Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 10.1 to support Clearcom SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya IP Office 10.1 to support Clearcom SIP Trunking Service.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the public switched telephone network (PSTN) with various Avaya endpoints.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) Trunking service between Clearcom and an Avaya SIP-enabled enterprise solution.

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of Avaya IP Office 500 V2 Release 10.1 (hereafter referred to as IP Office) and various Avaya endpoints, listed in **Section 4**.

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

The terms “service provider” or “Clearcom” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Clearcom’s network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities listed in **Section 2.1**.

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

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability the following features and functionalities were exercised during the interoperability compliance test:

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP and H.323 telephones at the enterprise. All incoming calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider network.
- Outgoing PSTN calls from Avaya endpoints, including SIP and H.323 telephones at the enterprise. All outgoing calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider network.
- Incoming and outgoing PSTN calls to/from Avaya Communicator for Windows.
- Dialing plans including local calls (within Mexico), international, outbound toll-free, etc.
- Caller ID presentation.

- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with coverage to voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two way speech-path. Testing was performed with codecs: G.729A, G.711A and G.711U, Clearcom's preferred codec order.
- Proper response to no matching codecs.
- Fax.
- Proper early media transmissions.
- Voicemail and DTMF tone support using RFC 2833 (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- Mobility twinning of incoming calls to mobile phones.

Items not supported or not tested included the following:

- REFER message for call redirection is supported by Clearcom but was not tested for reasons noted under **Section 2.2**.
- T.38 and G.711 fax pass-through was not tested for reasons noted under **Section 2.2**.
- Inbound toll-free call was not tested.
- 0, 0+10 digits and 911 Emergency were not tested.

2.2. Test Results

Interoperability testing of Clearcom SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Call transfer to the PSTN using REFER**: PSTN calls that were transferred back to the PSTN network using REFER message did not work properly. Calls that were blind transferred dropped. On attended transfers, the REFER message was accepted by Clearcom with a 202 message, but the trunks were not released. Due to these reasons, REFER was left disabled in the Avaya IP Office for the tests. With REFER disabled, blind and attended call transfers to the PSTN were allowed to complete, with the caveat that the IP Office was not released from the call path, and two trunks circuits remained seized for the duration of the call.
- **Outbound Calling Party Number (CPN) Block**: Clearcom did not allow outbound calls with privacy enabled. When an IP Office user activated "Withhold Number" to enable user privacy on an outbound call, IP Office sent "anonymous" in the "From" header and the "Privacy:id" header, while the caller information was still being sent in the **"**P-Asserted-Identity" header. Clearcom responded with a "403 PSTN calls are forbidden" message and the call was rejected.
- **Caller ID on inbound calls**: On inbound calls made from the test lab in the U.S., the Caller ID shown on the enterprise extensions occasionally showed "Unavailable", while in other cases showed numbers corresponding to local PSTN numbers in Mexico, not the number of the original caller. Calls made from a local test number in Mexico showed the correct caller ID.
- **Outbound call from an enterprise extension to a busy PSTN number**: Clearcom did not send a "486 Busy Here" message on an outbound call to a PSTN number that was busy, as it was expected on this condition. There was no direct impact to the user, who heard busy tone.
- **Caller ID on outbound calls**: On calls originating from IP Office extensions to PSTN telephones, the caller ID number displayed on the PSTN endpoint was always the main DID number assigned by Clearcom to the SIP trunk, not the specific DID assigned to the extension originating the call. This includes calls to "twinned" mobile phones, and calls that were forwarded or transferred back on the SIP trunk to the PSTN, where the number displayed on the PSTN endpoint was the main DID number on the trunk, not the originator's caller's ID. This may be a requirement of the Clearcom service for all outbound calls, it is listed here simply as an observation.
- **Fax support**: Fax calls using the T.38 protocol failed during the test. G.711 fax was also tested, but it behaved unreliably. Fax should not be used in this solution.

2.3. Support

For support on Clearcom systems visit the corporate Web page at: http://www.clearcom.mx/

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates the test configuration used for the DevConnect compliance testing. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Clearcom SIP Trunking Service through the public Internet.

The Avaya components used to create the simulated enterprise customer site includes:

- Avaya IP Office 500 V2.
- Avaya IP Office Application Server running Avaya Voicemail Pro.
- Avaya 96x1 Series H.323 IP Deskphones.
- Avaya 1100 Series SIP IP Deskphones.
- Avaya Communicator for Windows softphone.

The enterprise site contains the Avaya IP Office 500 V2 with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codecs. The **LAN1** port of Avaya IP Office is connected to the enterprise LAN (private network) while the **LAN2** port is connected to the public network. Endpoints include Avaya 96x1 Series IP Deskphones (with H.323 firmware), Avaya 1100 IP Deskphones (with SIP firmware) and a PC running Avaya Communicator for Windows. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the IP Office system, and an Avaya IP Office Application Server running Avaya Voicemail Pro, providing voice messaging service to the IP Office users. Mobile Twinning is configured for some of the IP Office users so that calls to these user's extensions will also ring and can be answered at the configured mobile phones.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between the Avaya system and the Clearcom network did not include the use of any specific encryption features.

The transport protocol between IP Office and Clearcom, across the public Internet, is SIP over UDP. The transport protocol between Avaya endpoints and IP Office, inside the enterprise private IP network (LAN), is SIP over TLS.

For the purposes of the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to Clearcom. The short code 9 was stripped off by IP Office but the remaining N digits were sent unaltered to the network. Refer to **Section 5.5** for configuration.

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

For confidentiality and privacy purposes, public IP addresses, domain names, and routable DID numbers used during the compliance testing have been masked.

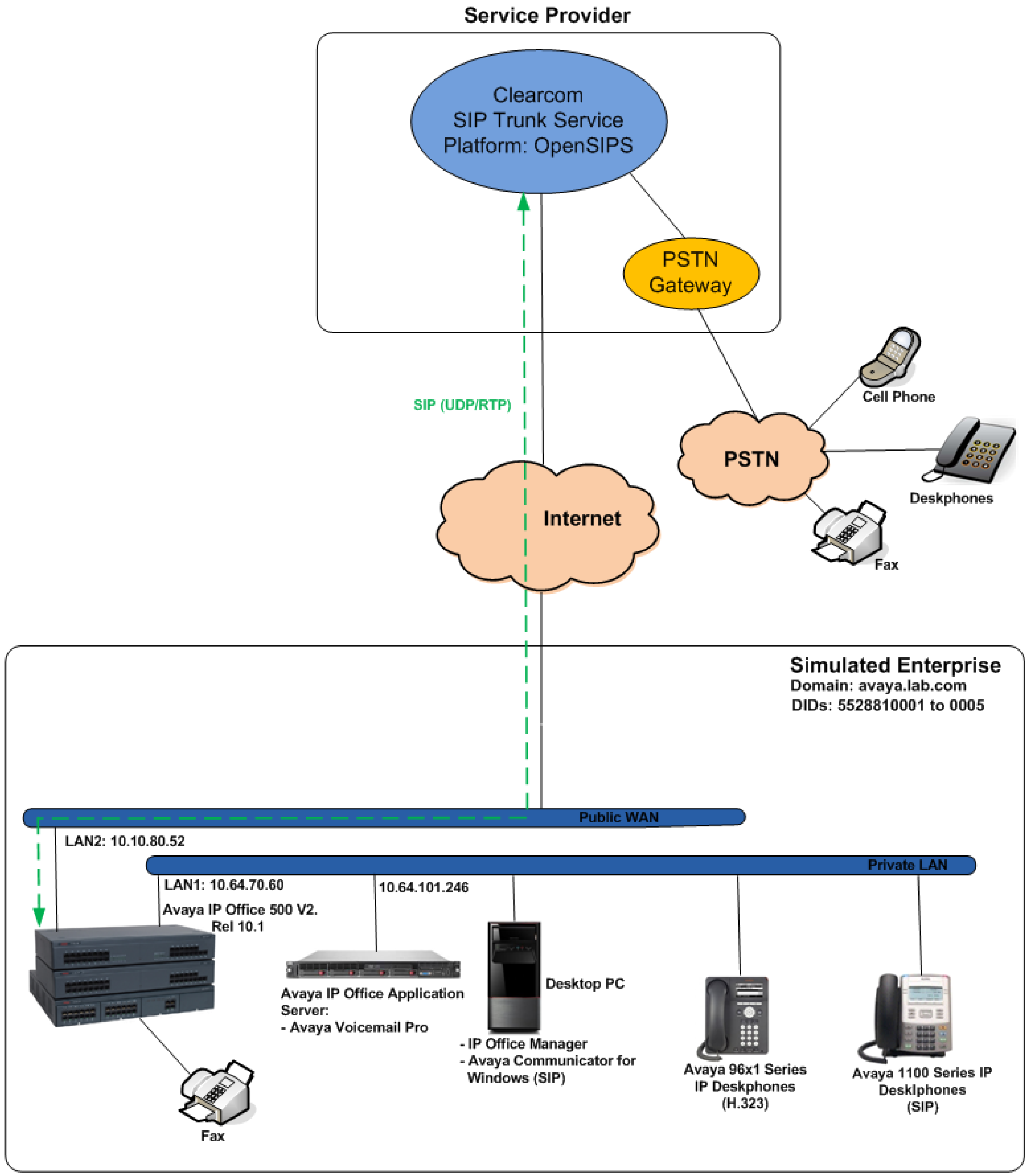


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya IP Office 500v2	10.1.0.1.0 Build 3
Avaya IP Office DIG DCPx16 V2	10.1.0.1.0 Build 3
Avaya IP Office Manager	10.1.0.1.0 Build 3
Avaya IP Office Application Server ▪ Voicemail Pro	10.1.0.1.0 Build 3 10.1.0.1.0 build 6
Avaya Session Border Controller for Enterprise (running on Portwell CAD-0208 platform)	7.2.1.0-05-14222
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6506
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya Communicator for Windows	2.1.4.274
Clearcom	
OpenSIPS Softswitch	1.9
OpenSIPS Session Border Controller	1.9

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition.

5. Configure Avaya IP Office

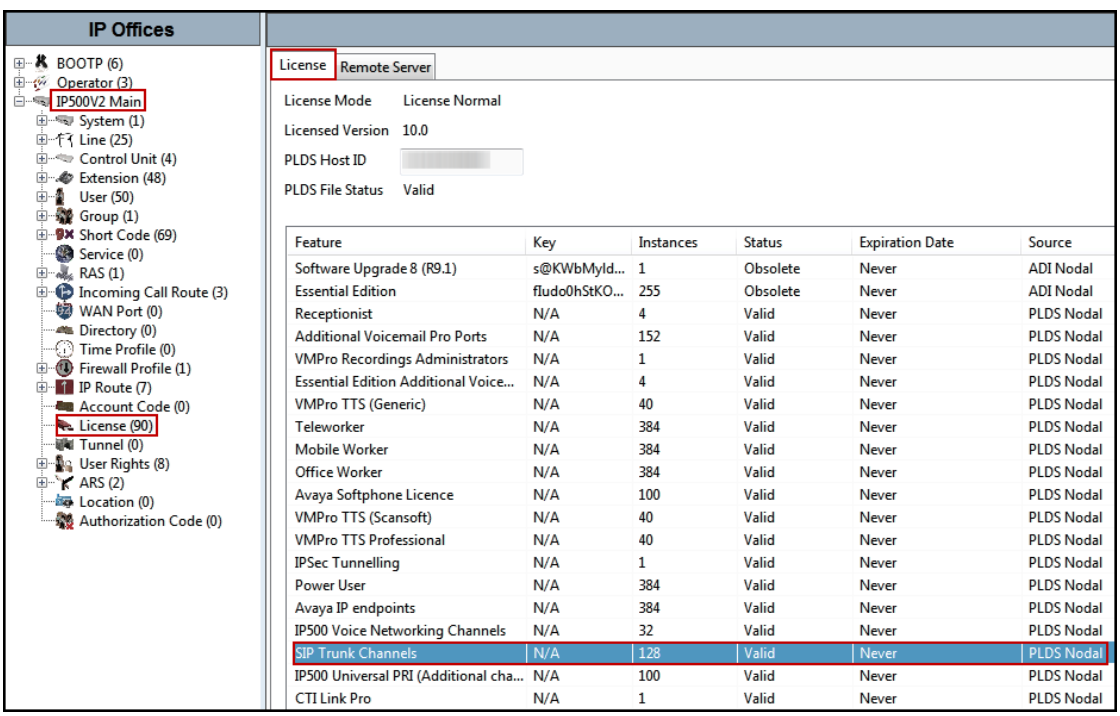
This section describes the IP Office configuration required to interwork with Clearcom SIP Trunking Service. IP Office is configured through Avaya IP Office Manager (IP Office Manager) which is a PC application. On the PC, select **Start → Programs → IP Office → Manager** to launch IP Office Manager. 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 in the next sections. 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 of IP Office have already been completed and are not discussed here. For further information on IP Office, please consult **Error! Reference source not found.** in **Section 9**.

5.1. Licensing and Physical Hardware

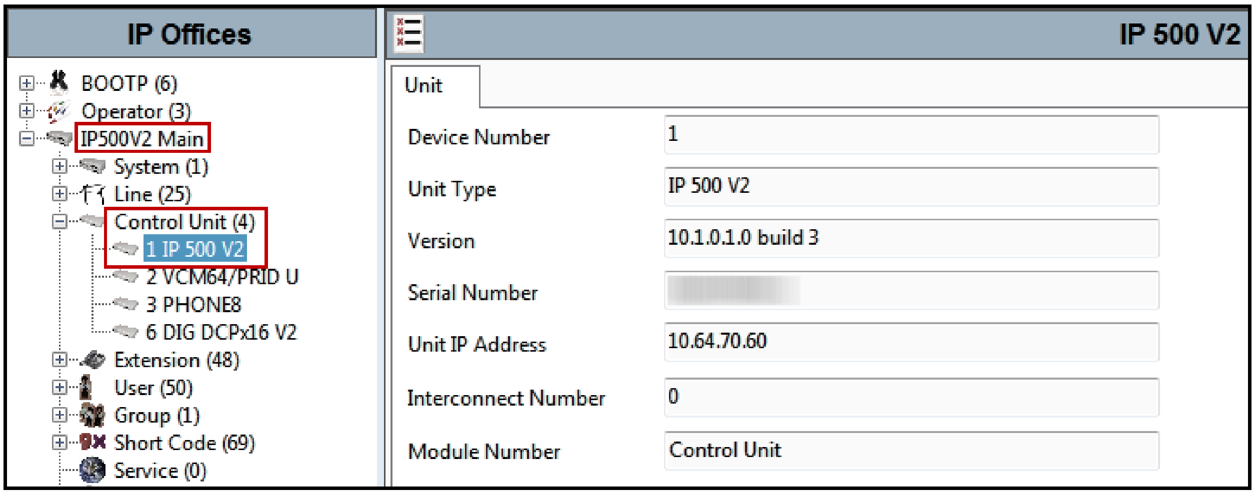
The configuration and features described in these Application Notes require the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

To verify that there is a SIP Trunk Channels License with sufficient capacity; click **License**, then from the license tab, locate **SIP Trunk Channels**. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the **Details** pane.



To view the physical hardware comprising IP Office, expand the components under the **Control Unit** in the **Navigation** pane. In the sample configuration, the Avaya IP Office 500 V2 is equipped with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module) for supporting VoIP codecs. An IP Office hardware configuration with a VCM component is necessary to support SIP trunking.

To view the details of the component, select the component in the Navigation pane. The following screen shows the details of the **IP 500 V2**.



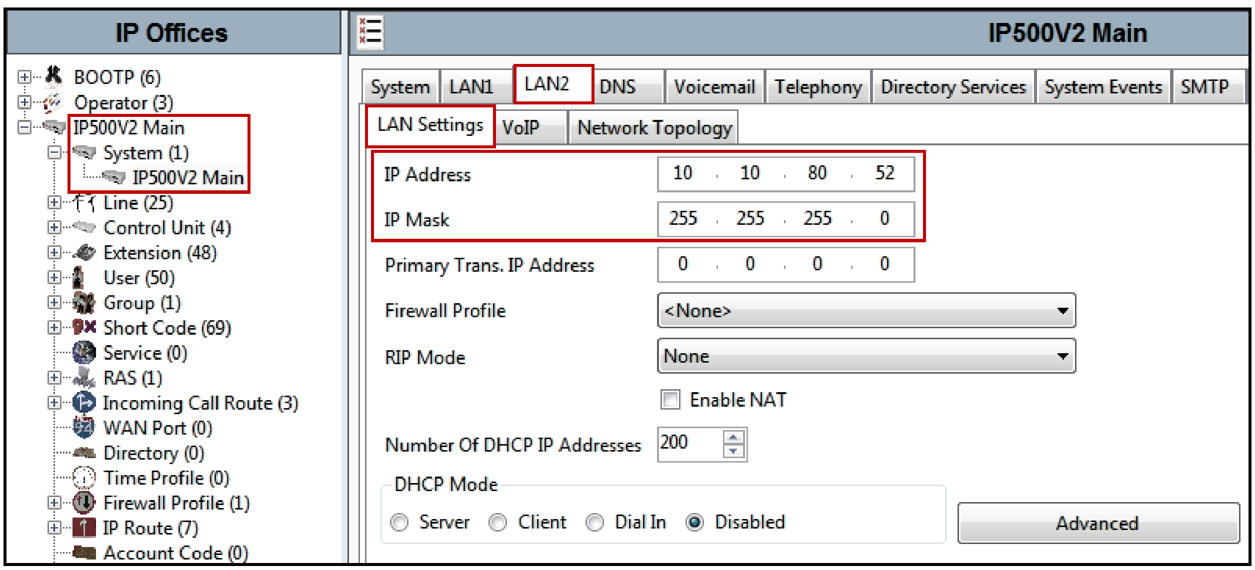
5.2. System

Configure the necessary system settings. In an IP Office the LAN2 tab settings correspond to the IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side).

5.2.1. System – LAN2 Tab

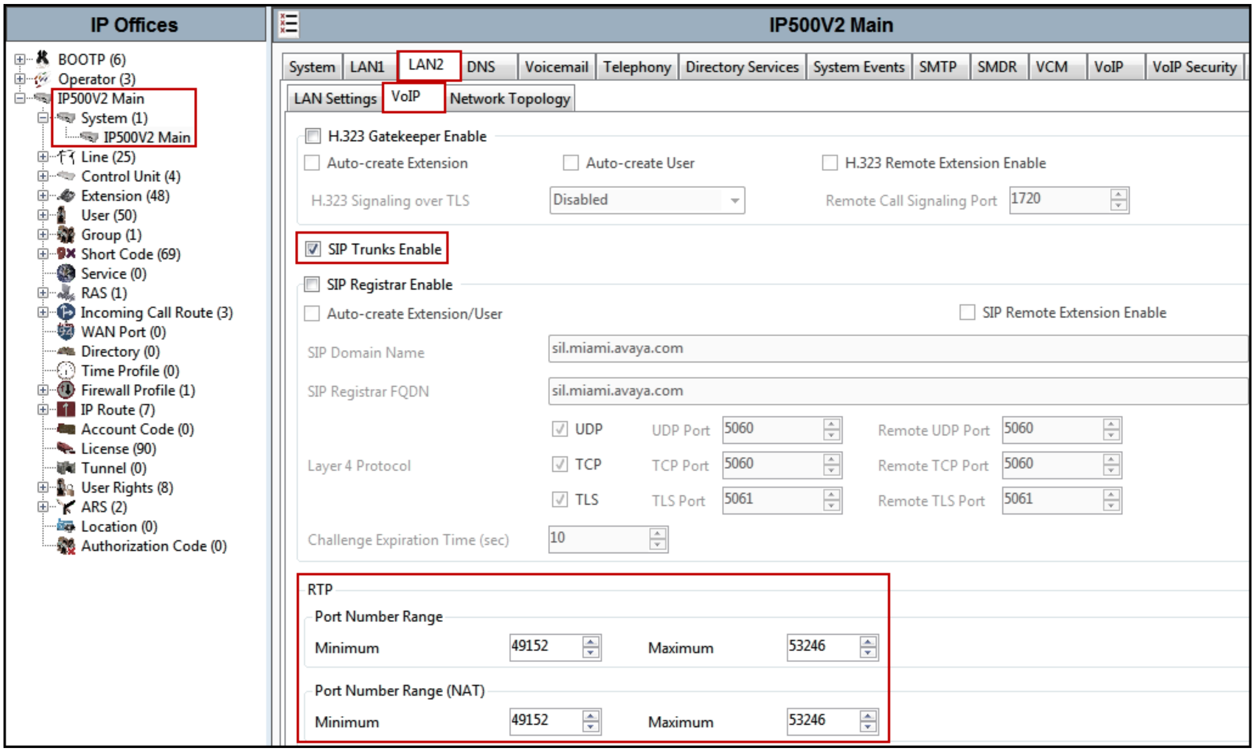
In the sample configuration, the IP Office WAN port was used to connect to Clearcom. The LAN2 settings correspond to the WAN port on the IP Office 500 V2. To access the LAN2 settings, first navigate to **System** → *<Name>*, where *<Name>* is the system name assigned to IP Office. In this compliance test, the system name is **IP500V2 Main**. Next, navigate to the **LAN2** → **LAN Settings** tab in the **Details** pane, configure the following parameters:

- Set the **IP Address** field to the public IP address assigned to the IP Office WAN port.
- Set the **IP Mask** field to the mask used with the public IP address. All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).



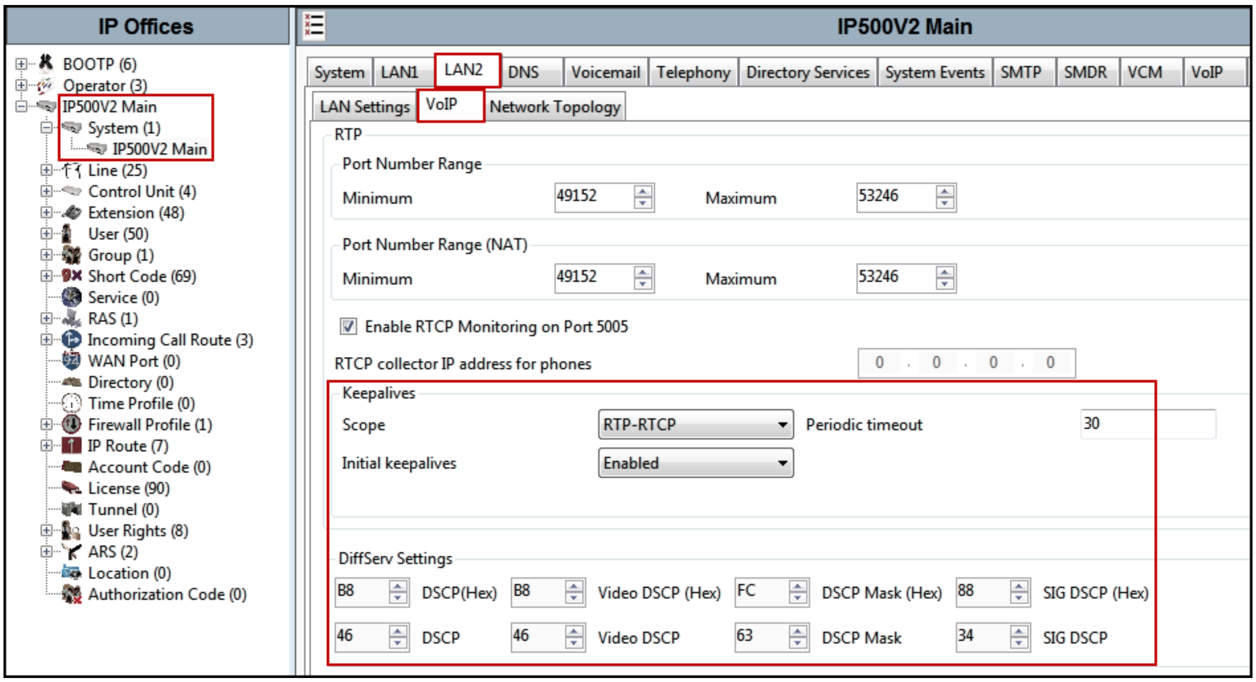
On the **VoIP** tab in the **Details** pane, configure the following parameters:

- Check the **SIP Trunks Enable** to enable the configuration of SIP Trunk connecting to Clearcom.
- Verify the **RTP Port Number Range** settings for a specific range for the RTP traffic. The **Minimum** and **Maximum** values were kept as default.



Scroll down the page:

- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. These settings will cause IP Office to send a RTP and RTCP keepalive packet starting at the time of initial connection and every 30 seconds thereafter if no other RTP/RTCP traffic is present. This facilitates the flow of media in cases where each end of the connection is waiting to see media from the other, as well as helping to keep firewall ports open for the duration of the call.
- In the **DiffServ Settings** section, IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signaling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signaling. The specific values used for the compliance test are shown in the example below and are also the default values. For a customer installation, if the default values are not sufficient, appropriate values will be provided by the customer.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).

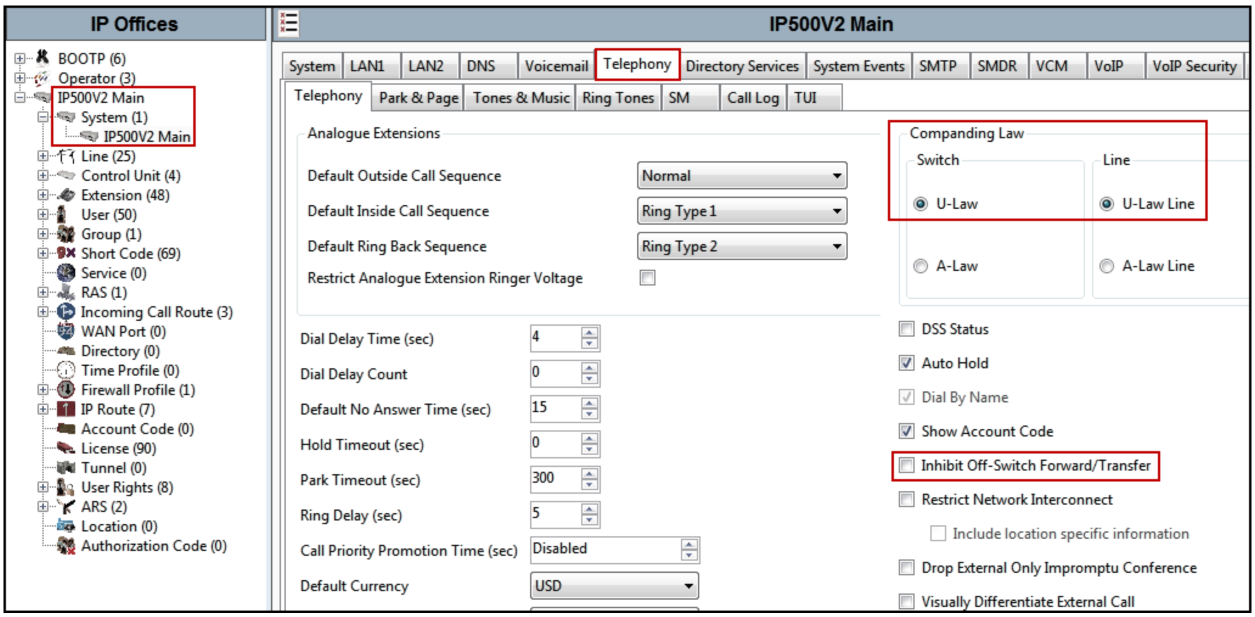


Note: In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network (private network). The LAN1 interface configuration is not directly relevant to the interface with the Clearcom SIP Trunking Service, and therefore is not described in these Application Notes.

5.2.2. System - Telephony Tab

To access the System Telephony settings, navigate to the **Telephony → Telephony** tab in the **Details** pane, configure the following parameters:

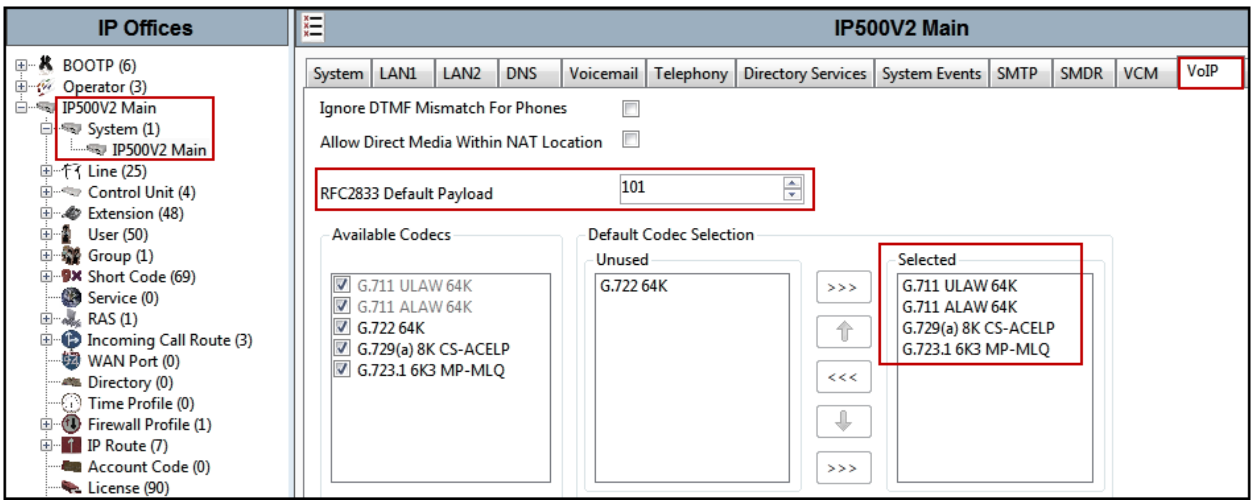
- Choose the **Companding Law** typical for the enterprise location, **U-Law** was used for the compliance test, **A-Law** could have been selected instead.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).



5.2.3. System - VoIP Tab

To view or change the System Codecs settings, navigate to the **VoIP** tab in the **Details** pane as shown in the following screen, configure the following parameters:

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order was used.
- Click **OK** to commit (not shown).

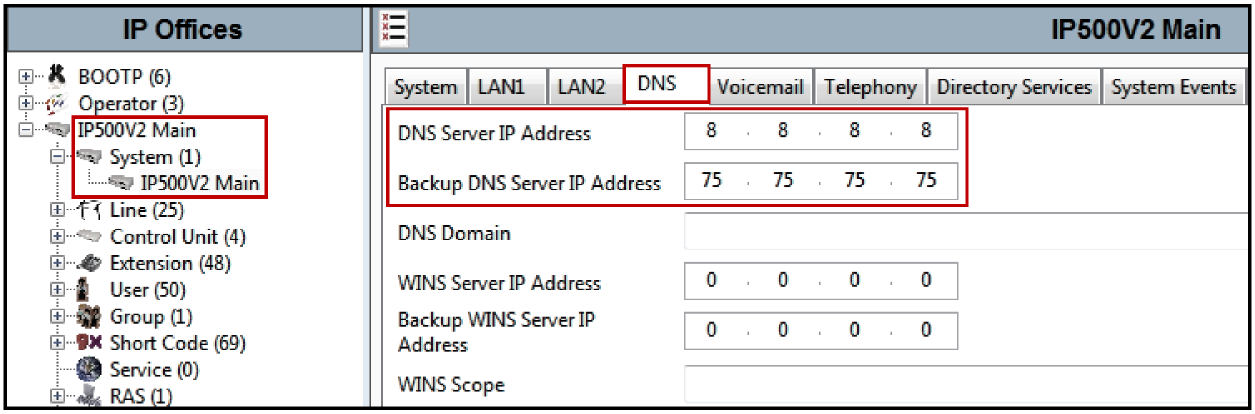


Note: The codec selections defined under this section (System – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.3.6** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.2.4. System - DNS Tab

Public DNS servers IP addresses are required to be configured, IP Office will retrieve Clearcom's Proxy IP Address via public DNS queries using Clearcom's ISTP Domain Name configured under in **Section 5.3.2**. To access the System DNS settings, navigate to the **DNS** tab in the **Details** pane, configure the following parameters:

- Under **DNS Server IP Address** and **Backup DNS Server IP Address** enter the primary and backup public DNS servers IP addresses. These IP addresses should be provided by Clearcom.
- Click **OK** to commit (not shown).

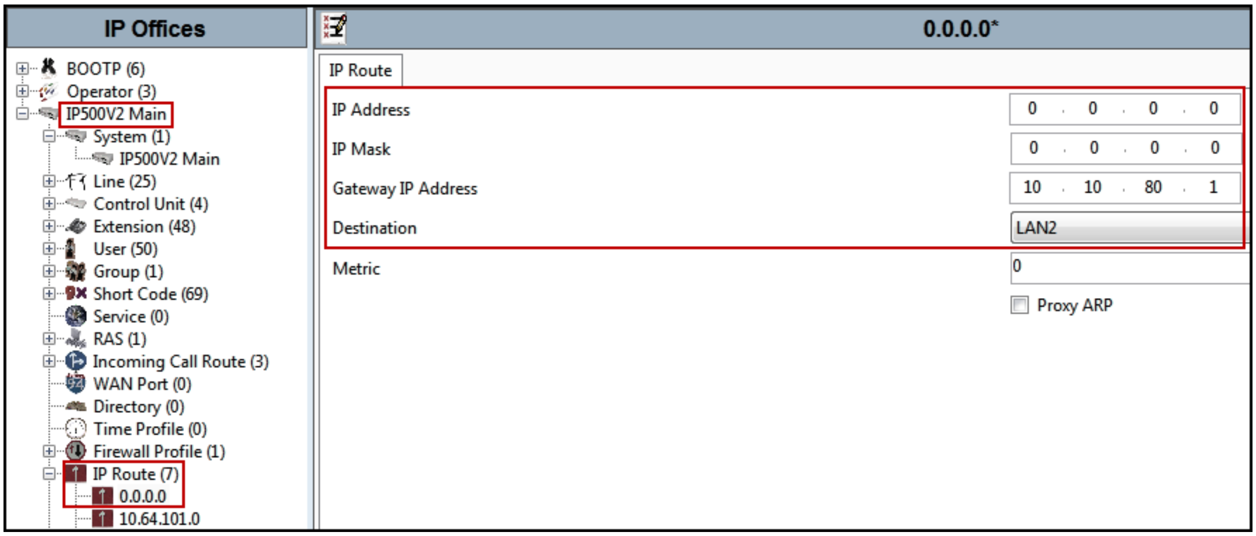


5.2.5. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to route calls to Clearcom's network.

Navigate to **IP Route**, right-click on **IP Route** and select **New**. The values used during the compliance test are shown below:

- Set the **IP Address** and **IP Mask** to **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP address of the gateway/router used to route calls to the public network, e.g., **10.10.80.1**.
- Set **Destination** to **LAN2** from the pull-down menu.
- Click **OK** to commit (not shown).



5.3. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Clearcom. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Sections 5.3.1** to create the SIP Line from the template.

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

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

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.3.2** to **5.3.7**.

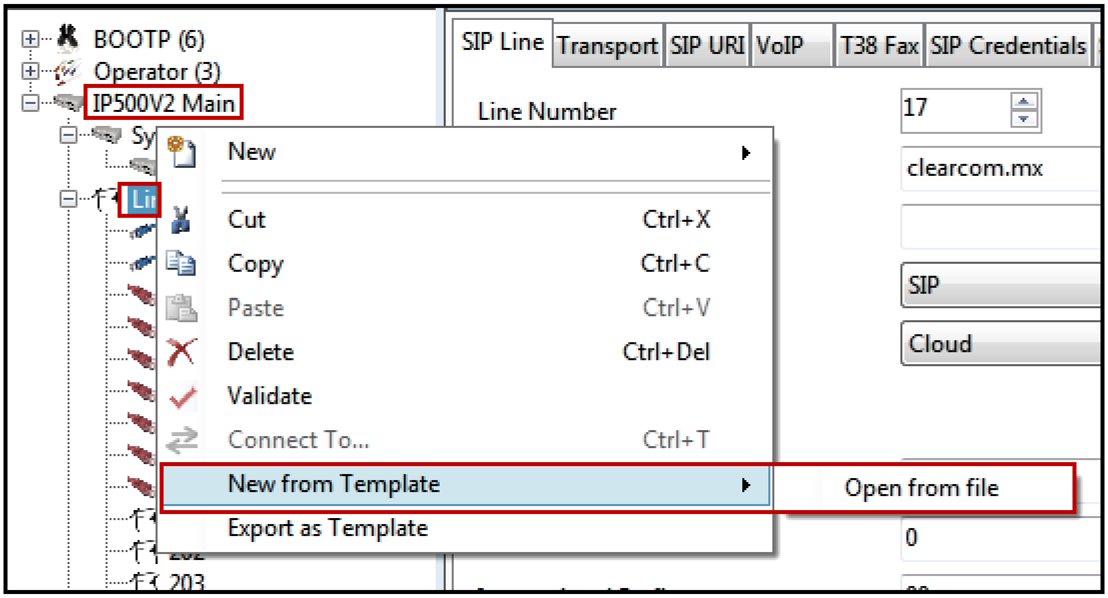
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.3.2** to **5.3.7**.

5.3.1. Creating a SIP Trunk from an XML Template

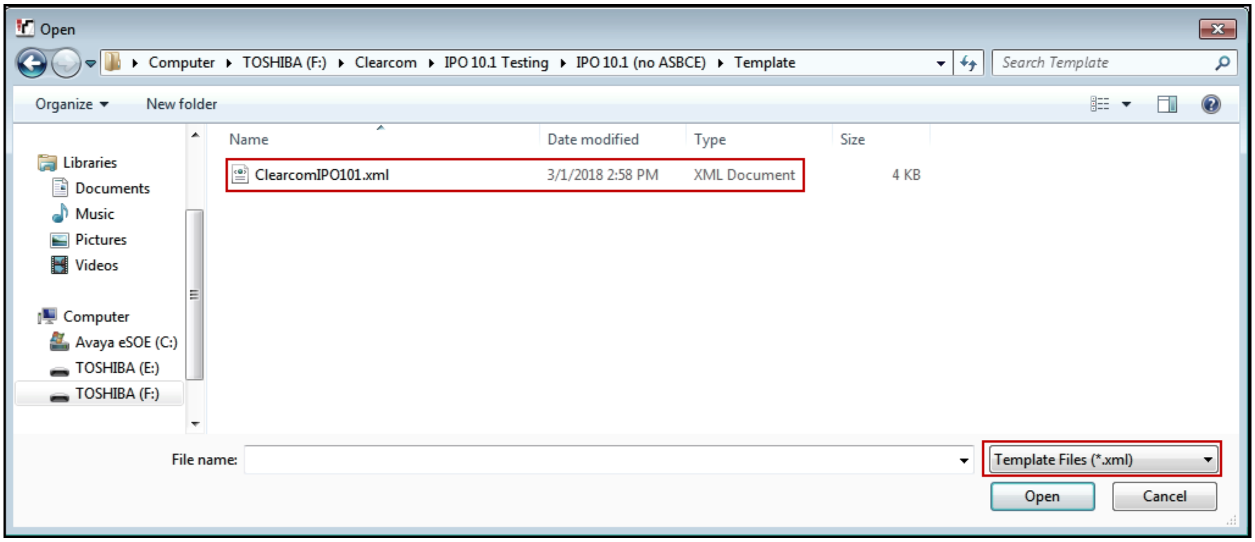
DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., *\temp*) on the same computer where IP Office Manager is installed.

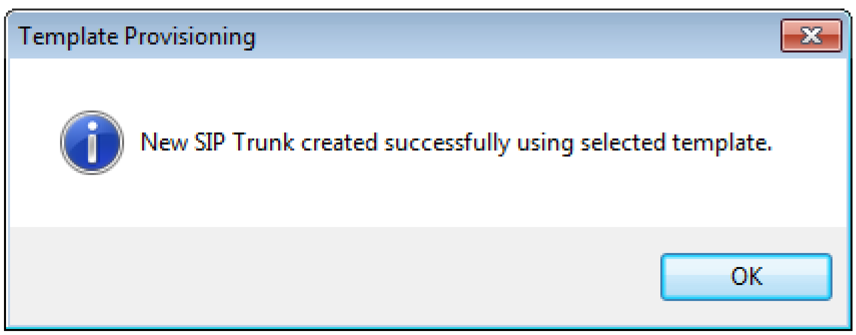
To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template→Open from file**.



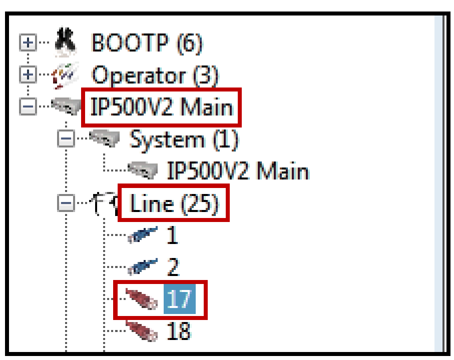
Navigate to the directory on the local machine where the template was copied and select the template.



After the import is complete, a final import status pop-up window will open stating success or failure. Click **OK**.



The newly created SIP Line will appear in the Navigation pane (e.g., SIP Line **17**).

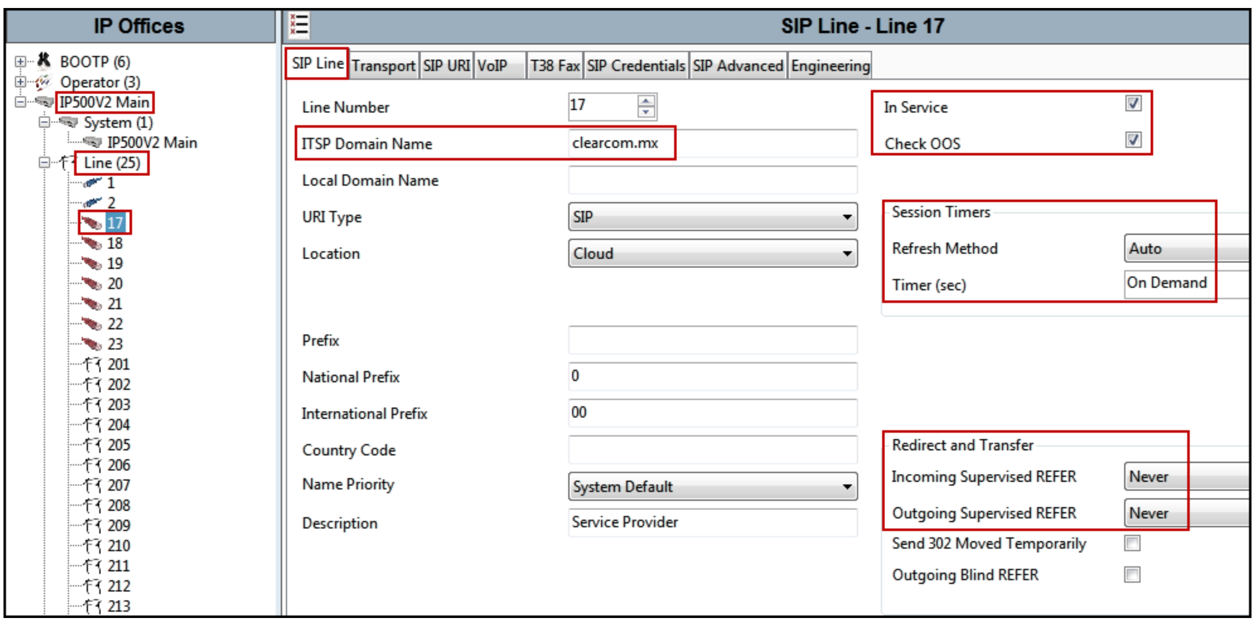


It is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Sections 5.3.2** to **5.3.7**.

5.3.2. SIP Line – SIP Line Tab

On the **SIP Line** tab in the **Details** pane, configure or verify the parameters as shown below:

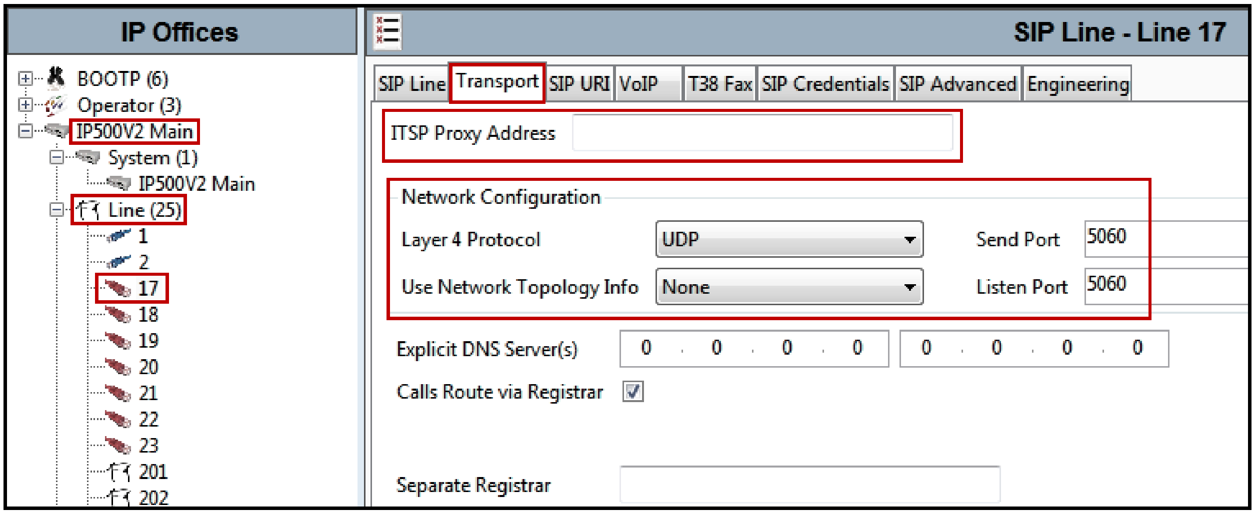
- Set **ITSP Domain Name** to **clearcom.mx**, the domain name provided by Clearcom.
- Verify that **In Service** box is checked, the default value. This makes the trunk available to incoming and outgoing calls.
- Verify that **Check OOS** box is checked, the default value. IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Verify that **Refresh Method** is set to **Auto**.
- Verify that **Timer (sec)** is set to **On Demand**.
- For the compliance test REFER support was disabled. Thus, **Incoming Supervised REFER** and **Outgoing Supervised REFER** should be set to **Never**. Refer to **Sections 2.1** and **2.2** for the reason this field was disabled.
- Click **OK** to commit (not shown).



5.3.3. SIP Line - Transport Tab

Select the **Transport** tab. Set or verify the parameters as shown below:

- Leave the **ITSP Proxy Address** blank (IP Office will retrieve the ITSP Proxy Address via public DNS queries using the ISTP Domain Name provided under in **Section 5.3.2**). The public DNS IP addresses were configured under **Section 5.2.4**.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** and **Listening Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

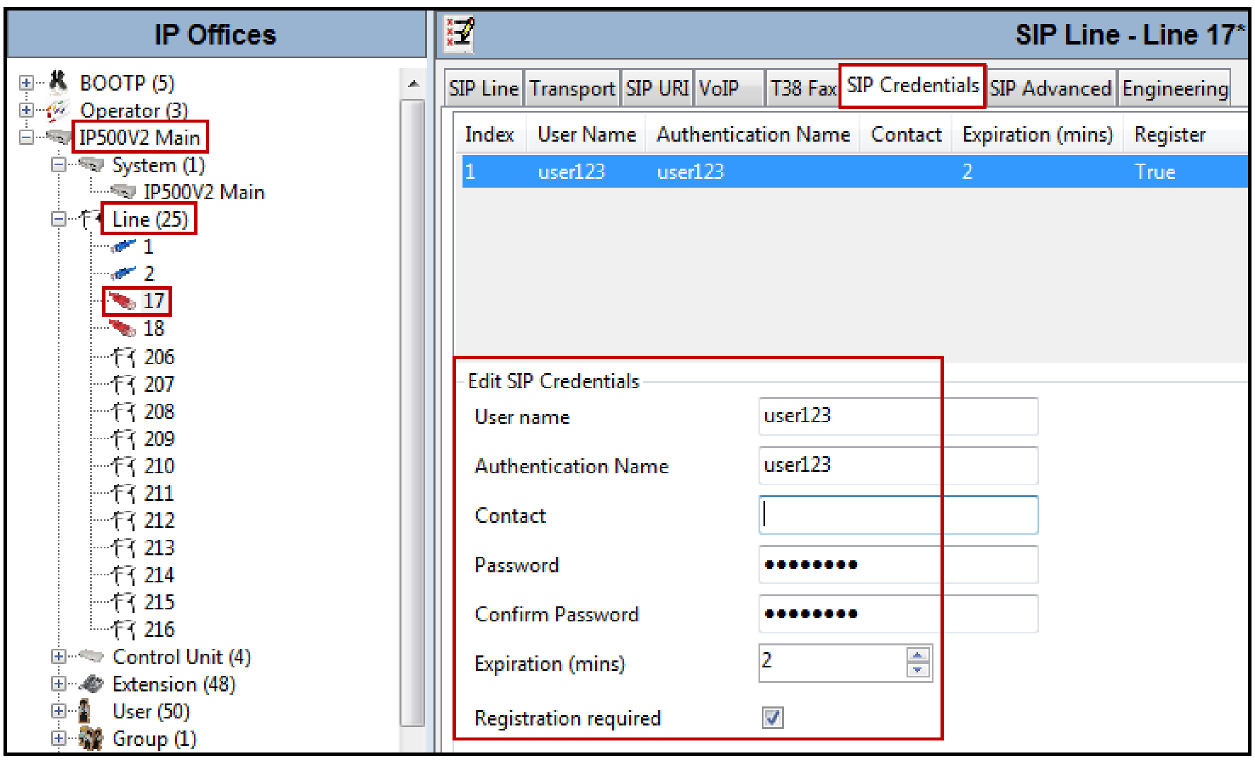


Note – For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was used in the test configuration. In addition, it was not necessary to configure the **System → LAN2 → Network Topology** tab for the purposes of SIP trunking. If a NAT is used between Avaya IP Office and the other end of the trunk, then the **Use Network Topology Info** field should be set to the LAN interface (LAN1 or LAN2) used by the trunk and the **System → LAN1 (or 2) → Network Topology** tab needs to be configured with the details of the NAT device.

5.3.4. SIP Line – SIP Credentials Tab

Select the **SIP Credentials** tab, and then click the **Add** button to add the SIP Trunk registration credentials. Set the parameters as show below:

- For **User name**, add the user name credential provided by Clearcom for SIP Trunk registration.
- For **Authentication Name**, add the authentication name credential provided by Clearcom for SIP Trunk registration. For the compliance test the same value used under **User Name** was used.
- Leave the **Contact** blank.
- For **Password** and **Confirm Password**, add the password credential provided by Clearcom for SIP Trunk registration.
- Set **Expiry (mins)** to a value acceptable to the enterprise. This setting defines how often registration with Clearcom is required following any previous registration. For the compliance test **2** minutes was used.
- Verify that **Registration required** is checked.
- Click the **OK** to commit (not shown).

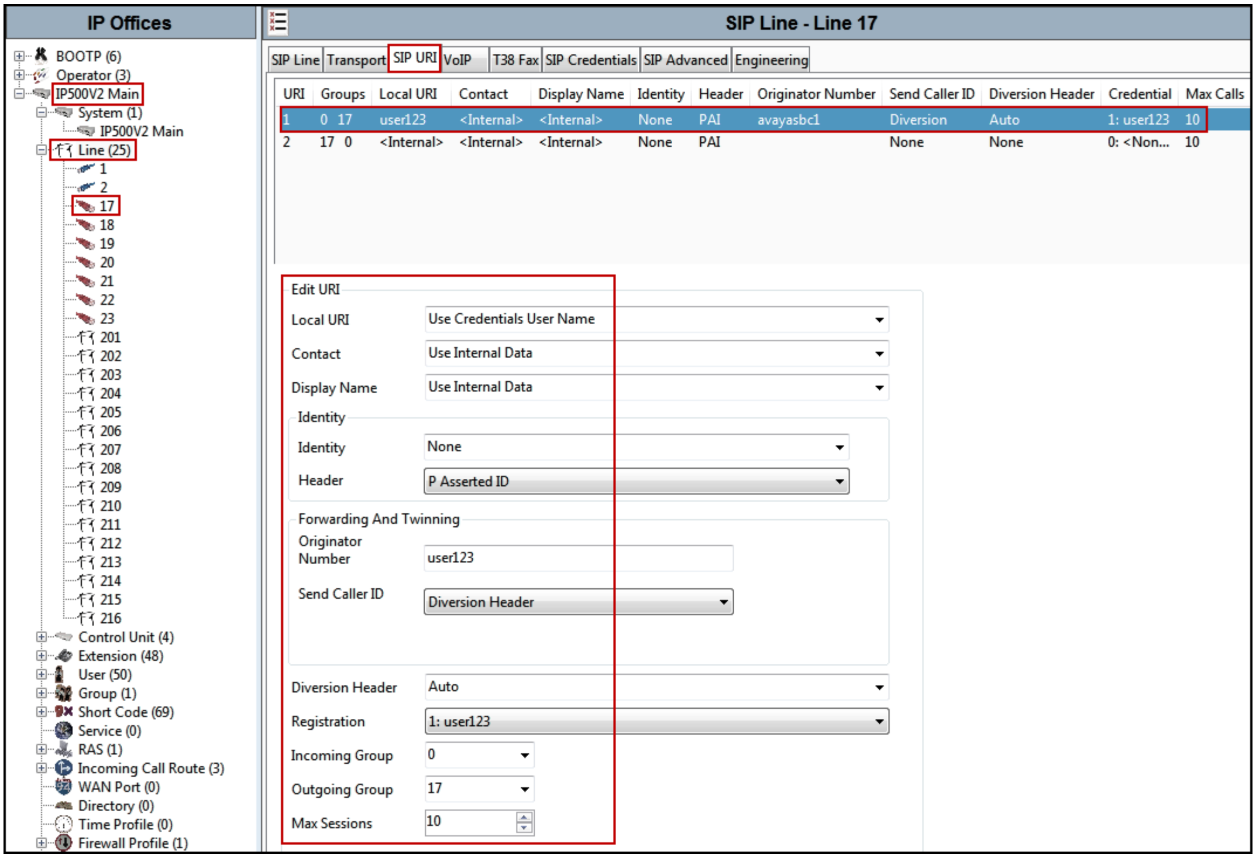


5.3.5. SIP Line - SIP URI Tab

Two SIP URI entries must be created to match each outgoing number that Avaya IP Office will send on this line and incoming numbers that Avaya IP Office will accept on this line.

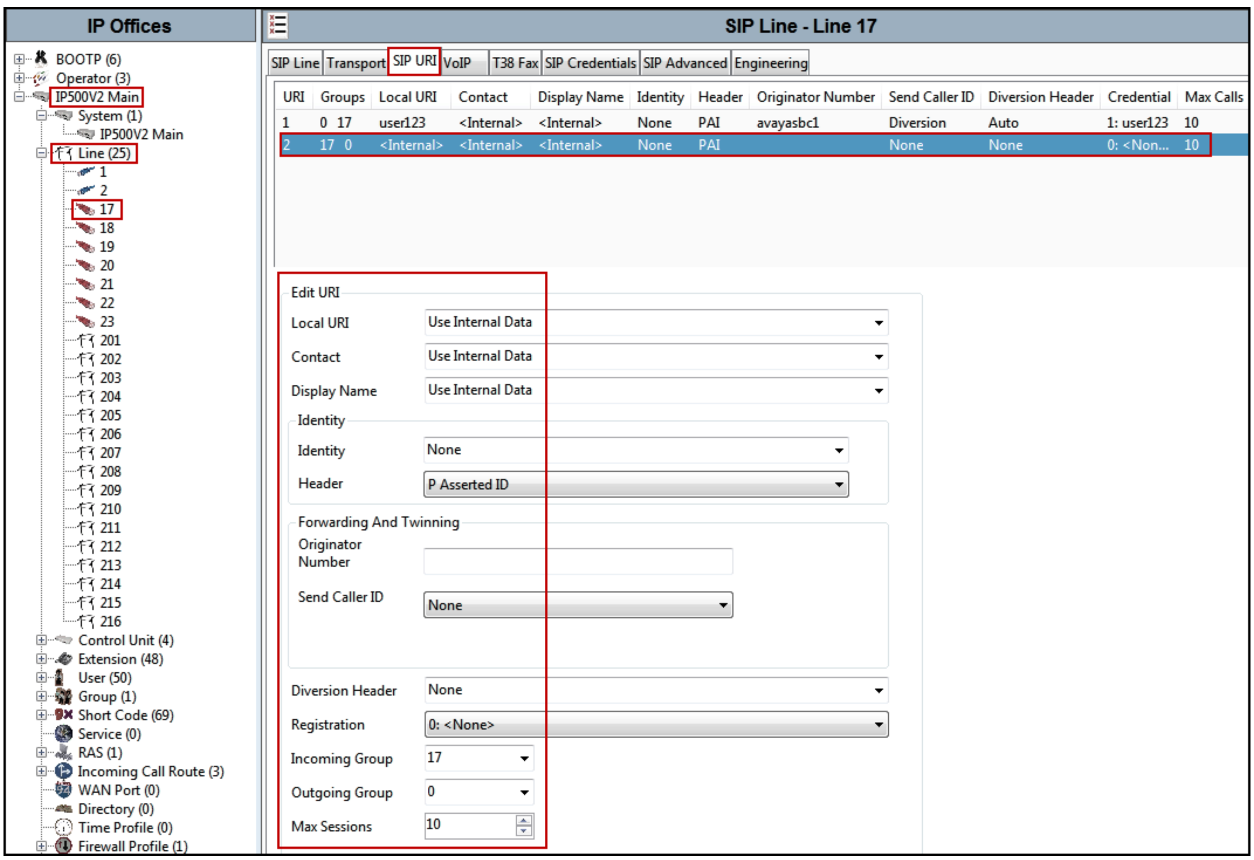
To set the SIP URI for outgoing numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

- Set **Local URI** to **Use Credential User Name**, the user name associated with the SIP trunk credentials provided by Clearcom. Clearcom required the user name to be sent in the “From” header.
- Set **Contact** and **Display Name** to **Use Internal Data**
- Set **Identity** under **Identity** to **None**.
- Set **Header** under **Identity** to **P Asserted ID**.
- Set **Originator Number** under **Forwarding and Twinning** to the user name associated with the SIP trunk registration credentials provided by Clearcom.
- Set **Send Caller ID** under **Forwarding and Twinning** to **Diversion Header**.
- Set **Diversion Header** to **Auto**.
- Under **Registration**, select **1: user123** from the pull-down menu (this field will default to the **User Name** used under the **SIP Credentials** tab).
- Set **Incoming Group** to **0**.
- Set **Outgoing Group** to **17** (SIP Line number being used).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit (not shown).
- Click **OK** to commit again (not shown).


IP Offices
BOOTP (6)
Operator (3)
IP500V2 Main
System (1)
IP500V2 Main
Line (25)
1
2
17
18
19
20
21
22
23
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
Control Unit (4)
Extension (48)
User (50)
Group (1)
Short Code (69)
Service (0)
RAS (1)
Incoming Call Route (3)
WAN Port (0)
Directory (0)
Time Profile (0)
Firewall Profile (1)
SIP Line - Line 17
SIP Line
Transport
SIP URI
VoIP
T38 Fax
SIP Credentials
SIP Advanced
Engineering
URI Groups Local URI Contact Display Name Identity Header Originator Number Send Caller ID Diversion Header Credential Max Calls
1 0 17 user123 <Internal> <Internal> None PAI avayasbc1 Diversion Auto 1: user123 10
2 17 0 <Internal> <Internal> <Internal> None PAI None None 0: <Non... 10
Edit URI
Local URI
Use Credentials User Name
Contact
Use Internal Data
Display Name
Use Internal Data
Identity
Identity
None
Header
P Asserted ID
Forwarding And Twinning
Originator Number
user123
Send Caller ID
Diversion Header
Diversion Header
Auto
Registration
1: user123
Incoming Group
0
Outgoing Group
17
Max Sessions
10

To set the SIP URI for incoming numbers, select the **SIP URI** tab, then click the **Add** button and the **New Channel** area will appear at the bottom of the pane. To edit an existing entry, click an entry in the list at the top, and click the **Edit** button. The entry was created with the parameters shown below:

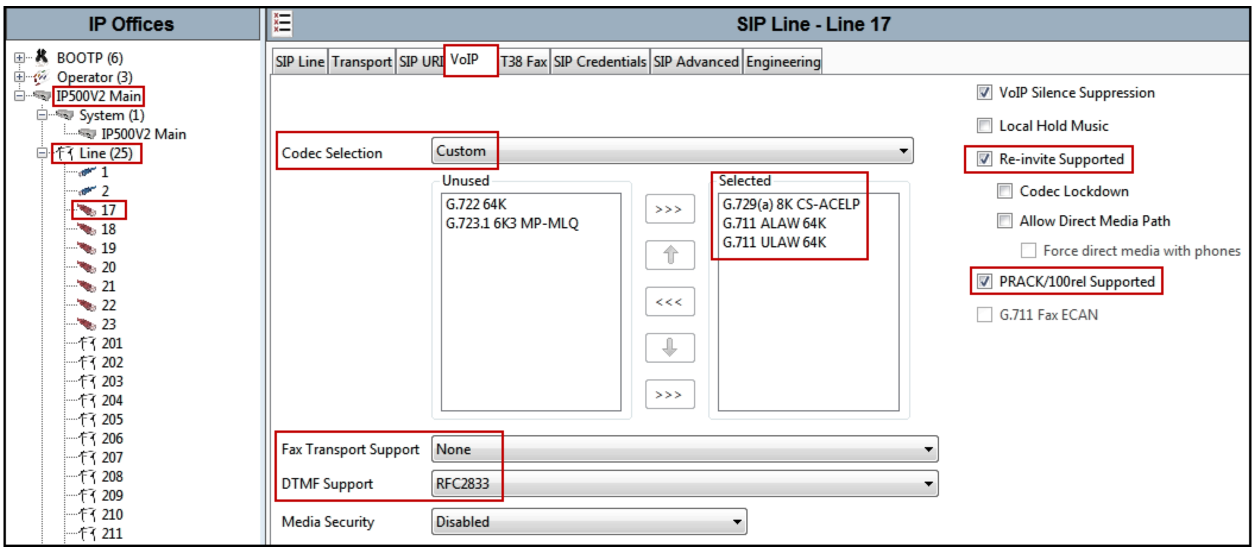
- Set **Local URI**, **Contact** and **Display Name** to **Use Internal Data**. This setting allows calls on this line that have a SIP URI that matches the number set in the **SIP** tab of any user as shown later in **Section 5.4**.
- Set **Identity** under **Identity** to **None**.
- Set **Header** under **Identity** to **P Asserted ID**.
- Set **Send Caller ID** under **Forwarding and Twinning** to **None**.
- Set **Diversion Header** to **None**.
- Under **Registration**, select **0: <None>** from the pull-down menu.
- Set **Incoming Group** to **17** (SIP Line number being used).
- Set **Outgoing Group** to **0**.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Click **OK** to commit (not shown).
- Click **OK** to commit again (not shown).



5.3.6. SIP Line - VoIP Tab

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

- The **Codec Selection** was configured using the **Custom** option, allowing an explicit order of codecs to be specified for the SIP Line. The buttons allow setting the specific order of preference for the codecs to be used on the SIP Line, as shown. Clearcom supports codec **G.729(a)**, **G.711ALAW** and **G.711ULAW** for audio, with G.729(a) being the preferred codec.
- Select **None** for **Fax Transport Support** (Refer to **Sections 2.1** and **2.2**).
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check the **Re-invite Supported** box.
- Check the **PRACK/100rel Supported** box.
- Default values may be used for all other parameters.
- Click the **OK** to commit (not shown).

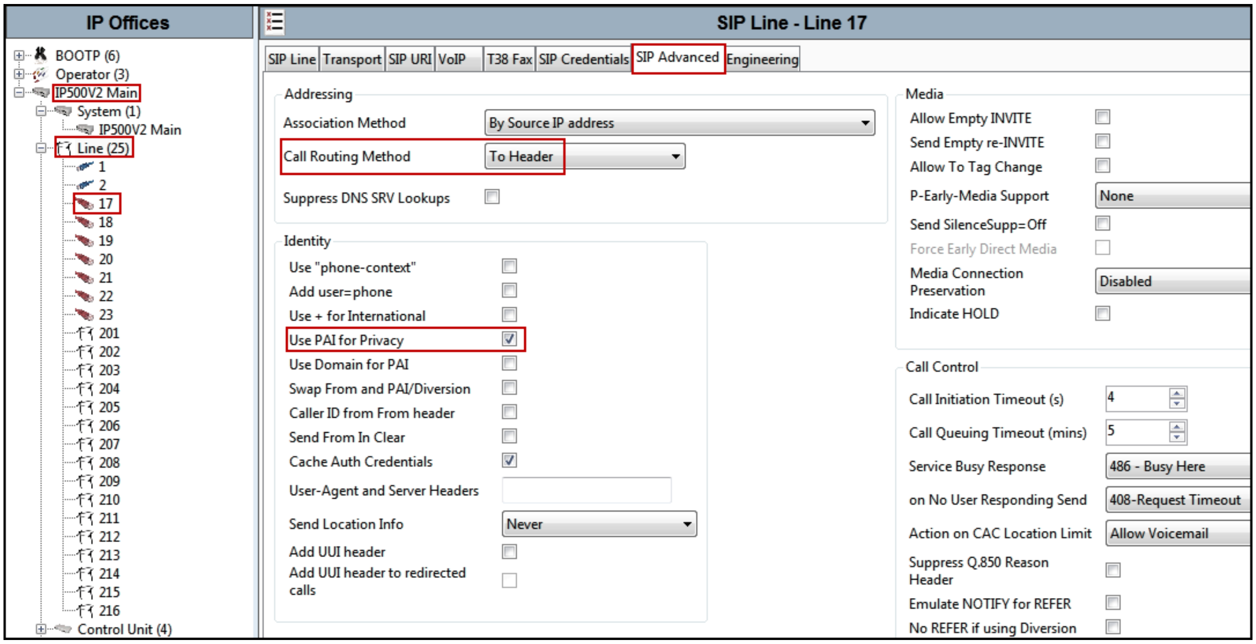


Note: The codec selections defined under this section (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.3** (System – VoIP tab) are the codecs selected for the IP phones/extension (H.323 and SIP).

5.3.7. SIP Line – SIP Advanced Tab

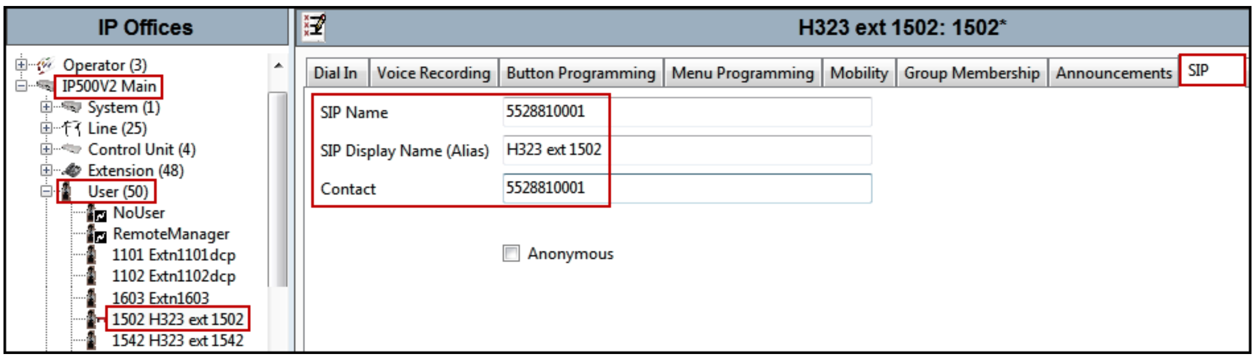
Select the **SIP Advanced** tab. Set or verify the parameters as shown below:

- Under **Call Routing Method** select **To Header** from the pull-down menu.
- Check the box for **Use PAI for Privacy**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).



5.4. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.3**. To configure these settings, first navigate to **User** → *Name* in the Navigation Pane where *Name* is the name of the user to be modified. In the example below, the name of the user is **IP H323 1502**. Select the **SIP** tab in the Details Pane. The values entered for the **SIP Name** allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.3.6**). The **SIP Name** and **Contact** are set to one of the DID numbers assigned to the enterprise by Clearcom. The **SIP Display Name (Alias)** parameter can optionally be configured with a descriptive name. If all calls involving this user and a SIP Line should be considered private, then the **Anonymous** box may be checked to withhold the user's information from the network. This can also be accomplished by activating **Withhold Number** on H.323 Deskphones. Click the **OK** to commit (not shown).



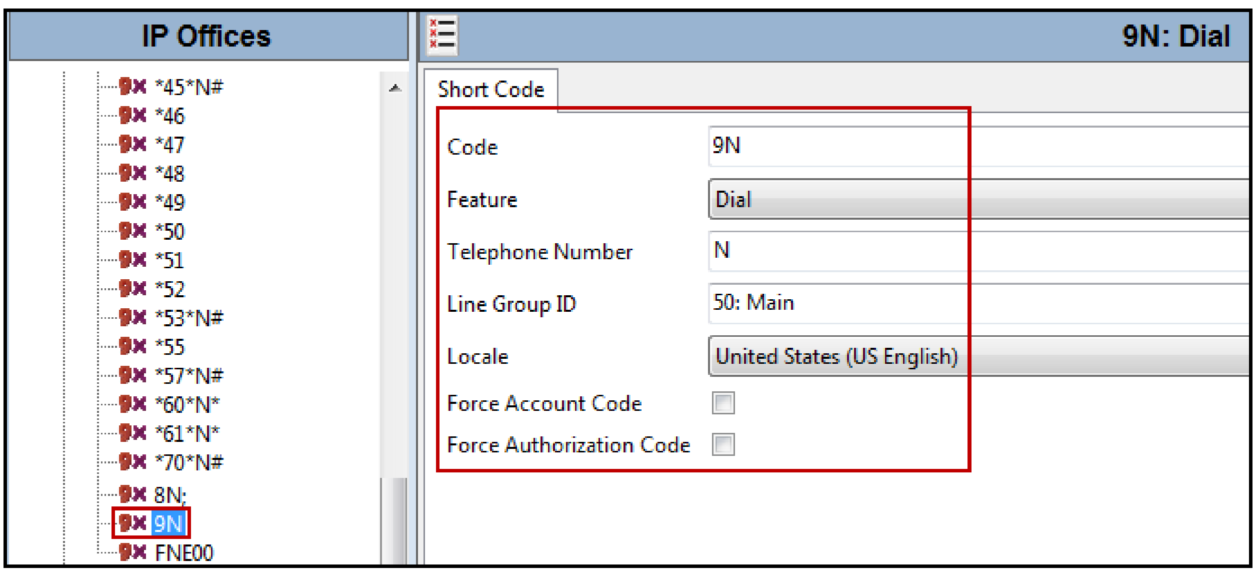
5.5. Outbound Call Routing

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

5.5.1. Short Codes and Automatic Route Selection

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

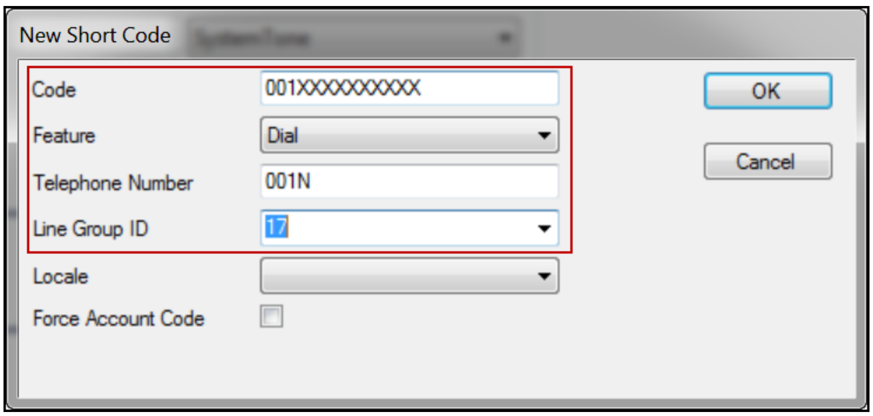
- In the **Code** field, enter the dial string which will trigger this short code. In this case, **9N** was used (note that the semi-colon is not used here).
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The value **N** represents the number dialed by the user after removing the **9** prefix. This value is passed to ARS.
- Set the **Line Group ID** to **50: Main** to be directed to **Line Group 50: Main**, this is configurable via ARS.
- For **Locale**, **United States (US English)** was used.
- Click the **OK** to commit (not shown).



The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **X**'s used in the **Code** column of the entries to specify the exact number of digits to be expected, following the access code and the first set of digits on the string. This type of setting results in a much quicker response in the delivery of the call by IP Office.

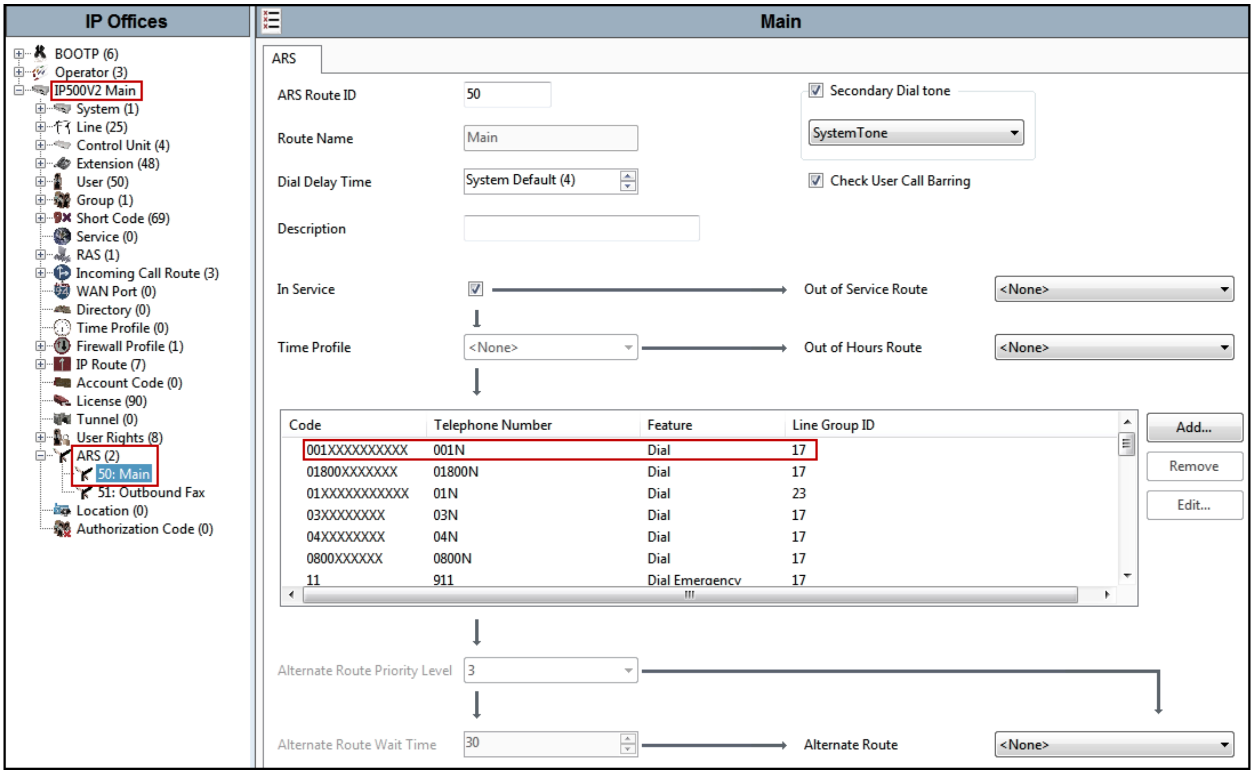
To create a short code to be used for ARS, select **ARS → 50: Main** on the Navigation Pane and click **Add**.

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **001** followed by **10 X**'s to represent the exact number of digits.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **001N**. The value **N** represents the additional number of digits dialed by the user after dialing **001** (The **9** will be stripped off).
- Set the **Line Group Id** to the Line Group number being used for the SIP Line, in this case Line **Group ID 17** was used.
- Click **OK** to commit.



Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

The first example highlighted below shows that for calls from Mexico to the North American numbering plan, the user dialed **9**, followed by **001** and **10** digits (represented by **10 X**'s). The **9** is stripped off, the remaining digits, including the **001** shown in the examples below, are included in the SIP INVITE message IP Office sends to Clearcom.



5.6. Incoming Call Route

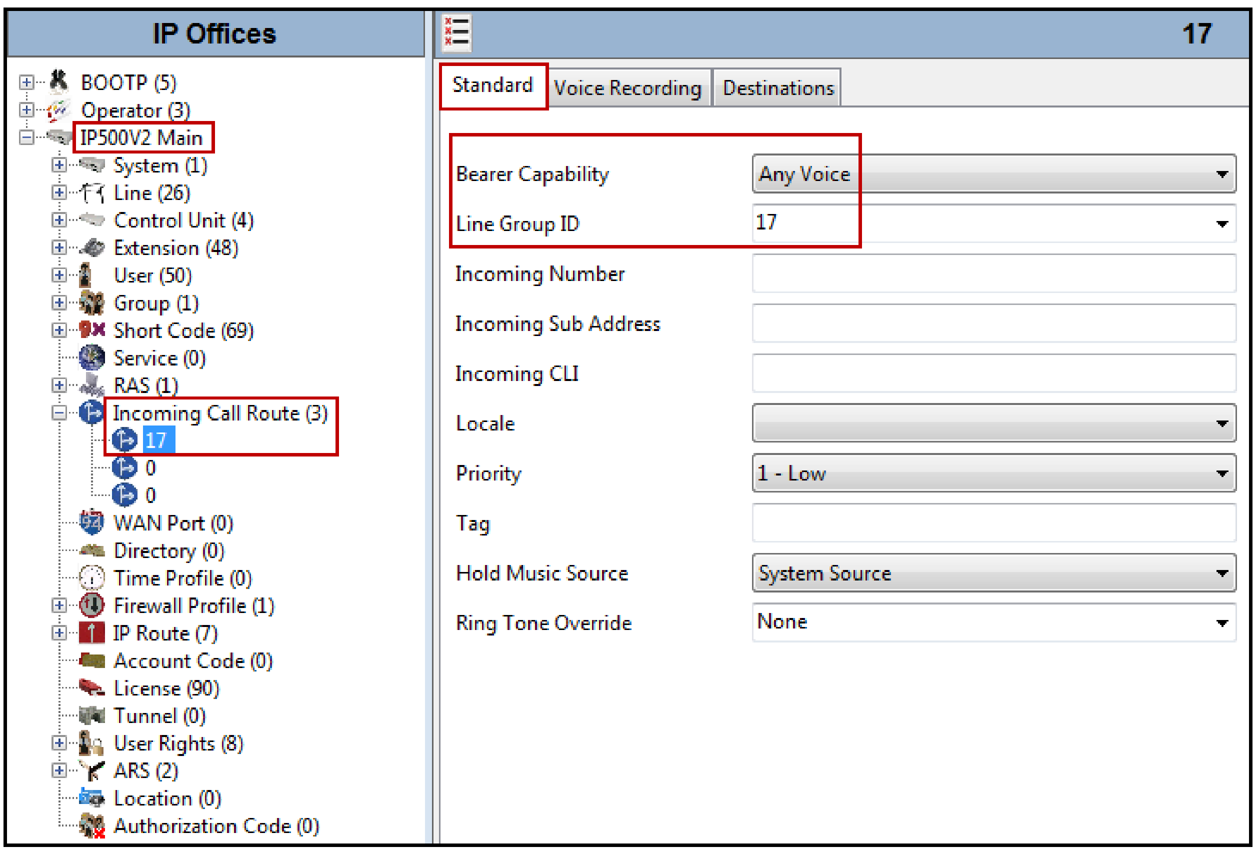
An incoming call route maps inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system.

In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any predefined extension in IP Office. The routing decision for the call is based on the parameters previously configured for **Call Routing Method** and **SIP URI** (**Section 5.3.5**) and the users **SIP Name** and **Contact**, already populated with the assigned Clearcom DID numbers (**Section 5.4**).

5.6.1. Incoming Call Route – Standard Tab

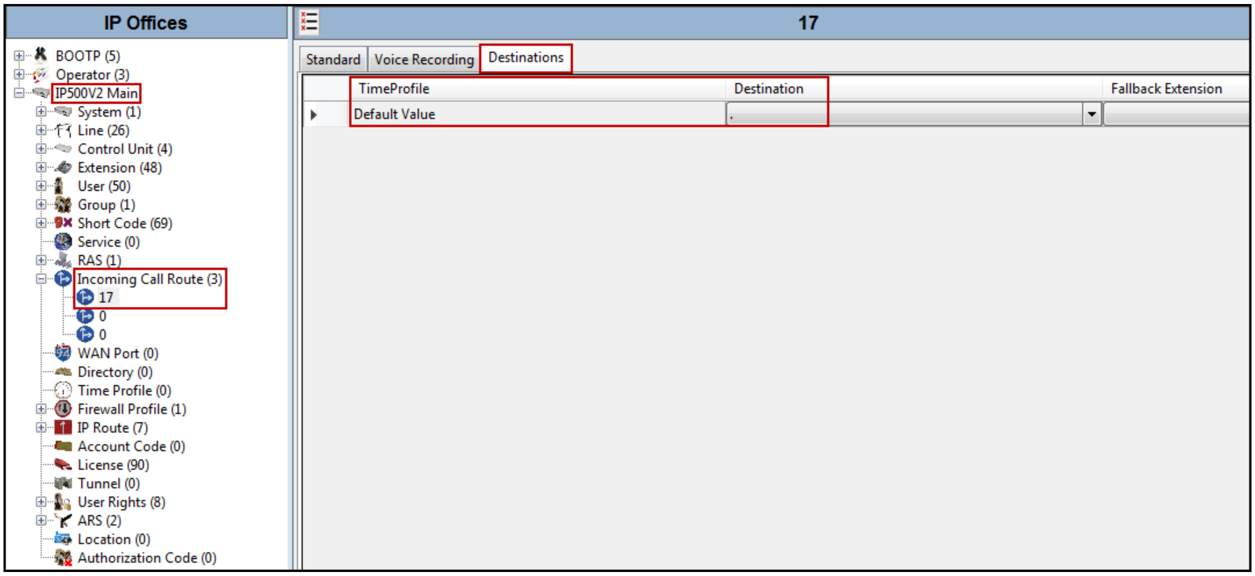
On the **Standard** tab of the **Details** pane, enter the parameters as shown below:

- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group ID** to the incoming line group of the SIP Line defined in **Section 5.3**, in this case **17** was used.
- Default values can be used for all other fields.



5.6.2. Incoming Call Route – Destinations Tab

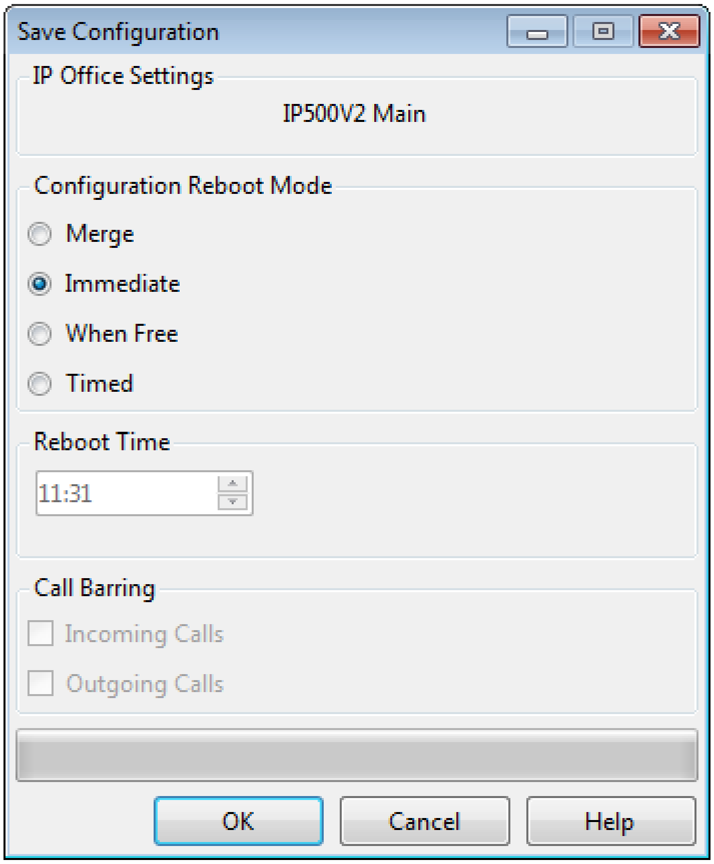
Under the **Destinations** tab, enter "**.**" for the **Default Value**. This setting will allow the call to be routed to any destination with a value on its **SIP Name** field, entered on the **SIP** tab of the **User**, which matches the number present on the user part of the "To" header on the incoming INVITE message received from Clearcom. Click **OK** to commit (not shown).



5.7. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections.

The following will appear, with either **Merge** or **Immediate** selected, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to proceed.



6. Clearcom SIP Trunking Service Configuration

To use Clearcom's SIP Trunking Service, a customer must request the service from Clearcom using the established sales processes. The process can be started by contacting Clearcom via the corporate web site at: http://www.clearcom.mx/ and requesting information.

During the signup process, Clearcom and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Clearcom's network.

Clearcom is responsible for the configuration of Clearcom SIP Trunking Service. The customer will need to provide the public IP address used to reach the IP Office at the enterprise. In the case of the compliance test, this is the public IP address of the IP Office WAN port (LAN2).

Clearcom will provide the customer the necessary information to configure Avaya IP Office and the Avaya SBCE following the steps discussed in the previous sections, including:

- SIP Trunk registration credentials (User Name, Password, etc.).
- Clearcom's Domain Name.
- DID numbers, etc.

7. Verification Steps

This section provides verification steps that may be performed to verify that the solution is configured properly.

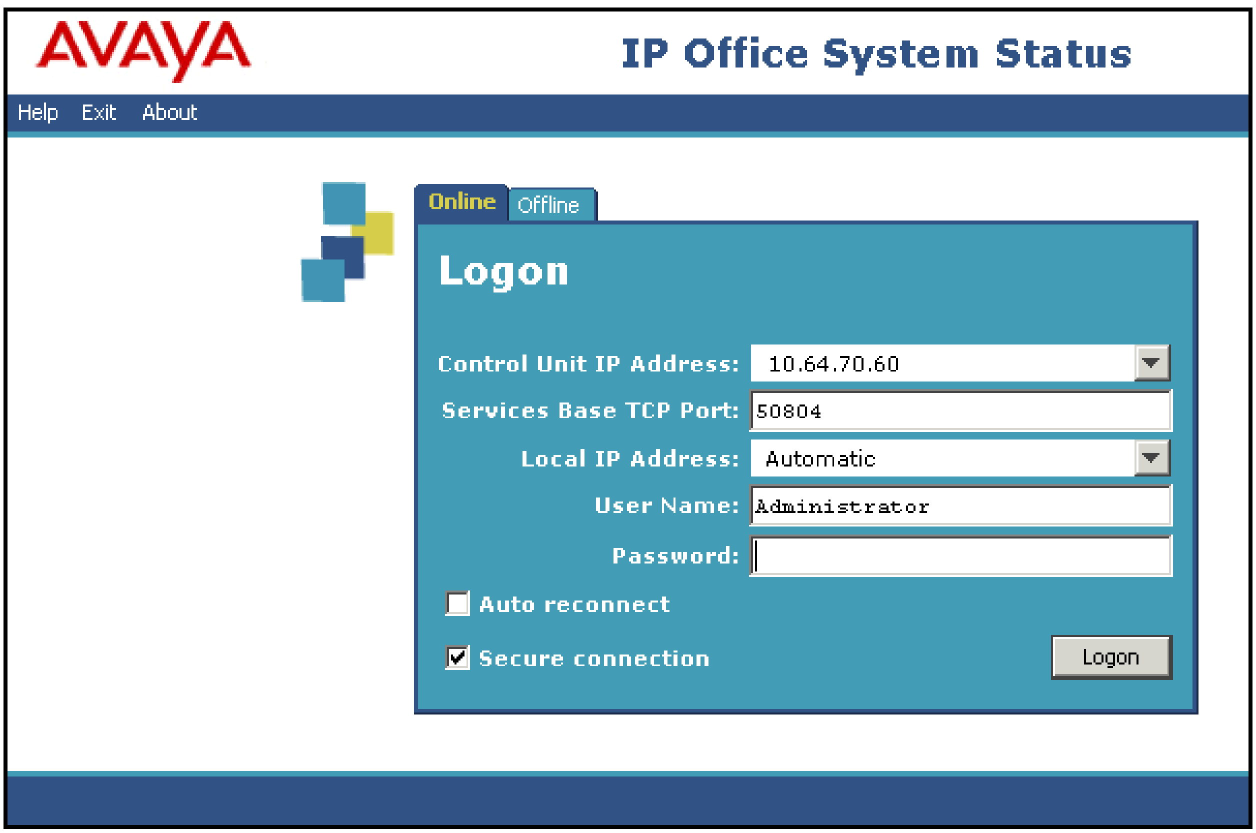
The following steps may be used to verify the configuration:

- Verify that endpoints at the enterprise site can place calls to the PSTN.
- Verify that endpoints at the enterprise site can receive calls from the PSTN.
- Verify that users at the PSTN can end active calls to endpoints at the enterprise by hanging up.
- Verify that endpoints at the enterprise can end active calls to PSTN users by hanging up.

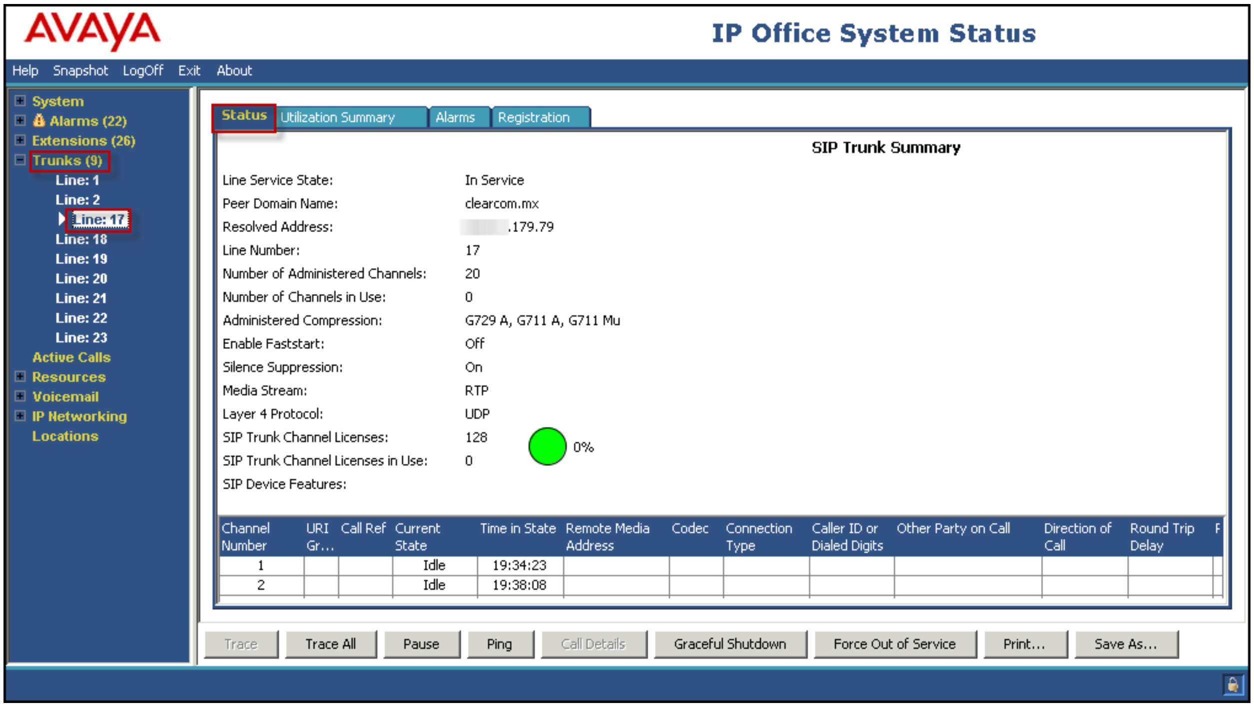
7.1. IP Office System Status

The following steps can also be used to verify the configuration.

Use the IP Office **System Status** application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed, log in with the proper credentials.

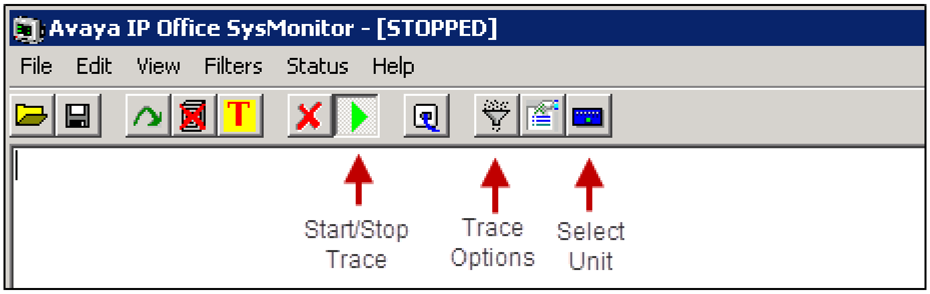


Select the SIP line under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** is **Idle** for each channel.

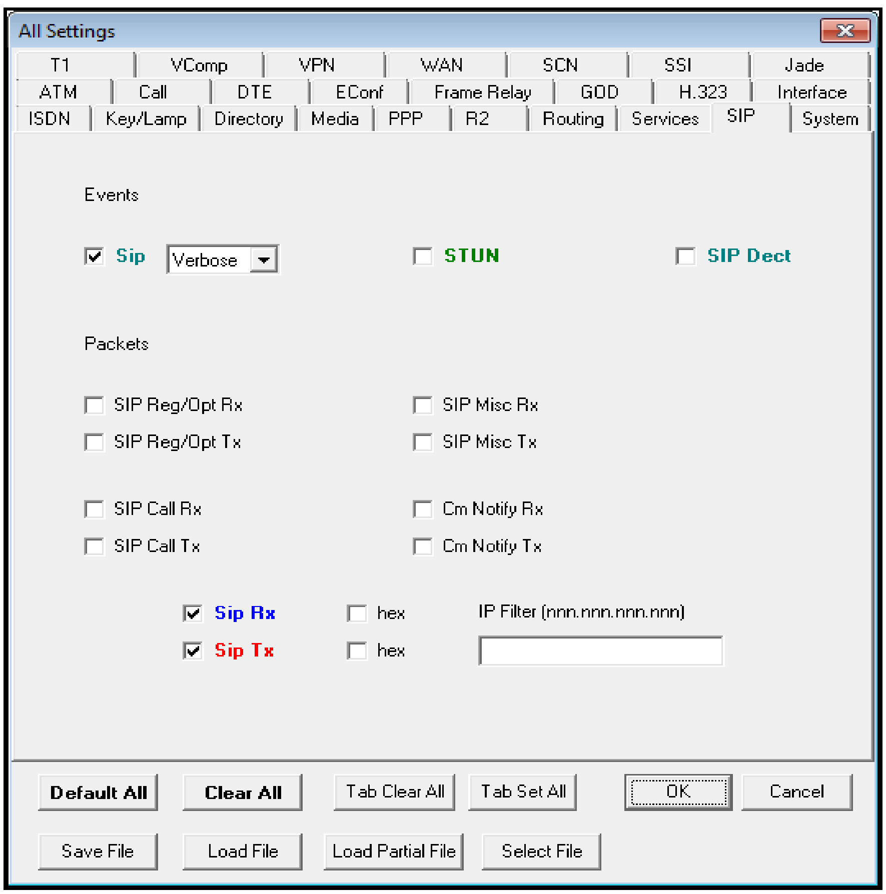


7.2. Monitor

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



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



8. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office Release 10.1 to Clearcom SIP Trunking Services. Clearcom SIP Trunking Services is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

9. Additional References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office, including the following, is available at: http://support.avaya.com/

[1] *Avaya IP Office Platform Solution Description, Release 10.1, Issue 1.2, September 2017*.
[2] *Avaya IP Office Platform Feature Description, Release 10.1, Issue 1a, September 2017*.
[3] *Deploying Avaya IP Office Platform IP500 V2, Document Number 15-601042, Issue 32m, January 22, 2017.*
[4] *Administering Avaya IP Office Platform with Manager, Release 10.1, Issue 14, July 2017*
[5] *Using Avaya Communicator for Windows on IP Office, Release 10, August 2016*.
[6] *Administering Avaya Communicator on IP Office, Release 10.0, Issue 01.01, August 2016.*
[7] *Avaya IP Office Platform Security Guidelines, Release 10. Issue 01e, May 8, 2017.*
[8] *IP Office Technical Bulletin number 175* (http://www.ipofficeinfo.com/TechBulletins/tb175.pdf)

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

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.