



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office Release 11.1 to support Telstra Enterprise 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 11.1 to support Telstra Enterprise SIP Trunking Service.

The Telstra Enterprise SIP Trunking Service offer referenced within these Application Notes provides customers with PSTN access via a SIP trunk between the enterprise and the service provider network. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly as an alternative to legacy analog or digital trunks. The Telstra Enterprise SIP Trunking Service provides you with a cost effective and flexible way to connect your business to the outside world. It helps your business use the internet bandwidth you already pay for in a more flexible way.

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 procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Telstra Enterprise SIP Trunking Service offering and a simulated Avaya enterprise solution. User Datagram Protocol (UDP) transport was used to connect the simulated enterprise solution to the Telstra Enterprise SIP Trunking Service offering (public side network side).

In the configuration used during the testing, the Avaya SIP-enabled enterprise solution consists of an Avaya IP Office Server Edition, two Avaya IP Office 500 V2 as expansion systems running software release 11.1 (hereafter referred to as IP Office) and various Avaya endpoints, listed in **Section 4**.

The Telstra Enterprise 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”, “Telstra” or “Telstra Enterprise” 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 Telstra’s network via the public Internet, as depicted in **Figure 1**, and exercise the features and functionalities listed in **Section 2.1**.

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

For the testing associated with this Application Note, the interface between the simulated enterprise site (private network) and the Telstra network (public network) did not include the use of any specific encryption features, UDP/RTP was used.

Encryption (TLS/sRTP) was used internal to the enterprise between Avaya products wherever possible.

2.1. Interoperability Compliance Testing

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

- Public DNS record queries to establish the SIP trunk connections.
- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, Digital and Analog 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, Digital and Analog 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 Workplace Client for Windows (SIP).
- Dialing plans including local calls, outbound toll-free, etc.
- Caller ID presentation.
- Privacy (blocking calling party number).
- 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.711ALAW, G.711ULAW and G.729A, Telstra preferred codec order.
- Proper response to no matching codecs.
- Proper early media transmissions.
- DTMF tone support using RFC 2833.
- 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.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- SIP REFER method for call re-direction from the enterprise to the PSTN.

Items that were not tested includes the following:

- 0, 0+10 digits, 411, 911 (Emergency) and international calls were not tested.
- G.711 pass-through fax is supported but was not tested.
- T.38 fax is not currently supported by Telstra.

2.2. Test Results

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

- **Outbound Calling Party Number (CPN) Block** – When the IP Office user activated “Withhold Number” to enable user privacy on outbound calls, IP Office sent “anonymous” in the “From” header, included the “Privacy: id” header, while the caller information (DID number) was included in the “P-Asserted-Identity” header of the outbound INVITE message. Telstra did not respond to the INVITE message sent by IP Office with “anonymous” in the “From” header, resulting on the call failing. Telstra requires a valid DID number in the “From” header, these DID numbers are provided by Telstra. This issue was resolved by enabling the “Send From In Clear” field under the SIP Line, Advanced tab (**Section 5.4.7**).
- **Disable “P Asserted ID” on the SIP Line “Call Details”** – For call forward and twinned calls to the PSTN the call id displayed at the terminating PSTN station was of the DID number assigned to the IP Office station with call forward or the mobility feature active, instead of the calling PSTN number. The workaround to display the calling PSTN number is to disable “P Asserted ID” under “Call Details” on the SIP Line being used.
- **SIP OPTIONS Messages** – During the compliance test Telstra did not send SIP OPTIONS messages to IP Office, IP Office did send SIP OPTIONS messages to Telstra, this was sufficient to keep the SIP trunk up in service.
- **SIP endpoints may indicate that a transfer failed even when it is successful** – Occasionally on a transfer operation, Avaya IP Office SIP endpoints (Avaya 1100 Series Deskphones) may indicate on the local call display that the transfer failed even though it was successful. The frequency of this behavior can be reduced by enabling “Emulate Notify for REFER” on the IP Office SIP Line (**Section 5.4.7**).
- **Telstra does not support REFER for call forward** – Telstra supports REFER for call transfers to the PSTN but does not support REFER for call forward to the PSTN. The call scenario in which Telstra does not support REFER is for inbound calls from the PSTN to IP Office which are then forwarded to another PSTN endpoint. In this scenario, if REFER is enabled (**Section 5.4.2**), Telstra responds with a “403 Forbidden” message in response to the REFER message sent by IP Office. The “403 Forbidden” response does not have any user impact; it’s simply ignored by IP Office (the call does not drop). This issue was solved by enabling “No REFER if using Diversion” on the IP Office SIP Line, which resulted in IP Office sending REFER during call transfers to the PSTN and not send it during call forwards to the PSTN (**Section 5.4.7**).

2.3. Support

For information on Telstra Enterprise SIP Trunking Service go to:

<https://www.telstra.com.au/>

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 compliance testing. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Telstra Enterprise SIP Trunking Service through the public Internet.

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

- IP Office Server Edition running in VMware environment.
 - Avaya IP Office Voicemail Pro.
- Two Avaya IP Office 500 V2 as expansion systems.
- Avaya J179 IP Deskphones (H.323).
- Avaya 1100 Series IP Deskphones (SIP).
- Avaya J129 IP Deskphones (SIP).
- Avaya 1400 Series Digital Deskphones.
- Analog Deskphones.
- Avaya Workplace Client for Windows (SIP).

Avaya IP Office provides the voice communications services for the enterprise. In the reference configuration, Avaya IP Office runs on the Avaya IP Office Server Edition platform. Note that this solution is extensible to deployments using the standalone IP500 V2 platform as well.

In the sample configuration, the Primary server runs the Avaya IP Office Server Edition Linux software. Avaya Voicemail Pro runs as a service on the Primary Server. The LAN1 port of the Primary Server is connected to the enterprise LAN. The LAN2 port was used to connect to the public network.

The Expansion Systems (IP500 V2) were used for the support of digital, analog and additional IP stations. The Avaya IP Office 500 V2s are equipped with analog and digital extension expansion modules, as well as a VCM64 (Voice Compression Module). The LAN1 port of the Avaya IP Office IP500 V2 expansion systems was connected to the enterprise LAN, the LAN2 port was not used.

IP endpoints at the enterprise included Avaya 1100 Series IP Deskphones (with SIP firmware), Avaya J100 Series IP Deskphones (with SIP and H.323 firmware), Avaya Workplace Client for Windows (SIP), Avaya Digital and Analog Deskphones. IP endpoints were registered to the Primary Server; non-IP endpoints (analog and digital) were registered to the Expansion Systems. The site also has a Windows PC running Avaya IP Office Manager to configure and administer the system. 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.

The transport protocols on the SIP trunk between IP Office and the Telstra network, across the public Internet, is UDP for signaling and RTP for media. The transport protocol between Avaya components inside the enterprise private IP network (LAN) is TLS for signaling and SRTP for media.

For the compliance test, users dialed a short code of 9 + N digits to make calls across the SIP trunk to the Telstra network. The short code 9 was stripped off by Avaya IP Office, but the remaining N digits were sent unaltered to the Telstra network.

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.

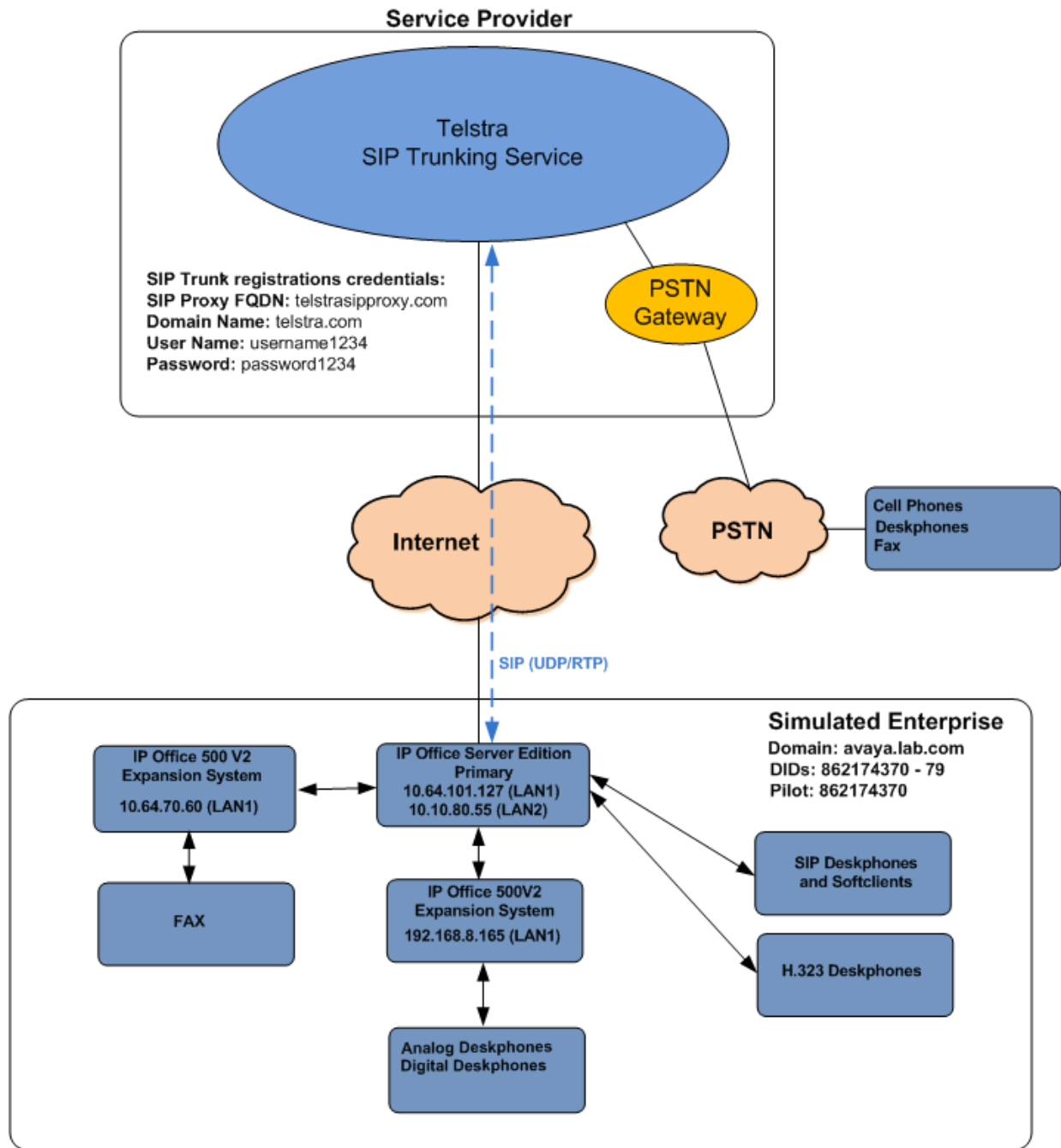


Figure 1: Avaya simulated enterprise site connected to the Telstra Enterprise SIP Trunking Service offering

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 Server Edition (Primary Server)	11.1.2.2.0 Build 20
• Avaya IP Office Voicemail Pro	11.1.2.2.0 Build 8
Avaya IP Office IP500 V2 (Expansion Systems)	11.1.2.2.0 Build 20
Avaya IP Office Manager	11.1.2.2.0 Build 20
Avaya J179 IP Telephone (H.323)	6.8304
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.7.0.7
Avaya 1408 Digital Telephone	48.02
Avaya Workplace Client for Windows (SIP)	3.24.0.84
Analog Telephone	---
Telstra	
BroadSoft	R23

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. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints.

5. Avaya IP Office Primary Server Configuration

Avaya IP Office is configured through the Avaya IP Office Manager application. From the PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the Manager application. Log in using the appropriate credentials.

Select IP Office

Name	IP Address	Type	Version	Edition
Server Edition 11.1				
<input checked="" type="checkbox"/> IPOSE-Primary	10.64.101.127	IPO-Linux-PC	11.1.2.2.0 build 20	Server (Primary) Select

Configuration Service User Login

IP Office: IPOSE-Primary (Primary System - IPO-Linux-PC)

Service User Name:

Service User Password:

TCP Discovery Progress

Unit/Broadcast Address

On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the “plus” sign next to the Primary server system name, e.g., **IPOSE-Primary**, on the navigation pane will expand the menu on this server.

Configuration

- BOOTP (3)
- Operator (3)
- Solution
 - User (32)
 - Group (2)
 - Short Code (48)
 - Directory (0)
 - Time Profile (0)
 - Account Code (0)
 - User Rights (9)
 - Location (1)
 - IPOSE-Primary
 - IP500V2-One
 - IP500V2-Two

Server Edition

Summary

Server Edition Primary

Hardware Installed

- Control Unit: IPO-Linux-PC
- Secondary Server: NONE
- Expansion Systems: 10.64.70.60; 192.168.8.165
- System Identification: 8de6c6d337bc354d6ec88494533af87bb2d6e950

System Settings

- IP Address: 10.64.101.127
- Sub-Net Mask: 255.255.255.0
- System Locale: United States (US English)
- System Location: 3: Thornton, CO
- Device ID: NONE
- Number of Extensions on System: 6

Open...

- Configuration
- System Status
- Voicemail Administration
- Resiliency Administration
- On-boarding
- IP Office Web Manager
- Help
- Set All Nodes License Source

Add...

- Secondary Server
- Expansion System

Link...

- Expansion System

Description	Name	Address	Primary Link	Secondary Link	Users Configured	Extensions Configured
Solution					32	54
Primary Server	IPOSE-Primary	10.64.101.127			6	6
Expansion System	IP500V2-One	192.168.8.165	Bothway		25	24
Expansion System	IP500V2-Two	10.64.70.60	Bothway		1	24

Ready

On Server Edition systems, the numbers of licenses to be assigned to the specific Server or Expansion Systems are reserved from the total pool of licenses present on the license server. On the screen below, **10 SIP Trunk Sessions** licenses were reserved to be used by the Primary Server.

Configuration

- BOOTP (4)
- Operator (3)
- Solution
 - User(32)
 - Group(2)
 - Short Code(48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - System (1)
 - IPOSE-Primary
 - Line (3)
 - Control Unit (8)
 - Extension (6)
 - User (7)
 - Group (0)
 - Short Code (2)
 - Service (0)
 - Incoming Call Route (4)
 - IP Route (3)
 - License (6)
 - ARS (1)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-One
 - IP500V2-Two

License Remote Server

Remote Server Configuration

License SourceWebLM
Domain Name (URL)10.64.101.127
PathWebLM/LicenseServer
Port Number52233
WebLM Client ID
WebLM Node ID-IPOSE-Primary

Reserved Licenses

SIP Trunk Sessions	10	Server Edition	1
SM Trunk Sessions	0	Avaya IP Endpoints	6
Voicemail Pro Ports	2	3rd Party IP Endpoints	0
VMPro Recordings Administrators	0	Receptionist	0
VMPro TTS Professional	0	Basic User	5
CTI Link Pro	0	Office Worker	0
UMS Web Services	0	Power User	1
Mac Softphones	0	Avaya Softphone	0
Avaya Contact Center Select	0	Web Collaboration	0
VM Media Manager	0		

5.2. System Settings

Configure the necessary system settings. 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).

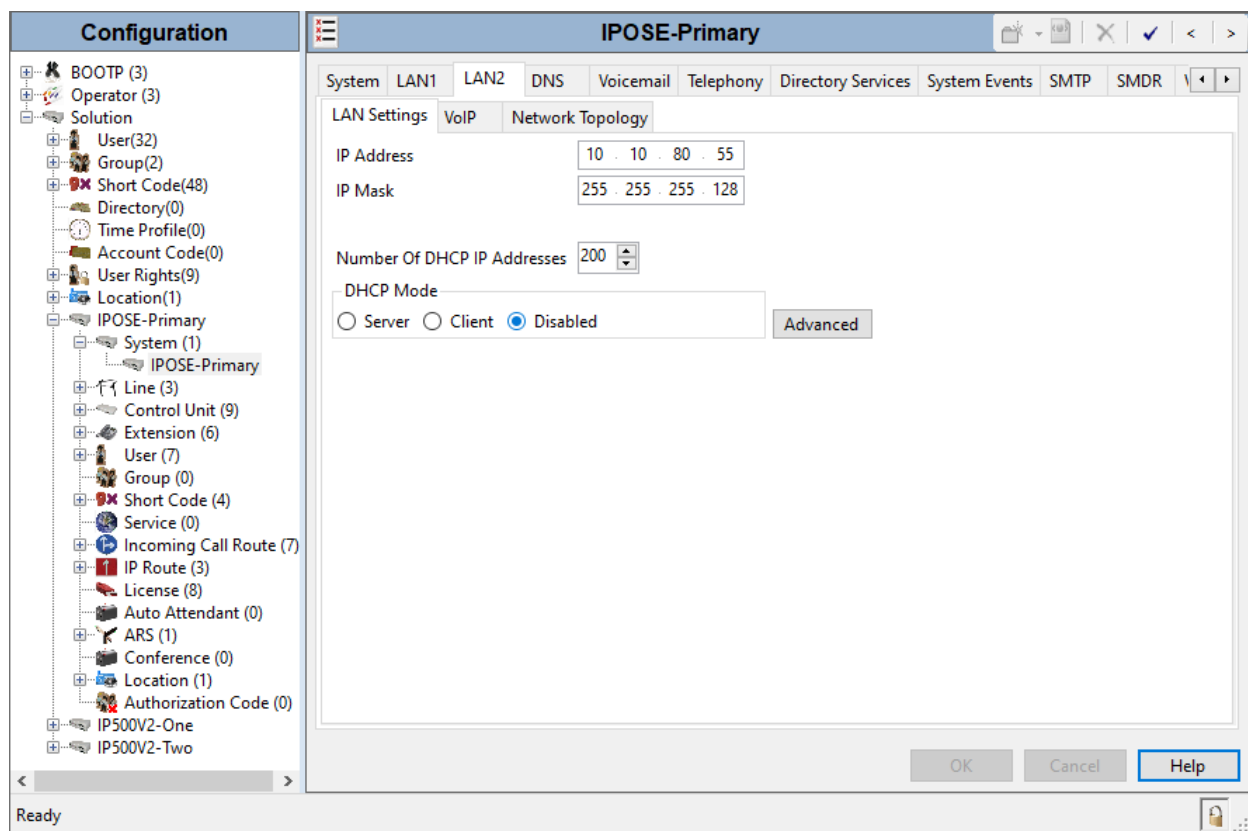
5.2.1. System – LAN2 Tab

In the sample configuration, the LAN2 interface is used for the SIP trunk connection to the Telstra network.

5.2.1.1 LAN2 – LAN Settings Tab

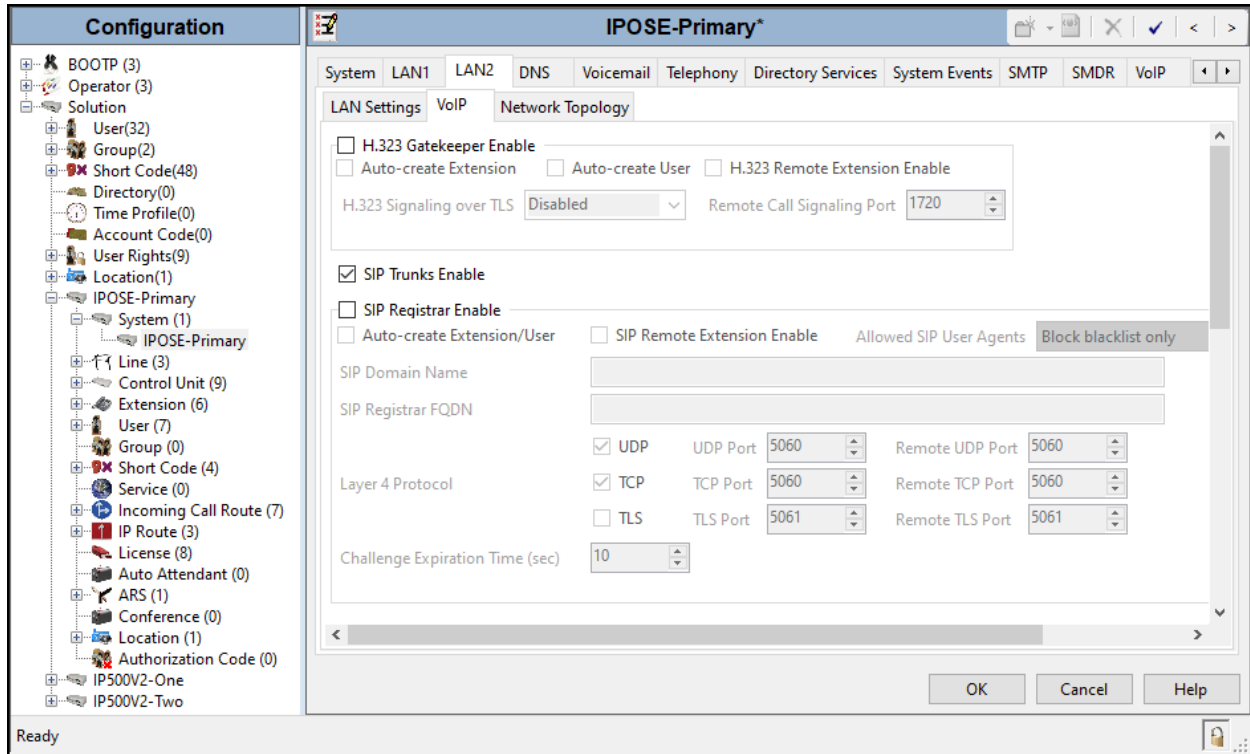
To view or configure the LAN2 IP address and subnet mask, select the **LAN2→ LAN Settings** tab, and enter the information as needed, according to the customer network requirements:

- **IP Address: 10.10.80.55** was used in the reference configuration, this is the public IP address assigned to IP Office.
- **IP Mask: 255.255.255.128** was used in the reference configuration.
- Other parameters on this screen are set to the defaults.



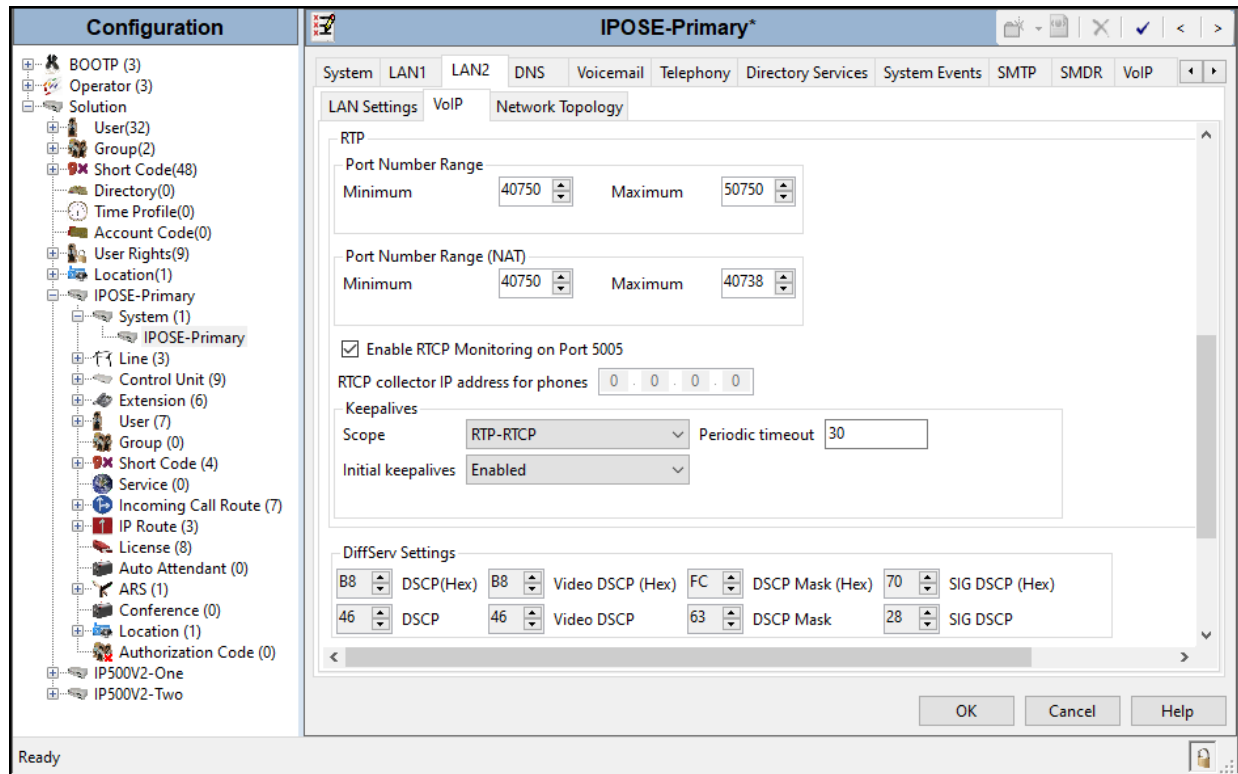
5.2.1.2 LAN2 – VoIP Tab

- Select the **LAN2 → VoIP** tab in the Details Pane. Check the **SIP Trunks Enable** box to allow the configuration of SIP trunks. Since no SIP endpoints are to register on this interface, leave the **SIP Registrar Enable** box unchecked.



Scroll down the page:

- Verify the **RTP Port Number Range**. Based on this setting, Avaya IP Office will request RTP media to be sent to a UDP port in the configurable range for calls using LAN2. The **Minimum** and **Maximum** port numbers were kept at their default values in the reference configuration.
- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. This is done to prevent possible issues with network firewalls closing idle RTP channels.
- In the **DiffServ Settings** section, IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services (QoS) policies for both signaling and media. The **DSCP** field is the value used for media, while the **SIG DSCP** is the value used for signaling. These settings should be set according to the customer's QoS policies in place. The default values used during the compliance test are shown.
- Click **OK** to commit.

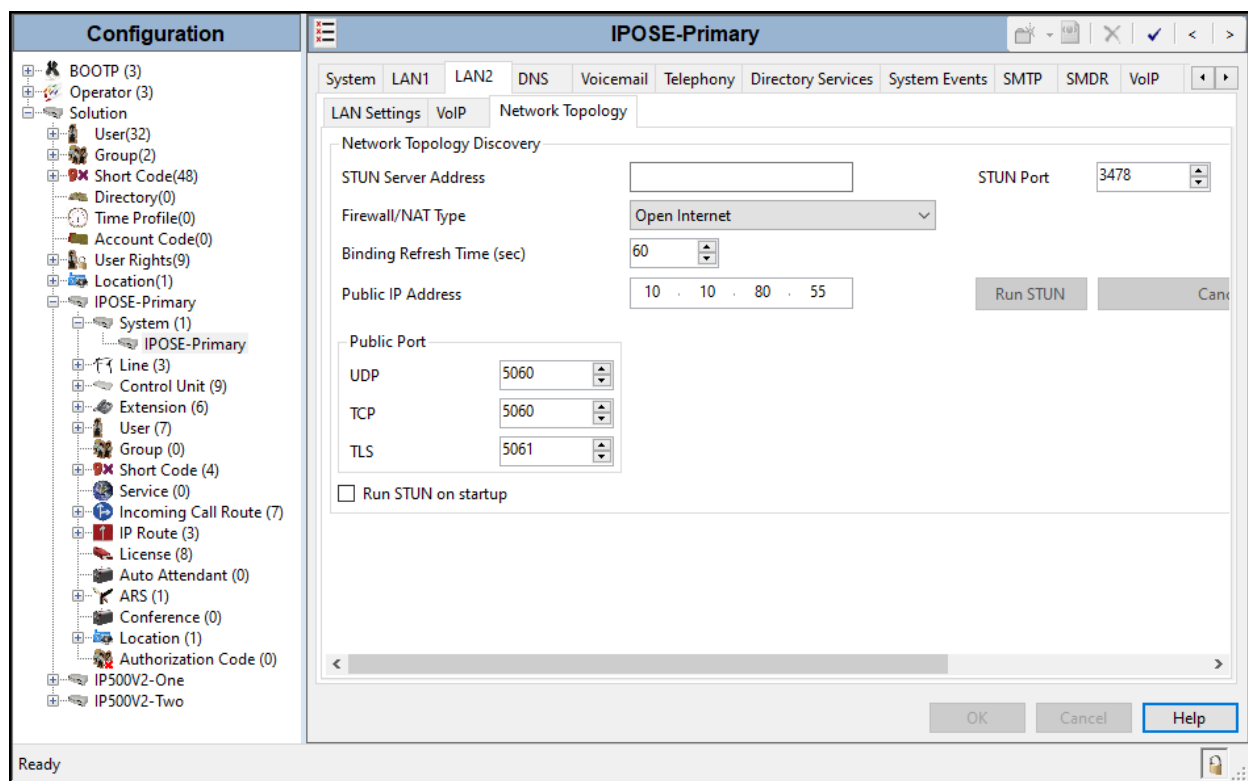


Note: In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network (private network). The LAN1 interface configuration is not directly relevant to the interface with the Telstra Enterprise SIP Trunking Service, and therefore is not described in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

5.2.1.3 LAN2 – Network Topology Tab

On the **LAN2 Network Topology** tab in the Details pane, set the following:

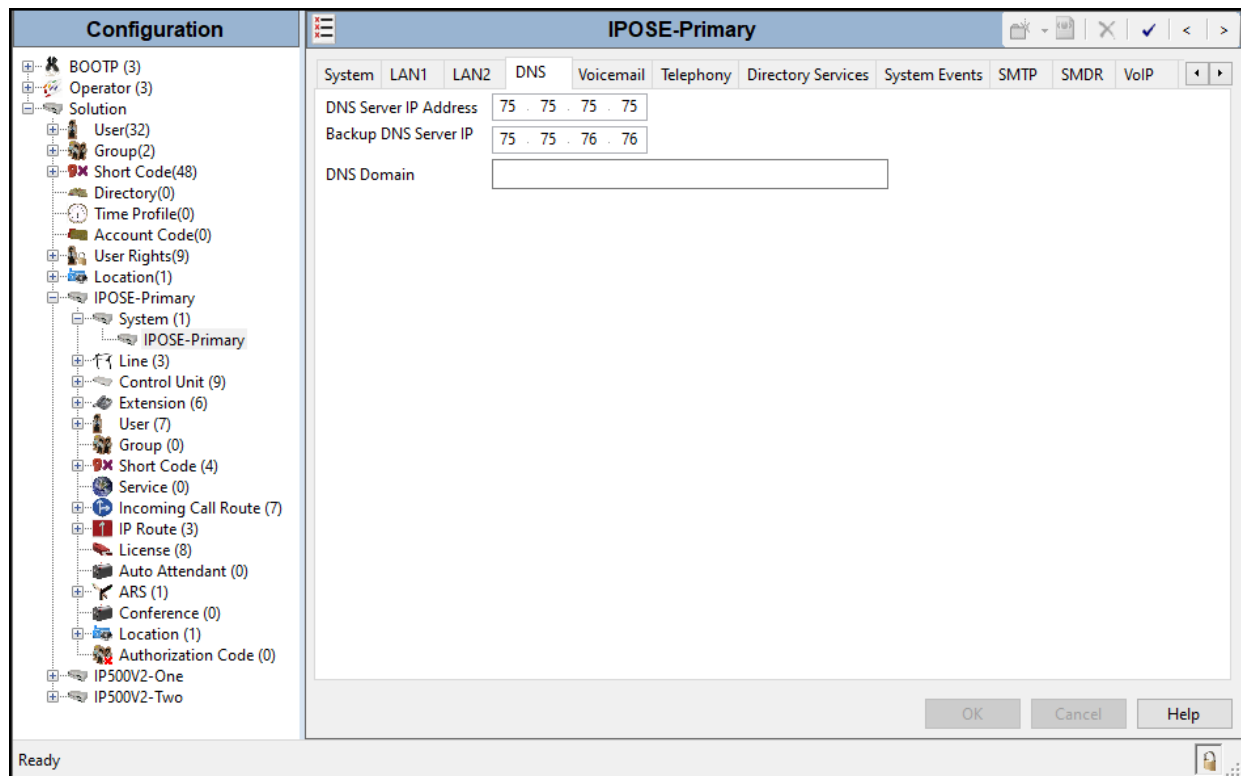
- Select the **Firewall/NAT Type** from the pull-down menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used.
- Set **Binding Refresh Time (seconds)** to **60**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider.
- Set **Public IP Address** to the same public IP address assigned to the Avaya IP Office LAN2.
- Set **Public Port / UDP** to **5060**.
- Default values were used for all other parameters.
- Click the **OK** button.



5.2.2. System – DNS Tab

Public DNS servers IP addresses are required to be configured; IP Office will retrieve the Telstra Proxy IP Addresses via public DNS queries using the ISTP Domain Name configured under in **Section 5.4.2**. To access the System DNS settings, navigate to the **DNS** tab in the **Details** pane, configure the following parameters:

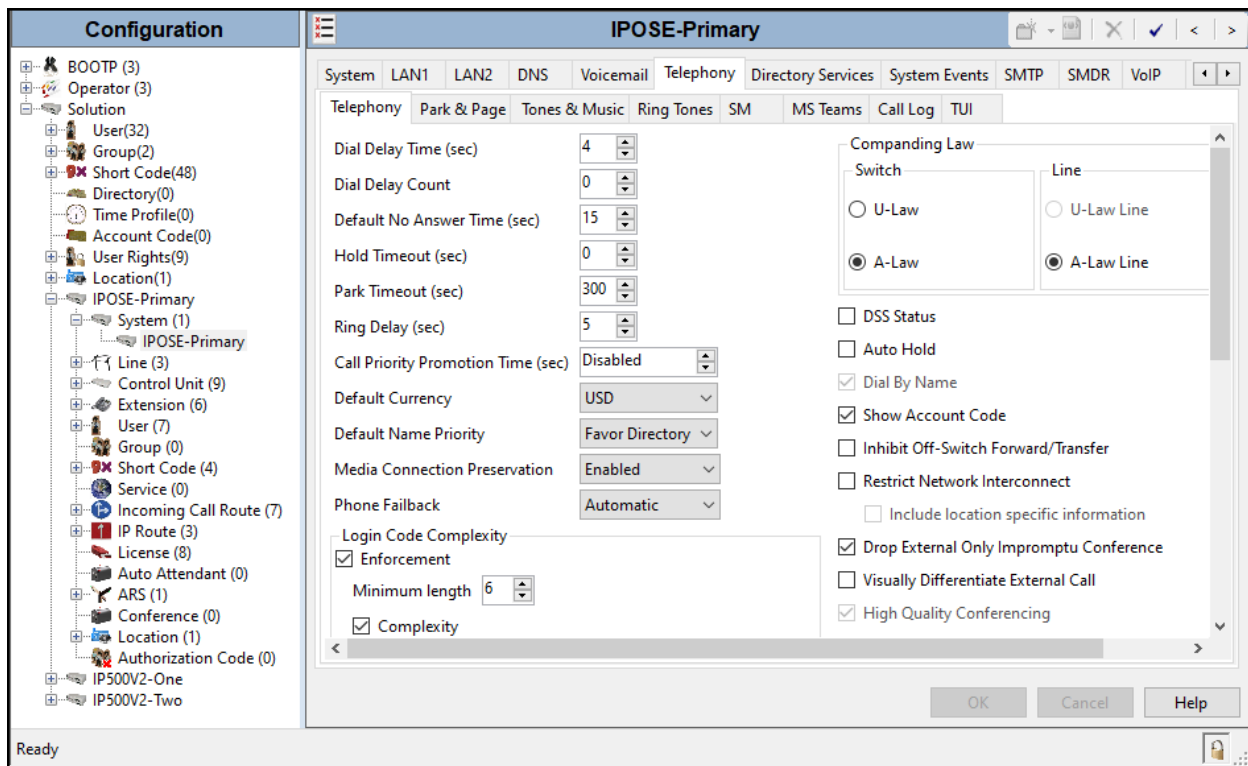
- Under DNS Server IP Address and Backup DNS Server IP Address enter the primary and backup public DNS servers IP addresses. These IP addresses should be provided by Telstra.
- Click **OK** to commit.



5.2.3. 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; **A-Law** was used for the compliance test.
- 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.



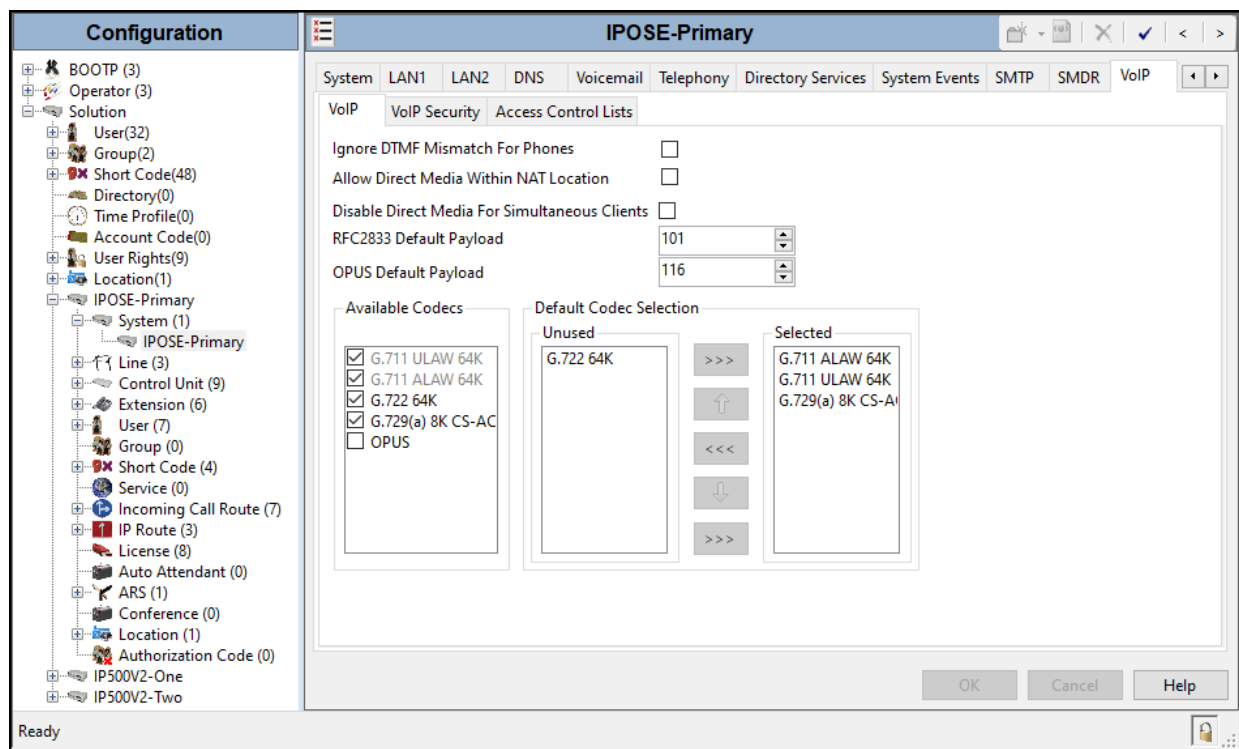
5.2.4. System – VoIP Tab

Navigate to the **VoIP** tab in the Details pane to view or change the system codecs and VoIP security settings.

5.2.4.1 VoIP – VoIP Tab

Select the **VoIP → VoIP** tab, 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).
- Click **OK** to commit.



Note: The codec selections defined under this section (VoIP – VoIP Tab) are the codecs selected for the IP phones/extensions. The codec selections defined under **Section 5.4.6** (SIP Line – VoIP tab) are the codecs selected for the SIP Line (Trunk).

5.2.4.2 VoIP – VoIP Security Tab

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

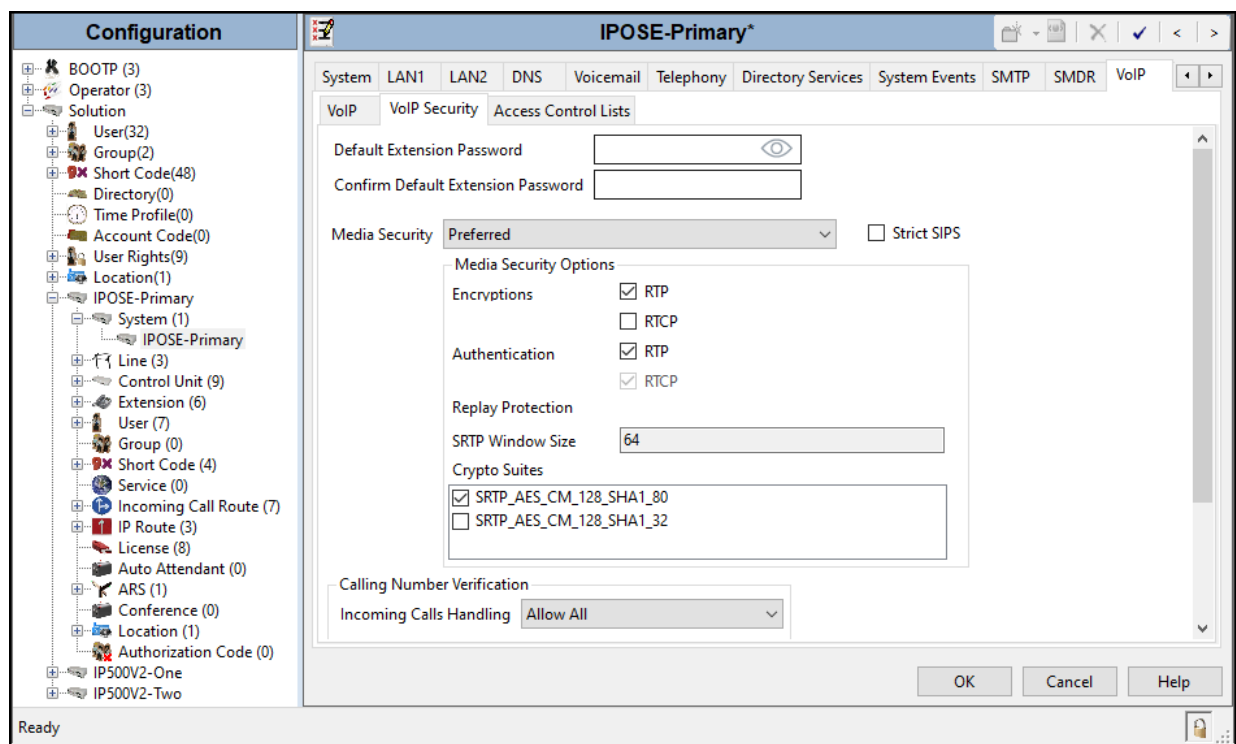
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- Disabled (default).
- Preferred.
- Enforced.

When enabling SRTP on the system, the recommended setting is **Preferred**. In this scenario, IP Office uses SRTP if supported by the far-end, otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the far-end, the call is not established.

To configure the use of SRTP, select the **VoIP → VoIP Security** tab on the Details pane.

- Set the **Media Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.
- Verify **Strict SIPS** is not checked.
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields.
- Under **Crypto Suites**, select **SRTP_AES_CM_128_SHA1_80**.
- Click **OK** to commit.

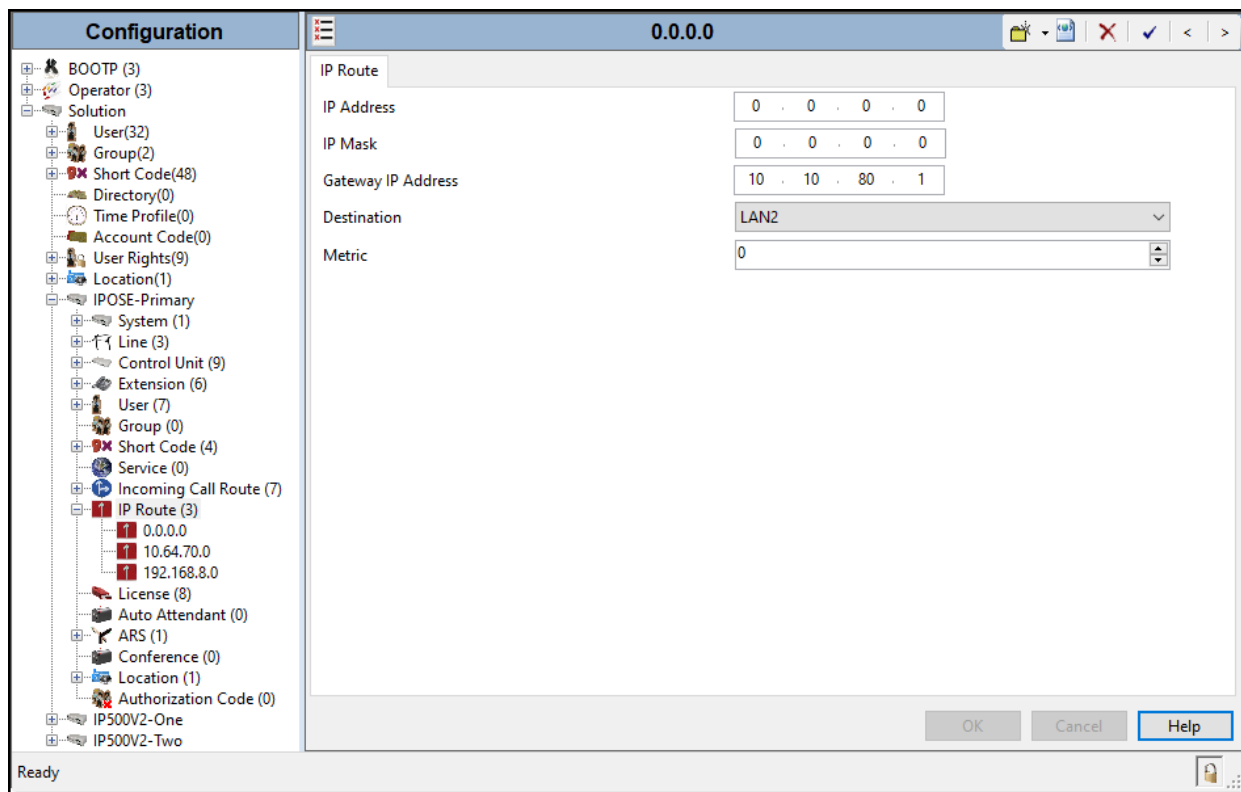


5.3. IP Route

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 the Telstra 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.



5.4. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Telstra network. 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 5.4.1** 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 5.4.2** to **5.4.7**.

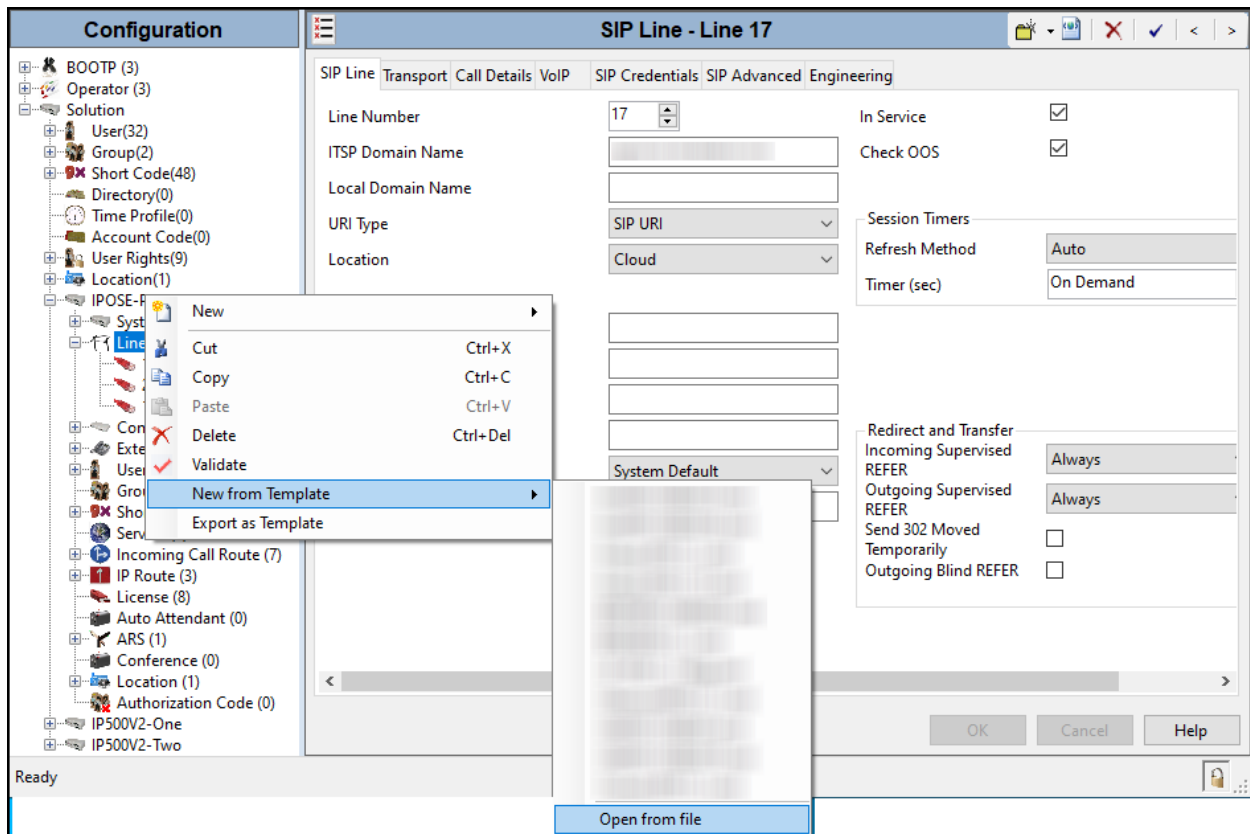
Alternatively, a SIP Line can be created manually. To do so, right-click on **Line** in the **Navigation** pane and select **New → SIP Line**. Then, follow the steps outlined in **Sections 5.4.2** to **5.4.7**.

5.4.1. Creating a SIP Trunk from an XML Template

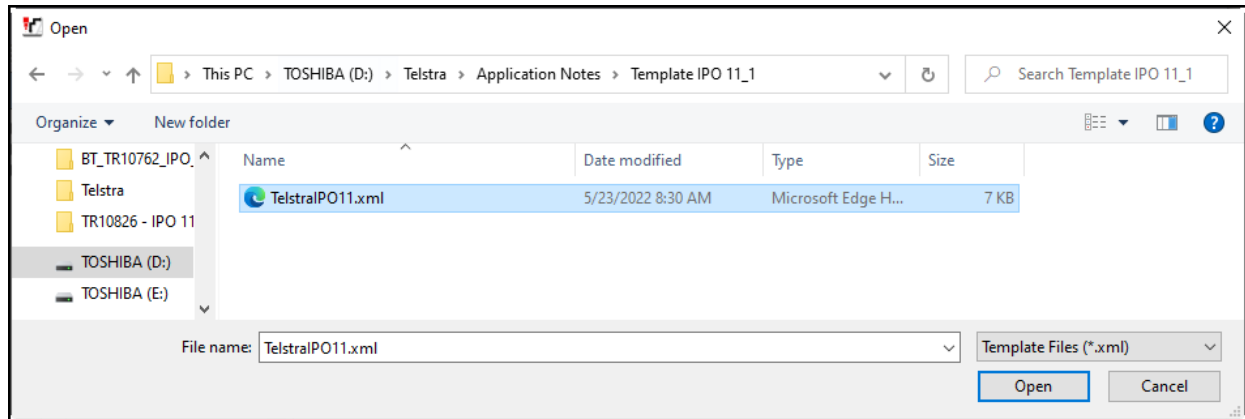
SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition 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.

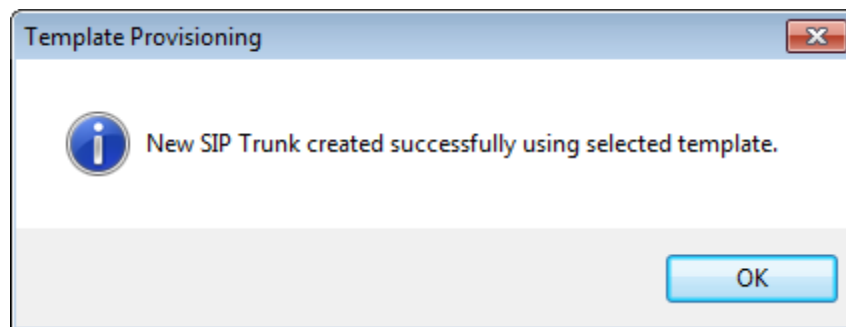
To create the SIP Trunk from the template, from the **Primary** server (**IPOSE-Primary**), right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template → Open from file**.



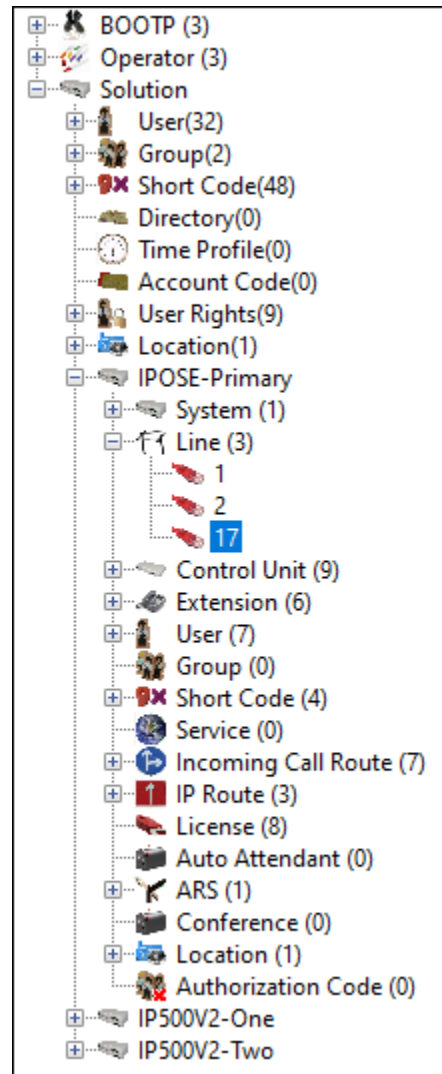
Navigate to the directory on the local machine where the template was copied and select the template.



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 5.4.2 to 5.4.7**.

5.4.2. 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 **Telstra.com**, the domain name provided by Telstra. **Note:** The Domain Name shown here and throughout this document has been masked for confidentiality and privacy purposes. Set the ITSP Domain Name to the domain name provided by Telstra instead of the domain shown here.
- 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**.
- Set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Always**.
- Click **OK** to commit.

The screenshot shows the 'SIP Line - Line 17' configuration window. The left pane displays a tree view of the system configuration, including BOOTP, Operator, Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, System, Line, Control Unit, Extension, User, Group, Short Code, Service, Incoming Call Route, IP Route, License, Auto Attendant, ARS, Conference, Location, Authorization Code, and IP500V2-One/Two. The right pane shows the 'SIP Line' tab with the following settings:

Parameter	Value	Parameter	Value
Line Number	17	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name	telstra.com	Check OOS	<input checked="" type="checkbox"/>
Local Domain Name		Session Timers	
URI Type	SIP URI	Refresh Method	Auto
Location	Cloud	Timer (sec)	On Demand
Prefix		Redirect and Transfer	
National Prefix		Incoming Supervised REFER	Always
International Prefix		Outgoing Supervised REFER	Always
Country Code		Send 302 Moved Temporarily	<input type="checkbox"/>
Name Priority	System Default	Outgoing Blind REFER	<input type="checkbox"/>
Description	Service Provider		

At the bottom of the window are buttons for OK, Cancel, and Help.

5.4.3. SIP Line – Transport Tab

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

- Set the **ITSP Proxy Address** to **telstrasipproxy.com**, the ITSP Proxy Address provided by Telstra. **Note:** The ITSP Proxy Address shown here and throughout this document has been masked for confidentiality and privacy purposes. Set the ITSP Proxy Address to the SIP proxy name provided by Telstra instead of the name shown here.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Use Network Topology Info** to **None** (refer to the note below).
- Set the **Send Port** and **Listen Port** to **5060**.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

The screenshot displays the Avaya SIP Line configuration window. On the left is a 'Configuration' tree showing a hierarchy of system components, with 'Line (3)' expanded to show 'Line 17' selected. The main panel is titled 'SIP Line - Line 17' and contains several tabs: 'SIP Line', 'Transport' (which is active), 'Call Details', 'VoIP', 'SIP Credentials', 'SIP Advanced', and 'Engineering'. The 'Transport' tab shows the following settings:

- ITSP Proxy Address:** telstrasipproxy.com
- Network Configuration:**
 - Layer 4 Protocol:** UDP (selected from a dropdown)
 - Send Port:** 5060
 - Use Network Topology Info:** None (selected from a dropdown)
 - Listen Port:** 5060
- Explicit DNS Server(s):** Two input fields, both containing '0 . 0 . 0 . 0'.
- Calls Route via Registrar:** ☒
- Separate Registrar:** An empty text input field.

The status bar at the bottom left of the window indicates 'Ready'.

Note – For the compliance testing, the **Use Network Topology Info** field was set to **None**, since no NAT was used in the test configuration. 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.

5.4.4. 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**, enter the pilot number provided by Telstra, the pilot number is used as part of the registration credentials.
- For **Authentication Name** enter the username credential provided by Telstra for SIP Trunk registration.
- Leave **Contact** blank.
- For **Password** and **Confirm Password**, enter the password credential provided by Telstra for SIP Trunk registration.
- Set **Expiry (mins)** to a value acceptable to the enterprise. This setting defines how often registration with Telstra is required following any previous registration. For the compliance test **60** minutes was used. This value should be chosen in consultation with the service provider.
- Verify **Registration required** was checked. When selected, the credentials fields above are included in the SIP INVITE messages sent to Telstra when making calls, required by Telstra.

The screenshot shows the Avaya IP Office Configuration window. On the left is a tree view of the configuration hierarchy. The main window is titled 'SIP Line - Line 17' and has several tabs: SIP Line, Transport, Call Details, VoIP, SIP Credentials (selected), SIP Advanced, and Engineering. The 'SIP Credentials' tab contains a table with the following data:

Index	User Name	Authentication Name	Contact	Expiration (mins)	Register
1	862174370	user1234		60	True

Below the table is the 'Edit SIP Credentials' form with the following fields:

- User name: 862174370
- Authentication Name: user1234
- Contact: (empty)
- Password: (masked with dots)
- Confirm Password: (masked with dots)
- Expiration (mins): 60
- Registration required: ☒

Buttons for 'Add...', 'Remove', and 'Edit...' are on the right. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

5.4.5. SIP Line – Call Details Tab

Select the **Call Details** tab, and then click the **Add...** button (not shown) and the screen shown below will appear. To edit an existing entry, click an entry in the list at the top, and click the **Edit...** button. In the example screen below a new entry was created with the parameters shown below:

- Associate this line with an incoming line group by entering a line group number in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new incoming and outgoing group **17** was defined that only contains this line (line 17).
- Under **Credentials**, select **1: 862174370** from the pull-down menu (this field will default to the **User Name** used under the **SIP Credentials** tab in **Section 5.4.4**).
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Verify **P Asserted ID** is unchecked (refer to **Section 2.2**).
- Verify **Diversion Header** is checked.
- Set the **Local URI**, **Contact** and **Diversion Header** fields to the values shown in the screenshot below.
- Set all remaining fields as shown on the screenshot below.
- Click **OK**.

SIP Line - 17 | Call Details | SIP URI

New URI

Incoming Group: 17 Max Sessions: 10

Outgoing Group: 17

Credentials: 1: 862174370

	Display	Content
Local URI	Auto	Auto
Contact	Auto	Auto
P Asserted ID	<input type="checkbox"/> None	None
P Preferred ID	<input type="checkbox"/> None	None
Diversion Header	<input checked="" type="checkbox"/> Auto	Auto
Remote Party ID	<input type="checkbox"/> None	None

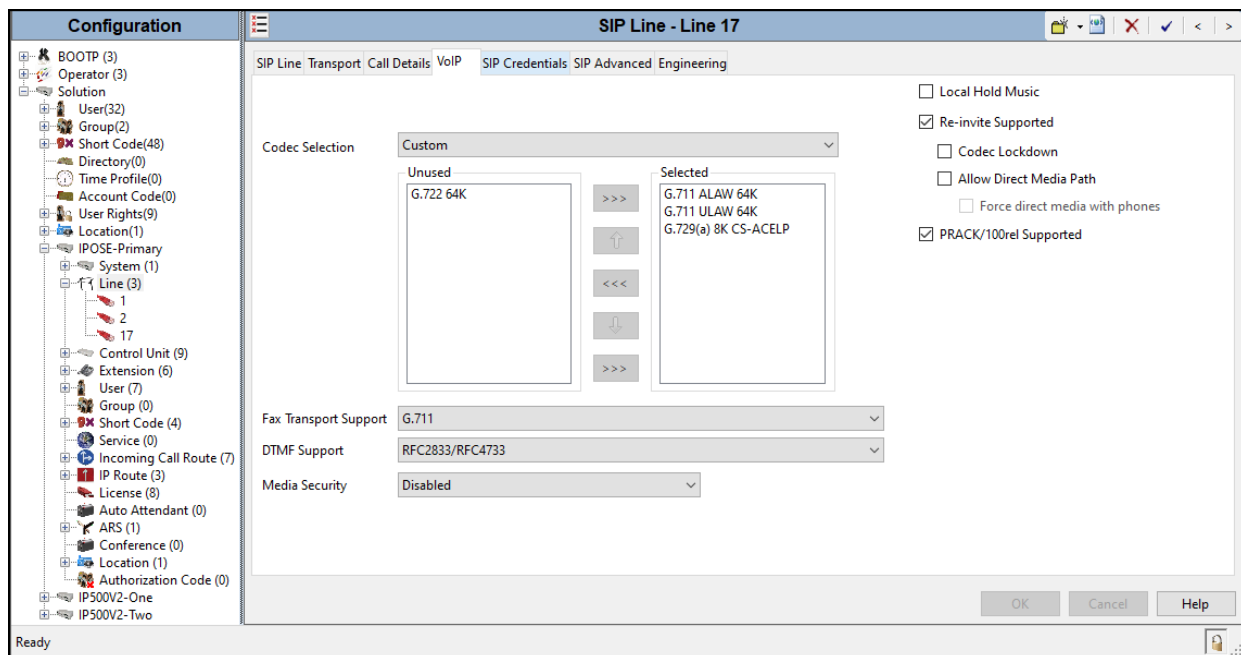
Field meaning		
Outgoing Calls	Forwarding/Twinning	Incoming Calls
Caller	Original Caller	Called
Caller	Original Caller	Called
None	None	None
None	None	None
None	Caller	None
None	None	None

OK Cancel Help

5.4.6. 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. Telstra supports codecs **G.711ALAW**, **G.711ULAW** and **G.729(a)** for audio.
- Select **G.711** for **Fax Transport Support** (refer to **Section 2.1**).
- Set the **DTMF Support** field to **RFC2833/RFC4733**. 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.



Note: The codec selections defined under this section are the codecs selected for the SIP Line (Trunk). The codec selections defined under **Section 5.2.4.1** are the codecs selected for the IP phones/extension (H.323 and SIP).

5.4.7. SIP Line – SIP Advanced Tab

In the **Addressing** area:

- Select **To Header** for **Call Routing Method**.

In the **Identity** area:

- The **Caller ID from From header** box is checked. Incoming calls can include caller ID information in both the From field and in the PAI fields. When this option is selected, the caller ID information in the From field is used rather than that in the PAI fields.
- The **Send From in Clear** is checked (Refer to **Section 2.2**)
- Verify that **Cache Auth Credentials** box is checked (Default = On). When set to On, allows the credentials challenge and response from a registration transaction to be automatically inserted into later SIP messages without waiting for a subsequent challenge.

In the **Call Control** area:

- Check **Emulate NOTIFY for REFER** (Refer to **Section 2.2**).
- Check **No REFER if using Diversion** (Refer to **Section 2.2**)
- Default values may be used for all other parameters.
- Click **OK** to commit.

The screenshot shows the 'SIP Line - Line 17' configuration window with the 'SIP Advanced' tab selected. The left sidebar shows a tree view of the configuration hierarchy, including 'Line 17'. The main area is divided into three sections: 'Addressing', 'Identity', and 'Call Control'.

Addressing Section:

- Association Method: By Source IP address
- Call Routing Method: To Header
- Use P-Called-Party: ☐
- Suppress DNS SRV Lookups: ☐

Identity Section:

- Use "phone-context": ☐
- Add user=phone: ☐
- Use + for International: ☐
- Use PAI for Privacy: ☐
- Use Domain for PAI: ☐
- Caller ID from From header: ☒
- Send From in Clear: ☒
- Cache Auth Credentials: ☒
- User-Agent and Server Headers:
- Send Location Info: Never
- Add UUI header: ☐
- Add UUI header to redirected calls: ☐

Call Control Section:

- Media:
 - Allow Empty INVITE: ☐
 - Send Empty re-INVITE: ☐
 - Allow To Tag Change: ☐
 - P-Early-Media Support: None
 - Send SilenceSup=Off: ☐
 - Force Early Direct Media: ☐
 - Media Connection Preservation: System
 - Indicate HOLD: ☒
 - Media Security: ☐
- Call Control:
 - Call Initiation Timeout (s): 4
 - Call Queuing Timeout (mins): 5
 - Service Busy Response: 486 - Busy Here
 - on No User Responding Send: 408-Request Timeout
 - Action on CAC Location Limit: Allow Voicemail
 - Suppress Q.850 Reason Header: ☐
 - Emulate NOTIFY for REFER: ☒
 - No REFER if using Diversion: ☒

At the bottom, there is a 'Calling Number Verification' section with 'Incoming Calls Handling' set to a dropdown menu. The window has 'OK', 'Cancel', and 'Help' buttons at the bottom right.

5.5. Mobility

Select the **Mobility** tab for the user. In the sample configuration user 3042 was one of the users configured to test the Mobile Twinning feature. The following screen shows the Mobility tab for user 3042. The Mobility Features and Mobile Call Control boxes are checked. The Twinned Mobile Number field is configured with the number to dial to reach the twinned telephone, including the dial access code “9”, in this case 9293521234. Other options can be set according to customer requirements.

Note: Checking the Mobile Call Control box allows a user receiving a call on their twinned device to access system dial tone and then perform dialing action including making calls and activating short codes.

The screenshot displays the Avaya Configuration Manager interface for user 3042. The left pane shows a tree view of the configuration hierarchy, including Solution, User (32), Group(2), Short Code(48), Directory(0), Time Profile(0), Account Code(0), User Rights(9), Location(1), IPOSE-Primary, System (1), Line (3), Control Unit (9), Extension (6), User (7), NoUser, 3050 3050, 3040 Ext3040 H323, 3041 Ext3041 H323, 3042 Ext3042 H323, 3047 Ext3047 SIPSoft, 3051 Ext3051 Deskph, Group (0), Short Code (4), Service (0), Incoming Call Route (7), IP Route (3), License (8), Auto Attendant (0), ARS (1), Conference (0), Location (1), Authorization Code (0), IP500V2-One, and IP500V2-Two. The right pane shows the Mobility configuration options for user 3042. The tabs are Button Programming, Menu Programming, Mobility, Group Membership, Announcements, and SIP. The Mobility tab is selected. The configuration options include: Simultaneous Coverage Delay (secs) set to 0, MS Teams URI field, Internal Twinning checkbox (unchecked), Twinned Handset dropdown set to <None>, Maximum Number of Calls dropdown set to 1, Twin Bridge Appearances checkbox (unchecked), Twin Coverage Appearances checkbox (unchecked), Twin Line Appearances checkbox (unchecked), Mobility Features checkbox (checked), Mobile Twinning checkbox (unchecked), Fallback Twinning checkbox (unchecked), Twinned Mobile Number (including dial access code) field set to 9293521234, Twinning Time Profile dropdown set to <None>, Mobile Dial Delay (sec) field set to 0, Mobile Answer Guard (sec) field set to 0, Hunt group calls eligible for mobile twinning checkbox (unchecked), Forwarded calls eligible for mobile twinning checkbox (unchecked), Twin When Logged Out checkbox (unchecked), one-X Mobile Client checkbox (unchecked), Mobile Call Control checkbox (checked), and Mobile Callback checkbox (unchecked). The status bar at the bottom indicates 'Ready'.

5.6. IP Office Line – Primary Server

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the P500V2-One Expansion System.

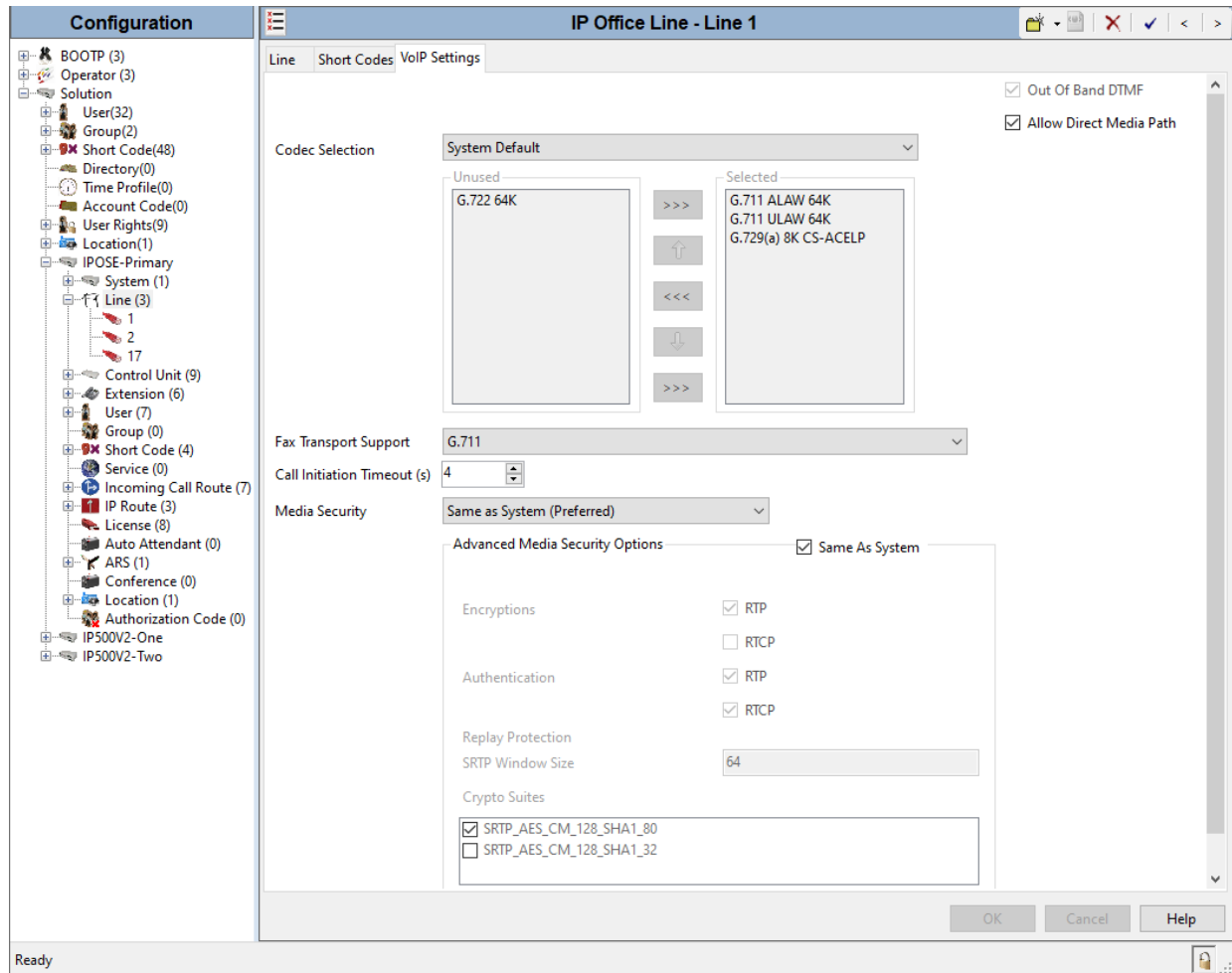
The screenshot displays the 'IP Office Line - Line 1' configuration window. The left-hand 'Configuration' pane shows a hierarchical tree with 'Line (3)' selected under the 'System (1)' node. The main configuration area is divided into several sections:

- Line Settings:** Includes fields for Line Number (1), Telephone Number, Transport Type (WebSocket Server), Prefix, Networking Level (SCN), Outgoing Group ID (99999), Security (Medium), Number of Channels (250), and Outgoing Channels (250).
- Gateway:** Includes fields for Address (192 . 168 . 8 . 165), Location (3: Thornton, CO), Password, and Confirm Password.
- SCN Resiliency Options:** A group box containing four unchecked checkboxes: 'Supports Resiliency', 'Backs up my IP phones', 'Backs up my hunt groups', 'Backs up my voicemail', and 'Backs up my IP DECT phones'.
- Description:** A text field at the bottom.

At the bottom of the window are 'OK', 'Cancel', and 'Help' buttons. The status bar at the very bottom indicates 'Ready'.

The screen below shows the IP Office Line, **VoIP Settings** tab:

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **G.711** for **Fax Transport Support** (refer to **Section 2.1**).
- Under **Media Security** verify **Same as System (Preferred)** is selected (default value).
- Click **OK** to commit.

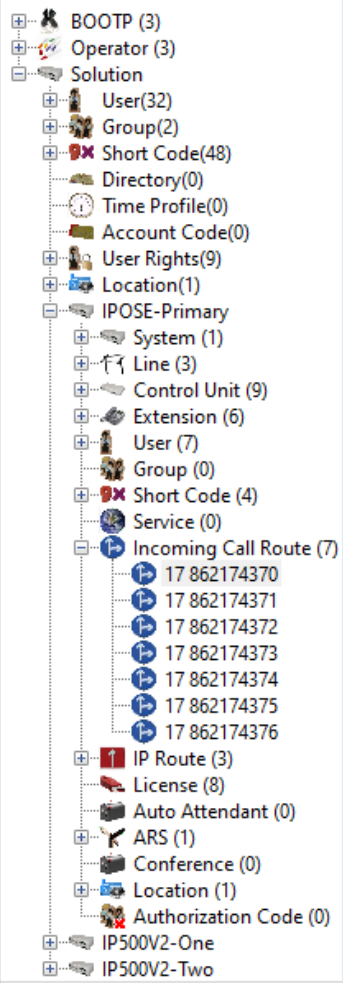


Repeat this process as needed to add additional Secondary server or Expansion Systems to the solution.

5.7. Incoming Call Route

Incoming call routes map inbound DID numbers on a specific line to internal extensions, hunt groups, short codes, etc., within the IP Office system. To add an incoming call route, right click on **Incoming Call Route** in the **Navigation** pane and select **New** (not shown). On the Details Pane, under the **Standard** tab, set the parameters as show below:

- Set **Bearer Capacity** to **Any Voice**.
- The **Line Group ID** is set to **17**. This matches the **Incoming Group** field configured in the **Call Details** tab for the SIP Line on **Section 5.4.5**.
- On the **Incoming Number**, enter one of the DID numbers provided by Telstra.
- Default values may be used for all other parameters.
- Click **OK** to commit (not shown).

Configuration	17 862174370
	<div>Standard Voice Recording Destinations</div> <div><div>Bearer Capability</div><div>Any Voice</div></div> <div><div>Line Group ID</div><div>17</div></div> <div><div>Incoming Number</div><div>862174370</div></div> <div><div>Incoming Sub Address</div><div></div></div> <div><div>Incoming CLI</div><div></div></div> <div><div>Locale</div><div></div></div> <div><div>Priority</div><div>1 - Low</div></div> <div><div>Tag</div><div></div></div> <div><div>Hold Music Source</div><div>System Source</div></div> <div><div>Ring Tone Override</div><div>None</div></div>
Ready	

Select the **Destinations** tab. From the **Destination** drop-down menu, select the IP Office extension associated with this DID number. In the reference configuration, the DID number 862174370 provided by Telstra was associated with the Avaya IP Office extension **3042 Ext3042 H323**.

The screenshot shows the Avaya IP Office configuration interface. On the left is a tree view of the configuration hierarchy. The right pane shows the 'Destinations' tab for the selected DID '17 862174370'. The 'Destinations' tab contains a table with the following data:

TimeProfile	Destination	Fallback Extension
Default Value	3042 Ext3042 H323	

The status bar at the bottom left indicates 'Ready'.

Repeat this process as needed to assign incoming call routes to additional IP Office users, as well as for other Avaya IP Office destinations (Hunt Group, Voicemail, Short Codes, etc.).

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.

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**, **Australia (UK English)** was used.
- Click the **OK** to commit (not shown).

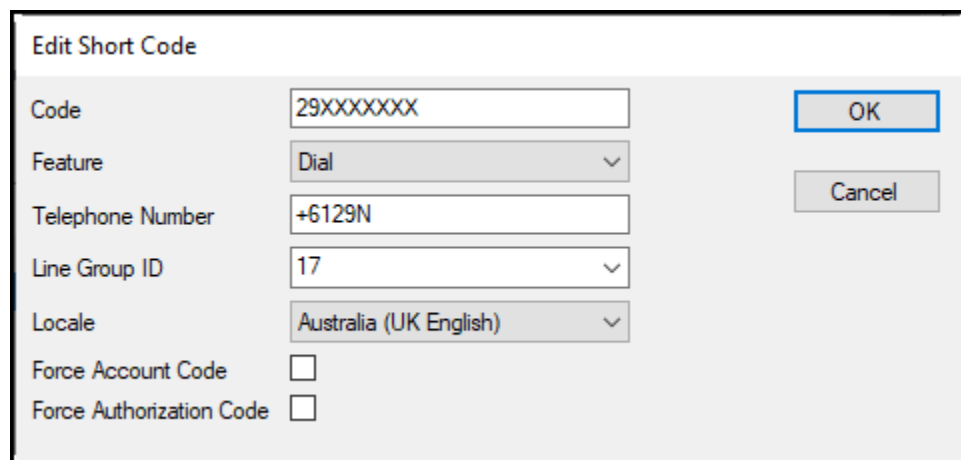
HG; Reviewed:
SPOC 7/8/2022

The following screen shows the example ARS configuration for the route **Main**. Note the sequence of **Xs** 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** (not shown). Configure the following parameters:

- In the **Code** field, enter the dial string which will trigger this short code. In this case, **29** followed by **7 Xs** 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 **+6129N**. The value **N** represents the additional number of digits dialed by the user after dialing **29** (The **9** will be stripped off). With this setting **+6129** and the dialed **7** digits number will be sent to the trunk, with **+6129** preceding the dialed **7**-digits number, **61** is the country code (Australia). The “+” (plus) is needed by Telstra to conform with the E.164 dialing format.
- 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.
- For **Locale**, **Australia (UK English)** was used
- Click **OK** to commit.

The following examples shows a subset of dial patterns used during the compliance test for calls made within Australia:



Edit Short Code	
Code	29XXXXXXXX
Feature	Dial
Telephone Number	+6129N
Line Group ID	17
Locale	Australia (UK English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

Edit Short Code

Code	<input type="text" value="03XXXXXXXX"/>	<input type="button" value="OK"/>
Feature	<input type="text" value="Dial"/>	<input type="button" value="Cancel"/>
Telephone Number	<input type="text" value="+613N"/>	
Line Group ID	<input type="text" value="17"/>	
Locale	<input type="text" value="Australia (UK English)"/>	
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

Edit Short Code

Code	<input type="text" value="04XXXXXXXX"/>	<input type="button" value="OK"/>
Feature	<input type="text" value="Dial"/>	<input type="button" value="Cancel"/>
Telephone Number	<input type="text" value="+614N"/>	
Line Group ID	<input type="text" value="17"/>	
Locale	<input type="text" value="Australia (UK English)"/>	
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

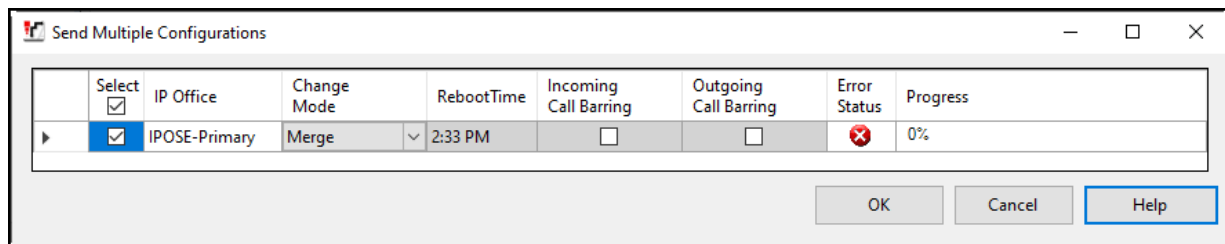
Repeat the above procedure for additional dial patterns to be used by the enterprise to dial out from IP Office.

5.9. Save IP Office Primary Server Configuration

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. At the top of the Avaya IP Office Manager page, click **File → Save Configuration** (if that option is grayed out, no changes are pending).

A screen similar to the one below will appear, with either **Merge** or **Reboot** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Reboot** option will save the configuration and cause the Avaya IP Office server to reboot.

Click **OK** to execute the save.







































6. Avaya IP Office Expansion System Configuration

Navigate to **File → Open Configuration** (not shown), select the proper Avaya IP Office system from the pop-up window, and log in using the appropriate credentials. Clicking the “plus” sign next to IP Office Expansion system.

Configuration	System Inventory
<ul style="list-style-type: none">BOOTP (3)Operator (3)Solution<ul style="list-style-type: none">User(32)Group(2)Short Code (48)Directory(0)Time Profile(0)Account Code(0)User Rights(9)Location(1)IPOSE-PrimaryIP500V2-OneIP500V2-Two	<h3>Server Edition Expansion System</h3> <ul style="list-style-type: none">Hardware Installed<ul style="list-style-type: none">Control Unit: IP 500 V2Internal Modules: VCM64/PRID U; PHONE8Expansion Modules: DIG DCPx16 V2System Settings<ul style="list-style-type: none">IP Address: 192.168.8.165Sub-Net Mask: 255.255.255.0System Locale: United States (US English)System Location: 3: Thornton, CODevice ID: NONENumber of Extensions on System: 24Features Configured<ul style="list-style-type: none">Licenses Installed: Server Edition(1); IP Office Select(1)Connected Extensions: 3043; 3044Users NOT Configured for Voicemail: NONEUsers assigned as Ex-Directory: NONEUsers assigned for Twinning: NONEUsers barred from making Outgoing Calls: NONEMusic on Hold: WAV File

6.1. Physical Hardware

In the sample configuration, the IP500 V2 Expansion System contained a PHONE8 analog card, for the support of analog extensions, a DIG DCPx16 V2, for support of digital extensions. Also included is a VCM64 (Voice Compression Module). The VCM64 cards provide voice compression channels to the control unit. Voice compression channels are needed to support VoIP calls, including IP extensions and or IP trunks.

Configuration	IP 500 V2
 BOOTP (3)	Unit
 Operator (3)	
 Solution	
 User(32)	Device Number <input type="text" value="1"/>
 Group(2)	Unit Type <input type="text" value="IP 500 V2"/>
 Short Code (48)	Version <input type="text" value="11.1.2.2.0 build 20"/>
 Directory(0)	Serial Number <input type="text" value="00e007060fca"/>
 Time Profile(0)	Unit IP Address <input type="text" value="10.64.70.60"/>
 Account Code(0)	Interconnect Number <input type="text" value="0"/>
 User Rights(9)	Module Number <input type="text" value="Control Unit"/>
 Location(1)	
 IPOSE-Primary	
 IP500V2-One	
 IP500V2-Two	
 System (1)	
 Line (19)	
 Control Unit (4)	
 1 IP 500 V2	
 2 VCM64/PRID U	
 3 PHONE8	
 6 DIG DCPx16 V2	
 Extension (24)	
 User (4)	
 Group (1)	
 Short Code (12)	
 Service (0)	
 RAS (1)	
 Incoming Call Route (4)	
 WAN Port (0)	
 Firewall Profile (1)	
 IP Route (2)	
 License (1)	
 Tunnel (0)	
 ARS (2)	
 Location (1)	
 Authorization Code (0)	

6.2. LAN Settings

In the sample configuration, LAN1 is used to connect the Expansion System to the enterprise network. To view or configure the LAN1 IP address, select **System** on the Navigation pane. Select the **LAN1 → LAN Settings** tab on the Details pane, and enter the following:

- **IP Address: 192.168.8.165** was used in the reference configuration.
- **IP Mask: 255.255.255.0** was used in the reference configuration
- Click the **OK** button (not shown).

The screenshot displays the Avaya IP500V2-One configuration interface. On the left is the 'Configuration' navigation pane with a tree structure. The 'System' node is expanded, showing 'IP500V2-One' and its sub-nodes. The 'IP500V2-One' node is selected. On the right is the 'IP500V2-One' details pane. The 'LAN1' tab is selected, and the 'LAN Settings' sub-tab is active. The configuration fields are as follows:

Field	Value
IP Address	192 . 168 . 8 . 165
IP Mask	255 . 255 . 255 . 0
Primary Trans. IP Address	0 . 0 . 0 . 0
RIP Mode	None
Enable NAT	<input type="checkbox"/>
Number Of DHCP IP Addresses	200
DHCP Mode	<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dial In <input checked="" type="radio"/> Disabled

An 'Advanced' button is located at the bottom right of the LAN Settings section. The status bar at the bottom left indicates 'Ready'.

Default values were used on the **VoIP** and **Network Topology** tabs (not shown).

6.3. IP Route

To create an IP route for the Expansion system, right-click on **IP Route** on the left Navigation pane. Select **New** (not shown).

- Enter **0.0.0.0** on the **IP Address** and **IP Mask** fields to make this the default route.
- Set **Gateway IP Address** to the IP Address of the default router in the IP Office subnet. The default gateway in the reference configuration was **192.168.8.1**
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).

The screenshot shows a network management interface. On the left is a 'Configuration' tree view. Under 'IP Route (3)', three routes are listed: '0.0.0.0', '10.64.101.0', and '192.168.99.0'. The '0.0.0.0' route is selected. On the right is the configuration window for the selected route, titled '0.0.0.0'. It contains the following fields:

IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	192 . 168 . 8 . 1
Destination	LAN1
Metric	0

Below the Metric field is a checkbox labeled 'Proxy ARP' which is currently unchecked.

6.4. IP Office Line – IP500 V2 Expansion System

In IP Office Server Edition systems, IP Office Lines are automatically created on each server when a Secondary server or Expansion System is added to the solution. To edit an existing IP Office Line, select **Line** in the Navigation pane, and select the appropriate line to be configured in the Group pane. The screen below shows the IP Office Line to the Primary server.

The screenshot displays the 'IP Office Line - Line 17' configuration window. On the left is a 'Configuration' navigation pane showing a tree structure of system components. The main area on the right is divided into tabs: 'Line', 'Short Codes', 'VoIP Settings', and 'T38 Fax'. The 'Line' tab is active, showing various configuration fields. The 'Gateway' section includes an 'Address' field with a dotted IP address (10.64.101.127), a 'Port' field set to 443, and a 'Location' dropdown menu set to '3: Thornton, CO'. There are also fields for 'Password' and 'Confirm Password', both masked with dots. The 'SCN Resiliency Options' section contains three checkboxes: 'Supports Resiliency', 'Backs up my IP phones', 'Backs up my hunt groups', and 'Backs up my IP DECT phones'. The 'Line Number' is set to 17, 'Transport Type' is 'WebSocket Client', 'Networking Level' is 'SCN', and 'Security' is 'Medium'. Other fields include 'Telephone Number', 'Prefix', 'Outgoing Group ID' (99999), 'Number of Channels' (250), and 'Outgoing Channels' (250). A 'Description' field is at the bottom. An 'OK' button is in the bottom right corner. The status bar at the very bottom of the window says 'Ready'.

IP Office Line - Line 17	
Line Number	17
Transport Type	WebSocket Client
Networking Level	SCN
Security	Medium
Telephone Number	
Prefix	
Outgoing Group ID	99999
Number of Channels	250
Outgoing Channels	250
Gateway	
Address	10 . 64 . 101 . 127
Port	443
Location	3: Thornton, CO
Password
Confirm Password
SCN Resiliency Options	
<input type="checkbox"/> Supports Resiliency	
<input type="checkbox"/> Backs up my IP phones	
<input type="checkbox"/> Backs up my hunt groups	
<input type="checkbox"/> Backs up my IP DECT phones	
Description	

The screen below shows the IP Office Line, **VoIP Settings** tab:

- Under **Codec Selection** verify **System Default** is selected (default value).
- Select **G.711** for **Fax Transport Support** (refer to **Section 2.1**).
- Under **Media Security Preferred** was selected.
- Under **Advanced Media Security Options Same as System** was selected.
- Click **OK** to commit (not shown).

The screenshot displays the 'IP Office Line - Line 17' configuration window, specifically the 'VoIP Settings' tab. The left sidebar shows a hierarchical tree of configuration elements, with 'Line 17' selected under 'IP500V2-One'. The main configuration area includes the following settings:

- Codec Selection:** A dropdown menu set to 'System Default'. Below it, two lists are shown: 'Unused' (containing 'G.723.1 6K3 MP-MLQ') and 'Selected' (containing 'G.711 ALAW 64K', 'G.711 ULAW 64K', and 'G.729(a) 8K CS-ACELP'). Navigation buttons (left arrow, right arrow, up arrow, down arrow) are positioned between the lists.
- Fax Transport Support:** A dropdown menu set to 'G.711'.
- Call Initiation Timeout (s):** A numeric input field set to '4'.
- Media Security:** A dropdown menu set to 'Preferred'.
- Advanced Media Security Options:** A section with a checkbox 'Same As System' which is checked. Below this, there are checkboxes for 'Encryptions' (RTP checked, RTCP unchecked), 'Authentication' (RTP checked, RTCP checked), and 'Replay Protection' (SRTP Window Size set to '64'). At the bottom, there are checkboxes for 'Crypto Suites' (SRTP_AES_CM_128_SHA1_80 checked, SRTP_AES_CM_128_SHA1_32 unchecked).
- Other Settings:** On the right side, there are checkboxes for 'VoIP Silence Suppression' (unchecked), 'Out Of Band DTMF' (checked), and 'Allow Direct Media Path' (checked).

6.5. Short Codes

Similar to the configuration of the Primary server in **Section 5.8.1**, create a Short Code to access ARS. In the reference configuration, the **Line Group ID** is set to the ARS route illustrated in the next section.

The screenshot displays the Avaya configuration interface. On the left is a 'Configuration' tree with a hierarchical structure of system components. On the right is a configuration panel for a 'Short Code' named '9N: Dial'.

Configuration Tree (Left):

- BOOTP (3)
- Operator (3)
- Solution
 - User(32)
 - Group(2)
 - Short Code (48)
 - Directory(0)
 - Time Profile(0)
 - Account Code(0)
 - User Rights(9)
 - Location(1)
 - IPOSE-Primary
 - IP500V2-One
 - System (1)
 - IP500V2-One
 - Line (3)
 - Control Unit (4)
 - Extension (24)
 - User (27)
 - Group (1)
 - Short Code (12)
 - 9N**
 - Service (0)
 - RAS (1)
 - Incoming Call Route (1)
 - WAN Port (0)
 - Firewall Profile (1)
 - IP Route (3)
 - License (1)
 - Tunnel (0)
 - ARS (2)
 - Location (1)
 - Authorization Code (0)
 - IP500V2-Two

9N: Dial Configuration Panel (Right):

Short Code	
Code	9N
Feature	Dial
Telephone Number	N
Line Group ID	51: To-Primary
Locale	Australia (UK English)
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

Ready

6.6. Automatic Route Selection – ARS

The following screen shows an example ARS configuration for the route named “**To-Primary**” on the Expansion System. The **Telephone Number** is set to **9N**. The **Line Group ID** is set to “**99999**” matching the number of the **Outgoing Group ID** configured on the IP Office Line 17 to the Primary server (**Section 6.4**).

The screenshot shows the ARS configuration window for the route named "To-Primary". The left sidebar displays a tree view of the configuration hierarchy, including Solution, User, Group, Short Code, Directory, Time Profile, Account Code, User Rights, Location, IPOSE-Primary, IP500V2-One, System, IP500V2-One, Line, Control Unit, Extension, User, Group, Short Code, Service, RAS, Incoming Call Route, WAN Port, Firewall Profile, IP Route, License, Tunnel, ARS, and IP500V2-Two.

The main configuration area for "To-Primary" includes the following fields and options:

- ARS Route ID: 51
- Route Name: To-Primary
- Dial Delay Time: System Default (4)
- Description: (empty)
- Secondary Dial tone: ☐ (unchecked)
- SystemTone: (dropdown menu)
- Check User Call Barring: ☐ (unchecked)
- In Service: ☒ (checked)
- Out of Service Route: <None>
- Time Profile: <None>
- Out of Hours Route: <None>

A table lists the route details:

Code	Telephone Number	Feature	Line Group ID
N	9N	Dial	99999

Buttons: Add..., Remove, Edit...

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

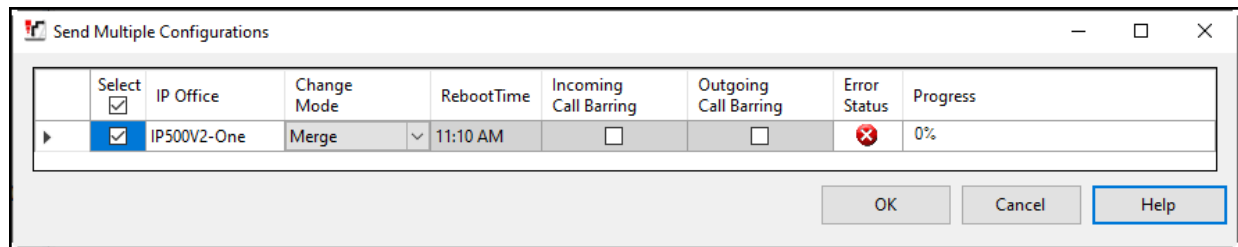
Alternate Route: <None>

Repeat the process described in **Section 6** on any additional Secondary server or Expansion Systems in the solution, as required.

6.7. Save IP Office Expansion System 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 **Reboot** 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.



7. Telstra Enterprise SIP Trunking Service Configuration

To use Telstra Enterprise SIP Trunking Service, a customer must request the service from Telstra using the established sales processes. The process can be started by contacting Telstra via the corporate web site at: <https://www.telstra.com.au/>

During the signup process, Telstra and the customer will discuss details about the preferred method to be used to connect the customer's Avaya enterprise network to the Telstra Enterprise SIP Trunking Service network.

Telstra will provide the following information:

- SIP Proxy FQDN.
- SIP domain name.
- SIP Trunk registration credentials (User Name, Password, etc.).
- DID numbers.
- Public DNS IP addresses.
- Etc.

Note: The SIP Trunk registration credentials, Domain Name, DIDs, etc., shown in this document, were masked for confidentiality and privacy purposes. During the signup process Telstra will provide the customer the necessary information to configure Avaya IP Office.

8. Verification Steps

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

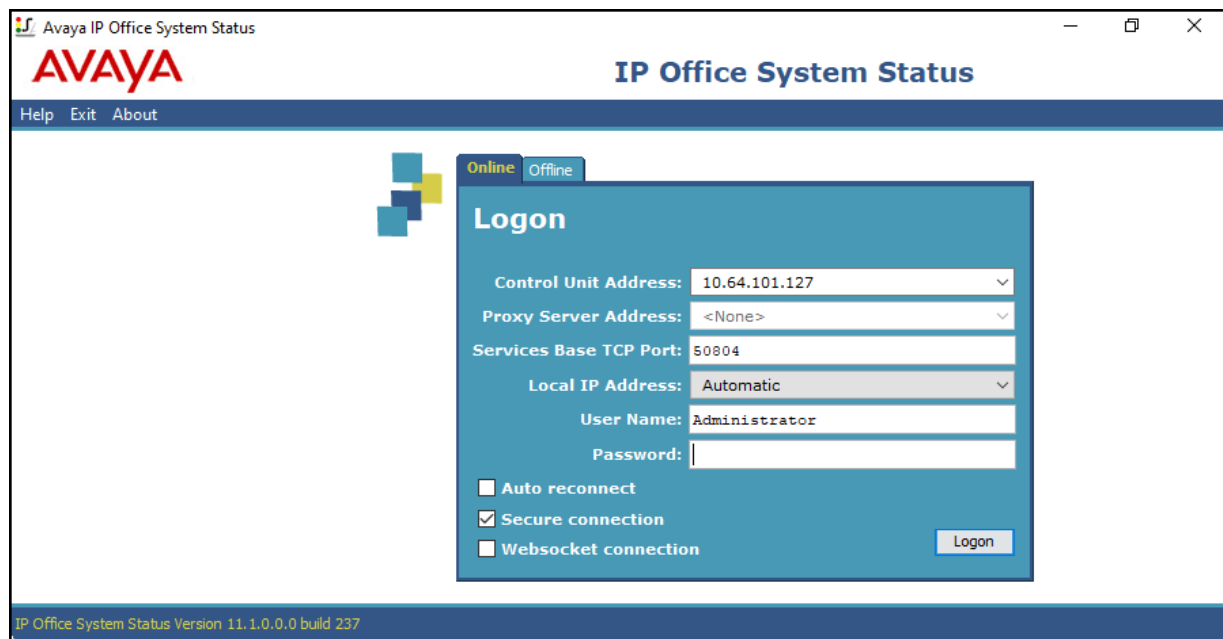
The following steps may be used to verify the configuration:

- 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.

8.1. 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.

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (20)
- Extensions (3)
- Trunks (3)
 - Line: 1
 - Line: 2
 - Line: 17
- Active Calls
- Resources
- Voicemail
- IP Networking
- Locations

Status Utilization Summary Alarms

SIP Trunk Summary

Line Service State: In Service

Peer Domain Name: telstra.com

Resolved Address: .164.8

Line Number: 17

Number of Administered Channels: 10

Number of Channels in Use: 0

Administered Compression: G711 A, G711 Mu, G729 A

Silence Suppression: Off

Media Stream: RTP

Layer 4 Protocol: UDP

SIP Trunk Channel Licenses: 100

SIP Trunk Channel Licenses in Use: 0

SIP Device Features: REFER (Incoming and Outgoing), UPDATE (Incoming

Cha...	U..	Call Ref	Cur...	Time in S...	Rem...	C...	Con...	Caller ID ...	Other Party ...	Dire...	Rou...	Rec...	Rec...
1			Idle	04:...									
2			Idle	04:...									
3			Idle	2 d...									
4			Idle	2 d...									
5			Idle	2 d...									
6			Idle	2 d...									
7			Idle	2 d...									
8			Idle	2 d...									
9			Idle	2 d...									
10			Idle	2 d...									

< >

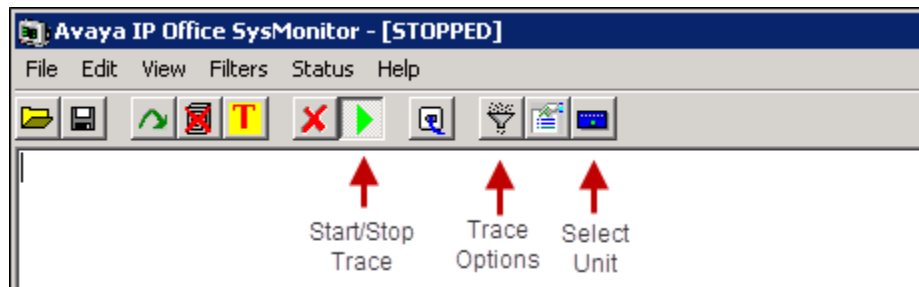
Trace Trace All Pause Ping Call Details Graceful Shutdown

Force Out of Service Print... Save As...

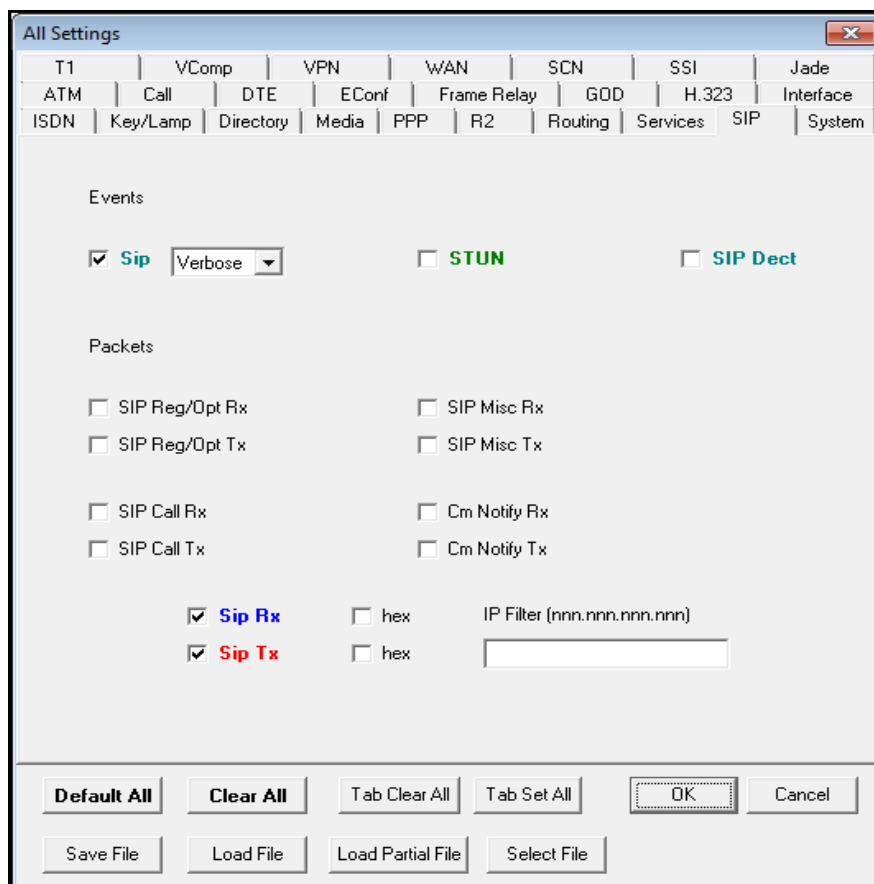
3:57:31 PM Online

8.2. Monitor

The Avaya IP Office SysMonitor 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.



9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya IP Office Release 11.1 to Telstra Enterprise SIP Trunking Service. Telstra Enterprise SIP Trunking Service 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**.

10. 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] *Deploying IP Office Server Edition*, Release 11.1 FP1, Issue 16, February 2021

[2] *Administering Avaya IP Office with IP Office Manager*, November 15, 2021.

[3] *Administering Avaya IP Office with Web Manager*, August 2021.

Additional Avaya IP Office documentation can be found at:

<https://ipofficekb.avaya.com/>

©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.