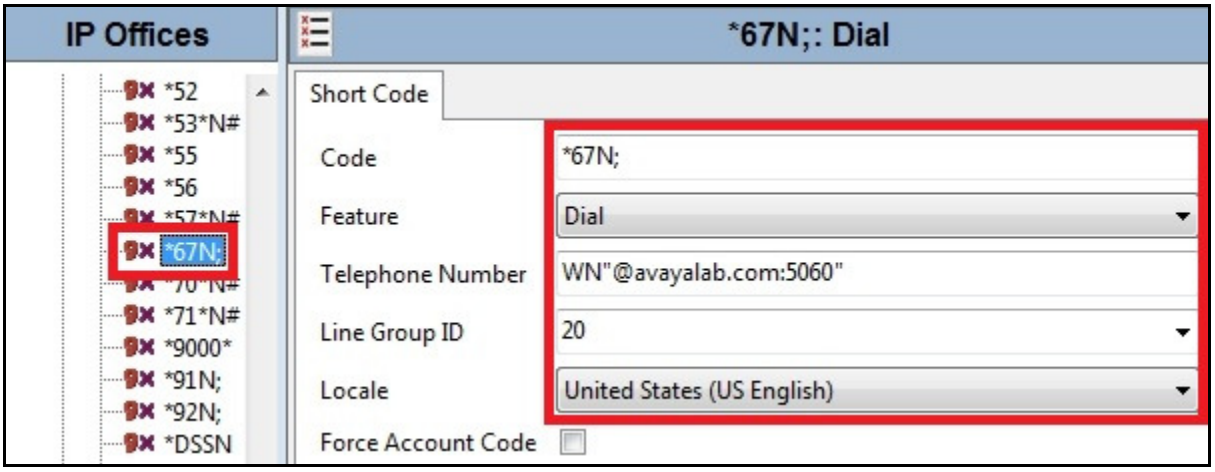
- In **Code** field, enter dial string which will trigger this short code, followed by a semi-colon. In this case, it is **97N;**. This short code will be invoked when user dials **97** followed by any number.
- Set **Feature** to **Dial**. This is the feature that the short code will invoke.
- Set **Telephone Number** to **N"@avayalab.com:5060"**. This field is used to construct the "Request URI" and "To" headers of outgoing calls. The value **N** represents the number dialed by user. The host part following the "@" is the enterprise SIP domain.
- Set **Line Group ID** field to the outgoing line group number **20** defined on **SIP URI** tab for **SIP Line** in **Section 5.5.1**. This short code uses this line group when placing outgoing calls.
- Set **Locale** to **United State (US English)**.



The **97N;** short codes illustrated above do not provide a mean of alternate routing if the configured SIP Line is out of service or temporarily not responding. When alternate routing options and/or more customized analysis of the digits following the short code are desired, Automatic Route Selection (ARS) feature may be used. In the following screenshot, short code 6N is illustrated for accessing to ARS. When IP Office user dials 6 plus any number N, rather than being directed to a specific **Line Group Id**, the call is directed to **Line Group Id 50: Main**, configurable via ARS. See **Section 5.9** for example of ARS route configuration for **50: Main** as well as a backup route.

For private outgoing calls, Short Code ***67N;*** was created as shown in the screenshot below. The digits ***67** was used as a prefix that IP Office user will dial to access to the SIP Trunk for private outgoing calls to PSTN. This causes the called PSTN party not to display Calling Party Name and Number associated with IP Office user.

- In **Code** field, enter dial string which will trigger this short code, followed by a semi-colon. In this case, it is ***67N;**. This short code will be invoked when the user dials ***67** followed by any number **N**.
- Set **Feature** to **Dial**. This is the feature that the short code will invoke.
- Set **Telephone Number** to **WN"@avayalab.com:5060"**. This field is used to construct the "Request URI" and "To" headers for private outgoing calls. The value **W** directs IP Office to mask the "From" header with **anonymous** to block Calling Party Name and Calling Party Number. The value **N** represents the number dialed by the user. The host part following the "@" is the service provider SIP domain.
- Set **Line Group ID** field to **20** which is the outgoing line group number defined on **SIP URI** tab on the **SIP Line** in **Section 5.5.1**. This short code will use this line group when placing private outgoing calls.
- Set **Locale** to **United State (US English)**.

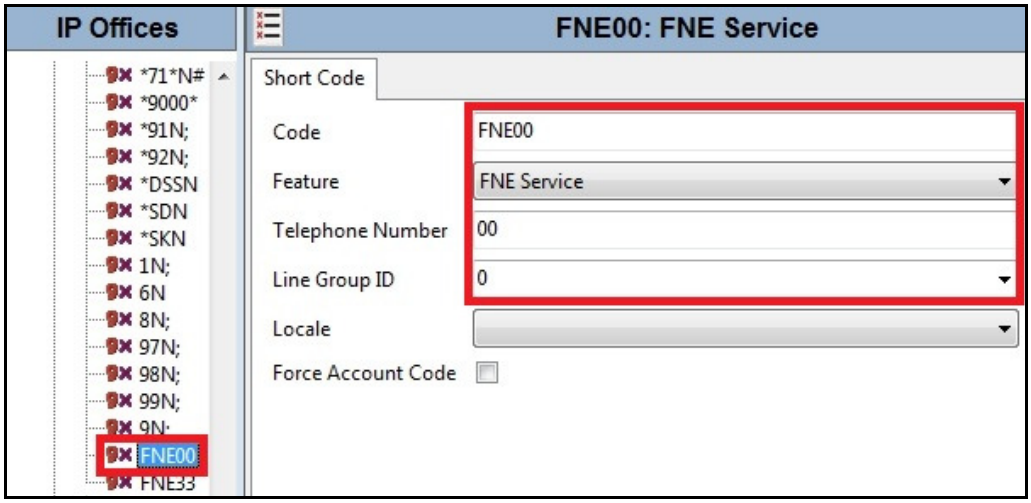


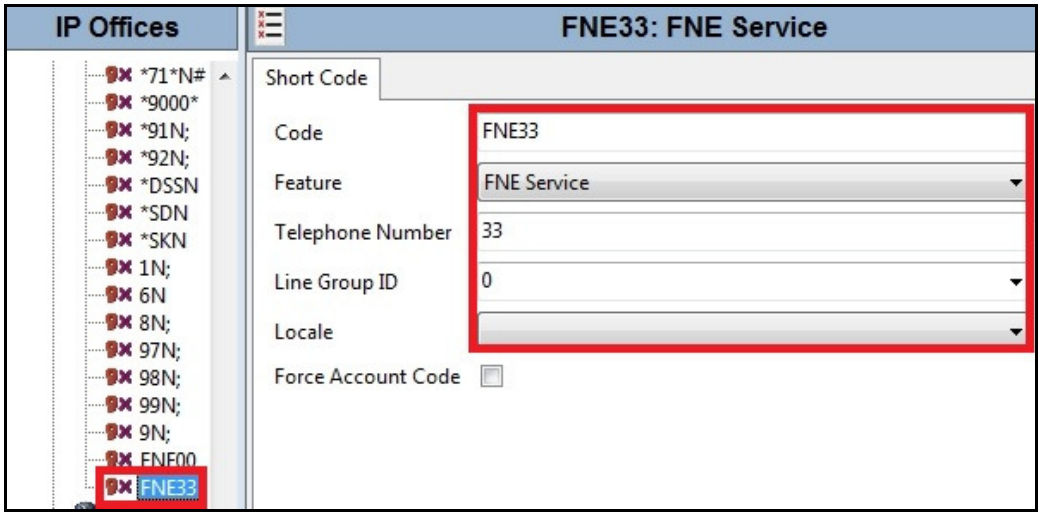
Note: For outgoing private calls, IP Office send "P-Preferred-Identity" header for call authentication purpose. For more information, refer to **Section 2.2**, observation **5**.

For incoming calls from mobility extension to FNE features hosted by IP Office to provide **Dial Tone** or **Mobilecallback** functionalities, Short Code **FNE00** and **FNE33** were created. The **FNE00** and **FNE33** were configured with following parameters.

- For **Code** field, enter FNE feature code as **FNE00** for **Dial Tone** or **FNE33** for **Mobile Callback**.
- Set **Feature** field to **FNE Service**.
- Set **Telephone Number** field to **00** for **FNE00** or **33** for **FNE33**.
- Set **Line Group ID** field to **0**.
- Retain default values for other fields.

The following screenshots illustrate **FNE00** and **FNE33** configurations.





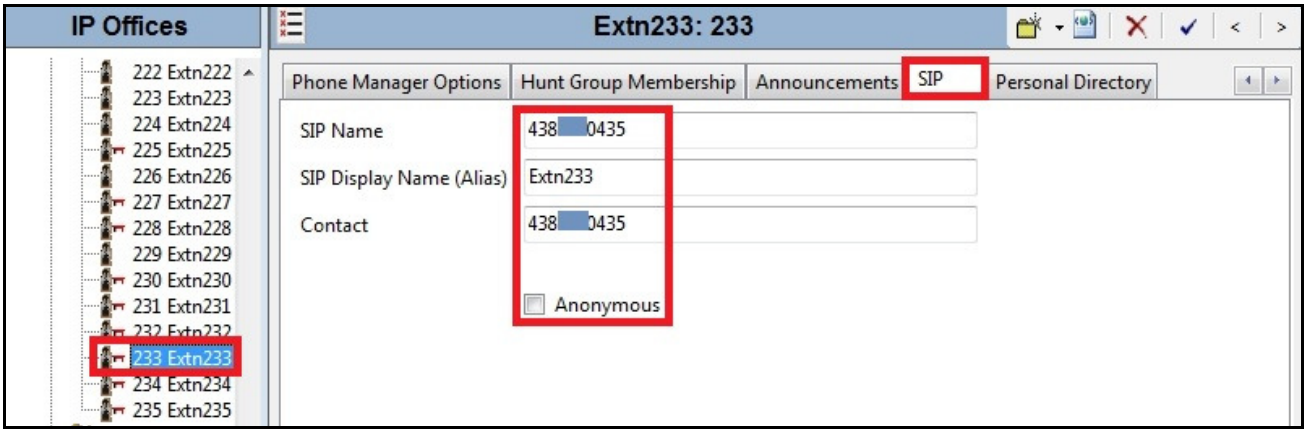
When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.7 User

Configure SIP parameters for each user that will be placing and receiving calls via the SIP Line as defined in **Section 5.5**. To configure these settings, first select **User** in the left Navigation Pane and then select name of the user to be modified. In the example below, with user **233 Exnt233** selected, select **SIP** tab in the Details Pane.

The values entered for **SIP Name** and **Contact** fields were used as URI-User in the "From" header for outgoing calls. They also allow matching of URI-User for incoming calls without having to enter this number as an explicit SIP URI for the SIP Line (see **Section 5.5**). **SIP Name** and **Contact** fields were set to one of the DID numbers assigned to the enterprise by ThinkTel. **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and SIP Line should be considered private then **Anonymous** box may be checked to withhold user information from the networks. **Note**: For outgoing private calls, IP Office send "P-Preferred-Identity" header for call authentication purpose. For more information, refer to **Section** Error! Reference source not found., observation **5**.

In the example below, with user **233 Extn233** selected, select **SIP** tab in the Details Pane. The values entered for **SIP Name** and **Contact** fields are used as the URI-User of the "From" header for outgoing calls. They also allow matching of URI-User for incoming calls without having to enter this number as an explicit SIP URI for the SIP Line (see **Section 5.5**). **SIP Name** and **Contact** fields were set to one of the DID numbers assigned to the enterprise by ThinkTel, e.g., **438XXX0435**. **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name, e.g., **Extn233**. If all calls involving this user and the SIP Line should be considered private then **Anonymous** box may be checked to withhold the user information from the networks.

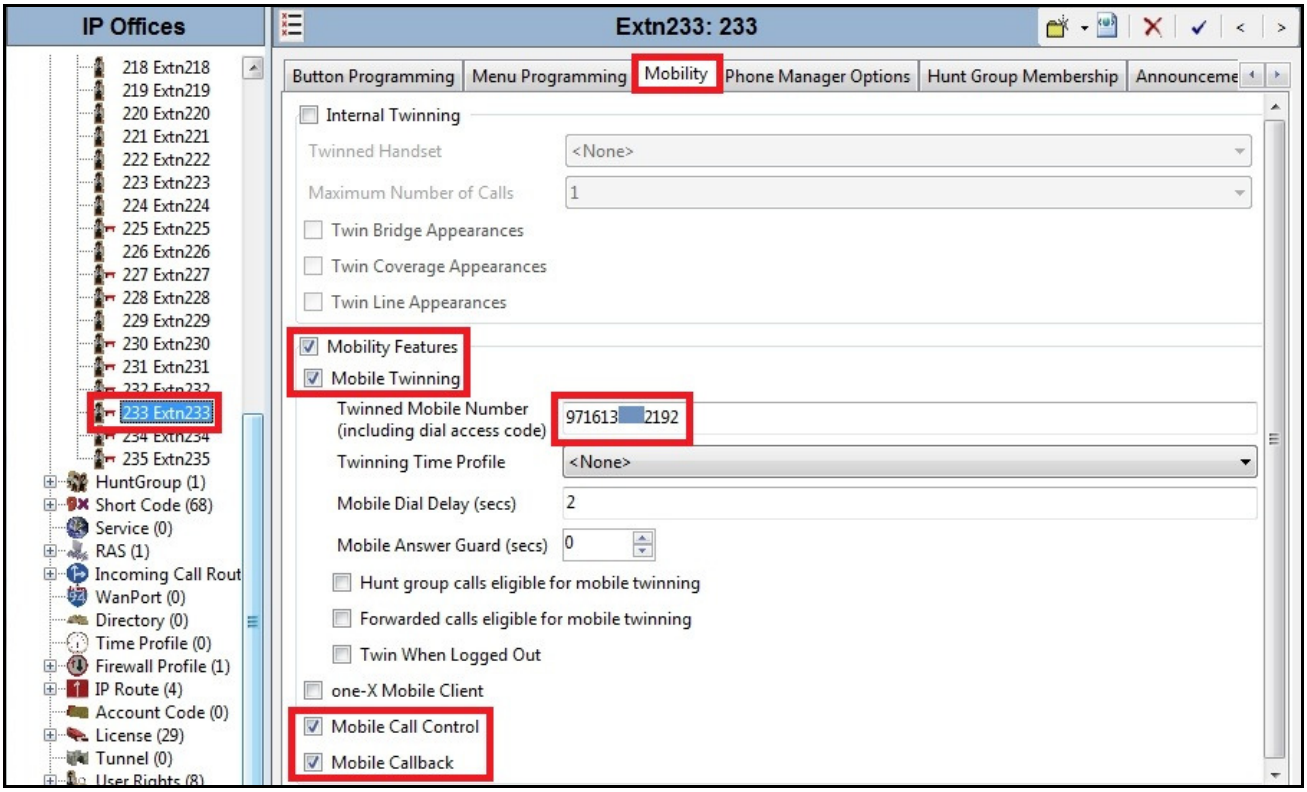


Mobile Twinning feature may be enabled on user to allow incoming calls to simultaneously alert desk phone and mobile phone. The following screenshot shows **Mobility** tab with **Mobility Features** and **Mobile Twinning** boxes checked. **Twinned Mobile Number** field was configured with the number to reach twinned mobile telephone, in this case **971613XXX2192**. Other options can be set according to customer requirements.

The following screenshot shows **Mobility** tab was configured with following parameters:

- **Mobility Features** and **Mobile Twinning** boxes were checked.

- **Twinned Mobile Number** was configured with the number to reach twinned mobile telephone, in this case it was **971613XXX2192** including digit 97 as dial access code and 1613XXX2192 as mobility extension.
- Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (see **Section** Error! Reference source not found.).
- Check **Mobile Callback** to allow IP Office to call back mobility extension to provide dial tone responding to incoming calls from mobility extension to access FNE33 (see **Section** Error! Reference source not found.).
- Other options can be set according to customer requirements.



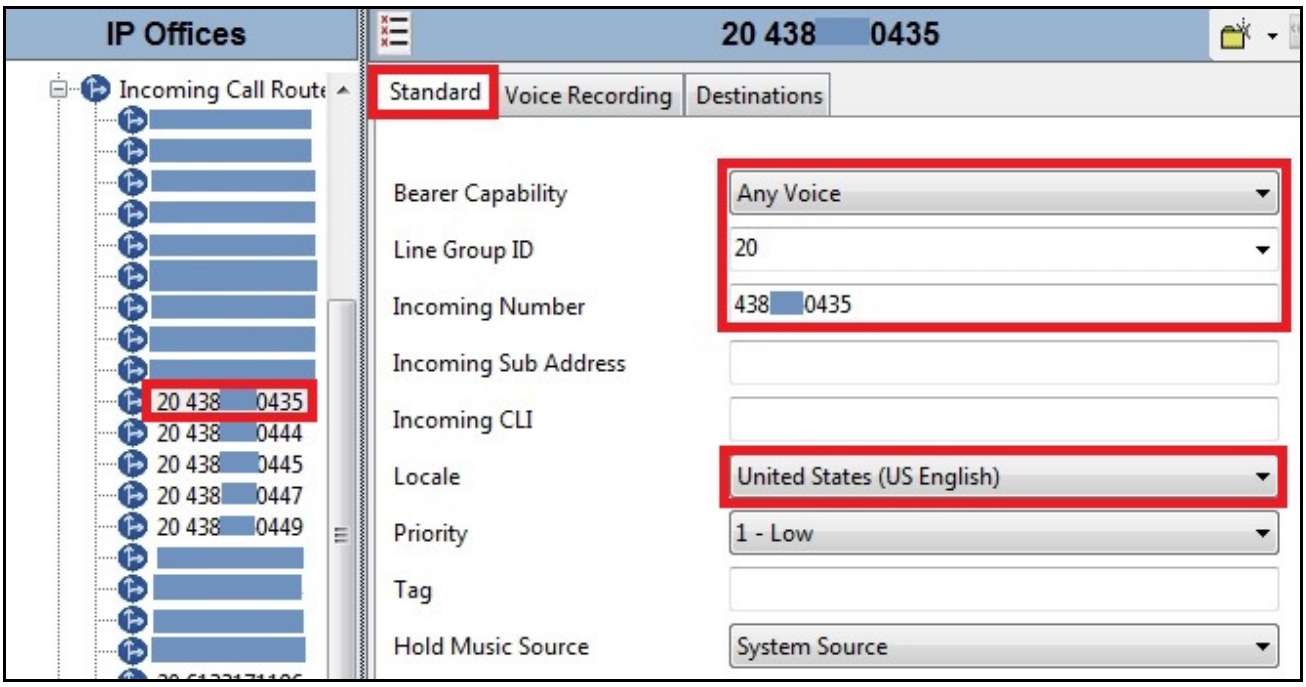
When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.8 Incoming Call Route

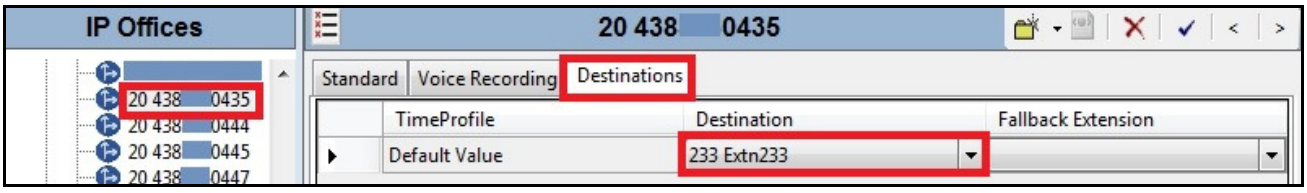
Incoming Call Route maps incoming call on specific SIP Line to internal extension. This procedure should be repeated for each DID number provided by service provider. To create Incoming Call Route, right click on **Incoming Call Route** in the left Navigation Pane and select **New** (not shown). On **Standard** tab of the Details Pane, enter following parameters.

- Set **Bearer Capability** to **Any Voice**.
- Set **Line Group ID** to SIP Line **20** as defined in **Section 5.5**.
- Set **Incoming Number** to DID number that associate to internal extension.
- Set **Locale** to **United State (US English)**
- Default values can be used for all other fields.

The screenshot below shows Incoming Call Route **20 438XXX0435** configured to receive incoming calls to DID number **438XXX0435** then alert local station **233**.

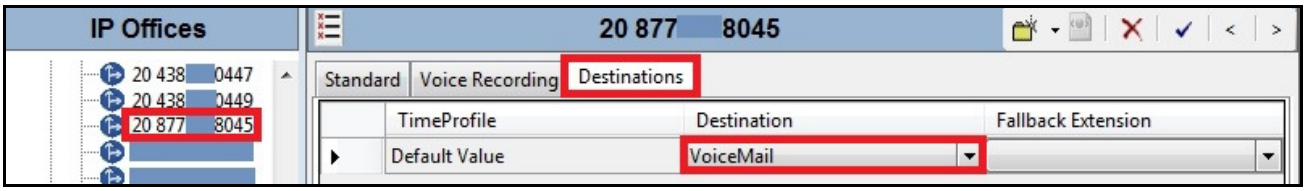


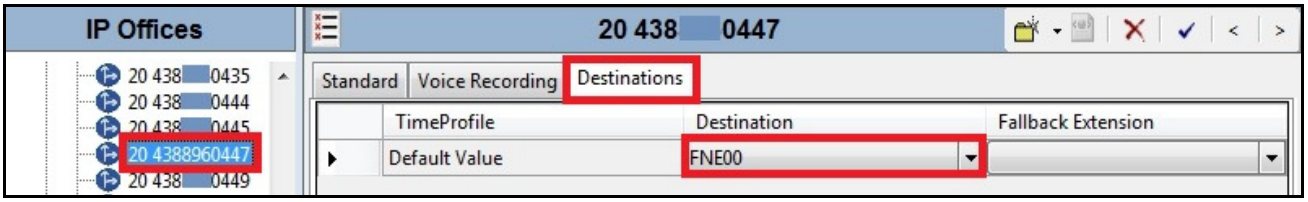
On **Destinations** tab, select destination extension from the pull-down menu of **Destination** field. In this example, incoming calls to **438XXX0435** on SIP Line 20 are routed to extension **233 Extn233**.



Following screenshots show Incoming Call Routes to receive incoming calls to DID numbers **877XXX8045**, **438XXX0447** and **438XXX0449** that were similarly configured to access **VoiceMail**, **FNE00** and **FNE33**. **Destinations** were appropriately defined as **VoiceMail**, **FNE00** and **FNE33**.

Note: FNE00 and FNE33 were entered manually by selecting **Destination** as **DialIn** (not shown) then input the appropriate FNE feature code.





When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.9 ARS and Alternate Routing

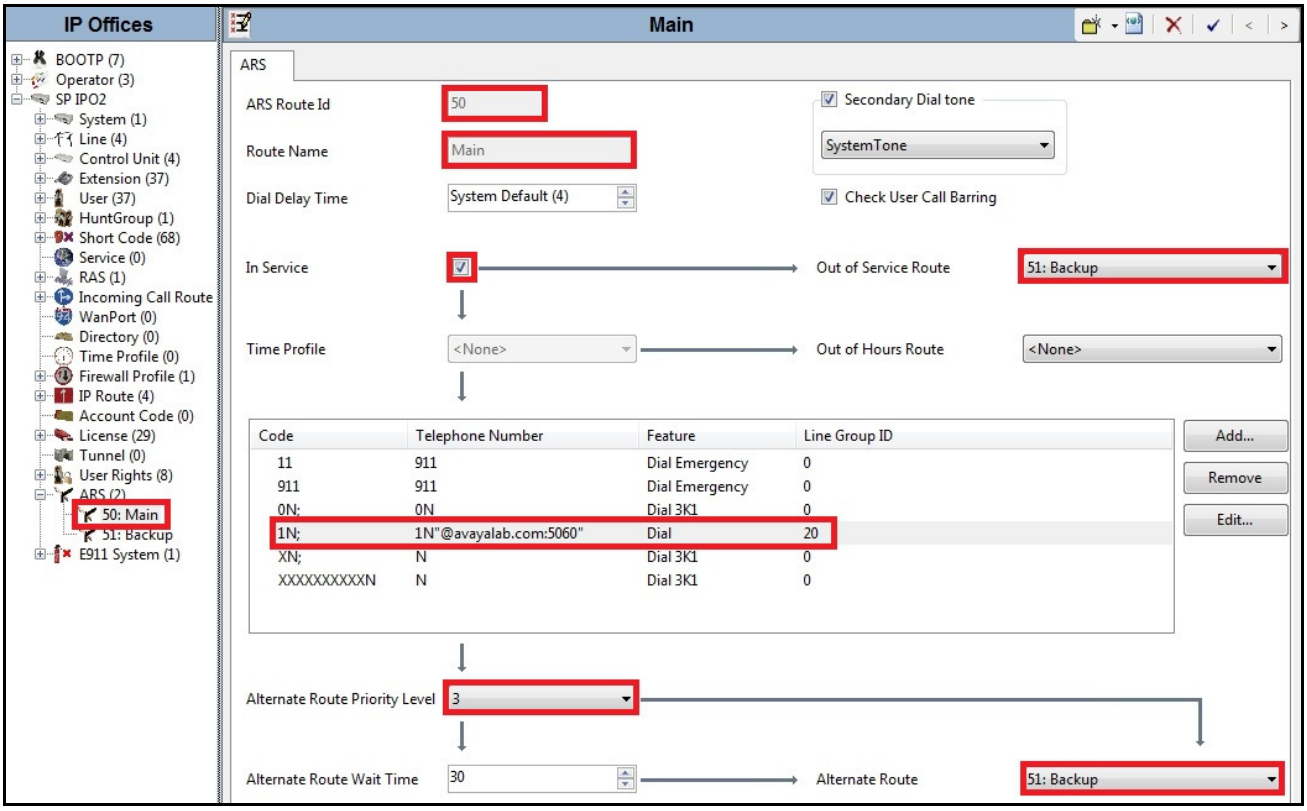
While detailed coverage of Automatic Route Selection (ARS) is beyond the scope of these Application Notes, this section includes basic ARS screenshot illustrations and considerations. ARS is illustrated here to demonstrate alternate routing configuration should the SIP Line be out of service or temporarily not responding.

Optionally, ARS can be used rather than the simple **97N;** Short Code approach as documented in **Section 5.6**. With ARS, a secondary dial tone can be provided after the access code, time-based routing criteria can be introduced, and alternate routing can be specified so that a call can be rerouted automatically if the primary route or outgoing line group is not available. Although not shown in this section, ARS also facilitates more specific dialed telephone number matching, enabling immediate routing and alternate treatment for different types of numbers following the access code. For example, if all 1+10 digit calls following an access code should use the SIP Line preferentially, but other local or service numbers following the access code should prefer a different outgoing line group, ARS can be used to distinguish the call behaviors.

A new ARS entry can be created by right-click **ARS** in the Navigation pane then select **New** (not shown). To view or edit an existing ARS route, select **ARS** in the Navigation pane then select the appropriate route name.

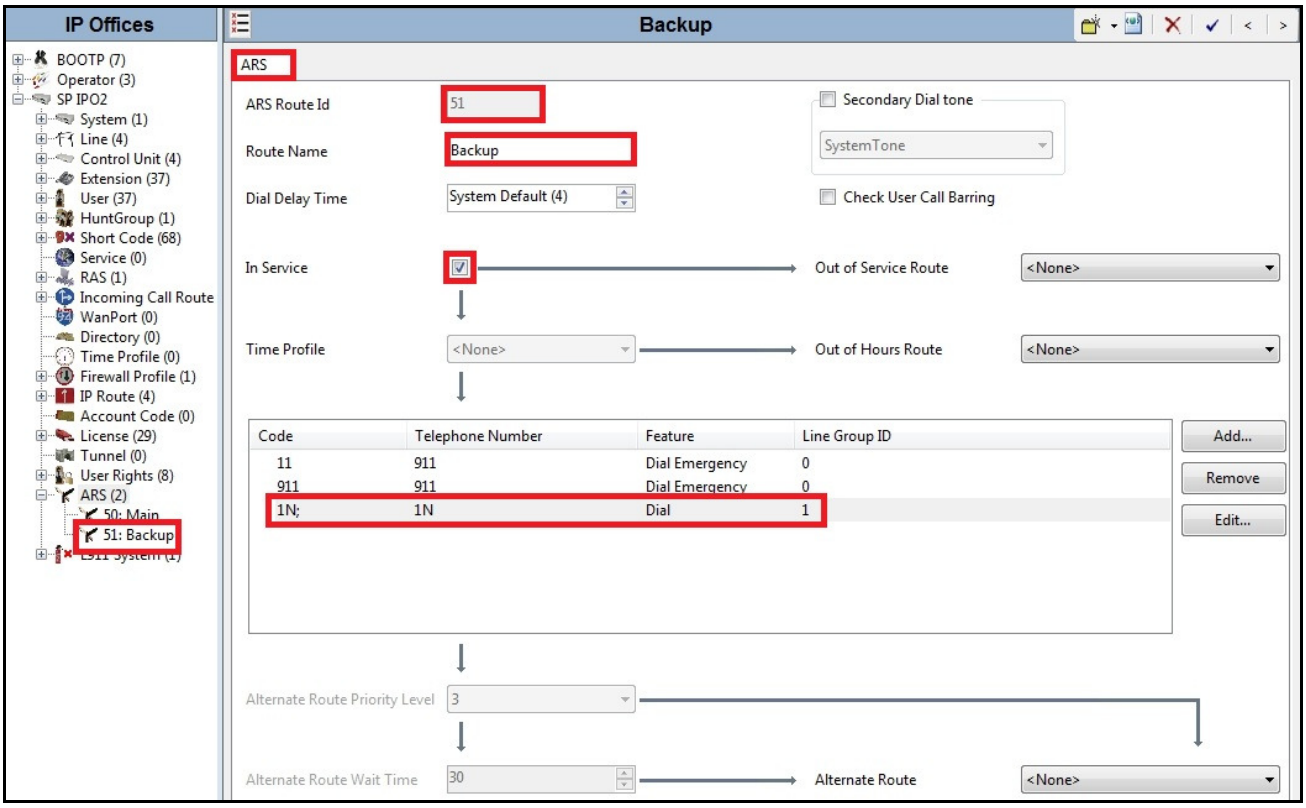
The following screenshot shows an example configuration for ARS **50:Main**. **In Service** parameter refers to the ARS form itself. If **In Service** box is unchecked, calls are routed to the ARS route name specified in **Out of Service Route** parameter. IP Office Short Codes may also be defined to allow

ARS route to be disabled or enabled from a telephone. The provisioning of Out of Service Route and the means to manually activate Out of Service Route can be helpful for scheduled maintenance or other known service-affecting events for the primary route.



Assuming the primary route is in-service, the number passed from the Short Code used to access ARS (e.g., **6N** in **Section 5.6**) can be further analyzed to direct the call to a specific Line Group ID. Per the sample screenshot above, if the user dialed **61613XXX5279**. Then the call will be directed to Line Group 20, which is the SIP Line configured and described in this Application Notes. If the Line Group 20 cannot be used, the call can automatically be routed to the **Alternate Route Priority Level 3** as shown in the screenshot. **Note**: Alternate routing can be considered a privilege not available to all callers, IP Office can control access to the alternate route by comparing the priority of calling users to the value in **Alternate Route Priority Level** field.

The following screenshot shows an example ARS configuration for the route ARS **51:Backup**. Continuing from the prior example, if the user dialed **61613XXX5279** and the call could not be routed via the primary route **50: Main** as described above, it will be delivered to the alternate route **51:Backup**. Per the configuration shown below, the call will be delivered to Line Group 1, using an analog trunk connecting IP Office to PSTN as a backup connection. In this case, the original dialed number (minus the Short Code **6**) will be dialed as is through the analog/PRI trunk to the PSTN. Additional codes (e.g., 411, 0+10, etc.) can be added to the ARS route by pressing **Add…** button on the right of the list of previously configured codes (not shown).



When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.10 Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screenshot to save the configuration performed in the preceding sections (not shown).

6. Configure the Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya SBCE. It is assumed that software has already been installed. For additional information on these configuration tasks, see **References** [**4**], [**5**] and [**6**].

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

Trunk Server configuration elements for service provider - ThinkTel:

- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Signaling Manipulation
  - Server Configuration
- Domain Policies:
  - Application Rules
  - Media Rules
  - Signaling Rules
  - Endpoint Policy Group
  - Session Policy
- Device Specific Settings:
  - Network Management
  - Media Interface
  - Signaling Interface
  - End Point Flows → Server Flows
  - Session Flows

Call Server configuration elements for the enterprise - IP Office:

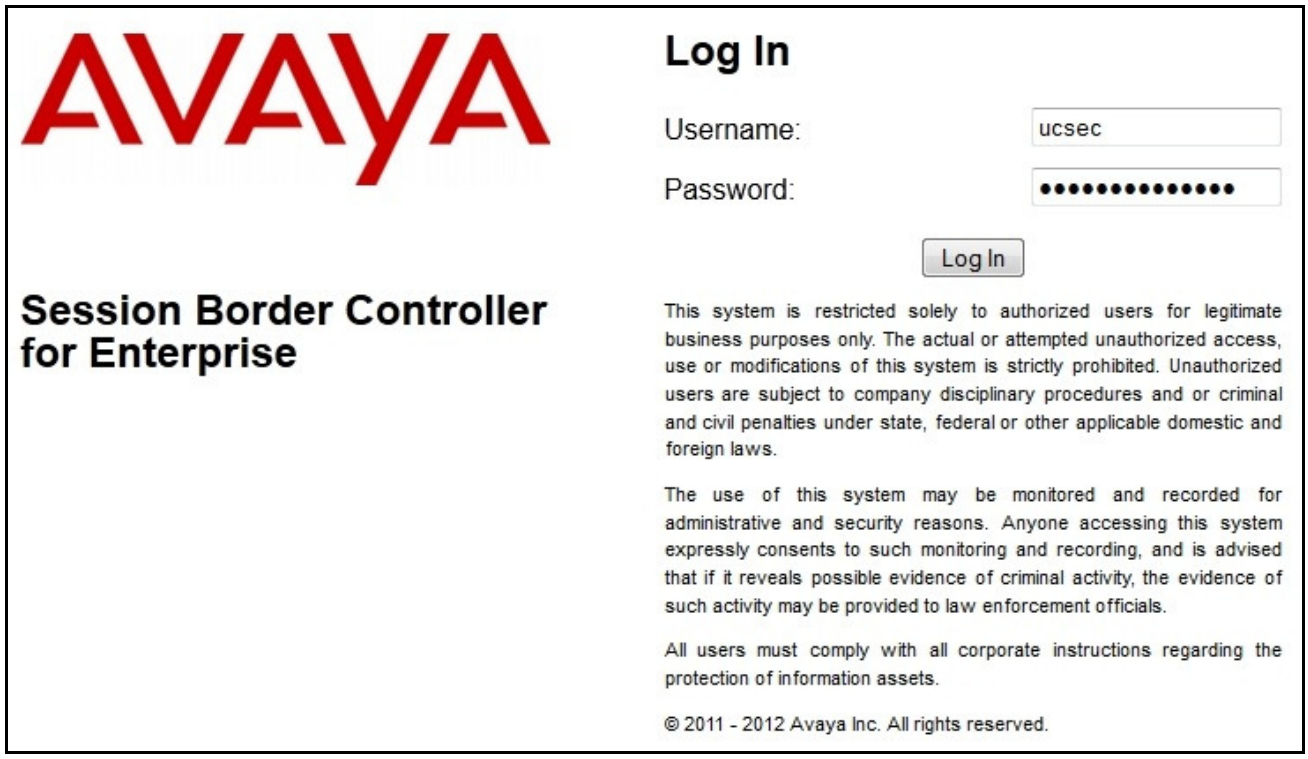
- Global Profiles:
  - URI Groups
  - Routing
  - Topology Hiding
  - Server Interworking
  - Server Configuration
- Domain Policies:
  - Application Rules
  - Media Rules
  - Signaling Rules
  - Endpoint Policy Group
  - Session Policy
- Device Specific Settings:
  - Network Management

- Media Interface
- Signaling Interface
- End Point Flows → Server Flows
- Session Flows

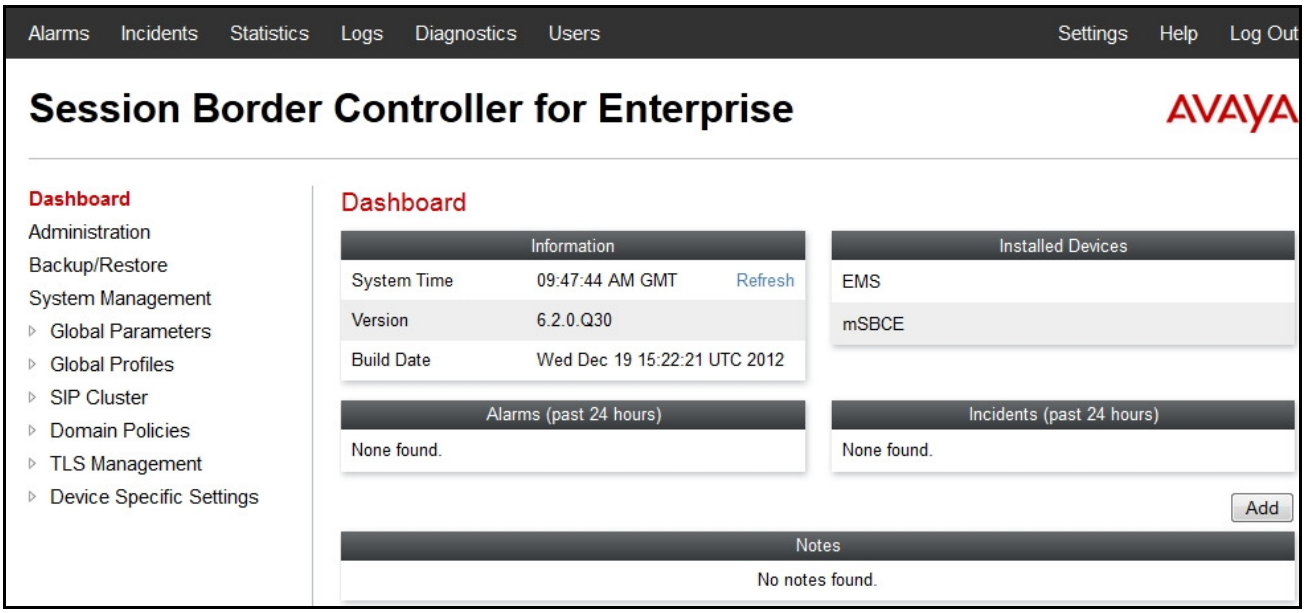
6.1 Log into Avaya Session Border Controller for Enterprise

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

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

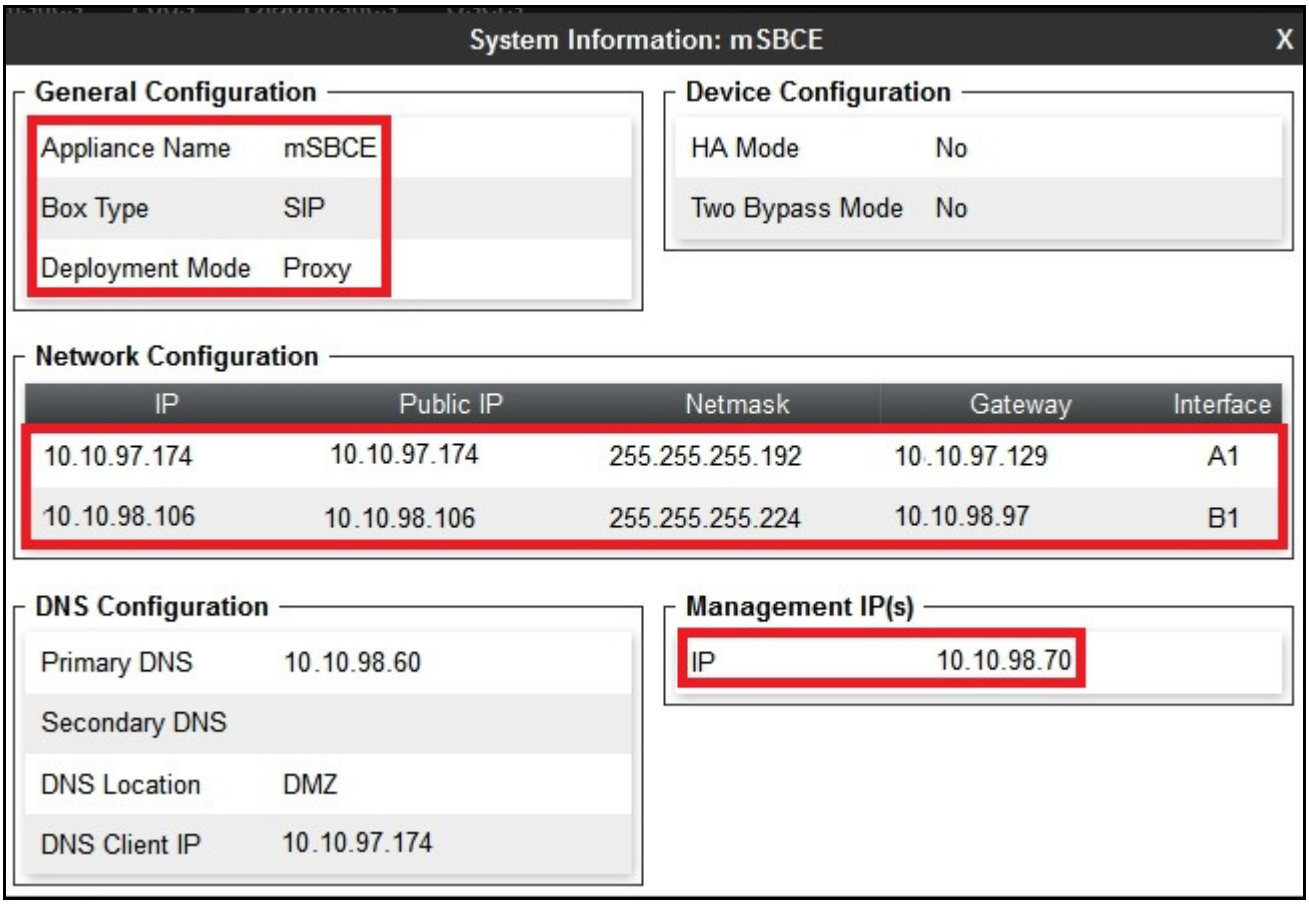


Dashboard main page will appear as shown below.



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

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



6.2 Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.2.1 Uniform Resource Identifier (URI) Groups

URI Group feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

To add URI Group, select **Global Profiles → URI Groups** then click **Add** button (not shown).

In the compliance testing, URI Group **ThinkTel** was added with URI type as **Regular Expression**. It consists of enterprise SIP domains "**.*avayalab\.com**" for regular calls and "**.*nonymous\.invalid**" for private calls, IP address based service provider SIP domains "**.*10\.20\.161\.101**" and "**.*10\.10\.98\.106**", IP addresses based URI-Host of the OPTIONS heartbeat originated by IP Office "**.*10\.10\.97\.46**" and "**.*10\.10\.97\.174**". The OPTIONS

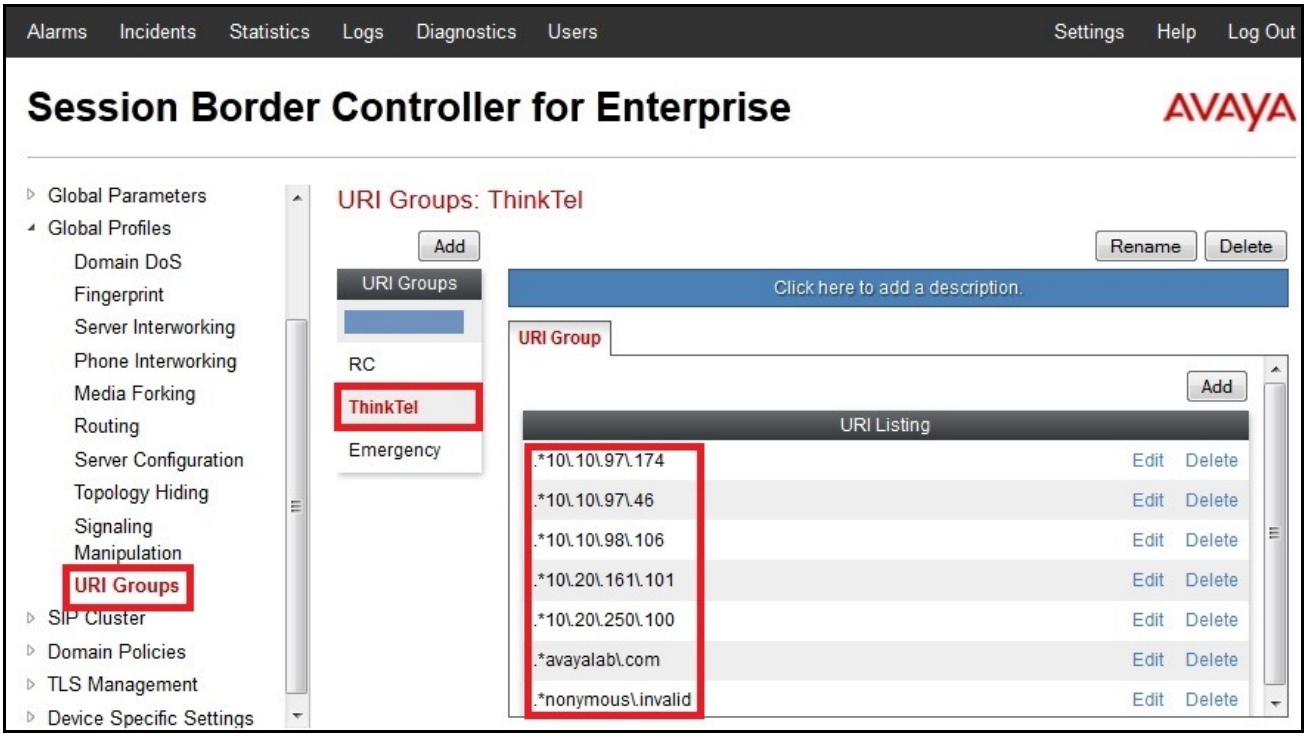
heartbeat originated by service provider had the same IP address based SIP domains defined for regular calls. **Note**: IP address based service provider SIP domains "**.*10\.20\.161\.101**" was provided by ThinkTel and it is different from Session Border Controller IP address at service provider side **10.20.250.100** as shown in **Figure 1**.

SIP domain "**.*nonymous\.invalid**" was defined for private outgoing calls from IP Office which URI-Host was masked to **anonymous.invalid**. The enterprise SIP domain "**.*avayalab\.com**" was defined as per description in **Section 5.5.1** for enterprise SIP traffic originated from IP Office. For the public SIP Trunk between Avaya SBCE and ThinkTel, the URI-Host in the "From", "PAI", and "Diversion" headers, presents SIP domain "**10.10.98.106**" while the URI-Host in the "Request-URI" and "To" headers, will have SIP domain "**10.20.250.100**". These domains are assigned by ThinkTel. The IP addresses and value of URI-Host in OPTIONS heartbeat were also defined for routing incoming and outgoing OPTIONS between IP Office and ThinkTel.

URI-Group **ThinkTel** was used to match the "From" and "To" headers in a SIP call dialog received from both IP Office and ThinkTel. If there is a match, Avaya SBCE will apply appropriate Routing Profiles (see Section **6.2.2**) and Server Flow (see **Section 6.4.4**) to route incoming and outgoing calls to the right destinations.

Note: For the compliance testing, the addition of URI-Group is optional to isolate incoming and outgoing calls between ThinkTel and Avaya lab which is a shared testing environment. For the field deployment, the use of URI-Group may not be required.

The screenshot below illustrates the URI listing for URI Group **ThinkTel**.



6.2.2 Routing Profiles

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

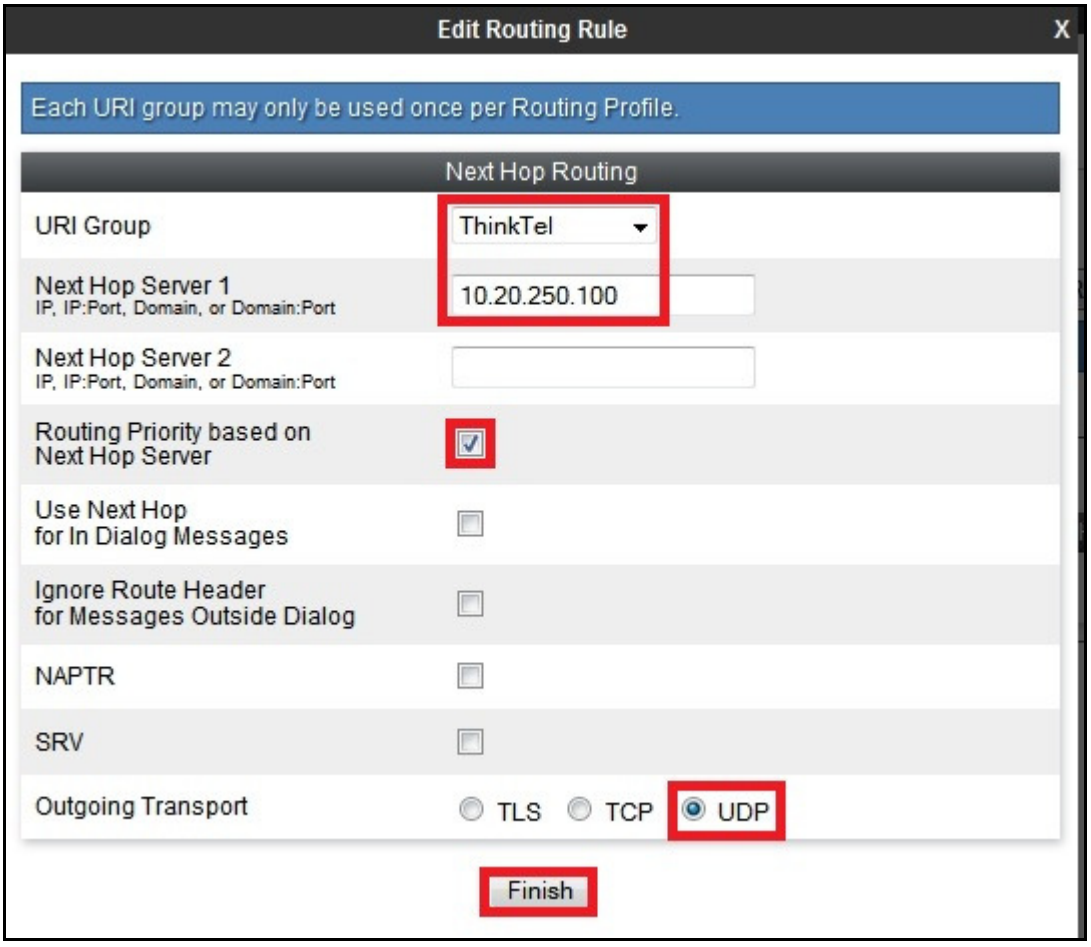
To create Routing profile, select **Global Profiles → Routing** then click **Add** button (not shown).

In the compliance testing, Routing profile **To_ThinkTel** was created to be used in conjunction with Server Flow (see **Section 6.4.4**) defined for IP Office. This entry is to route outgoing calls from the enterprise to ThinkTel.

In the opposite direction, Routing profile **To_IPO** was created to be used in conjunction with a Server Flow (see **Section 6.4.4**) defined for ThinkTel. This entry is to route incoming calls from ThinkTel to the enterprise.

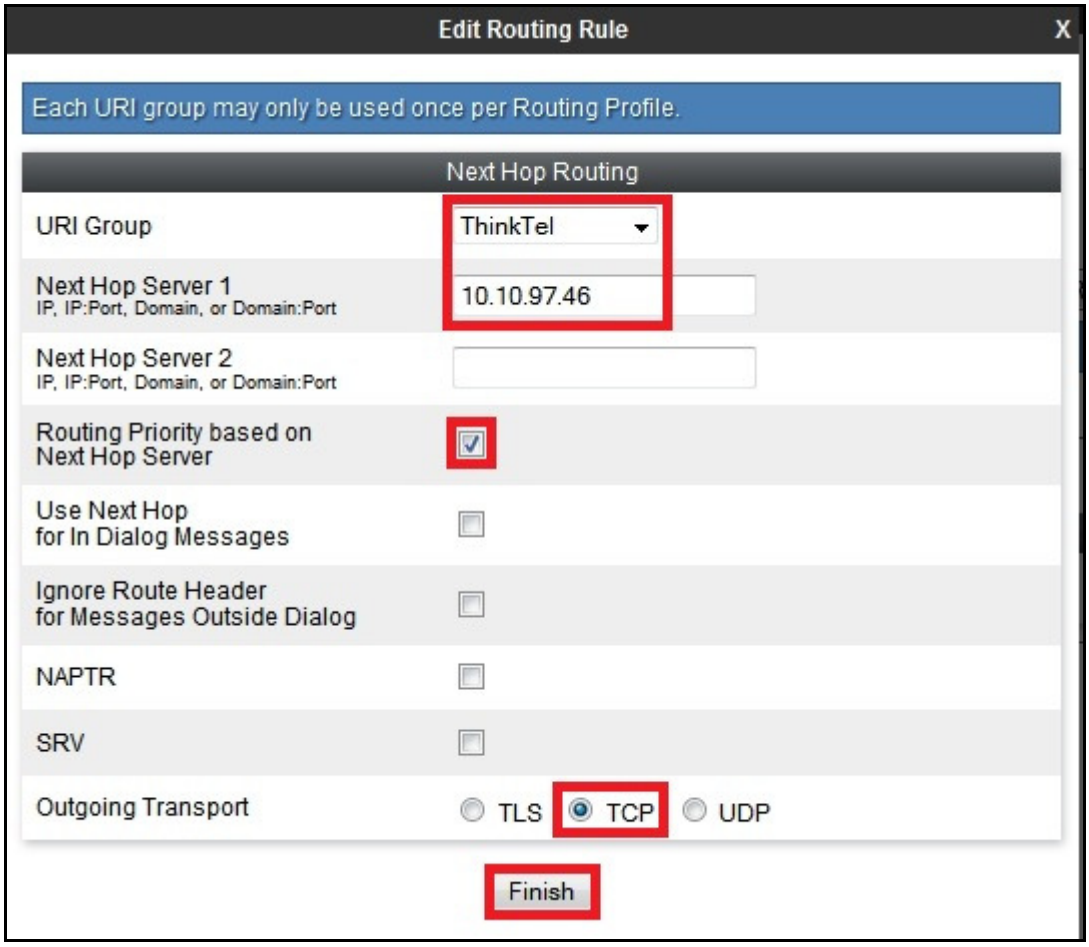
6.2.2.1 Routing Profile for ThinkTel

To display **Edit Routing Rule** dialog of Routing profile **To_ThinkTel**, select **Global Profiles → Routing**: **To_ThinkTel**. As shown in the screenshot below, if there is a match in the SIP domain of the "To" header with the URI Group **ThinkTel** defined in **Section 6.2.1**, outgoing calls will be routed to **Next Hop Server 1** defined as **10.20.250.100** which is the IP address of ThinkTel Trunk Server, on implied default port **5060**. As shown in **Figure 1**, ThinkTel SIP Trunking Service was connected with transportation protocol **UDP**. The other options were kept as default.



6.2.2.2 Routing Profile for Avaya IP Office

Similarly, Routing profile **To_IPO** was created to route incoming calls to the **Next Hop Server 1** as defined as **10.10.97.46** which is the IP address of IP Office, on implied default port **5060** if there is a match on the SIP domain of the "To" header with the URI Group **ThinkTel** defined in **Section 6.2.1**. As shown in **Section 5.5.2**, IP Office was connected with transportation protocol **TCP**.
To display **Edit Routing Rule** dialog of Routing profile **To_IPO**, select **Global Profiles → Routing**: **To_IPO** then click **Edit** (not shown).



Note: The **Routing Priority based on Next Hop Server** was checked to use default settings.

6.2.3 Topology Hiding

Topology Hiding is a security feature of Avaya SBCE which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

To create Topology Hiding profile, select **Global Profiles → Topology Hiding** then click **Add** button (not shown).

In the compliance testing, two Topology Hiding profiles were created: **To_ThinkTel** and **To_IPO**.

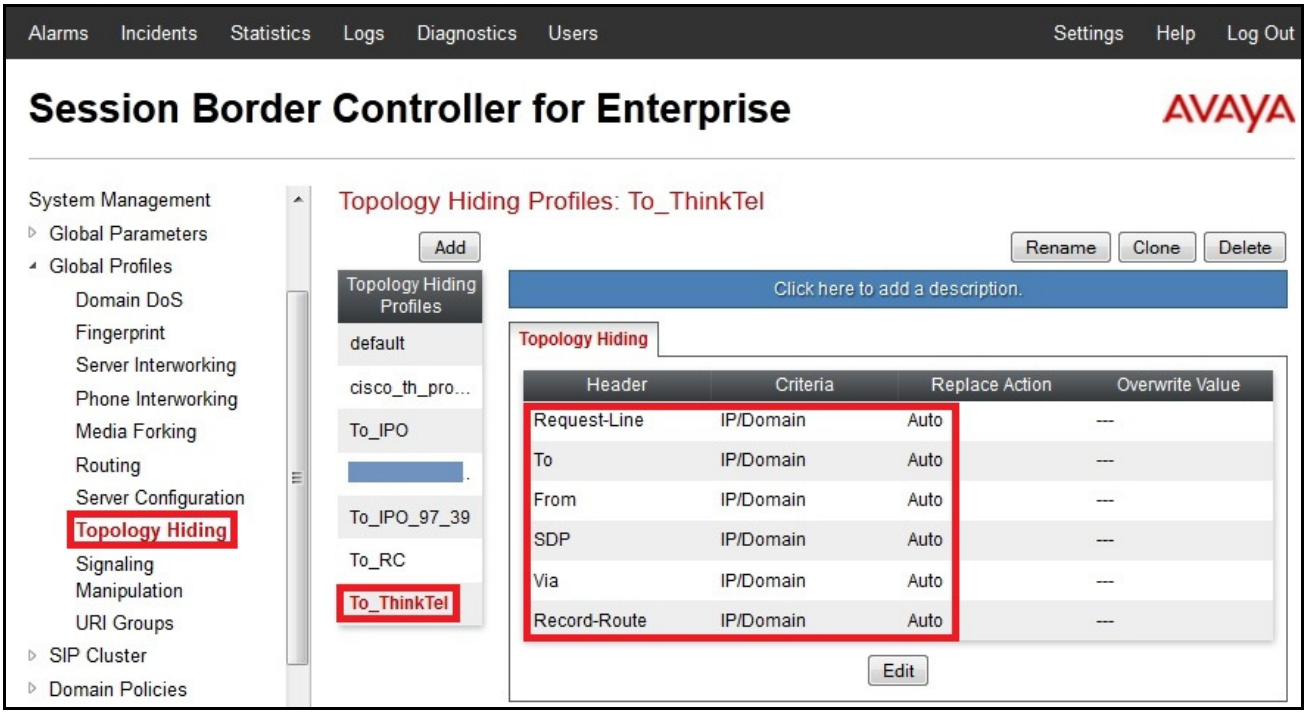
6.2.3.1 Topology Hiding Profile for ThinkTel

Topology Hiding profile **To_ThinkTel** was defined for outgoing calls to ThinkTel:

- Mask URI-Host of the "**Request-Line**" and "**To**" headers with service provider SIP domain **10.20.206.80** to meet the requirements of ThinkTel. This can be done by selecting **Auto** for **Replace Action** setting.
- Mask URI-Host of the "**From**" header CPE SIP domain with the outside IP address of Avaya SBCE, i.e., **10.10.98.106**. This can be done by selecting **Auto** for **Replace Action** setting.
- Change the "**Record-Route**", "**Via**" headers and "**SDP"** added by IP Office, with the outside IP address of Avaya SBCE which is known to ThinkTel.

This implementation is to secure the enterprise network topology and also to meet SIP requirements from service provider.

The screenshots below illustrate Topology Hiding profile **To_ThinkTel**.

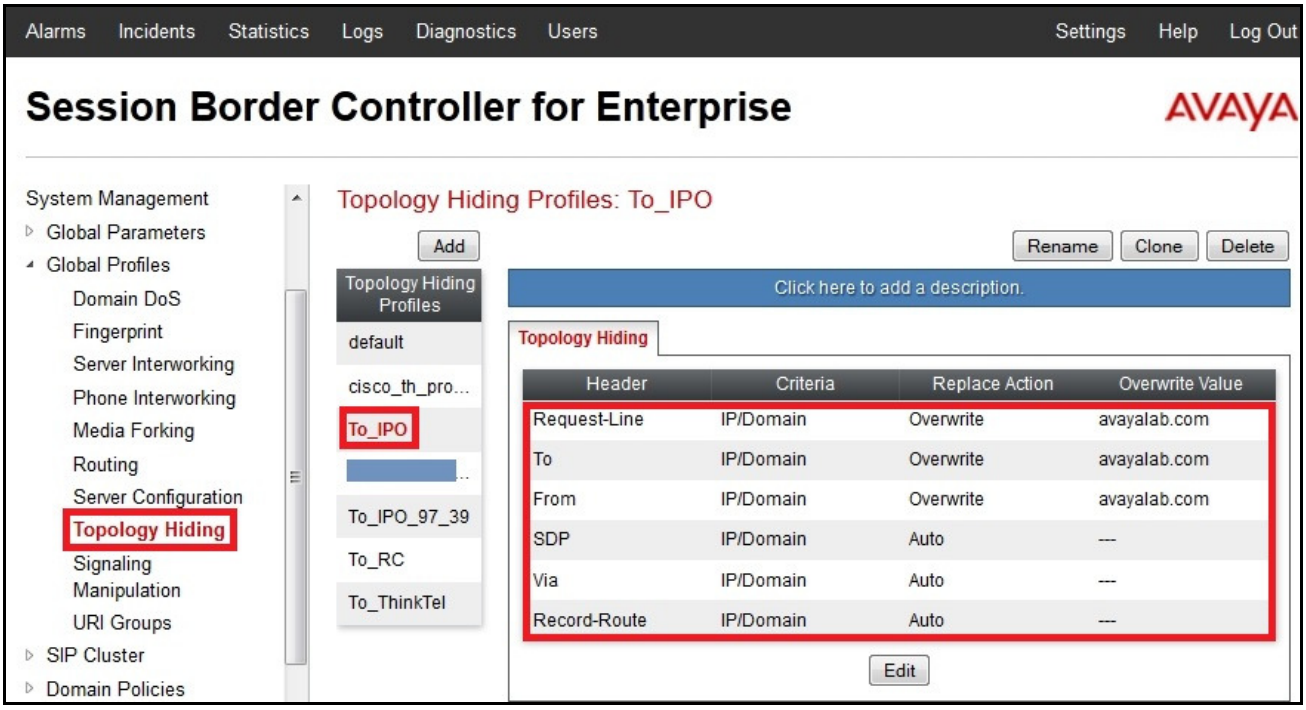


6.2.3.2 Topology Hiding Profile for IP Office

Topology Hiding profile **To_IPO** was defined for incoming calls to IP Office:

- Mask URI-Host of the "**Request-Line**", "**To**", and "**From**" headers with the enterprise SIP domain **avayalab.com**.
- Change the "**Record-Route**", "**Via**" headers and "**SDP**" added by ThinkTel with the inside IP address of Avaya SBCE which is known to IP Office.

The screenshots below illustrate Topology Hiding profile **To_IPO**.



Notes:

- **Criteria** should be **IP/Domain** to allow Avaya SBCE to mask both domain name and IP address presenting in the URI-Host.
- Masking applies to the "**From**" header also applies to the "Referred-By" and "P-Asserted-Identity" headers.
- Masking applies to the "**To**" header also applies to "Refer-To" headers.

6.2.4 Server Interworking

Server Interworking profile features are configured differently for Call Server and Trunk Server. To create Server Interworking profile, select **UC-Sec Control Center → Global Profiles → Server Interworking** then click **Add** button (not shown).

In the compliance testing, two Server Interworking profiles **ThinkTel** and **IPO** were created for ThinkTel (Trunk Server) and IP Office (Call Server).

6.2.4.1 Server Interworking Profile for ThinkTel

Server Interworking profile **ThinkTel** was defined to match SIP specification of ThinkTel. **General** and **Advanced** tabs were configured with following parameters while other tabs **Timers, URI Manipulation** and **Header Manipulation** were kept as default.

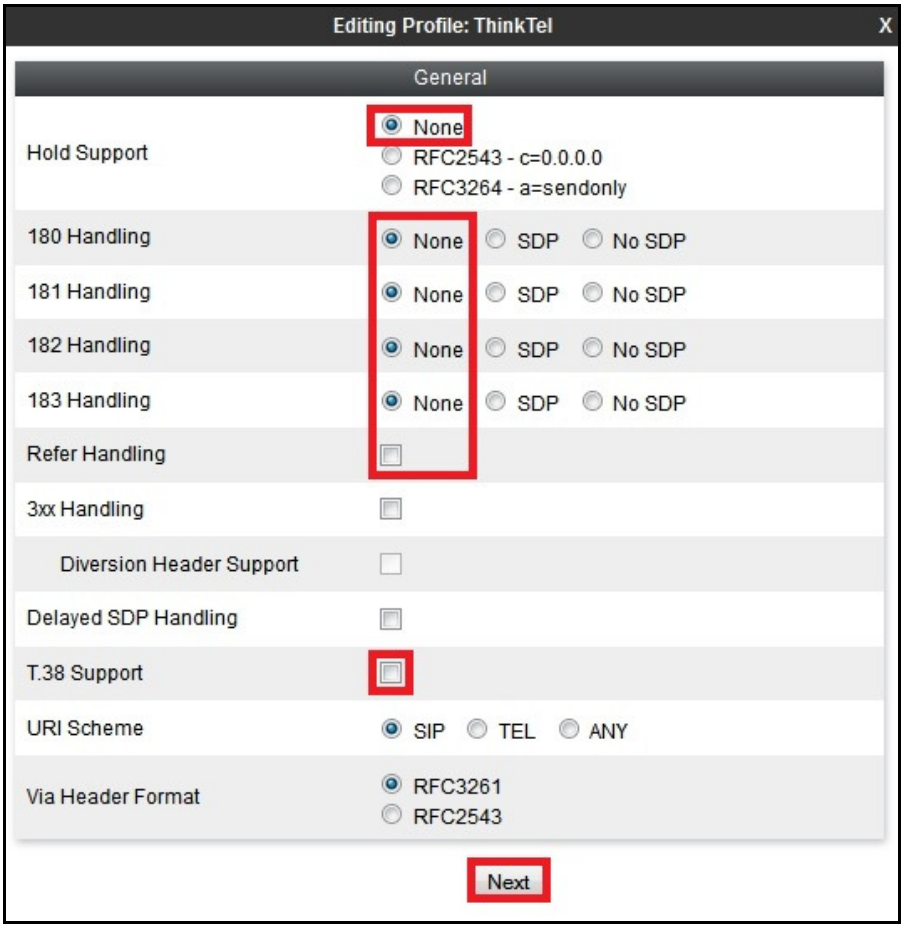
General settings:

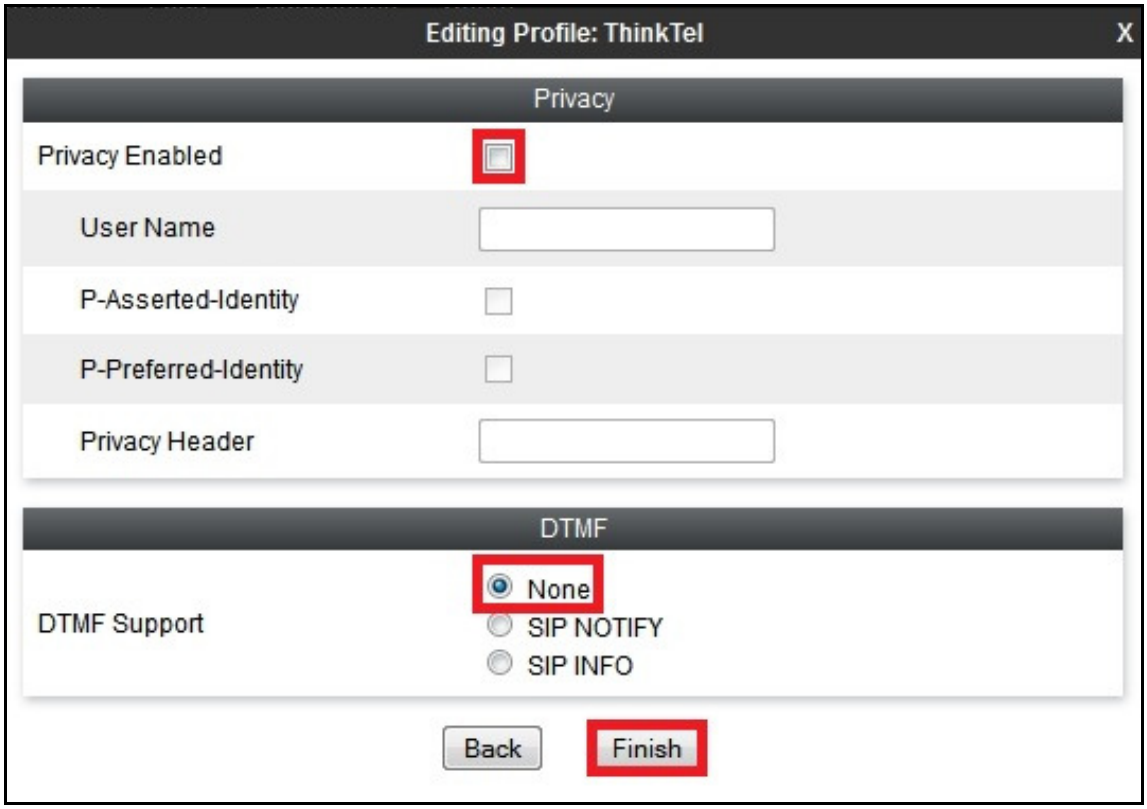
- **Hold Support = None**.
- **18X Handling = None**.
- **Refer Handling = Unchecked**.
- **T.38 Support = Unchecked**. ThinkTel did not supported T.38 fax in the compliance testing.
- **Privacy Enabled = Unchecked**.
- **DTMF Support = None**.

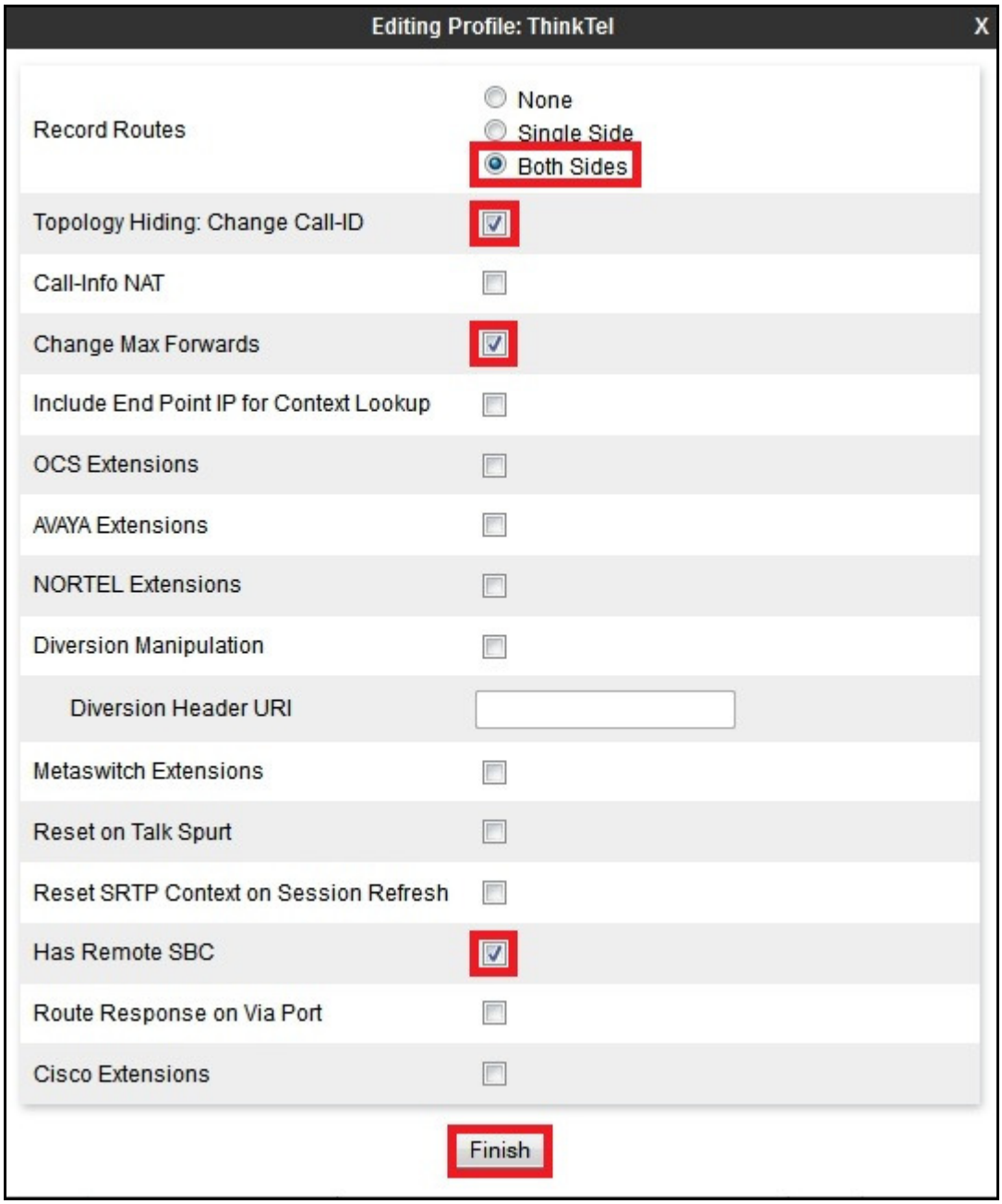
Advanced settings:

- **Record Routes = Both Sides**.
- **Topology-Hiding**: **Change Call-ID = Checked**.
- **Change Max-Forwards = Checked**.
- **Has Remote SBC = Checked**.

Server Interworking profile **ThinkTel** is shown in the following screenshots.

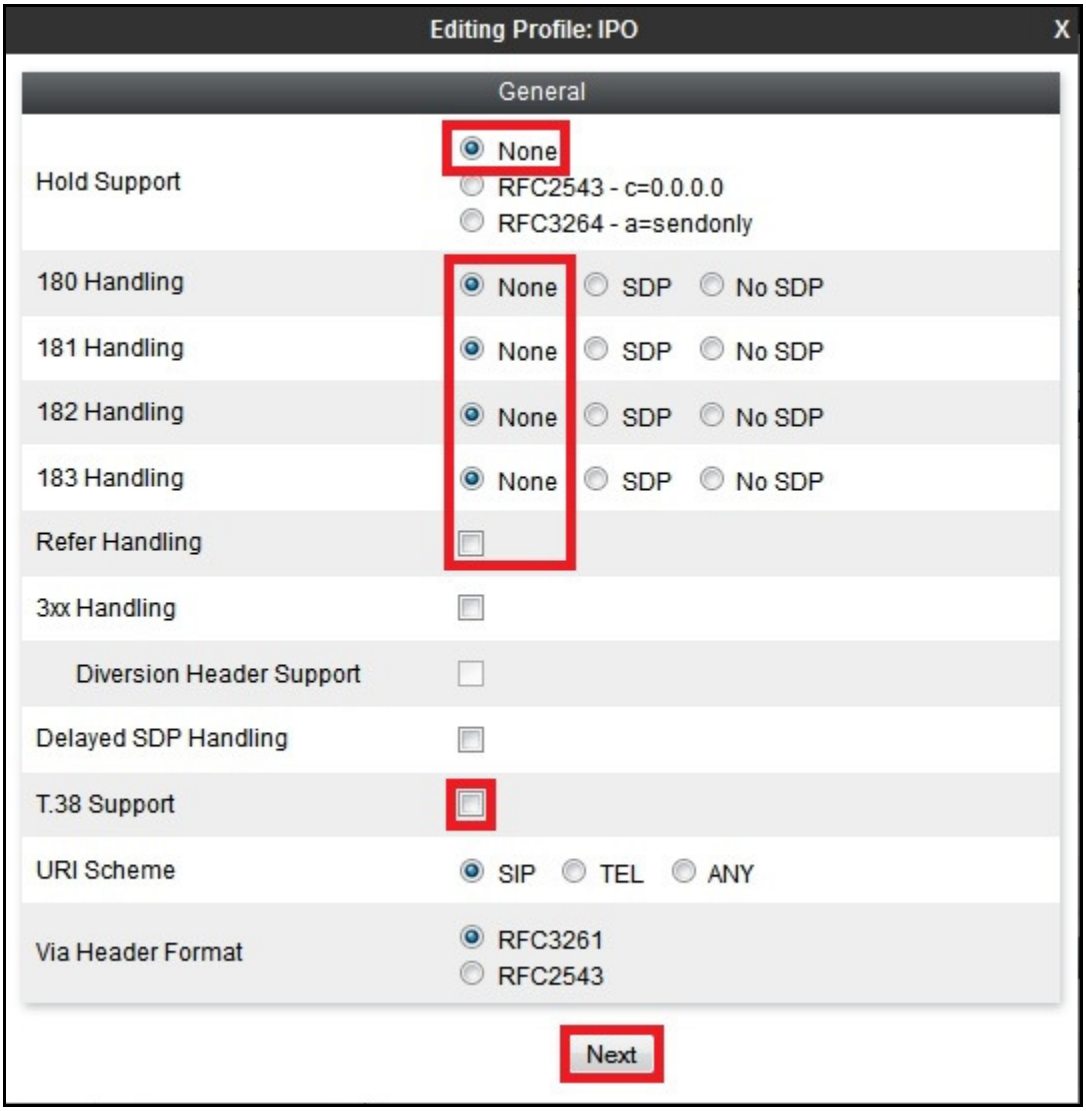


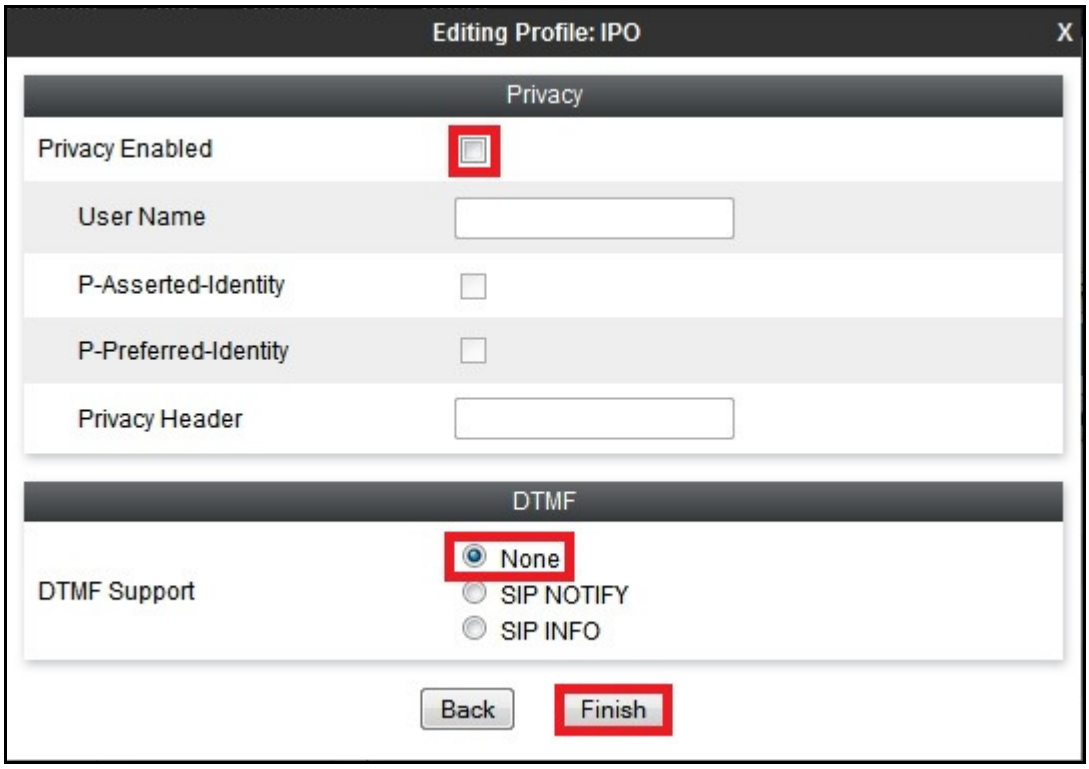


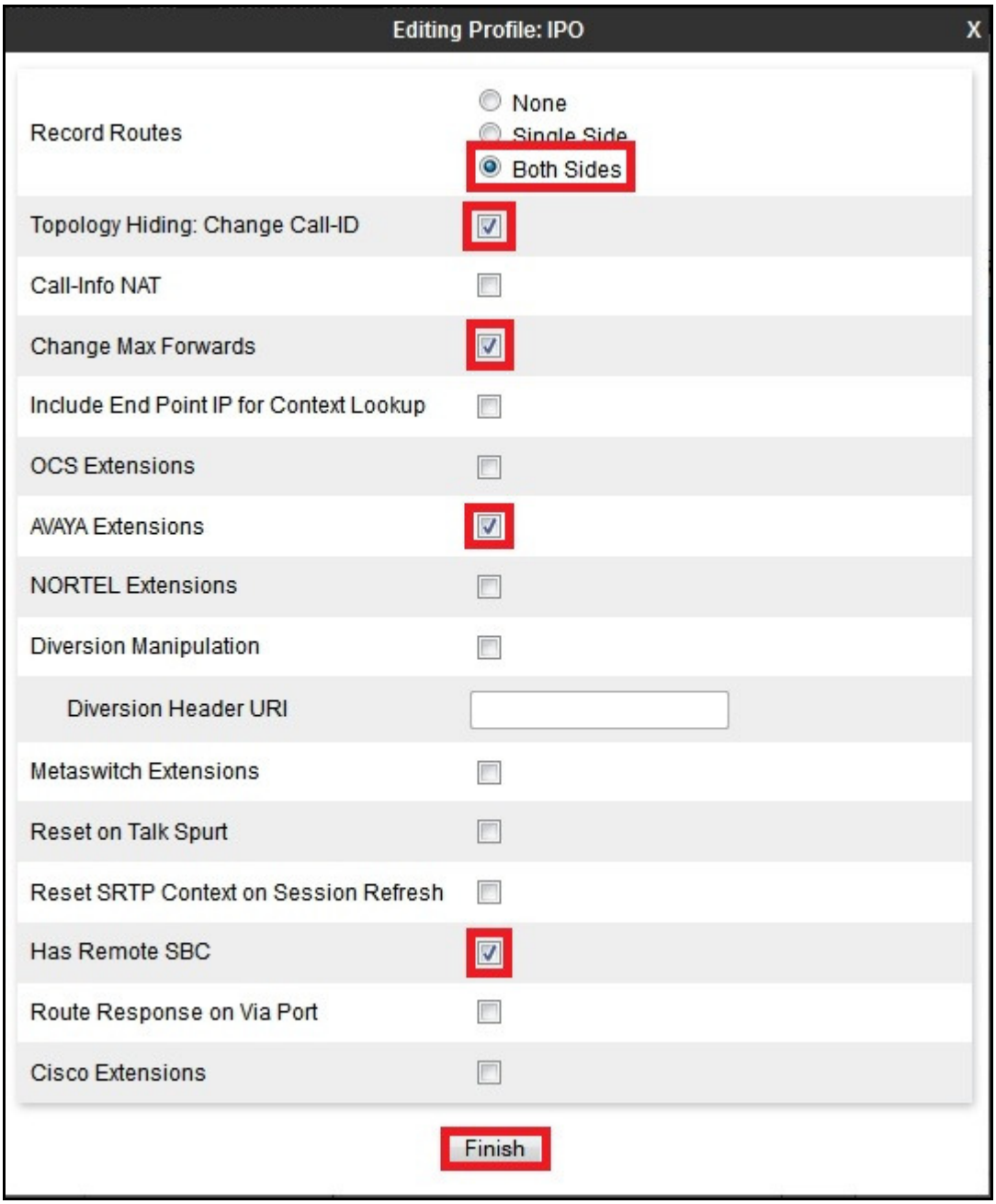


6.2.4.2 Server Interworking Profile for IP Office

Server Interworking profile **IPO** shown in the screenshots below, was similarly defined to match the specification of IP Office with the exception of the support for **Avaya Extensions** was enabled.







6.2.5 Server Configuration

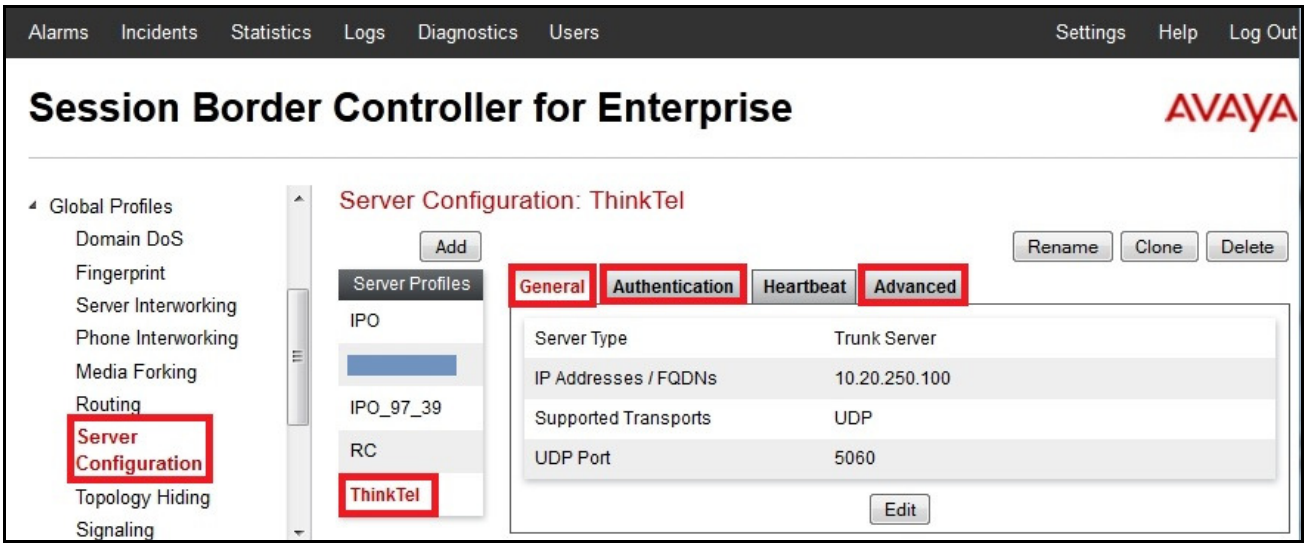
Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create Server Configuration, select **Global Profiles →Server Configuration** then click **Add** button (not shown).

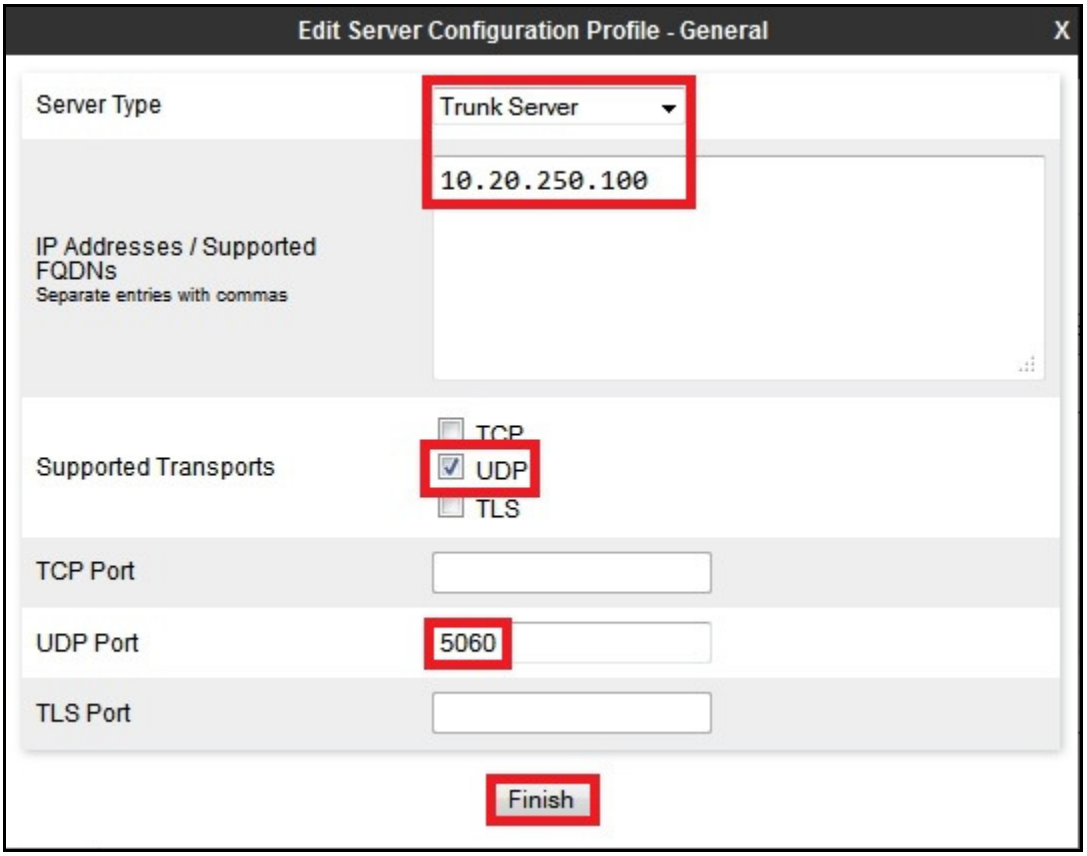
In the compliance testing, two separate Server Configurations were created, server entry **ThinkTel** for ThinkTel and server entry **IPO** for IP Office.

6.2.5.1 Server Configuration for ThinkTel

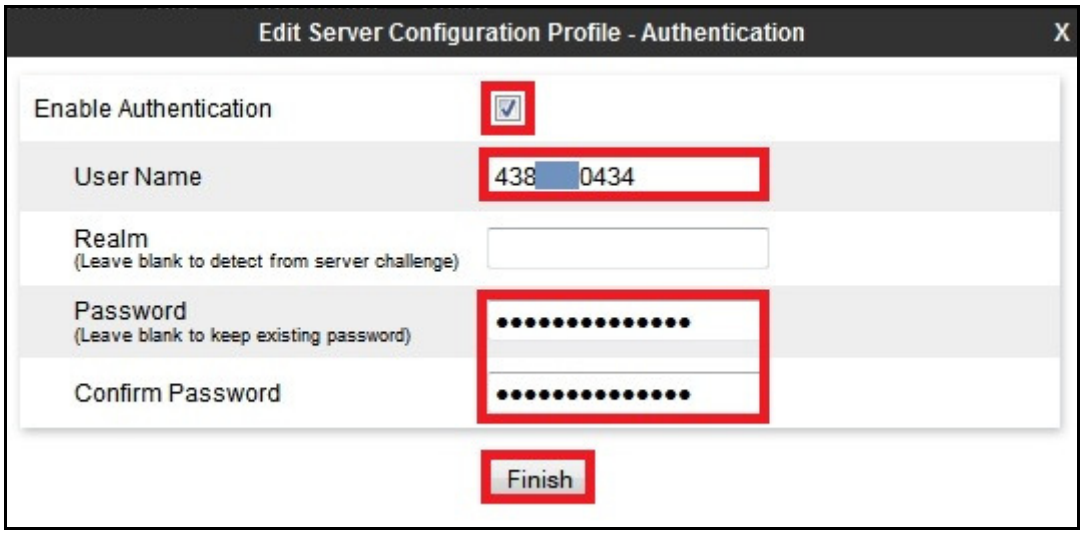
Server Configuration **ThinkTel** was added for ThinkTel, it is discussed in detail below. **General**, **Authentication** and **Advanced** tabs were provisioned. **Heartbeat** tab, however, was disabled as default to allow Avaya SBCE to forward the OPTIONS heartbeat originated from IP Office to ThinkTel (to query for the status of the SIP Trunk).



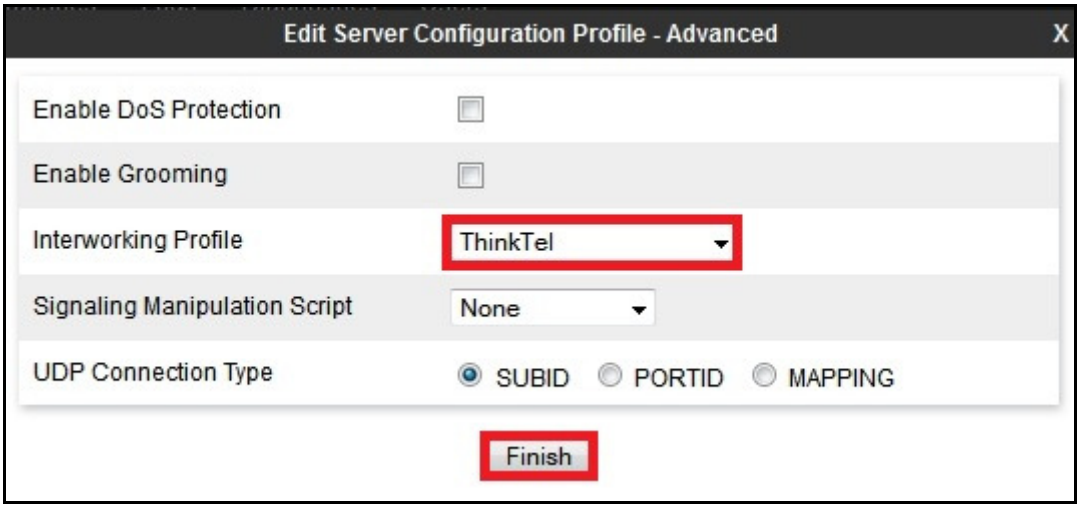
Under **General** tab, specify Server Type for ThinkTel as **Trunk Server**. IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, ThinkTel supported transport protocol **UDP** on IP address **10.20.250.100** and listened on port **5060**.



Authentication tab was configured with **Enable Authentication** selected to allow Avaya SBCE to provide proper credential for Digest Authentication implemented by ThinkTel. Keep **Realm** field as as default blank, but configure the credential which was obtained from service provider, with **User Name 438XXX0434** and predefined **Password** for the compliance testing.

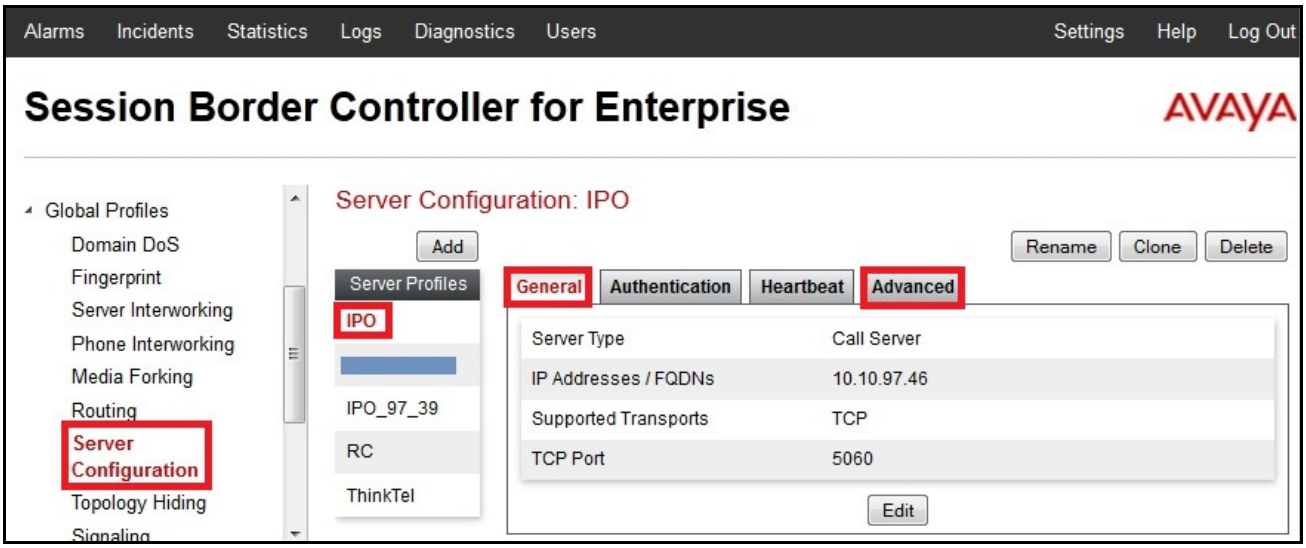


For **Advanced** tab, Interworking Profile was set to use **ThinkTel** as defined in **Section 6.2.4.1**. Other settings were kept as default.

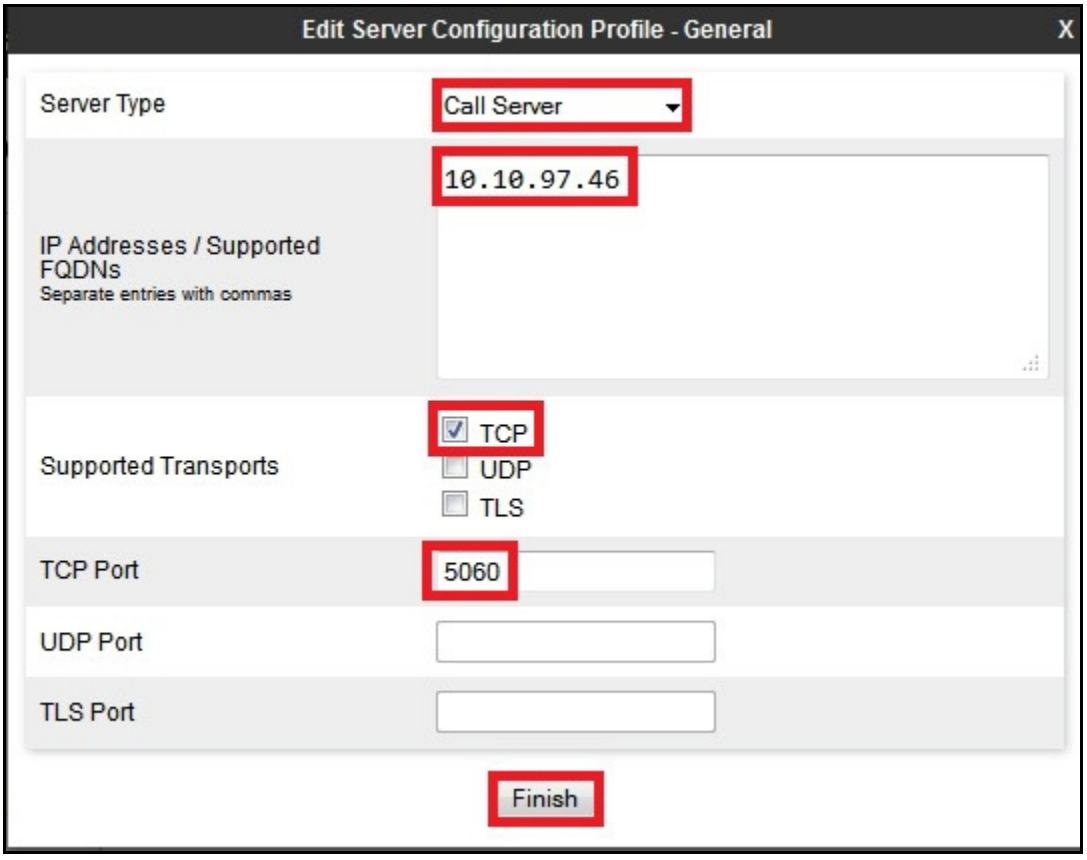


6.2.5.2 Server Configuration for Avaya IP Office

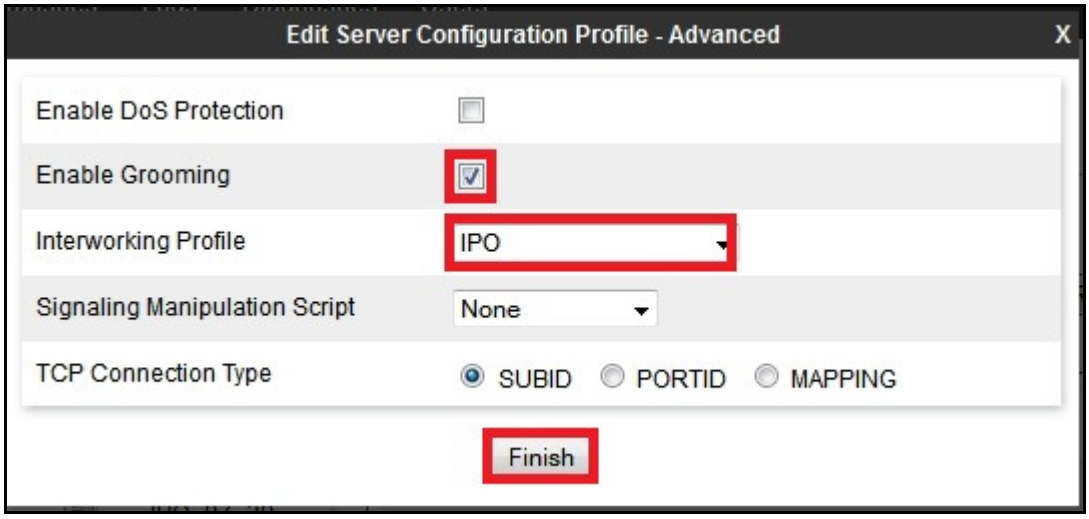
Server Configuration **IPO** was similarly created for IP Office, and is discussed in detail below. Only **General** and **Advanced** tabs required provisioning. **Heartbeat** tab was kept disabled as default to allow Avaya SBCE to forward the OPTIONS heartbeat from ThinkTel to IP Office (to query for the status of the SIP Trunk).



Under **General** tab, specify Server Type as **Call Server**. IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, IP Office was configured with transport protocol **TCP** on IP address **10.10.97.46** and listens on port **5060**.



For **Advanced** tab, select Interworking Profile **IPO** as defined in **Section 6.2.4.2** and **Enable Grooming** was enabled. Other settings were kept as default.



6.3 Domain Policies

Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

6.3.1 Application Rules

Application Rules define which types of SIP-based applications Avaya SBCE security device will protect: voice, video, and/or instant messaging (IM). In addition, it is possible to configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

For the certification testing, Application Rule was created to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

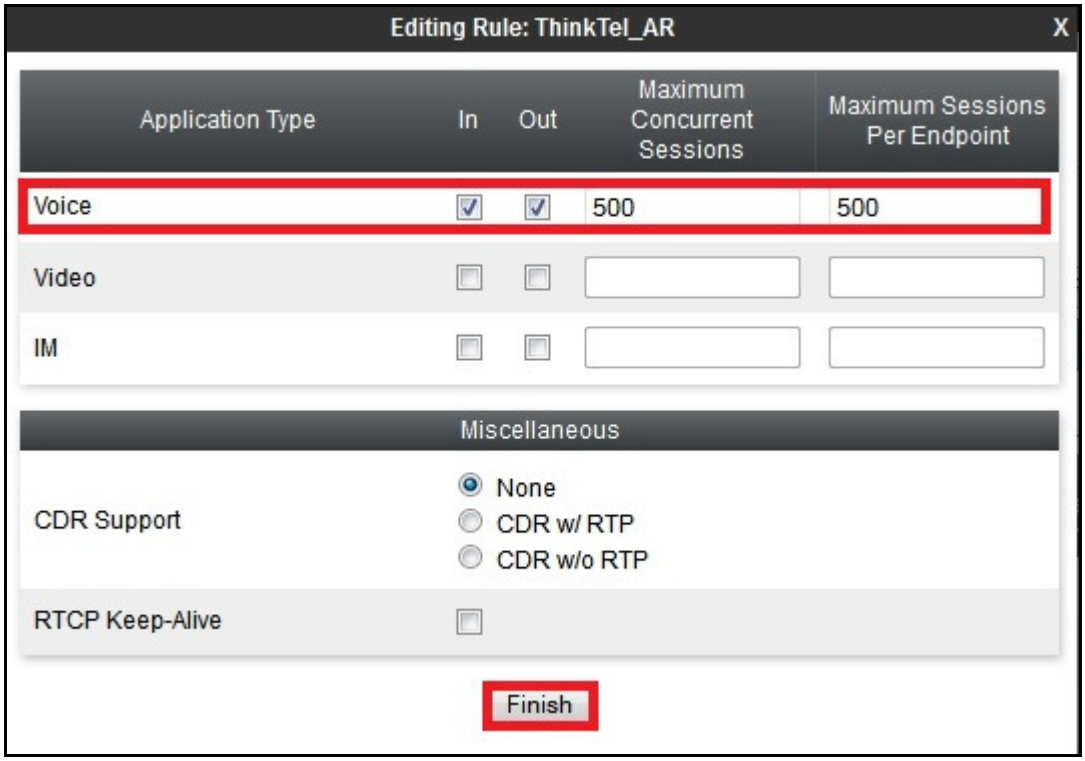
In the compliance testing, two **Application Rules** were created for ThinkTel and IP Office.

6.3.1.1 Application Rule for ThinkTel

To clone Application Rule, navigate to **Domain Policies → Application Rules**, select **default** rule then click **Clone** button (not shown).

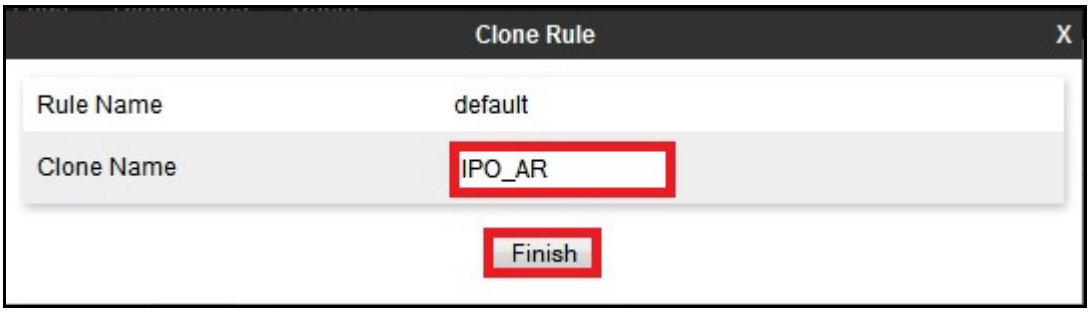
Enter a descriptive name, e.g., **ThinkTel_AR** for the new rule then click **Finish** button.

Click **Edit** button (not shown) to modify the rule. Set **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for **Voice** application to a value high enough for the amount of traffic the network is able to process. The following screen shows the modified Application Rule with **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** set to **500**. In the compliance testing, IP Office was programmed to control concurrent sessions by setting **Max Calls per Channel** (see **Section 5.5.3**) to the allotted number. Therefore, values in the Application Rule **ThinkTel_AR** were set high enough to be considered non-blocking.

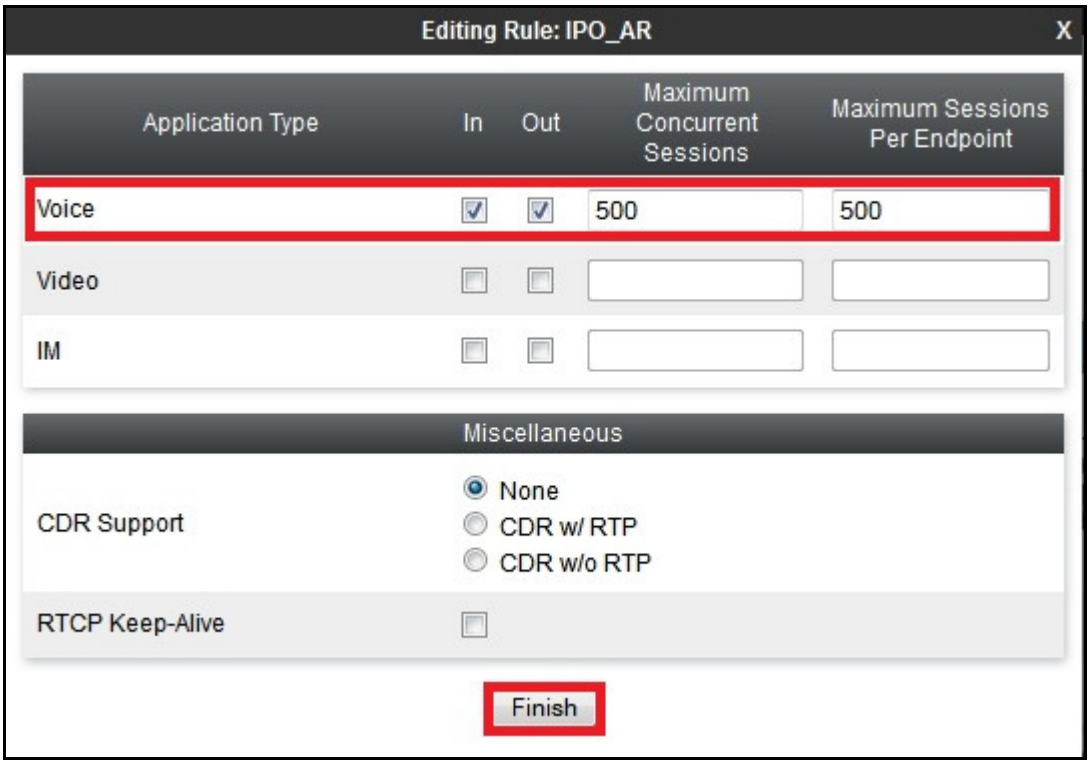


6.3.1.2 Application Rule for IP Office

Clone Application Rule with a descriptive name, e.g., **IPO_AR** for IP Office and click **Finish** button.



The Application Rule **IPO_AR** was similarly configured as shown in the screenshots below.



6.3.2 Media Rules

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

Custom Media Rules were created to set **Quality of Service** and **Media Anomaly Detection**. In the compliance testing, two **Media Rules** were created for ThinkTel and IP Office.

6.3.2.1 Media Rule for ThinkTel

To create **Media Rule**, navigate to **Domain Policies → Media Rules**, select **default-low-med** rule then click **Clone** button (not shown).

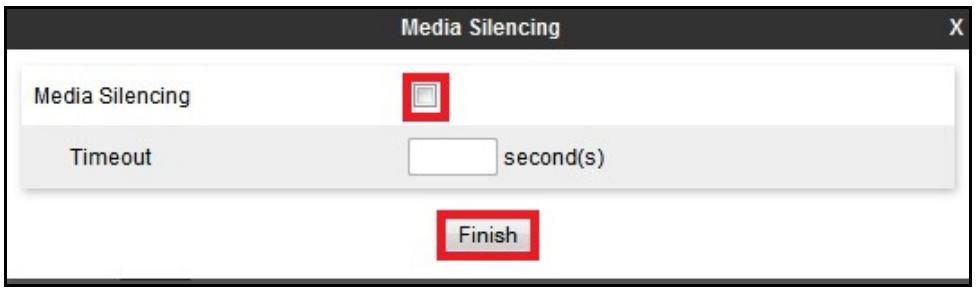
Enter a descriptive name, e.g., **ThinkTel_MR** for the new rule then click **Finish** button.

When RTP changes while active call is in progress, Avaya SBCE interprets this as an anomaly and alerts will be created in **Incidents Log**. Thus, disabling **Media Anomaly Detection** could prevent RTP Injection Attack alerts from being created in the log.

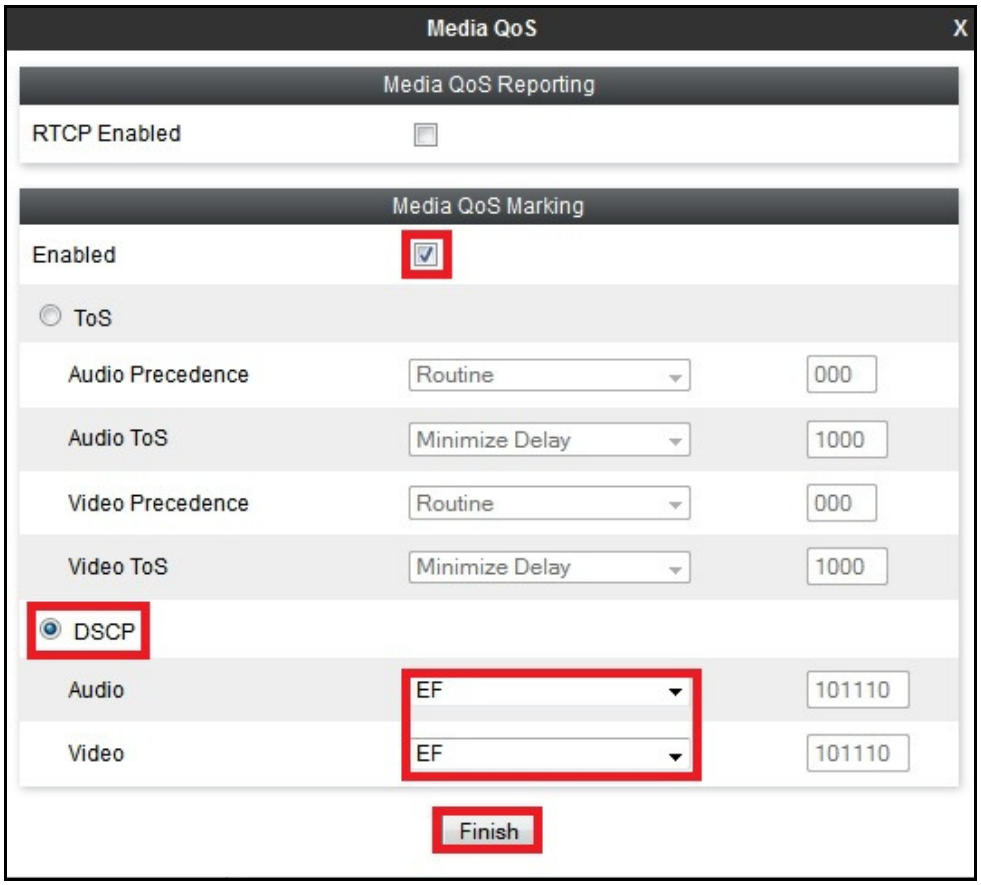
To modify Media Anomaly, select **Media Anomaly** tab and click **Edit** button (not shown). Then uncheck **Media Anomaly Detection** and click **Finish** button.

Media Silencing feature detects the silence while active call is in progress. If the silence is detected and exceeds an allowed duration, Avaya SBCE generates alerts in **Incidents Log**. In the compliance testing, Media Silencing detection was disabled to prevent the call from unexpectedly disconnected due to RTP packet lost on the public internet.

To modify Media Silencing, select **Media Silencing** tab and click **Edit** button (not shown). Then uncheck **Media Silencing** and click **Finish** button.

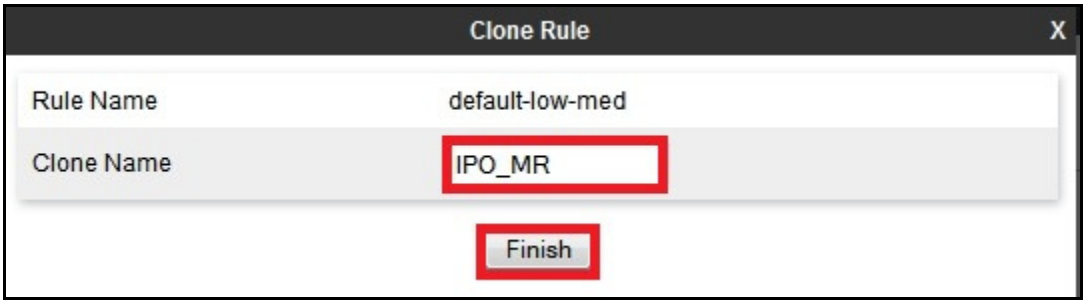


Under **Media QoS** tab, click **Edit** button (not shown) to configure Quality of Service (QoS). Avaya SBCE can be configured to mark Differentiated Services Code Point (DSCP) in IP packet header with specific values to support Quality of Services policy for media. The following screen shows QoS values used for the compliance testing.



6.3.2.2 Media Rule for IP Office

Clone a Media Rule with a descriptive name, e.g., **IPO_MR** for IP Office then click **Finish** button.



Media Rule **IPO_MR** was similarly configured for **Media Anomaly**, **Media Silencing** and **Media QoS** (not shown).

6.3.3 Signaling Rules

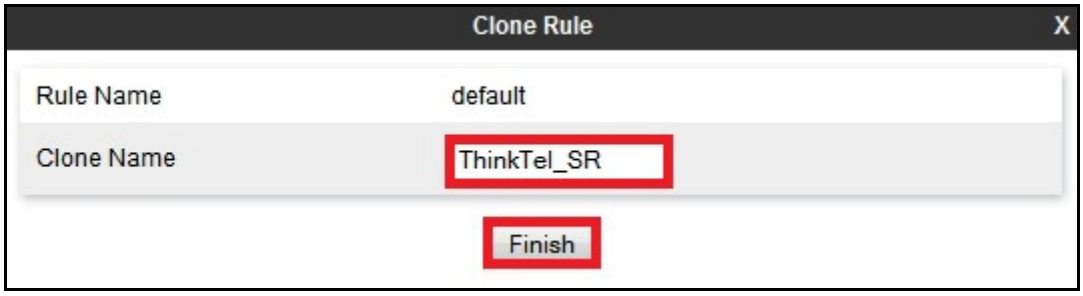
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and "pattern-matched" against particular signaling criteria defined by these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

To clone Signaling Rule, navigate to **Domain Policies → Signaling Rules**, select **default** rule then click **Clone** button (not shown).

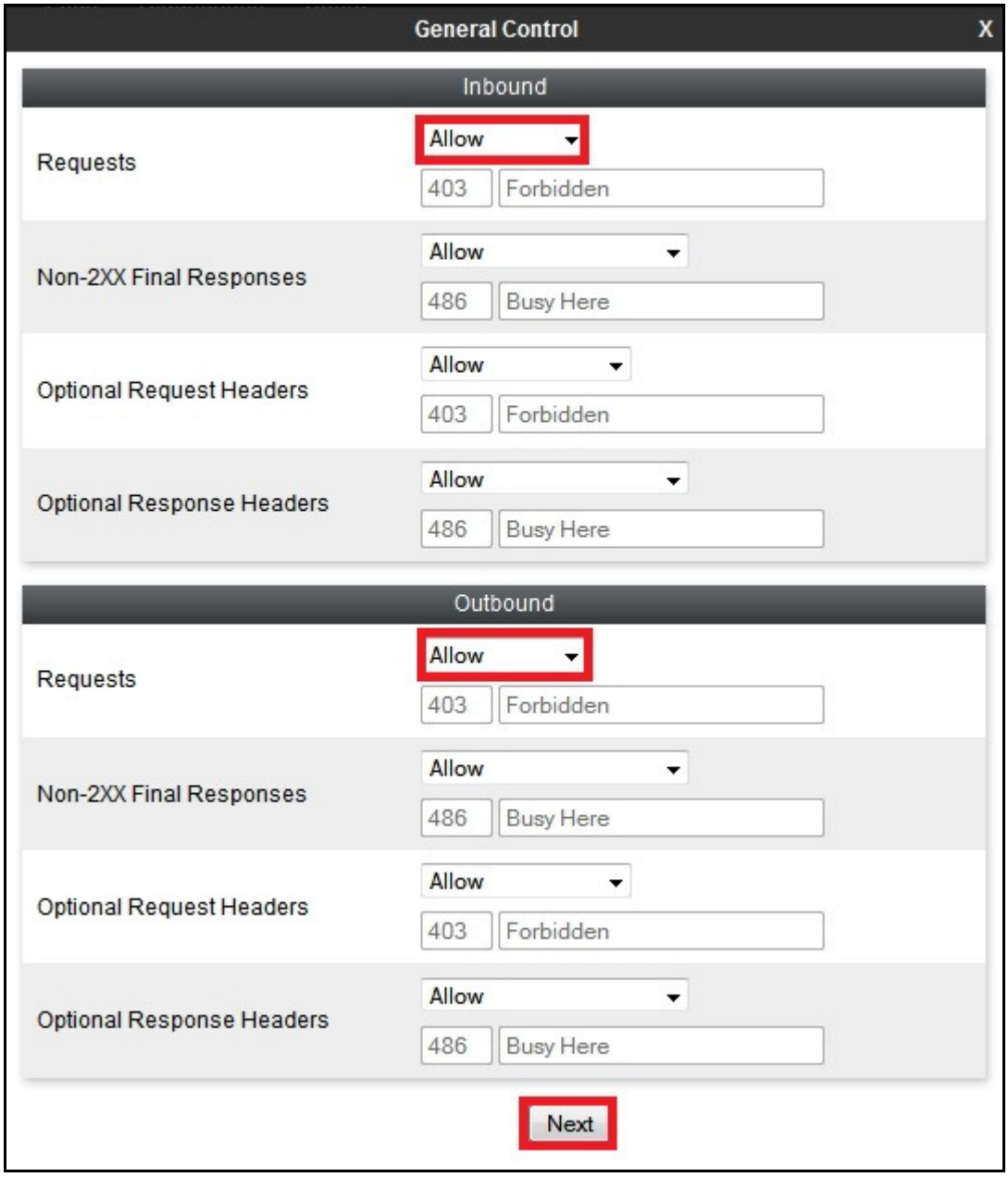
In the compliance testing, two **Signaling Rules** were created for ThinkTel and IP Office.

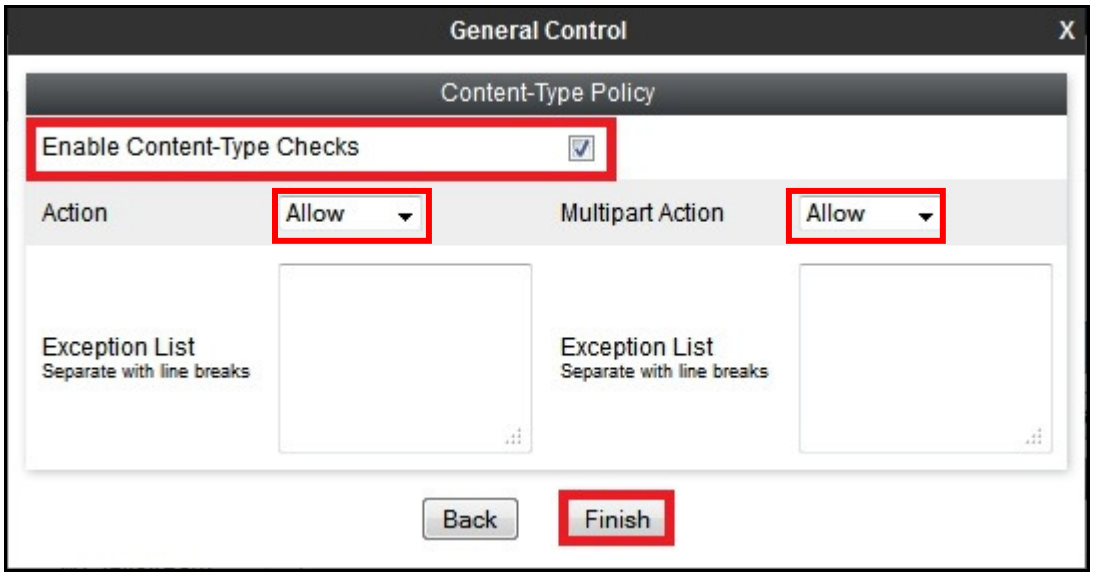
6.3.3.1 Signaling Rule for ThinkTel

Clone Signaling Rule with a descriptive name, e.g., **ThinkTel_SR** and click **Finish** button.



Cloning from Signaling Rule default, verify that **General** settings of **ThinkTel_SigR** with **Inbound** and **Outbound Requests** were set to **Allow**, and **Enable Content-Type Checks** was enabled with **Action** and **Multipart-Action** were set to **Allow** as shown in the following screenshots.

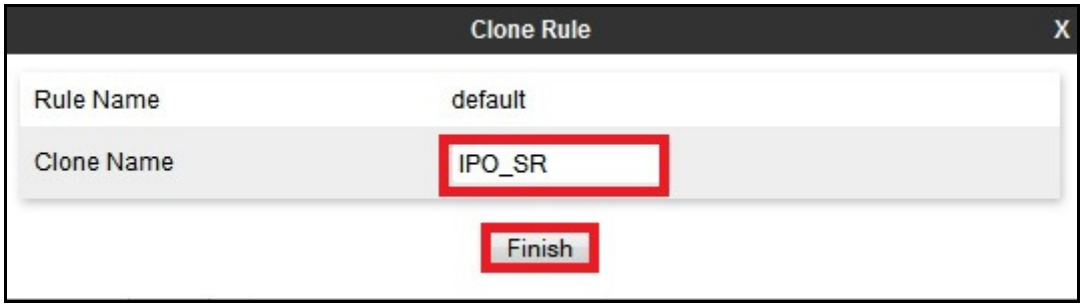




For **Signaling QoS** tab, select proper Quality of Service (QoS). Avaya SBCE can be configured to mark Differentiated Services Code Point (DSCP) in IP packet header with specific values to support Quality of Services policies for signaling. The following screen shows QoS values used for the compliance testing.

6.3.3.2 Signaling Rule for IP Office

Clone Signaling Rule with a descriptive name, e.g., **IPO_SR** for IP Office then click **Finish** button.



Signaling Rule **IPO_SR** was similarly configured for **General** and **Signaling QoS** settings.

6.3.4 Endpoint Policy Groups

The rules created within Domain Policy section are assigned to Endpoint Policy Group which is then applied to Server Flow defined in **Section 6.4.4**.

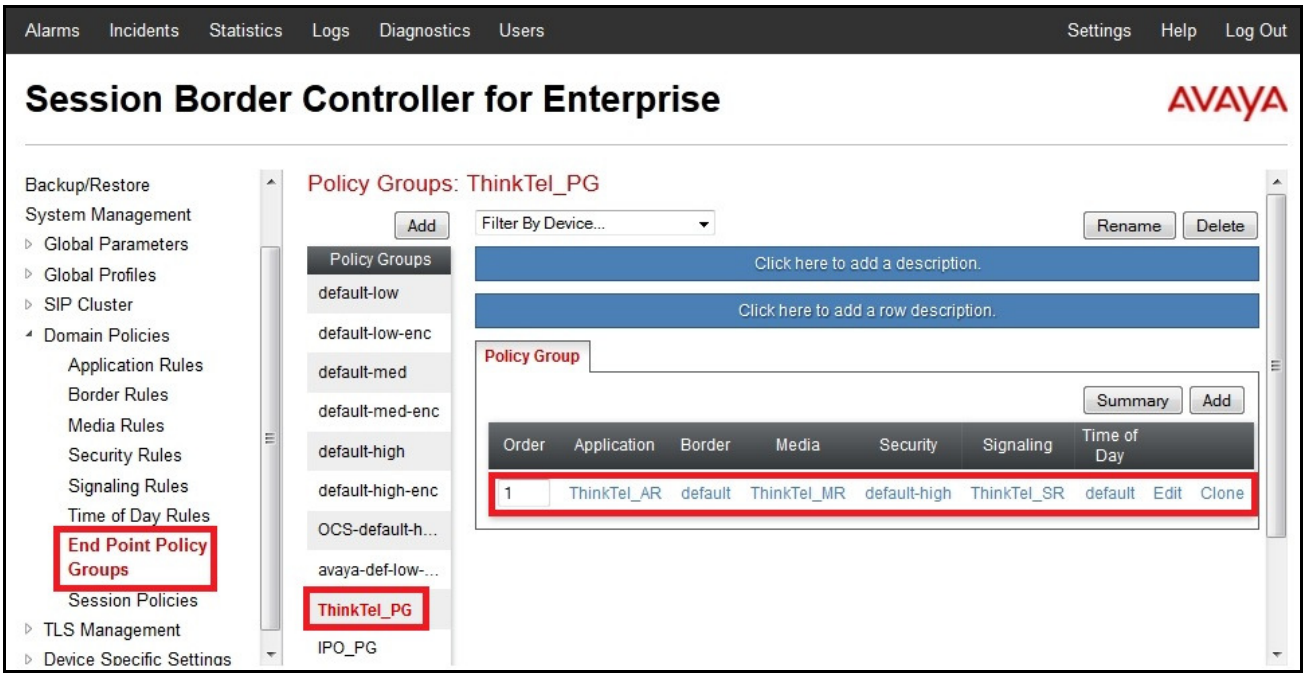
Endpoint Policy Groups were separately created for ThinkTel and IP Office.

To create Policy Group, navigate to **Domain Policies → Endpoint Policy Groups** and click **Add** button (not shown).

6.3.4.1 Endpoint Policy Group for ThinkTel

The following screen shows Endpoint Policy Group **ThinkTel_PG** created for ThinkTel.

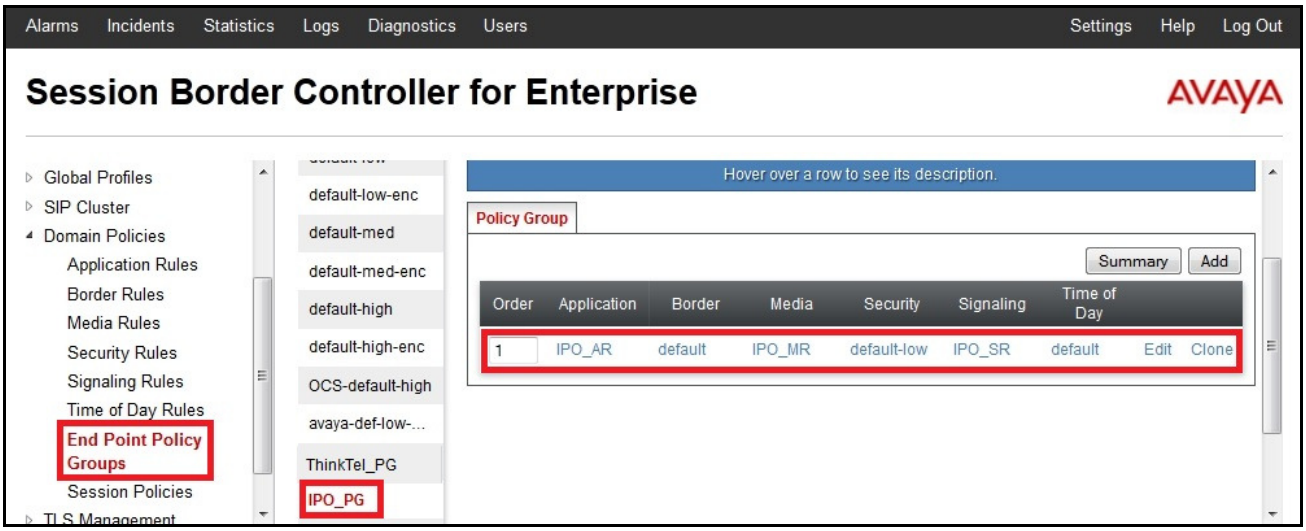
- Set Application Rule to **ThinkTel_AR** which was created in **Section 6.3.1.1**.
- Set Media Rule to **ThinkTel_MR** which was created in and **Section 6.3.2**.1.
- Set Signaling Rule to **ThinkTel_SR** which was created in **Section 6.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.



6.3.4.2 Endpoint Policy Group for IP Office

The following screen shows Endpoint Policy Group **IPO_PG** created for IP Office.

- Set Application Rule to **IPO_AR** which was created in **Section 6.3.1.2**.
- Set Media Rule to **IPO_MR** which was created in and **Section 6.3.2.2**.
- Set Signaling Rule **IPO_SR** which was created in **Section 6.3.3.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.



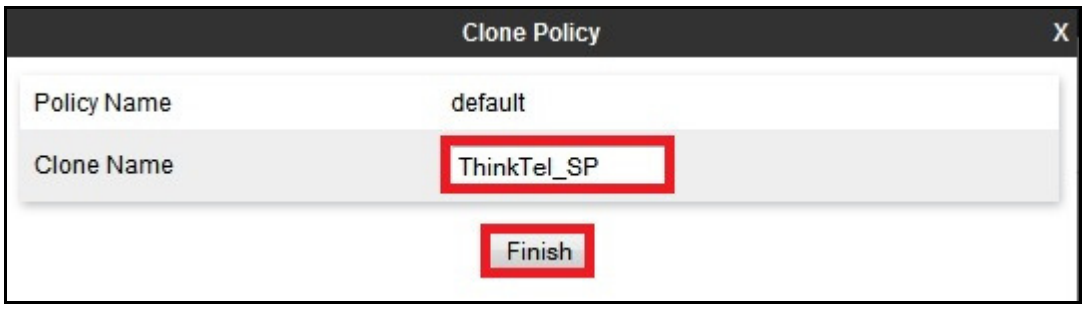
6.3.5 Session Policy

Session Policy is applied based on the source and destination of a media session, i.e., which codec is to be applied to the media session between its source and destination. The source and destination are defined in the URI Group shown in **Section 6.2.1**.

In the compliance testing, Session Policy **ThinkTel_SP** was created to match codec configuration on ThinkTel. The policy also allows Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.

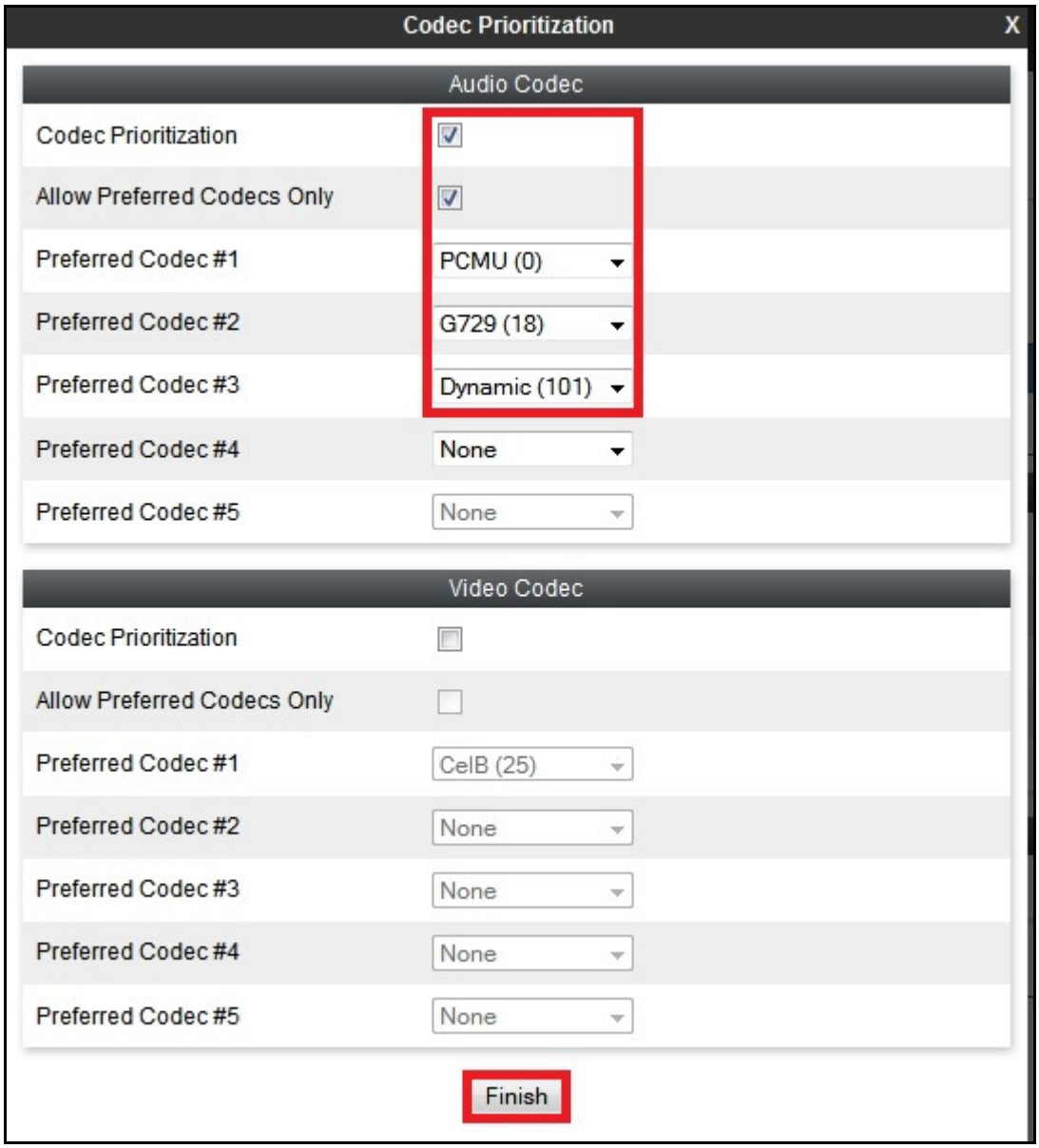
To clone Session Policy which applies to both ThinkTel and IP Office, navigate to **Domain Policies** → **Session Policies**, select **default** rule then click **Clone** button (not shown).

Enter a descriptive name, .e.g., **ThinkTel_SP** for the new policy and click on the **Finish** button.

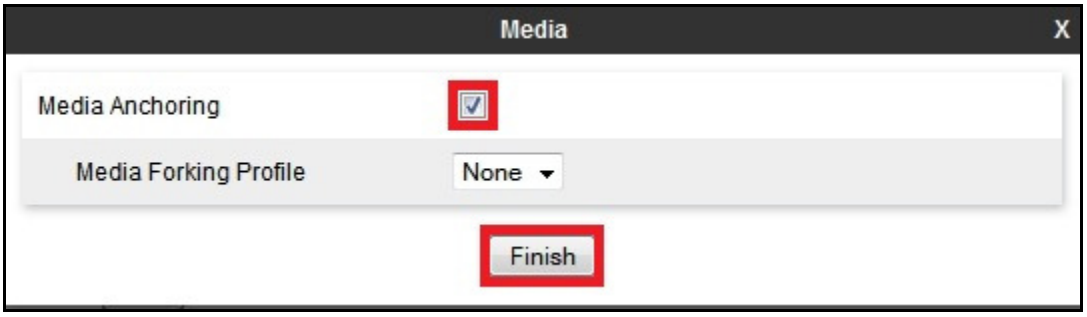


In the compliance testing, even ThinkTel supported G.729 as the first choice and G.711MU as the second choice for RTP, but G.711MU should be set as higher priority on Avaya SBCE to support fax over IP. Otherwise, the fax calls would fail because both ThinkTel and IP Office cannot re-negotiate to change the RTP from using other codec to G.711MU for fax.

To define **Codec Prioritization** for **Audio Codec**, select profile **ThinkTel_SP** created above then click **Edit** button (not shown). Select **Preferred Codec #1** as **PCMU (0)**, **Preferred Codec #2** as **G.729 (18)**, and **Preferred Codec #3** as **Dynamic (101)** for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent the unsupported codec from being sent to both ends.



Under **Media** tab of Session Policy **ThinkTel_SP** created above, click **Edit** button (not shown) then check **Media Anchoring** to allow Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.



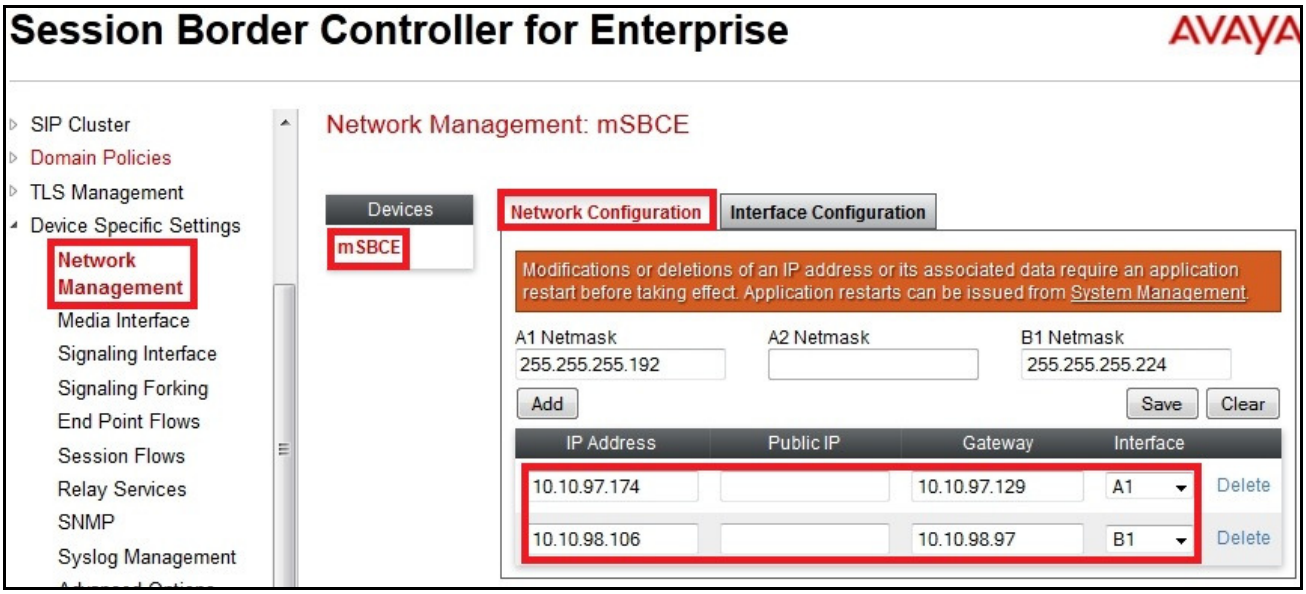
6.4 Device Specific Settings

Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

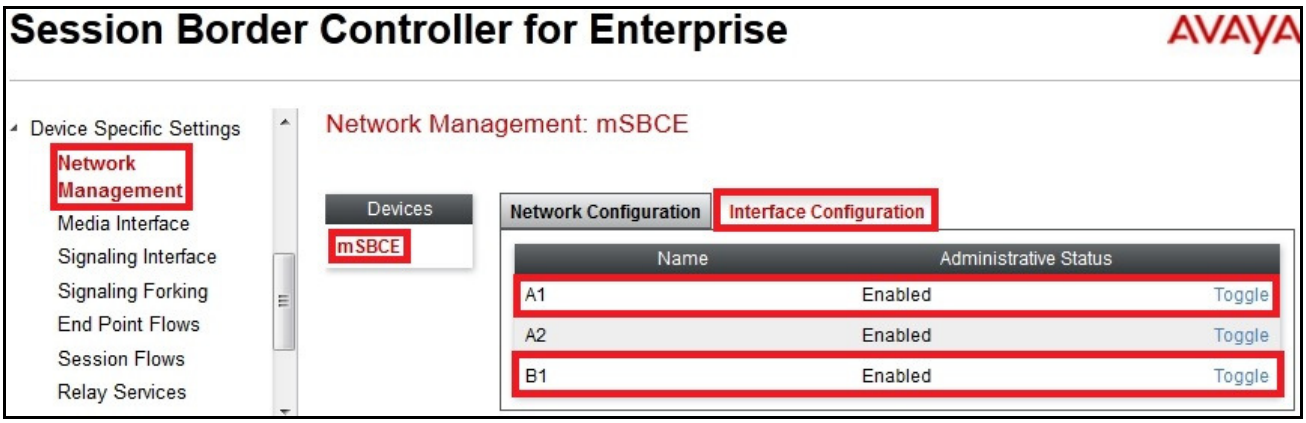
6.4.1 Network Management

Network Management page is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address, public IP address, subnet mask, gateway, etc. to interface the device to the networks. This information populates the various Network Management tabs which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management**, under **Network Configuration** tab, verify IP addresses assigned to the interfaces and that the interfaces were enabled. The following screen shows private interface was assigned to **A1** and public interface was assigned to **B1** appropriate to the parameters shown in the **Figure 1**.



On **Interface Configuration** tab, enable the interfaces connecting to inside enterprise and outside service provider networks. To enable interface, click the appropriate **Toggle State** button. The following screen shows interface **A1** and **B1** were **Enabled**.



6.4.2 Media Interface

Media Interface screen is where media ports are defined. Avaya SBCE will open connection for RTP traffic on the defined ports.

To create **Media Interface**, navigate to **Device Specific Settings → Media Interface** and click **Add** button (not shown).

Two separate Media Interfaces were needed for inside and outside interfaces. The following screen shows Media Interfaces **InsideMedia** and **OutsideMedia** were created for the compliance testing.

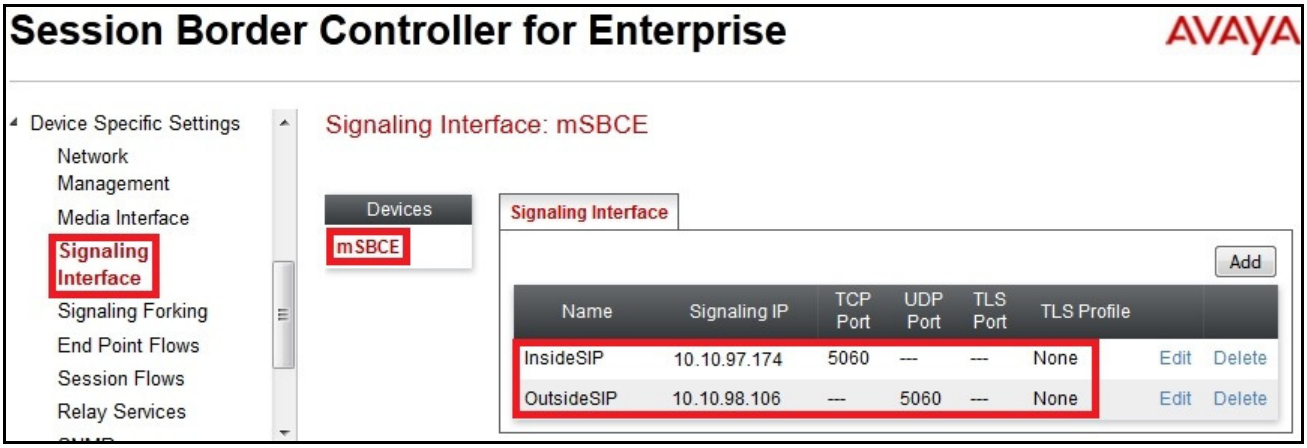
Note: After media interfaces are created, an application restart is necessary before the changes will take effect.

6.4.3 Signaling Interface

Signaling Interface screen is where SIP signaling port is defined. Avaya SBCE will listen for SIP request on the defined port.

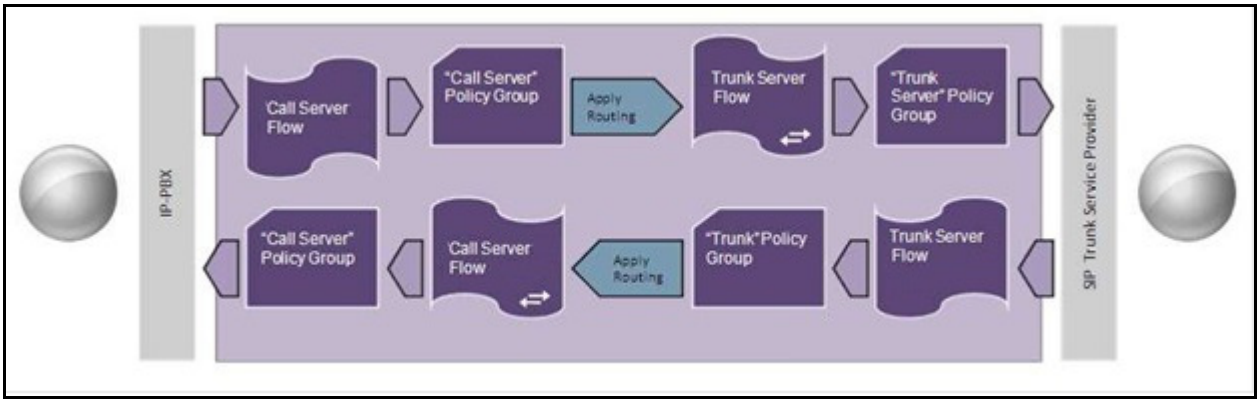
To create **Signaling Interface**, navigate to **Device Specific Settings → Signaling Interface** and click **Add** button (not shown).

Two separate Signaling Interfaces were needed for inside and outside interfaces. The following screen shows Signaling Interfaces **InsideSIP** and **OutsideSIP** were created in the compliance testing with **TCP/5060** and **UDP/5060** respectively configured for inside and outside interfaces.



6.4.4 End Point Flows - Server Flow

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

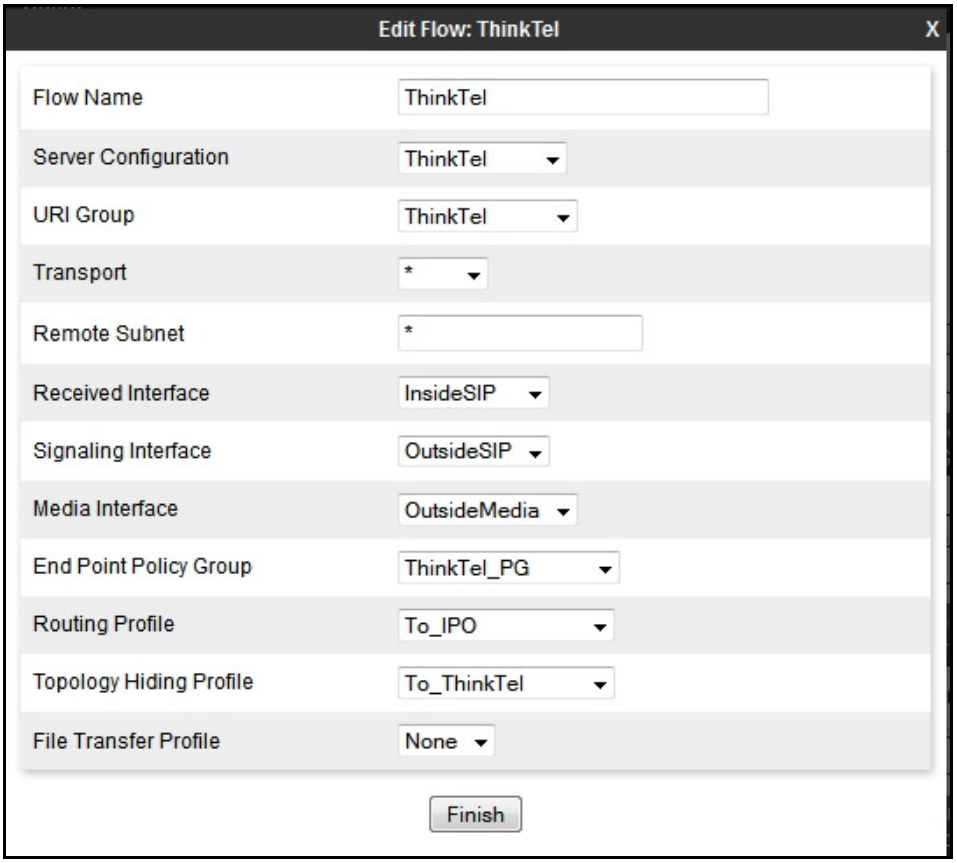


In the compliance testing, two separate Server Flows were created for ThinkTel and IP Office.

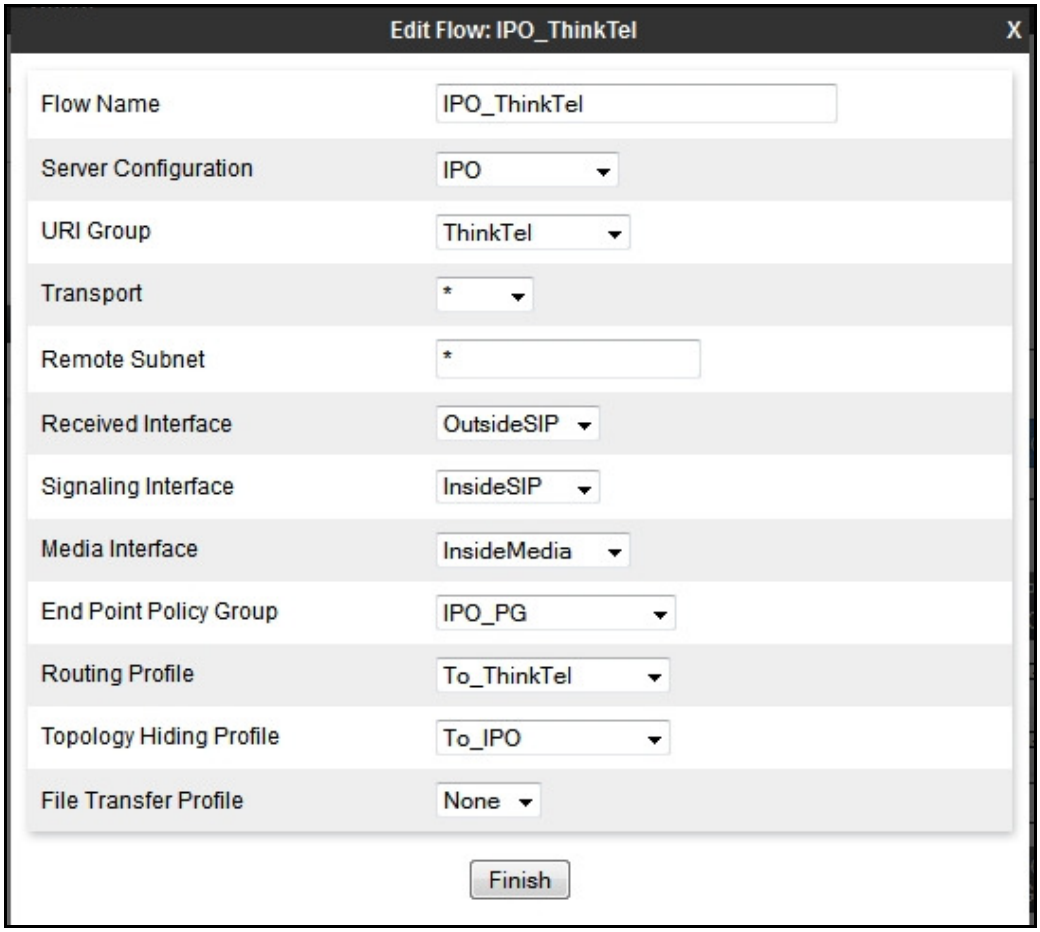
To create Server Flow, navigate to **Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click **Add** button (not shown). In the new window that appears, enter following values while other fields were kept as default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select Server Configuration created in **Section 6.2.55.1**which the Server Flow associates to.
- **URI Group**: Select URI Group **ThinkTel** created in **Section 6.2.1**.
- **Received Interface**: Select Signaling Interface created in **Section 6.4.3** which is Server Configuration designed to receive SIP signaling.
- **Signaling Interface**: Select Signaling Interface created in **Section 6.4.3** which is Server Configuration designed to send SIP signaling.
- **Media Interface**: Select Media Interface created in **Section 6.4.2** which is Server Configuration designed to send RTP.
- **End Point Policy Group**: Select End Point Policy Group created in **Section 6.3.4** which the Server Flow associates to.
- **Routing Profile**: Select Routing Profile created in **Section 6.2.2** which is Server Configuration is designed to route the calls to.
- **Topology Hiding Profile**: Select Topology Hiding profile created in **Section 6.2.3** to apply toward Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows Server Flow **ThinkTel** created for ThinkTel.



The following screen shows Server Flow **IPO_ThinkTel** created for IP Office.



6.4.5 Session Flows

Session Flows feature allows defining certain parameters that pertain to media portions of a call, whether it originates from the enterprise or outside the enterprise. This feature provides the complete and unparalleled flexibility to monitor, identify and control very specific types of calls based upon these user-definable parameters. Session Flows profiles SDP media parameters, to completely identify and characterize a call placed through the network.

A common Session Flow **ThinkTel_SF** was created for both ThinkTel and IP Office.

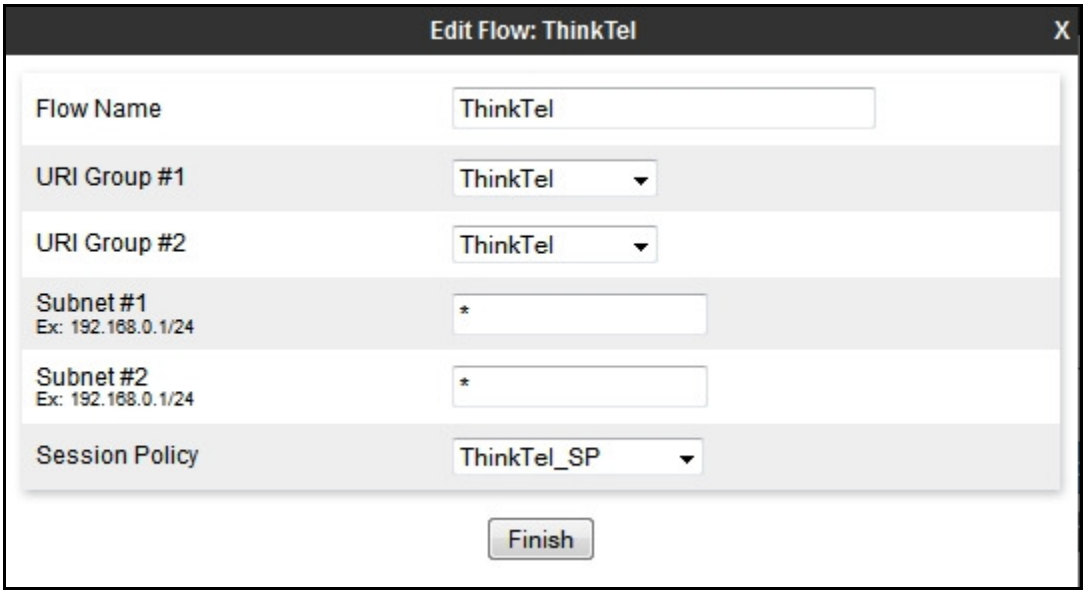
To create Session Flow, navigate to **Device Specific Settings → Session Flows** then click **Add** (not shown). In the new window that appears, enter following values while remaining fields were kept as default.

- **Flow Name**: Enter a descriptive name.
- **URI Group #1**: Select URI Group **ThinkTel** created in **Section 6.2.1** to assign to the Session Flow as source URI Group.
- **URI Group #2**: Select URI Group **ThinkTel** created in **Section 6.2.1** to assign to the Session Flow as destination URI Group.

- **Session Policy**: Select Session Policy **ThinkTel_SP** created in **Section 6.3.5** to assign to the Session Flow.
- Click **Finish** button.

Note: A unique URI Group is used for source and destination, since it contains multiple URIs defined for source as well as for destination.

The following screen shows Session Flow **ThinkTel_SF**.



7. ThinkTel SIP Trunking Service Configuration

ThinkTel is responsible for the configuration of ThinkTel SIP Trunking Service. ThinkTel will provide customer with necessary information to configure SIP Trunk for Avaya IP Office solution. The provided information from ThinkTel includes:

- IP address of ThinkTel SIP proxy.
- Credential for Digest Authentication.
- DID numbers.
- Supported codecs.
- A customer specific SIP signaling reference.

The sample configuration between the enterprise and ThinkTel for the compliance testing was a dynamic configuration and the registration was implemented on Avaya SBCE.

8. Verification and Troubleshooting

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

8.1 Verification Steps

Following activities were made to each test scenario:

- Verify that endpoints at the enterprise site can place and receive calls to PSTN and that the call remains active for more than 35 seconds.
- Verify that user on both PSTN and the enterprise sides can end an active call by hanging up.

8.2 Protocol Traces

Following SIP message headers were inspected using sniffer trace analysis tool:

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

Following attributes in SIP message body were inspected using sniffer trace analysis tool:

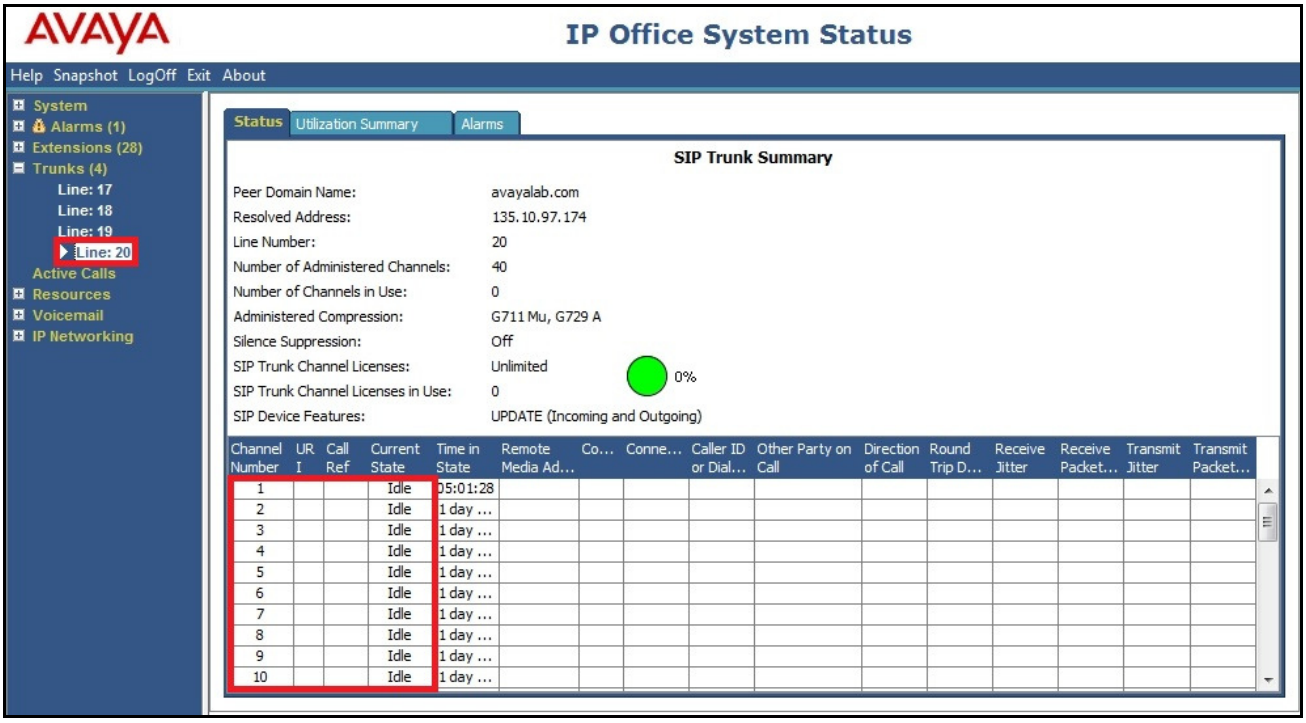
- Connection Information (c line): Verify correct IP addresses of near and far endpoints.
- Time Description (t line): Verify correct session timeout value of near and far endpoints.
- Media Description (m line): Verify correct audio port, codec, DTMF event description.
- Media Attribute (a line): Verify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

8.3 Troubleshooting

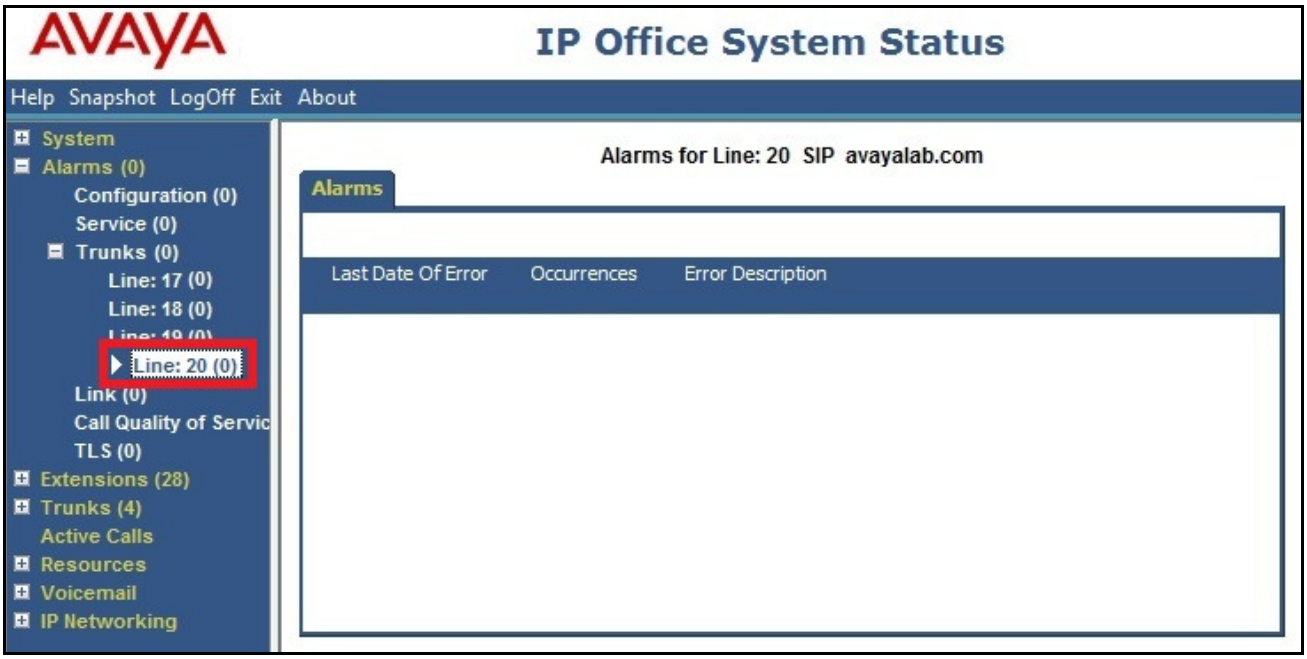
8.3.1 IP Office System Status

Following steps may be used to verify the configuration.

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



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



8.3.2 Sniffer Traces Analysis

Using network sniffing tool, e.g., WireShark to monitor SIP signaling between the enterprise and ThinkTel. The sniffer traces are captured at the public interface of Avaya SBCE.

Following screenshots show an example incoming call from ThinkTel to the enterprise.

- Incoming INVITE request from ThinkTel.

```
INVITE sip:438XXX0435@10.10.98.106:5060;transport=udp SIP/2.0
Record-Route: <sip:10.20.250.100;r2=on;lr;ftag=10.20.161.101+1+232727+a1a69da2>
Record-Route: <sip:10.20.250.20;r2=on;lr;ftag=10.20.161.101+1+232727+a1a69da2>
Via: SIP/2.0/UDP 10.20.250.100;branch=z9hG4bKded5.f53183c5.0
Via: SIP/2.0/UDP 10.20.161.101:5060;received=10.20.161.101;rport=5060;branch=z9hG4bK-
1f046f99d6aa1cf2b70f7206363acd4a1-10.20.161.101-1
Allow-Events: message-summary, refer, dialog, line-seize, presence, call-info, as-feature-
event
Max-Forwards: 69
Call-ID: 9CC9CE26@10.20.161.101
From: "Avaya CS1K"
<sip:647XXX1232@10.20.161.101:5060;transport=udp>;tag=10.20.161.101+1+232727+a1a69da2;isup-
oli=00
To: <sip:438XXX0435@10.10.98.106>
CSeq: 432686727 INVITE
Expires: 180
Organization: MetaSwitch
Supported: resource-priority, 100rel
Content-Length: 199
Content-Type: application/sdp
Contact: "Avaya CS1K" <sip:647XXX1232@10.20.161.101:5060;transport=udp>;isup-oli=00
P-Asserted-Identity: "Avaya CS1K" <sip:647XXX1232@10.20.161.101:5060>

v=0
o=- 3566153655 3566153655 IN IP4 10.20.250.10
s=-
c=IN IP4 10.20.250.102
t=0 0
m=audio 15758 RTP/AVP 18 0 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
a=nortpproxy:yes
```

- 200OK response from the enterprise.

```
SIP/2.0 200 OK
From: "Avaya CS1K"
<sip:647XXX1232@10.20.161.101:5060;transport=udp>;tag=10.20.161.101+1+232727+a1a69da2;isup-
oli=00
To: <sip:438XXX0435@10.10.98.106>;tag=574c50f31f269abb
CSeq: 432686727 INVITE
Call-ID: 9CC9CE26@10.20.161.101
Contact: "Extn233" <sip:438XXX0435@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=127033;lr;transport=udp>
Record-Route: <sip:10.20.250.100;r2=on;lr;ftag=10.20.161.101+1+232727+a1a69da2>
Record-Route: <sip:10.20.250.20;r2=on;lr;ftag=10.20.161.101+1+232727+a1a69da2>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
Supported: timer,100rel
Via: SIP/2.0/UDP 10.20.250.100;branch=z9hG4bKded5.f53183c5.0
Via: SIP/2.0/UDP 10.20.161.101:5060;received=10.20.161.101;rport=5060;branch=z9hG4bK-
1f046f99d6aa1cf2b70f7206363acd4a1-10.20.161.101-1
Server: IP Office 8.1 (69)
Content-Type: application/sdp
Content-Length: 202

v=0
o=UserA 2381524454 1312691928 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 35738 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Following screenshots show an example outgoing call from the enterprise to ThinkTel.

- Outgoing INVITE request from the enterprise.

```
INVITE sip:647XXX1226@10.20.250.100:5060 SIP/2.0
From: "Extn234" <sip:438XXX0444@10.10.98.106:5060>;tag=cdb70a46fb5f5ef3
To: <sip:647XXX1226@10.20.250.100:5060>
CSeq: 682693711 INVITE
Call-ID: 9fa8e3363dfa673c4246f328dc117c25
Contact: "Extn234" <sip:438XXX0444@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=127034;lr;transport=udp>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
Supported: timer,100rel
User-Agent: IP Office 8.1 (69)
Max-Forwards: 69
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-000104380759-1--s1632-
P-Asserted-Identity: "Extn234" <sip:438XXX0444@10.10.98.106:5060>
Content-Type: application/sdp
Content-Length: 200

v=0
o=UserA 894996724 474276637 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 35740 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

- Incoming 401 from ThinkTel to request Digest Authentication.

```
SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest
realm="tor.trk.tprm.ca",nonce="ccc6adbae624",stale=false,algorithm=MD5,qop="auth"
Call-ID: 9fa8e3363dfa673c4246f328dc117c25
CSeq: 682693711 INVITE
From: "Extn234" <sip:438XXX0444@10.10.98.106:5060>;tag=cdb70a46fb5f5ef3
To: <sip:647XXX1226@10.20.250.100:5060>;tag=10.20.161.101+1+2fb10d+9d23721c
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-000104380759-1--s1632-
Server: DC-SIP/2.0
Organization: MetaSwitch
Supported: resource-priority, 100rel
Content-Length: 0
```

- Outgoing re-INVITE from the enterprise with the Authorization header.

```
INVITE sip:647XXX1226@10.20.250.100:5060 SIP/2.0
From: "Extn234" <sip:438XXX0444@10.10.98.106:5060>;tag=cdb70a46fb5f5ef3
To: <sip:647XXX1226@10.20.250.100:5060>
CSeq: 682693712 INVITE
Call-ID: 9fa8e3363dfa673c4246f328dc117c25
Contact: "Extn234" <sip:438XXX0444@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=127034;lr;transport=udp>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
Supported: timer,100rel
User-Agent: IP Office 8.1 (69)
Max-Forwards: 69
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-001433866827-1--s1632-
Authorization: Digest username="438XXX0434", realm="tor.trk.tprm.ca",
nonce="ccc6adbae624", uri="sip:avayalab.com",
response="43fdd349b7b026259ab540b132d19cbb", algorithm=MD5, cnonce="0a4f113b",
qop=auth, nc=00000001
P-Asserted-Identity: "Extn234" <sip:438XXX0444@10.10.98.106:5060>
Content-Type: application/sdp
Content-Length: 200

v=0
o=UserA 894996724 474276637 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 35740 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

- Incoming 200OK response from ThinkTel.

```
SIP/2.0 200 OK
Call-ID: 9fa8e3363dfa673c4246f328dc117c25
CSeq: 682693712 INVITE
From: "Extn234" <sip:438XXX0444@10.10.98.106:5060>;tag=cdb70a46fb5f5ef3
To: <sip:647XXX1226@10.20.250.100:5060>;tag=10.20.161.101+1+2f4923+a0d808e3
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-001433866827-1--s1632-
Server: DC-SIP/2.0
Organization: MetaSwitch
Allow-Events: message-summary, refer, dialog, line-seize, presence, call-info, as-
feature-event
Supported: resource-priority, 100rel
Allow: INVITE, ACK, CANCEL, BYE, REGISTER, OPTIONS, PRACK, UPDATE, SUBSCRIBE, NOTIFY,
REFER, INFO, PUBLISH
Accept-Encoding: identity
Accept: application/sdp, application/simple-message-summary, message/sipfrag,
application/x-simple-call-service-info, text/plain
Record-Route: <sip:10.20.250.20;r2=on;lr;ftag=cdb70a46fb5f5ef3>
Record-Route: <sip:10.20.250.100;r2=on;lr;ftag=cdb70a46fb5f5ef3>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=127034;lr;transport=udp>
Contact: <sip:647XXX1226@10.20.161.101:5060>
Content-Length: 196
Content-Type: application/sdp

v=0
o=- 3566173746 3566173746 IN IP4 10.20.250.11
s=-
c=IN IP4 10.20.250.107
t=0 0
m=audio 26722 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
a=nortpproxy:yes
```

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise R6.2 to ThinkTel SIP Trunking Service.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The ThinkTel SIP Trunking Service is considered **compliant** with Avaya IP Office Release 8.1.

10. References

Documentation for Avaya products may be found at http://support.avaya.com.

[1] *IP Office 8.1 IP500/IP500 V2 Installation*, Document Number 15-601042, Issue 27f, 04 March 2013.
[2] *IP Office 8.1 Manager FP1 10.1*, Document Number 15-601011, Issue 29t, 20 February 2013.
[3] *IP Office 8.1 Administering Voicemail Pro*, Document Number 15-601063, Issue 8b, 11 December 2012.
[4] *Administering Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.
[5] *Installing Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.
[6] *Upgrading Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, March 2013.

Product documentation for ThinkTel SIP Trunking Service is available from ThinkTel.

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.