Avaya Solution & Interoperability Test Lab

Application Notes for configuring Edgewater Networks Enterprise Session Border Controllers supporting SIP Trunk Connectivity between sites with Avaya IP Office 8.0 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the EdgeProtect and EdgeMarc Enterprise Session Border Controllers (SBCs) from Edgewater Networks, to interoperate with Avaya IP Office 8.0 supporting Session Initiation Protocol (SIP) Trunking between a headquarters and a branch office location of an Enterprise.

Located at headquarters locations, the EdgeProtect Session Border Controller terminates Transport Layer Security (TLS) connections from multiple remote branch offices where the EdgeMarc SBCs are deployed. This is done to provide confidentiality, authentication and encryption for all VoIP communication between the Enterprise locations, across an untrusted network.

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 the EdgeProtect and EdgeMarc Enterprise Session Border Controllers from Edgewater Networks, to interoperate with an Avaya IP Office solution, in a distributed IP Telephony scenario with separate headquarters and branch office locations.

The EdgeProtect and EdgeMarc solution uses a VoIP Traversal mechanism, which allows the creation of a secure tunnel from a remote client to an external server across the untrusted network. All VoIP traffic flowing between the headquarters and branch sites will travel through this tunnel. The VoIP traffic will be encrypted, using Transport Layer Security (TLS) protocol.

2. General Test Approach and Test Results

The test approach was to configure a simulated enterprise cloud in the Test Lab, with one headquarters and one branch sites, each site containing an Avaya IP Office 500v2, Release 8. A SIP Trunk connection is configured between the two IP Offices, across the Session Border Controllers and the untrusted network.

The EdgeProtect SBC is located at the headquarters location, and the EdgeMarc SBC is located at the branch site. Both SBCs have a Public side, which connects to the untrusted network, and a Private side that connects to the enterprise network at each location, where the respective IP Offices are located. All SIP and RTP traffic entering or leaving each location flows through the SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The transport protocol between the IP Office and the SBC at each location is UDP. The transport protocol between the two SBCs across the untrusted network is TLS.

In addition to the VoIP Traversal, the EdgeMarc at the branch site uses the Application Layer Gateway (ALG) feature, which provides the proxy and call control capabilities needed for the support of the SIP trunk across its WAN and LAN interfaces.

All tests performed were completed successfully, with the observation noted in **Section 2.2**.

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 interoperability, the following features and functionality were covered during the compliance test:

- Basic call scenarios using G.711U and G.729A codecs.
- Quality of Service.
- DTMF transmission using RFC 2833.
- Avaya soft clients.
- Voicemail with message waiting indicators (MWI).
- User features such as call hold and resume, forward, transference and conference.
- Network Call Redirection between sites using the SIP REFER method.
- T.38 Fax.

2.2. Test Results

Interoperability testing was completed with successful results for all test cases with the exception of the observations/limitations described below:

Application Layer Gateway (ALG) dynamic IP address assignment. At the time of writing these Application Notes, with version 11.6.6 of the Edgewater VoIP Operating System (VOS), the IP address of the WAN ALG in the EdgeMarc is assigned dynamically on the traversal subnet by the EdgeProtect DHCP server. This address is used in the configuration of the SIP Line of the IP Office at the Main Site, as the ITSP Proxy Address. In a site to site configuration like the one used for the compliance test, where DNS was not used, this parameter should be a static IP address, not dynamic. Edgewater Networks will provide the option in future software loads for entering this IP address statically, directly from the browser configuration screens

2.3. Support

For technical support on the Edgewater Networks products described in these Application Notes visit http://www.edgewaternetworks.com/support.

3. Reference Configuration

Figure 1 below shows the configuration used for the compliance test. It shows the **Main Site** and the **Branch Office**, connected by the SIP trunk across the untrusted network.

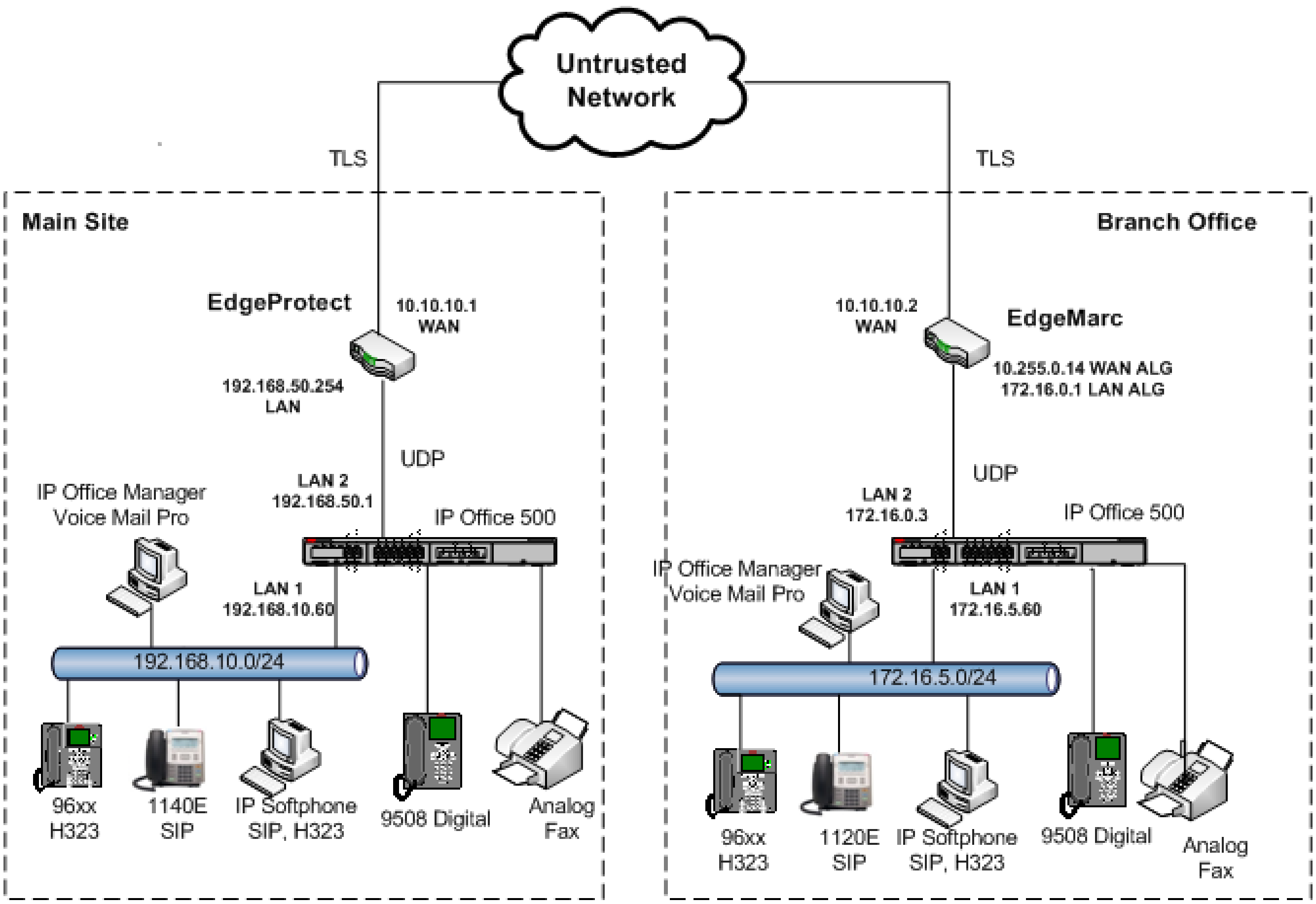


Figure 1.Test Configuration

Each location contains an Avaya IP Office 500v2 Release 8.0, Avaya Voicemail Pro, Avaya IP Office soft clients, and Avaya hard phones including SIP, H.323, digital, and analog endpoints. The IP Office connects to the local area network through its LAN1 port, while it uses the LAN2 port to connect to the LAN side of the EdgeProtect or the EdgeMarc SBC. The SBCs connect to the untrusted network through their WAN interface.

In this configuration, all endpoints register with their local IP Office. VoIP traffic will only traverse the untrusted network when placing calls between the sites.

For security purposes, private addresses are shown in **Figure 1** for the WAN network interfaces of the EdgeProtect and the EdgeMarc, instead of the real public IP addresses used during the compliance tests.

4. Equipment and Software Validated

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

Component	**Version**
Avaya	
Avaya IP Office 500v2	8.0 (16)
Avaya IP Office Digital Expansion Module DCPx16	10.0 (16)
Avaya IP Office Manager	10.0 (16)
Avaya IP Office Voicemail Pro	8.0.8.29
Avaya 96x0 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.1
Avaya 9608 IP Telephone (H.323)	Avaya one-X Deskphone. Release 6.1380
Avaya 1140E IP Telephones (SIP)	04.03.09.00
Avaya 1120E IP Telephones (SIP)	04.03.09.00
Avaya Digital Phone 9508	N/A
Avaya IP Office Softphone (SIP)	3.1.2.17_59616
Avaya IP Office Phone Manager	4.2.39
Edgewater Networks	
EdgeProtect Enterprise Session Border Controller 5300LF2 series	11.6.6
EdgeMarc Enterprise Session Border Controller 4550 series	11.6.6

5. Configure IP Office

This section describes the configuration steps to support a SIP trunk connection between the Avaya IP Offices at the headquarters and branch locations. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running the Avaya IP Office Manager application, select **Start** → **Programs** → **IP Office** → **Manager** to launch the application. Navigate to **File** → **Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials. A management window will appear similar to the one shown in the next section.

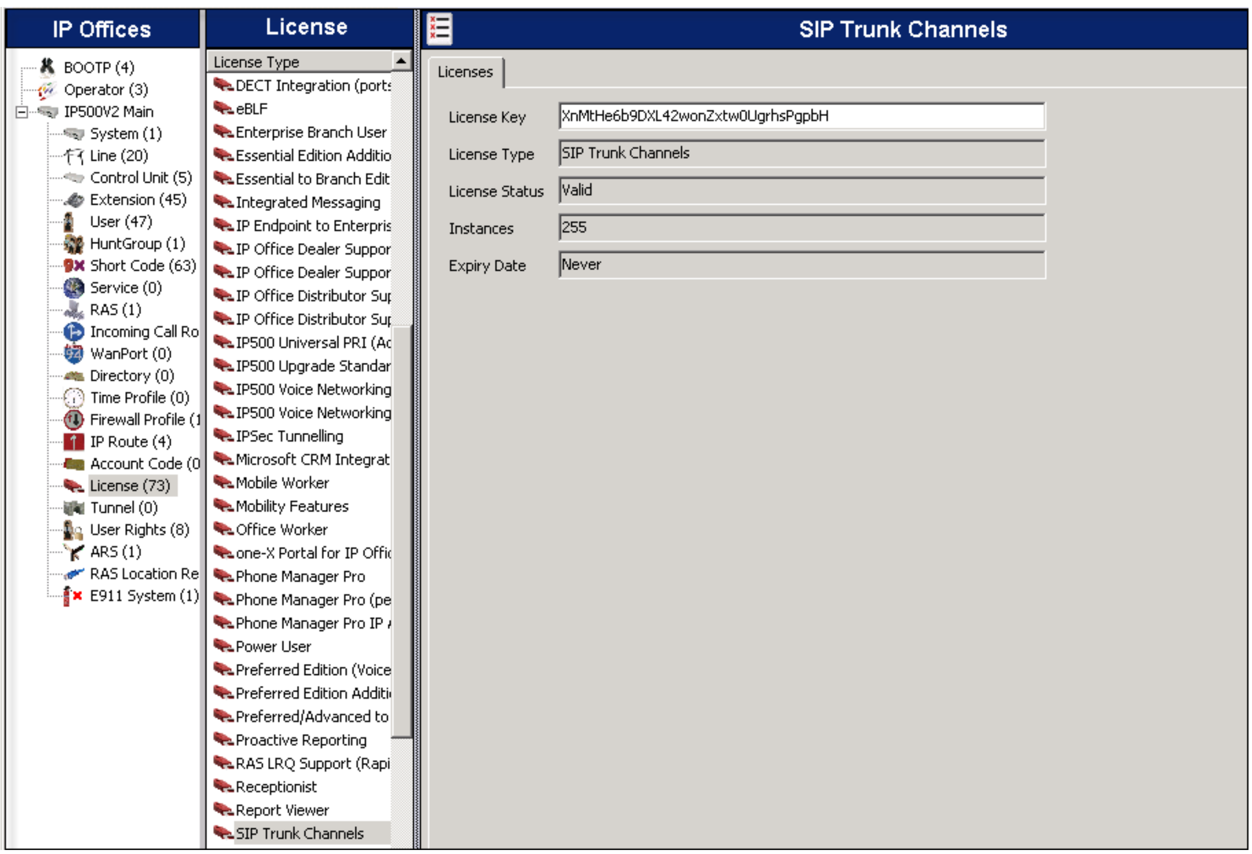
The appearance of the IP Office Manager can be customized using the **View** menu. In the screens presented in this section, the View menu was configured to show the Navigation pane on the left side, the Group pane in the center and the Details pane on the right side. These panes will be referenced throughout the Avaya IP Office configuration. Proper licensing as well as standard feature configurations that are not directly related to the test case described (such as the LAN1 interface configuration, Voicemail, etc) is assumed to be already in place, and they are not part of these Application Notes.

During the next configuration sections, many of the configuration parameters are common for the IP Offices at the Main and Branch sites. In those cases where the same settings apply for both systems, a single screenshot will be shown. Separate screens will be presented for each IP Office only when different parameters need to be specified for each case.

5.1. Licensing

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

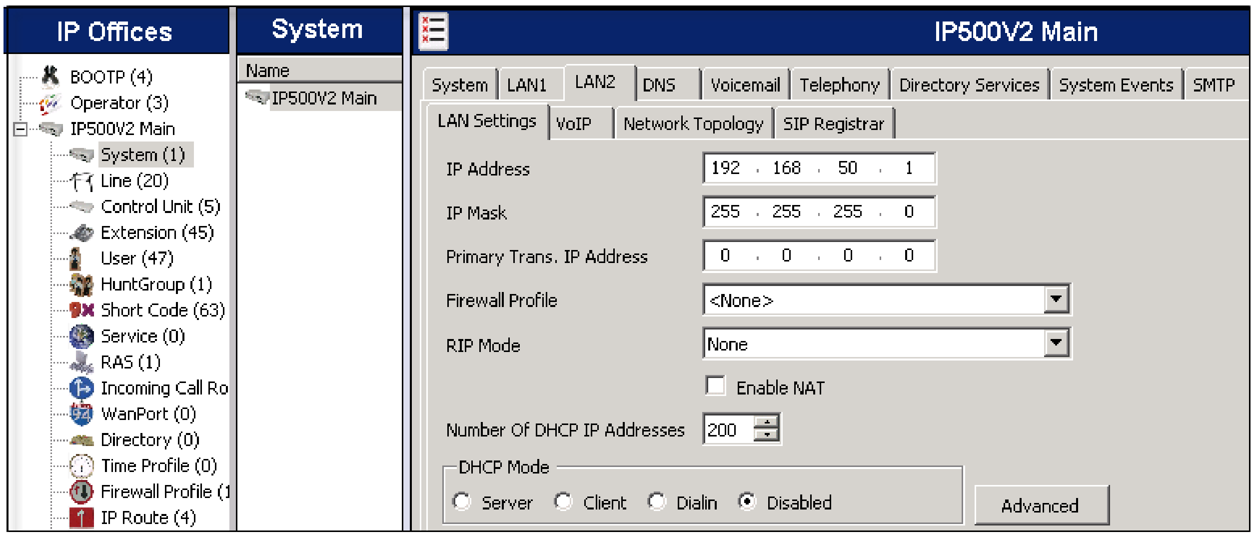
In the sample configuration, **IP500V2 Main** and **IP500V2 Branch** were used as the system names for the IP Offices at the two locations. To verify that there is a SIP Trunk Channels License with sufficient capacity; navigate on each IP Office to **License → SIP Trunk Channels** in the Navigation and Group panes. Confirm that there is a valid license with sufficient "Instances" (trunk channels) in the Details pane.



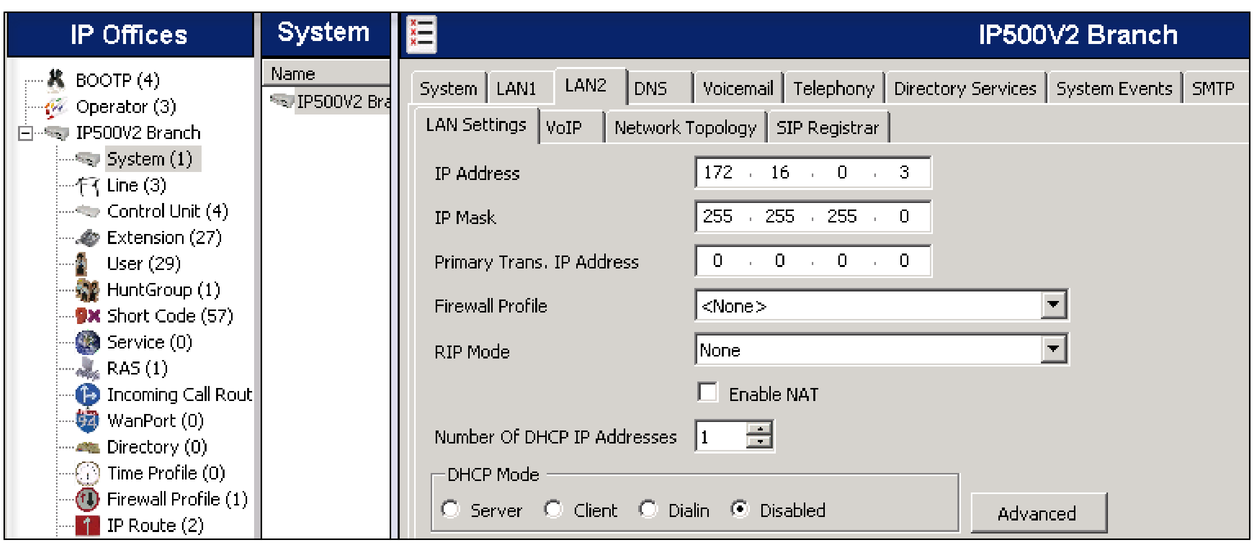
5.2 LAN2 Settings

In the sample configuration, the LAN2 port was used to connect the Avaya IP Office to the Inside port of the SBC at each location. The LAN2 settings correspond to the WAN port on the Avaya IP Office. To access the LAN2 settings, first navigate to **System (1)** in the Navigation pane. Select the appropriate **System Name** on the Group pane and then navigate to the **LAN2 → LAN Settings** tab in the Details pane. Set the **IP Address** and **IP Mask** fields to the values assigned to the Avaya IP Office LAN2 port (see **Figure 1**). All other parameters should be set according to customer requirements.

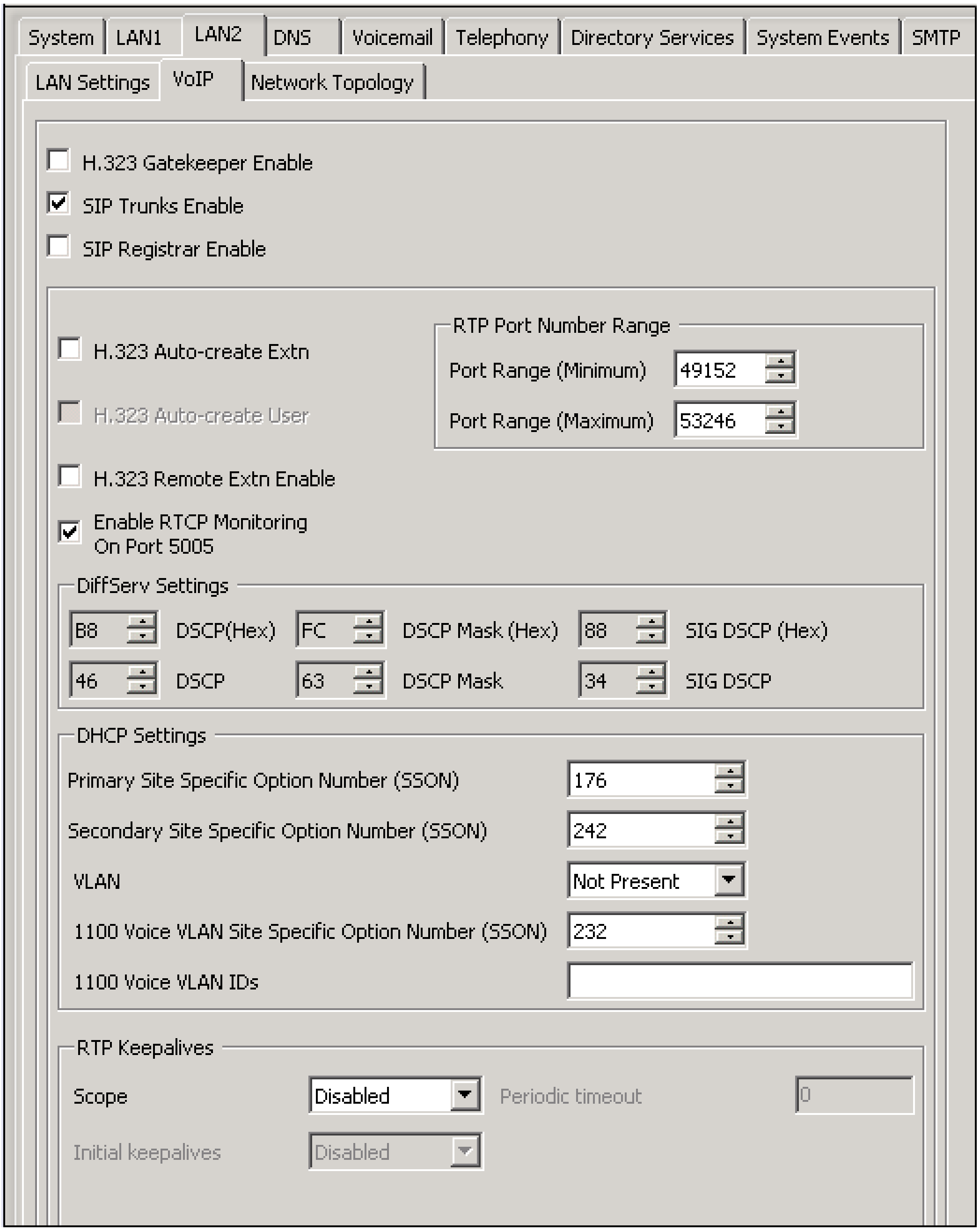
For the Main Site:



For the Branch Office:



On the **VoIP** tab in the Details pane, check the **SIP Trunks Enable** box to enable the configuration of SIP trunks on this interface. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media for calls using LAN2. Defaults values were used. Avaya 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 screen below.

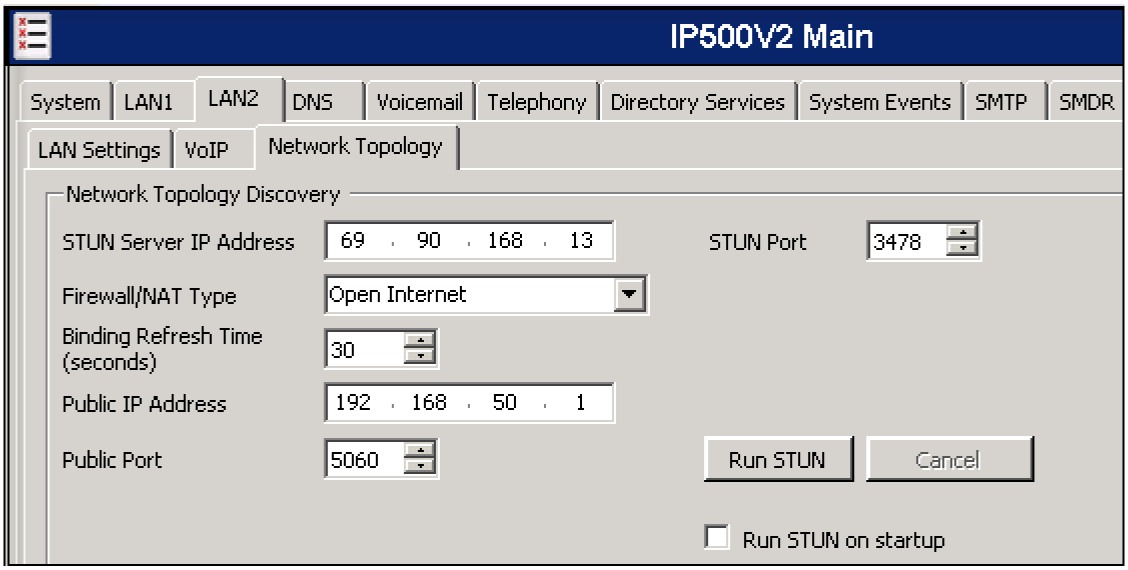


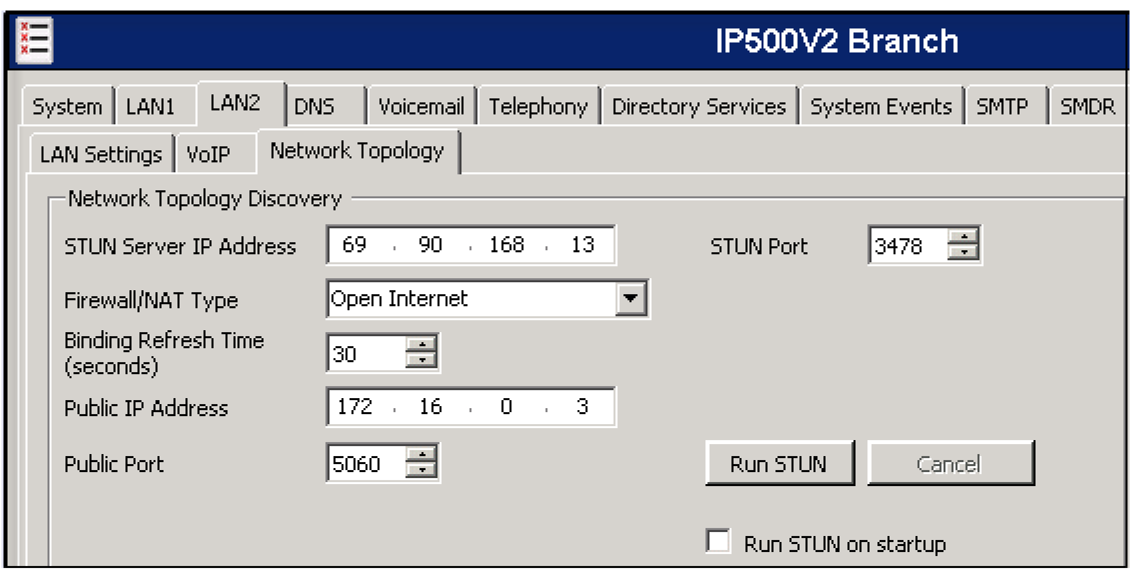
On the **Network Topology** tab in the Details pane, configure the following parameters:

- 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 **30**. This value determines the frequency at which Avaya IP Office will send SIP OPTIONS messages to the far-end SIP proxy of a SIP trunk on this interface.
- Set **Public IP Address** to the IP address that was set for LAN2.
- Set **Public Port** to **5060**.

Default values were used for the rest of the parameters on this screen.

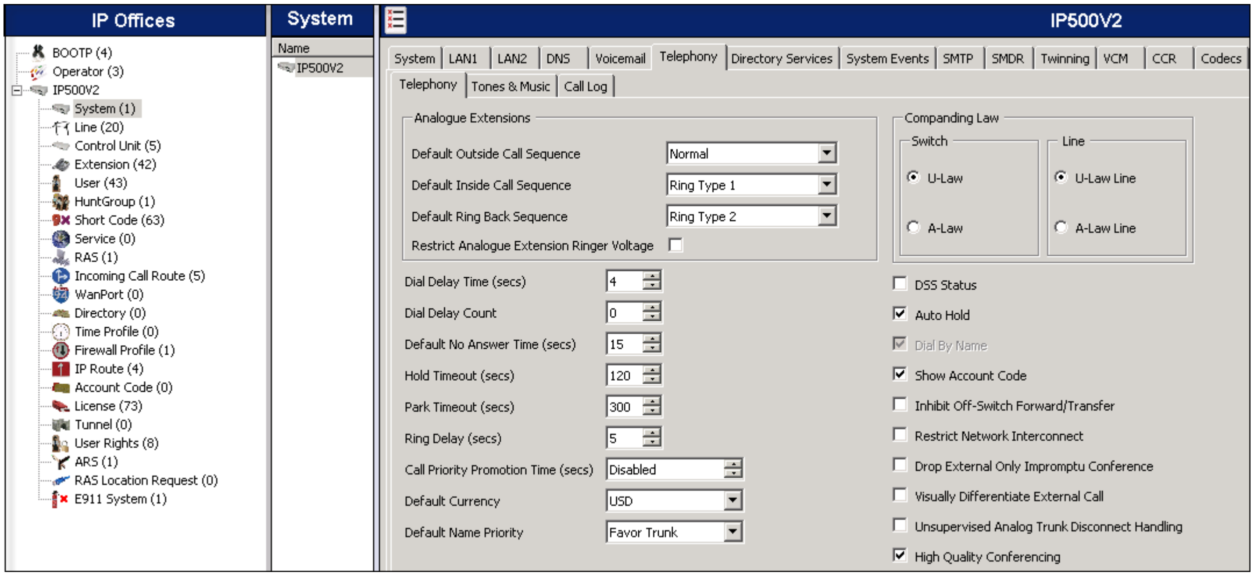
The screens below show the **Network Topology** settings for the Main and the Branch sites:





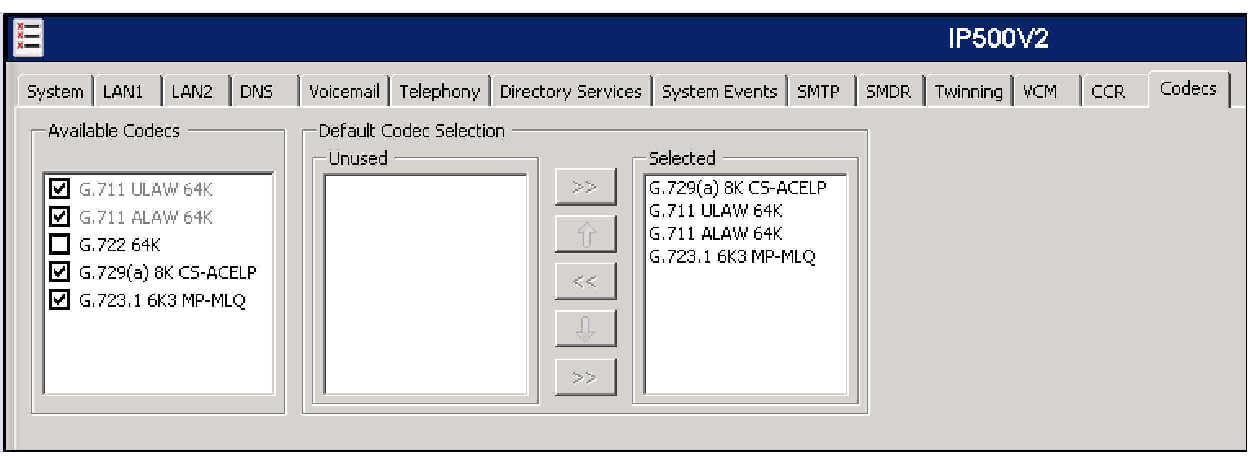
5.3. System Telephony Settings

Navigate to the **Telephony** → **Telephony** Tab in the Details Pane. Choose the **Companding Law** typical for the enterprise location. In North America, ***U-LAW*** is normally used. For the compliance test, the **Inhibit Off-Switch Forward/Transfer** box was unchecked to allow call forwarding and call transfers out to the SIP Trunk. Defaults were used for all other parameters.



5.4. System's Default Codec Selection

The **System** →**Codecs** tab is new in IP Office Release 8. The list of **Available Codecs** shows all the codecs supported by the system, and those selected as usable. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and the **Selected** lists, and to change the order of preference of the codecs in the **Selected** list. By default, all IP (SIP and H.323) lines and extensions will use this system default codec selection, unless configured otherwise for a specific line or extension.

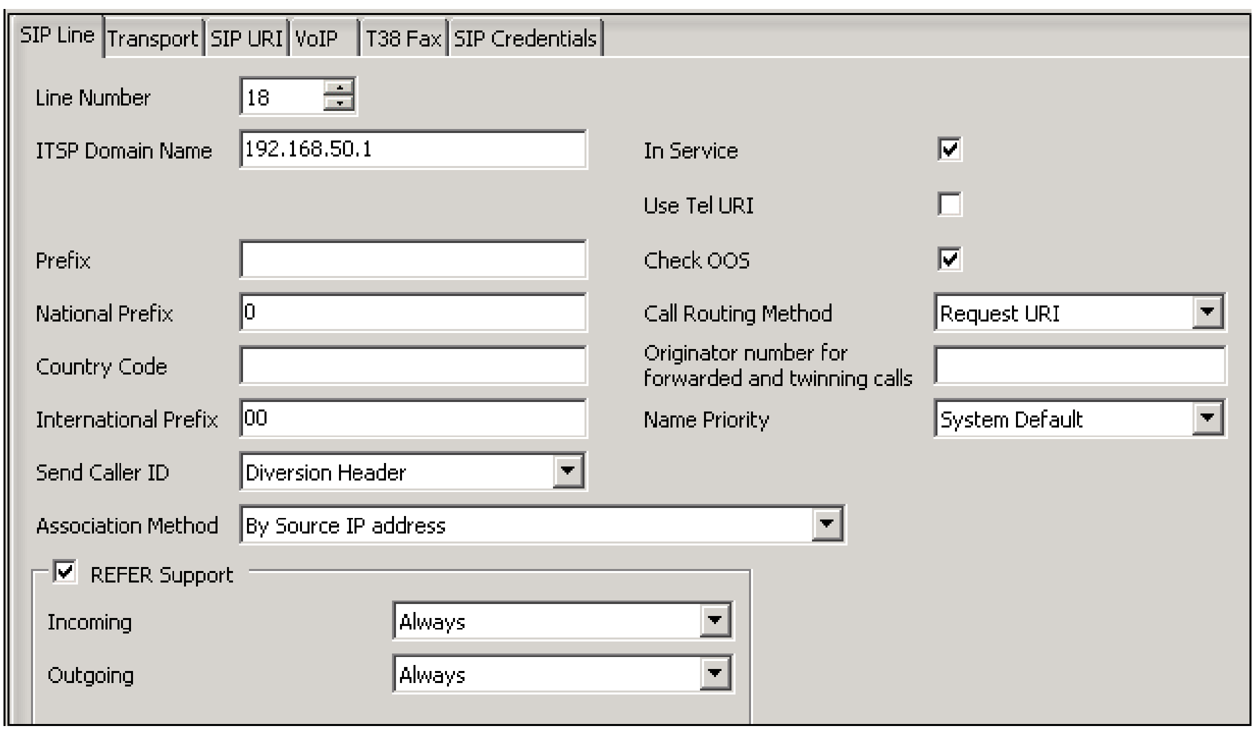


5.5. Administer SIP Line

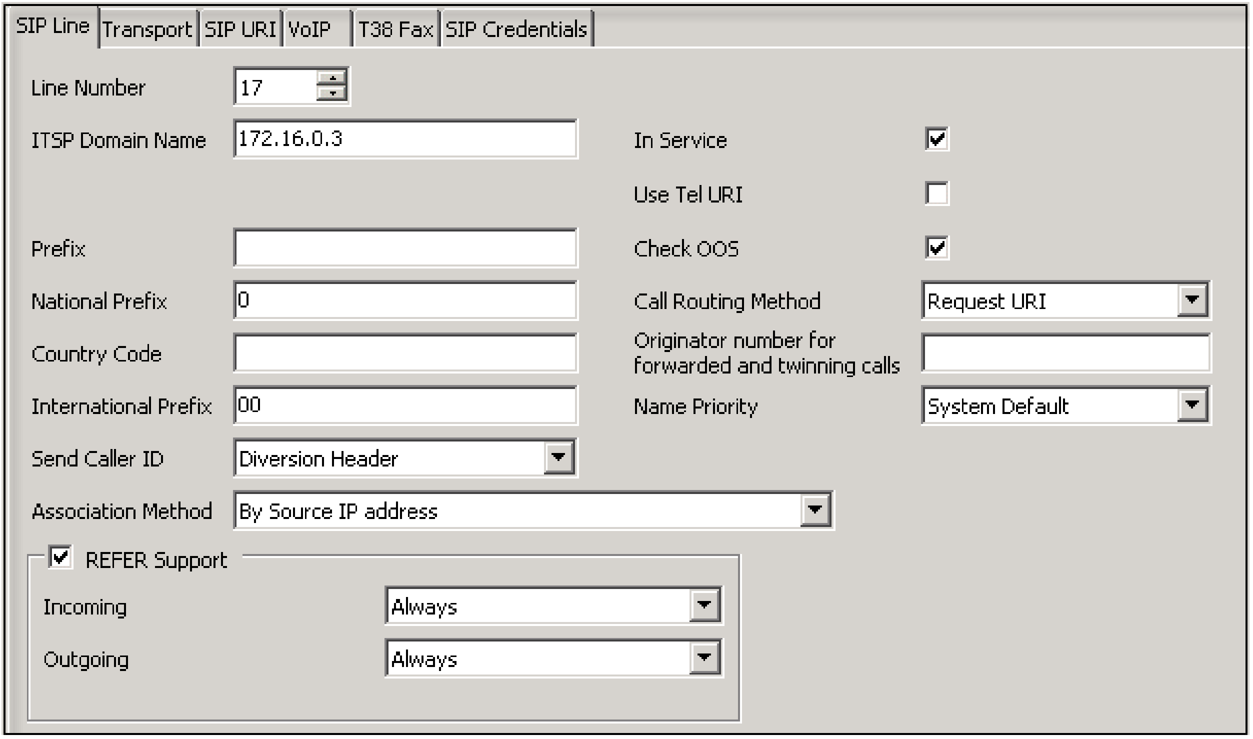
To create the SIP line which will connect the Main and Branch Offices, begin by navigating to **Line** in the Navigation Pane. Right-click and select **New →SIP Line**. On the **SIP Line** tab in the Details Pane, configure the parameters as shown below:

- Set the **ITSP Domain Name** to the IP address of the LAN 2 interface. IP Office will use this IP address as the host portion of the SIP URI in SIP headers, such as From headers, in messages sent to the network.
- Check the **In Service** box.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line
- Set **Send Caller ID** to **Diversion Header**. This field is only used if the **Send original calling party information for Mobile Twinning** box is unchecked in the **System → Twinning** tab. For twinning and call forwarding off-net calls, Avaya IP Office will include the Diversion header in the outbound SIP INVITE message, containing the number associated with the party originating the call.
- Check the **REFER support** box. Select **Always** for both **Incoming** and **Outgoing** to enable the IP Office to send REFER headers for transferred and forwarded calls that are routed back to the SIP Trunk.
- Default values may be used for all other parameters.

Main Site:



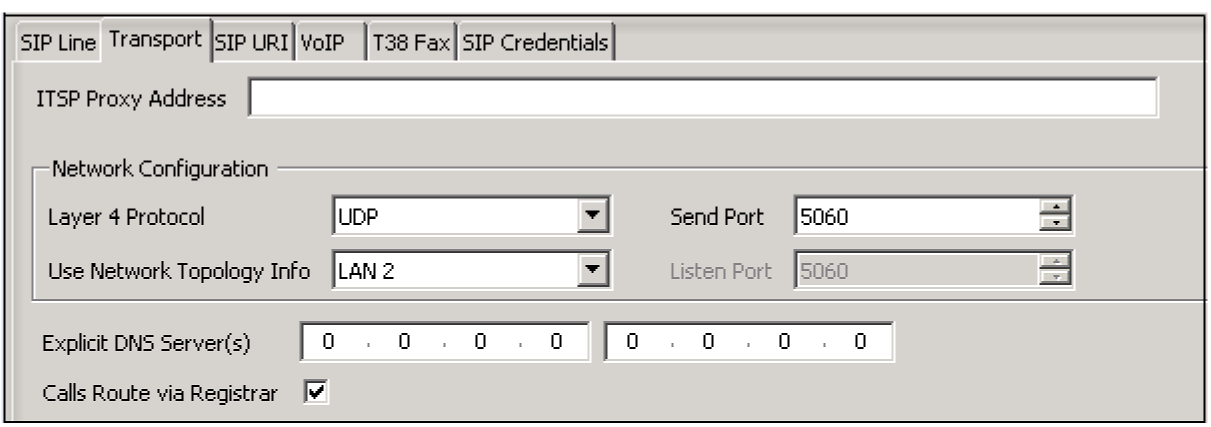
Branch Site:



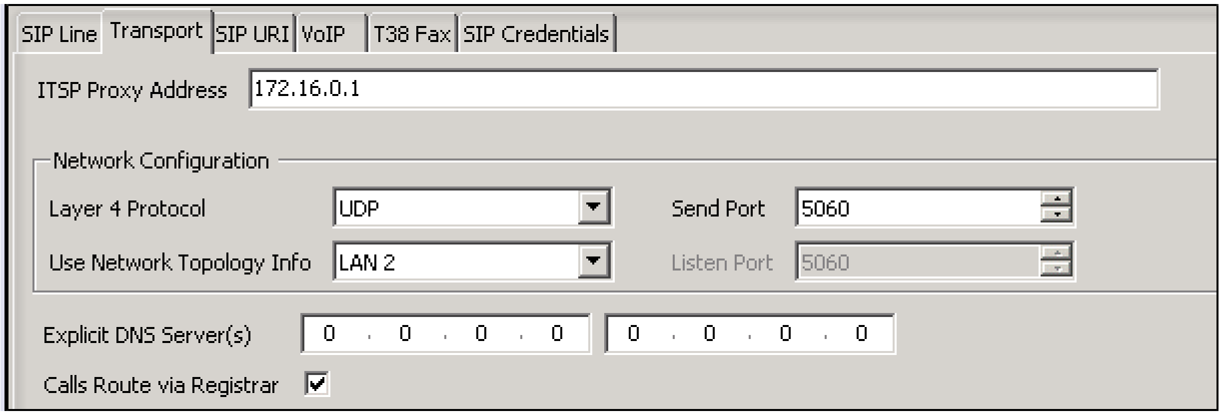
Select the **Transport** tab and set the following:

- Set the **ITSP Proxy Address** to the IP address of the trunk far-end proxy server.
- Set the **Layer 4 Protocol** to ***UDP***.
- Set **Use Network Topology Info** to ***LAN2***.
- Set the **Send Port** to **5060**.

For the IP Office at the Main site, the **ITSP Proxy Address** field is the IP address of the WAN ALG on the EdgeMarc. Leave this field blank for now. It will be revisited later in the configuration, after this value is defined in **Section 6.2.4** later in this document.



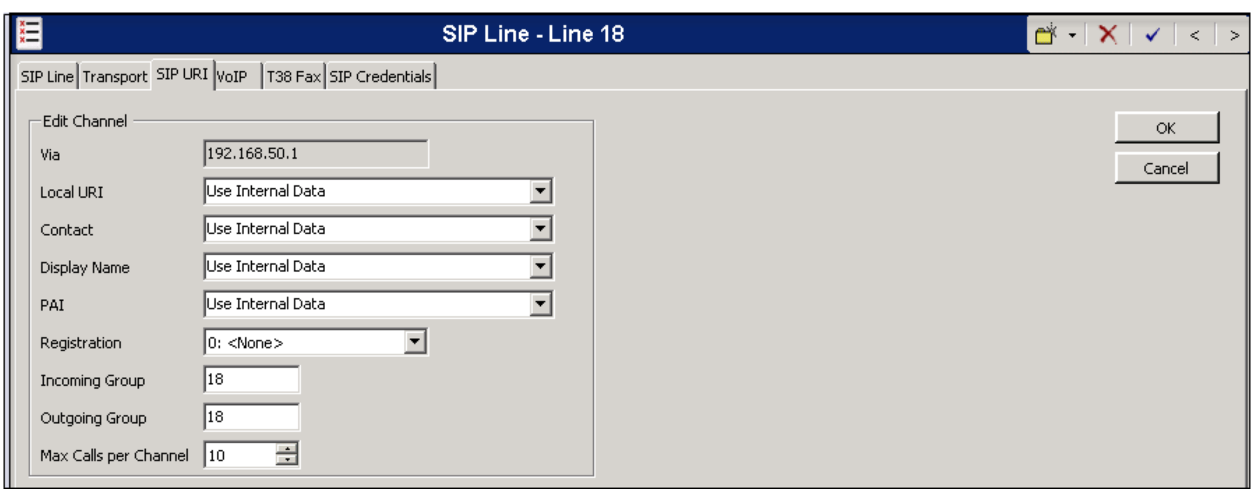
For the IP Office at the Branch site, on the **ITSP Proxy Address** field, enter the IP address of the LAN ALG on the EdgeMarc. This parameter is discussed further in **Section 6.2.1.**



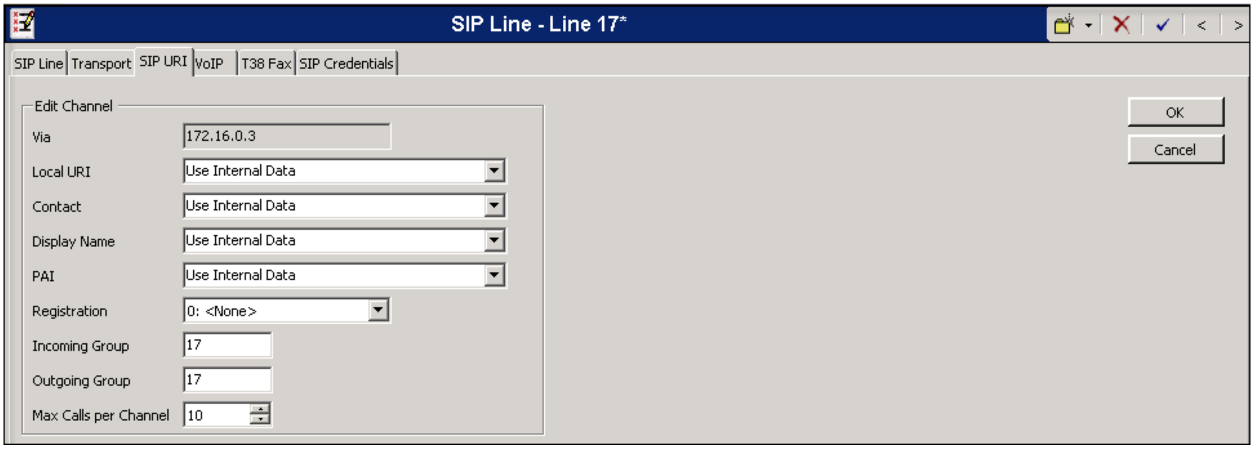
A SIP URI entry must be created for each number that is allowed to traverse the SIP trunk. To create a SIP URI entry, first select the **SIP URI** tab. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane. For the compliance test, a single SIP URI entry was created that matched any number assigned to an Avaya IP Office user. The entry was created with the parameters shown below.

- Set **Local URI**, **Contact, Display Name** and **PAI** to ***Use Internal Data***
- 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
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.

Main Site:

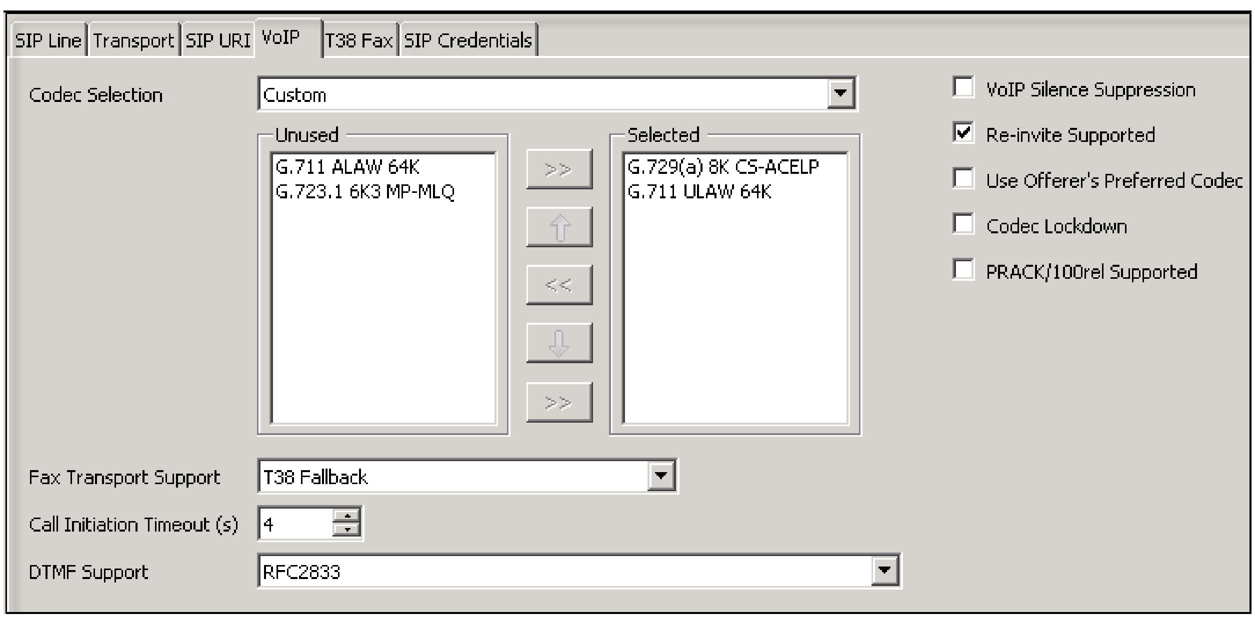


Branch Office:

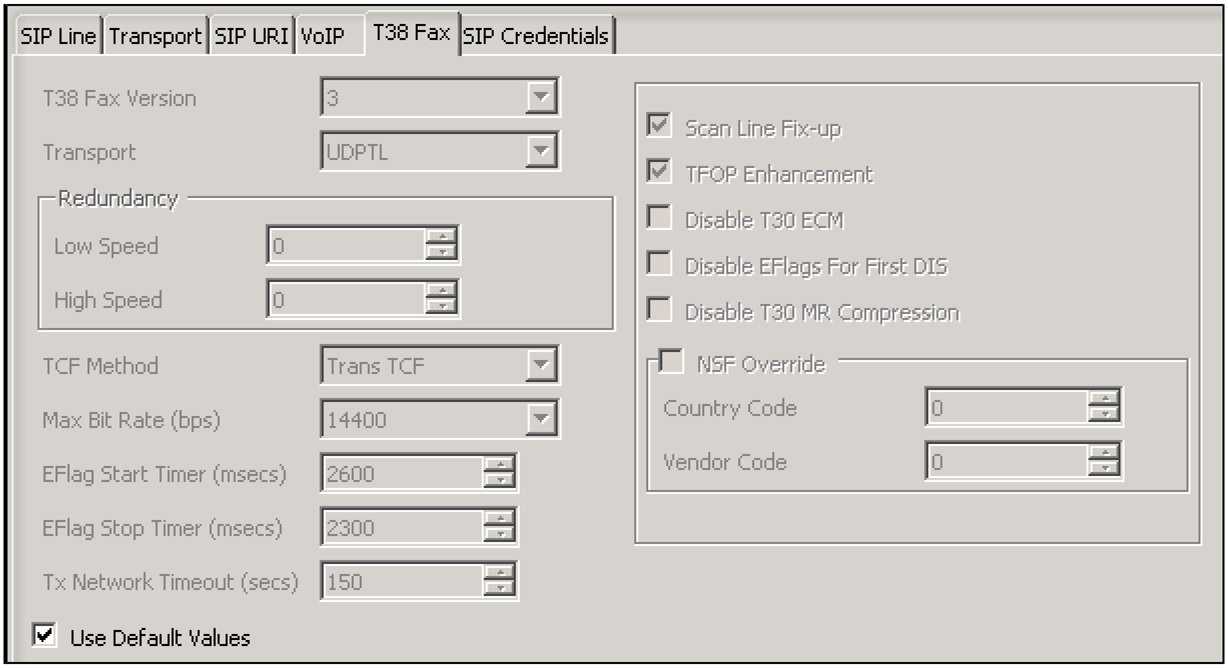


Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- In the sample configuration, the **Codec Selection** was configured using the "Custom" option, allowing an explicit ordered list of codecs to be specified. The buttons allow setting an explicit list of codecs to be used on the line, in that specific order of preference.
- For **Fax Transport Support**, select ***T38 Fallback.***
- Set the **DTMF Support** field to ***RFC2833***. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of an incoming call or transfer does not support the codec originally negotiated on the trunk.



Select the T38 Fax tab. Verify that **Use Default Values** is checked.



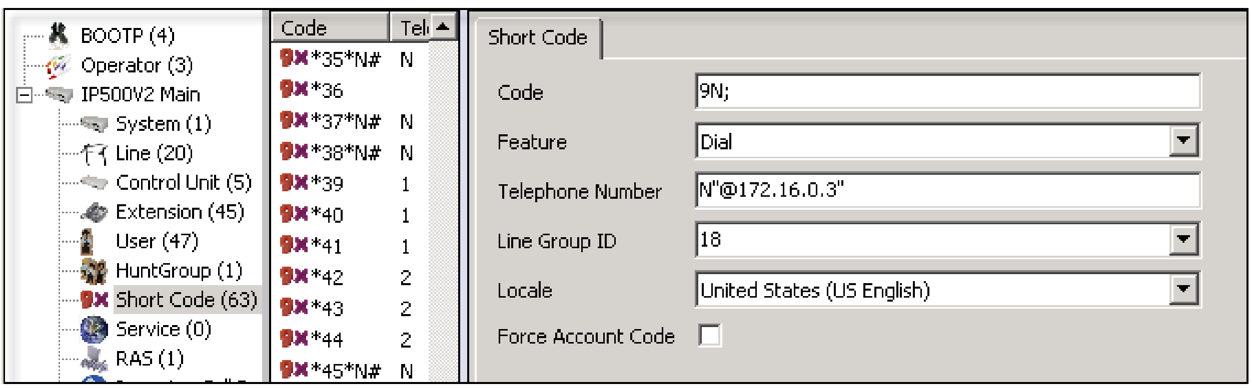
 Solution & Interoperability Test Lab Application Notes

5.6. Short Codes

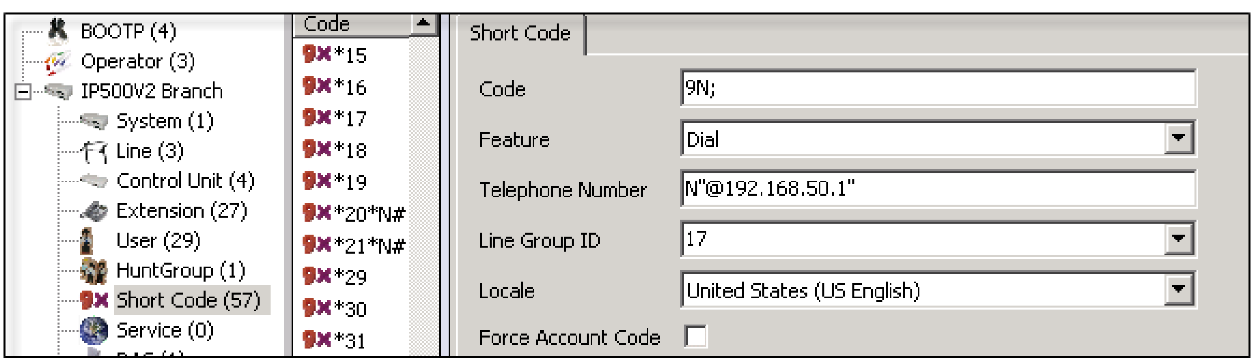
Define a short code to route outbound traffic to the SIP line. To create a short code, right-click on **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. In this case, ***9N;***. This short code will be invoked when the user dials 9 followed by any number.
- Set **Feature** to ***Dial***. This is the action that the short code will perform.
- Set **Telephone Number** to ***N"@<RemoteIP>"***. This field is used to construct the Request URI and To headers in the outgoing SIP INVITE message. The value ***N*** is the number dialed by the user. The value ***RemoteIP*** represents the IP address of the far-end IP Office LAN2 interface.
- Set the **Line Group Id** to the outgoing line group number defined on the **SIP URI** tab on the **SIP Line**. This short code will use this line group when placing outbound calls.
- Default values may be used for all other parameters.

Main Site:



Branch Office:

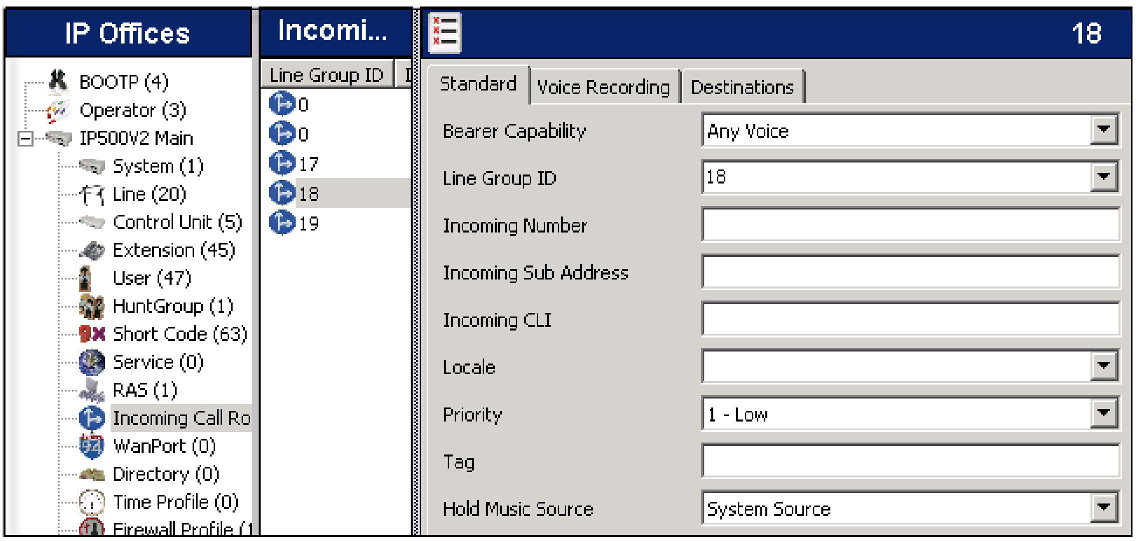


5.7. Incoming Call Routing

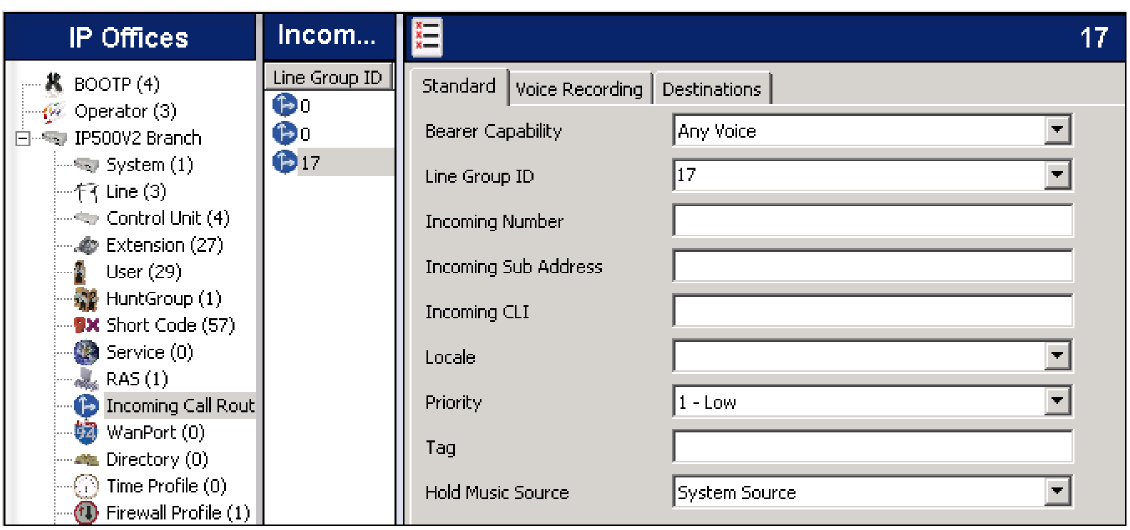
Incoming call routes map inbound calls on a specific line to internal extensions, hunt groups, short codes, voicemail, etc. in the IP Office. In a scenario like the one used for the compliance test, only one incoming route is needed, which allows any incoming number arriving on the SIP trunk to reach any extension in IP Office. On the left Navigation Pane, right-click on **Incoming Call Route** and select **New.** On the Details Pane, under the **Standard** tab, set the parameters as show bellow:

- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5**.
- Default values may be used for all other parameters.

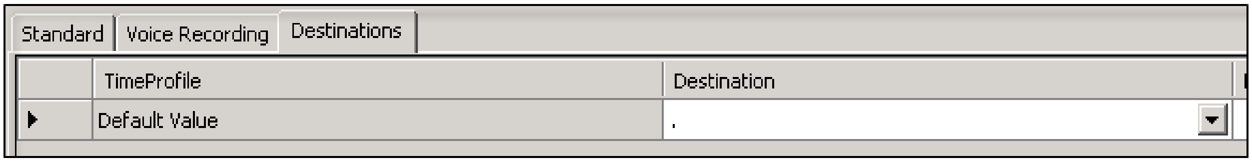
Main site:



Branch Office:



Under the **Destinations** tab, enter "**.**" as the **Default Value**. This will enable all incoming calls to be routed to any user in the IP Office.



5.8. Save Configuration

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

6. Configure the EdgeProtect and EdgeMarc Session Border Controllers

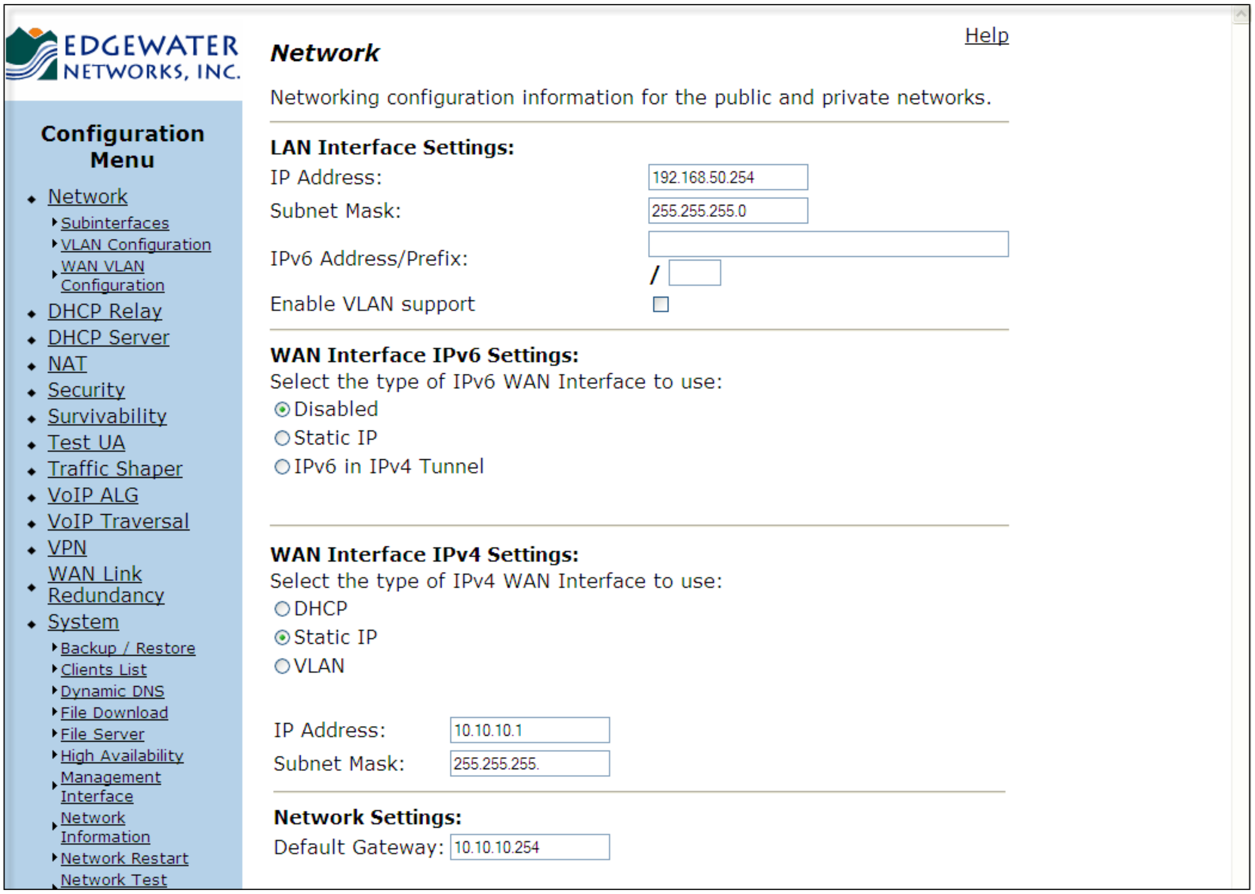
This section describes the configuration steps for the EdgeProtect and the EdgeMarc Session Border Controllers, in order to implement the test configuration shown on **Figure 1**. All the screens and configuration settings presented in the next sections of this document have the purpose of simply illustrate the sample configuration used during the compliance test, and are not intended to be prescriptive.

6.1 EdgeProtect Configuration

Connect a PC to the **Port 1** interface in the front of the EdgeProtect. Establish a browser connection to the default IP address of 192.168.1.1, subnet mask 255.255.255.0. Login using the proper credentials.

6.1.1. Network Settings

Choose **Network** from the **Configuration Menu**. Enter the settings under the **LAN Interface Settings** and **WAN Interface IPv4 Settings** sections as appropriate.



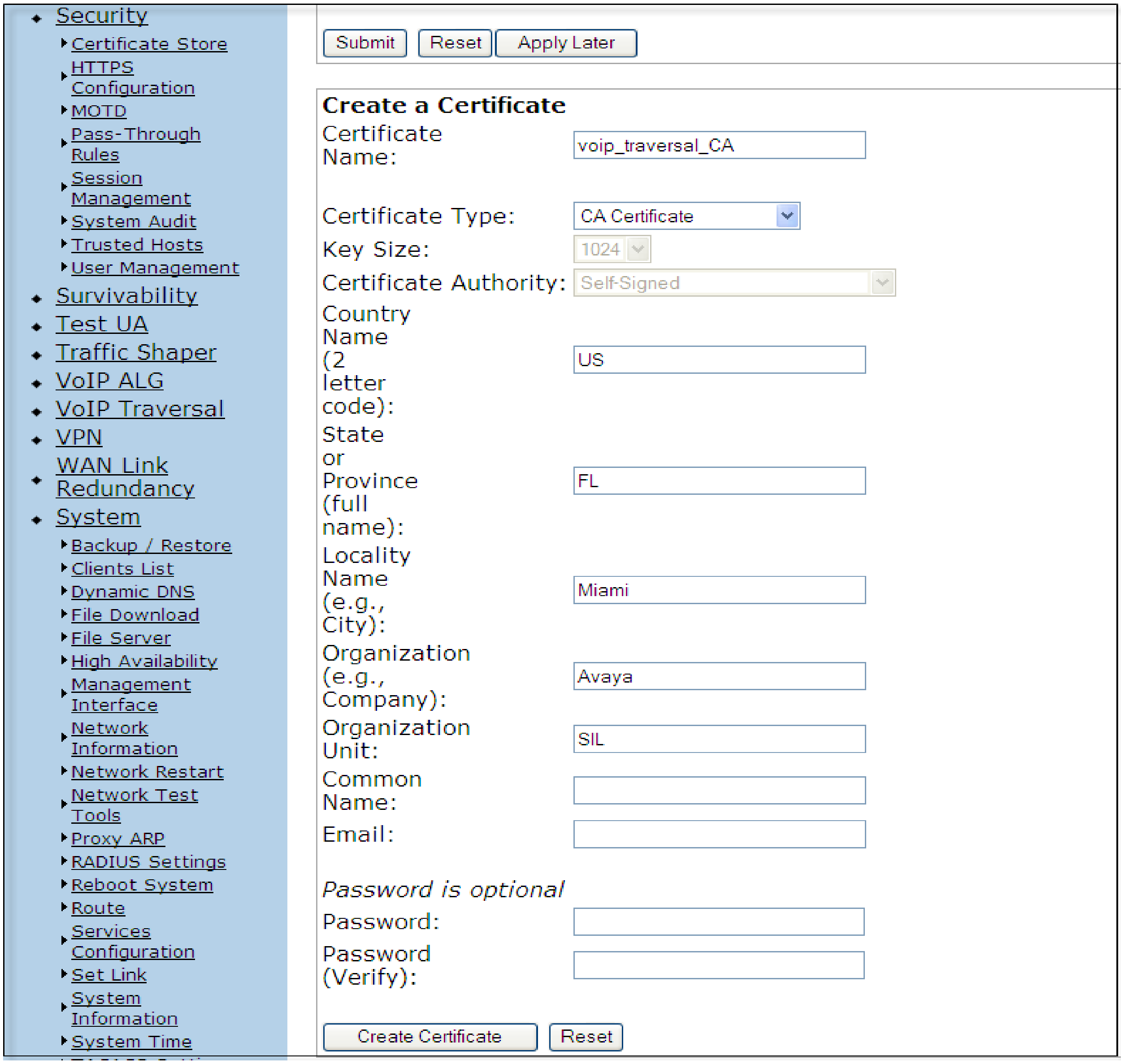
6.1.2. TLS Certificates

Three certificates are needed for the VoIP Traversal feature to function:

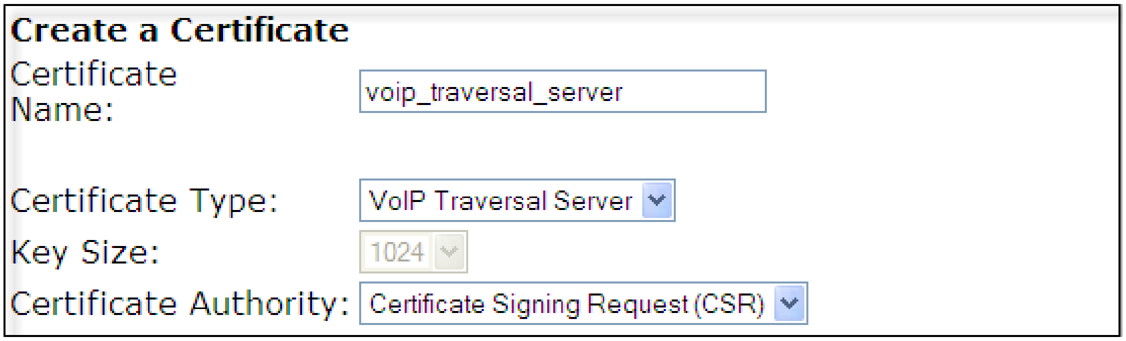
- A Certificate Authority (CA) certificate, used to sign other certificates. This is needed in both the server and the client.
- VoIP Traversal Server - A certificate used by a VoIP Traversal server (EdgeProtect)
- VoIP Traversal Client - A certificate used by a VoIP Traversal client (EdgeMarc)

The Certificate Store contains the certificates for use by the VoIP Traversal. Once these certificates are created on the server, the CA and the client certificates and keys can be downloaded and saved to the local PC. They will need to be uploaded to the client later in the EdgeMarc configuration section.

On the **Configuration Menu**, select **Security → Certificate Store.** To create the CA certificate, enter the name and select **CA Certificate** under the **Certificate Type** pull-down menu. Enter all others parameters as appropriate. Click **Create Certificate**.

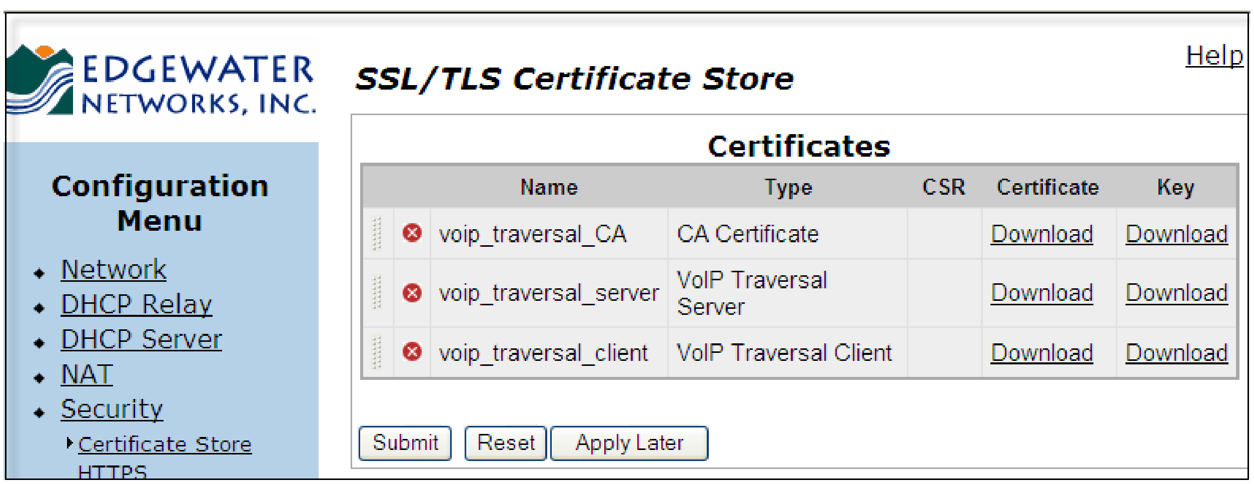


Create a certificate for the server. Enter the **Certificate Name**. Choose **VoIP Traversal Server** from the pull-down menu under **Certificate Type**. Enter all others parameters as appropriate. Click **Create Certificate** (not shown).



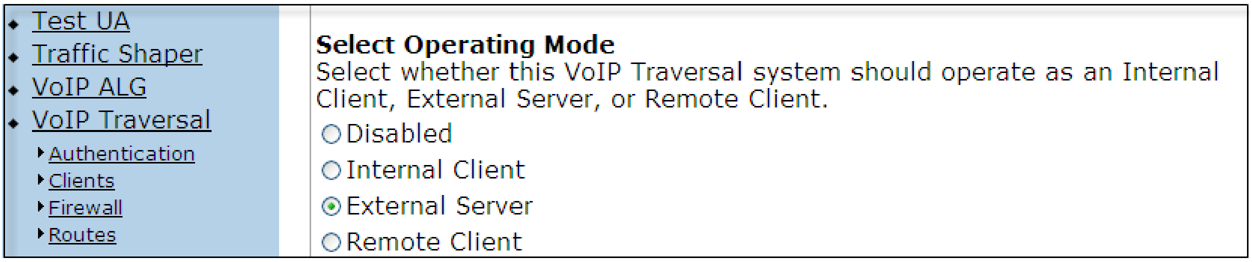
Similarly, create the certificate for the client. Select **VoIP Traversal Client** from the pull-down menu under **Certificate Type**. Enter all others parameters as appropriate. Click **Create Certificate** (not shown).

After creating all three certificates, click the **Submit** button. The complete list is shown.

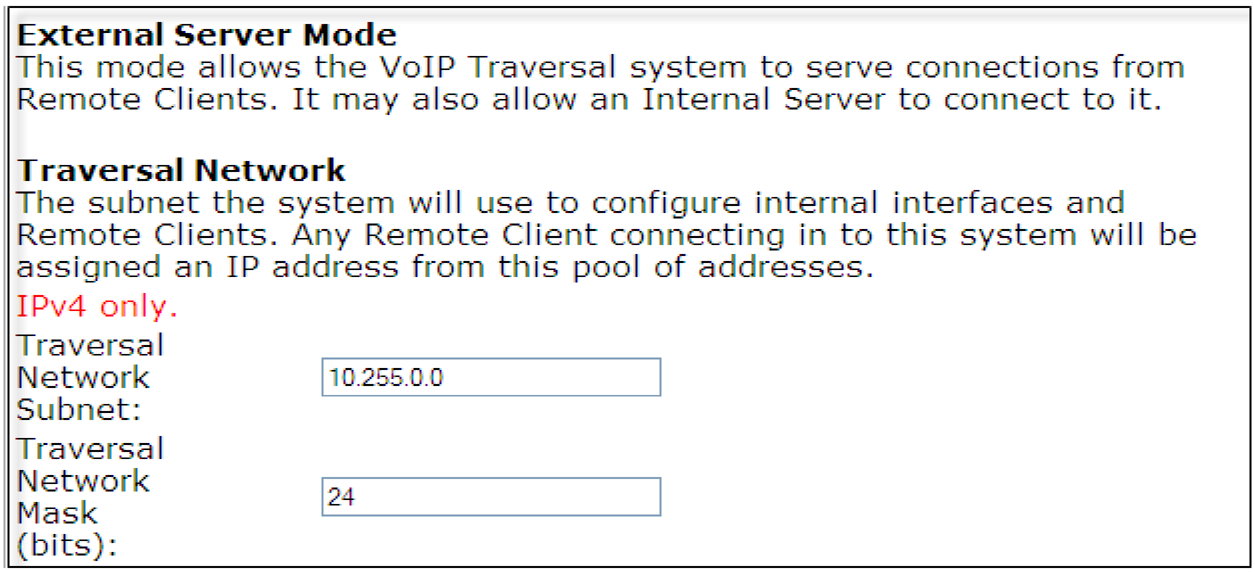


6.1.3. VoIP Traversal

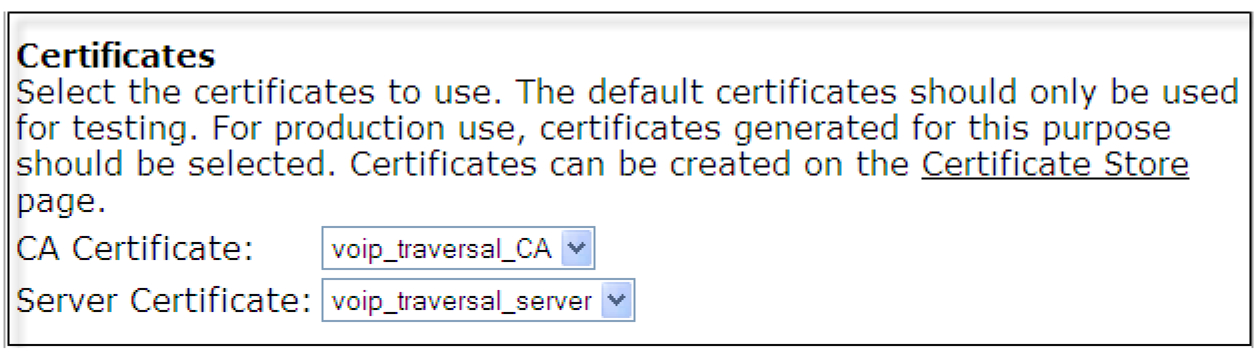
On the **Configuration Menu**, select **VOIP Traversal.** Choose **External Server** under **Select Operating Mode**.



On the same screen, enter the subnet and mask to be used in the traversal network.



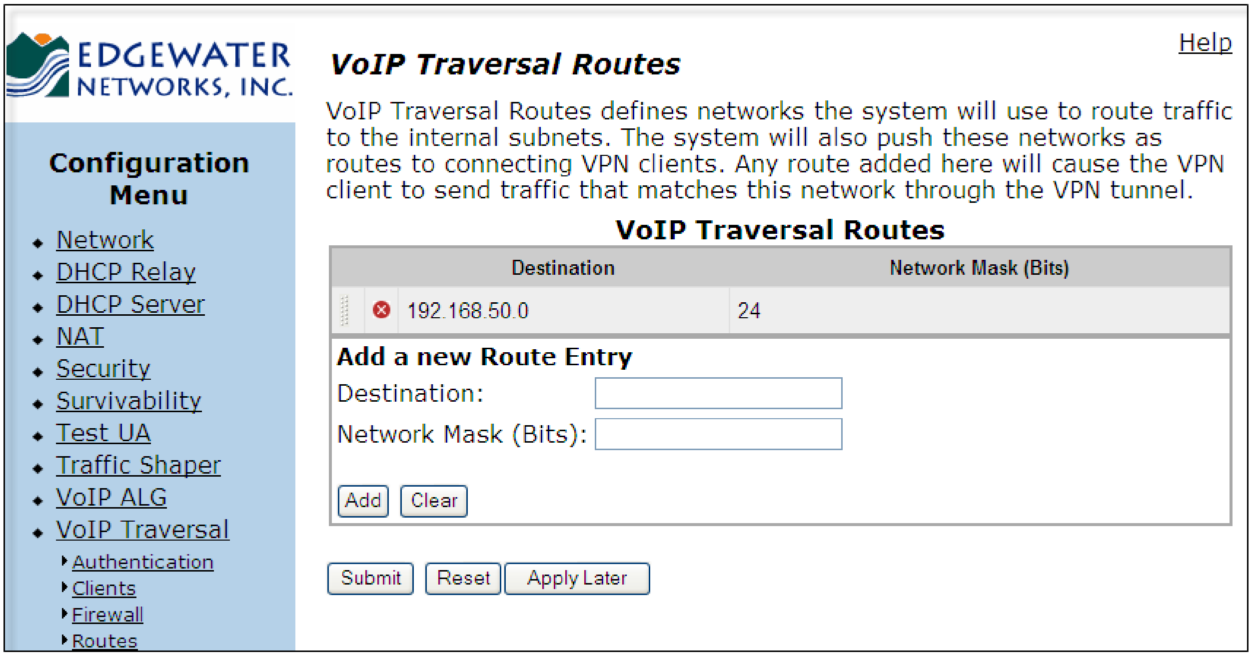
Further down on the screen, choose the TLS certificates to be used on the server:



Click **Submit** (not shown).

Select the **VoIP Traversal → Routes** submenu. Enter the following:

- **Destination**: Local subnet where VoIP traffic is going to be routed (**192.168.50.0**)
- **Network Mask (Bits)**: **24**
- Click **Submit.**

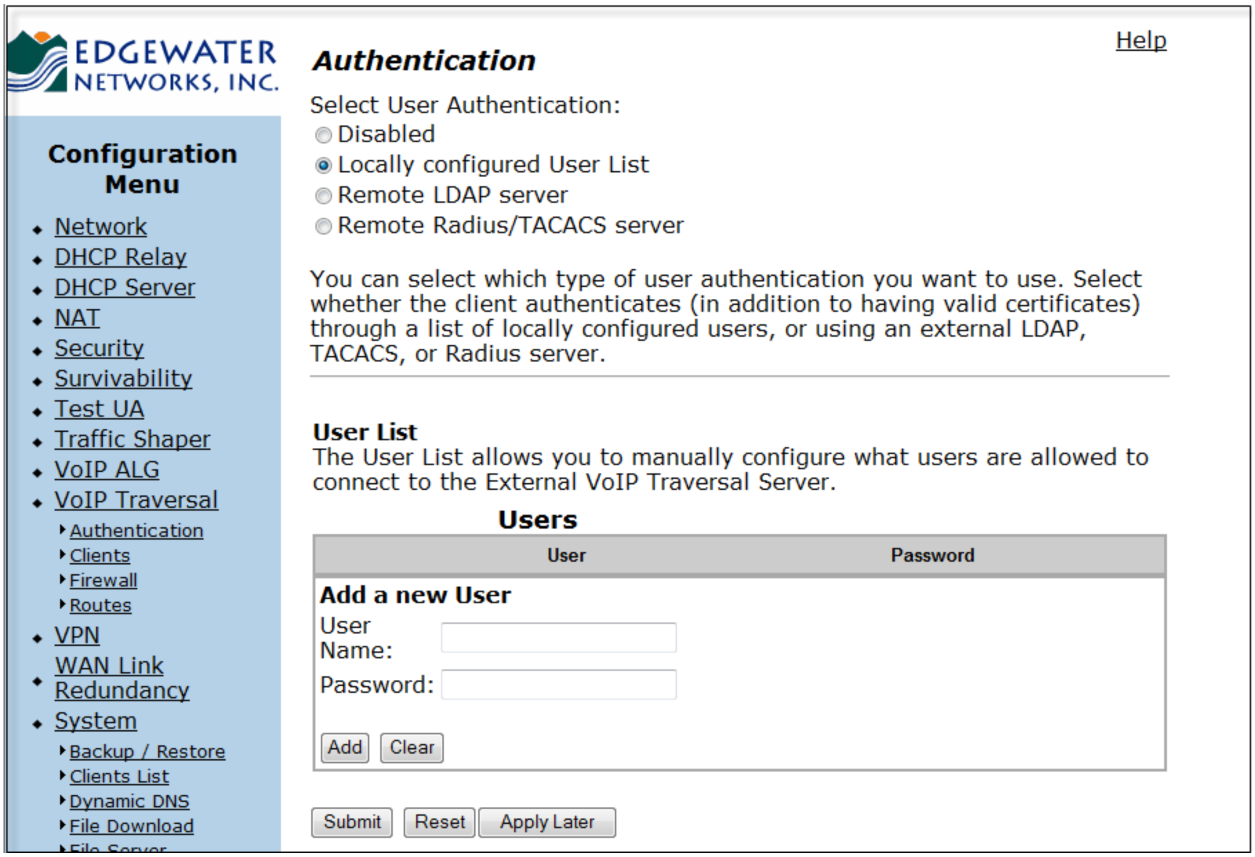


6.1.4. Authentication.

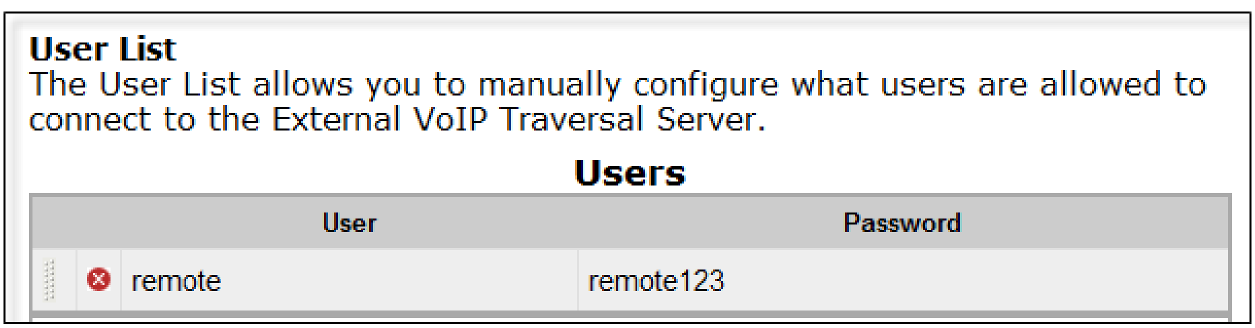
The Authentication page allows selecting the type of authentication to be used for connecting VoIP Traversal clients. A local user list will be used, containing a set of credentials needed to allow the connection of the remote EdgeMarc.

On the **Configuration Menu**, select **VOIP Traversal → Authentication.**

- Check **Locally configured User List**
- On the **Users** section, enter the username and password assigned to the EdgeMarc.



- Click **Add** and **Submit**. The screen below shows the user created in the test configuration.

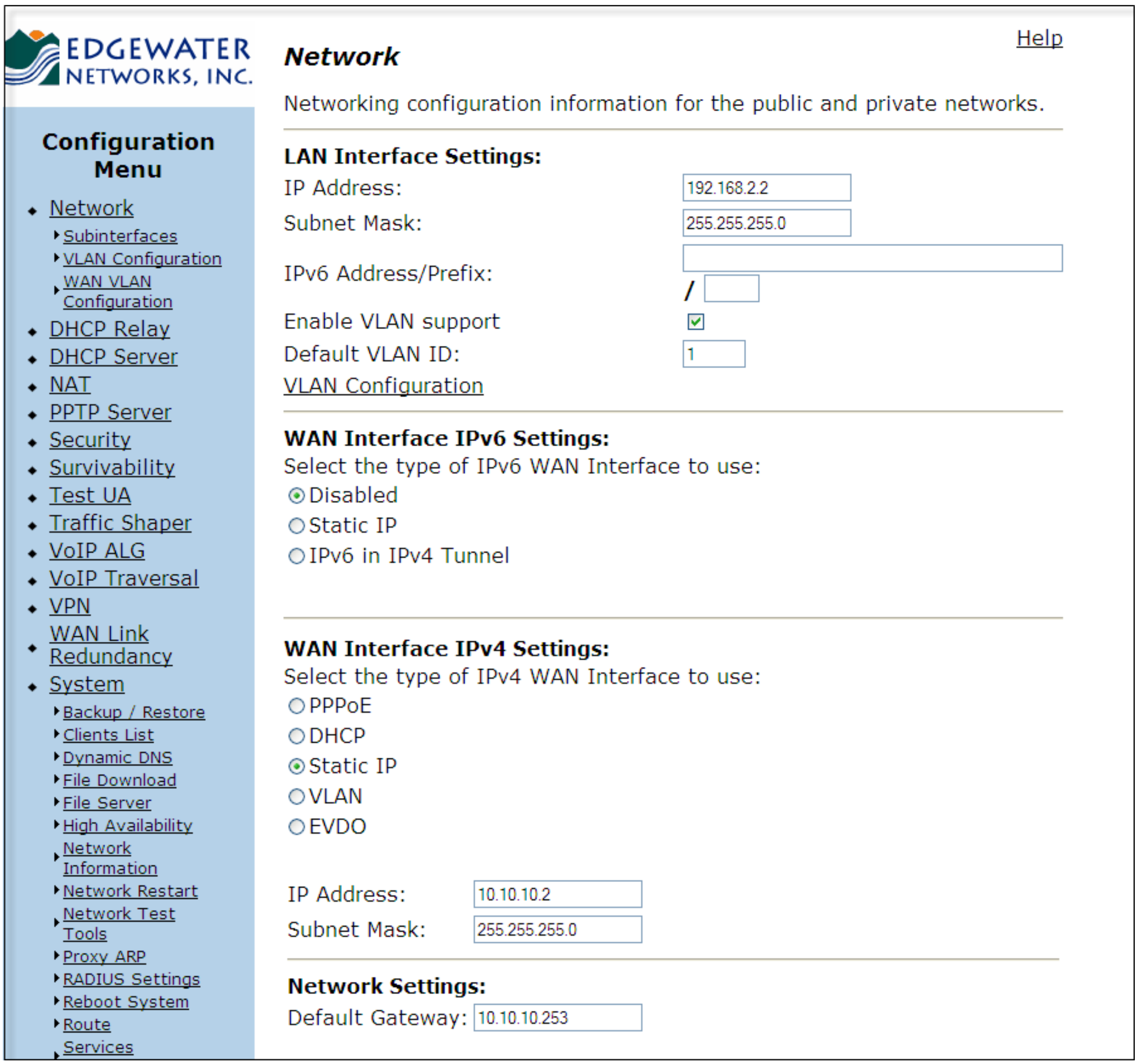


6.2 EdgeMarc Configuration.

Connect a PC to the **Port 1** interface in the back of the EdgeMarc. Establish a browser connection to the default IP address of 192.168.1.1, subnet mask 255.255.255.0.
Login using the proper credentials.

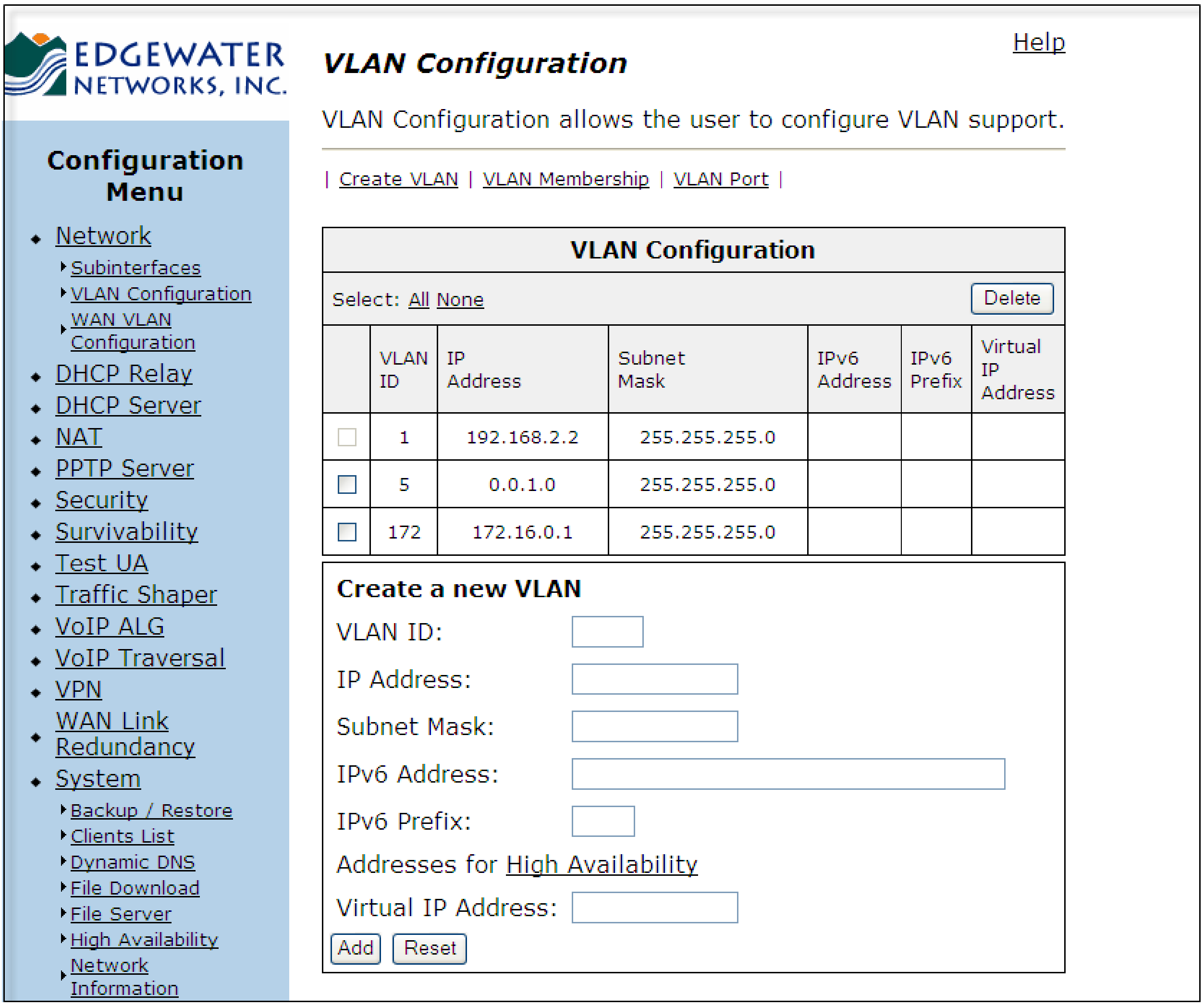
6.2.1. Network Settings

Choose **Network** from the **Configuration Menu**. Enter the settings under **LAN Interface Settings** and **WAN Interface IPv4 Settings** sections as appropriate. Make sure to check the **Enable VLAN support** box.



From the **Configuration Menu** select **Network → VLAN Configuration.**

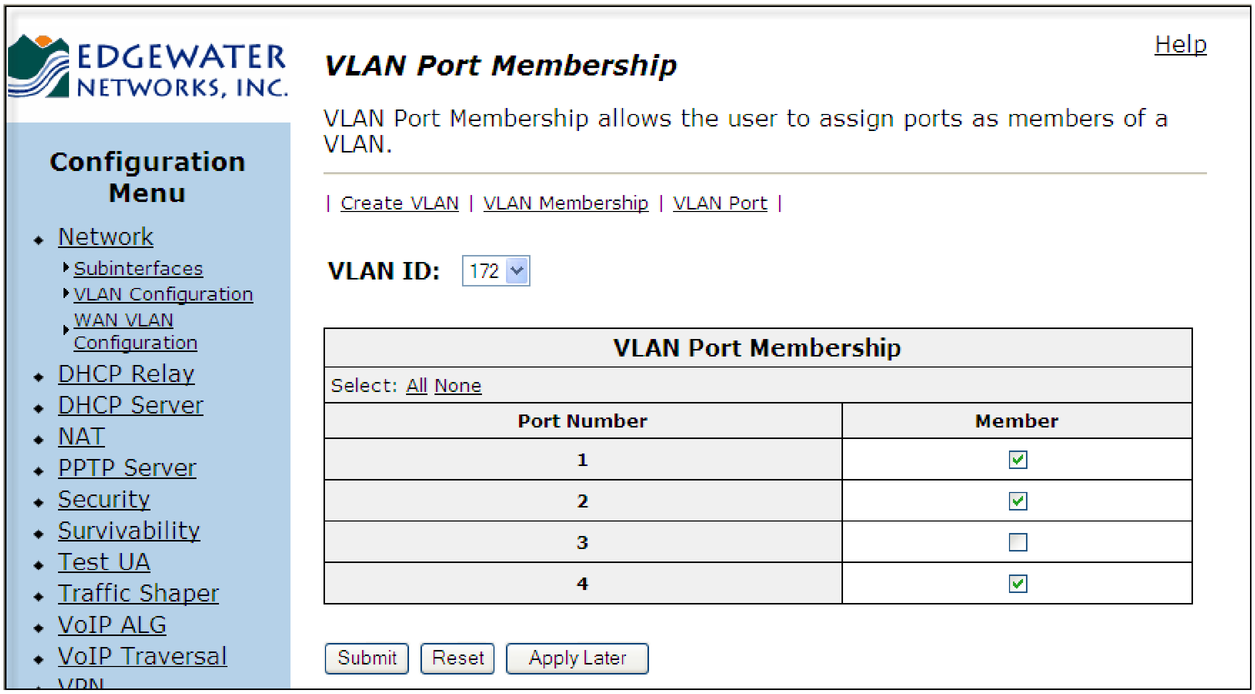
The following screen shows the list of all VLANs on the EdgeMarc. For the compliance test, VLAN **1** was the default native VLAN, and VLANs **5** and **172** were manually created using the **Create a New VLAN** section. They were needed for the Application Layer Gateway feature used in this configuration to be able to work together with the VoIP Traversal and TLS encryption.



For the test configuration, any IP address could have been assigned to VLAN 5, since its use is internal and limited to segregate the ALG traffic in the LAN side of the EdgeMarc from the VoIP Traversal traffic going to the network. No physical ports were assigned to this VLAN.

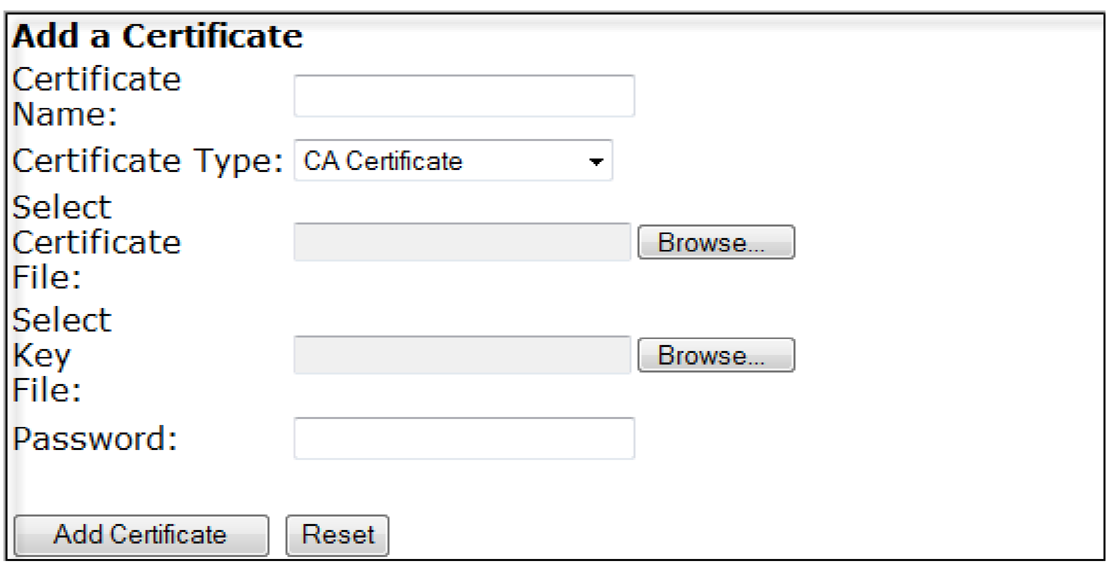
The local IP Office is connected to port 1 of the EdgeMarc. Assigning the IP address 172.16.0.1 to VLAN 172 makes this the LAN side ALG address of the EdgeMarc. This value matches the IP address used in the **ITSP Proxy Address** field, in the configuration of the SIP Line in the IP Office at the Branch Office, earlier on **Section 5.5**.

To assign the ports to a VLAN, select **VLAN Membership** on the **VLAN Configuration** screen on the previous page. The following screen shows the port membership for VLAN **172**. Ports **1**, **2** and **4** were assigned to it.



6.2.2. TLS Certificates

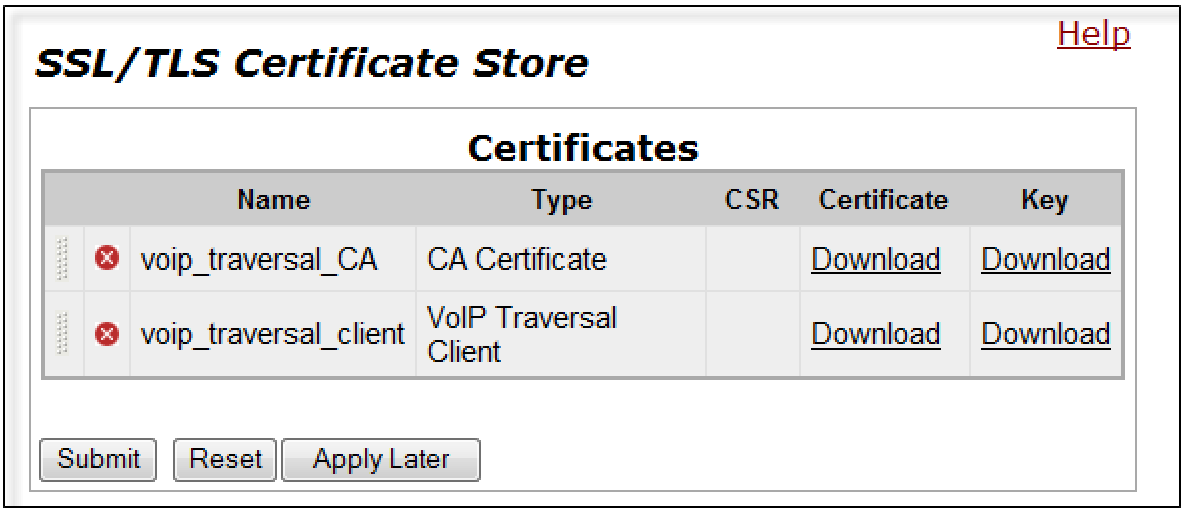
The Certificate Store of the EdgeMarc should contain the CA and VoIP Traversal Client certificates that were previously created and saved in **Section 6.1.2.** On the **Configuration Menu**, select **Security → Certificate Store.** Use the **Add a Certificate** section at the bottom of the screen to upload the CA and Client certificates and keys from the local PC.



Complete the following:

- **Certificate Name:** Enter the name of the certificate
- **Certificate Type:** The type of the certificate (**CA Certificate** or **VoIP Traversal Client**)
- **Select Certificate File:** browse to the certificate file that was saved in the local PC
- **Select Key File:** browse to the key file that goes with the certificate, previously saved in the PC
- **Password**: no password is required for VoIP Traversal
- Click **Add Certificate**

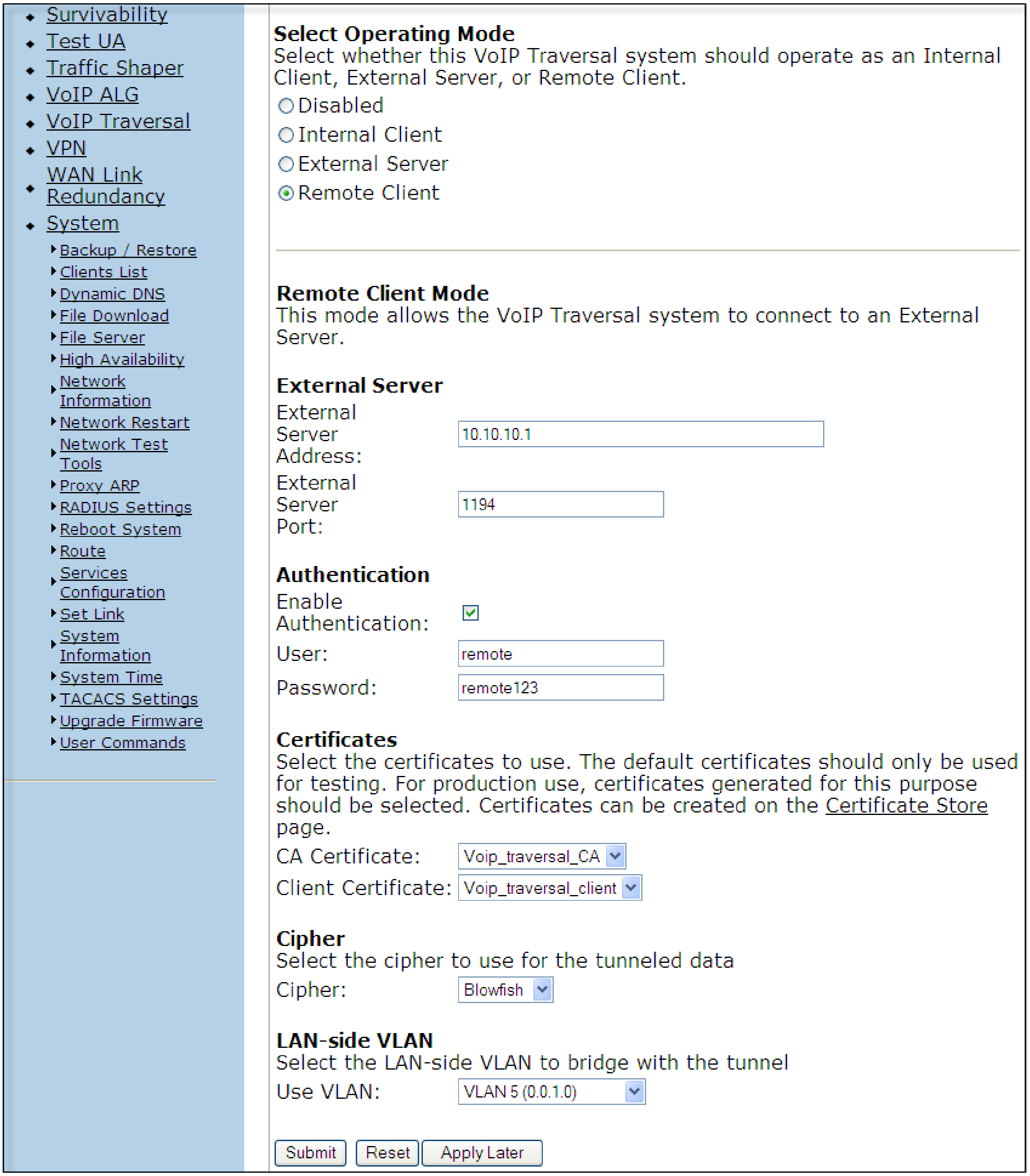
Once the two certificates are uploaded, click **Submit**.



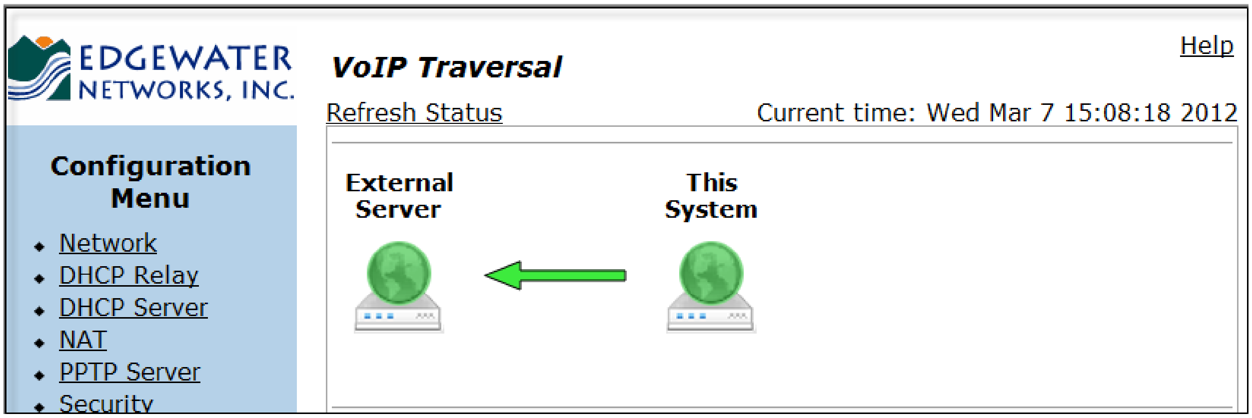
6.2.3. VoIP Traversal

On the **Configuration Menu**, select **VOIP Traversal.** Enter the following parameters:

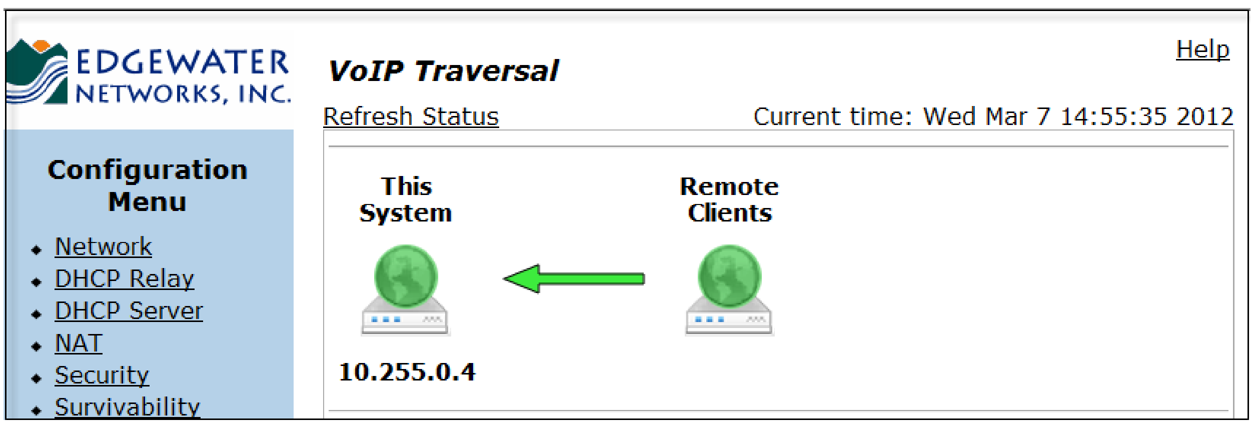
- **Select Operating Mode: Remote Client**
- **External Server Address:** enter the IP address of the WAN interface of the EdgeProtect
- Check the **Enable Authentication** box
- Enter the User and Password created in **Section 6.1.4**
- **Certificates**: choose the CA and Client certificates to be used.
- **LAN side VLAN**: select **VLAN 5** from the drop-down menu.
- Click **Submit**


Survivability
Test UA
Traffic Shaper
VoIP ALG
VoIP Traversal
VPN
WAN Link Redundancy
System
Backup / Restore
Clients List
Dynamic DNS
File Download
File Server
High Availability
Network Information
Network Restart
Network Test Tools
Proxy ARP
RADIUS Settings
Reboot System
Route
Services Configuration
Set Link
System Information
System Time
TACACS Settings
Upgrade Firmware
User Commands
Select Operating Mode
Select whether this VoIP Traversal system should operate as an Internal Client, External Server, or Remote Client.
Disabled
Internal Client
External Server
Remote Client
Remote Client Mode
This mode allows the VoIP Traversal system to connect to an External Server.
External Server
External Server Address:
10.10.10.1
External Server Port:
1194
Authentication
Enable Authentication:
User:
remote
Password:
remote123
Certificates
Select the certificates to use. The default certificates should only be used for testing. For production use, certificates generated for this purpose should be selected. Certificates can be created on the Certificate Store page.
CA Certificate:
Voip_traversal_CA
Client Certificate:
Voip_traversal_client
Cipher
Select the cipher to use for the tunneled data
Cipher:
Blowfish
LAN-side VLAN
Select the LAN-side VLAN to bridge with the tunnel
Use VLAN:
VLAN 5 (0.0.1.0)
Submit
Reset
Apply Later

At this point, after all the settings in the previous pages have been submitted, the VoIP Traversal between the EdgeMarc and the EdgeProtect should become operational. The status of the VoIP Traversal, as seen from the EdgeMarc, is shown at the top of the page. The symbols should be green, as shown in the following screen:



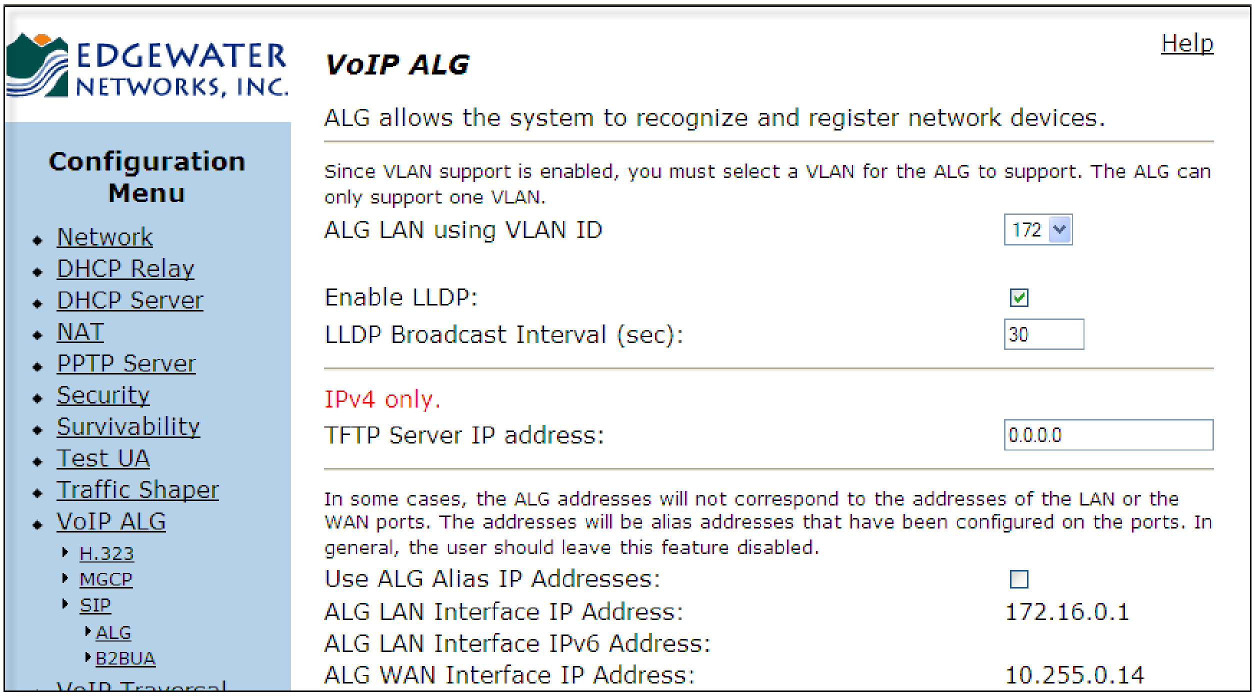
Similarly, the status of the VoIP Traversal can be checked from the Main Site. Login again to the EdgeProtect and select **VOIP Traversal** from the **Configuration Menu**. The screen should look like this:



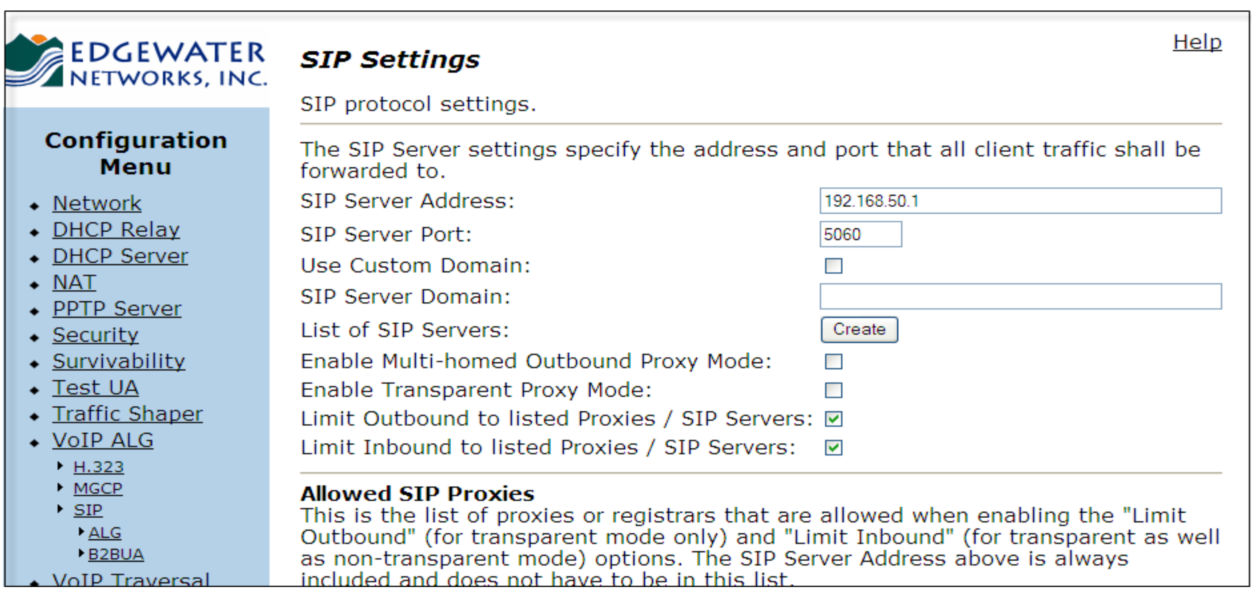
The IP address 10.255.0.4 is automatically assigned to the server during the setup process of the traversal subnet. This address is not part of the DHCP pool, and it will not change. The address will be used later in **Section 6.3** to setup static routes on the EdgeMarc.

6.2.4. VoIP Application Layer Gateway

On the **Configuration Menu**, select **VoIP ALG**. Choose **172** from the drop-down menu under **ALG LAN using VLAN ID.** Take note of the IP address under **ALG WAN Interface IP Address**. This address is assigned automatically, and this value should be entered as the **ITSP Proxy Address** in the configuration of the SIP Line in the IP Office at the Main Site, as mentioned in **Section 5.5**. See note in **Section 2.2** for additional comments about this parameter.

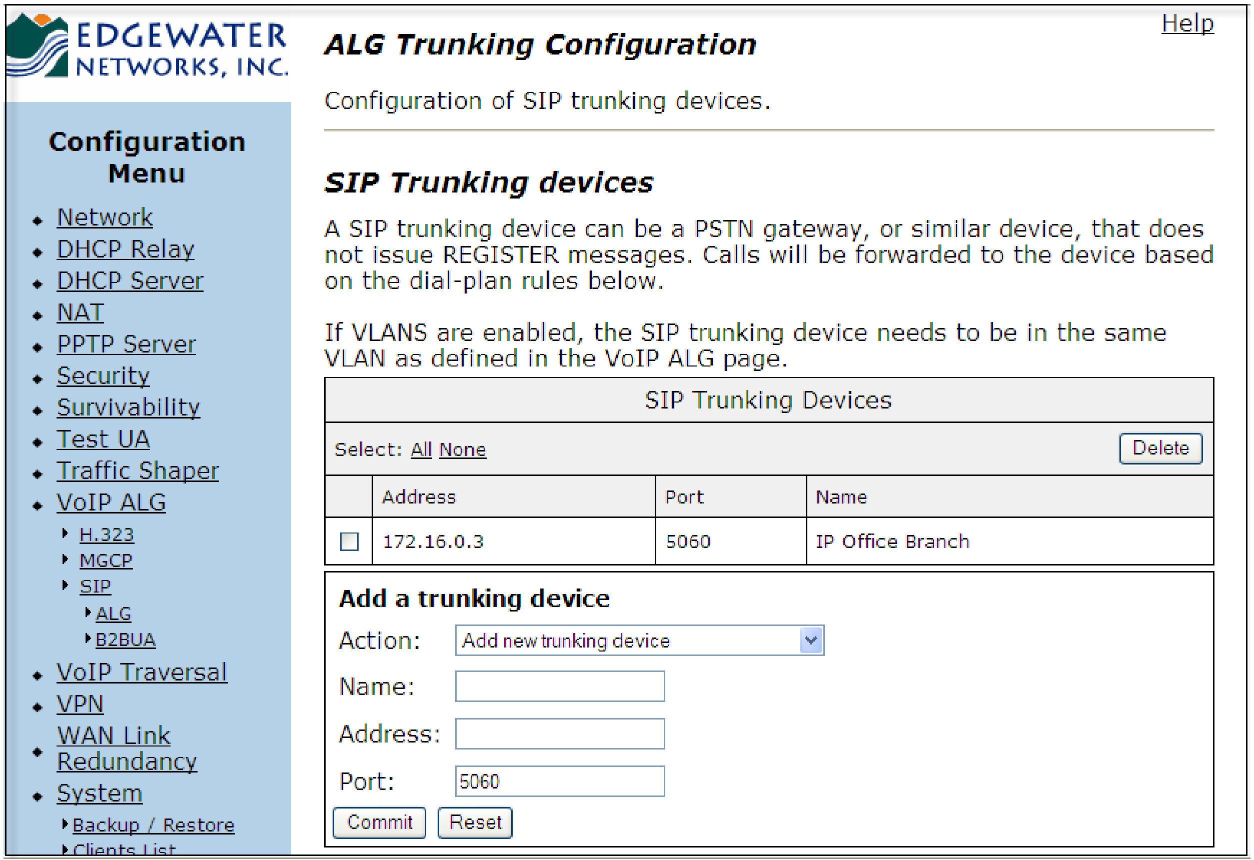


On the **VoIP ALG → SIP** submenu, under **SIP Server Address**, enter the IP address of the LAN 2 interface of the IP Office at the Main Site. Enter **5060** for **SIP Server Port**.



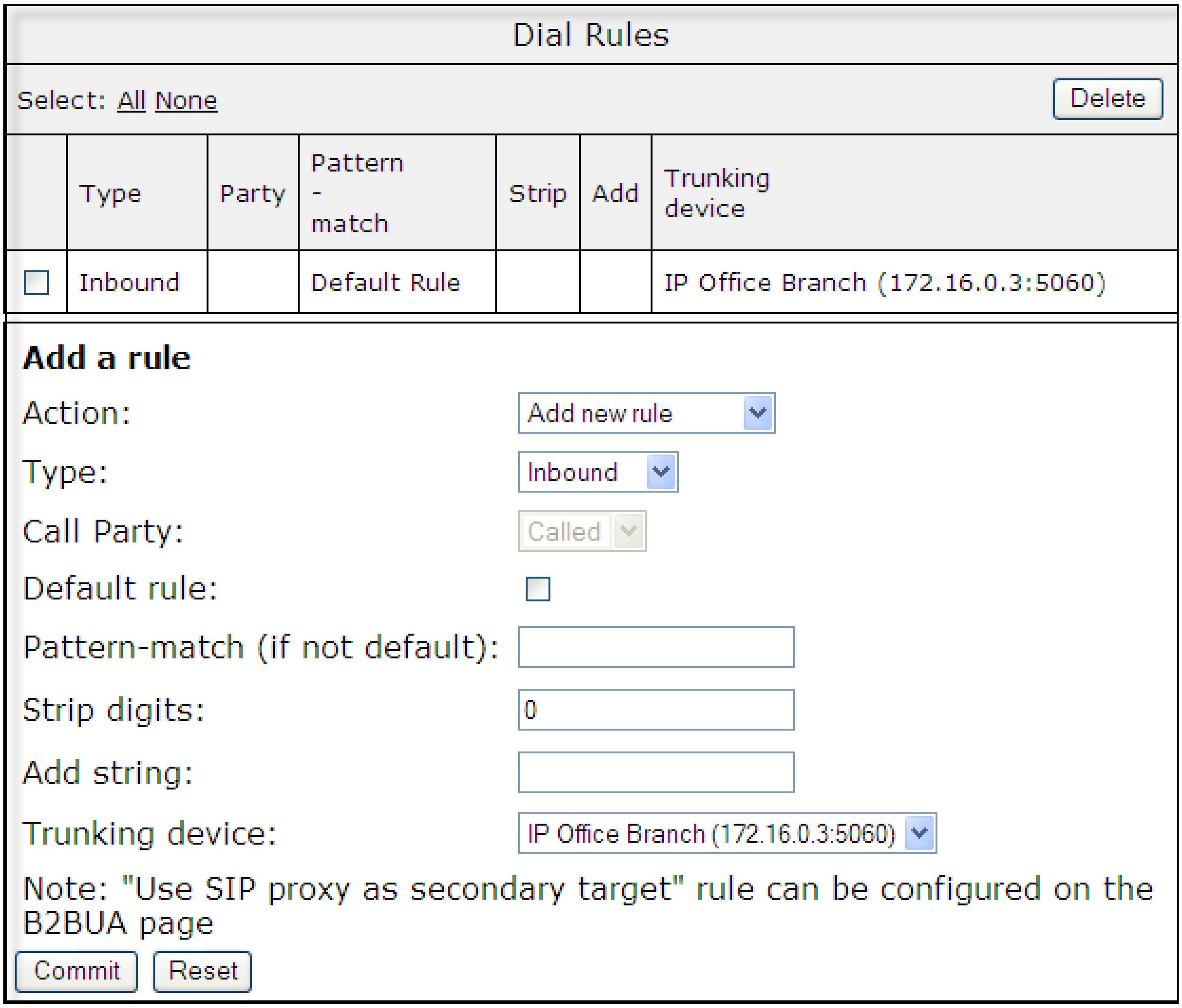
Select the **VoIP ALG → SIP → ALG** submenu**.** This brings up the **ALG Trunking Configuration** screen. In the **Add a trunking device section**, enter the following:

- **Action**: select **Add a new trunking device**
- **Name**: **IP Office Branch** was used.
- **Address**: IP address of the LAN 2 interface of the IP Office at the Branch Site.
- **Port**: **5060**
- Click **Commit.**



Back in the **ALG Trunking Configuration** page, under the **Rules** section, apply the default inbound rule for the trunking device:

- **Action**: **Add new rule**
- **Type: Inbound**
- Check the **Default rule** box.
- **Trunking device**: select the trunking device created previously.
- Click **Commit**.

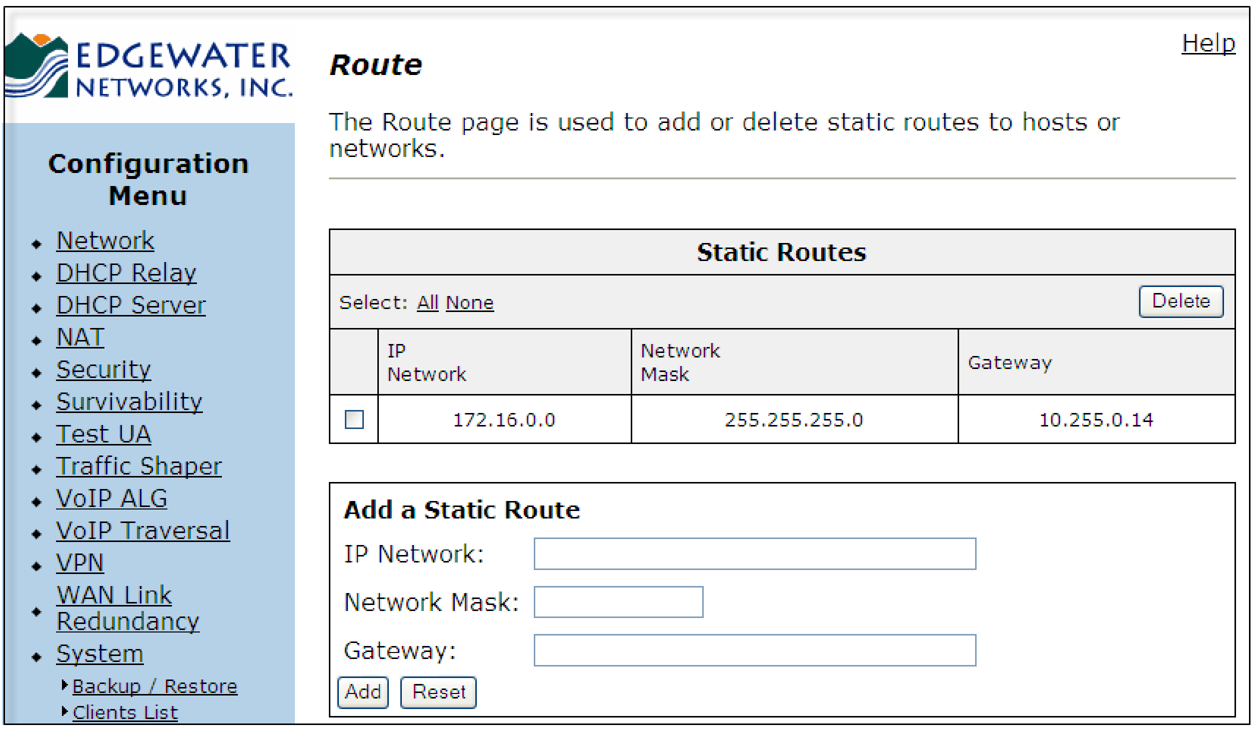


6.3. Static Routes

Static routes need to be created in both the EdgeProtect and EdgeMarc to be able to reach the networks at the far ends.

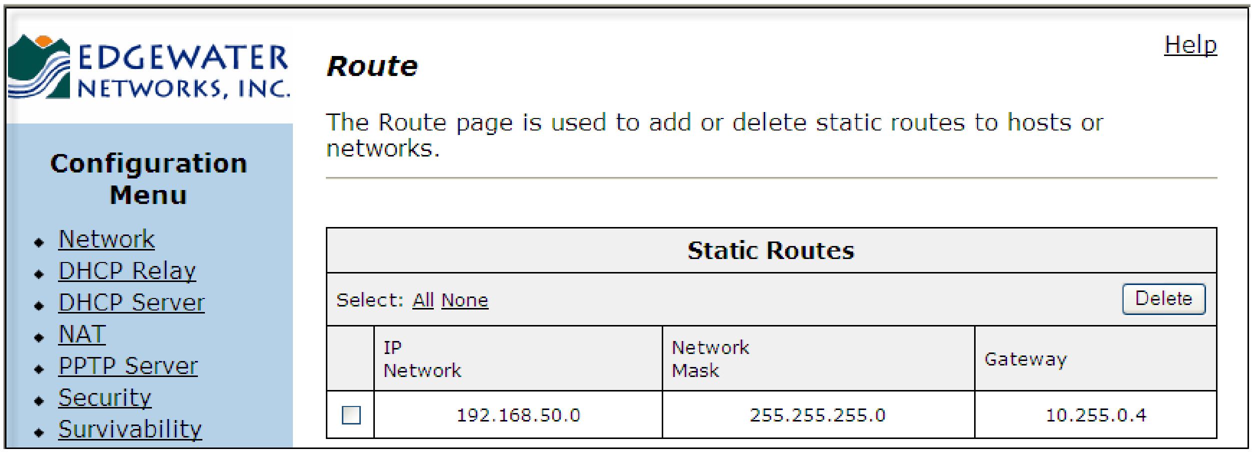
Create a route on the EdgeProtect at the Main Site, to reach the far-end IP Office LAN2 interface, located in network 172.16.0.0 at the Branch location. On the EdgeProtect **Configuration Menu**, select **System → Route**

- **IP Network:** local network at the Branch site IP Office, LAN2.
- **Network Mask:** enter the subnet mask.
- **Gateway:** enter the IP address of the WAN ALG at the Branch Office, as seen previously in **Section 6.2.4**
- Click **Add.**



On the EdgeMarc at the Branch Site, add a route to reach the far-end IP Office LAN2 interface, located in network 192.168.50.0 at the Main Site. From the EdgeMarc **Configuration Menu**, select **System → Route**

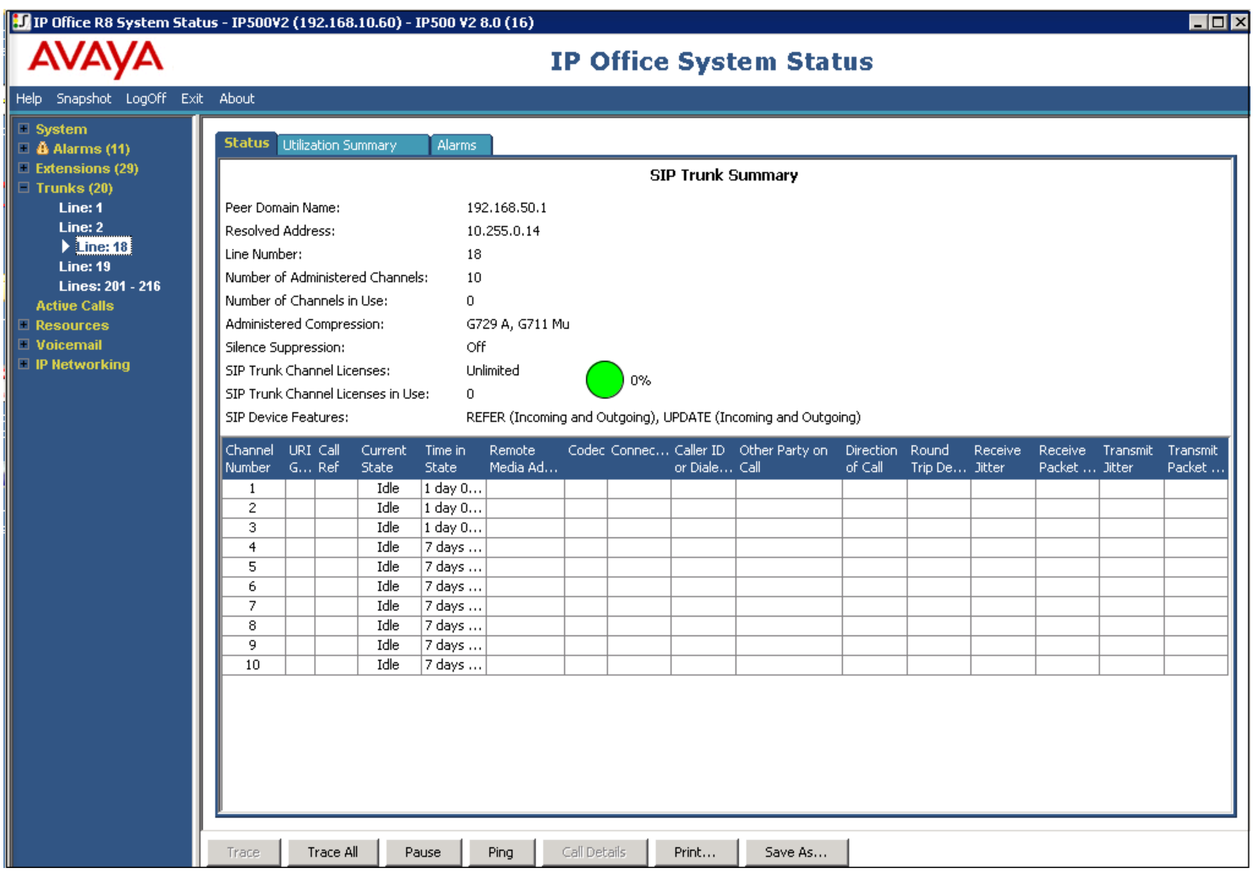
- **IP Network:** local network at the Main Site IP Office, LAN2.
- **Network Mask:** enter the subnet mask.
- **Gateway:** enter the IP address of the VoIP Traversal at the server (EdgeProtect) side, as seen on **Section 6.2.3**
- Click **Add.**



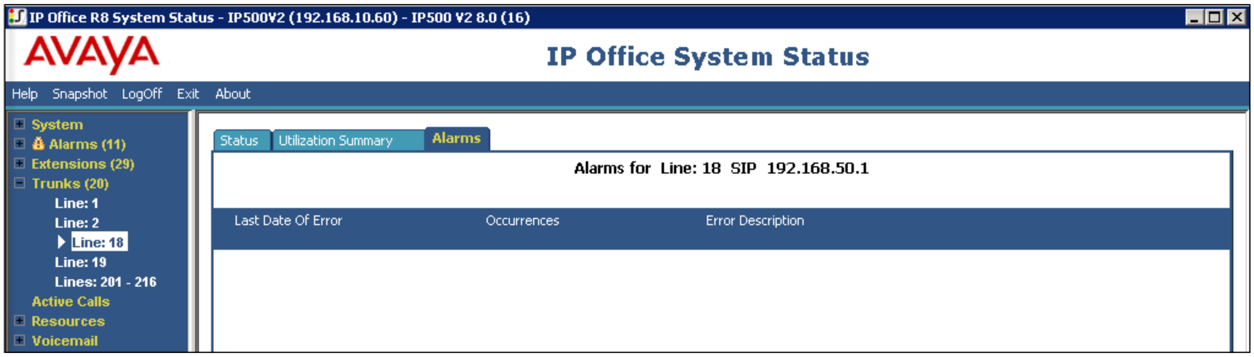
7. Verification Steps

The following steps may be used to verify the working state of the configuration.

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



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



- Check the status of the VoIP Traversal. On the EdgeProtect and EdgeMarc **Configuration Menu**, select **VOIP Traversal.** The symbols on the top of the page should be green (see **Section 6.2.3**). By moving the mouse cursor over the image, a more detailed description of the current status can be seen. If an error has occurred, the error message will be shown here. The status of the VoIP Traversal can be updated clicking the **Refresh Status** link.
- Verify that phones connected to Avaya IP Office at each site can successfully place calls to users at the remote IP Office, with two-way audio.

8. Conclusion

These Application Notes describe the procedures for configuring the EdgeProtect and EdgeMarc Enterprise Session Border Controllers from Edgewater Networks, to interoperate with an Avaya IP Office solution, in a distributed IP Telephony scenario with separate headquarters and branch office locations, as shown on **Figure 1**.

9. Additional References

[1] IP Office 8.0 Installation Manual, Document Number 15-601042, December 2011.
[2] IP Office Manager Manual 10.0, Document Number 15-601011, January 2012.
[3] IP Office System Status Application, Document Number 15-601758, November 2011
[4] IP Office Release 8.0 Implementing Voicemail Pro, Document Number 15-601064, December, 2011
[5] IP Office Softphone Installation, Issue 3c, October, 2011.

Product documentation for Avaya products may be found at http://support.avaya.com
Product documentation for Edgewater Networks products may be found at http://www.edgewaternetworks.com/support

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.