Avaya Solution & Interoperability Test Lab

Application Notes for MTS Allstream 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 MTS Allstream Session Initiation Protocol (SIP) Trunking Service with Avaya IP Office Release 8.1 and Avaya Session Border Controller for Enterprise Release 6.2.

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

MTS Allsteram 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 MTS Allstream 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.

MTS Allstream SIP Trunking Service (MTS Allstream) referenced within these Application Notes is designed for business customers. The 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 MTS Allstream via the 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 MTS Allstream SIP Trunking interoperability, following features and functionalities were exercised during the compliance testing:

- Incoming PSTN calls to various phone types including SIP, H.323, digital and analog telephones at the enterprise. All incoming calls from PSTN are routed to the enterprise across the SIP Trunk from the service provider networks.
- Outgoing PSTN calls from various phone types including SIP, H.323, digital and analog telephone at the enterprise. All outgoing calls to PSTN are routed from the enterprise across the SIP trunk to the service provider networks.
- 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 toll-free calls, local directory assistance (411), etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Proper codec negotiation of 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 T.38.
- 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.
- Response to OPTIONS heartbeat.
- Session Timer refresh per RFC 4028.
- Response to incomplete call attempts and trunk errors.

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

- Outgoing emergency (E911), international, operator and operator assisted calls are supported but not tested during the compliance testing.
- Off-net call transfer with REFER method is not supported.
- Off-net call forward with History-Info method is not supported.

2.2 Test Results

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

1. **For outgoing calls from IP Office**, **MTS Allstream does not validate Calling Party Name and Number**. Configuring an IP Office station with any Calling Party Name and Number for outgoing calls over the SIP Trunk, MTS Allstream transmitted the original Calling Party Name and Number to the called PSTN party without any modification. This is not expected because the display information from the enterprise is not trusted, it should be examined by the service provider before being sent to PSTN. This is a known behavior on the MTS Allstream SIP Trunking Service with no available resolution at this time.

2. **Outgoing calls from unassigned DID number are unexpectedly successful**. IP Office station originated an outgoing call with any unassigned DID numbers, the call successfully passed to PSTN. This behavior is not expected. MTS Allstream should examine the Calling Party Number of the originator to grant access only if it matches the subscribed DID range. This is a known behavior on the MTS Allstream SIP Trunking Service with no available resolution at this time.

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. **Calling Party Number is not properly displayed before the SIP station completes the blind transfer of an outgoing PSTN call to the H.323 station**. Before the H.323 station answers the blind transferred call, it displayed "External" instead of displaying Calling Party Number of the called PSTN party. The issue does not occur when using the H.323 station to perform the blind transfer. 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.

6. **For off-net call forward or Mobility Twinning calls**, **Calling Party Name and Number of original calling PSTN party are not displayed on terminated called PSTN party**. Outgoing calls to the terminated PSTN party or mobile extension, had the "P-Asserted-Identity" containing the Calling Party Name and Number of IP Office station. This is not expected because MTS Allstream based on the "P-Asserted-Identity" header for call display purpose. A workaround has been implemented by using SigMa script on the Avaya SBCE (see **Section 6.2.5**) to replicate the "From" header which contains original Calling Party Name and Number of the calling PSTN party. With this workaround, the display on the forwarded PSTN party or mobile extension was corrected. This is a known behavior of IP Office with no available resolution at this time. This issue has low user impact, and is listed as an observation.

7. **Long duration outgoing calls are now corrected**. The signaling from MTS Allstream negotiated that MTS Allstream is the Session Timer refresher. However, after sending the UPDATE request to refresh the Session Timer for the first time, MTS Allstream stopped sending subsequent Session Timer refreshes. When the "Session-Expires" timer has been reached in 90 minutes, IP Office sent the BYE request to disconnect the call. MTS Allstream responded "481 Transaction Does Not Exist" to imply that the call has been already terminated. MTS Allstream corrected the settings of the SIP Trunk to continuously sending UPDATE to refresh the Session Timer and the issue has been fixed.

8. **T.38 fax is now working**. For incoming fax calls, MTS Allstream originally did not send re-INVITE(t.38) to switch the channel from voice to fax. MTS Allstream corrected the settings of the SIP Trunk to actively sending re-INVITE (t.38) and the issue has been fixed. However, MTS Allsltream failed to treat outgoing fax calls the same way. There was no re-INVITE (t.38) received from MTS Allstream for outgoing fax calls. This issue has been fixed by defining **Equipment Classification** as **Fax Machine** for fax terminal. For detailed configuration, see **Section 5.5.5**. This makes IP Office send the initial INVITE (t.38) to set up the fax channel, without establishing a voice call as the first stage. During the testing, incoming and outgoing faxes were successfully transmitted with acceptable quality.

2.3 Support

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

For technical support on MTS Allstream SIP Trunking Service, contact MTS Allstream technical support at:

- Phone: (204) 225-5687 or 1-800-883-2054
- Website: http://www.mts.ca/support

3. Reference Configuration

Figure 1 below illustrates the test configuration. It shows an enterprise site connected to the MTS Allstream networks through the Internet.

For confidentiality and privacy purposes, actual public IP addresses and PSTN routable phone numbers 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 v500
- 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 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 the internal interface of the Avaya SBCE across the enterprise network. On the public side, the external interface of the Avaya SBCE connects to MTS Allstream networks via the Internet.

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

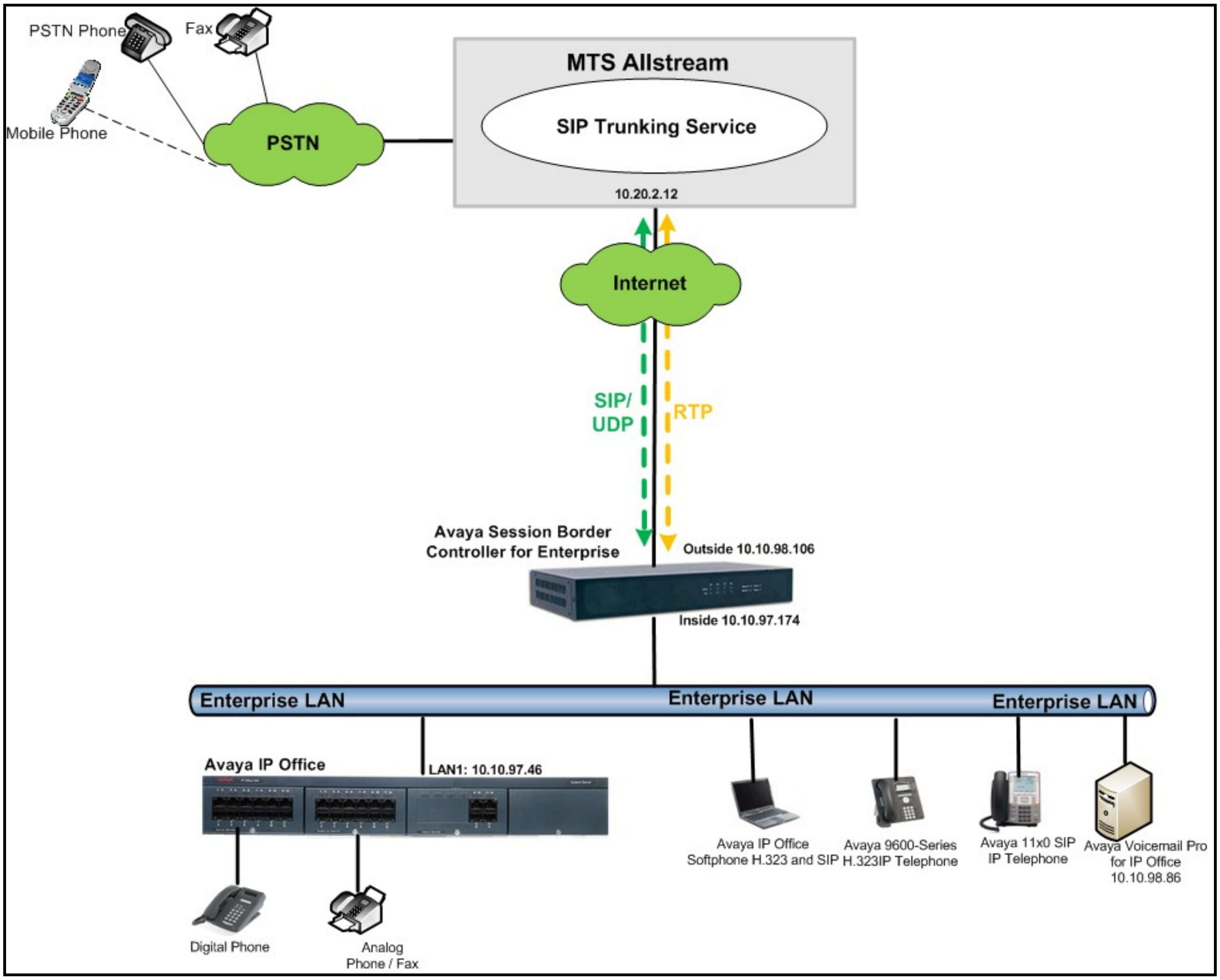


Figure 1: Avaya IP Telephony Network Connecting to MTS Allstream SIP Trunking Service.

For the compliance testing, MTS Allstream provided the service provider public SIP domain as its Central Office (CO) IP address **10.20.2.12** 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 and RTP traffic between MTS Allstream and the Avaya SBCE, using transport protocol UDP.

For outgoing calls, IP Office sent 11 digits in destination headers, e.g. "Request-URI" and "To", and sent 10 digits in source headers, e.g. "From", "Contact", and "P-Asserted-Identity". For incoming calls, MTS Allstream sent 10 digits in destination headers and sent 11 digits in source headers.

In an actual customer configuration, the enterprise site may also include additional network components between the service provider and the enterprise 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 the service provider and the enterprise 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.

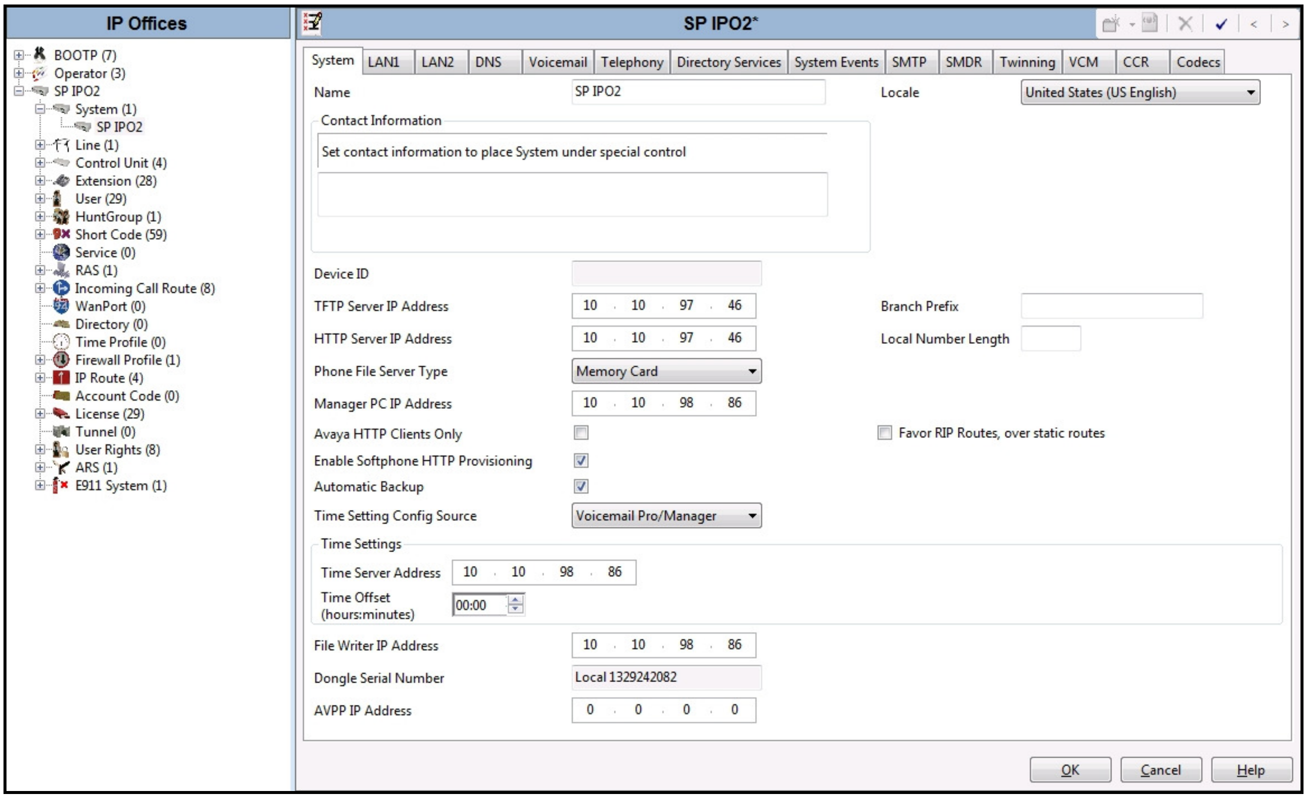
Avaya Telephony Components	
Equipment/Software	**Release/Version**
Avaya IP Office 500v2	8.1 (65)
Avaya IP Office DIG DCP*16 V2	8.1 (65)
Avaya IP Office Ext Card Phone 8	8.1
Avaya IP Office Manager	10.1 (65)
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	6.2 (6.2.0 Q30)
Avaya Voicemail Pro for IP Office	8.1.1003.0
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

MTS Allstream SIP Trunking Service Components	
Equipment/Software	**Release/Version**
Genband S3	7.1.10.3
CS2K	CVM15

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 MTS Allstream. It is 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 the proper IP Office from the pop-up window, and log in with the 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 the **Navigation Pane** on the left side and the **Details Pane** on the right side. These panes will be referenced throughout these Application Notes.



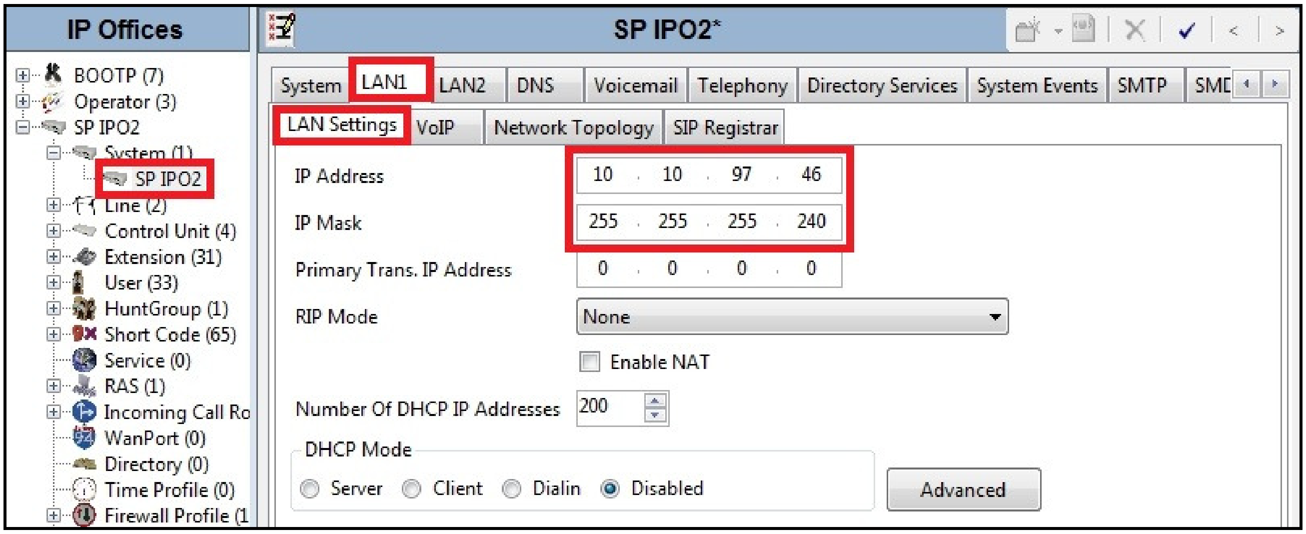
These Application Notes assume the basic installation and configuration have already been completed and are not discussed here. For further information on IP Office, please consult **References** in **Section 10**.

5.1 LAN

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

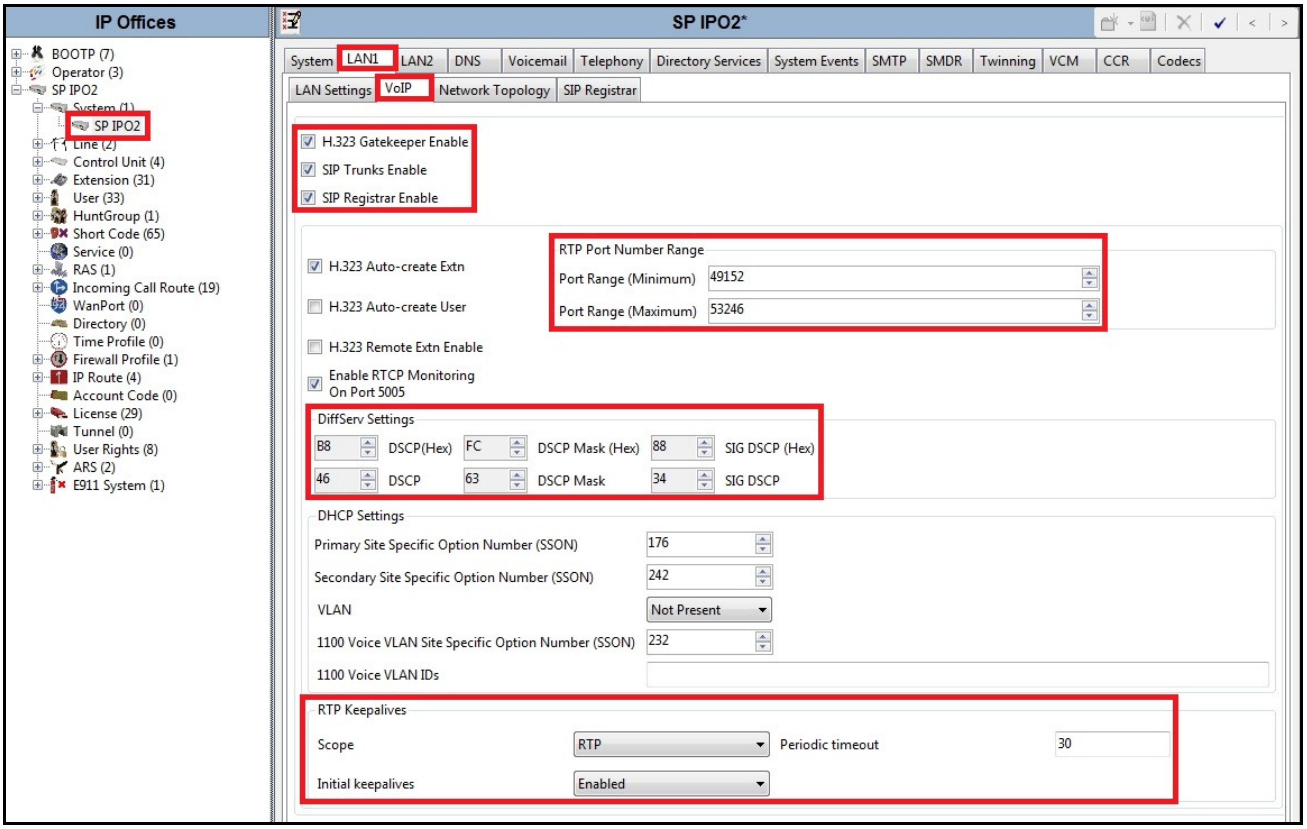
- Set the **IP Address** field to the LAN IP address, e.g. **10.10.97.46**.
- Set the **IP Mask** field to the subnet mask of the public network, e.g. **255.255.255.240**.

- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.



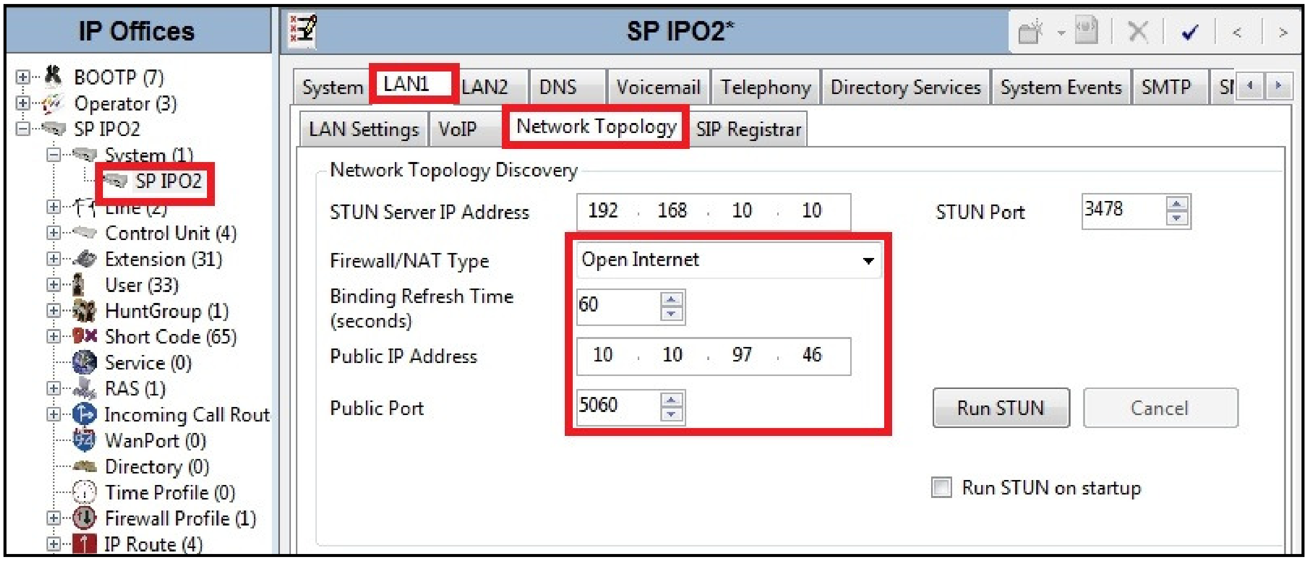
The **VoIP** tab as shown in the screenshot below was configured with following settings.

- Check the **H323 Gatekeeper Enable** to allow Avaya IP Telephones/Softphones using the H.323 protocol to register.
- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to MTS Allstream.
- Check the **SIP Registrar Enable** to allow Avaya IP Telephones/Softphones to register using the SIP protocol.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Port Range (Minimum)** and **Port Range (Maximum)** values were kept as default.
- Verify the **DiffServ Settings** were kept as default for the Differentiated Services Code Point (DSCP) parameters in the IP packet headers to support Quality of Services policies for both signaling and media, the **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling.
- Verify **RTP Keepalives** settings were enabled with **Scope** as **RTP**, **Periodic timeout** in **30** seconds, and **Initial keepalives** as **Enabled**. This allows IP Office to send IP packets to keep the active RTP session alive in every 30 seconds if there is no audio detected on the SIP Trunk.
- All other parameters should be set according to customer requirements.
- Click OK to commit (not shown) then press Ctrl + S to save.



In the **Network Topology** tab, configure the following parameters:

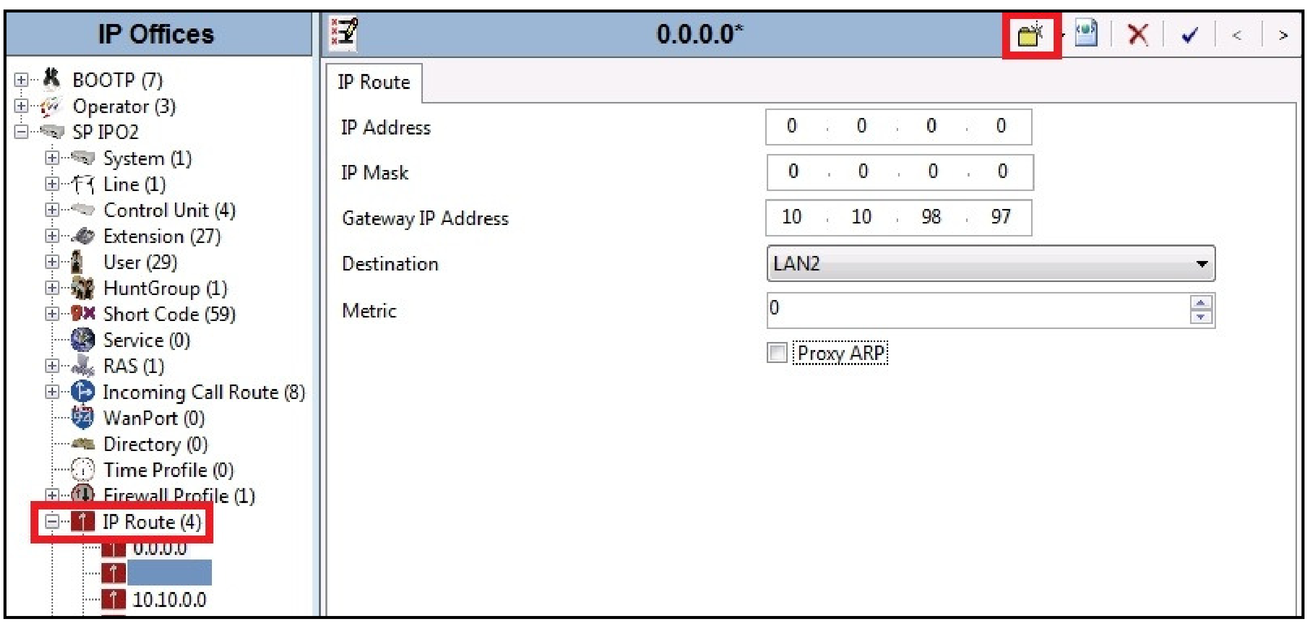
- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. In the compliance testing, it was set to **Open Internet**. With this configuration, even the default STUN settings are populated but they will not be used.
- Set the **Binding Refresh Time (seconds)** to **60**. This value is used to determine the frequency that IP Office will send OPTIONS heartbeat to the service provider.
- Set the **Public IP Address** to IP Office LAN IP address, e.g. **10.10.97.46**.
- Set the **Public Port** is 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 an IP Route **10.10.0.0** on LAN1 connecting to the Avaya SBCE for SIP and RTP traffic to MTS Allstream, and a second IP Route **10.33.0.0** on the same LAN1 connecting to the private enterprise networks.

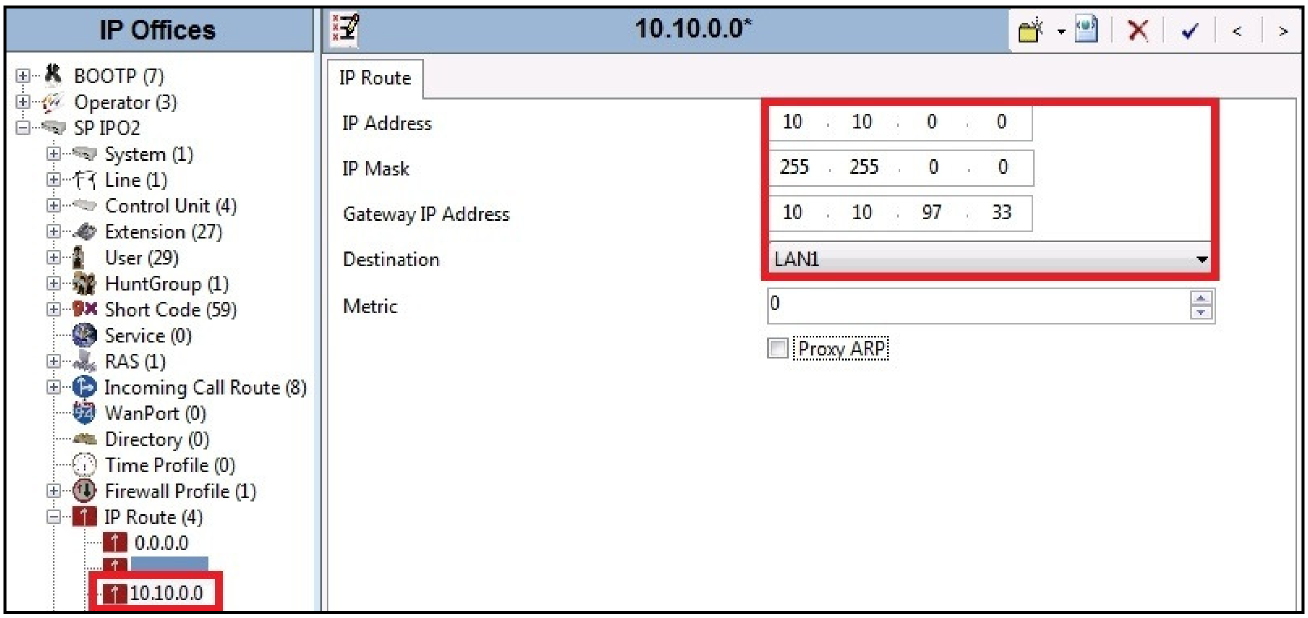
To create an IP Route, select **IP Route** in the Navigation Pane, then click "**Create a New Record**" icon as shown in the screenshot below.



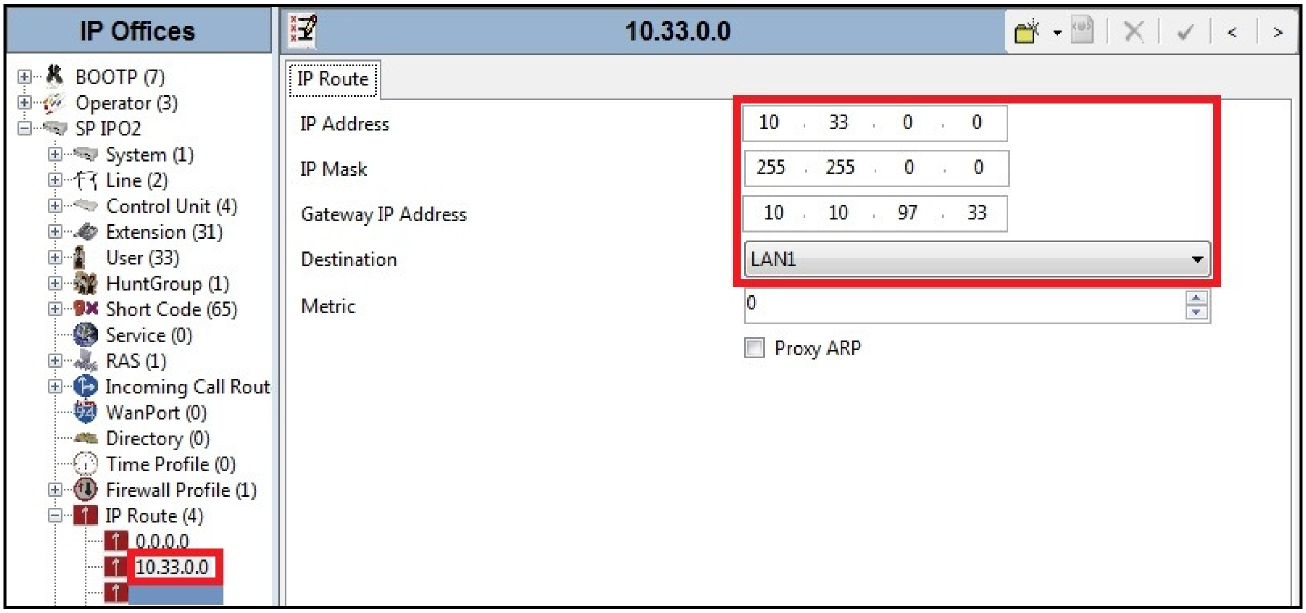
The IP Routes were configured using the following settings.

- Set the **IP Address** to the address of the destination network.
- Set the **IP Mask** to the subnet mask of the destination network.
- Set the **Gateway IP Address** to the IP address of the enterprise gateway that routes traffic to the destination network.
- Set the **Destination** to the 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 the IP Route **10.10.0.0** that was created on **LAN1** for SIP and RTP traffic to MTS Allstream via the Avaya SBCE. **LAN1** was assigned to the 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 the enterprise network that connects to **LAN1**.



Similarly, the IP Route **10.33.0.0** was created on **LAN1** for IP phone connections across the enterprise network. **LAN1** was assigned to the 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 the enterprise network that connects to **LAN1**.

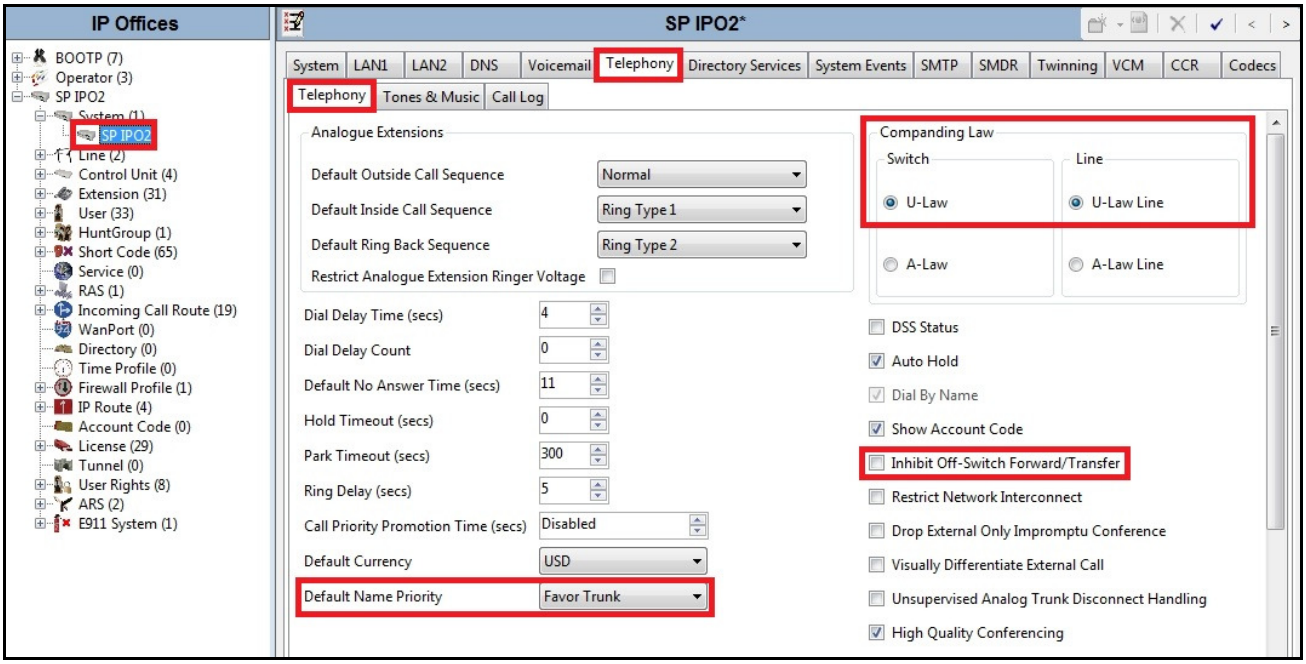


5.3 System Telephony and Codecs

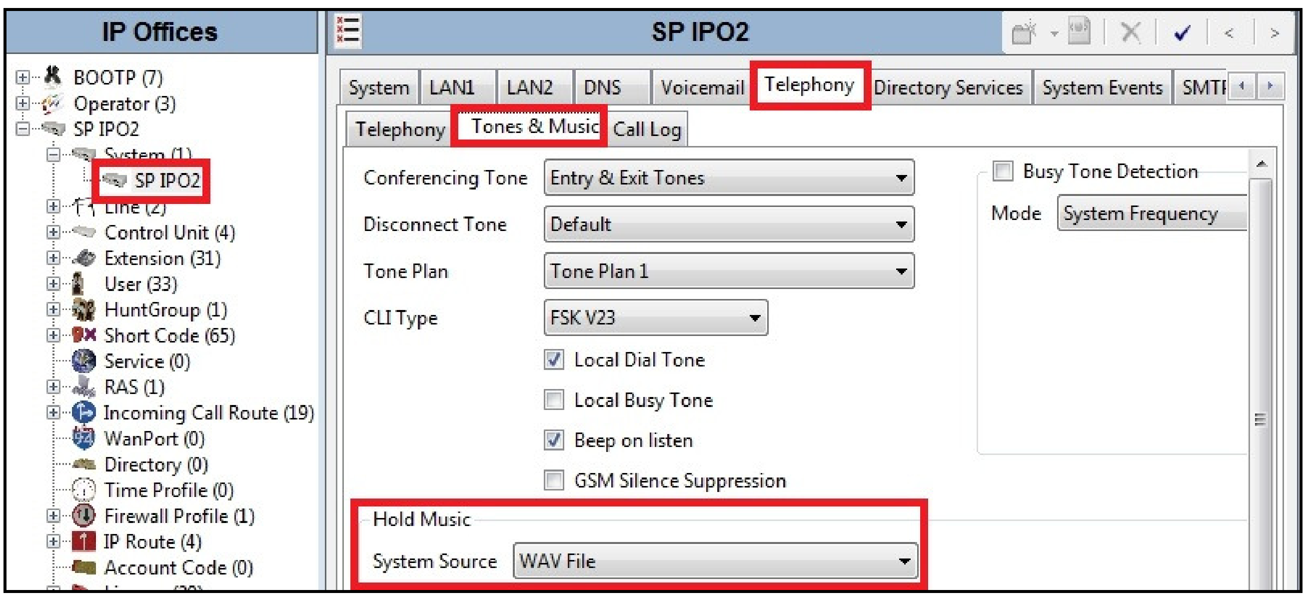
Navigate to the **System (1)** → **SP IPO2** in the Navigation Pane then select **Telephony** → **Telephony** tab in the Details Pane.

The **Telephony** settings were configured with following parameters.

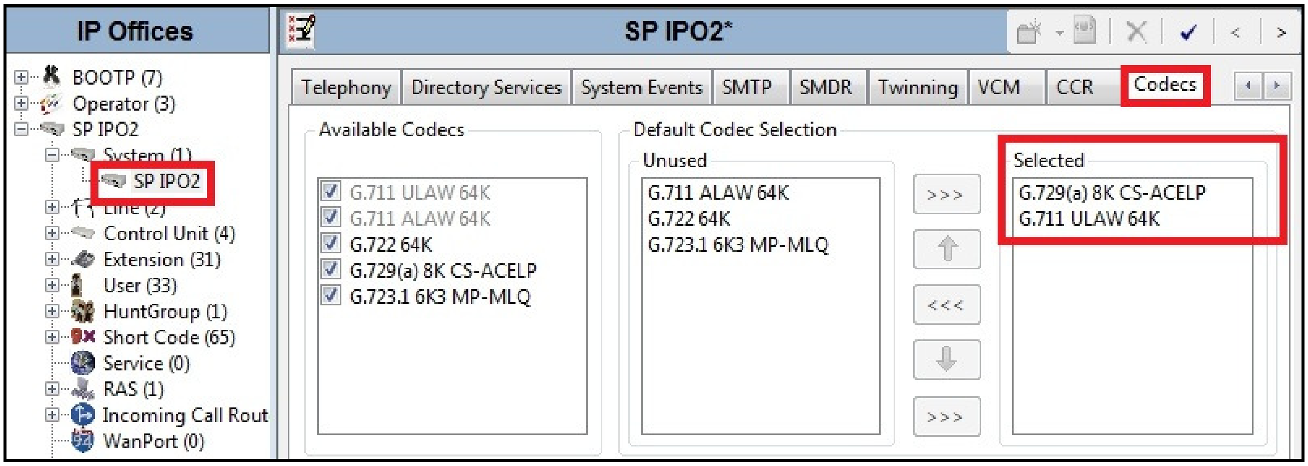
- Choose the **Companding Law** typical for the enterprise location. For North America, **U-LAW** was used for both **Switch** and **Line**.
- Set **Default Name Priority** to **Favor Trunk**. This allows IP Office to use information received from SIP Trunk for call display purpose rather than overriding it with pre-defined internal settings.
- Uncheck the **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 medium to provide Music on Hold on the SIP Trunk.



For **Codecs** settings, navigate to the **System (1) → SP IPO2** in the Navigation Pane, and then select **Codecs**. The **Codecs** settings are shown in the screenshot below with G.729 and G.711MU were selected in prioritized order. In the compliance testing, MTS Allstream supported G.729 as the first choice and G.711MU as the second choice for RTP traffic.



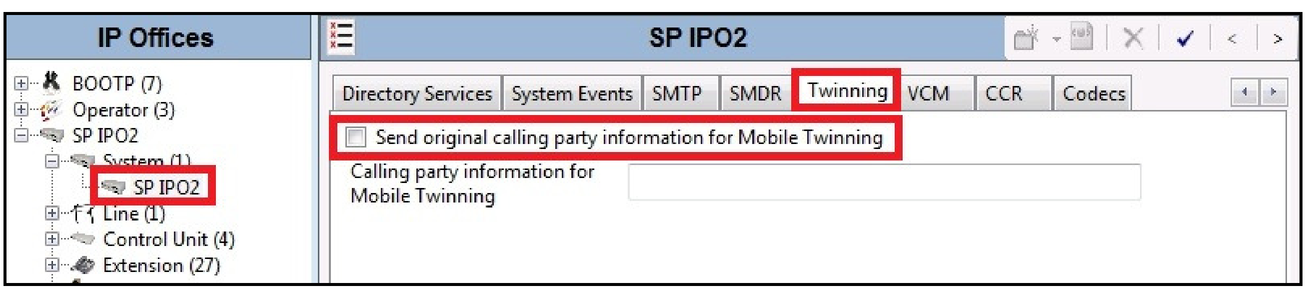
Click OK to commit (not shown) then press Ctrl + S to save.

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 the **Send original calling party information for Mobile Twinning** box on the **System→Twinning** tab. The second parameter is the **Send Caller ID** parameter on the **SIP Line** form shown in **Section 5.5.1**.

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

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



5.5 Administer SIP Line

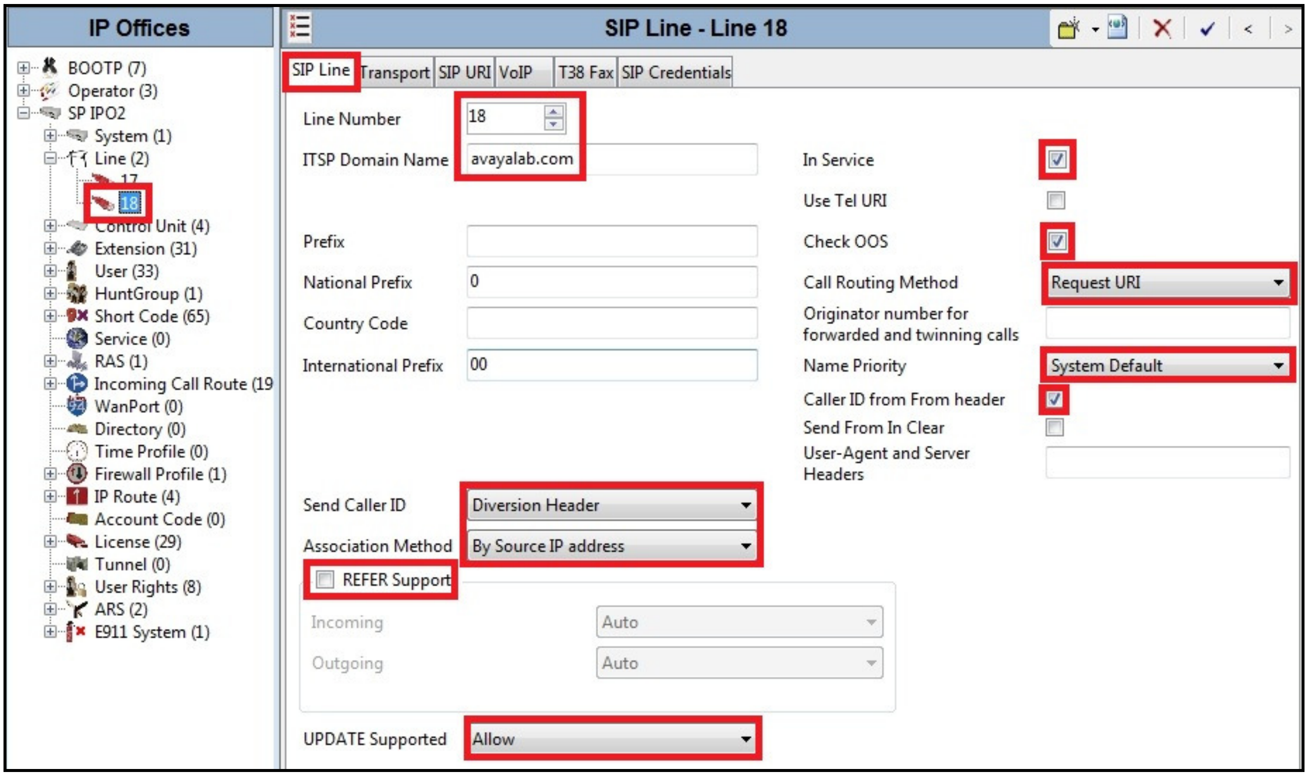
A SIP Line was needed to establish the SIP Trunk between IP Office and MTS Allstream.

To create a 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 the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

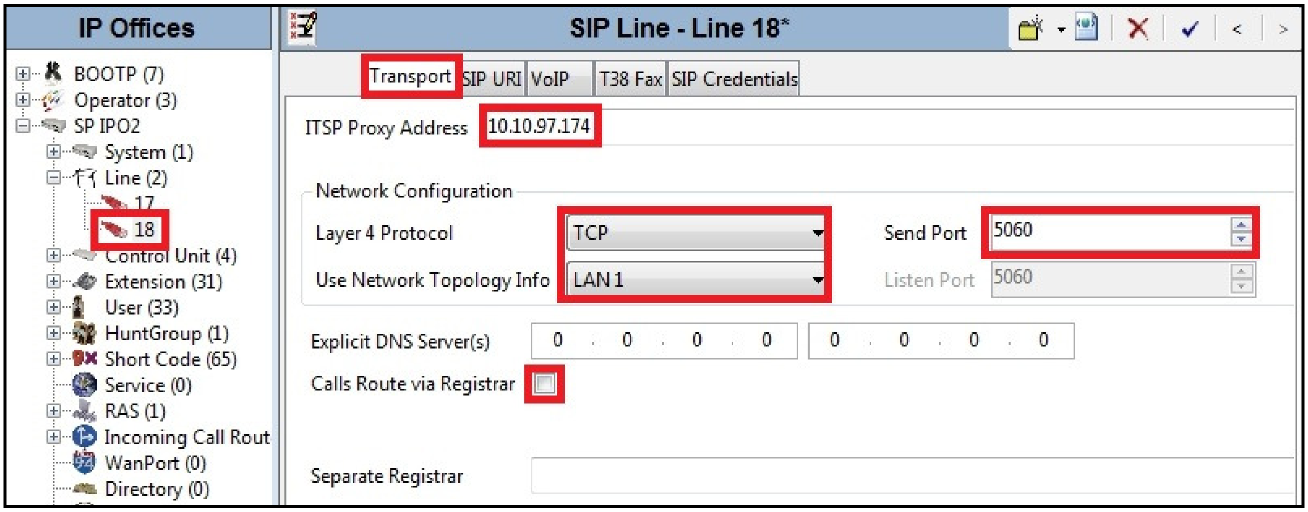
- Set the **Line Number** to an unassigned number, e.g. **18**.
- Set the **ITSP Domain Name** to the FQDN or IP address that will be used as the enterprise SIP domain so that IP Office uses this domain as the URI-Host of the “From”, “P-Asserted-Identity” and “Diversion” headers. In the compliance testing, the enterprise SIP domain was defined as **avayalab.com** for the internal traffic between IP Office and the Avaya SBCE. This domain will be changed by Topology-Hiding configured on the Avaya SBCE (see **Section 6.2.3**) to the public IP address of the Avaya SBCE **10.10.98.106**, it is to meet the requirement from MTS Allstream.
- Set the **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 the **Association Method** to **By Source IP address**. This setting allows IP Office to apply the configuration for the public SIP Trunk to incoming and outgoing calls from/ to MTS Allstream, if the traffic was originated from/ to the IP address of the far end proxy server (which is the internal IP address of the Avaya SBC).
- Uncheck the **REFER Support** because REFER method is not supported by MTS Allstream in this certification testing.
- Set the **UPDATE Supported** field to **Allow** as MTS Allstream supported the UPDATE method in this certification testing.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will send the OPTIONS heartbeat to check status of the SIP Trunk.
- Set the **Call Routing Method** field to **Request URI**.
- Set the **Name Priority** field to **System Default**.
- Check the **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 the **Transport** tab then configure the parameters as shown below.

- The **ITSP Proxy Address** was set to the internal IP Address of the Avaya SBCE **10.10.97.174** as shown in **Figure 1**.
- In the **Network Configuration** area, **TCP** was selected as the **Layer 4 Protocol** and the **Send Port** was set to the well-known port number **5060** which is the port that the Avaya SBCE opens for SIP traffic.
- The **Use Network Topology Info** parameter was set to **LAN 1**. This associates the SIP Line 18 with the parameters in the **System → LAN1 → Network Topology** tab.
- The **Calls Route via Registrar** was unchecked. In this certification testing, MTS Allstream did not support the dynamic Registration on the SIP Trunk.
- Other parameters retain default values.
- Click OK to commit (not shown) then press Ctrl + S to save.

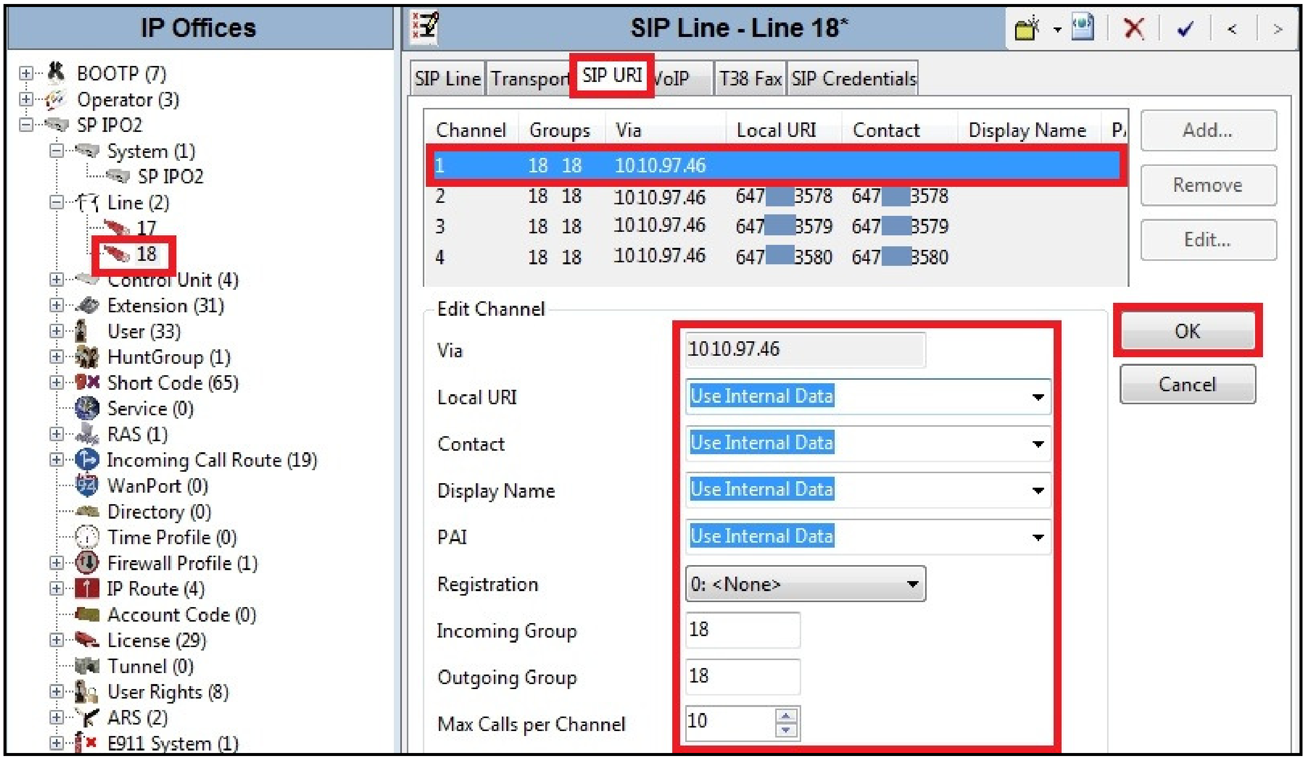


5.5.3 Administer SIP URI Settings

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

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

- Set the **Local URI**, **Contact**, **Display Name** and **PAI** to **Internal Data**. This setting will use Calling Party Number defined under the **SIP** tab of **User** as shown in **Section 5.7** for the public SIP calls.
- For the **Registration** field, select **<None>** to disable the Registration.
- Associate SIP Line **18** to the **Incoming Group** and **Outgoing Group**. The line group number will be used in defining incoming or outgoing call routes for this SIP Line.
- Set the **Max Calls per Channel** to **10** which is the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

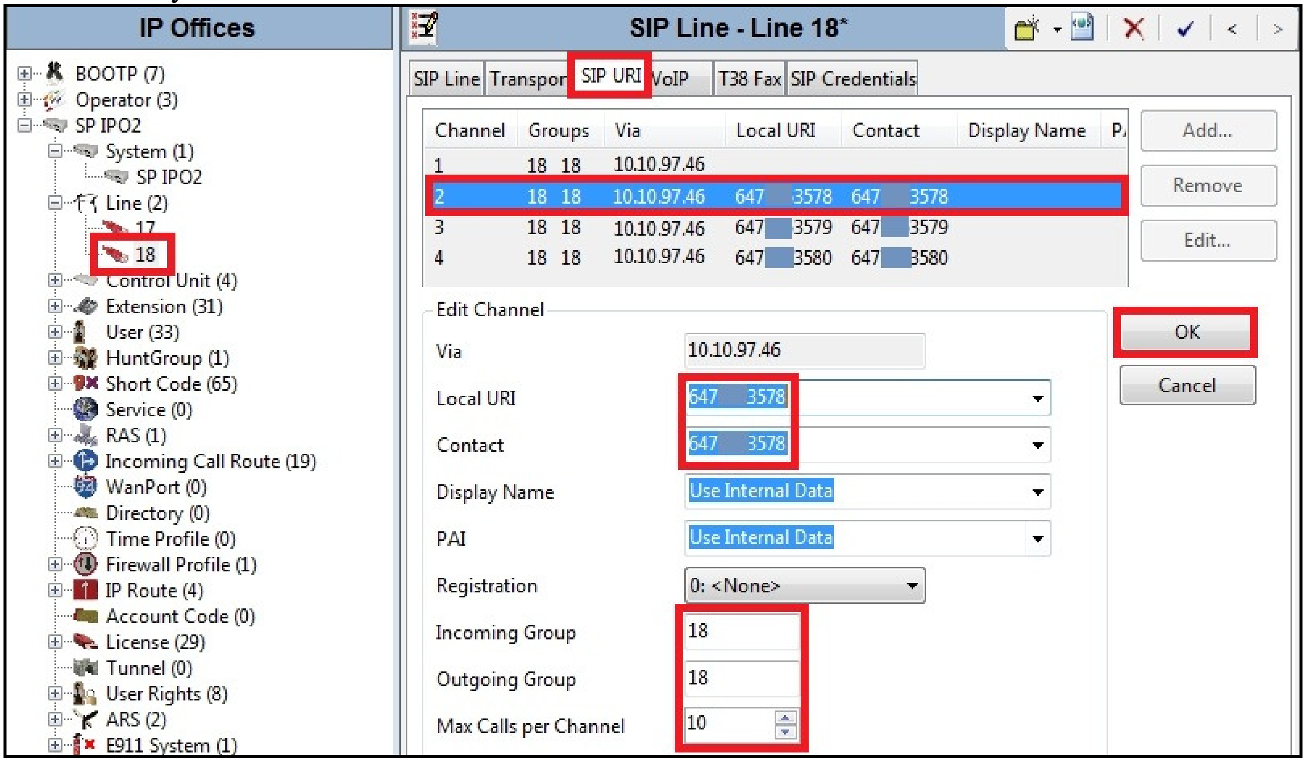


SIP URI entries with **Channel 2**, **Channel 3** and **Channel 4** were similarly created for incoming calls appropriately to pre-define DID numbers **647XXX3578**, **647XXX3579** and **647XXX3580** for access to Feature Name Extension 00 (FNE00), Feature Name Extension 33 (FNE33), and VoiceMail. The Short Codes for FNE00 and FNE33 were defined in **Section 5.6** to provide Dial Tone and Mobile Callback for mobility extension.

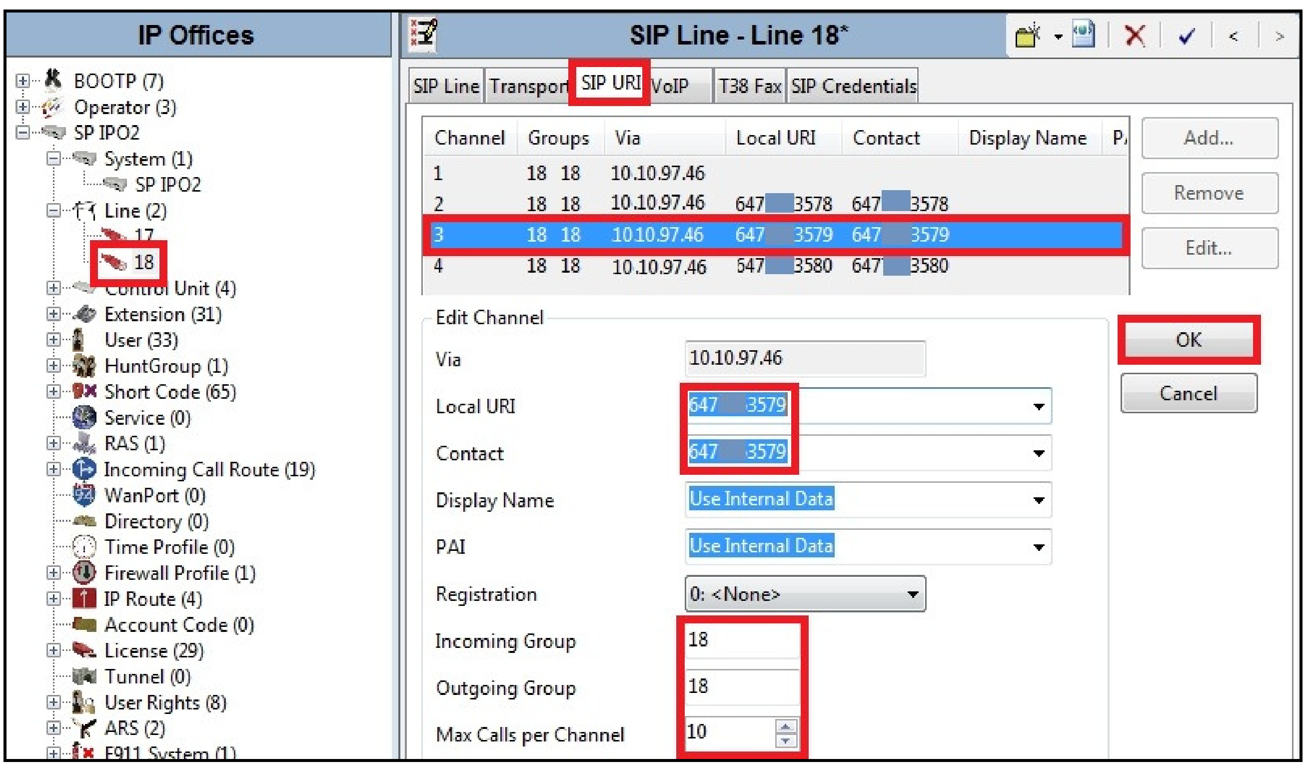
The **Channel 2**, **Channel 3** and **Channel 4** as shown in the screenshot below, were configured with following parameters.

- Set the **Local URI** and **Contact** fields to pre-define DID number **647XXX3578**, **647XXX3579** and **647XXX3580** appropriately for **Channel 2**, **Channel 3** and **Channel 4**.
- Associate **Incoming Group** and **Outgoing Group** to SIP Line 18.
- Set the **Max Calls per Channel** field to **10**.
- Other parameters retain default values.
- Click OK to commit.

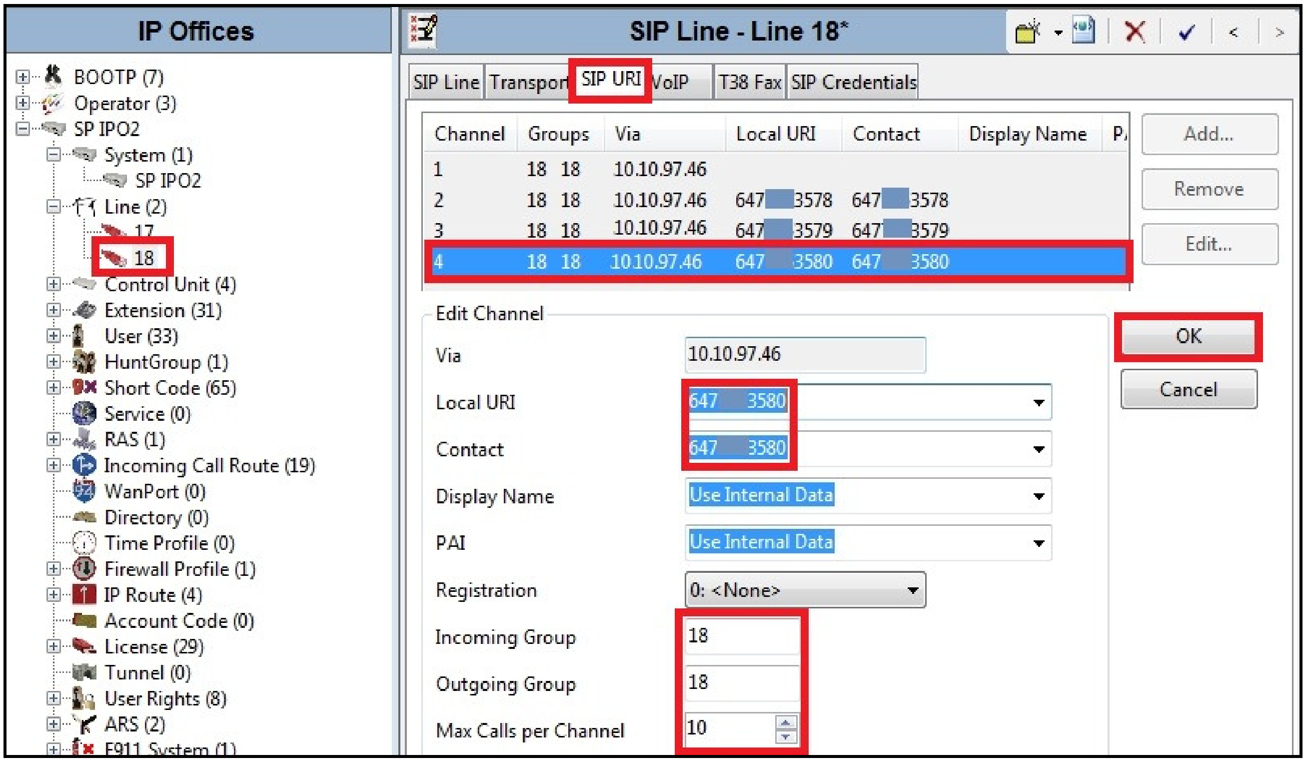
SIP URI entry for **Channel 2**:



SIP URI entry for **Channel 3**:



SIP URI entry for **Channel 4**:



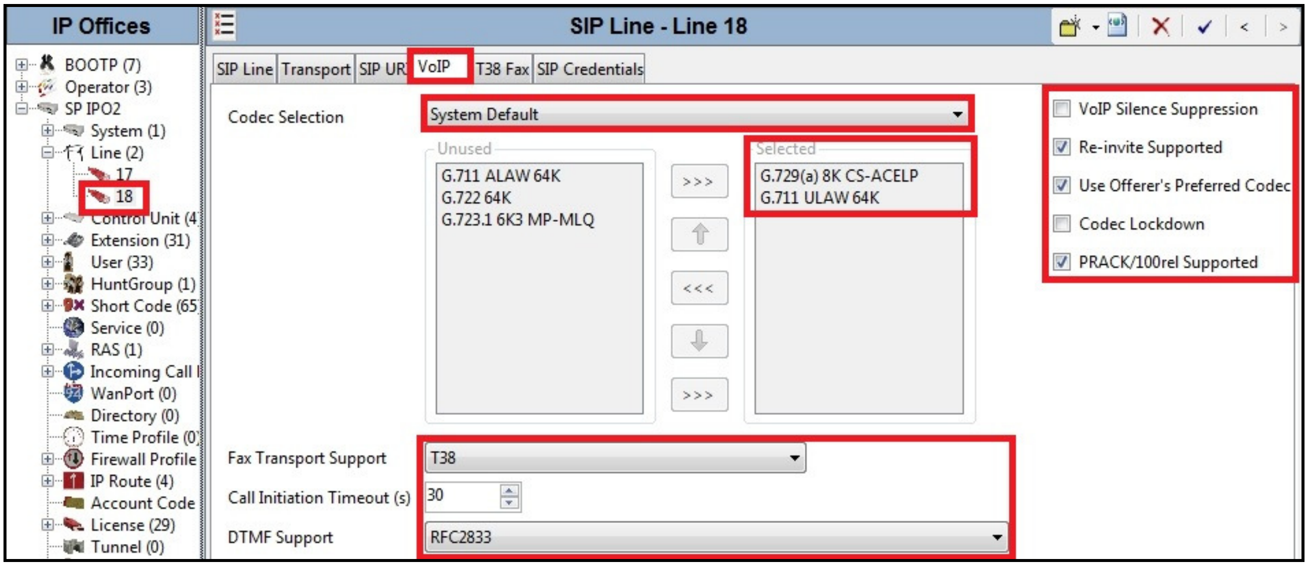
Click OK to commit (not shown) then press Ctrl + S to save.

5.5.4 Administer VoIP Settings

Select the **VoIP** tab, then set the Voice over Internet Protocol parameters of the SIP Line as following:

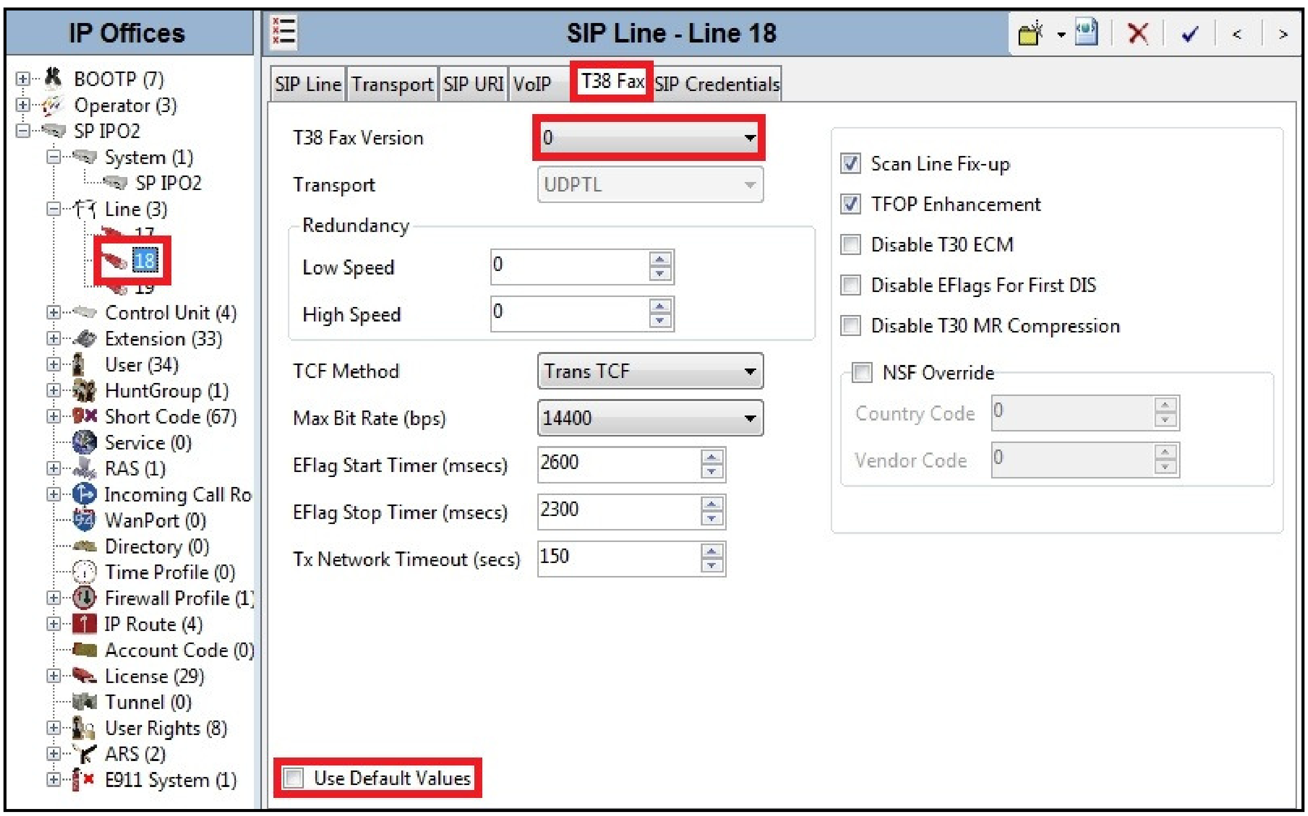
- The **Codec Selection** can be selected by choosing **System Default** from the pull-down menu to use the System Codecs as defined in **Section 5.3**. The codec order was configured as **G.729(a) 8K CS-ACELP** and **G.711 ULAW 64K** which are supported by MTS Allstream. IP Office includes these codes in the right prioritized order in the Session Description Protocol (SDP) offer or answer defined for the RTP traffic.
- Set the **Fax Transport Support** to **T.38** from the pull-down menu.
- Set the **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 the **DTMF Support** to **RFC2833** from the pull-down menu. This directs IP Office to send out-of-band DTMF tones using RTP events per RFC 2833.
- Uncheck the **VoIP Silence Suppression** box. By unchecking the **VoIP Silence Suppression** box, calls can be established with the G.729 codec but without silence suppression.
- Check the **Re-invite Supported** box.
- Check **Use Offerer's Preferred Codec** box.
- Uncheck **Codec Lockdown** box.
- Check the **PRACK/100rel** because MTS Allstream supported 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.



5.5.5 Administer T38 Fax Settings

Select the **T38 Fax** tab then uncheck the **Use Default Values** to change the **T38 Fax Version** to **0** which is the matching version that MTS Allstream prefers. Retain the other settings as default as shown below.



Note: In order for fax calls to be successfully transmitted using T.38 as described in **Section 2.2**, observation #**8**, the **Equipment Classification** setting of the fax terminal has to be set to **Fax Machine** as shown **Section 5.11**.

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

5.6 Short Code

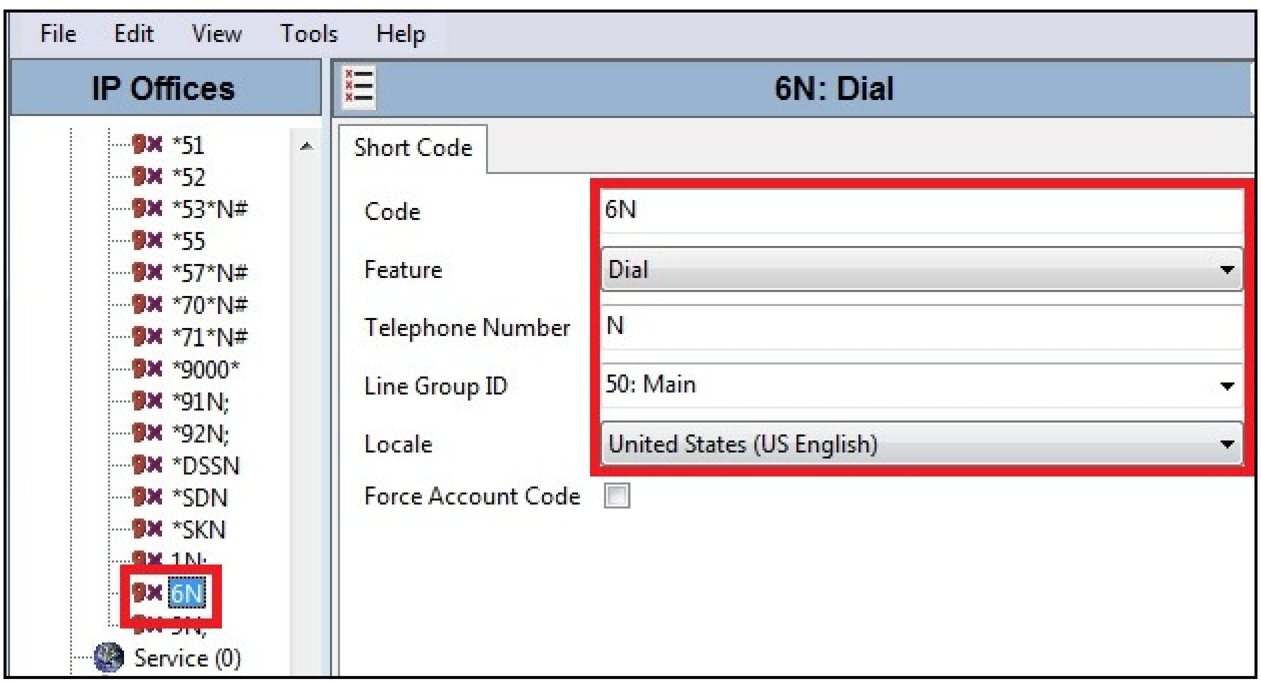
Short Codes were defined to route general outgoing calls and private outgoing calls to PSTN over the SIP Line. In addition, Short Codes were also defined for incoming calls from mobility extensions to access Feature Name Extensions (FNE) hosted on IP Office, or incoming calls to retrieve voice message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

To create a short code, select **Short Code** in the left Navigation Pane then right-click and select **New** (not shown). On the **Short Code** tab in the Details Pane, configure the parameters for the new short code to be created.

The screenshot below shows the details of the Short Code **9N;** that was created for outgoing calls in the test configuration. The digit **9** was used as a prefix that IP Office user will dial to access to SIP Trunk for outgoing calls to PSTN.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, it is **9N;**. This short code will be invoked when the user dials **9** followed by any number.
- Set the **Feature** to **Dial**. This is the feature that the short code will invoke.
- Set the **Telephone Number** to **11129N"@avaylab.com:5060"**. This field is used to construct the "Request URI" and "To" headers of outgoing calls. The value **11129** is the prefix obtained from the service provider and it is assigned per SIP Trunk basis. MTS Allstream requires outgoing calls from IP Office with a pre-define prefix, .e.g. **11129** to support the billing implementation on the SIP Trunk. The value **N** represents the number dialed by the user. The host part following the "@" is the enterprise SIP domain.
- Set the **Line Group ID** field to **18** which is the outgoing line group number defined on the **SIP URI** tab of the **SIP Line** in **Section 5.5.1**. This short code will use this line group when placing outgoing calls.
- Set **Locale** to **United State (US English)**.

The **9N;** short code illustrated above does not provide a means of alternate routing if the configured SIP Line is out of service or temporarily does not respond. When alternate routing options and/or more customized analysis of the digits following the short code are desired, the Automatic Route Selection (ARS) feature may be used. In the following example screenshot, the short code **6N** is illustrated for accessing ARS. When the IP Office user dials **6** plus any number **N**, rather than being directed to a specific **Line Group Id**, the call will be directed to **Line Group Id 50: Main**, configurable via ARS. See **Section 5.9** for example ARS route configuration for **50: Main** as well as a backup route.



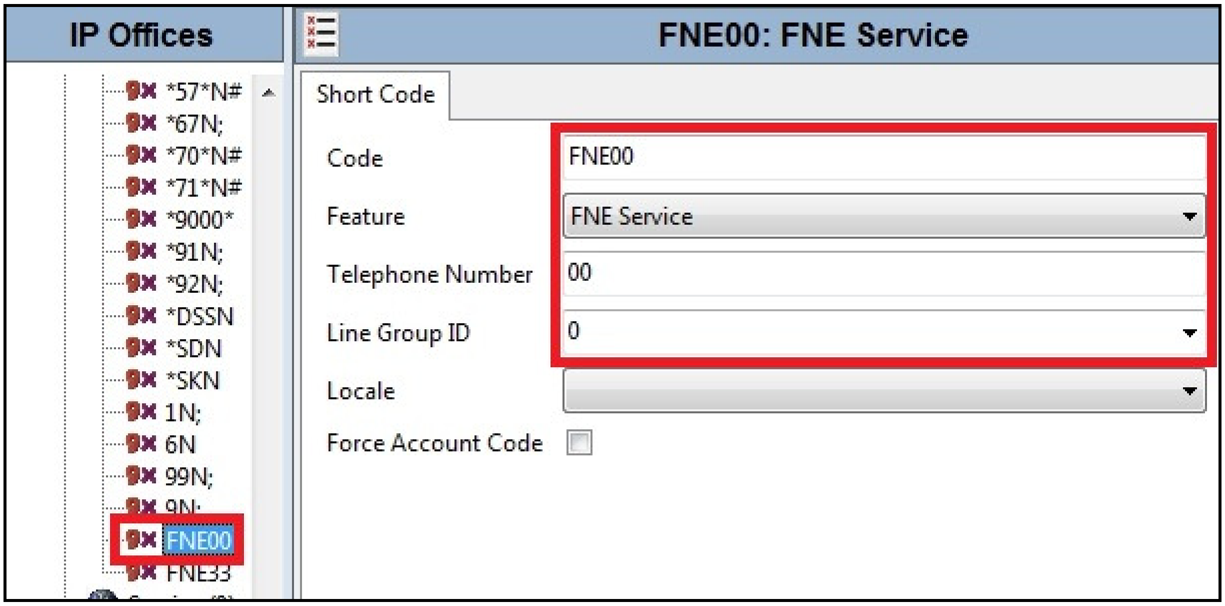
For private outgoing calls, Short Code ***67N;** was created as shown in the screenshot below. The digits ***67** was used as a prefix that IP Office user will dial to access to the SIP Trunk for private outgoing calls to PSTN. This causes the called PSTN party not to display Calling Party Name and Number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

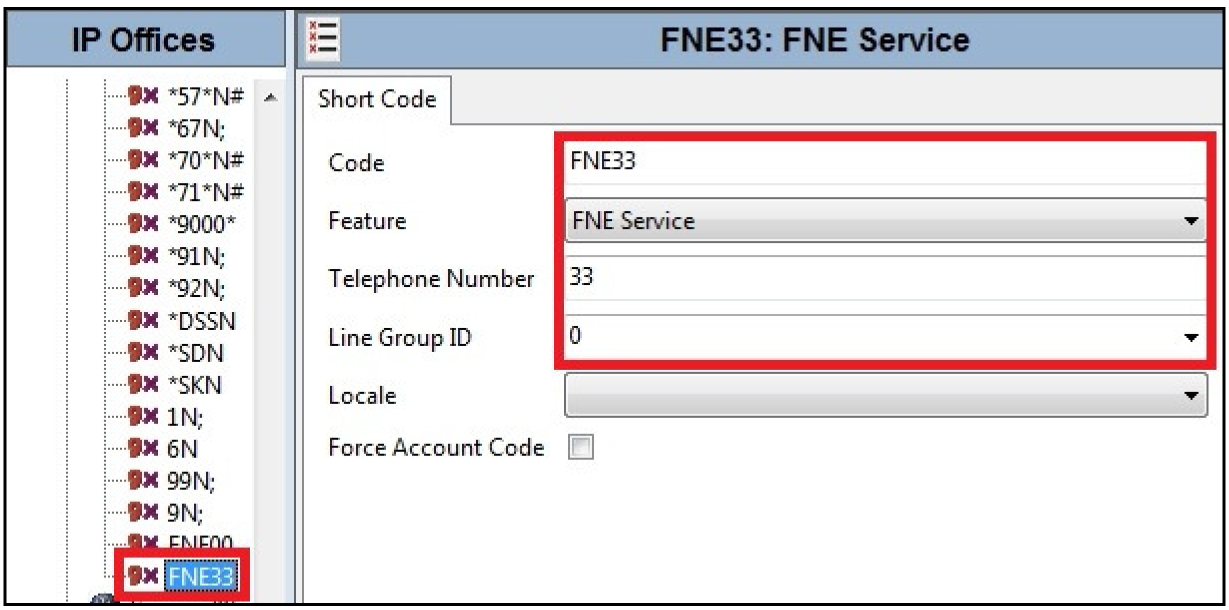
- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, it is ***67N;**. This short code will be invoked when the user dials ***67** followed by any number.
- Set the **Feature** to **Dial**. This is the feature that the short code will invoke.
- Set the **Telephone Number** to **W11129N"@avaylab.com:5060"**. This field is used to construct the "Request URI" and "To" headers of 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 for private outgoing calls. The value **11129** is the prefix obtained from the service provider, it is assigned per SIP Trunk basis. MTS Allstream requires outgoing calls from IP Office with a pre-define prefix, .e.g. **11129** to support the billing implementation on the SIP Trunk. The value **N** represents the number dialed by the user. The host part following the "@" is the enterprise SIP domain.
- Set the **Line Group ID** field to **18** which is the outgoing line group number defined on the **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)**.

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 respectively created. The **FNE00** and **FNE33** were configured with the following parameters.

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

Following screenshots illustrate **FNE00** and **FNE33** configurations.



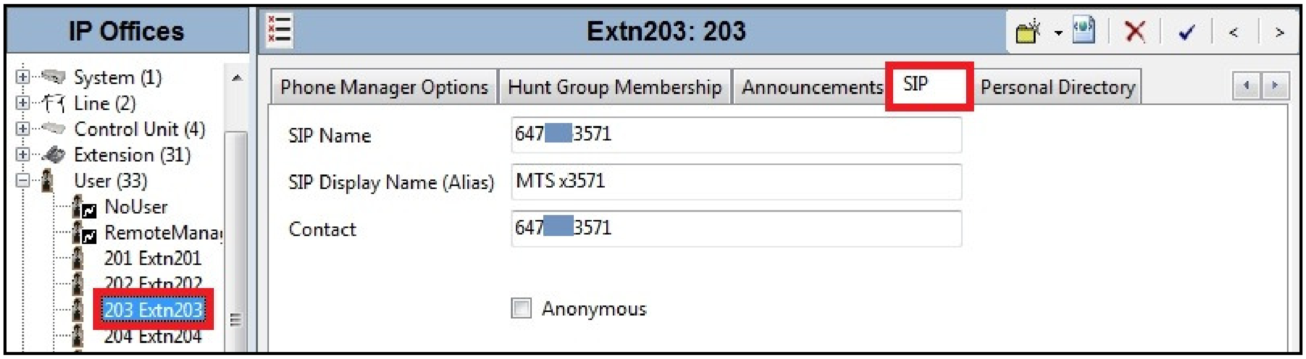


When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.7 User

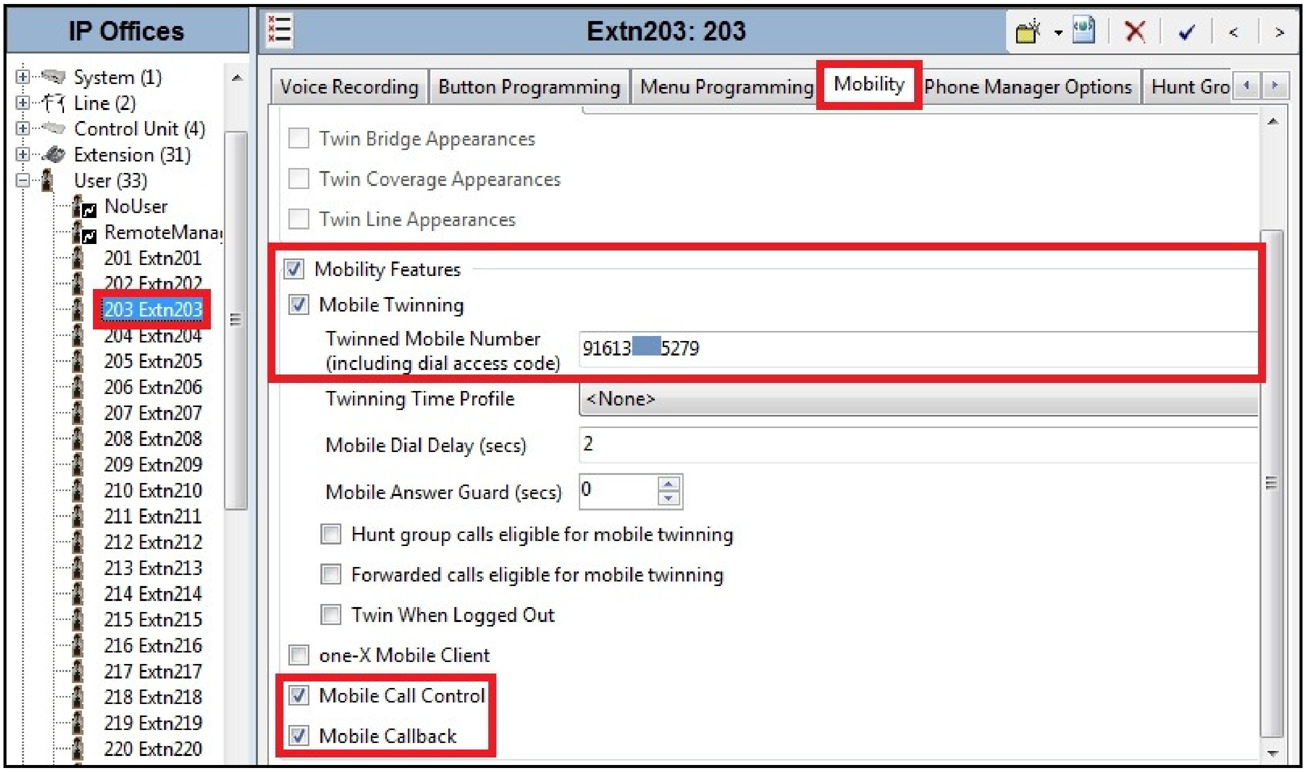
Configure the SIP parameters for each user that will be placing and receiving calls via the SIP Line as defined in **Section 5.5**. To configure these settings, first select **User** in the left Navigation Pane, and then select the name of the user to be modified.

In the example below, with the user **Extn203** selected, select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** and **Contact** fields are used as the 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**). The **SIP Name** and **Contact** fields were set to one of the DID numbers assigned to the enterprise by MTS Allstream, e.g. **647XXX3571**. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name, e.g., **MTS x3571**. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user information from the networks.



Mobile Twinning feature may be enabled on the user to allow incoming calls to simultaneously alert the desk phone and the mobile phone. The following screenshot shows the **Mobility** tab.

- The **Mobility Features** and **Mobile Twinning** boxes were checked.
- The **Twinned Mobile Number** was configured with the number to reach the twinned mobile telephone, in this case it was **91613XXX5279** including digit 9 as the dial access code and 1613XXX5279 as the mobility extension.
- Check **Mobile Call Control** to allow incoming calls from mobility extension to access FNE00 (see **Section 5.6**).
- 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 5.6**).
- Other options can be set according to customer requirements.



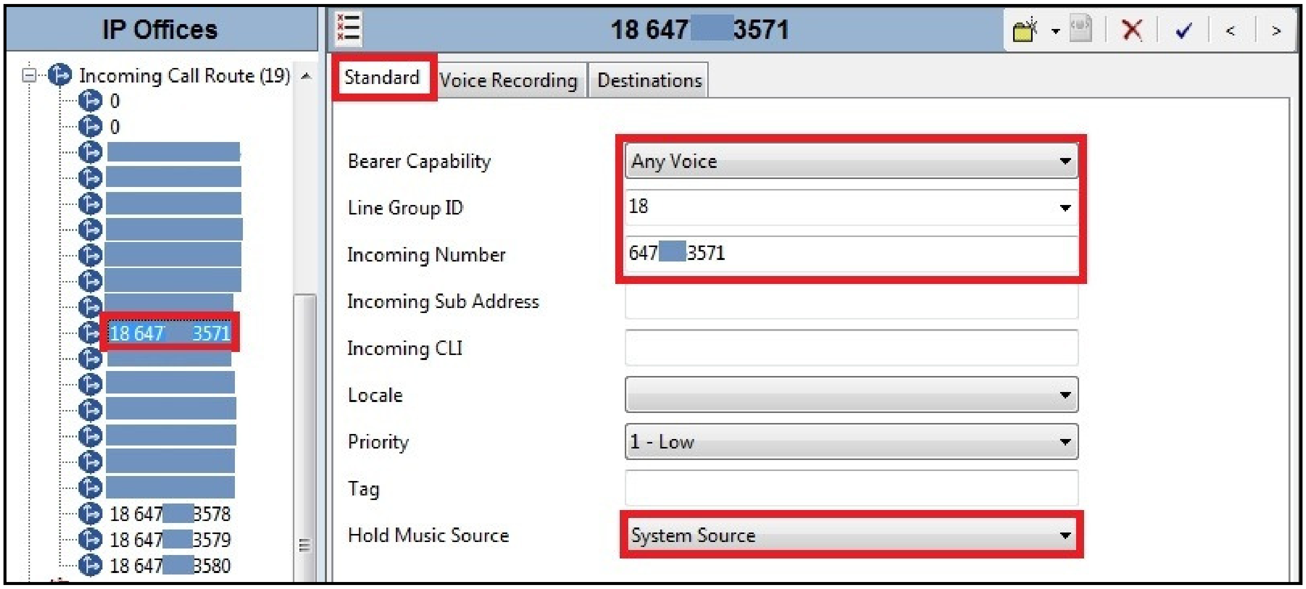
When complete, click OK to commit (not shown) then press Ctrl + S to save.

5.8 Incoming Call Route

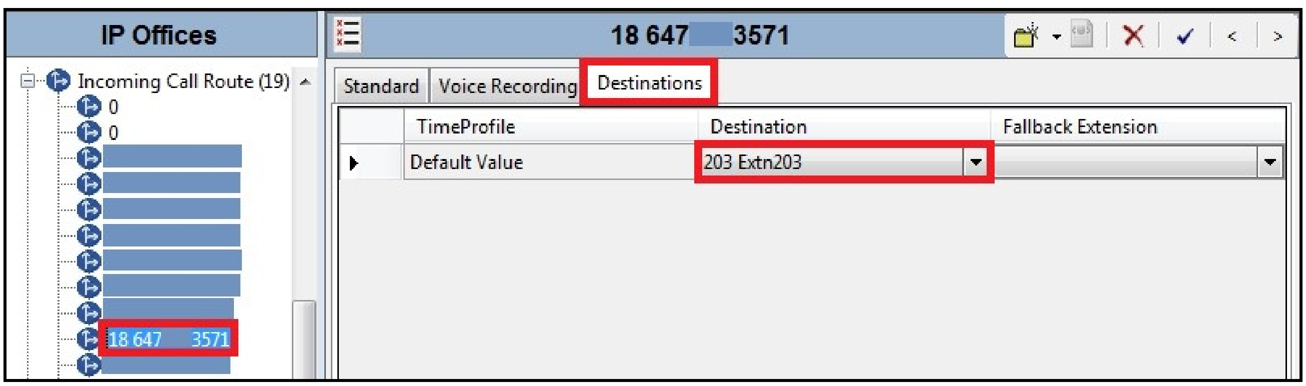
An Incoming Call Route maps an incoming call on a specific SIP Line to an internal extension. This procedure should be repeated for each DID number provided by the service provider. To create an Incoming Call Route, right click on the **Incoming Call Route** in the left Navigation Pane and select **New**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

- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group ID** to SIP Line **18** as defined in **Section 5.5**.
- Set the **Incoming Number** to the DID number that associate to the internal extension.
- Set **Locale** to **United State (US English)**
- Default values can be used for all other fields.

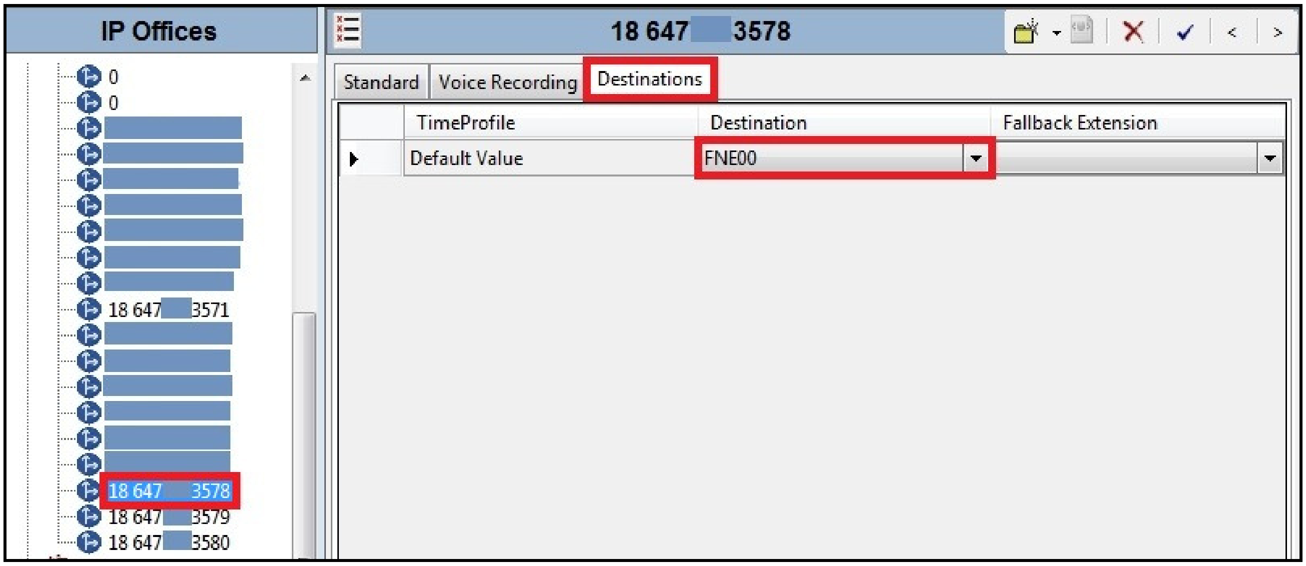
The screenshot below shows Incoming Call Route **18 647XXX3571** configured to receive an incoming call to DID number **647XXX3571** then alert local station **203**.

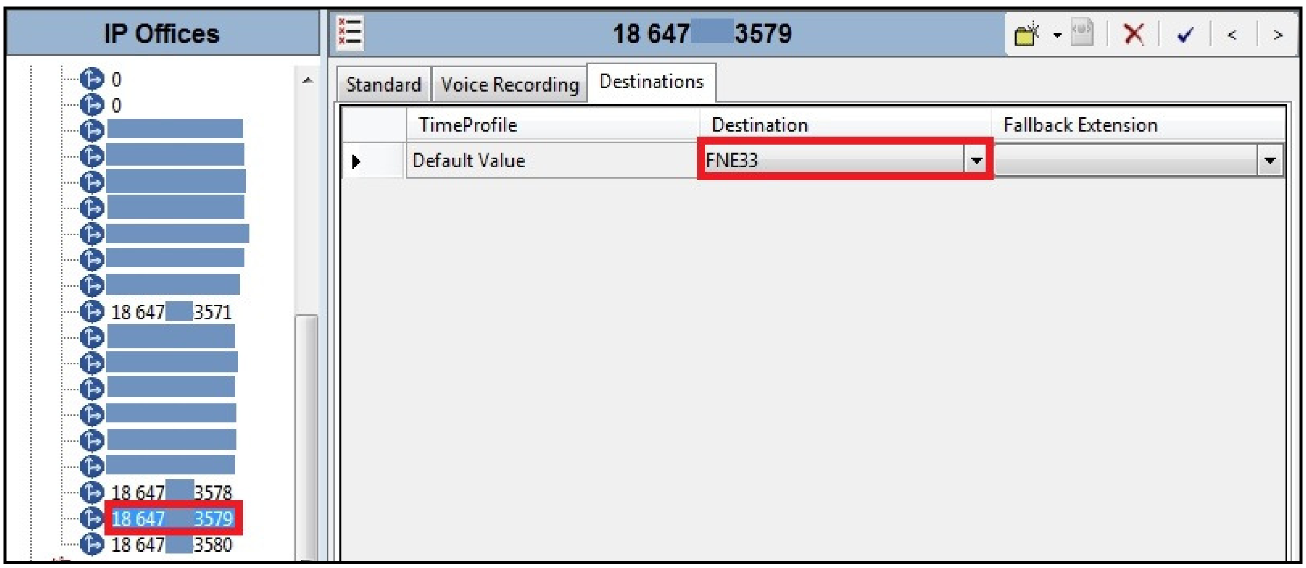


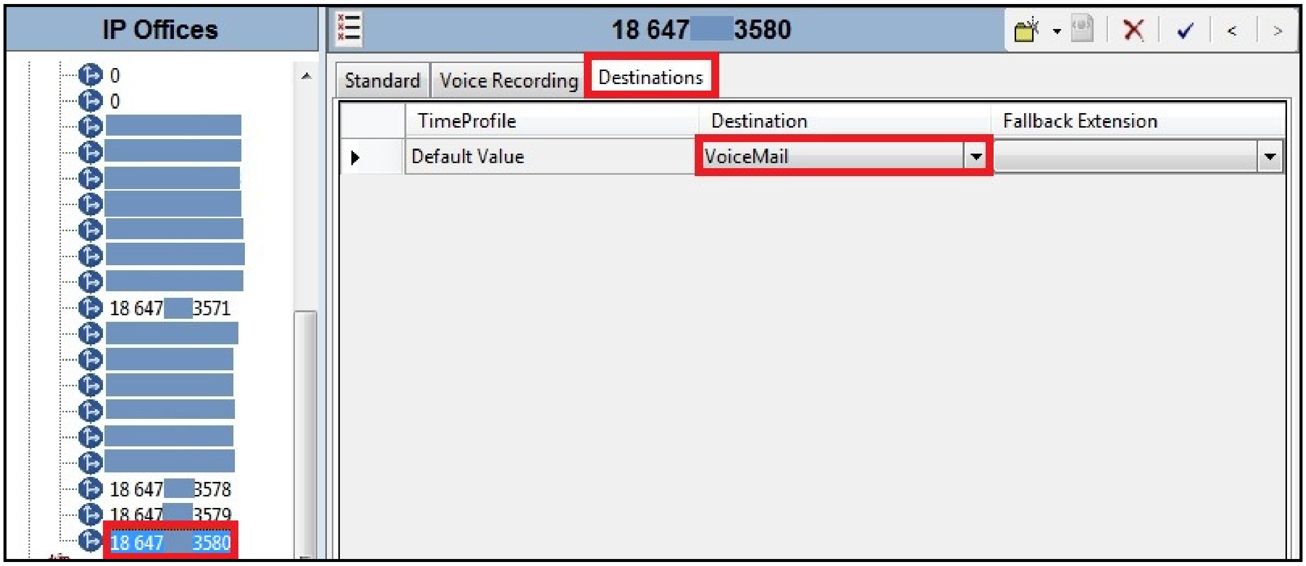
On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. In this example, incoming calls to **647XXX3571** on SIP Line 18 are routed to extension **203 Extn203**.



Following screenshots show Incoming Call Routes to receive incoming calls to DID numbers **647XXX3578**, **647XXX3579** and **647XXX3580** that were similarly configured to access **FNE00**, **FNE33** and **VoiceMail**. The **Destinations** were appropriately defined as **FNE00**, **FNE33** and **VoiceMail**. **Note**: FNE00 and FNE33 were entered manually by selecting **Destination** as **DialIn** (not shown) then input the appropriate FNE feature code.


IP Offices
18 647 3578
Standard
Voice Recording
Destinations
TimeProfile
Destination
Fallback Extension
Default Value
FNE00
0
0
18 647 3571
18 647 3578
18 647 3579
18 647 3580


IP Offices
18 647 3579
Standard
Voice Recording
Destinations
TimeProfile
Destination
Fallback Extension
Default Value
FNE33
0
0
18 647 3571
18 647 3578
18 647 3579
18 647 3580



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

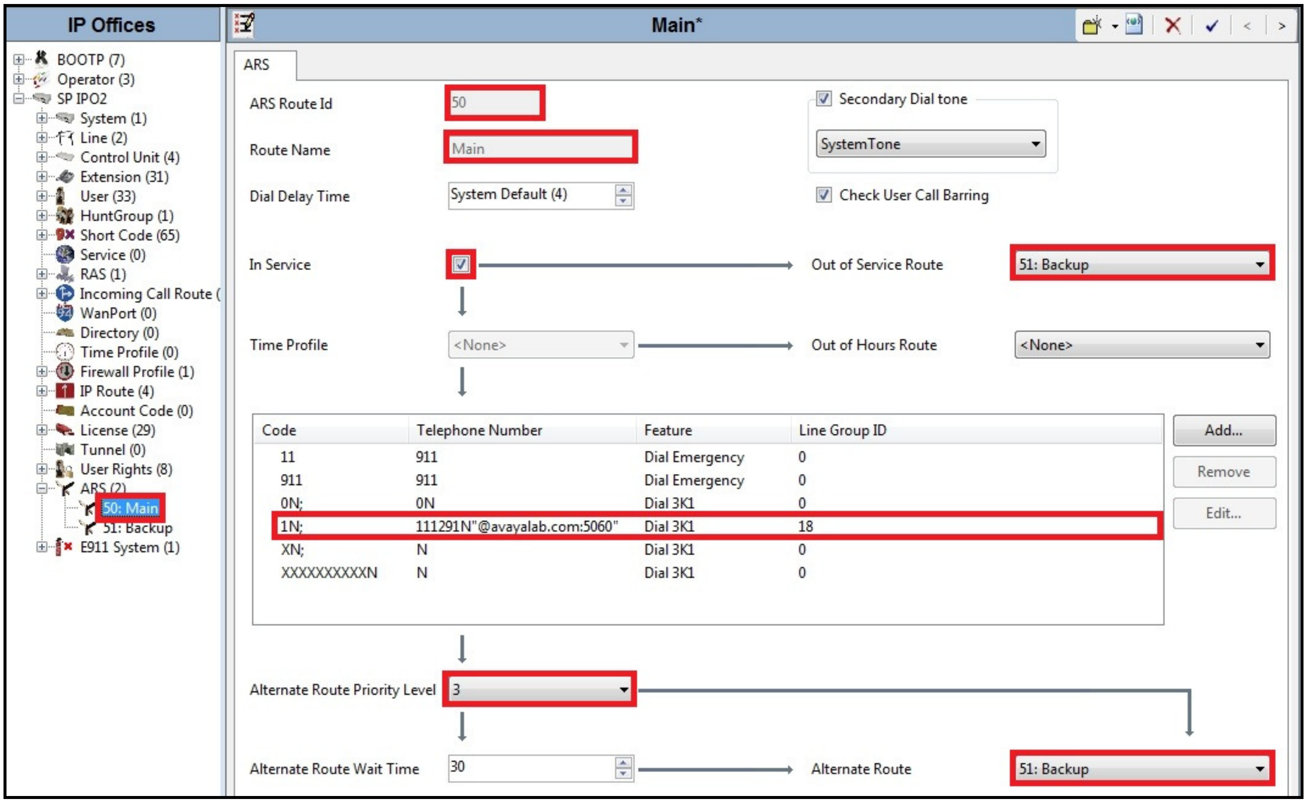
5.9 ARS and Alternate Routing

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 **9N;** 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.

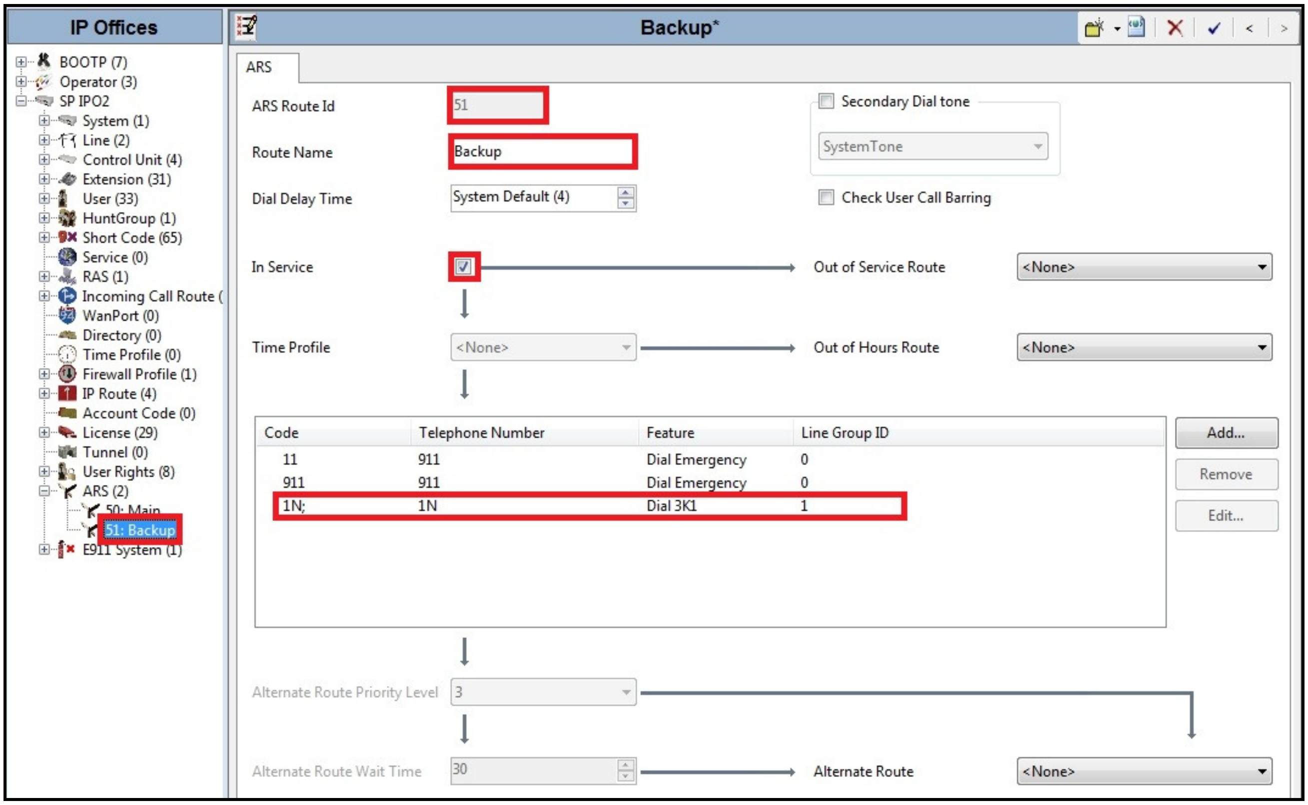
A new ARS entry can be created by right-click **ARS** in the Navigation pane then select **New** (not shown). To view or edit an existing ARS route, select **ARS** in the Navigation pane then select the appropriate route name.

The following screenshot shows an example configuration for ARS **50:Main**. The **In Service** parameter refers to the ARS form itself. If the **In Service** box is unchecked, calls are routed to the ARS route name specified in the **Out of Service Route** parameter. IP Office Short Codes may also be defined to allow an ARS route to be disabled or enabled from a telephone. The provisioning of an Out of Service Route and the means to manually activate the 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**, the dial prefix **11129** will be prepended as per the requirement from MTS Allstream. Then the call will be directed to Line Group 18, which is the SIP Line configured and described in these Application Notes. If the Line Group 18 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 the calling users to the value in the **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, the call 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 (sans 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 the **Add…** button to 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.

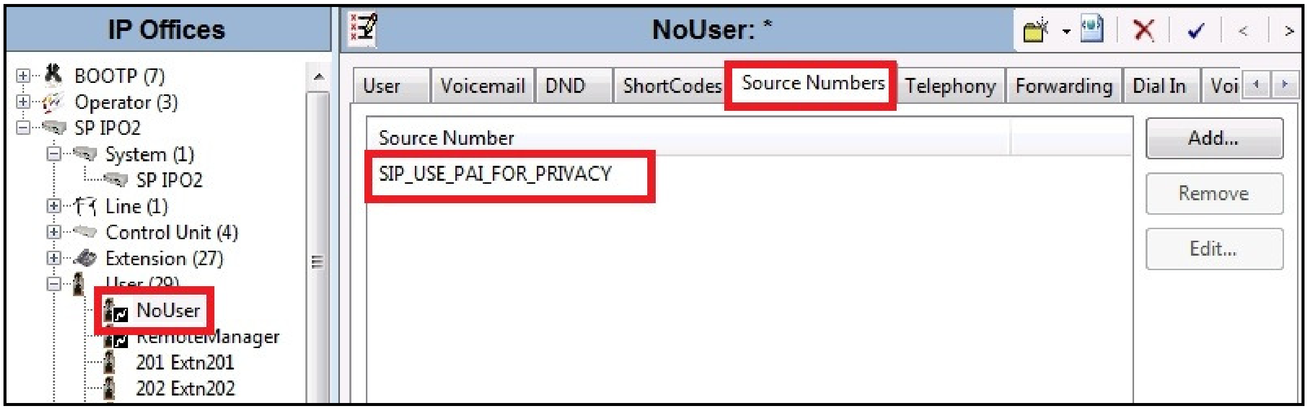
5.10 Privacy/Anonymous Calls

For outgoing calls with privacy (anonymous) enabled by dialing Short Code *67 as shown in **Section 5.6** or checking on the **Anonymous** option on **SIP** tab under **User** settings as shown in **Section 5.7**, IP Office will replace Calling Party Number in the "From" and "Contact" headers with "restricted" and "anonymous" respectively. IP Office can be configured to use the "P-Preferred-Identity" or "P-Asserted-Identity" header to pass the actual Calling Party information for authentication and billing purposes. For the compliance testing, the "P-Asserted-Identity" header was used.

To configure IP Office to use the "P-Asserted-Identity" header for private calls, navigate to **User → noUser** in the Navigation Pane. Select the **Source Numbers** tab in the Details Pane. Click the **Add** button (not shown).

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

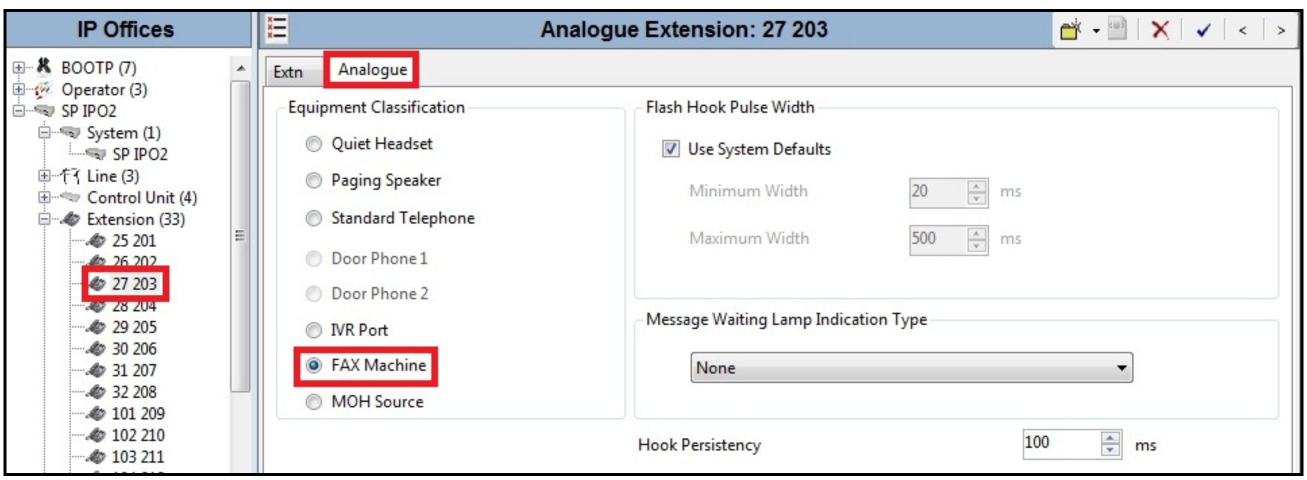
The **SIP_USE_PAI_FOR_PRIVACY** parameter will appear in the list of Source Numbers as shown below.



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

5.11 Extension Settings for T.38 Fax Calls

In order for fax calls to be successfully transmitted using T.38 as described in **Section 2.2**, observation #**8**, the **Equipment Classification** setting of the fax terminal has to be set to **Fax Machine** as shown in the screenshot below.



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

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

The compliance testing comprised the configuration for two major components, Trunk Server for the 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 the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for the service provider - MTS Allstream:

- 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:

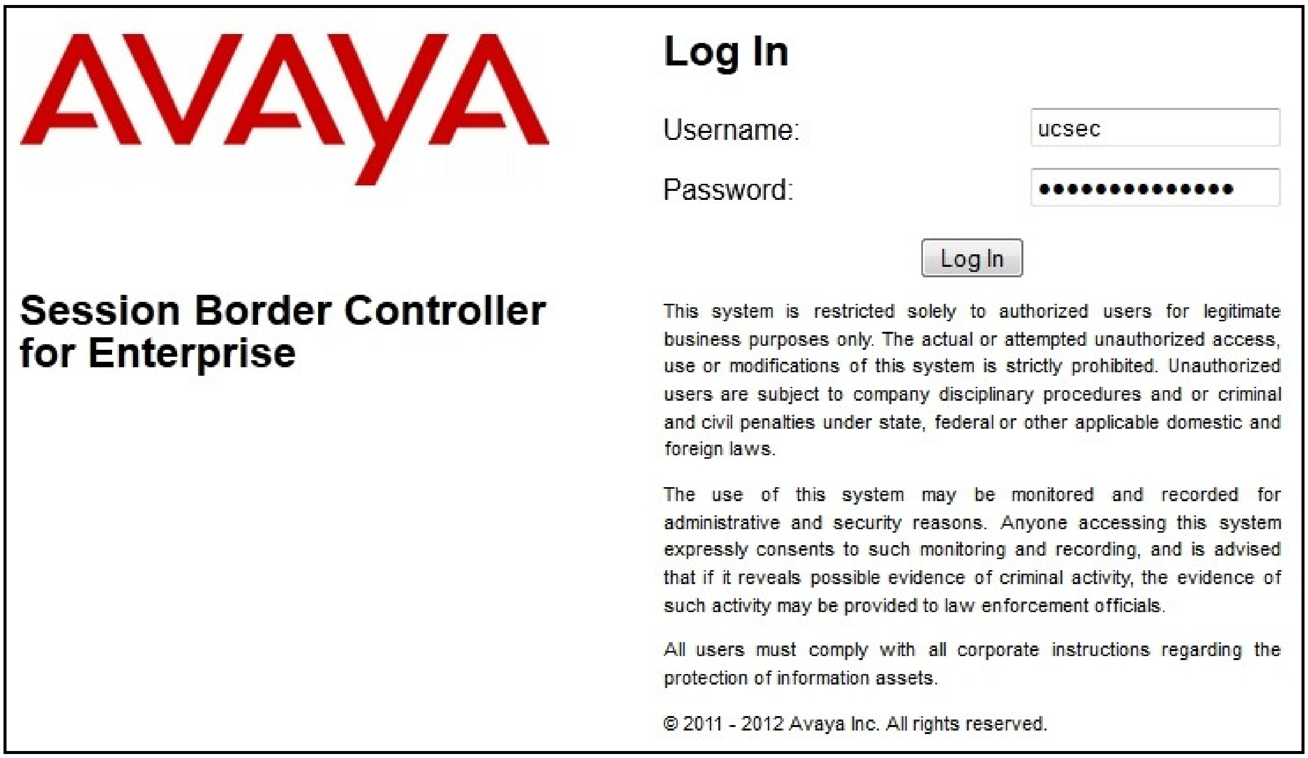
- Global Profiles:
    - URI Groups
    - Routing
    - Topology Hiding
    - Server Interworking
    - Server Configuration
- Domain Policies:
    - Application Rules
    - Media Rules
    - Signaling Rules
    - Endpoint Policy Group
    - Session Policy
- Device Specific Settings:

- o Network Management
- o Media Interface
- o Signaling Interface
- o End Point Flows → Server Flows
- o Session Flows

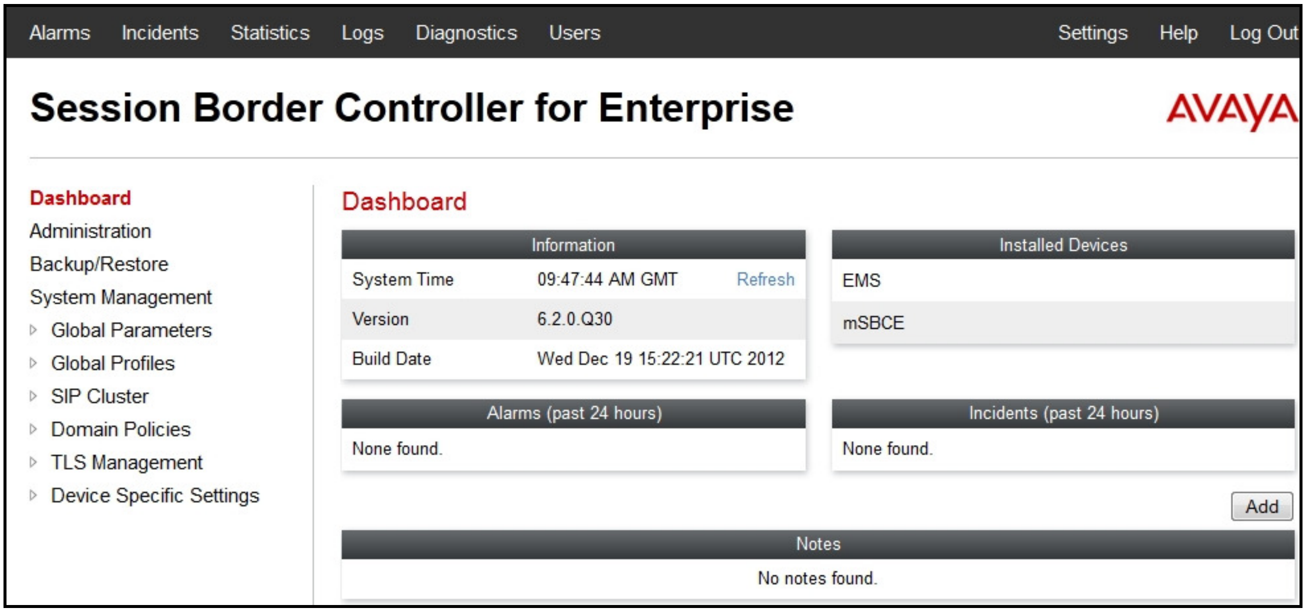
6.1 Log into the Avaya Session Border Controller for Enterprise

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

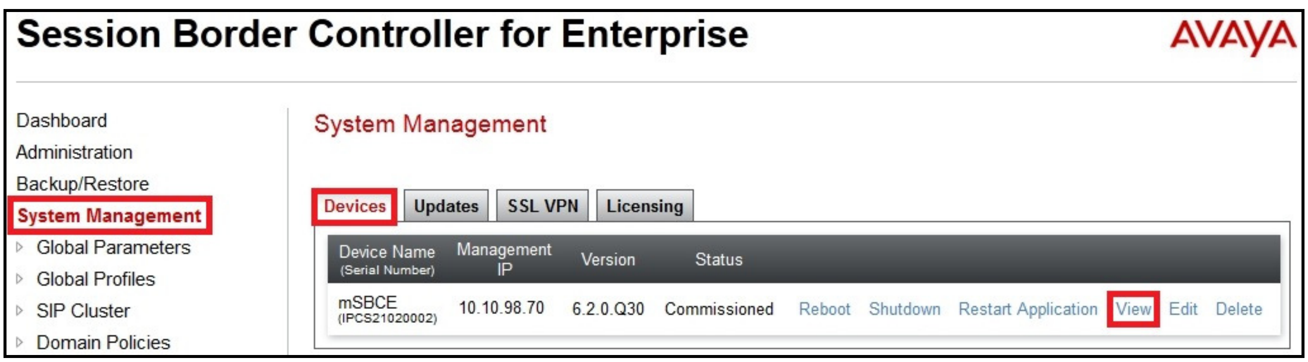
Enter the appropriate credentials then click **Log In**.



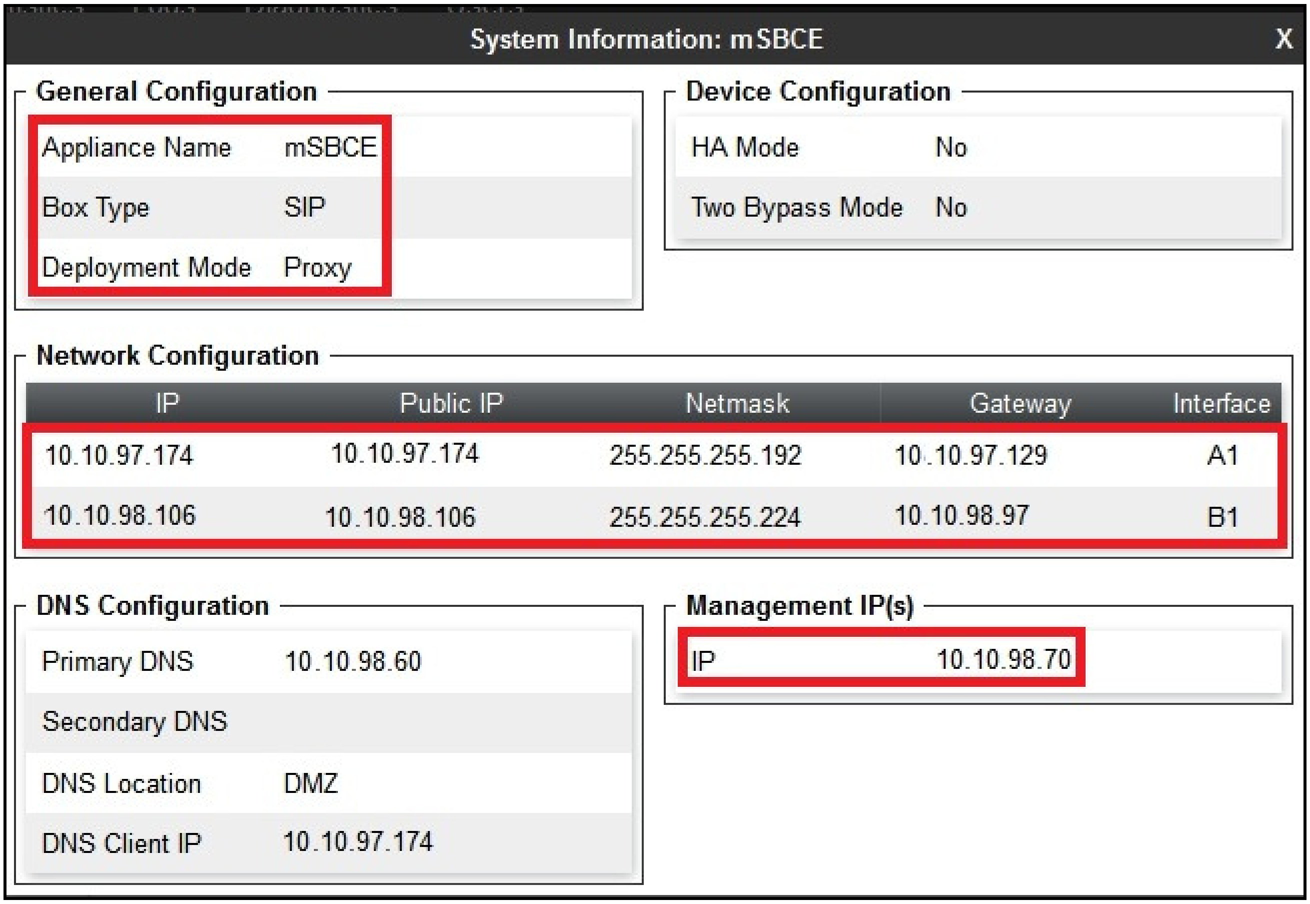
The **Dashboard** main page will appear as shown below.



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 the **View** as shown in the screenshot below.



The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponded to **Figure 1**. The **Box Type** was set to **SIP** and the **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 an URI Group, select **Global Profiles → URI Groups** and click on the **Add Group** button (not shown).

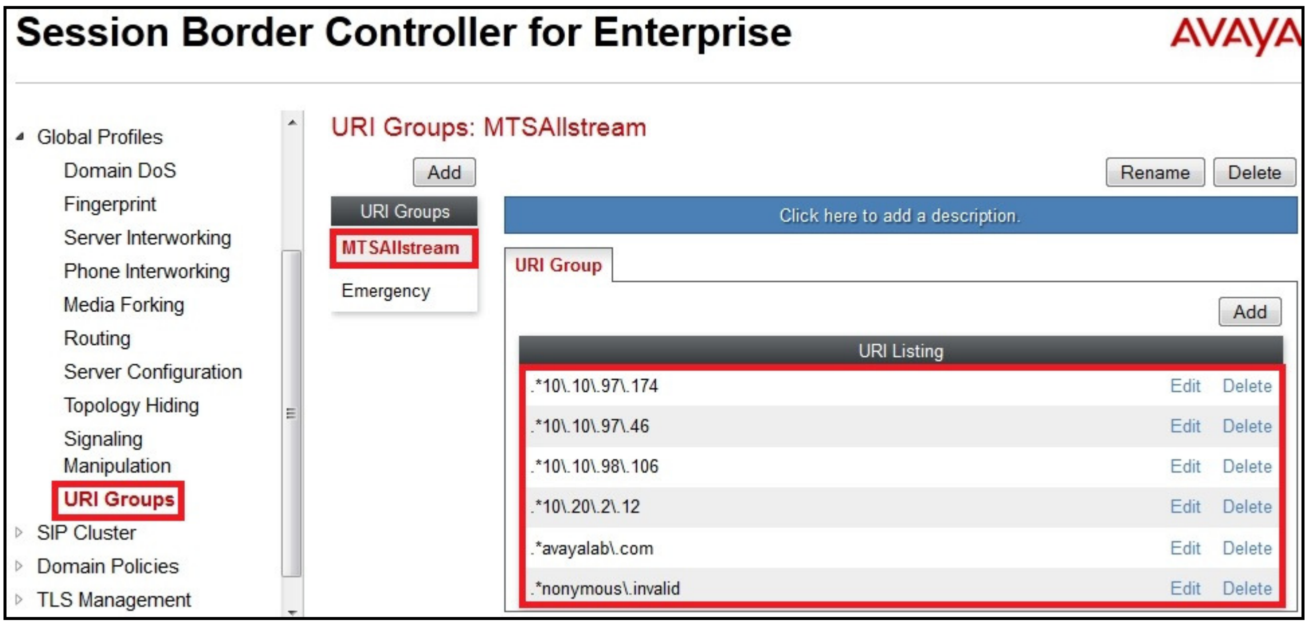
In the compliance testing, URI Group **MTSAllstream** was added with URI type as **Regular Expression**. It consists of enterprise SIP domains "**.*avaya\.com**" for regular calls and "**.*nonymous\.invalid**" for private calls, IP address based service provider SIP domains "**.*10\.20\.2\.12**" and "**.*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 the service provider had the same IP address based SIP domains defined for regular calls.

SIP domain "**.*nonymous\.invalid**" was defined for private outgoing calls from IP Office which URI-Host is masked as **anonymous.invalid**. The enterprise SIP domain "**.*avaya\.com**" was defined as per description in **Section 5.5.1** for the enterprise SIP traffic originated from IP Office. For the public SIP Trunk between the Avaya SBCE and MTS Allstream, the URI-Host in the "From", "PAI", and "Diversion" headers includes SIP domain "**10.10.98.106**" while the URI-Host in the "Request-URI" and "To" headers will have SIP domain "**10.20.2.12**". These domains are assigned by MTS Allstream. The IP addresses and value of URI-Host in OPTIONS heartbeat were also defined to route incoming and outgoing OPTIONS between IP Office and MTS Allstream.

The URI-Group **MTSAllstream** was used to match the "From" and "To" headers in a SIP call dialog received from both IP Office and MTS Allstream. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (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 MTS Allstream 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 **MTSAllstream**.



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.

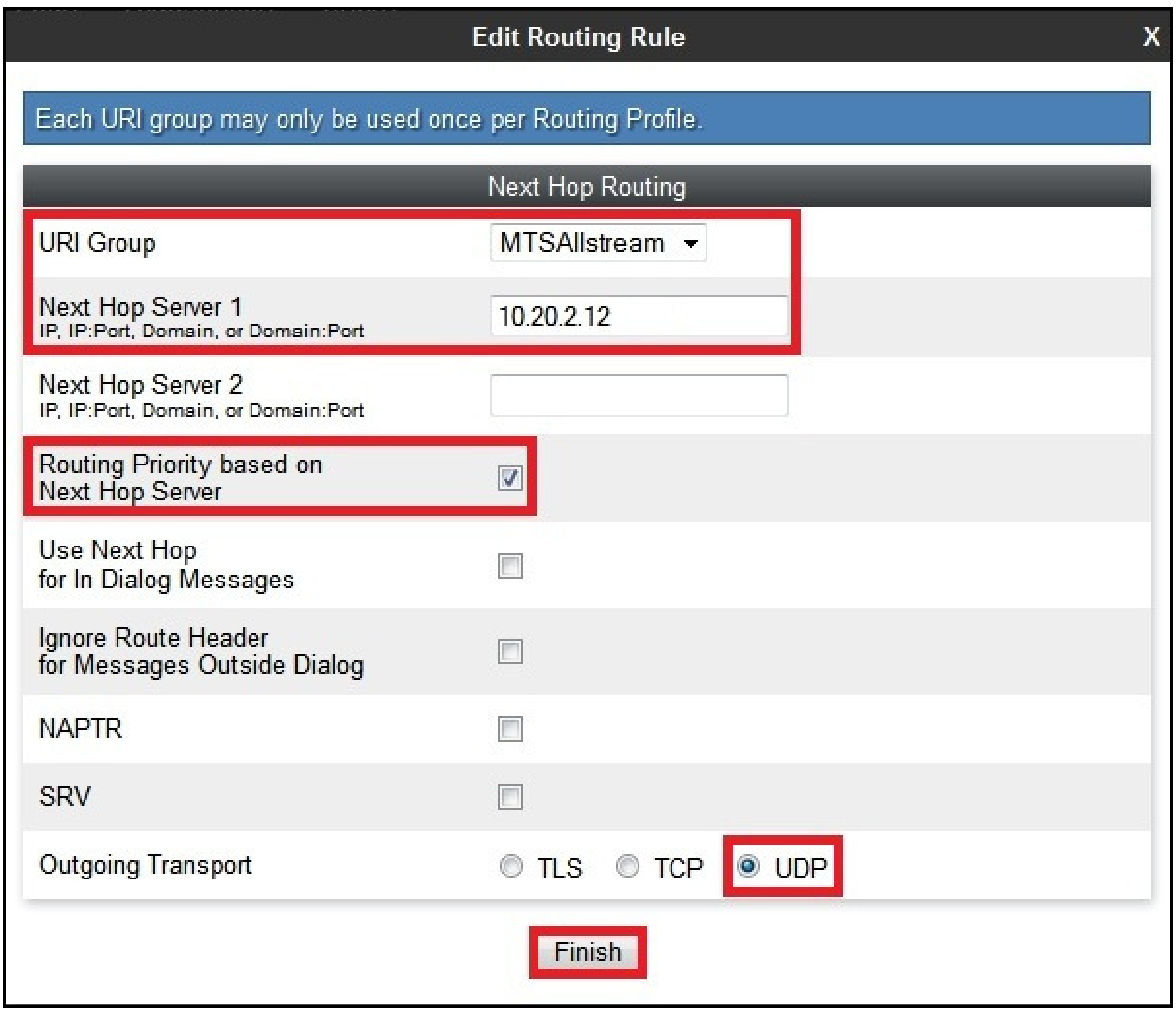
To create a Routing profile, select **Global Profiles → Routing** then click on the **Add Profile** button (not shown).

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

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 MTS Allstream. This entry is to route incoming calls from MTS Allstream to the enterprise.

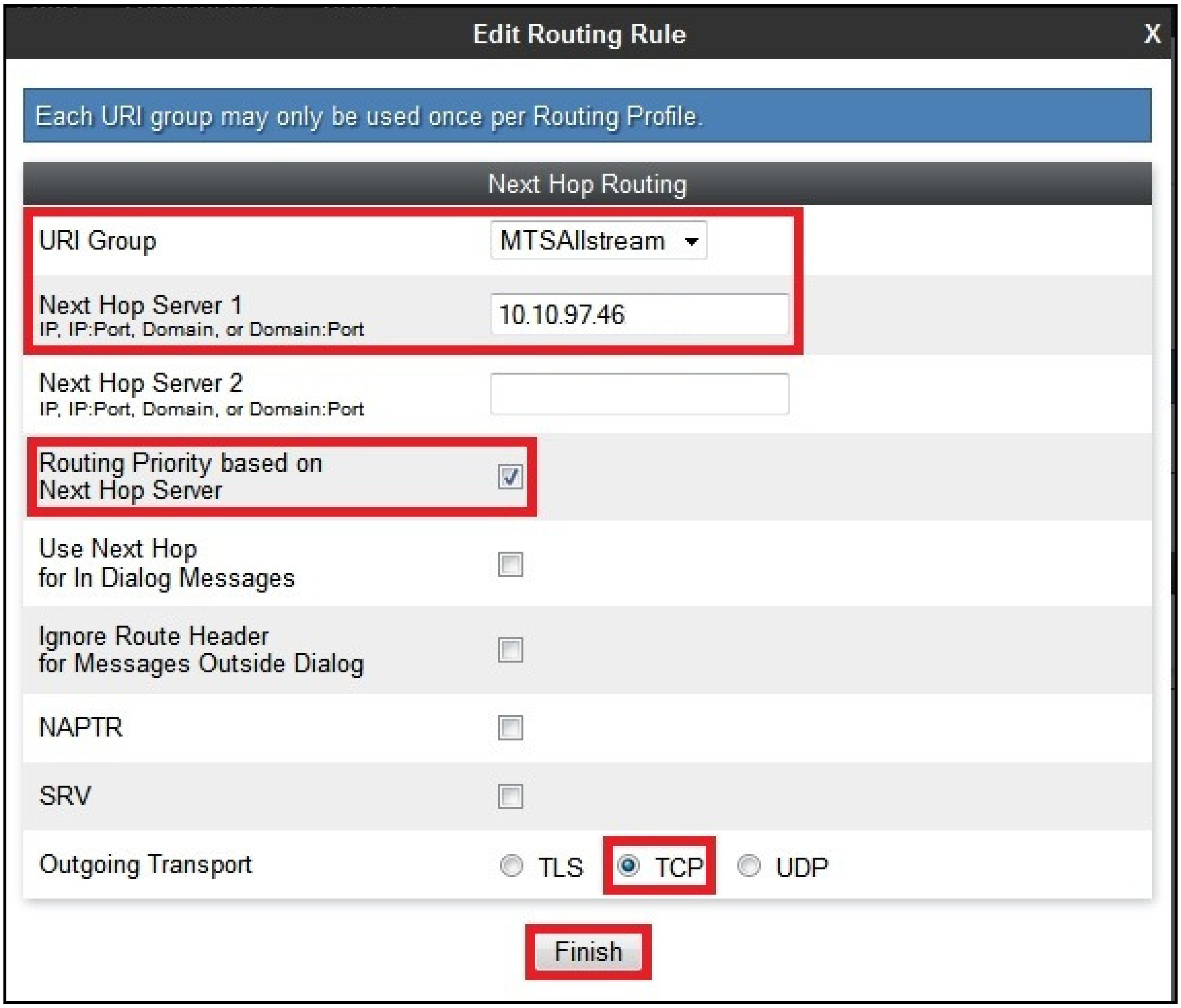
6.2.2.1 Routing Profile for MTS Allstream

To display **Edit Routing Rule** dialog of Routing profile **To_MTSAllstream**, select **Global Profiles → Routing**: **To_MTSAllstream**. As shown in the screenshot below, if there is a match on the SIP domain of the "To" header with the URI Group **MTSAllstream** defined in **Section 6.2.1**, outgoing calls will be routed to the **Next Hop Server 1** as defined as **10.20.2.12** which is the IP address of MTS Allstream Trunk Server, on implied default port **5060**. As shown in **Figure 1**, MTS Allstream 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 **MTSAllstream** defined in **Section 6.2.1**. As shown in **Figure 1**, 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 the default settings.

6.2.3 Topology Hiding

Topology Hiding is a security feature of the 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 a Topology Hiding profile, select **Global Profiles → Topology Hiding** then click on the **Add Profile** (not shown).

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

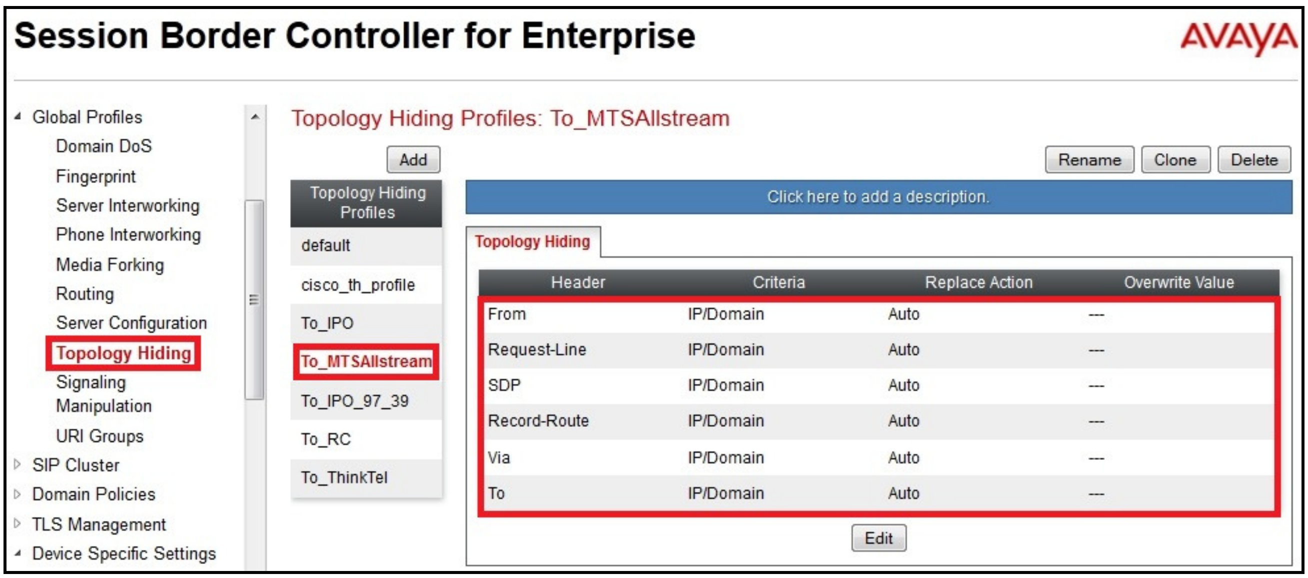
6.2.3.1 Topology Hiding Profile for MTS Allstream

Topology Hiding profile **To_MTSAllstream** was defined for outgoing calls to MTS Allstream to:

- Mask URI-Host of the "Request-URI" and "To" headers with service provider SIP domain **10.20.2.12** to meet the requirements of MTS Allstream. 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 the 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 the SBCE which is known to MTS Allstream.

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

The screenshots below illustrate the Topology Hiding profile **To_MTSAllstream**.

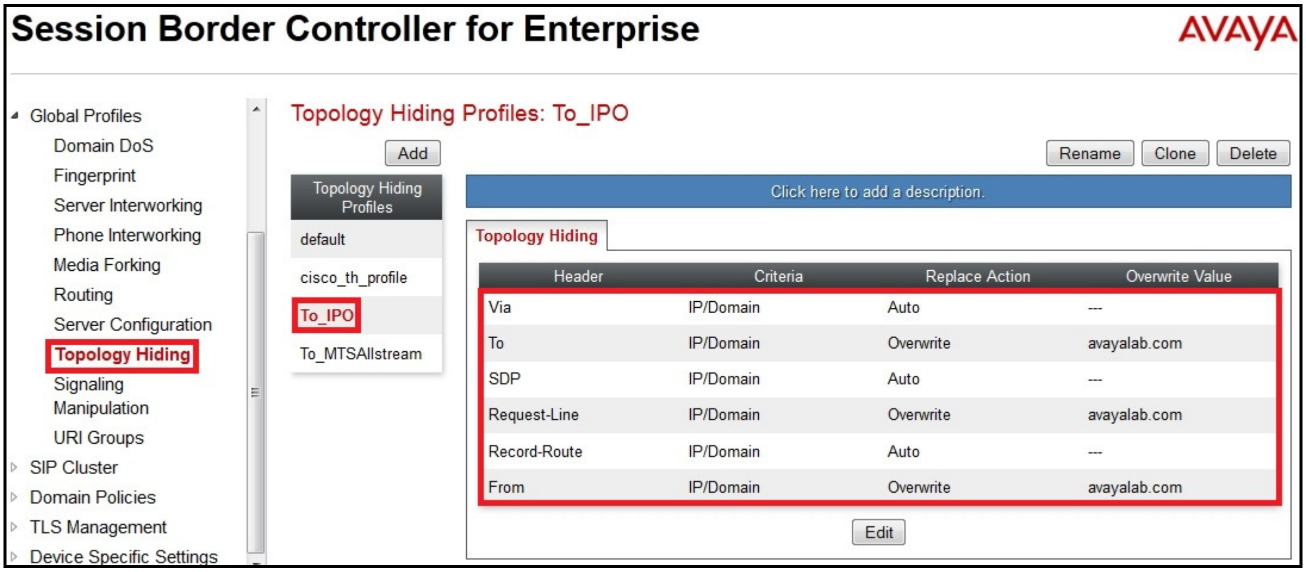


6.2.3.2 Topology Hiding Profile for IP Office

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

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

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



Notes:

- The **Criteria** should be **IP/Domain** to allow the Avaya SBCE to mask both domain name and IP address presenting in the URI-Host.
- The masking applies to the "From" header also applies to the "Referred-By" and "P-Asserted-Identity" headers.
- The 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 a Server Interworking profile, select **UC-Sec Control Center → Global Profiles → Server Interworking** then click on the **Add Profile** button (not shown).

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

6.2.4.1 Server Interworking Profile for MTS Allstream

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

General settings:

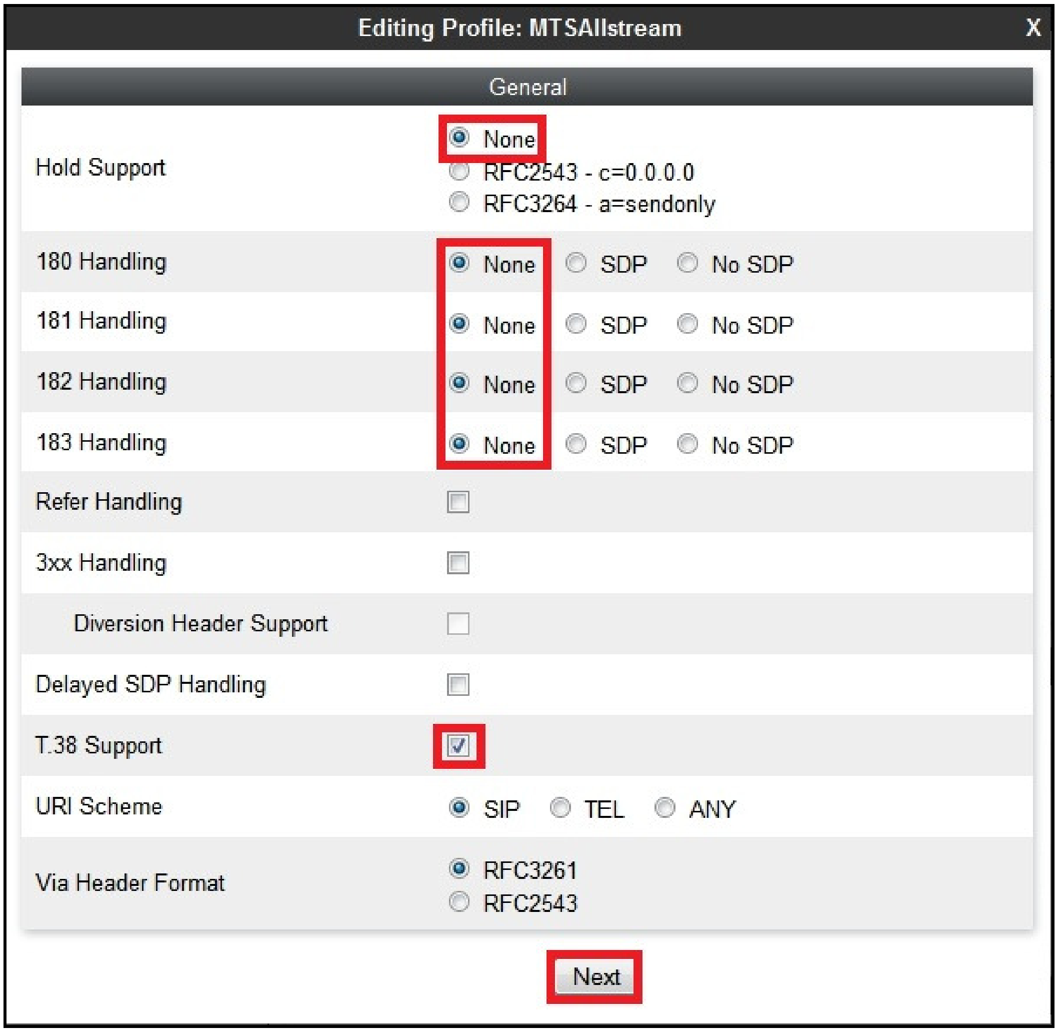
- **Hold Support** = **None**.
- **18X Handling** = **None**. **Refer Handling** = **Unchecked**.
- **T.38 Support** = **Checked**. MTS Allstream supported the T.38 codec for fax over IP in the compliance testing.
- **Privacy Enabled** = **Unchecked**.
- **DTMF Support** = **None**.

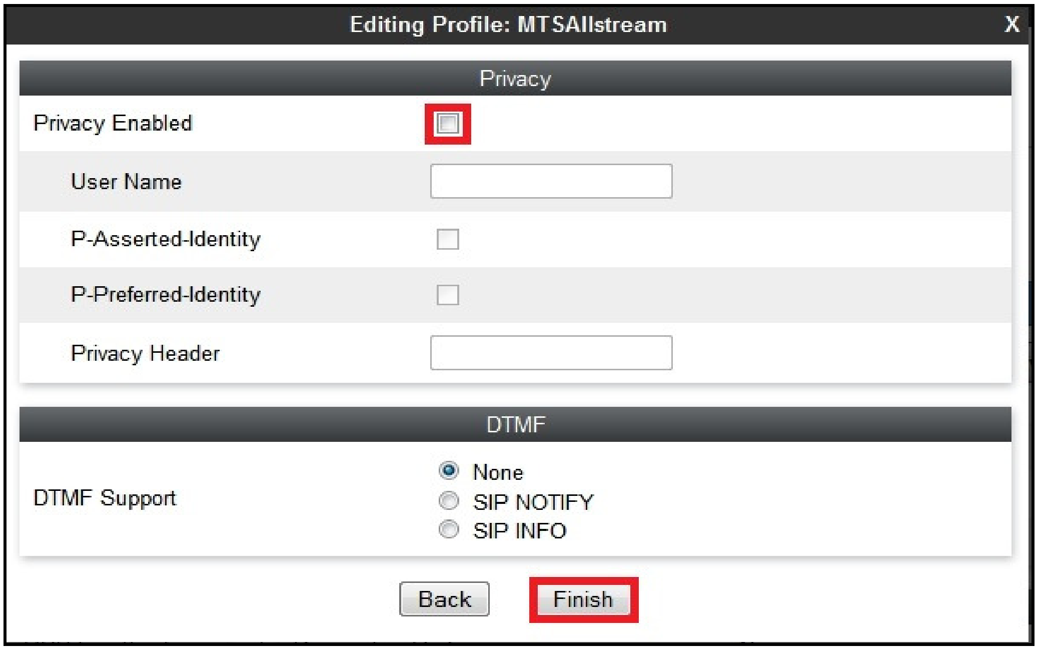
Advanced settings:

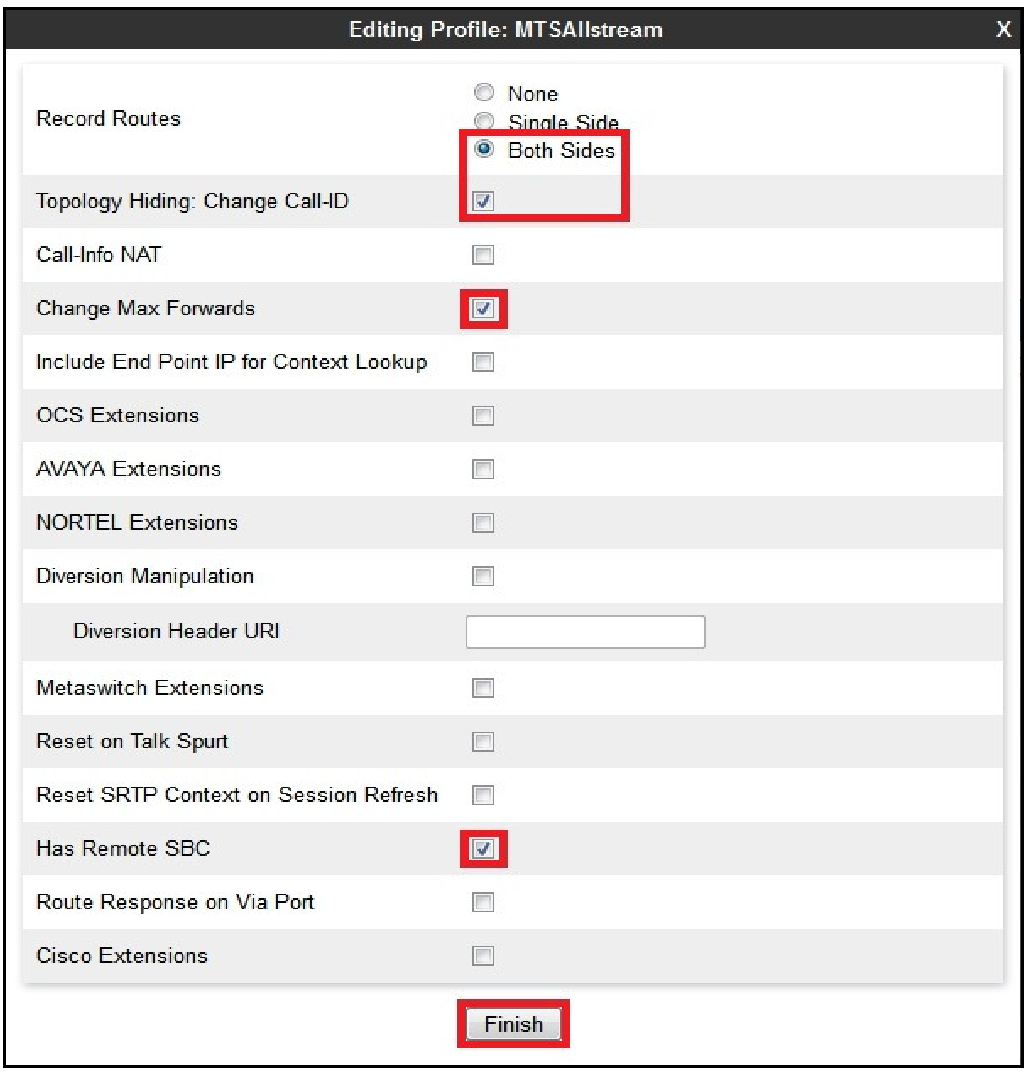
- **Record Routes** = **Both Sides**.

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

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

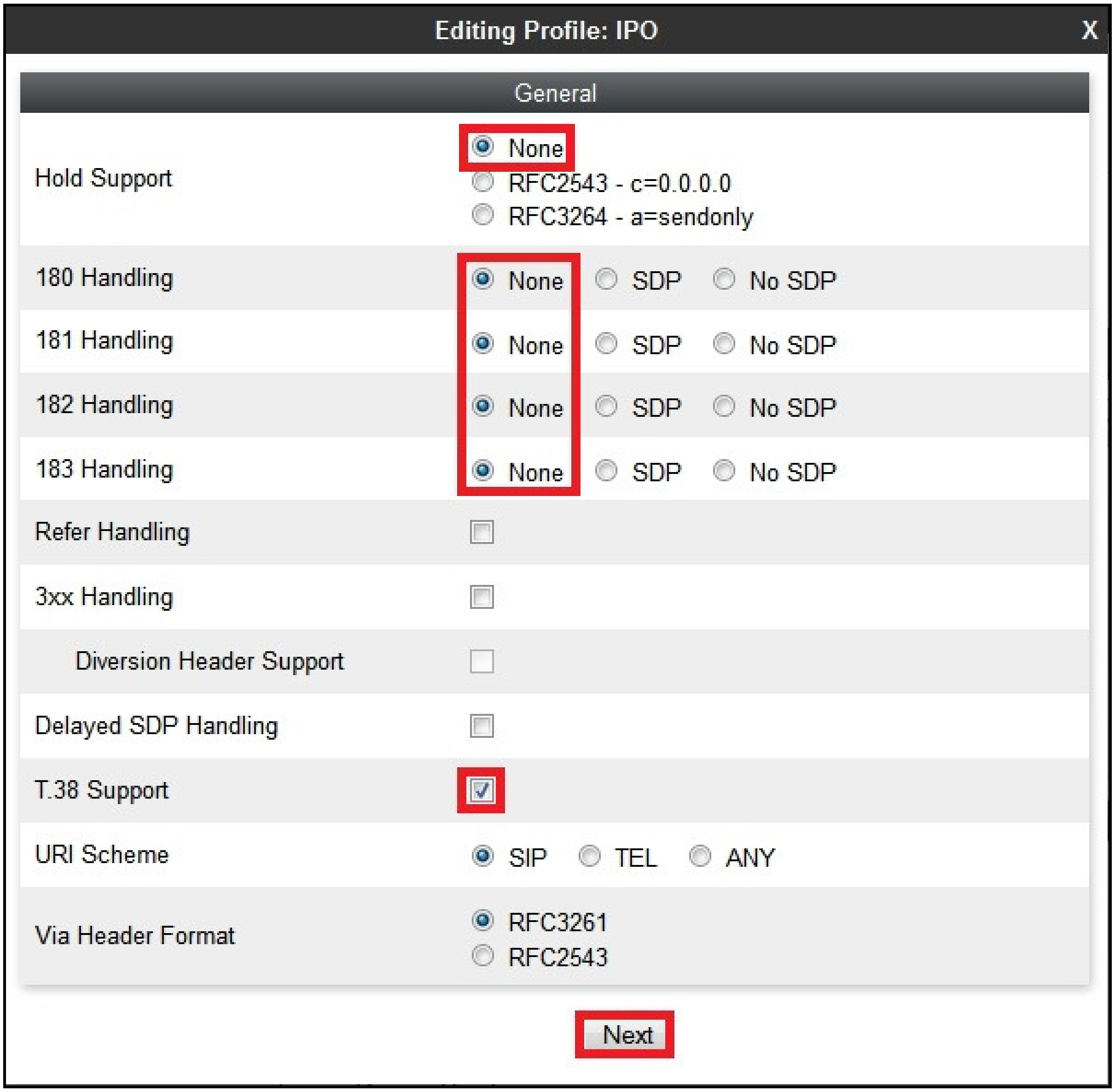


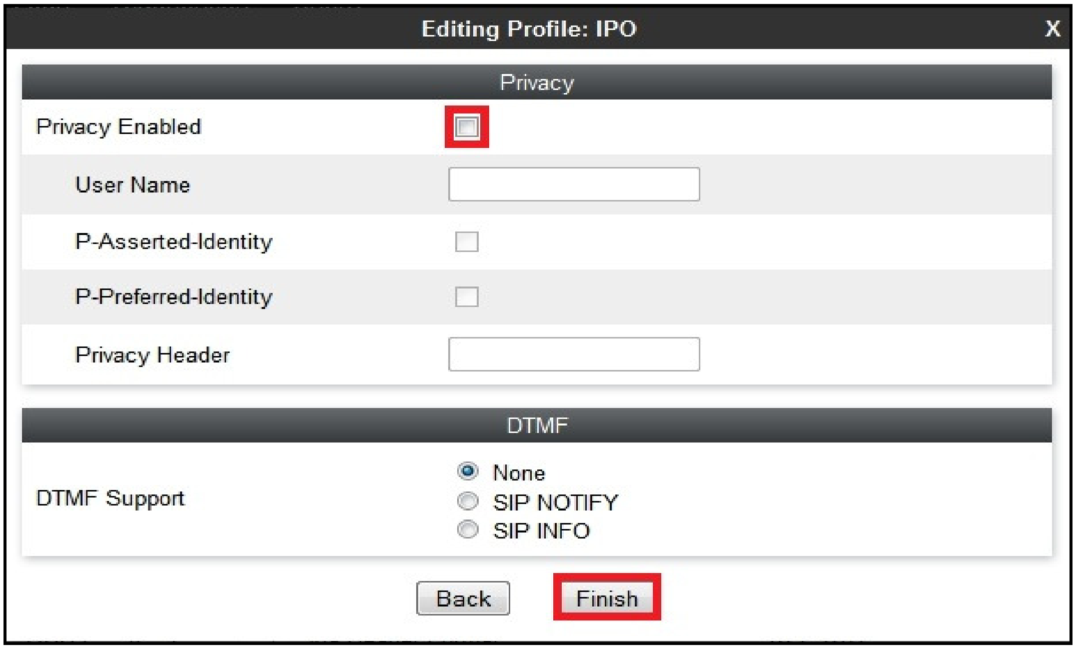

Editing Profile: MTSAllstream
X
Privacy
Privacy Enabled
User Name
P-Asserted-Identity
P-Preferred-Identity
Privacy Header
DTMF
DTMF Support
None
SIP NOTIFY
SIP INFO
Back
Finish

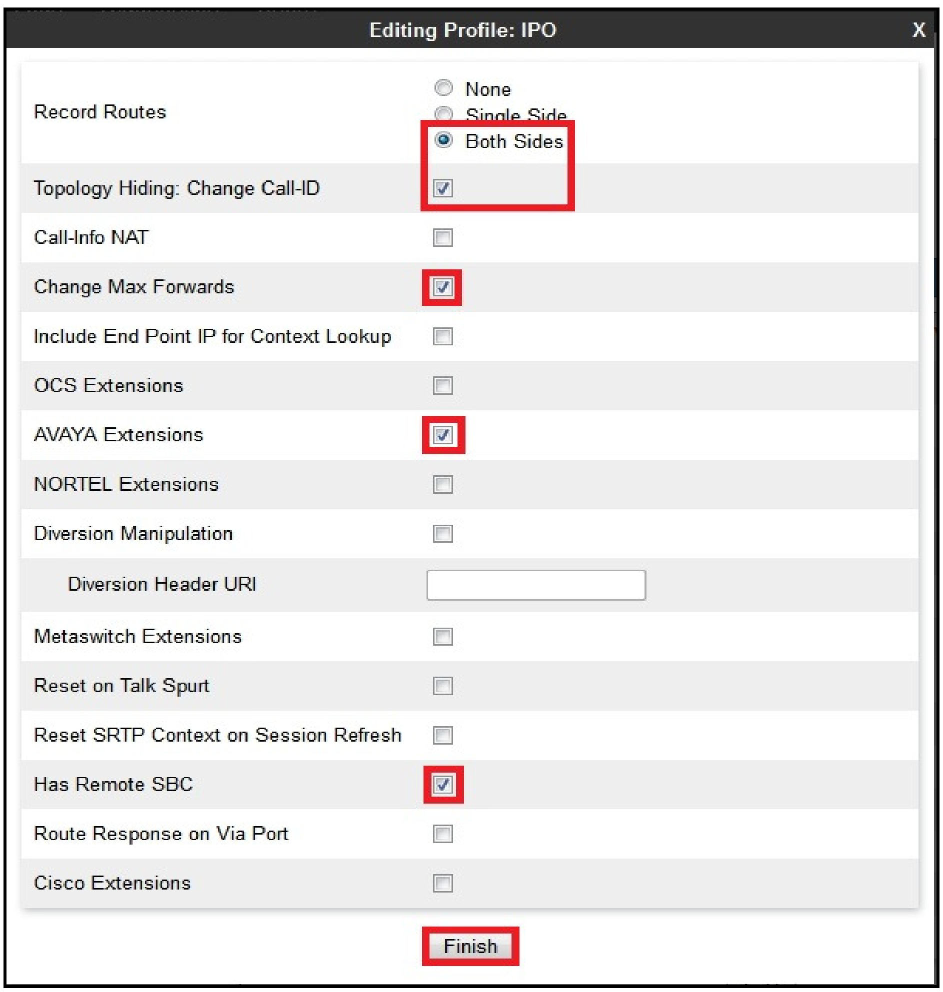

Editing Profile: MTSAllstream
X
Record Routes
None
Single Side
Both Sides
Topology Hiding: Change Call-ID
Call-Info NAT
Change Max Forwards
Include End Point IP for Context Lookup
OCS Extensions
AVAYA Extensions
NORTEL Extensions
Diversion Manipulation
Diversion Header URI
Metaswitch Extensions
Reset on Talk Spurt
Reset SRTP Context on Session Refresh
Has Remote SBC
Route Response on Via Port
Cisco Extensions
Finish

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.




Editing Profile: IPO
X
Privacy
Privacy Enabled
User Name
P-Asserted-Identity
P-Preferred-Identity
Privacy Header
DTMF
DTMF Support
None
SIP NOTIFY
SIP INFO
Back
Finish


Editing Profile: IPO
X
Record Routes
None
Single Side
Both Sides
Topology Hiding: Change Call-ID
Call-Info NAT
Change Max Forwards
Include End Point IP for Context Lookup
OCS Extensions
AVAYA Extensions
NORTEL Extensions
Diversion Manipulation
Diversion Header URI
Metaswitch Extensions
Reset on Talk Spurt
Reset SRTP Context on Session Refresh
Has Remote SBC
Route Response on Via Port
Cisco Extensions
Finish

6.2.5 Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulations done by the Avaya SBCE. Using this language, a script can be written and tied to a given Server Configuration (see **Section 6.2.6**) through the Avaya SBCE Web interface. The Avaya SBCE appliance then interprets this script at the given entry point or "hook point".

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in Topology Hiding.

To create a Signaling Manipulation script, select **Global Profiles → Signaling Manipulation** then click on the **Add Script** button (not shown).

In the compliance testing, SigMa script **MTSAllstream** was created for the Server Configuration for MTS Allstream as shown in **Section 6.2.6.1** and described in detail as follows:

```
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
        {
             if (exists(%HEADERS["Diversion"][1])) then
                {
                %HEADERS["P-Asserted-Identity"][1]=%HEADERS["From"][1];
                %HEADERS["P-Asserted-Identity"][1].regex_replace(";tag.*","");
                }
        }
}
```

The statement **`act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"`** is to specify the script will take effect on all type of SIP messages for outgoing calls to MTS Allstream and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

A set of rules as shown in the screenshot below were added in an "if" statement to check for the existence of the "Diversion" header which is a condition to match off-net call forward or Mobility Twinning call scenarios. For these call scenarios, as described in **Section 2.2**, observation #**6**, Calling Party Name and Calling Party Number of the original calling PSTN party was corrected by replacing the "P-Asserted-Identity" header with the display information from the "From" header.

```
if (exists(%HEADERS["Diversion"][1])) then
{
  %HEADERS["P-Asserted-Identity"][1]=%HEADERS["From"][1];
  %HEADERS["P-Asserted-Identity"][1].regex_replace(";tag.*","");
}
```

Note: The SigMa script for the Server Configuration for IP Office is not necessary as all signaling manipulations have been done on the Server Configuration for MTS Allstream. The modification will apply to both inbound and outbound SIP traffic toward MST Allstream.

6.2.6 Server Configuration

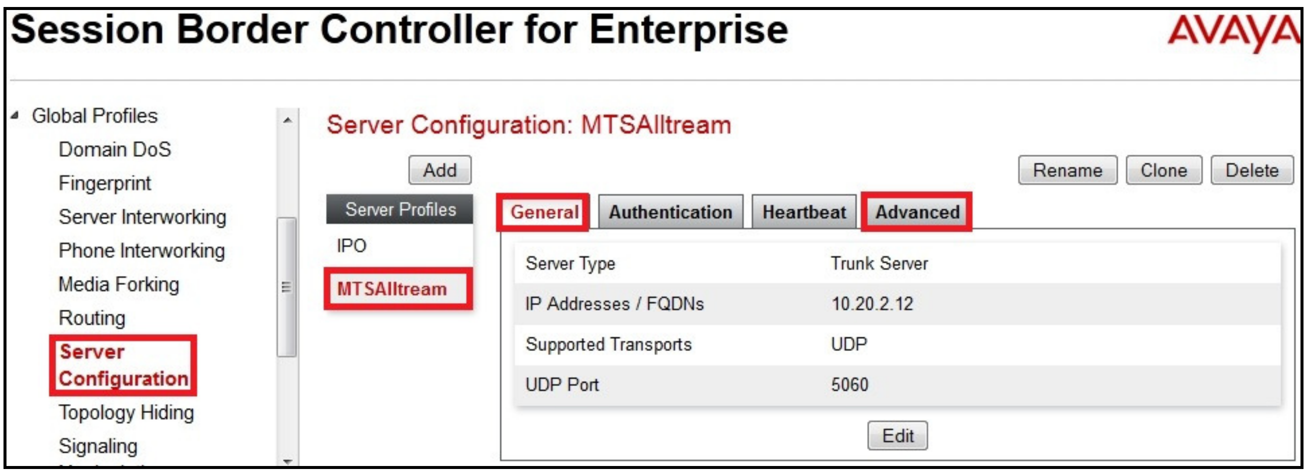
The Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and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

To create a Server Configuration entry, select **Global Profiles →Server Configuration** then click on the **Add Profile** button (not shown).

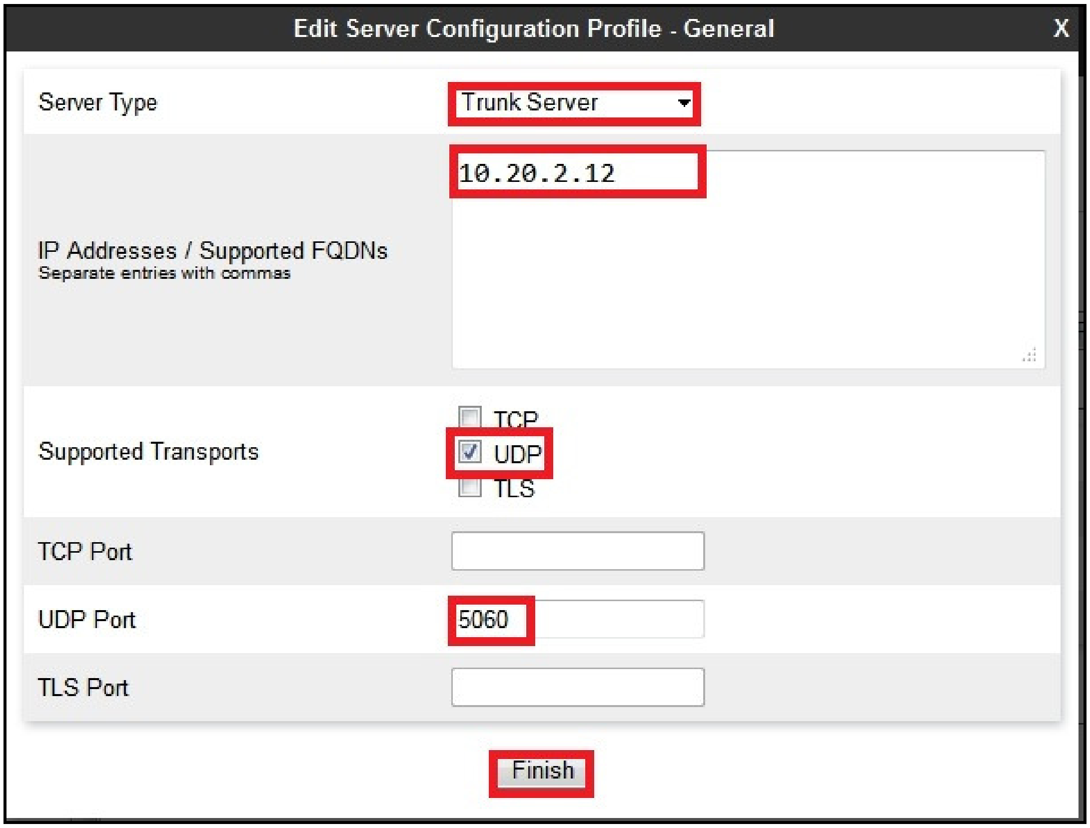
In the compliance testing, two separate Server Configurations were created, server entry **MTSAllstream** for MTS Allstream and server entry **IPO** for IP Office.

6.2.6.1 Server Configuration for MTS Allstream

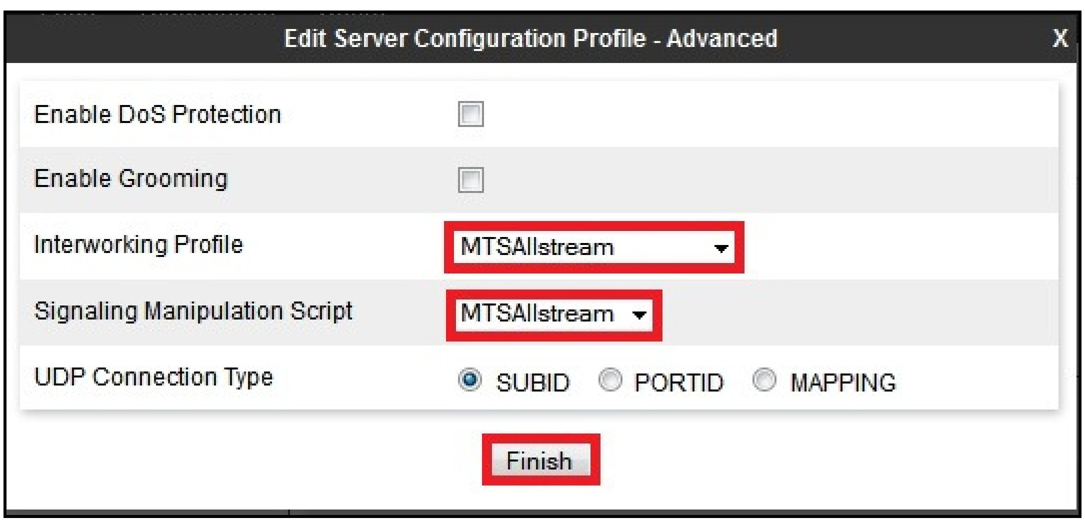
The Server Configuration **MTSAllstream** was added for MTS Allstream, it is discussed in detail below. The **General** and **Advanced** tabs were provisioned. The **Heartbeat** tab, however, was disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat originated from IP Office to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



In the **General** tab, specify Server Type for MTS Allstream as a **Trunk Server**. The IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, MTS Allstream supported transport protocol **UDP** on IP address **10.20.2.12** and listened on port **5060**.

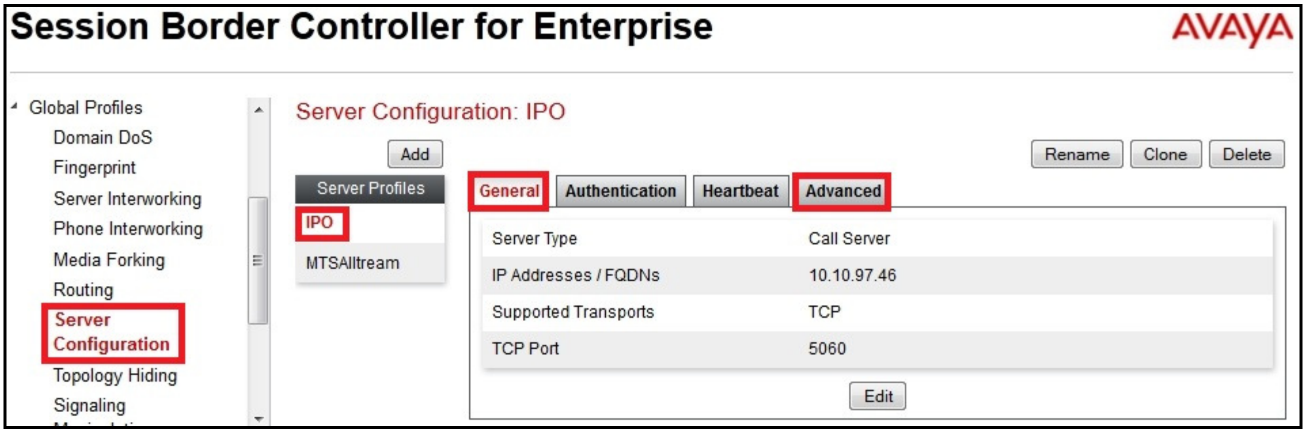


Under **Advanced** tab, for Interworking Profile drop down list, select **MTSAllstream** as defined in **Section 6.2.4.1** and for Signaling Manipulation Script drop down list, select **MTSAllstream** as defined in **Section 6.2.5**. These configurations are applied to the specific SIP profile and SigMa rules for the traffic from and to MTS Allstream. The other settings were kept as default.

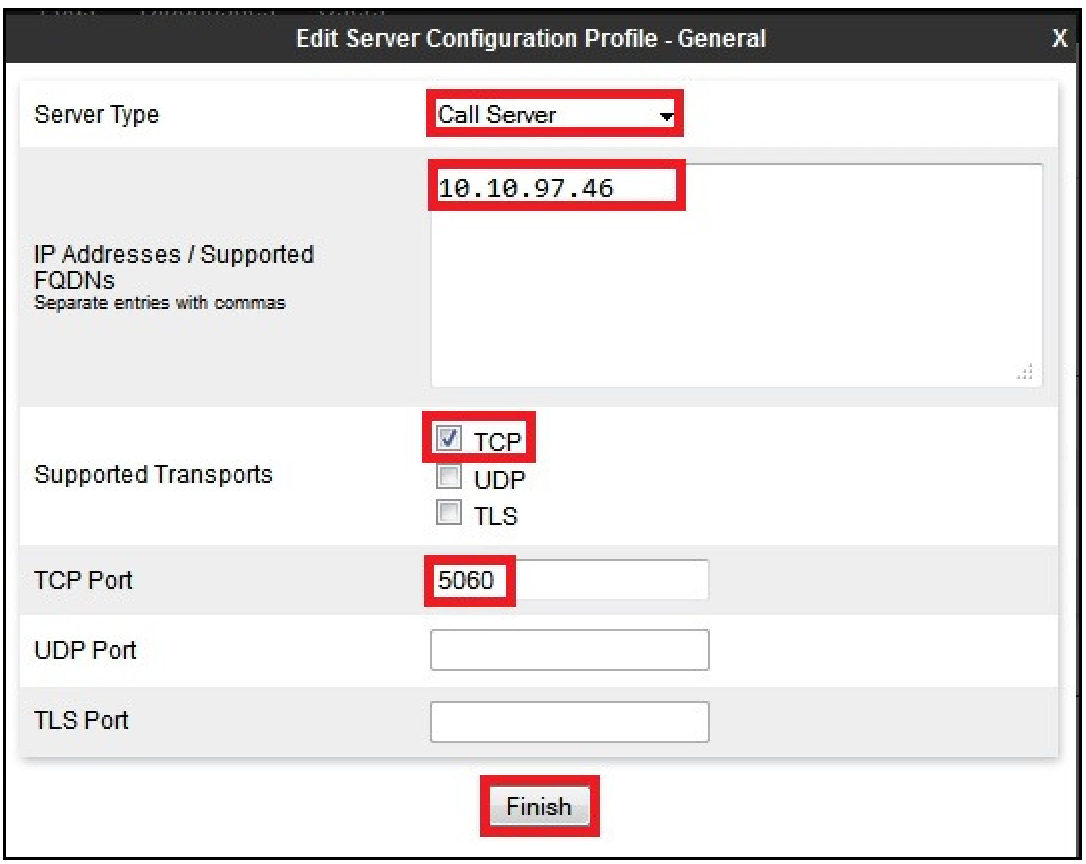


6.2.6.2 Server Configuration for Avaya IP Office

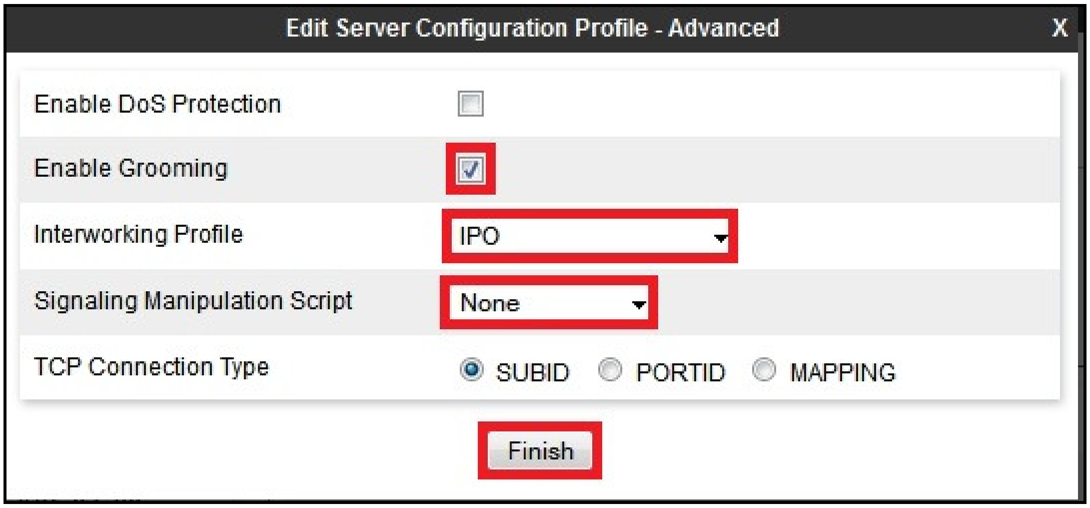
The Server Configuration **IPO** was similarly created for IP Office, and is discussed in detail below. Only the **General** and **Advanced** tabs required provisioning. The **Heartbeat** tab was kept disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from MTS Allstream to IP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



In the **General** tab, specify Server Type as **Call Server**. The 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**.



Under **Advanced** tab, for Interworking Profile drop down list, select **IPO** as defined in **Section 6.2.4.2** and for Signaling Manipulation Script drop down list select **None**. The 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 the 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 the 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**.

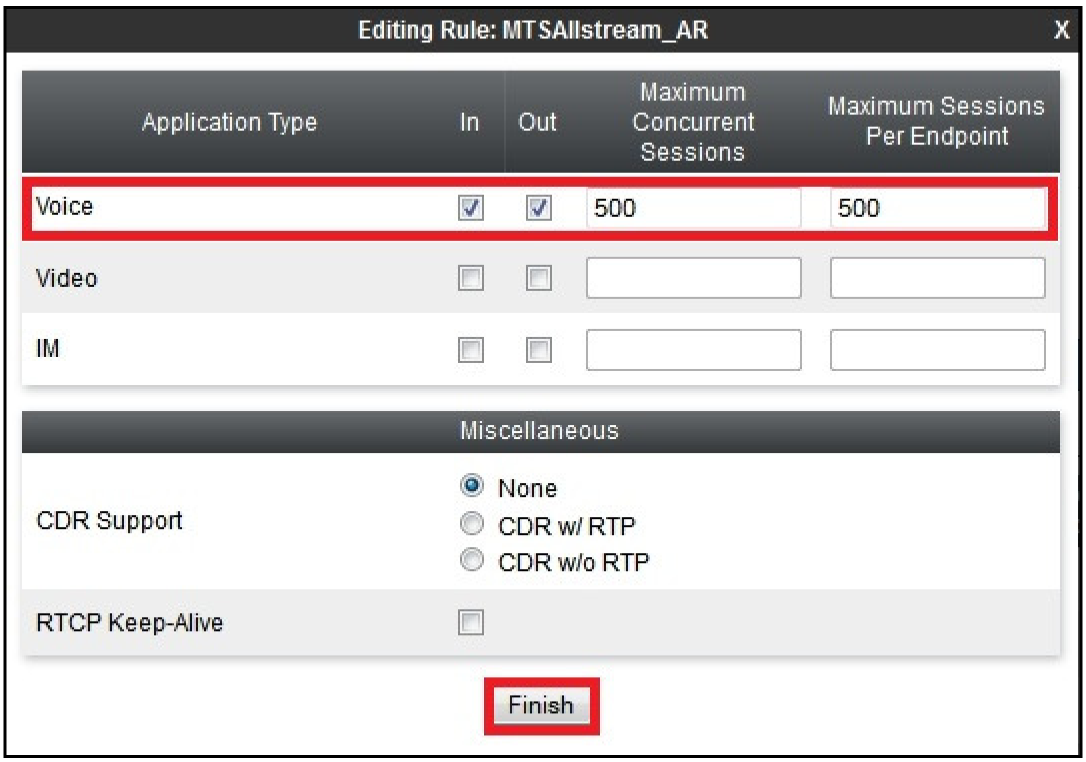
In the compliance testing, two **Application Rules** were created for MTS Allstream and IP Office.

6.3.1.1 Application Rule for MTS Allstream

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

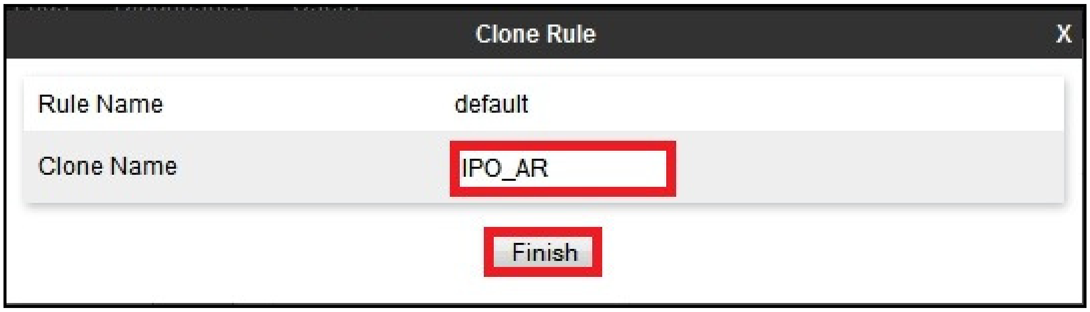
Enter a descriptive name e.g. **MTSAllstream_AR** for the new rule then click on the **Finish** button.

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

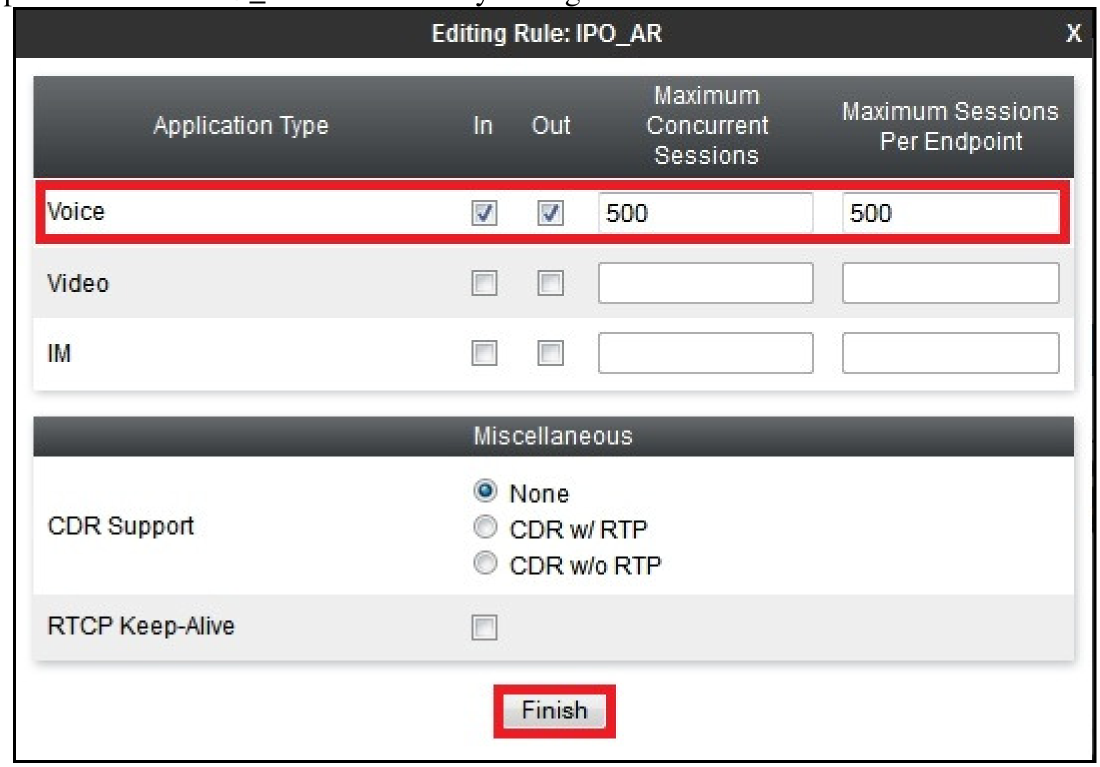


6.3.1.2 Application Rule for IP Office

Clone a Application Rule with a descriptive name e.g. **IPO_AR** for IP Office and click on the **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 the Avaya SBCE security product.

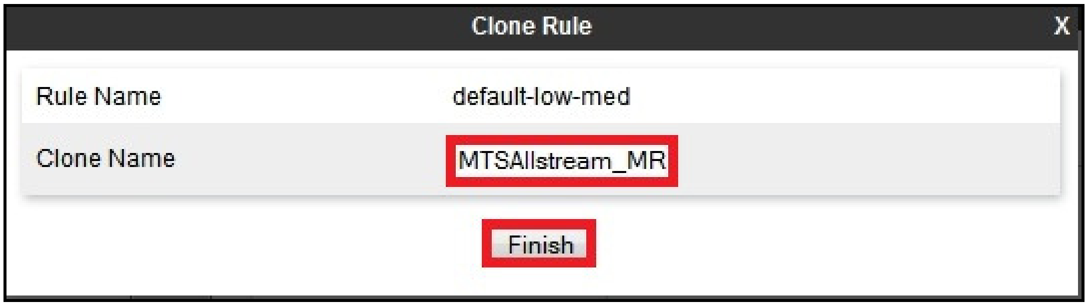
A custom Media Rule was created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration showed Media Rule **MTSAllstream_MR** which was used for both the enterprise and MTS Allstream networks.

In the compliance testing, two **Media Rules** were created for MTS Allstream and IP Office.

6.3.2.1 Media Rule for MTS Allstream

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

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



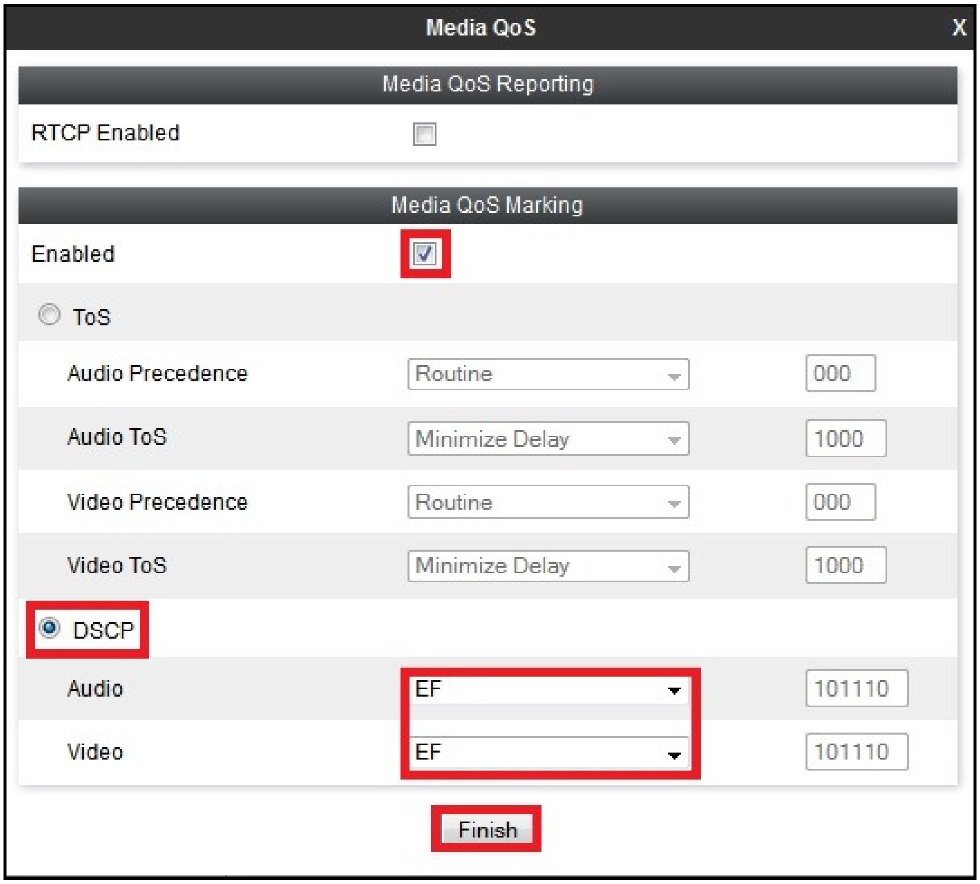
When the RTP changes while the call is in progress, the Avaya SBCE interprets this as an anomaly and an alert will be created in the **Incidents Log**. Disabling **Media Anomaly Detection** could prevent the **RTP Injection Attack** alerts from being created in the log when the audio attributes change.

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

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

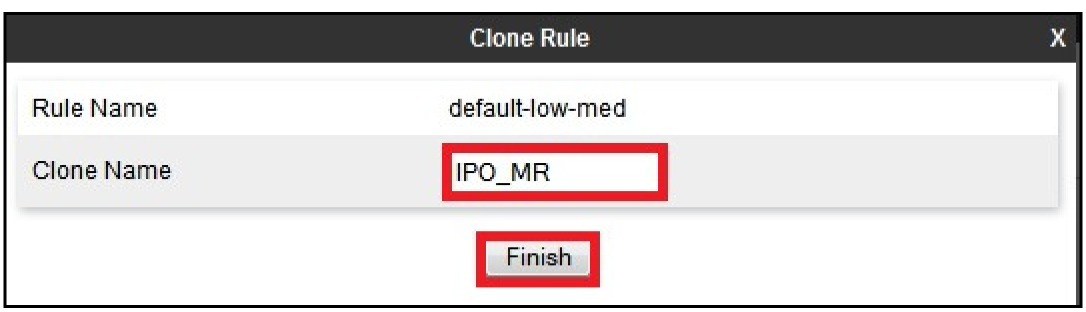
To modify Media Silencing, select the **Media Silencing** tab and click on the **Edit** button (not shown). Then uncheck **Media Silencing** and click on the **Finish** button.

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



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

6.3.3 Signaling Rules

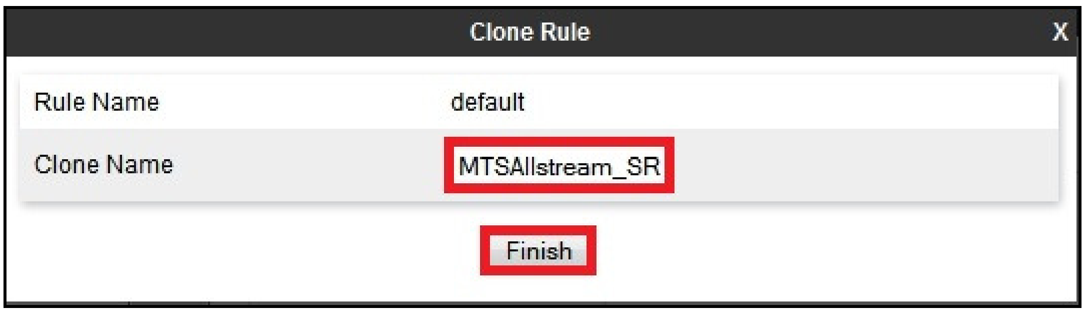
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling criteria defined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

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

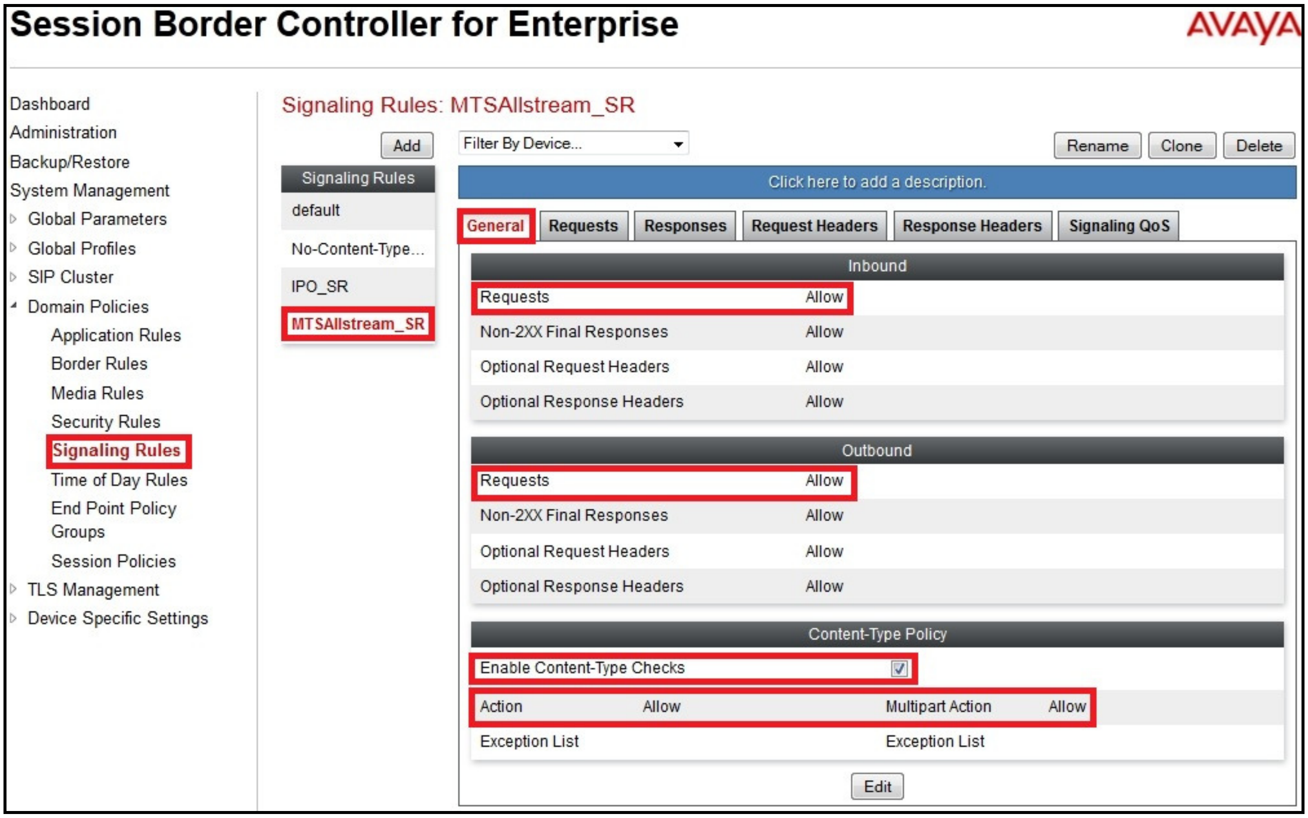
In the compliance testing, two **Signaling Rules** were created for MTS Allstream and IP Office.

6.3.3.1 Signaling Rule for MTS Allstream

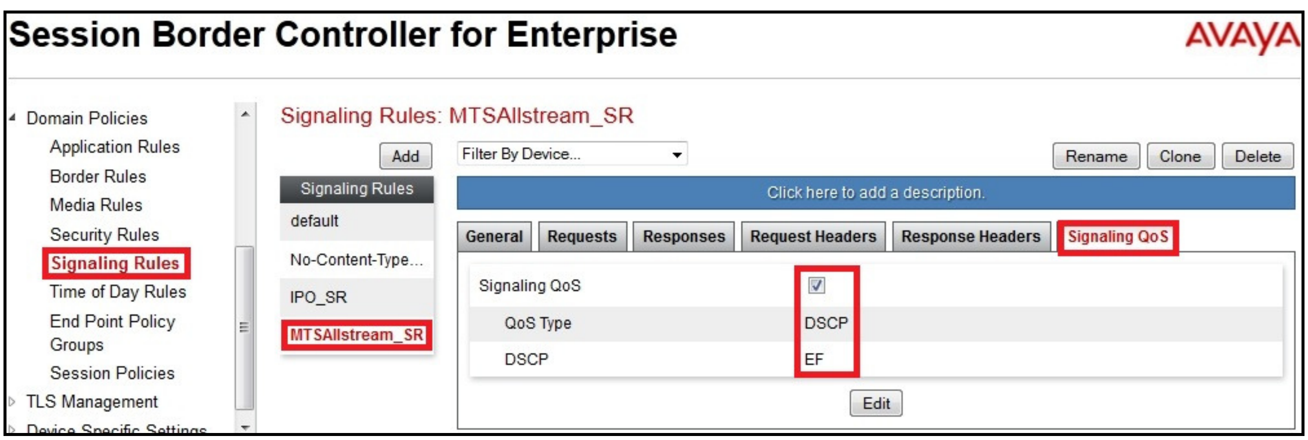
Clone a Signaling Rule with a descriptive name e.g. **MTSAllstream_SR** and click on the **Finish** button.



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

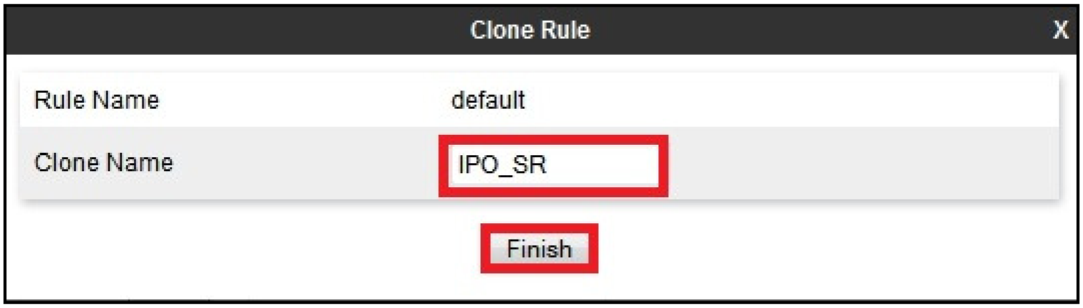


On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value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

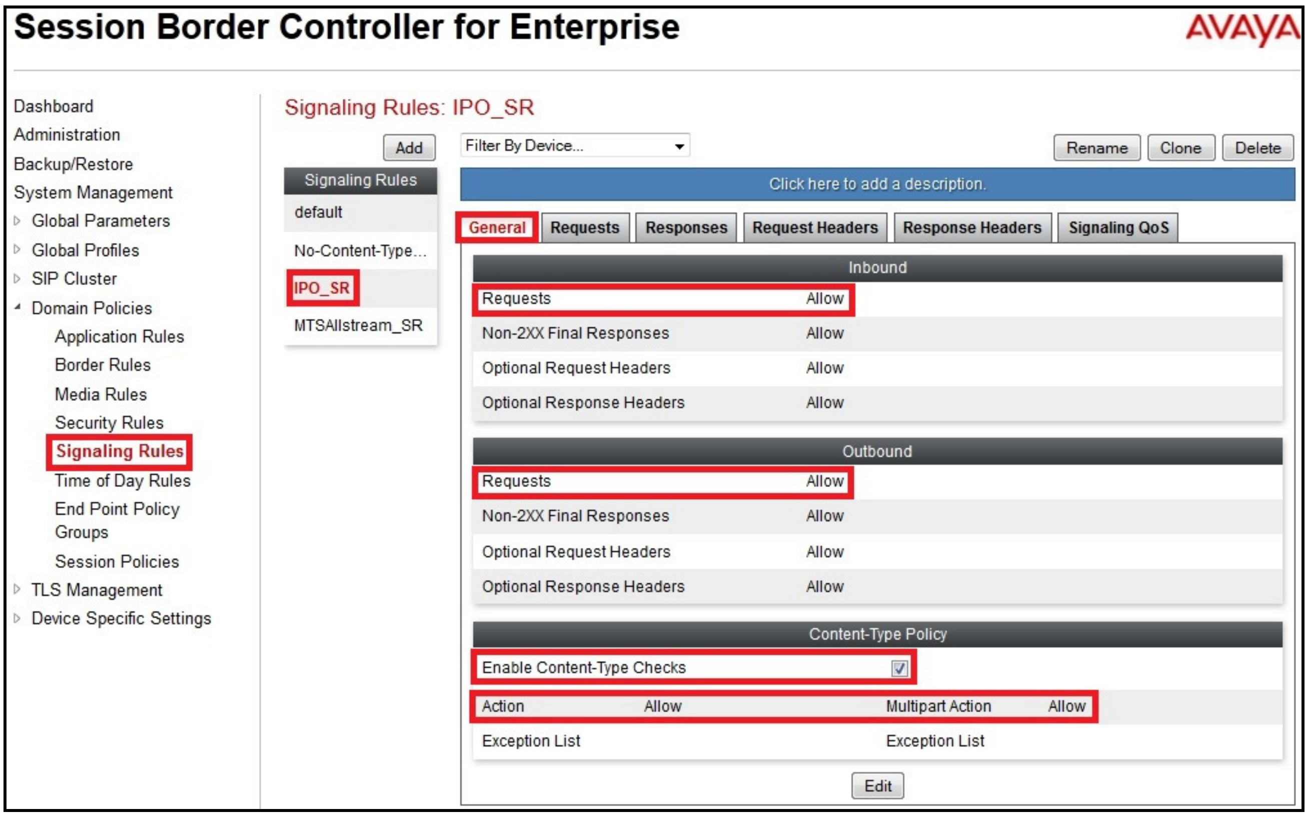


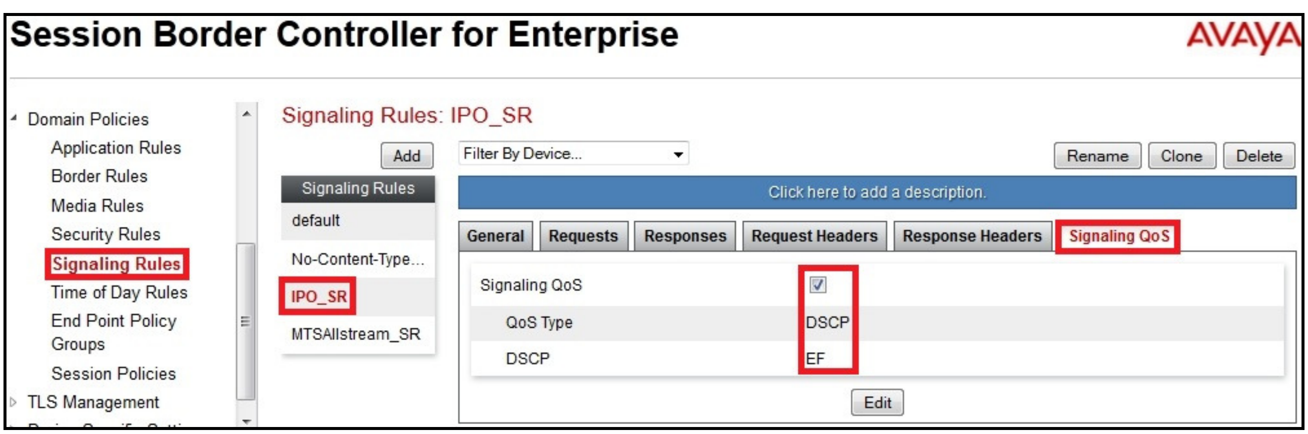
6.3.3.2 Signaling Rule for IP Office

Clone a Signaling Rule with a descriptive name e.g. **IPO_SR** for IP Office and click on the **Finish** button.



The Signaling Rule **IPO_SR** was similarly configured as shown in the screenshots below.





6.3.4 Endpoint Policy Groups

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

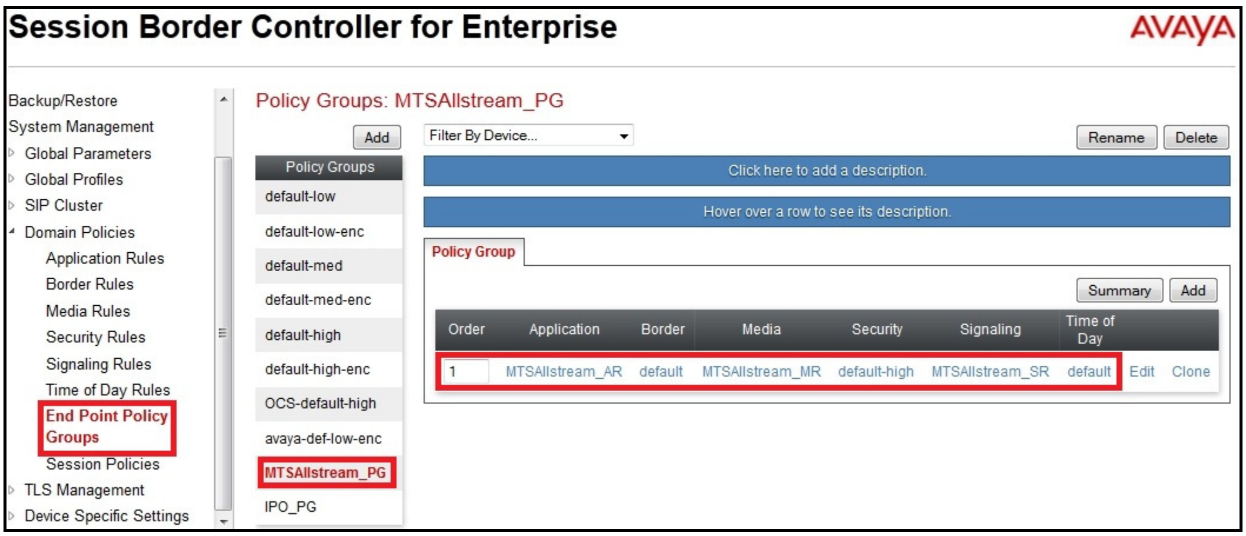
Endpoint Policy Groups were separately created for MTS Allstream and IP Office.

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

6.3.4.1 Endpoint Policy Group for MTS Allstream

The following screen shows **MTSAllstream_PG** created for MTS Allstream.

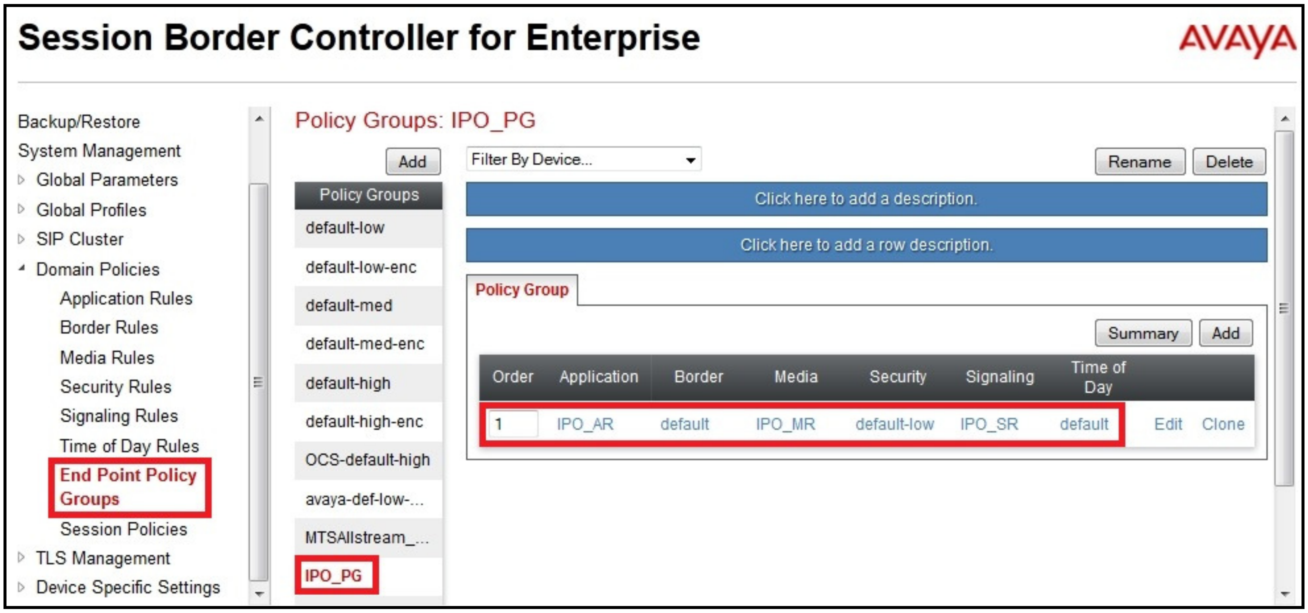
- Set Application Rule to **MTSAllstream_AR** which was created in **Section 6.3.1.1**.
- Set Media Rule to **MTSAllstream_MR** which was created in and **Section 6.3.2**.
- Set Signaling Rule to **MTSAllstream_SR** which was created in **Section 6.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.



6.3.4.2 Endpoint Policy Group for IP Office

The following screen shows 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**.



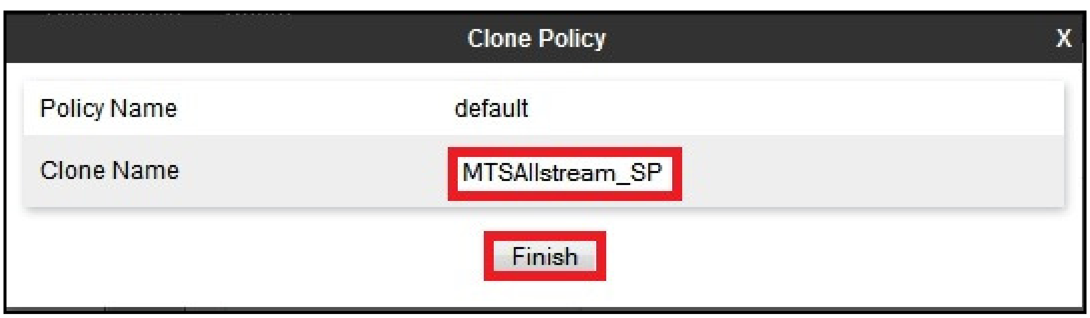
6.3.5 Session Policy

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, the Session Policy **MTSAllstream_SP** was created to match the codec configuration on MTS Allstream. The policy also allows the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.

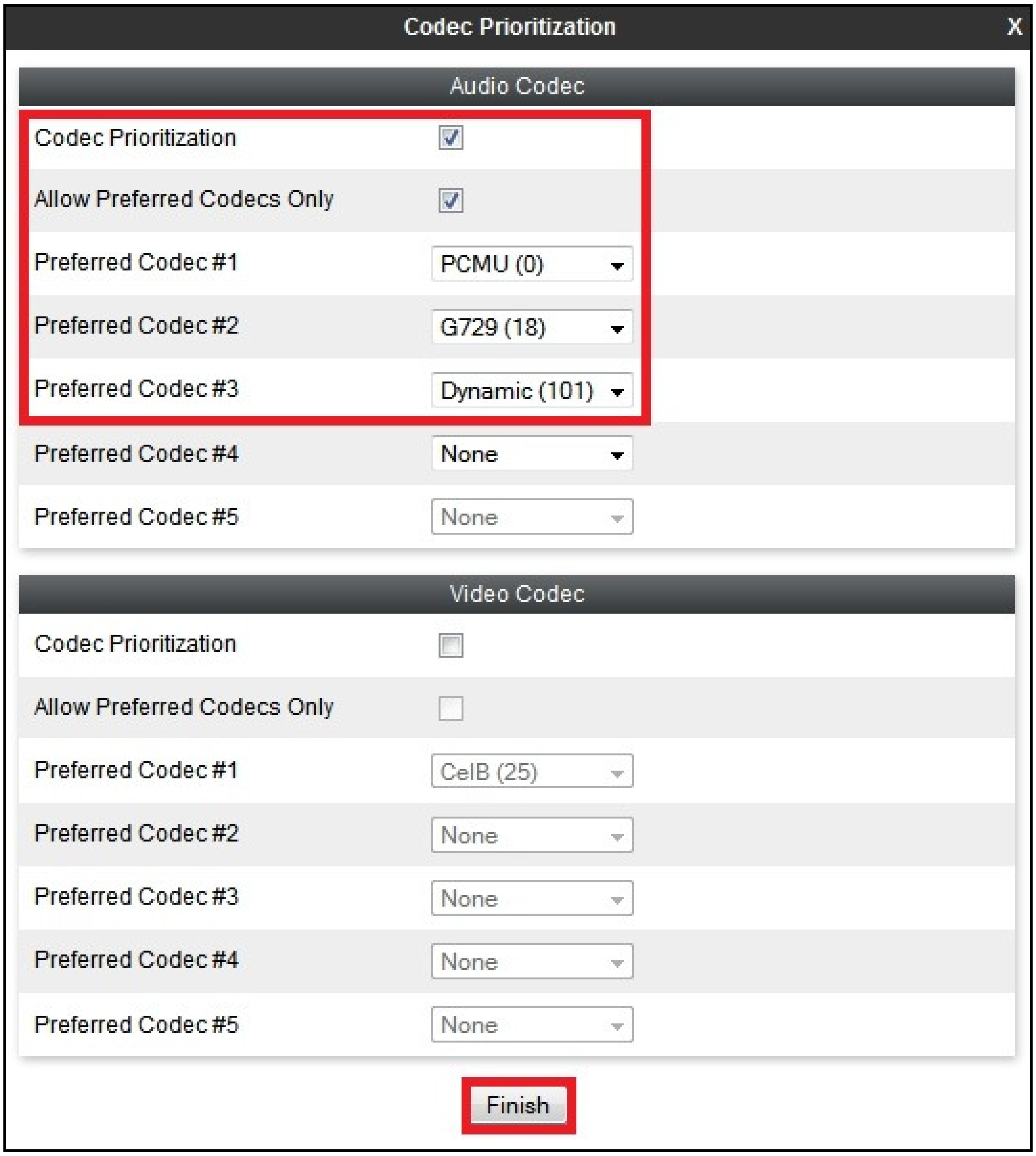
To clone a common Session Policy which applies to both MTS Allstream and IP Office, navigate to **Domain Policies → Session Policies**, select the **default** rule then click on the **Clone Rule** button (not shown).

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

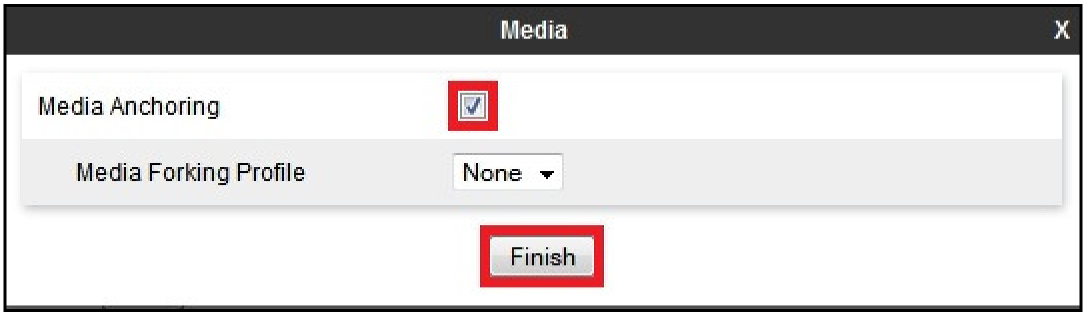


MTS Allstream supports G.729 and G.711MU voice codecs in prioritized order and payload **101** for RFC2833/ DTMF. To define **Codec Prioritization** for **Audio Codec**, select the profile **MTSAllstream_SP** created above, click on the **Edit** button (not shown). Select **Preferred Codec #1** as **PCMU (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 the Session Policy **MTSAllstream_SP** created above, click on the **Edit** button (not shown) then check on **Media Anchoring** to allow the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.



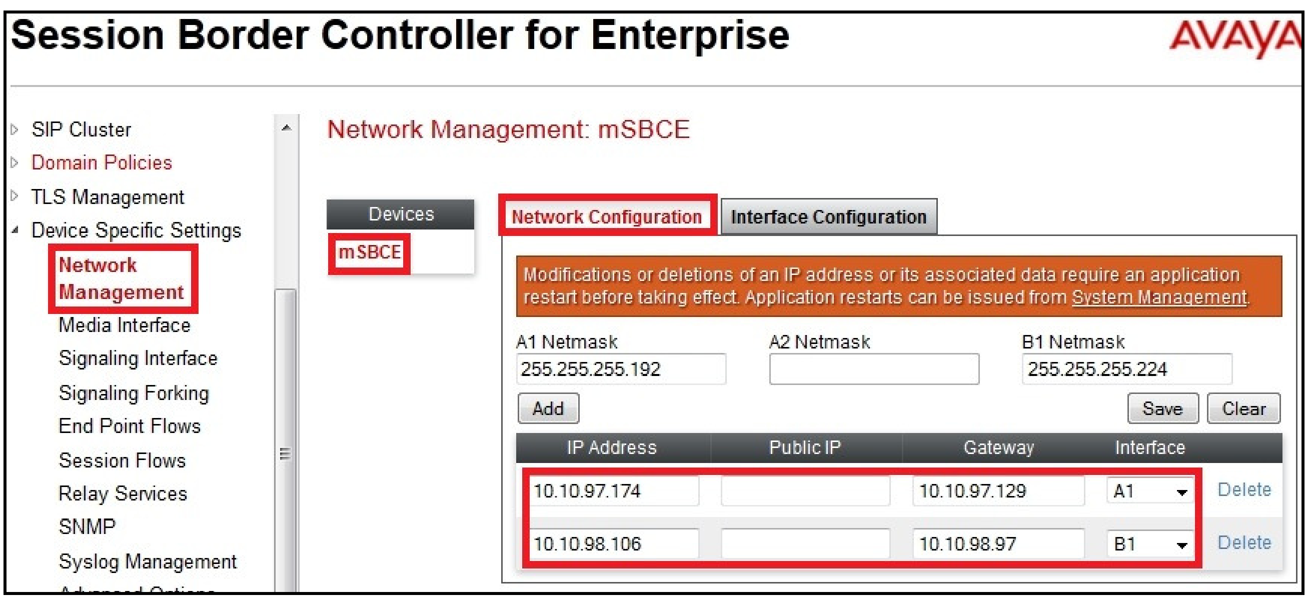
6.4 Device Specific Settings

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.

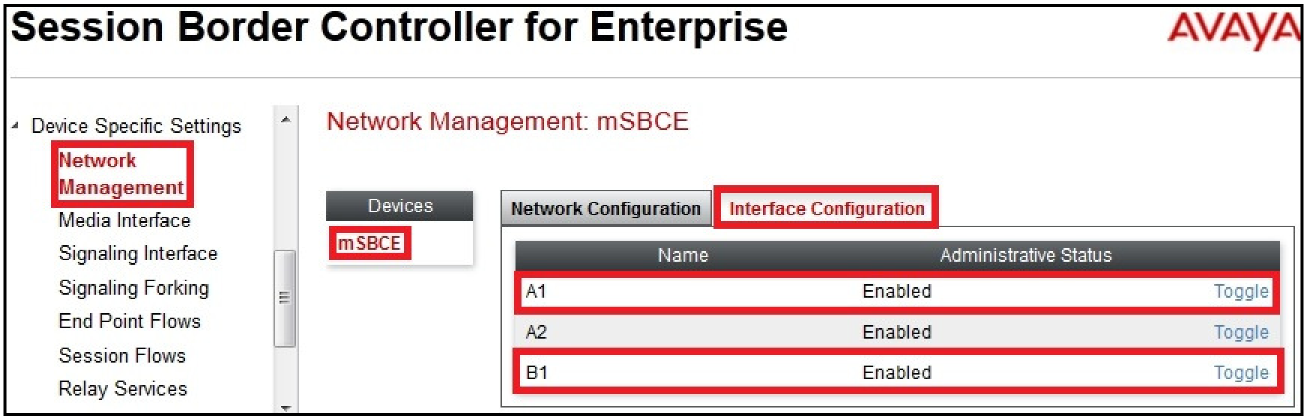
6.4.1 Network Management

Network Management page is where the network interface settings are configured and enabled. During the installation process of the 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 the IP addresses assigned to the interfaces and that the interfaces were enabled. The following screen shows the private interface was assigned to **A1** and the public interface was assigned to **B1** appropriate to the parameters shown in the **Figure 1**.



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



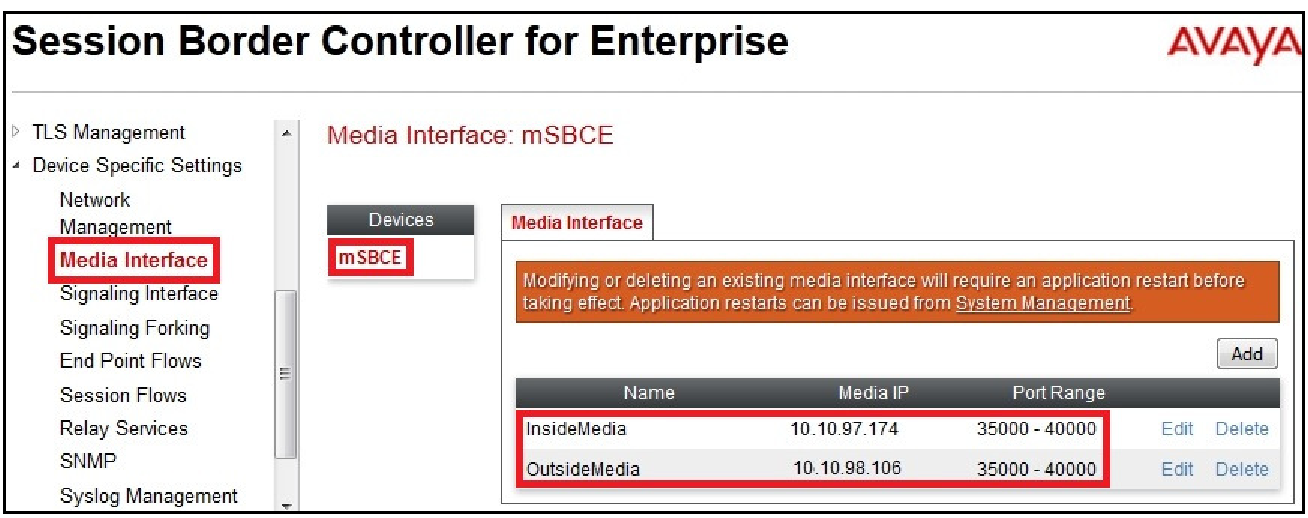
6.4.2 Media Interface

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

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

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

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

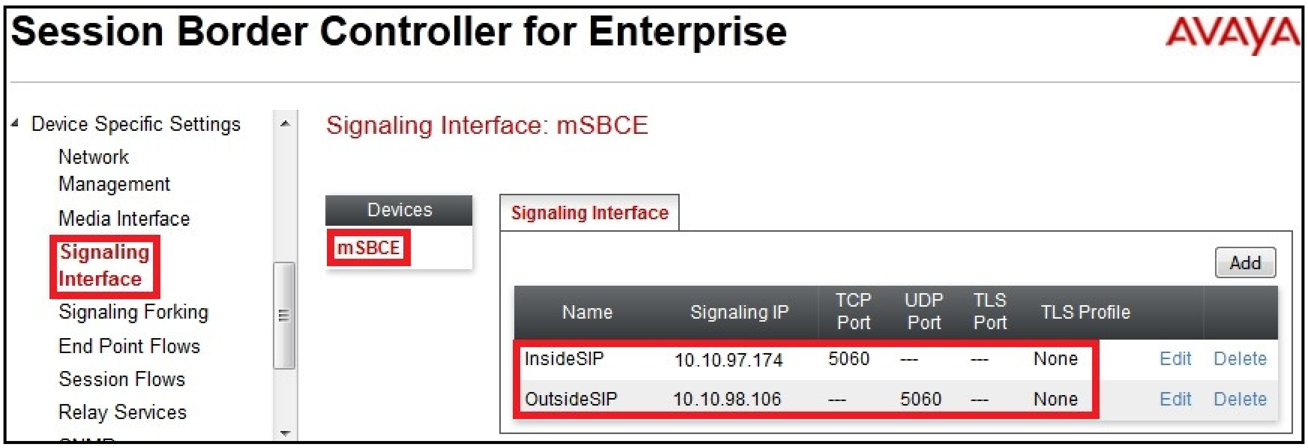


6.4.3 Signaling Interface

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

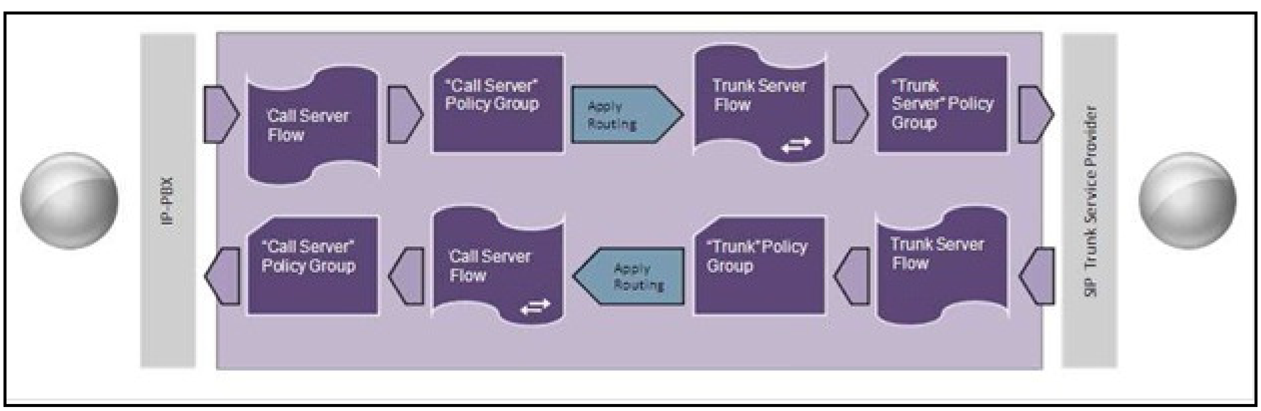
To create a new **Signaling Interface**, navigate to **Device Specific Settings → Signaling Interface** and click on the **Add Signaling Interface** button (not shown).

Two separate Signaling Interfaces are needed for both inside and outside interfaces. The following screen shows the 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 the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

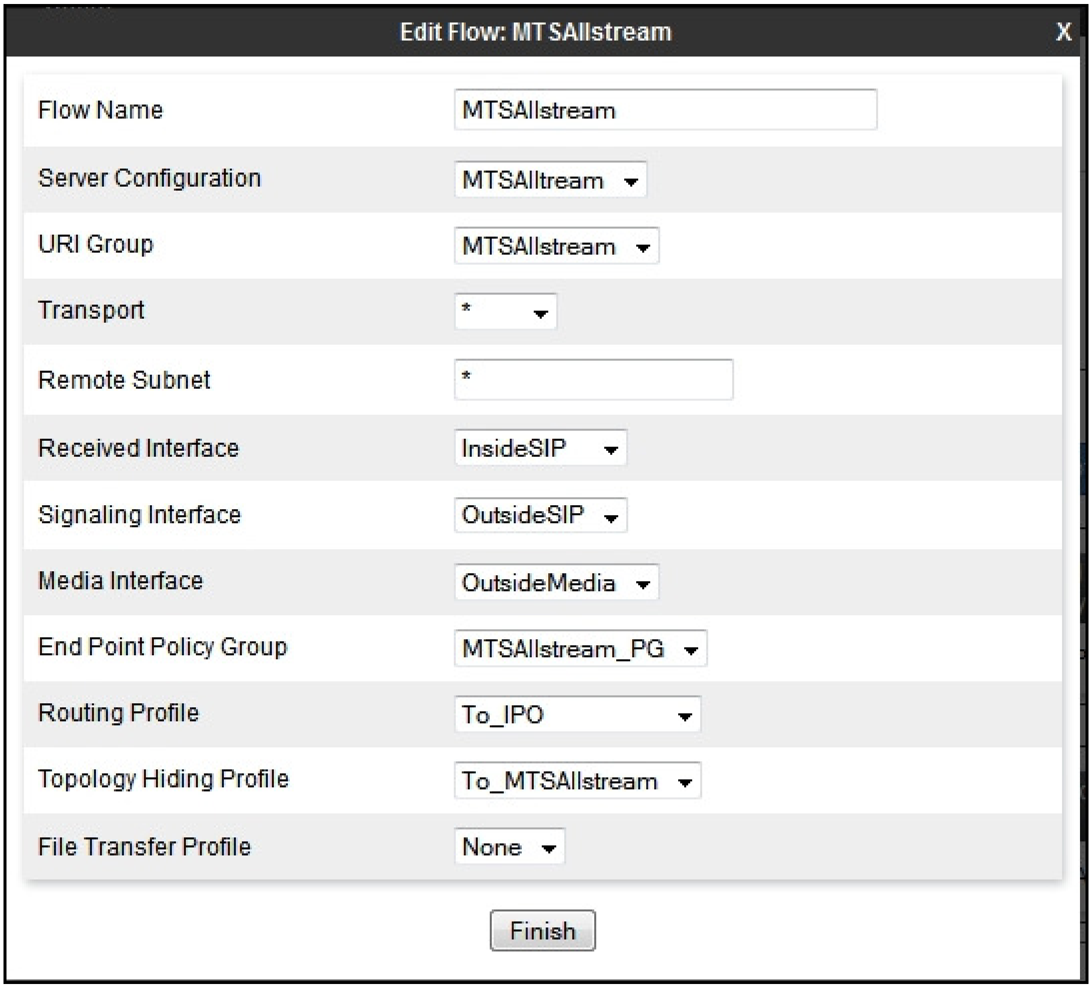


In the compliance testing, two separate Server Flows were created for MTS Allstream and IP Office.

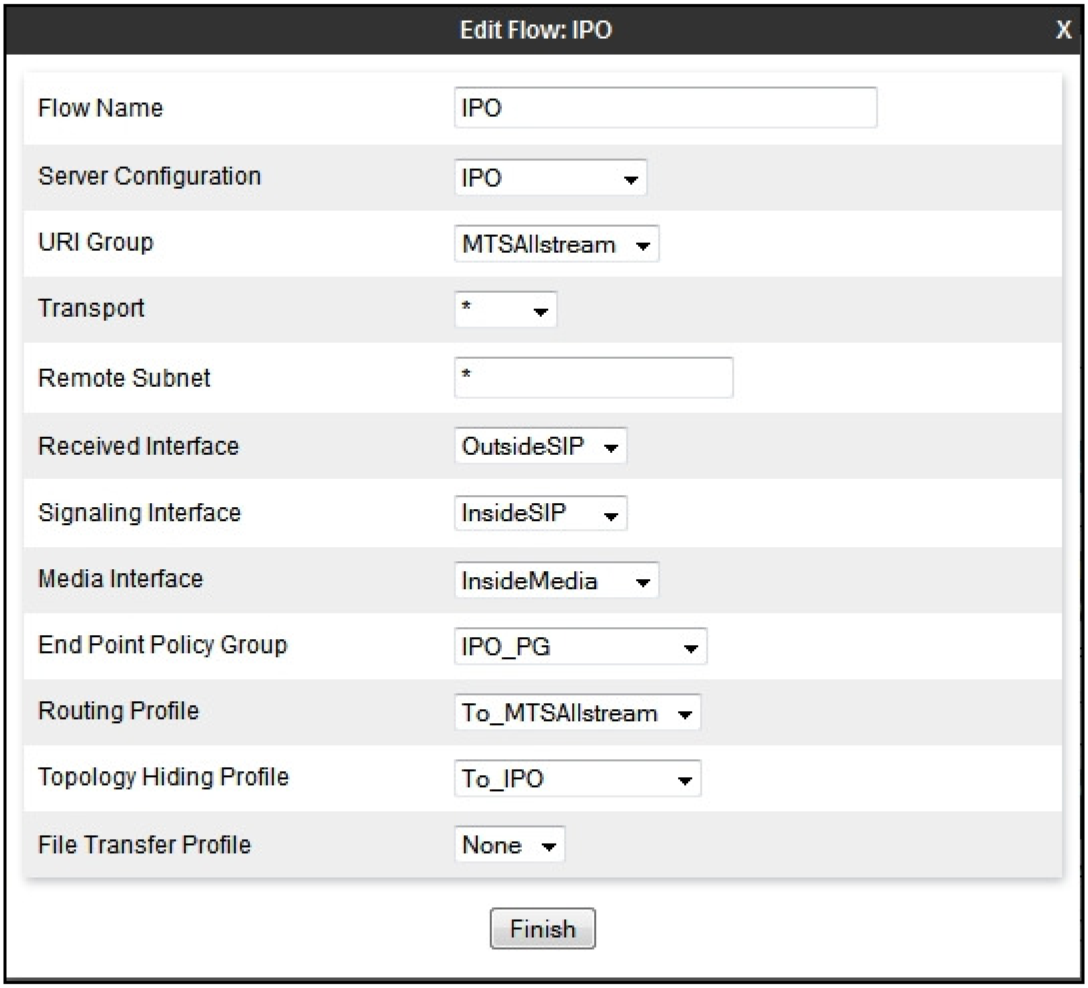
To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the other fields were kept as default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select a Server Configuration created in **Section 6.2.6** which the Server Flow associates to.
- **URI Group**: Select the URI Group **MTSAllstream** created in **Section 6.2.1**.
- **Received Interface**: Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration designed to receive the SIP signaling.
- **Signaling Interface**: Select the Signaling Interface created in **Section 6.4.3** which is the Server Configuration designed to send the SIP signaling.
- **Media Interface**: Select the Media Interface created in **Section 6.4.2** which is the Server Configuration designed to send the RTP.
- **End Point Policy Group**: Select the End Point Policy Group created in **Section 6.3.4**.
- **Routing Profile**: Select the Routing Profile created in **Section 6.2.2** which is used to which is the Server Configuration is designed to route the calls to.
- **Topology Hiding Profile**: Select the Topology Hiding profile created in **Section 6.2.3** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

The following screen shows the Server Flow **MTSAllstream** for MTS Allstream.



The following screen shows the Server Flow **IPO** for IP Office.



6.4.5 Session Flows

Session Flows feature allows defining certain parameters that pertain to the 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 **MTSAllstream_SF** was created for both the MTS Allstream and IP Office.

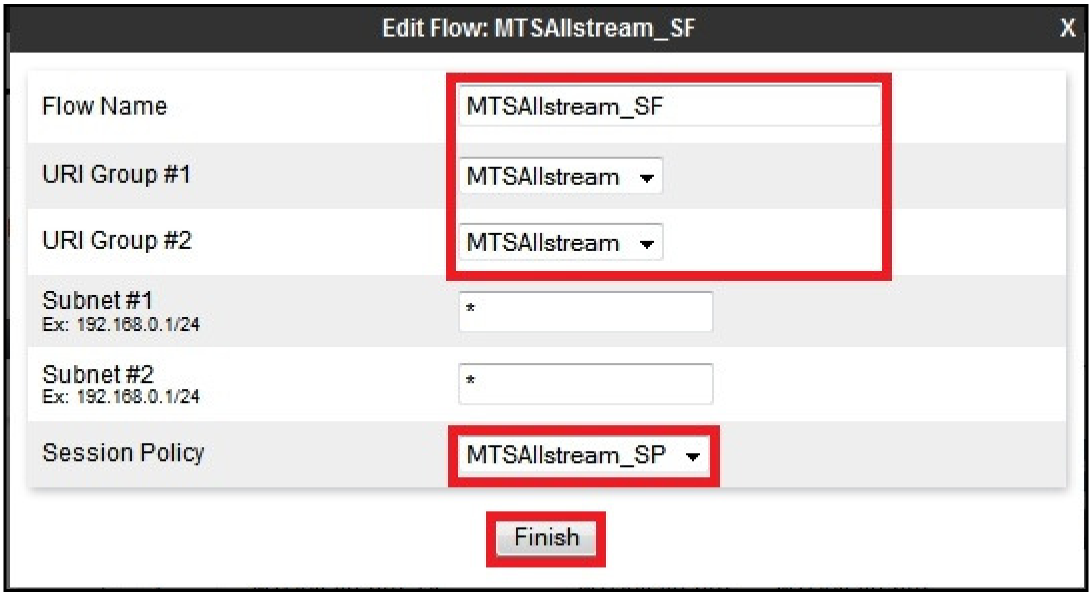
To create a Session Flow, navigate to **Device Specific Settings → Session Flows** then click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the remaining fields were kept as default.

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

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

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

The following screen shows the Session Flow named **MTSAllstream_SF**.



7. MTS Allstream SIP Trunking Service Configuration

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

- IP address of the MTS Allstream SIP proxy.
- DID numbers.
- Supported codecs.
- A customer specific SIP signaling reference.

The sample configuration between the enterprise and MTS Allstream for the compliance testing was a static configuration. There was no registration on the SIP Trunk implemented on either MTS Allstream or enterprise side.

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 to troubleshoot the solution.

8.1 Verification Steps

The following activities are made to each test scenario:

- Verify that endpoints at the enterprise site can place calls to PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

8.2 Protocol Traces

The following SIP message headers are inspected using sniffer trace analysis tool:

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

The following attributes in SIP message body are inspected using sniffer trace analysis tool:

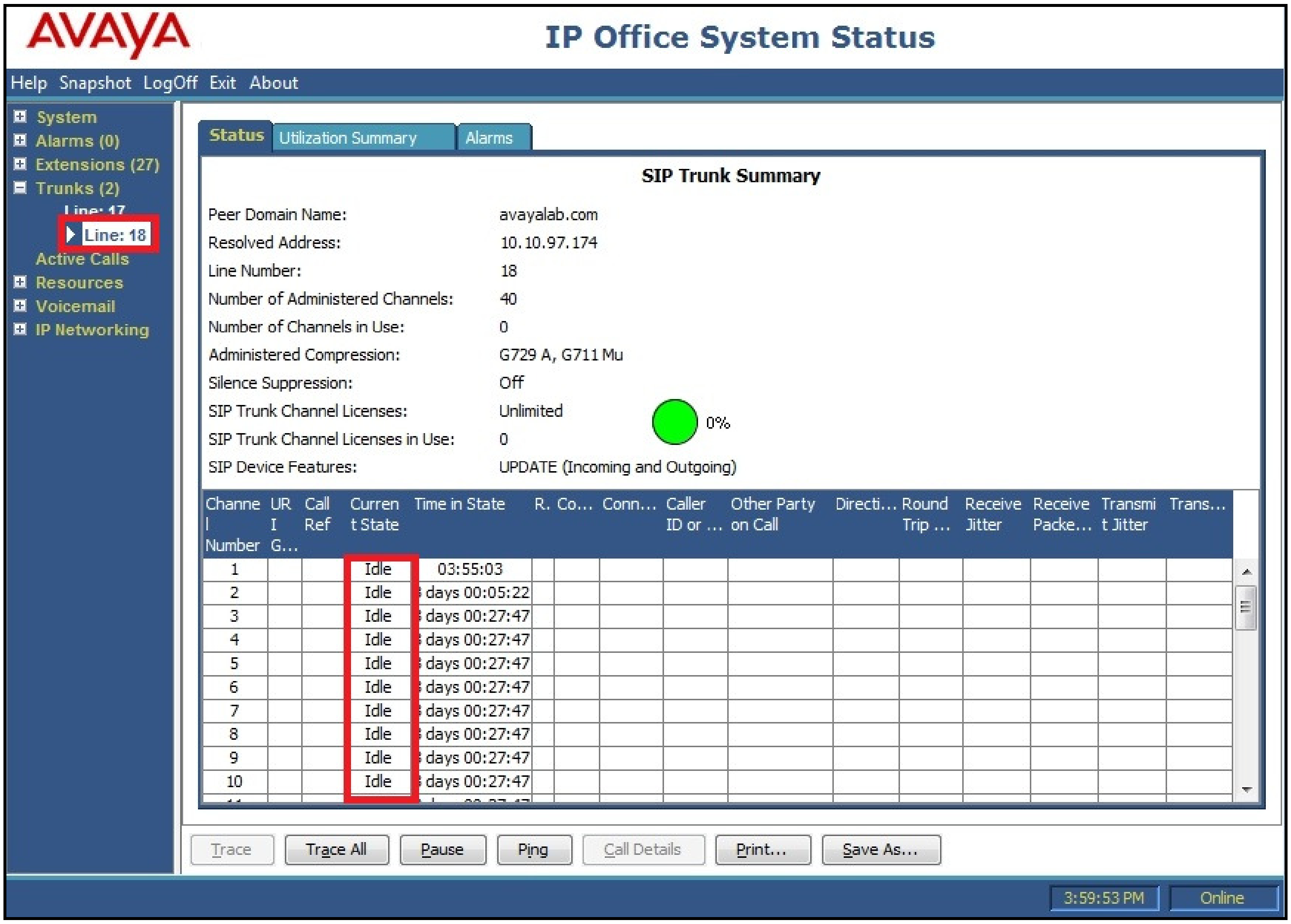
- Connection Information (c line): Verify IP addresses of near end and far end endpoints.
- Time Description (t line): Verify session timeout value of near end and far end endpoints.
- Media Description (m line): Verify audio port, codec, DTMF event description.
- Media Attribute (a line): Verify specific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

8.3 Troubleshooting

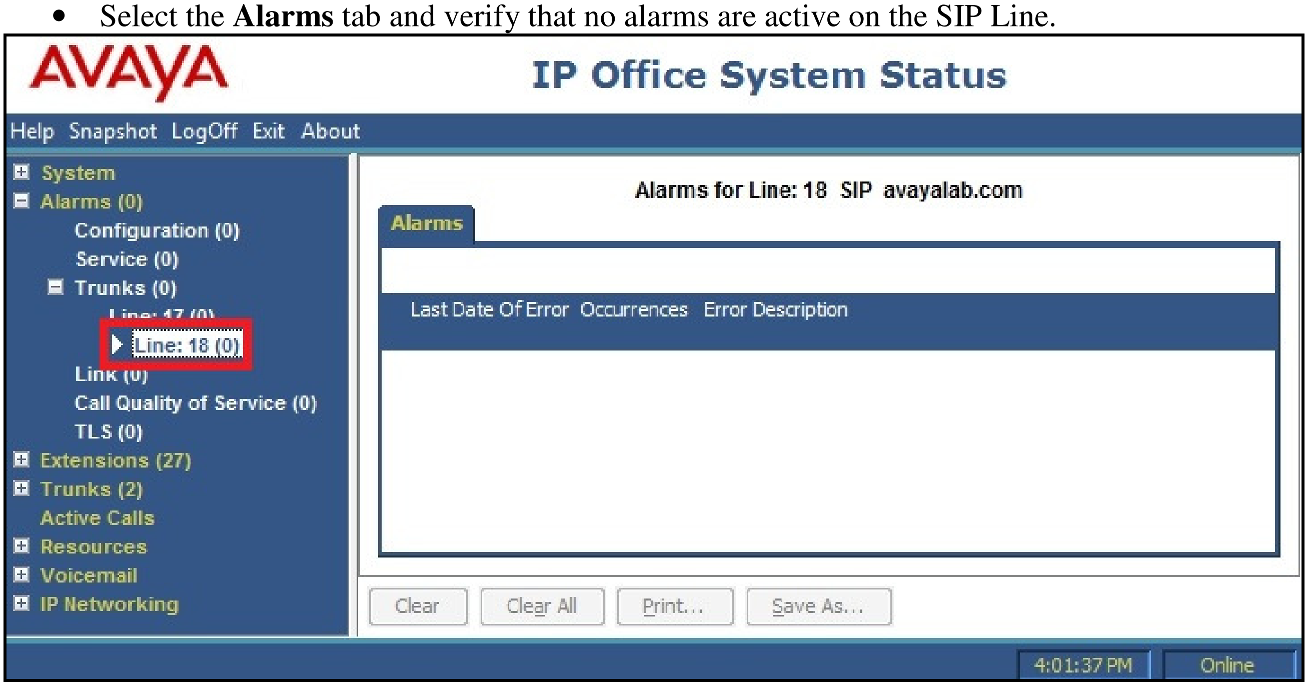
8.3.1 IP Office System Status

The following steps may be used to verify the configuration.

- Use the 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 the **Status** tab in the right pane, verify that the **Current State** is ***Idle*** for each channel (assuming no active calls at present time).



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



8.3.2 Sniffer Traces Analysis

Using a network sniffing tool e.g. Wireshark to monitor the SIP signaling between the enterprise and MTS Allstream. The sniffer traces are captured at the public interface of the Avaya SBCE.

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

- Incoming INVITE request from MTS Allstream.

```
INVITE sip:647XXX3572@10.10.98.106;user=phone SIP/2.0
Max-Forwards: 69
Session-Expires: 3600;refresher=uac
Min-SE: 600
Supported: timer, 100rel
To: <sip:647XXX3572@10.10.98.106;user=phone>
From: <sip:1613XXX5279@10.20.2.12;user=phone>;tag=3573576568-10778
P-Asserted-Identity: <sip:1613XXX5279@10.20.2.12;user=phone>
Call-ID: 78556-3573576568-10770@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 10.20.2.12:5060;branch=z9hG4bKe625439785663db37aaea40f10797b97
Contact: <sip:1613XXX5279@10.20.2.12:5060;tgrp=TOROONSBCIOT1>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 271

v=0
o=nextone-msw-lab-3 581599781 581599781 IN IP4 10.20.2.12
s=sip call
c=IN IP4 10.20.2.13
t=0 0
m=audio 18604 RTP/AVP 18 0 8 101
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

- 200OK response from the enterprise.

```
SIP/2.0 200 OK
From: <sip:1613XXX5279@10.20.2.12;user=phone>;tag=3573576568-10778
To: <sip:647XXX3572@10.10.98.106;user=phone>;tag=b74a4de9120bbf8a
CSeq: 1 INVITE
Call-ID: 78556-3573576568-10770@nextone-msw-lab-3.mtsallstream.com
Contact: "MTS x3572" <sip:647XXX3572@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=29557;lr;transport=udp>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
Supported: timer,100rel
Via: SIP/2.0/UDP 10.20.2.12:5060;branch=z9hG4bKe625439785663db37aaea40f10797b97
Require: timer
Server: IP Office 8.1 (65)
Session-Expires: 3600;refresher=uac
Min-SE: 3600
Content-Type: application/sdp
Content-Length: 224

v=0
o=UserA 440622765 2981016667 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 35612 RTP/AVP 18 101
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

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

- Outgoing INVITE request from the enterprise.

```
INVITE sip:111291613XXX5279@10.20.2.12 SIP/2.0
From: "MTS x3572" <sip:647XXX3572@10.10.98.106>;tag=a0ed22b7b5e1e6ce
To: <sip:111291613XXX5279@10.20.2.12>
CSeq: 1309331781 INVITE
Call-ID: ed115b6619c4dc5396e9b55191992430
Contact: "MTS x3572" <sip:647XXX3572@10.10.98.106:5060;transport=udp>
Record-Route: <sip:10.10.98.106:5060;ipcs-line=29561;lr;transport=udp>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
Supported: timer,100rel
User-Agent: IP Office 8.1 (65)
Max-Forwards: 69
Via: SIP/2.0/UDP 10.10.98.106:5060;branch=z9hG4bK-s1632-002092052492-1--s1632-
P-Asserted-Identity: "MTS x3572" <sip:647XXX3572@10.10.98.106>
Content-Type: application/sdp
Content-Length: 248

v=0
o=UserA 637963966 2199313965 IN IP4 10.10.98.106
s=Session
c=IN IP4 10.10.98.106
t=0 0
m=audio 35614 RTP/AVP 0 18 101
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

- Incoming 200OK response from MTS Allstream.

```
SIP/2.0 200 OK
Session-Expires: 3600;refresher=uas
Require: timer
Via: SIP/2.0/UDP 10.10.98.106:5060;received=10.10.98.106;branch=z9hG4bK-s1632-
002092052492-1--s1632-
Record-Route: <sip:10.10.98.106:5060;ipcs-line=29561;lr;transport=udp>
To: <sip:111291613XXX5279@10.20.2.12>;tag=3573576734-450439
From: "MTS x3572" <sip:647XXX3572@10.10.98.106>;tag=a0ed22b7b5e1e6ce
Call-ID: ed115b6619c4dc5396e9b55191992430
CSeq: 1309331781 INVITE
Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:111291613XXX5279@10.20.2.12:5060>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 583264586 583264586 IN IP4 10.20.2.12
s=sip call
c=IN IP4 10.20.2.13
t=0 0
m=audio 18610 RTP/AVP 18 0 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

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 MTS Allstream 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 MTS Allstream SIP Trunking Service is considered **compliant** with Avaya IP Office Release 8.1.

10. References

[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.

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

Product documentation for MTS Allstream SIP Trunking Service is available from MTS Allstream.

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.