Avaya Solution & Interoperability Test Lab

Application Notes for configuring Edgewater Networks Enterprise Session Border Controllers with Avaya IP Office 8.0 in a Branch Office and Remote Users environment - 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 in a distributed IP Telephony environment, supporting a Branch Office with remote users.

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 Enterprise headquarter and branch 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. This 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 a main site containing the Avaya IP Office and the EdgeProtect SBC, and a branch site, where the remote users and the EdgeMarc were located.

The focus of the compliance test was to verify the connectivity of the remote users to the infrastructure at the main site, through the TLS tunnel between the sites, their ability to make and receive different types of calls, and the use of the resources and most common features in the IP Office.

All tests 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:

- Registration of SIP and H.323 remote endpoints to the IP Office.
- Basic call scenarios using G.711U and G.729A codecs.
- Quality of Service.
- Media Path Redirection.
- 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.

2.2. Test Results

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

- **Duplicated IP Address messages on EdgeMarc LAN segment.** During the compliance test, it was observed that any device connected to the LAN side of the EdgeMarc at the branch site, with a static IP address outside of the assigned tunnel subnet, will have its ARP request answered by the External Server (EdgeProtect), who will send a "duplicated IP address" message to the device. This was observed on the Ethernet switch servicing the remote users, on the static IP address corresponding to the switch Management Interface. At the time of writing these Application Notes, this issue is under study by Edgewater Networks engineers for resolution. The behavior described here did not affect the service in any noticeable way.

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 through the untrusted network.

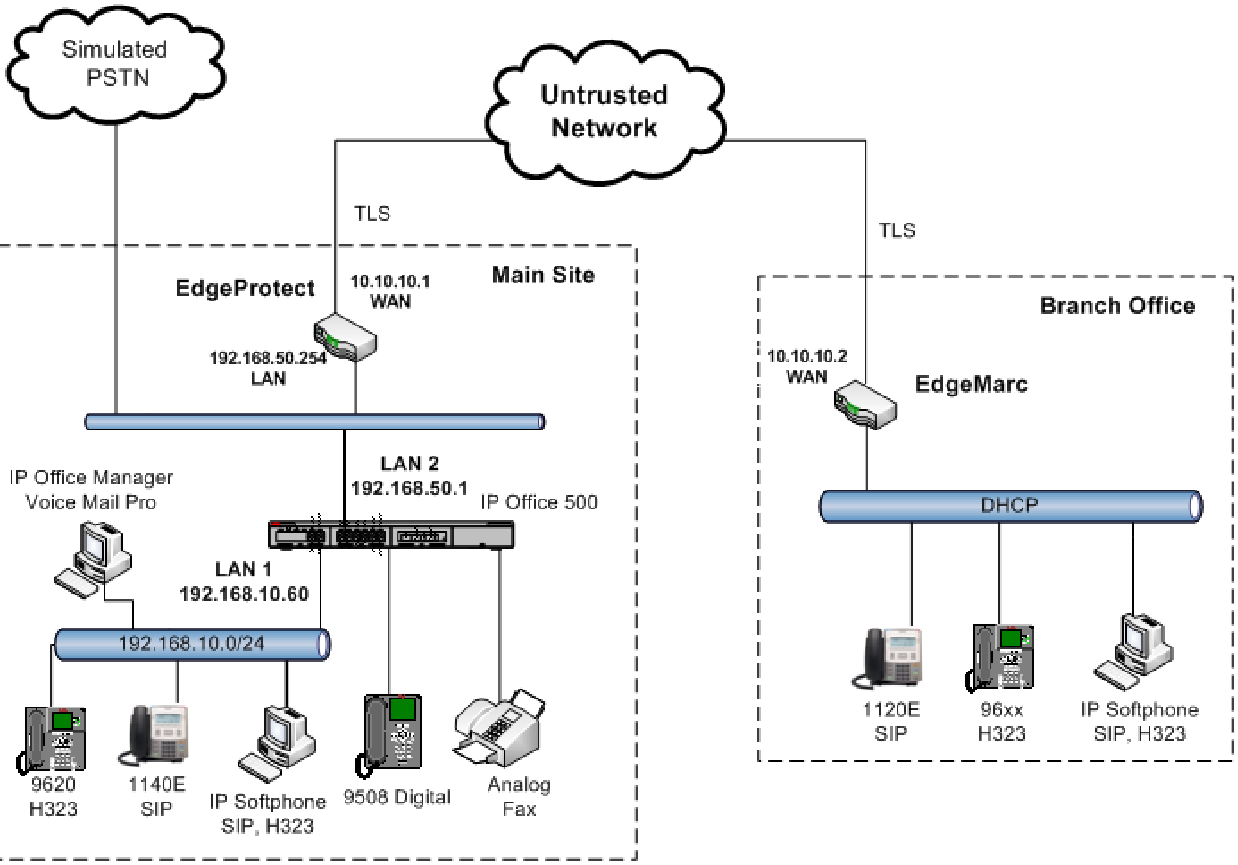


Figure 1.Test Configuration

The Main Site (headquarters) location consists of 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 SBC. The SBC connects to the untrusted network through its WAN interface. A separate SIP line is configured in the IP Office to connect to a simulated PSTN source, a SIP trunk to another PBX in the Lab, which was used during the tests to simulate inbound and outbound PSTN calls to the IP Office.

The Branch Office location contains the remote users, consisting of Avaya SIP and H323 hard phones and Avaya IP Office Softphones. The phones connect to the LAN side of the EdgeMarc. The site connects to the cloud through the WAN port of the EdgeMarc SBC.

All the users at the Branch Office were configured to use the IP address of the LAN2 interface of the IP Office at the Main site, 192.168.50.1, as their SIP Proxy Server (for SIP users) or

Call Server (for H323 users). They were also configured to obtain their own IP addresses by using DHCP, which they obtained from the EdgeProtect SBC, via the TLS tunnel between the two SBCs.

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

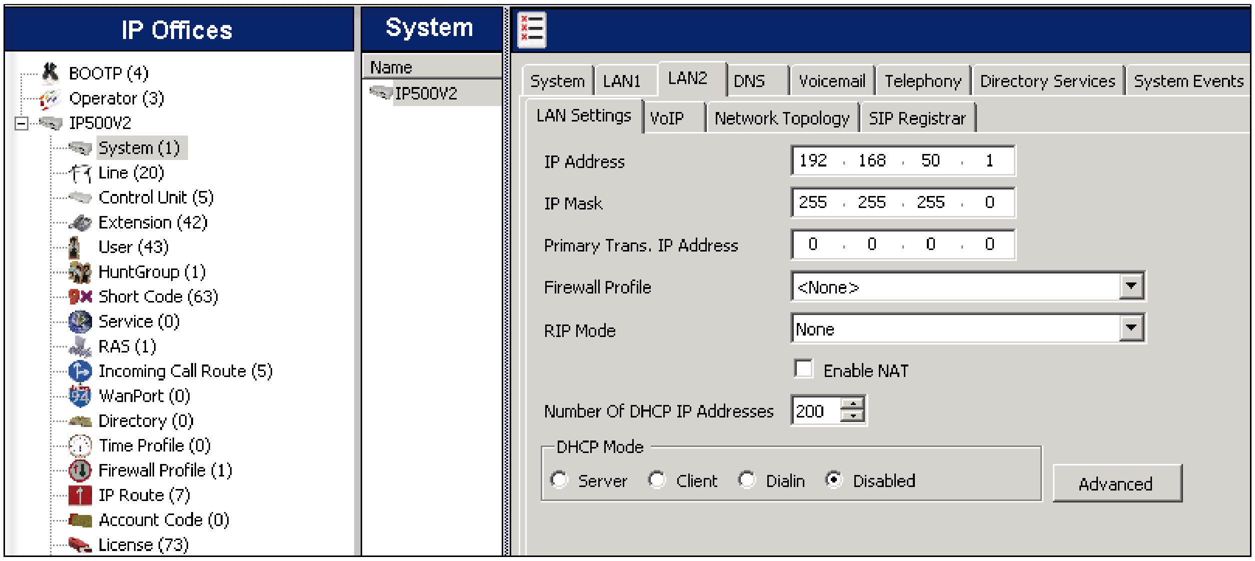
This section describes the Avaya IP Office configuration to support the registration of the remote users located at the Branch Office. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From the PC running the Avaya IP Office Manager application, select **Start** → **Programs** → **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.

All the screens and configuration settings presented in the next sections of this document have the purpose to simply illustrate the sample configuration used during the compliance test, and are not intended to be prescriptive.

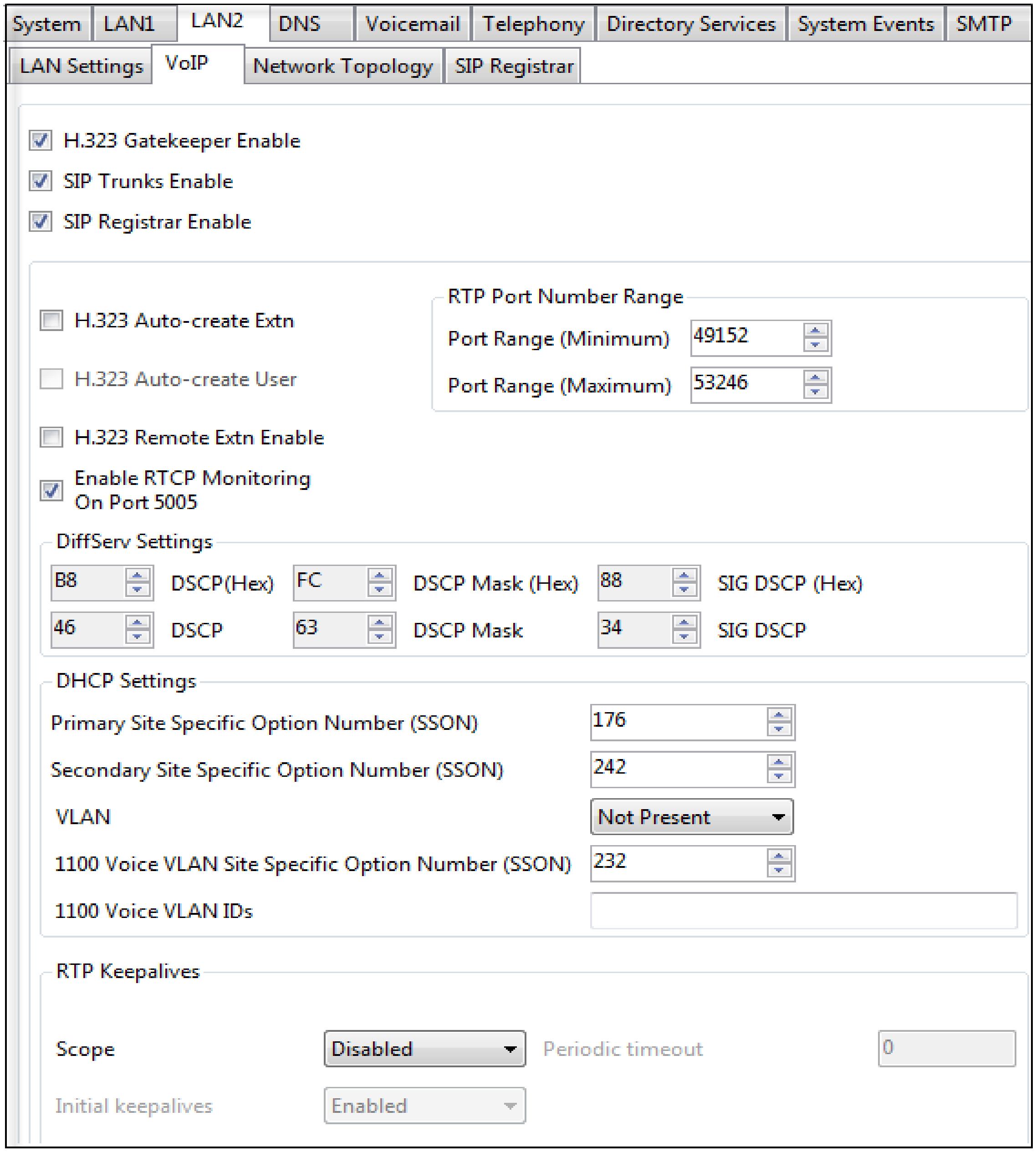
5.1. LAN2 Settings

In the sample configuration, IP500V2 was used as the system name, and the LAN2 port was used to connect the Avaya IP Office to the Inside port of the EdgeProtect SBC. The LAN2 settings correspond to the WAN port on the Avaya IP Office. To access the LAN2 settings, first navigate to **System (1)** → **IP500V2** in the Navigation and Group panes 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 WAN port (see **Figure 1**). All other parameters should be set according to customer requirements.



IP Address: 192 . 168 . 50 . 1
IP Mask: 255 . 255 . 255 . 0
Primary Trans. IP Address: 0 . 0 . 0 . 0
Firewall Profile: <None>
RIP Mode: None
☐ Enable NAT
Number Of DHCP IP Addresses: 200
DHCP Mode: ○ Server ○ Client ○ Dialin ● Disabled

On the **VoIP** tab in the Details pane, check the **H.323 Gatekeeper Enable** and **SIP Registrar Enable** boxes to enable the registration of the remote users through this interface. Even though it is not necessary to support the remote users, 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.



☑ H.323 Gatekeeper Enable

☑ SIP Trunks Enable

☑ SIP Registrar Enable

□ H.323 Auto-create Extn

□ H.323 Auto-create User

RTP Port Number Range

Port Range (Minimum)	49152
Port Range (Maximum)	53246

□ H.323 Remote Extn Enable

☑ Enable RTCP Monitoring On Port 5005

DiffServ Settings

B8	DSCP(Hex)	FC	DSCP Mask (Hex)	88	SIG DSCP (Hex)
46	DSCP	63	DSCP Mask	34	SIG DSCP

DHCP Settings

Primary Site Specific Option Number (SSON)	176
Secondary Site Specific Option Number (SSON)	242
VLAN	Not Present
1100 Voice VLAN Site Specific Option Number (SSON)	232
1100 Voice VLAN IDs	

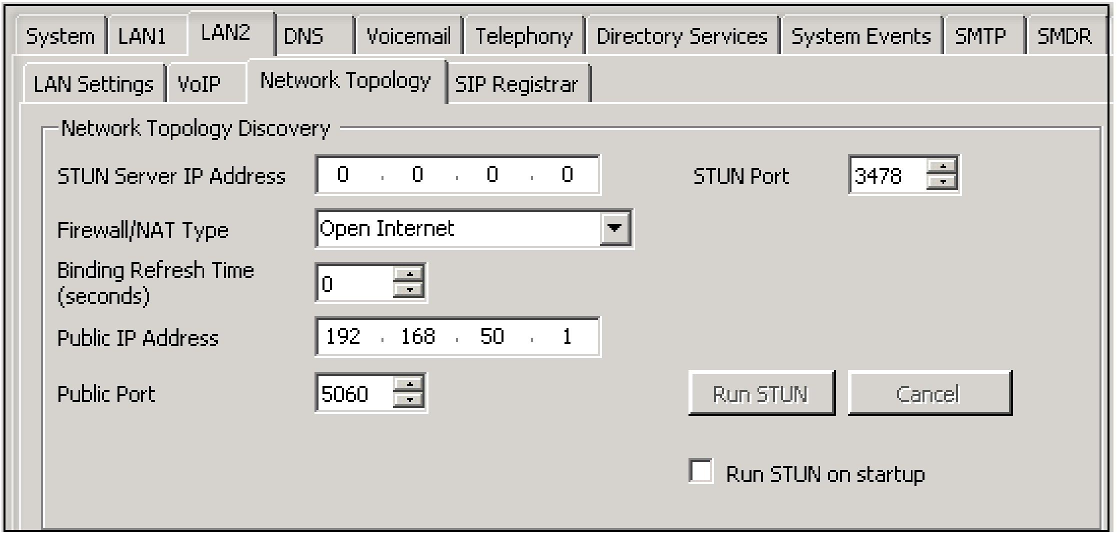
RTP Keepalives

Scope	Disabled	Periodic timeout	0
Initial keepalives	Enabled		

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 **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.



Network Topology Discovery

STUN Server IP Address: 0 . 0 . 0 . 0

STUN Port: 3478

Firewall/NAT Type: Open Internet

Binding Refresh Time (seconds): 0

Public IP Address: 192 . 168 . 50 . 1

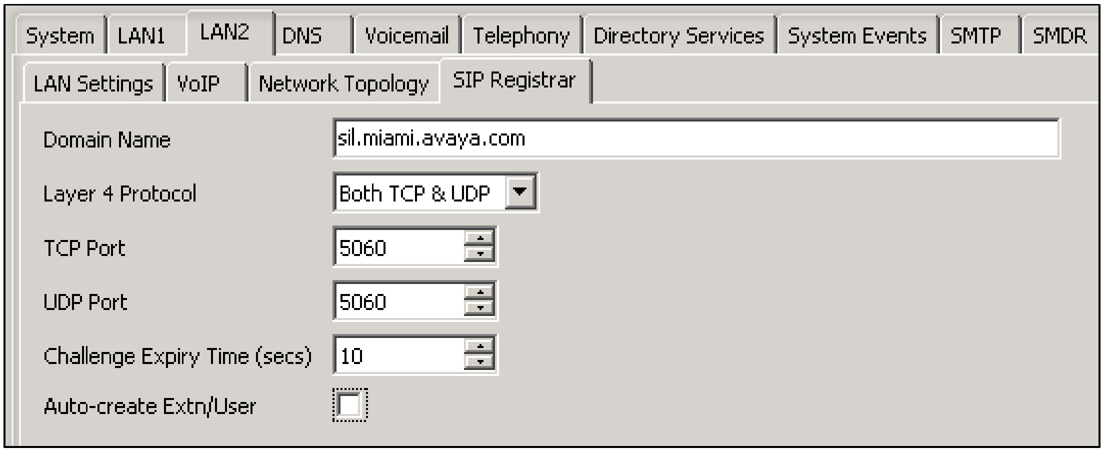
Public Port: 5060

□ Run STUN on startup

On the **SIP Registrar** tab, configure the following:

- Under **Domain Name** enter the SIP domain used on the enterprise.
- Uncheck **Auto-create Ext/User.** By setting this, remote users can only register against existing configuration entries in the IP Office.

Default values are used in the remaining fields.



Domain Name: sil.miami.avaya.com

Layer 4 Protocol: Both TCP & UDP

TCP Port: 5060

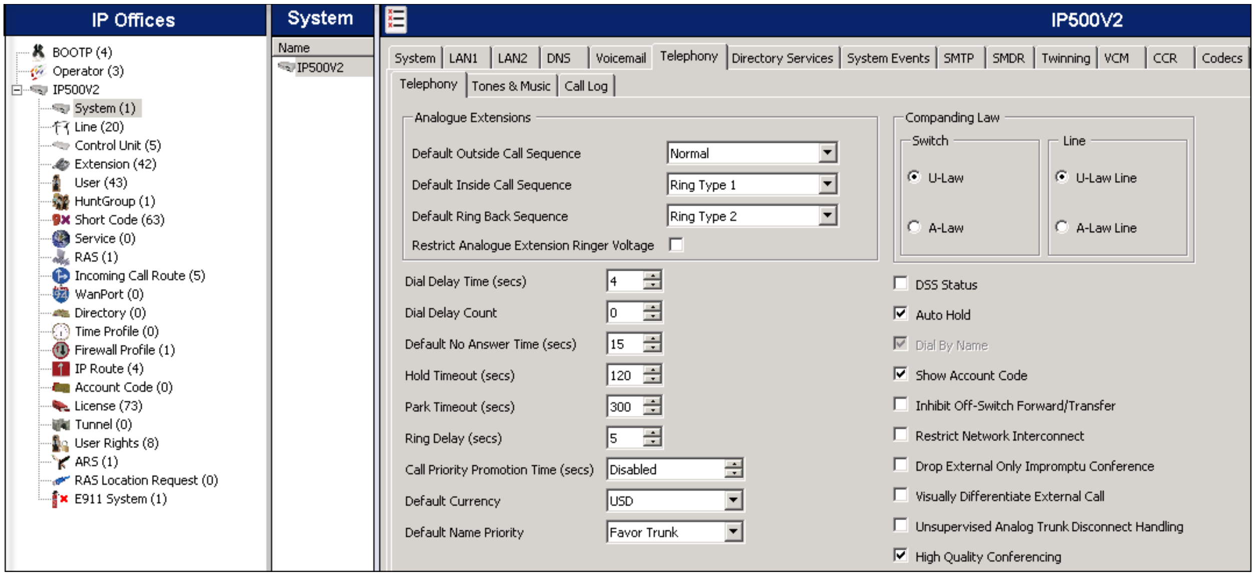
UDP Port: 5060

Challenge Expiry Time (secs): 10

Auto-create Extn/User: □

5.2. 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 back to the simulated PSTN. Defaults were used for all other parameters.



Analogue Extensions

Default Outside Call Sequence: Normal

Default Inside Call Sequence: Ring Type 1

Default Ring Back Sequence: Ring Type 2

Restrict Analogue Extension Ringer Voltage ☐

Dial Delay Time (secs): 4

Dial Delay Count: 0

Default No Answer Time (secs): 15

Hold Timeout (secs): 120

Park Timeout (secs): 300

Ring Delay (secs): 5

Call Priority Promotion Time (secs): Disabled

Default Currency: USD

Default Name Priority: Favor Trunk

Companding Law

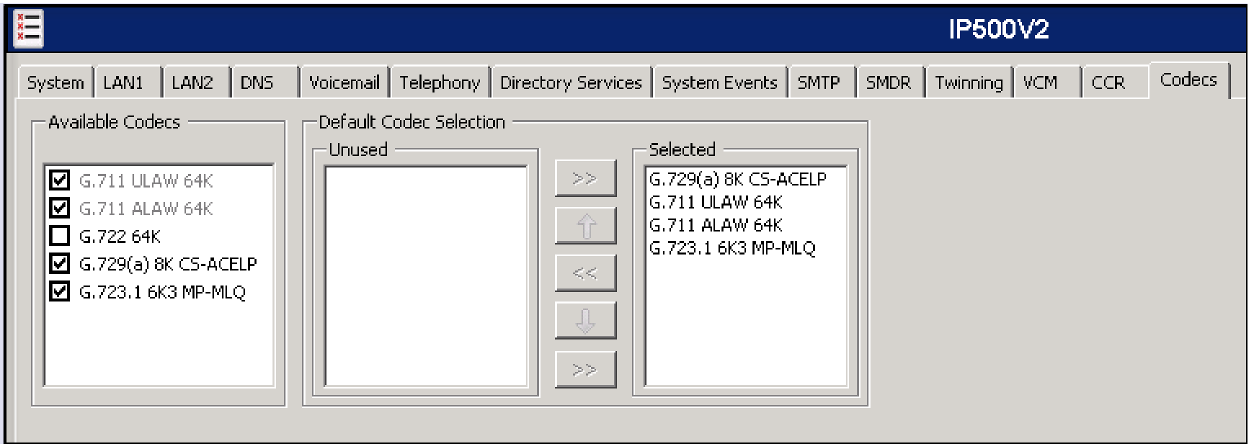
Switch: ● U-Law ○ A-Law

Line: ● U-Law Line ○ A-Law Line

☐ DSS Status
☑ Auto Hold
☑ Dial By Name
☑ Show Account Code
☐ Inhibit Off-Switch Forward/Transfer
☐ Restrict Network Interconnect
☐ Drop External Only Impromptu Conference
☐ Visually Differentiate External Call
☐ Unsupervised Analog Trunk Disconnect Handling
☑ High Quality Conferencing

5.3. 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.


IP500V2
System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Directory Services | System Events | SMTP | SMDR | Twinning | VCM | CCR | Codecs
>>
⇧
<<
⇩
>>

Available Codecs

☑ G.711 ULAW 64K
☑ G.711 ALAW 64K
☐ G.722 64K
☑ G.729(a) 8K CS-ACELP
☑ G.723.1 6K3 MP-MLQ

Default Codec Selection

Unused

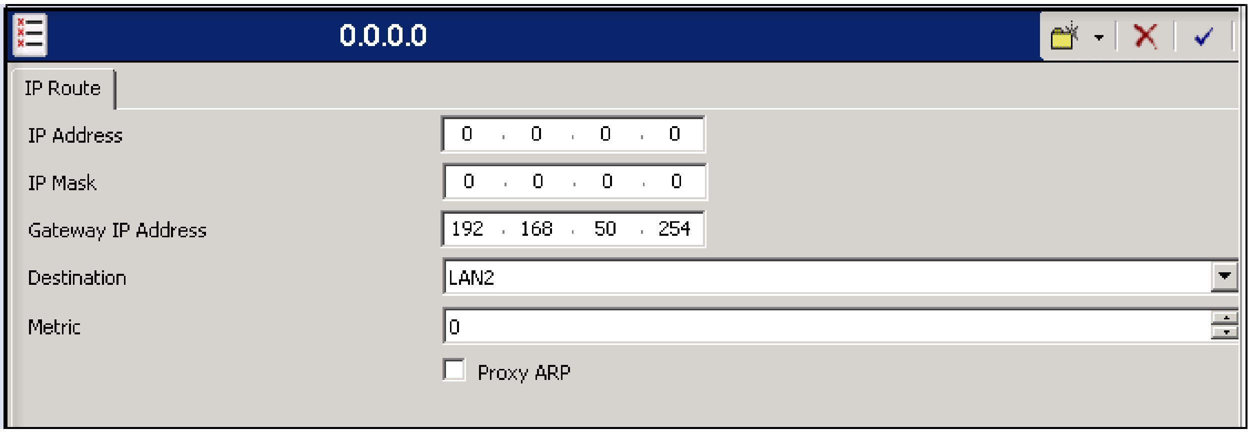
Selected

G.729(a) 8K CS-ACELP
G.711 ULAW 64K
G.711 ALAW 64K
G.723.1 6K3 MP-MLQ

5.4. IP Route

Create a default IP route to specify the gateway or router address where the IP Office needs to send the packets, in order to reach the network in the remote Branch site. On the left navigation pane, right-click on **IP Route**. Select **New**. Enter the following parameters:

- Set **IP Address** and **IP Mask** to ***0.0.0.0***.
- Set **Gateway IP Address** to the IP Address of the LAN interface of the EdgeProtect SBC (see **Figure 1**).
- Set **Destination** to ***LAN2*** from the drop-down list.

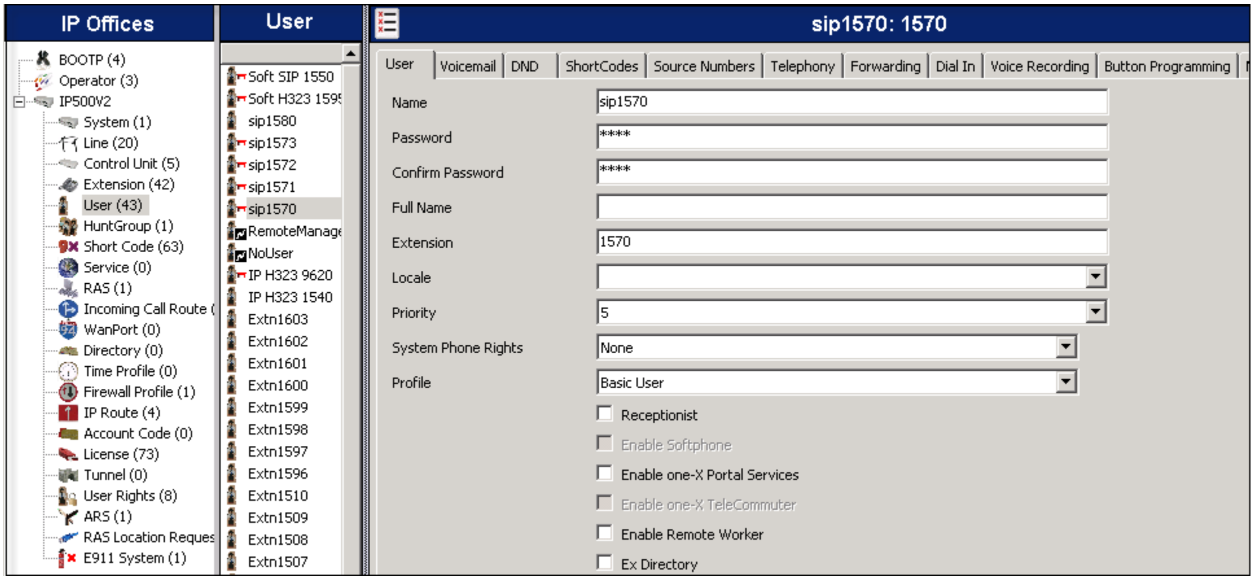


IP Address	0 . 0 . 0 . 0
IP Mask	0 . 0 . 0 . 0
Gateway IP Address	192 . 168 . 50 . 254
Destination	LAN2
Metric	0

□ Proxy ARP

5.5. Remote Users

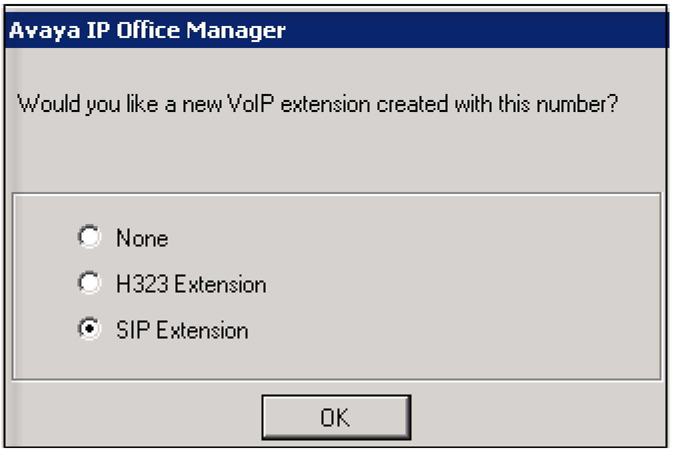
All H.323 and SIP users in the remote Brach Office need to have their entries created in order to be able to register to the IP Office. To add a User, right click on **User** in the Navigation pane, and select **New.** The creation of the SIP extension 1570 is shown as an example in the following screens.



Name	sip1570
Password	****
Confirm Password	****
Full Name	
Extension	1570
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User

□ Receptionist
□ Enable Softphone
□ Enable one-X Portal Services
□ Enable one-X TeleCommuter
□ Enable Remote Worker
□ Ex Directory

Click **OK** at the bottom of the screen. The following window appears. Select the extension type to be created. Click **OK**.

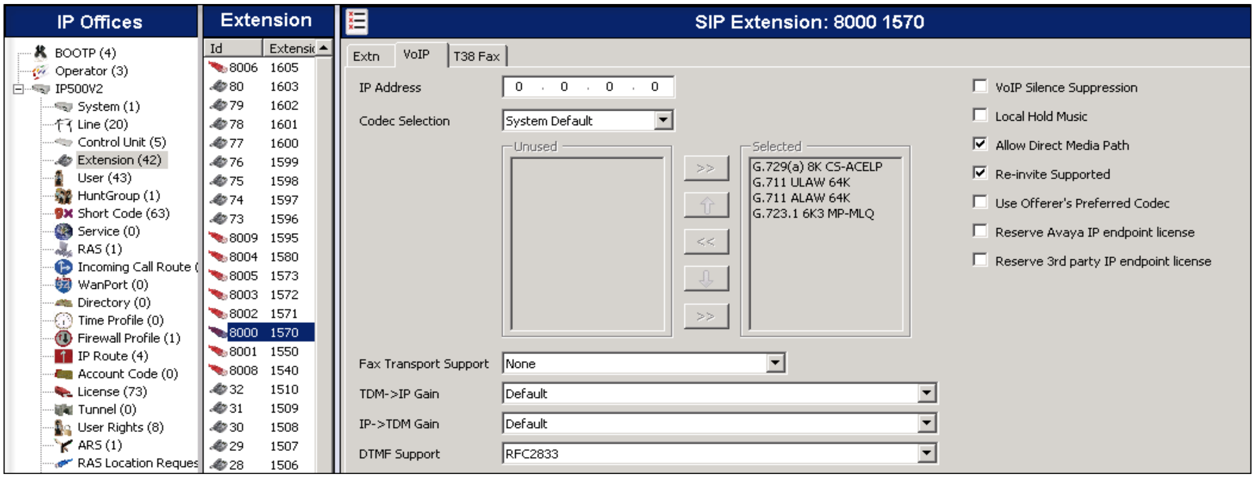


Avaya IP Office Manager

Would you like a new VoIP extension created with this number?

○ None
○ H323 Extension
● SIP Extension

Select **Extensions** on the Navigation pane. Select the newly created extension **1570** in the Group pane. On the **VoIP** tab, check the **Allow Direct Media Path** box**.** This will enable the redirection of the RTP packets for local calls to other SIP users inside the Branch, eliminating the need for these packets for travelling to the IP Office at the Main site and back to the Branch, for this type of local calls.



Extension

Id	Extensic
8006	1605
80	1603
79	1602
78	1601
77	1600
76	1599
75	1598
74	1597
73	1596
8009	1595
8004	1580
8005	1573
8003	1572
8002	1571
8000	1570
8001	1550
8008	1540
32	1510
31	1509
30	1508
29	1507
28	1506

SIP Extension: 8000 1570

IP Address: 0 . 0 . 0 . 0

Codec Selection: System Default

Unused:

Selected:
G.729(a) 8K CS-ACELP
G.711 ULAW 64K
G.711 ALAW 64K
G.723.1 6K3 MP-MLQ

Fax Transport Support: None

TDM->IP Gain: Default

IP->TDM Gain: Default

DTMF Support: RFC2833

□ VoIP Silence Suppression
□ Local Hold Music
☑ Allow Direct Media Path
☑ Re-invite Supported
□ Use Offerer's Preferred Codec
□ Reserve Avaya IP endpoint license
□ Reserve 3rd party IP endpoint license

5.6. 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 SBCs.

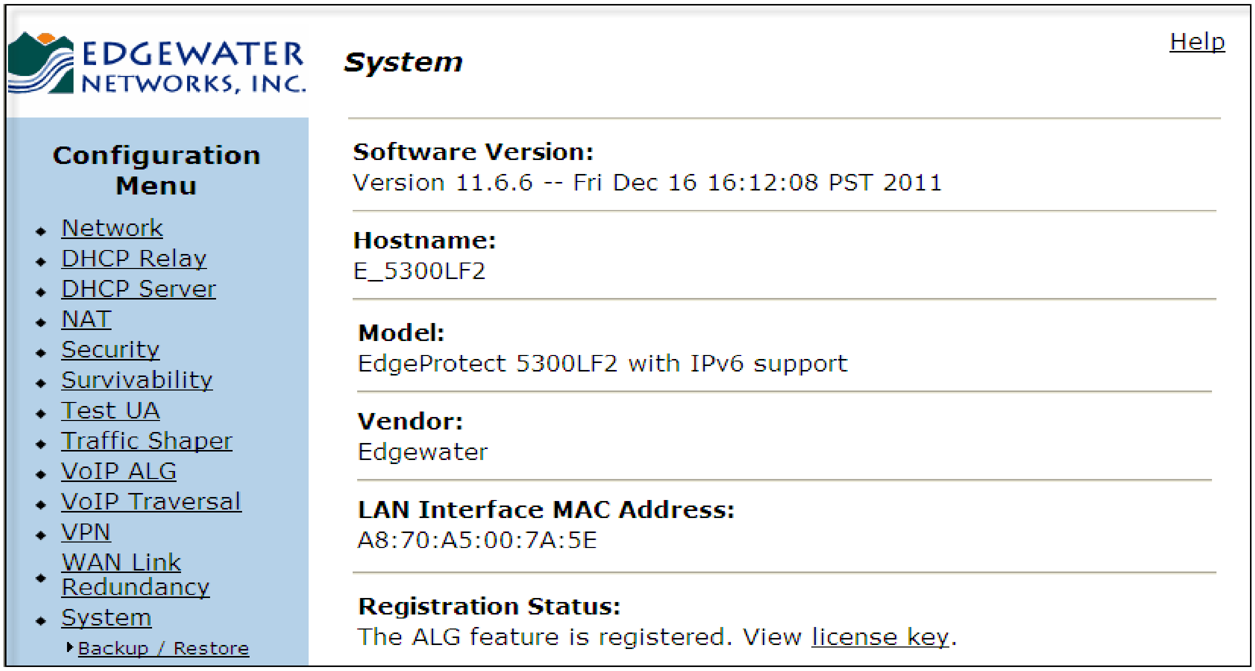
This section describes the configuration steps for the EdgeProtect and the EdgeMarc Session Border Controllers, in order to implement the test configuration shown on **Figure 1**.

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. Licensing

Select **System** on the **Configuration Menu** and click the **license key**.



System

Software Version:
Version 11.6.6 -- Fri Dec 16 16:12:08 PST 2011

Hostname:
E_5300LF2

Model:
EdgeProtect 5300LF2 with IPv6 support

Vendor:
Edgewater

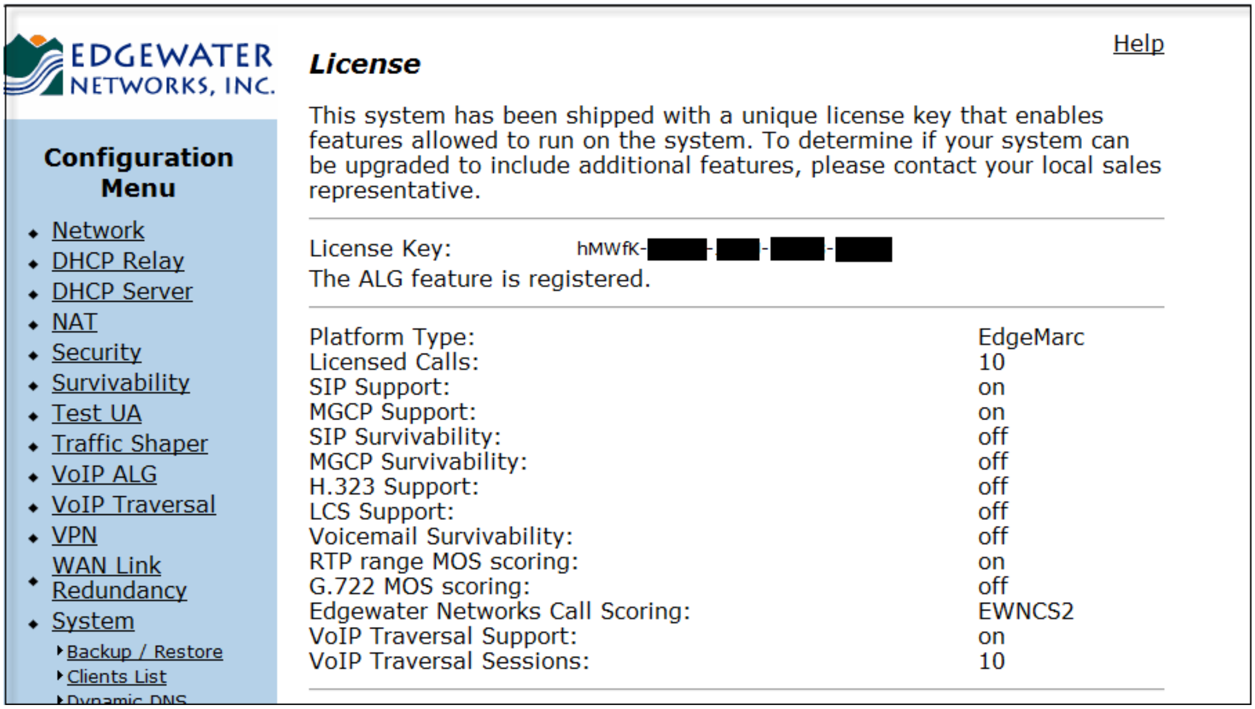
LAN Interface MAC Address:
A8:70:A5:00:7A:5E

Registration Status:
The ALG feature is registered. View license key.

The **License** page is shown on the next screen. Verify the following parameters:

- **Platform Type** is set to **EdgeMarc**.
- **VoIP Traversal Support** is **ON**.
- The number of **Licensed Calls** is sufficient to support all users at the Branch Office.

Note that since the Application Layer Gateway (ALG) functionality of the EdgeProtect and EdgeMarc is not used in the current configuration, and VoIP Traversal is used instead, it is not strictly necessary to enable SIP or H.323 support in this page.



License

This system has been shipped with a unique license key that enables features allowed to run on the system. To determine if your system can be upgraded to include additional features, please contact your local sales representative.

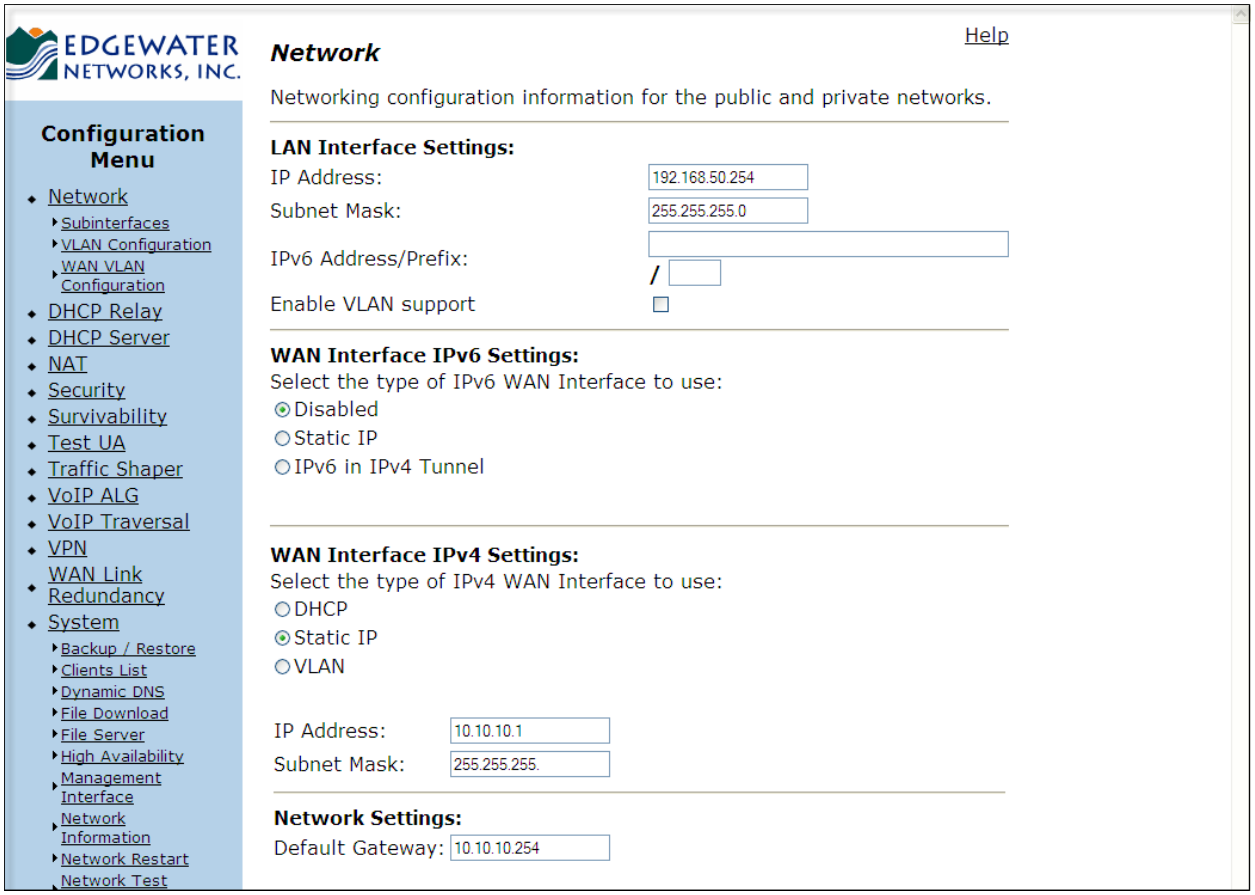
License Key: hMWfK-[redacted]-[redacted]-[redacted]-[redacted]

The ALG feature is registered.

Platform Type:	EdgeMarc
Licensed Calls:	10
SIP Support:	on
MGCP Support:	on
SIP Survivability:	off
MGCP Survivability:	off
H.323 Support:	off
LCS Support:	off
Voicemail Survivability:	off
RTP range MOS scoring:	on
G.722 MOS scoring:	off
Edgewater Networks Call Scoring:	EWNCS2
VoIP Traversal Support:	on
VoIP Traversal Sessions:	10

6.1.2. Network Settings

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



Network

Networking configuration information for the public and private networks.

LAN Interface Settings:

IP Address: 192.168.50.254
Subnet Mask: 255.255.255.0
IPv6 Address/Prefix: /
Enable VLAN support □

WAN Interface IPv6 Settings:

Select the type of IPv6 WAN Interface to use:
● Disabled
○ Static IP
○ IPv6 in IPv4 Tunnel

WAN Interface IPv4 Settings:

Select the type of IPv4 WAN Interface to use:
○ DHCP
● Static IP
○ VLAN

IP Address: 10.10.10.1
Subnet Mask: 255.255.255.

Network Settings:

Default Gateway: 10.10.10.254

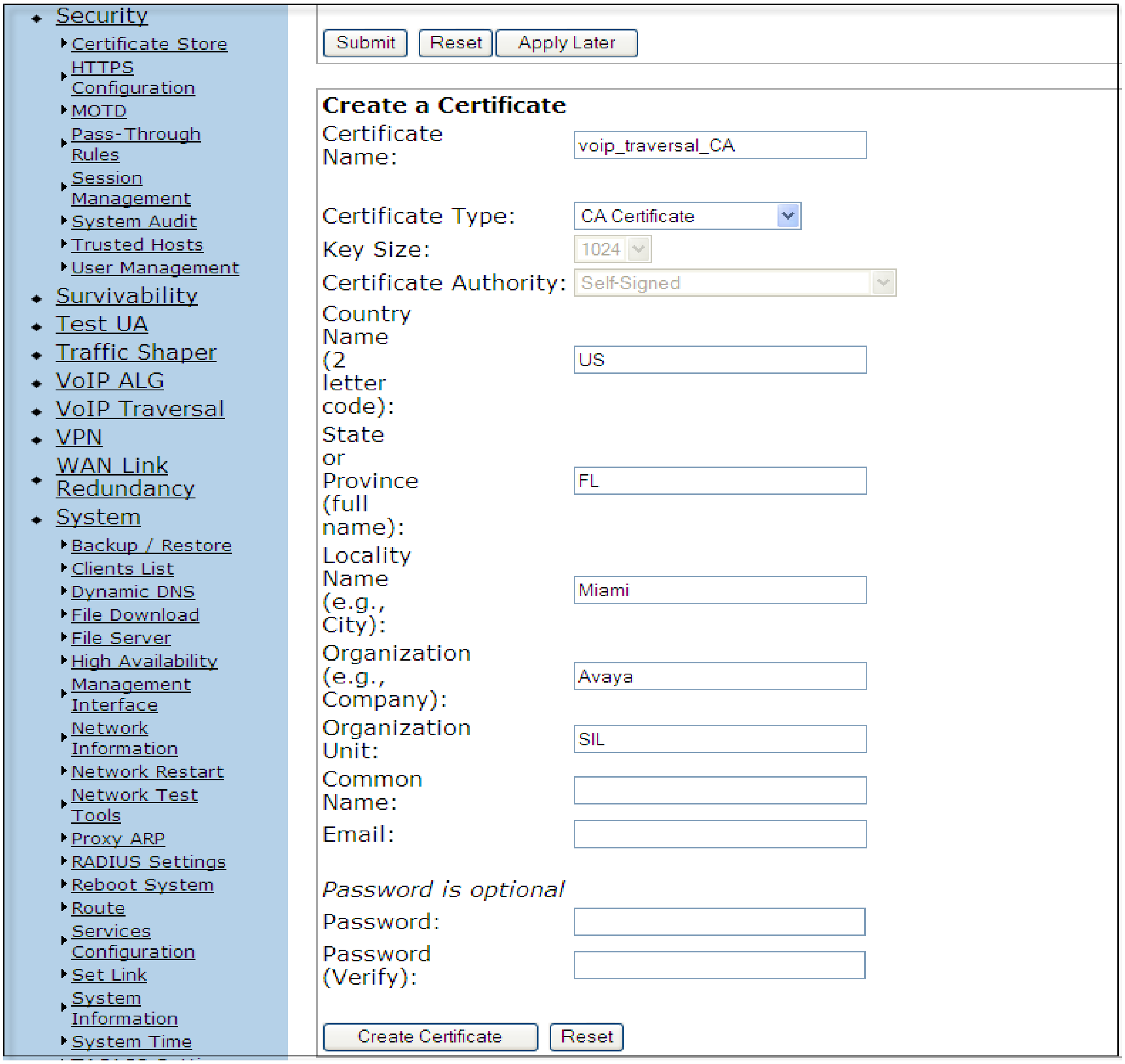
6.1.3. TLS Certificates

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**.



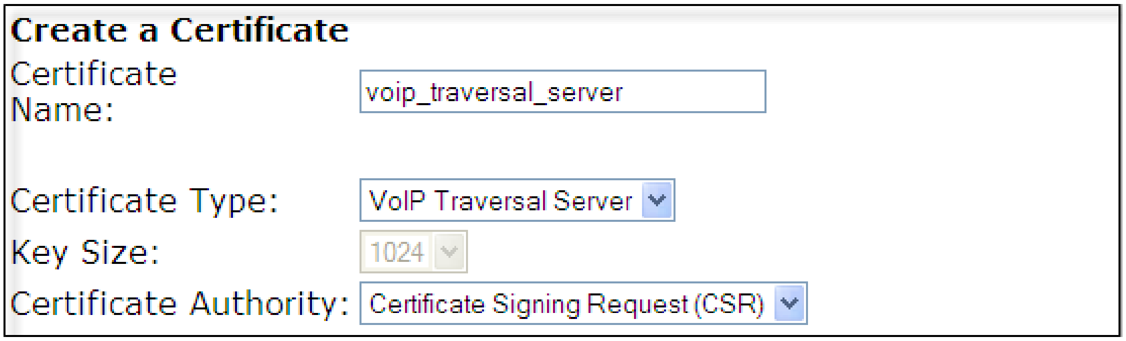
Create a Certificate

Certificate Name:	voip_traversal_CA
Certificate Type:	CA Certificate
Key Size:	1024
Certificate Authority:	Self-Signed
Country Name (2 letter code):	US
State or Province (full name):	FL
Locality Name (e.g., City):	Miami
Organization (e.g., Company):	Avaya
Organization Unit:	SIL
Common Name:	
Email:	

Password is optional

Password:	
Password (Verify):	

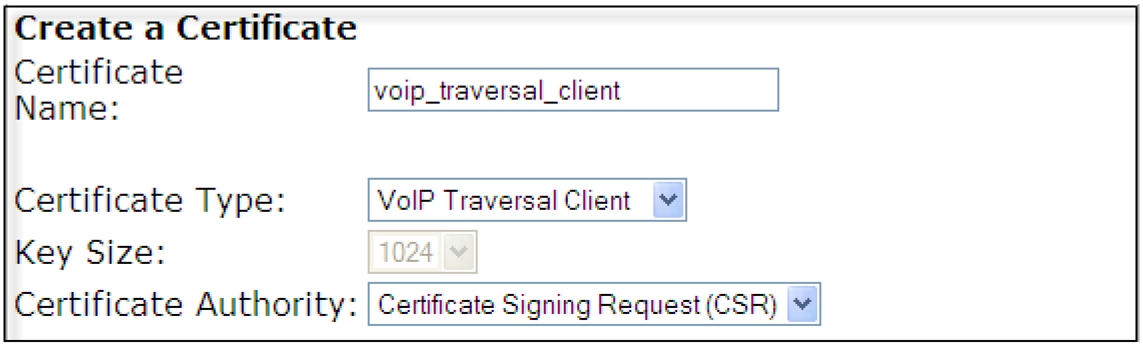
Create a certificate for the server. Enter the **Certificate Name**. Choose **VoIP Traversal Server** from the pull-down menu under **Certificate Type**. Enter all others parameters as appropriate. Click **Create Certificate** (not shown).



Create a Certificate

Certificate Name:	voip_traversal_server
Certificate Type:	VoIP Traversal Server
Key Size:	1024
Certificate Authority:	Certificate Signing Request (CSR)

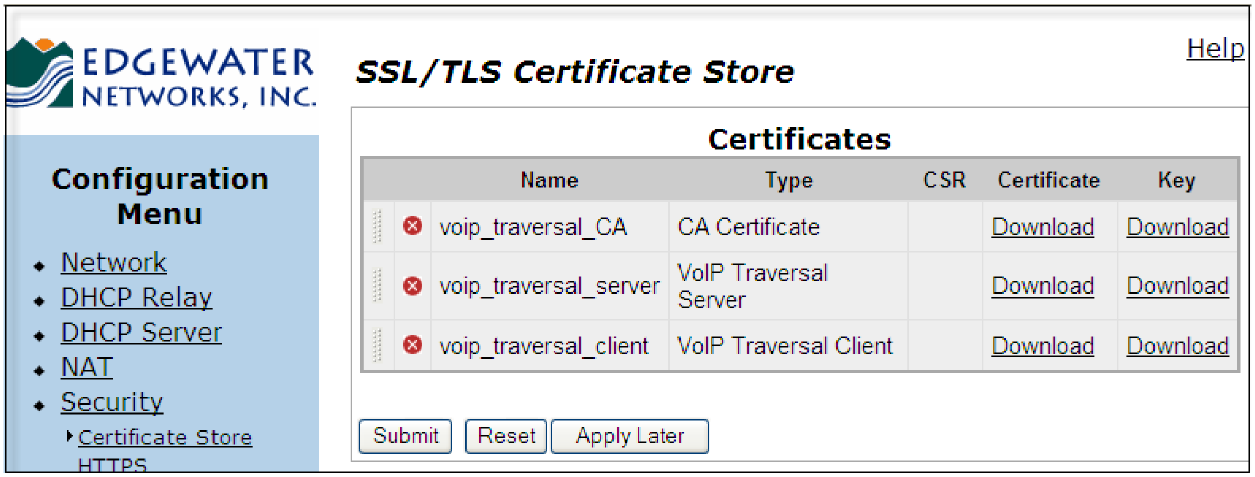
Similarly, create the certificate for the client. Select **VoIP Traversal Client** from the pull-down menu under **Certificate Type**. Enter all others parameters as appropriate. Click **Create Certificate**.



Create a Certificate

Certificate Name:	voip_traversal_client
Certificate Type:	VoIP Traversal Client
Key Size:	1024
Certificate Authority:	Certificate Signing Request (CSR)

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



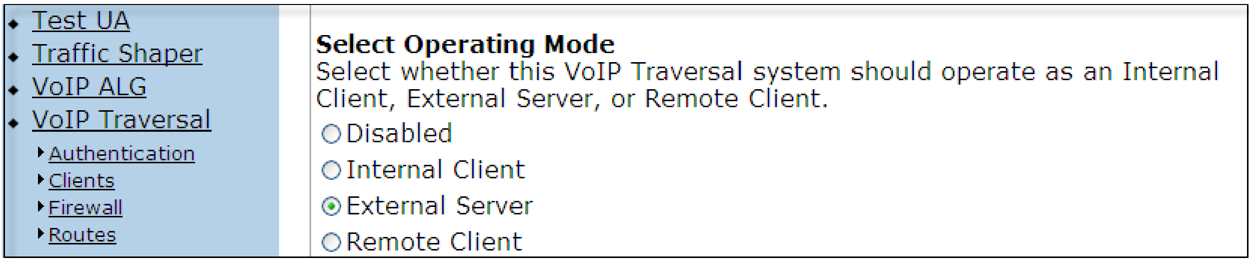
SSL/TLS Certificate Store

Certificates

Name	Type	CSR	Certificate	Key
voip_traversal_CA	CA Certificate		Download	Download
voip_traversal_server	VoIP Traversal Server		Download	Download
voip_traversal_client	VoIP Traversal Client		Download	Download

6.1.4 VoIP Traversal

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



Select Operating Mode

Select whether this VoIP Traversal system should operate as an Internal Client, External Server, or Remote Client.

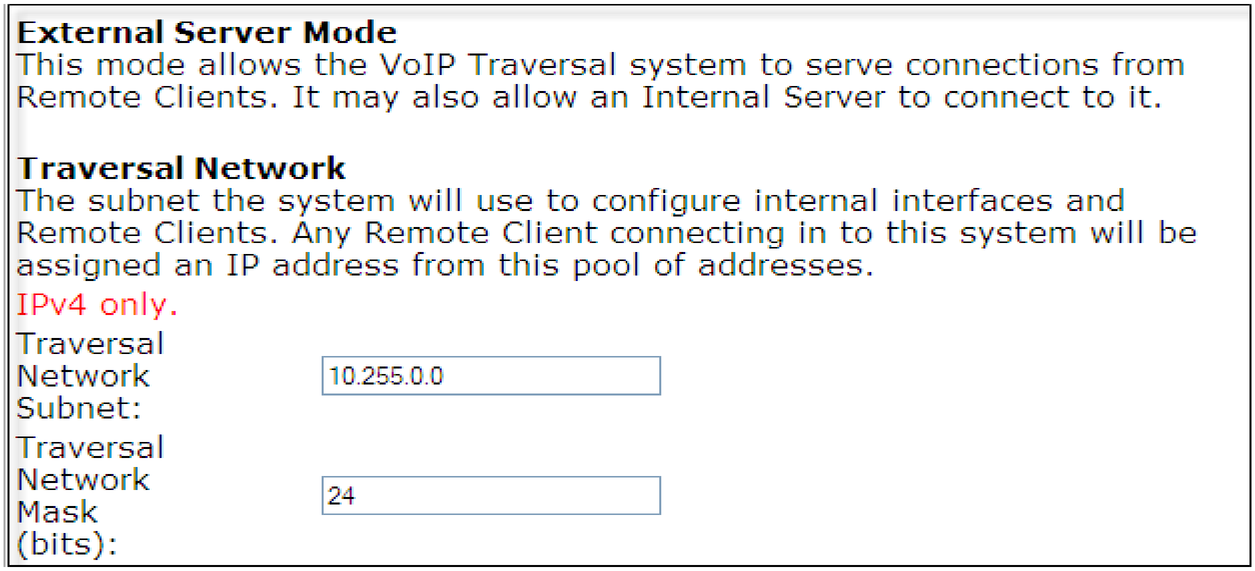
○ Disabled

○ Internal Client

● External Server

○ Remote Client

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



External Server Mode

This mode allows the VoIP Traversal system to serve connections from Remote Clients. It may also allow an Internal Server to connect to it.

Traversal Network

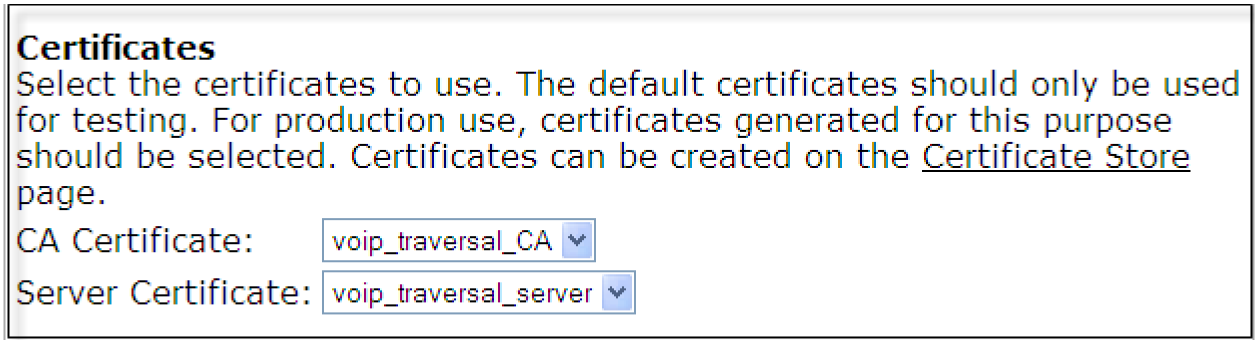
The subnet the system will use to configure internal interfaces and Remote Clients. Any Remote Client connecting in to this system will be assigned an IP address from this pool of addresses.

IPv4 only.

Traversal Network Subnet: 10.255.0.0

Traversal Network Mask (bits): 24

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



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

Server Certificate: voip_traversal_server

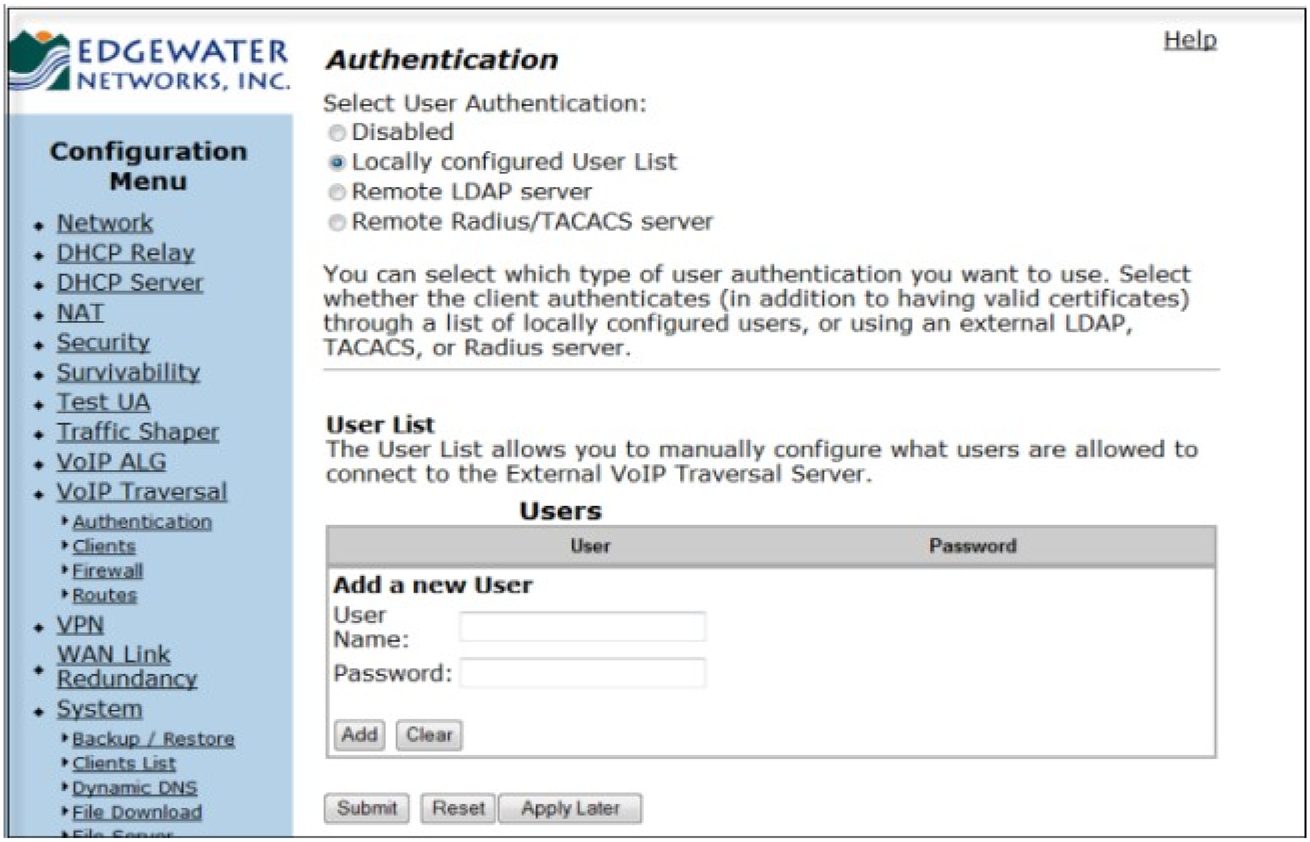
Click **Submit** (not shown).

6.1.5. 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.



Authentication

Select User Authentication:

○ Disabled
● Locally configured User List
○ Remote LDAP server
○ Remote Radius/TACACS server

You can select which type of user authentication you want to use. Select whether the client authenticates (in addition to having valid certificates) through a list of locally configured users, or using an external LDAP, TACACS, or Radius server.

User List

The User List allows you to manually configure what users are allowed to connect to the External VoIP Traversal Server.

Users

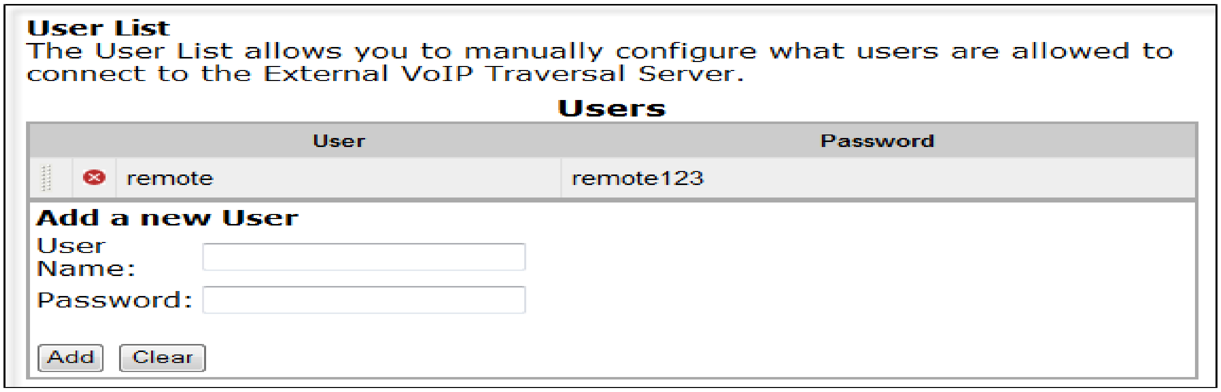
User	Password

Add a new User

User Name:

Password:

- Click **Add** and **Submit**.



User List

The User List allows you to manually configure what users are allowed to connect to the External VoIP Traversal Server.

Users

User	Password
remote	remote123

Add a new User

User Name:

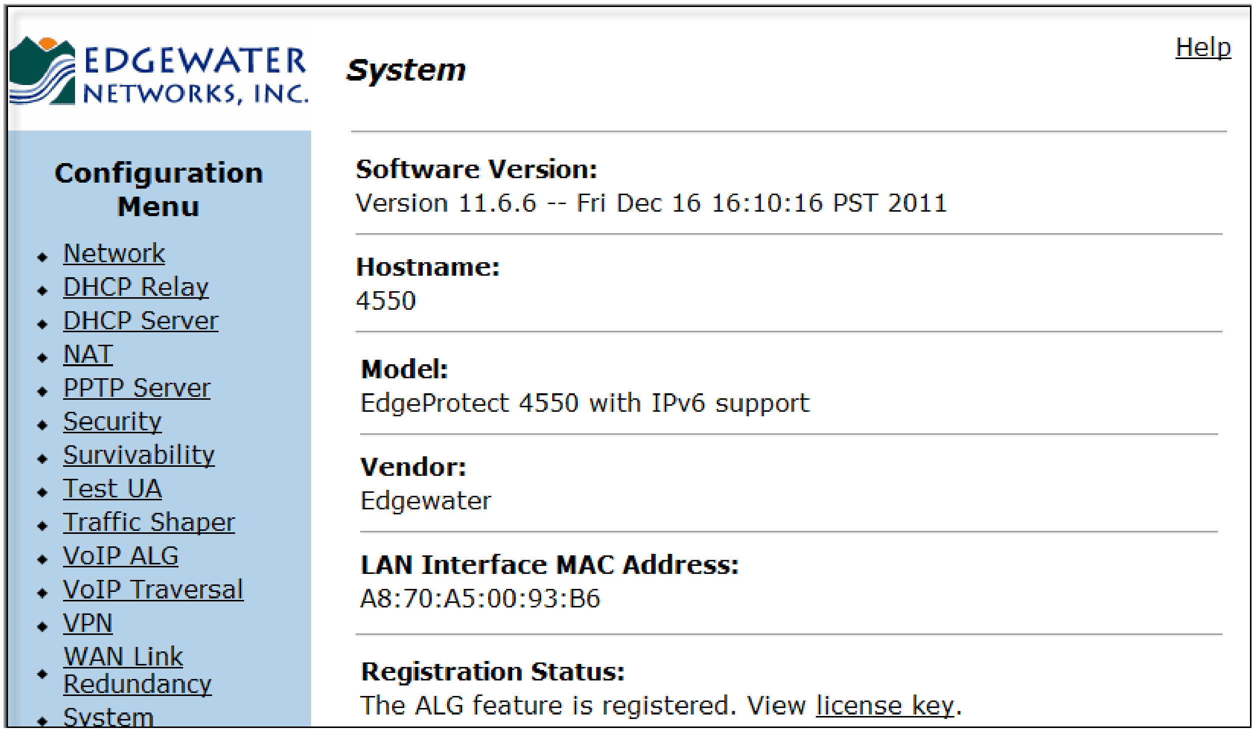
Password:

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. Licensing

Select **System** on the **Configuration Menu** and click the **license key**.



Software Version:
Version 11.6.6 -- Fri Dec 16 16:10:16 PST 2011

Hostname:
4550

Model:
EdgeProtect 4550 with IPv6 support

Vendor:
Edgewater

LAN Interface MAC Address:
A8:70:A5:00:93:B6

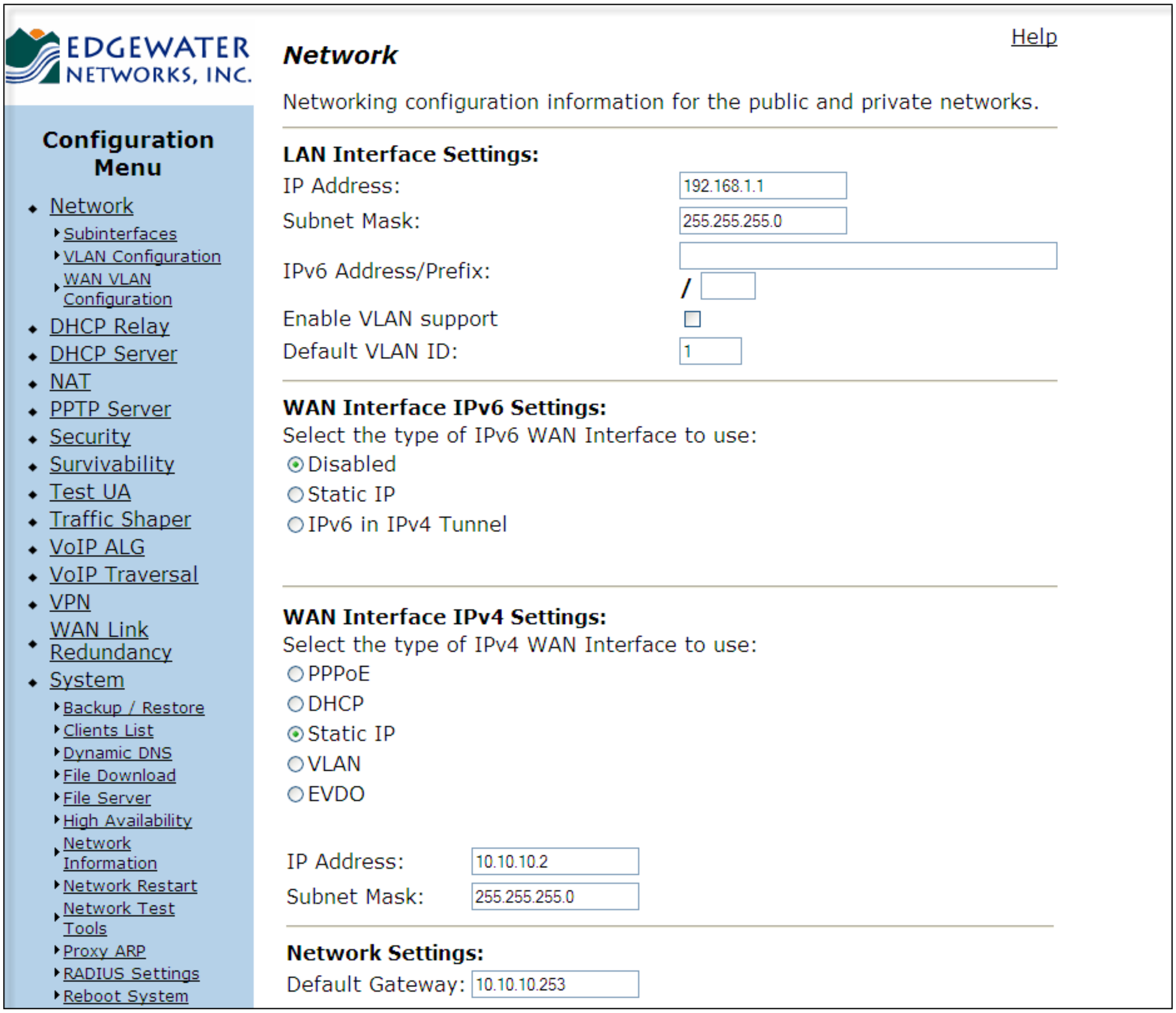
Registration Status:
The ALG feature is registered. View license key.

This brings you to the License Key screen, similar to the one shown for the EdgeProtect in **Section 6.1.1**. Verify the following parameters:

- **Platform Type** is set to **EdgeMarc**.
- **VoIP Traversal Support** is **ON**.
- The number of **Licensed Calls** is sufficient to support all users at the Branch Office.

6.2.2. Network Settings

Choose **Network** from the **Configuration Menu**. Enter the settings under **WAN Interface IPv4 Settings** sections as appropriate. There is no need to change the IP address of the LAN interface of the EdgeMarc. The EdgeMarc uses the VoIP traversal to obtain the IP addresses for all the users in its LAN segment, via DHCP from the EdgeProtect.



Network

Networking configuration information for the public and private networks.

LAN Interface Settings:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

IPv6 Address/Prefix: /

Enable VLAN support □

Default VLAN ID: 1

WAN Interface IPv6 Settings:

Select the type of IPv6 WAN Interface to use:

● Disabled
○ Static IP
○ IPv6 in IPv4 Tunnel

WAN Interface IPv4 Settings:

Select the type of IPv4 WAN Interface to use:

○ PPPoE
○ DHCP
● Static IP
○ VLAN
○ EVDO

IP Address: 10.10.10.2

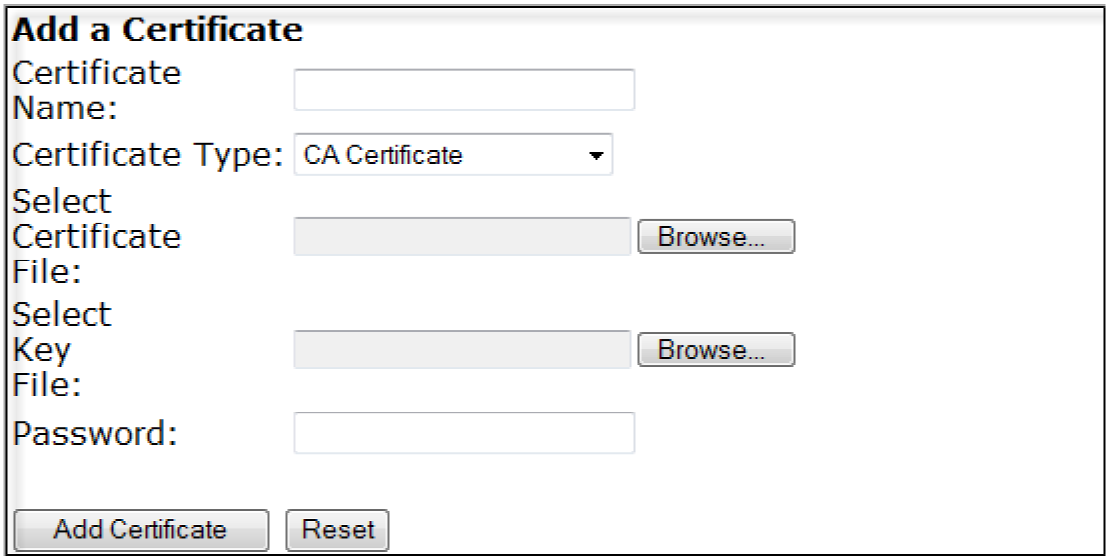
Subnet Mask: 255.255.255.0

Network Settings:

Default Gateway: 10.10.10.253

6.2.3. 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 6.1.3.** 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.



Add a Certificate

Certificate Name:

Certificate Type: CA Certificate

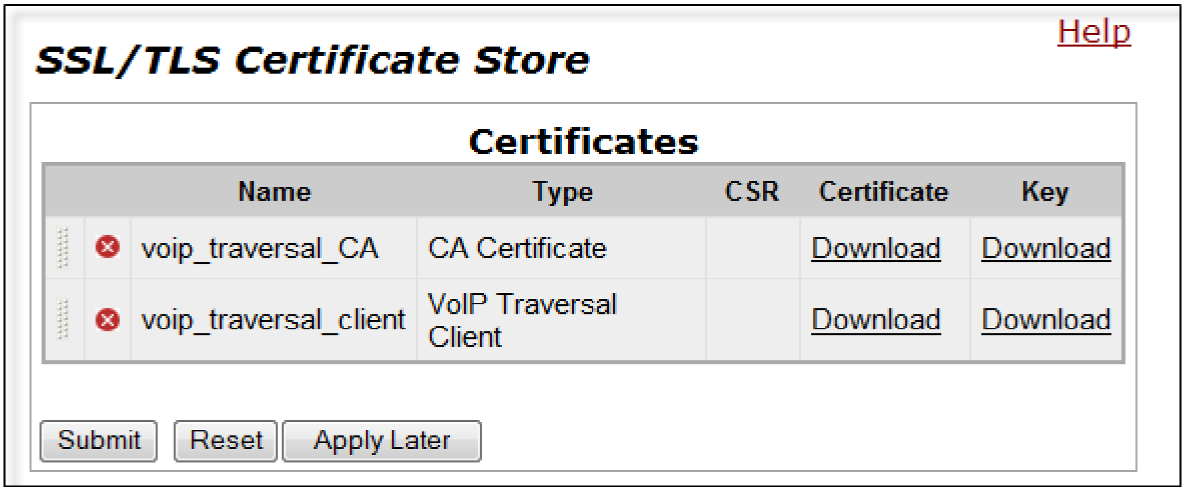
Select Certificate File:

Select Key File:

Password:

- **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**.



SSL/TLS Certificate Store

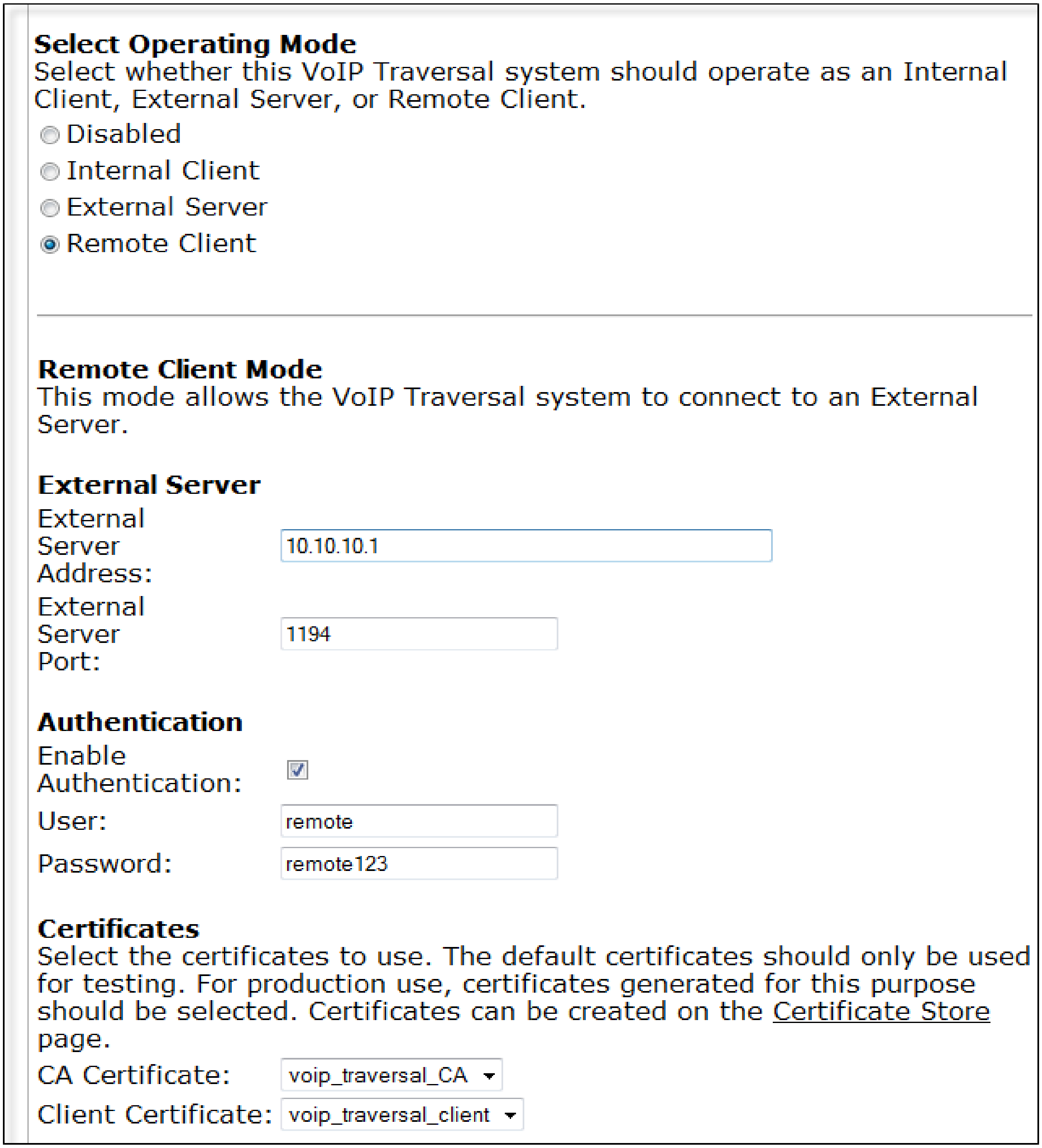
Certificates

Name	Type	CSR	Certificate	Key
voip_traversal_CA	CA Certificate		Download	Download
voip_traversal_client	VoIP Traversal Client		Download	Download

6.2.4. 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 6.1.5**
- **Certificates**: choose CA and Client certificates to be used. Click **Submit** (not shown).



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

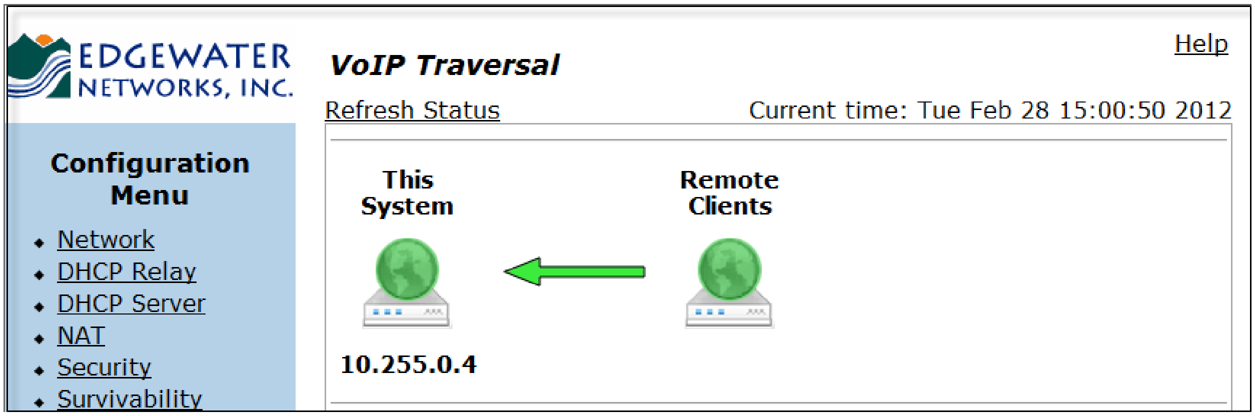
Select the certificates to use. The default certificates should only be used for testing. For production use, certificates generated for this purpose should be selected. Certificates can be created on the Certificate Store page.

CA Certificate:	voip_traversal_CA
Client Certificate:	voip_traversal_client

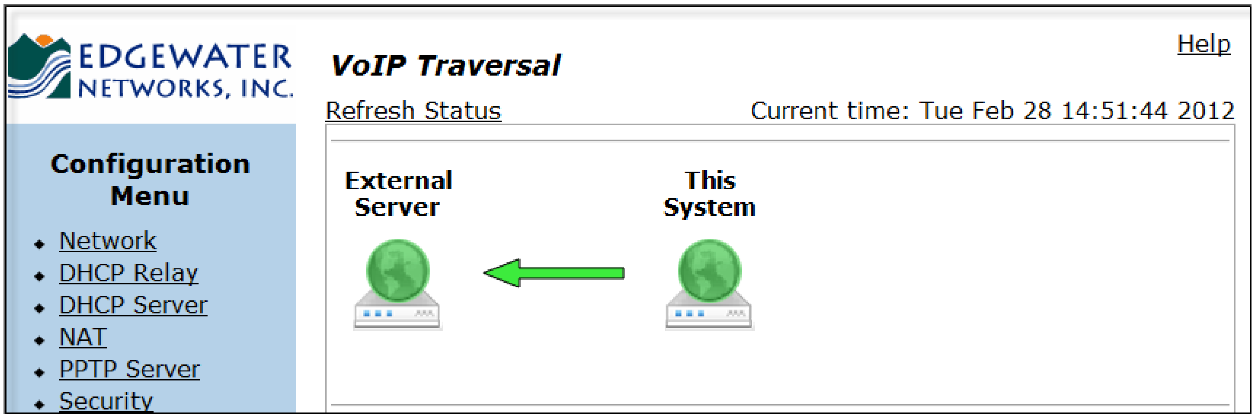
7. Verification Steps

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

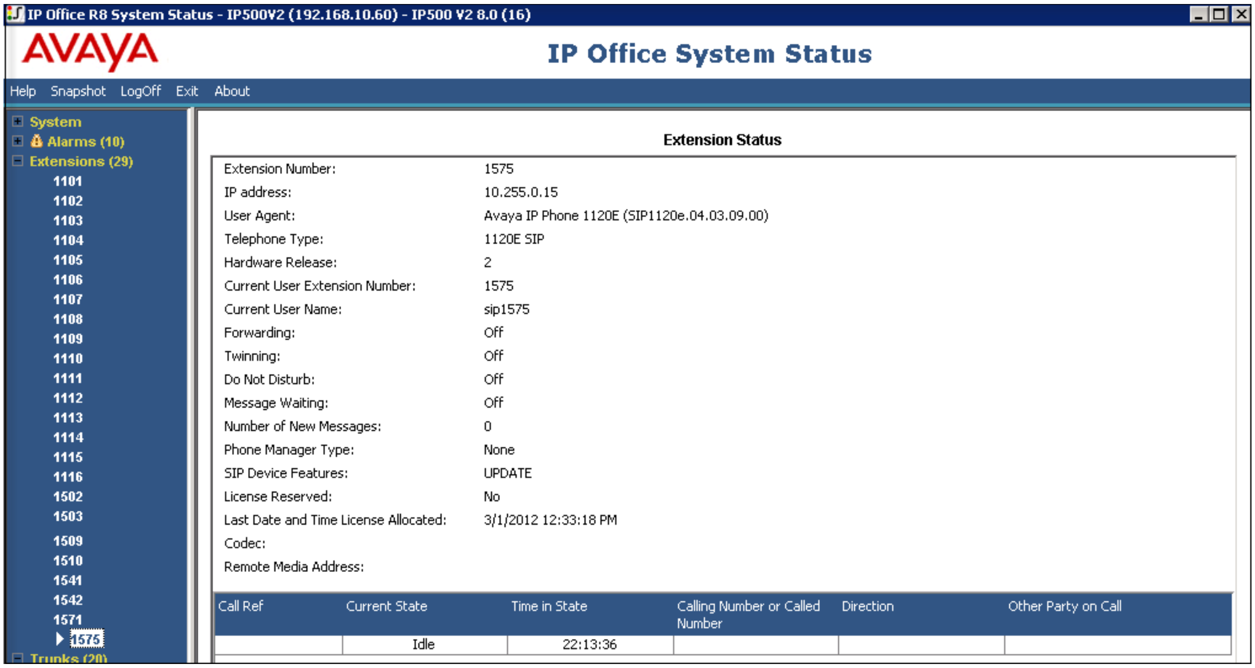
- On the EdgeProtect **Configuration Menu**, select **VOIP Traversal.** The symbols on the top of the page should be green, like in the screen below. By moving the mouse cursor over the image, a more detailed description of the current status can be seen. If an error has occurred, the error message will be shown here. The status of the VoIP Traversal can be updated clicking the **Refresh Status** link.



- Similarly, the same screen on the EdgeMarc should look like this:



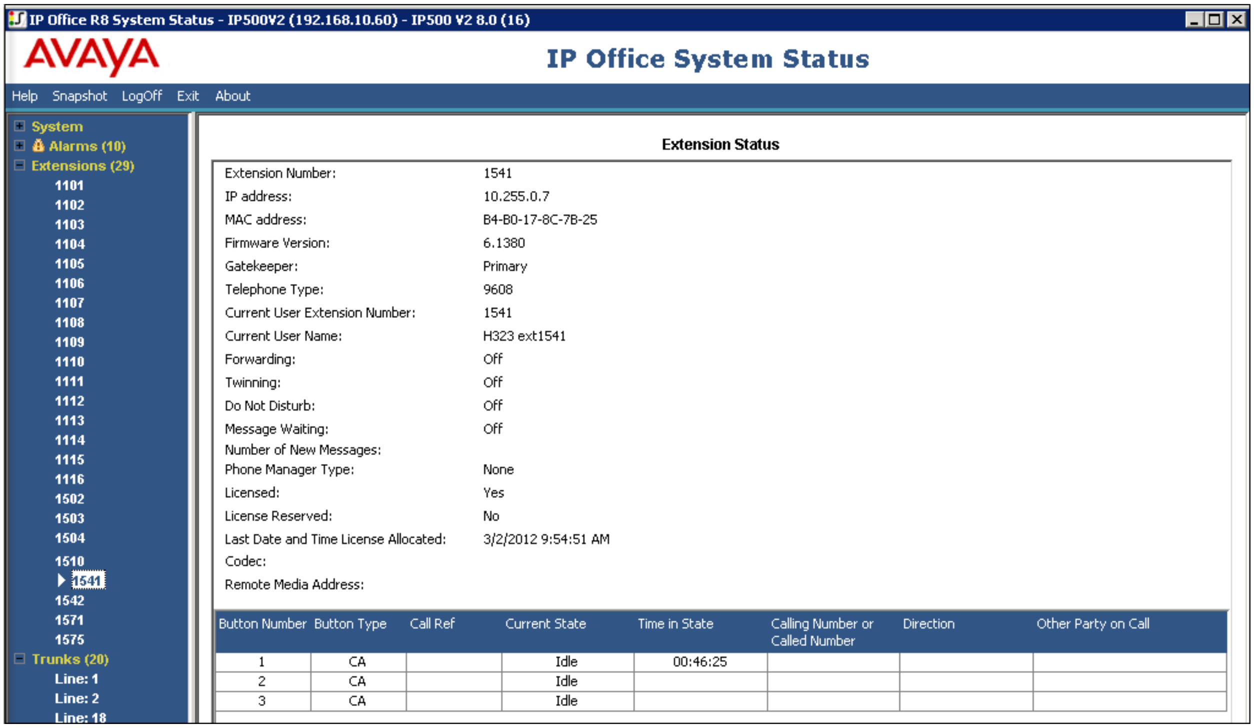
- The Avaya IP Office System Status Application may be used to verify the service state of the remote extensions. Launch the application from **Start → Programs → IP Office →System Status.** The screens show examples for one SIP and one H.323 extension.



Extension Status

Extension Number: 1575
IP address: 10.255.0.15
User Agent: Avaya IP Phone 1120E (SIP1120e.04.03.09.00)
Telephone Type: 1120E SIP
Hardware Release: 2
Current User Extension Number: 1575
Current User Name: sip1575
Forwarding: Off
Twinning: Off
Do Not Disturb: Off
Message Waiting: Off
Number of New Messages: 0
Phone Manager Type: None
SIP Device Features: UPDATE
License Reserved: No
Last Date and Time License Allocated: 3/1/2012 12:33:18 PM
Codec:
Remote Media Address:

Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
	Idle	22:13:36			

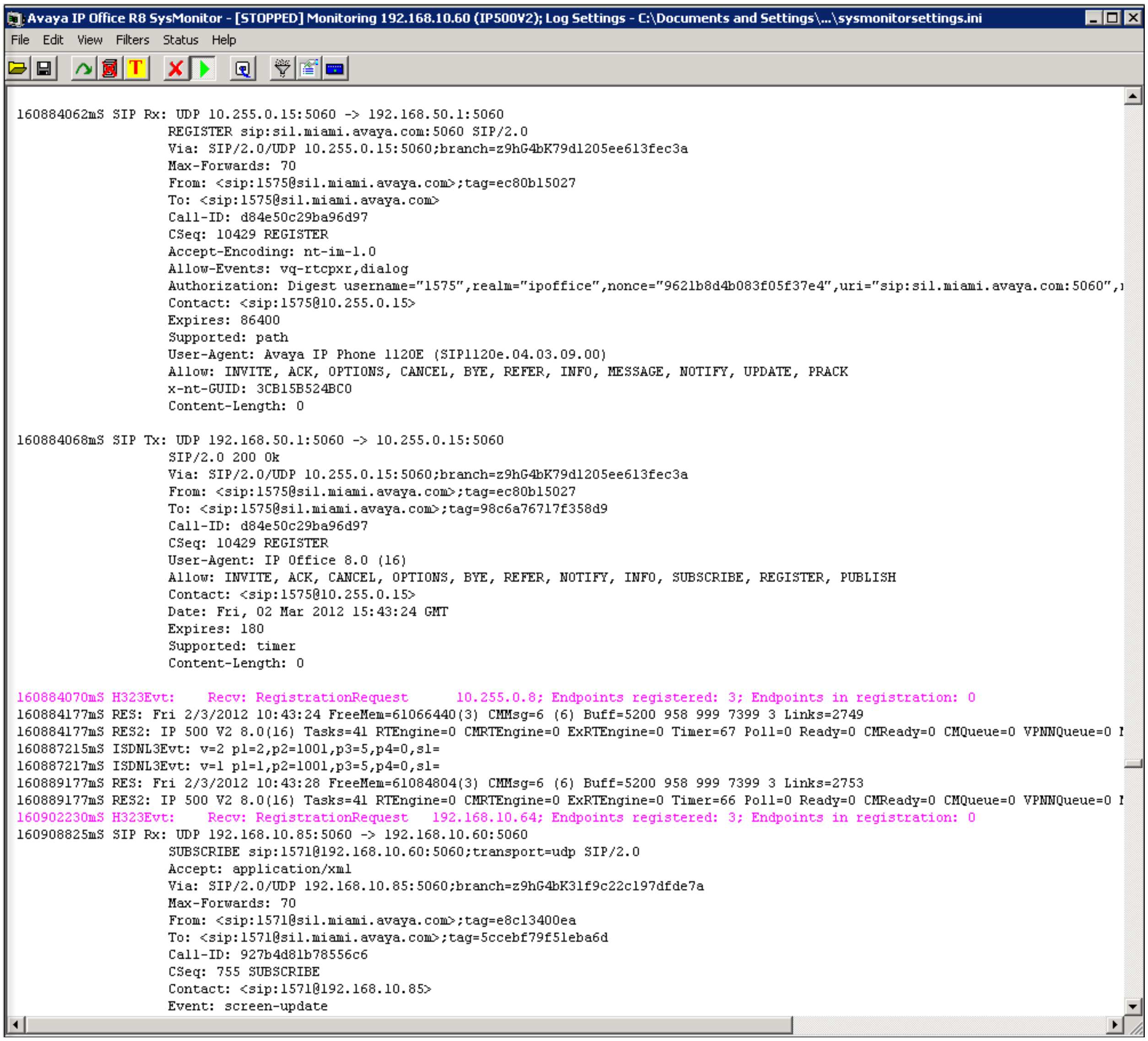


Extension Status

Extension Number: 1541
IP address: 10.255.0.7
MAC address: B4-B0-17-8C-7B-25
Firmware Version: 6.1380
Gatekeeper: Primary
Telephone Type: 9608
Current User Extension Number: 1541
Current User Name: H323 ext1541
Forwarding: Off
Twinning: Off
Do Not Disturb: Off
Message Waiting: Off
Number of New Messages:
Phone Manager Type: None
Licensed: Yes
License Reserved: No
Last Date and Time License Allocated: 3/2/2012 9:54:51 AM
Codec:
Remote Media Address:

Button Number	Button Type	Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
1	CA		Idle	00:46:25			
2	CA		Idle				
3	CA		Idle				

- The registration of the remote users can be monitored in IP Office by means of the System Monitor utility. Launch the application from **Start → Programs → IP Office →Monitor.**

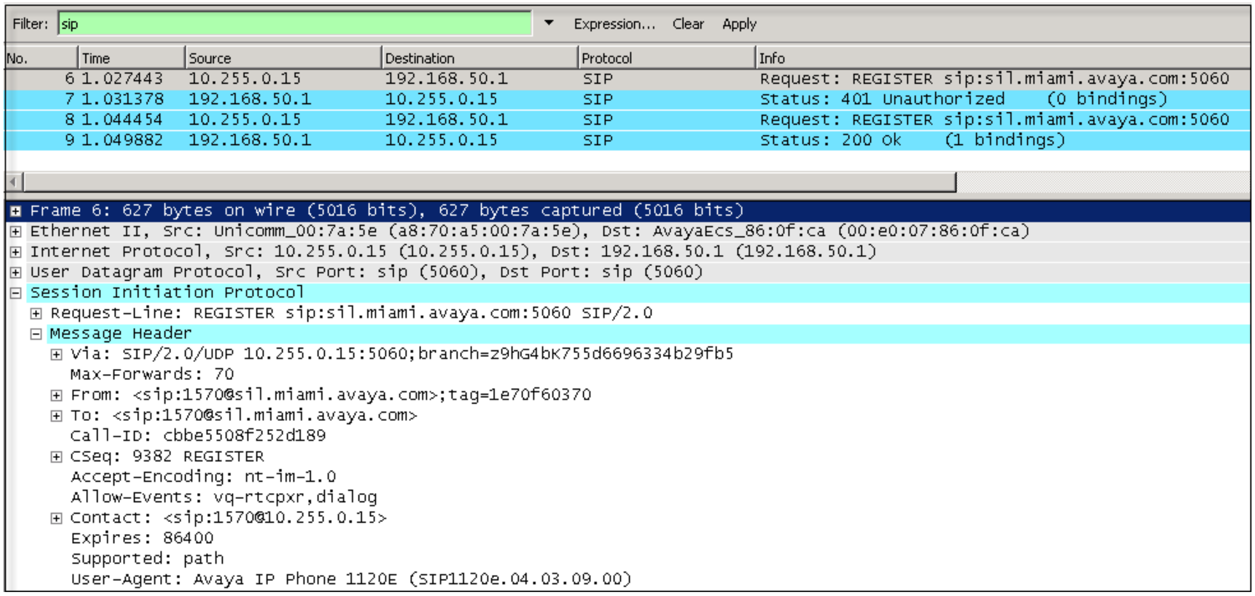

Avaya IP Office R8 SysMonitor - [STOPPED] Monitoring 192.168.10.60 (IP500V2); Log Settings - C:\Documents and Settings\...\sysmonitorsettings.ini
File
Edit
View
Filters
Status
Help

```
160884062mS SIP Rx: UDP 10.255.0.15:5060 -> 192.168.50.1:5060
                    REGISTER sip:sil.miami.avaya.com:5060 SIP/2.0
                    Via: SIP/2.0/UDP 10.255.0.15:5060;branch=z9hG4bK79d1205ee613fec3a
                    Max-Forwards: 70
                    From: <sip:1575@sil.miami.avaya.com>;tag=ec80b15027
                    To: <sip:1575@sil.miami.avaya.com>
                    Call-ID: d84e50c29ba96d97
                    CSeq: 10429 REGISTER
                    Accept-Encoding: nt-im-1.0
                    Allow-Events: vq-rtcpxr,dialog
                    Authorization: Digest username="1575",realm="ipoffice",nonce="9621b8d4b083f05f37e4",uri="sip:sil.miami.avaya.com:5060",
                    Contact: <sip:1575@10.255.0.15>
                    Expires: 86400
                    Supported: path
                    User-Agent: Avaya IP Phone 1120E (SIP1120e.04.03.09.00)
                    Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, REFER, INFO, MESSAGE, NOTIFY, UPDATE, PRACK
                    x-nt-GUID: 3CB15B524BC0
                    Content-Length: 0

160884068mS SIP Tx: UDP 192.168.50.1:5060 -> 10.255.0.15:5060
                    SIP/2.0 200 Ok
                    Via: SIP/2.0/UDP 10.255.0.15:5060;branch=z9hG4bK79d1205ee613fec3a
                    From: <sip:1575@sil.miami.avaya.com>;tag=ec80b15027
                    To: <sip:1575@sil.miami.avaya.com>;tag=98c6a76717f358d9
                    Call-ID: d84e50c29ba96d97
                    CSeq: 10429 REGISTER
                    User-Agent: IP Office 8.0 (16)
                    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, SUBSCRIBE, REGISTER, PUBLISH
                    Contact: <sip:1575@10.255.0.15>
                    Date: Fri, 02 Mar 2012 15:43:24 GMT
                    Expires: 180
                    Supported: timer
                    Content-Length: 0

160884070mS H323Evt:    Recv: RegistrationRequest      10.255.0.8; Endpoints registered: 3; Endpoints in registration: 0
160884177mS RES: Fri 2/3/2012 10:43:24 FreeMem=61066440(3) CMMsg=6 (6) Buff=5200 958 999 7399 3 Links=2749
160884177mS RES2: IP 500 V2 8.0(16) Tasks=41 RTEngine=0 CMRTEngine=0 ExRTEngine=0 Timer=67 Poll=0 Ready=0 CMReady=0 CMQueue=0 VPNNQueue=0
160887215mS ISDNL3Evt: v=2 pl=2,p2=1001,p3=5,p4=0,sl=
160887217mS ISDNL3Evt: v=1 pl=1,p2=1001,p3=5,p4=0,sl=
160889177mS RES: Fri 2/3/2012 10:43:28 FreeMem=61084804(3) CMMsg=6 (6) Buff=5200 958 999 7399 3 Links=2753
160889177mS RES2: IP 500 V2 8.0(16) Tasks=41 RTEngine=0 CMRTEngine=0 ExRTEngine=0 Timer=66 Poll=0 Ready=0 CMReady=0 CMQueue=0 VPNNQueue=0
160902230mS H323Evt:    Recv: RegistrationRequest   192.168.10.64; Endpoints registered: 3; Endpoints in registration: 0
160908825mS SIP Rx: UDP 192.168.10.85:5060 -> 192.168.10.60:5060
                    SUBSCRIBE sip:1571@192.168.10.60:5060;transport=udp SIP/2.0
                    Accept: application/xml
                    Via: SIP/2.0/UDP 192.168.10.85:5060;branch=z9hG4bK31f9c22c197dfde7a
                    Max-Forwards: 70
                    From: <sip:1571@sil.miami.avaya.com>;tag=e8c13400ea
                    To: <sip:1571@sil.miami.avaya.com>;tag=5ccebf79f51eba6d
                    Call-ID: 927b4d81b78556c6
                    CSeq: 755 SUBSCRIBE
                    Contact: <sip:1571@192.168.10.85>
                    Event: screen-update
```

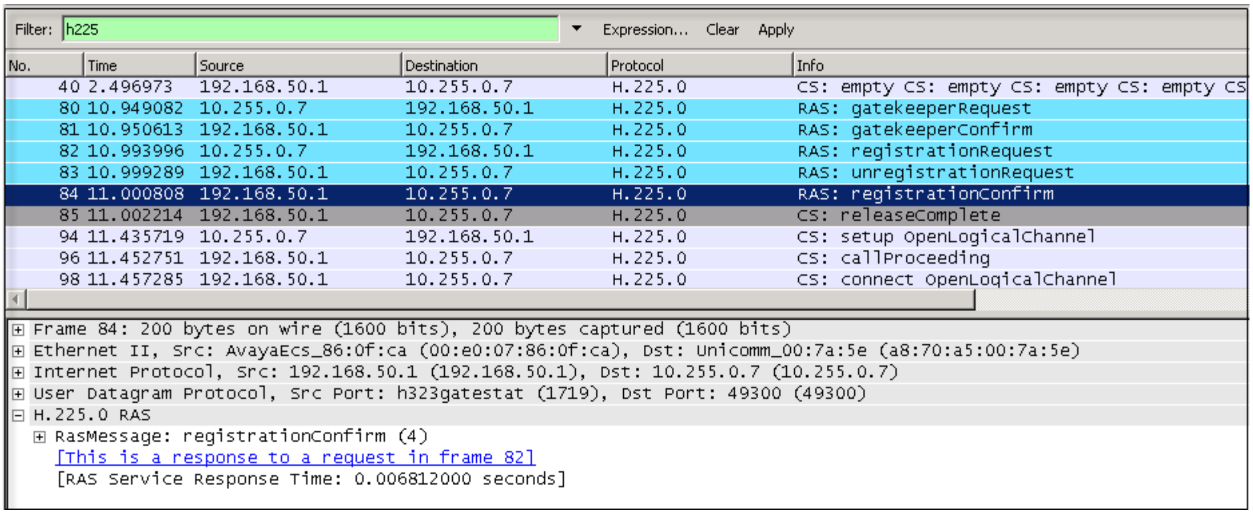
- Wireshark captures can be taken to verify the registration requests from the remote users. The next screen shows an example of the registration of the SIP remote user 1570, taken at the LAN2 interface of the IP Office.



```
No.  Time      Source         Destination    Protocol  Info
   6 1.027443  10.255.0.15    192.168.50.1   SIP       Request: REGISTER sip:sil.miami.avaya.com:5060
   7 1.031378  192.168.50.1   10.255.0.15    SIP       Status: 401 Unauthorized    (0 bindings)
   8 1.044454  10.255.0.15    192.168.50.1   SIP       Request: REGISTER sip:sil.miami.avaya.com:5060
   9 1.049882  192.168.50.1   10.255.0.15    SIP       Status: 200 Ok     (1 bindings)
```

```
⊞ Frame 6: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits)
⊞ Ethernet II, Src: Unicomm_00:7a:5e (a8:70:a5:00:7a:5e), Dst: AvayaEcs_86:0f:ca (00:e0:07:86:0f:ca)
⊞ Internet Protocol, Src: 10.255.0.15 (10.255.0.15), Dst: 192.168.50.1 (192.168.50.1)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:sil.miami.avaya.com:5060 SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 10.255.0.15:5060;branch=z9hG4bK755d6696334b29fb5
      Max-Forwards: 70
    ⊞ From: <sip:1570@sil.miami.avaya.com>;tag=1e70f60370
    ⊞ To: <sip:1570@sil.miami.avaya.com>
      Call-ID: cbbe5508f252d189
    ⊞ CSeq: 9382 REGISTER
      Accept-Encoding: nt-im-1.0
      Allow-Events: vq-rtcpxr,dialog
    ⊞ Contact: <sip:1570@10.255.0.15>
      Expires: 86400
      Supported: path
      User-Agent: Avaya IP Phone 1120E (SIP1120e.04.03.09.00)
```

The next screen shows the capture of the registration of the H.323 remote user 1541, taken at the LAN2 interface of the IP Office.



```
No.  Time       Source         Destination    Protocol  Info
  40 2.496973   192.168.50.1   10.255.0.7     H.225.0   CS: empty CS: empty CS: empty CS: empty CS
  80 10.949082  10.255.0.7     192.168.50.1   H.225.0   RAS: gatekeeperRequest
  81 10.950613  192.168.50.1   10.255.0.7     H.225.0   RAS: gatekeeperConfirm
  82 10.993996  10.255.0.7     192.168.50.1   H.225.0   RAS: registrationRequest
  83 10.999289  192.168.50.1   10.255.0.7     H.225.0   RAS: unregistrationRequest
  84 11.000808  192.168.50.1   10.255.0.7     H.225.0   RAS: registrationConfirm
  85 11.002214  192.168.50.1   10.255.0.7     H.225.0   CS: releaseComplete
  94 11.435719  10.255.0.7     192.168.50.1   H.225.0   CS: setup OpenLogicalChannel
  96 11.452751  192.168.50.1   10.255.0.7     H.225.0   CS: callProceeding
  98 11.457285  192.168.50.1   10.255.0.7     H.225.0   CS: connect OpenLogicalChannel
```

```
⊞ Frame 84: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
⊞ Ethernet II, Src: AvayaEcs_86:0f:ca (00:e0:07:86:0f:ca), Dst: Unicomm_00:7a:5e (a8:70:a5:00:7a:5e)
⊞ Internet Protocol, Src: 192.168.50.1 (192.168.50.1), Dst: 10.255.0.7 (10.255.0.7)
⊞ User Datagram Protocol, Src Port: h323gatestat (1719), Dst Port: 49300 (49300)
⊟ H.225.0 RAS
  ⊞ RasMessage: registrationConfirm (4)
    [This is a response to a request in frame 82]
    [RAS Service Response Time: 0.006812000 seconds]
```

8. Conclusion

These Application Notes describe the procedures for configuring the EdgeProtect and EdgeMarc Enterprise Session Border Controllers from Edgewater Networks, to interoperate with Avaya IP Office 8.0 in a distributed IP Telephony environment, supporting a Branch Office with Remote Users, 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

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.