



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.

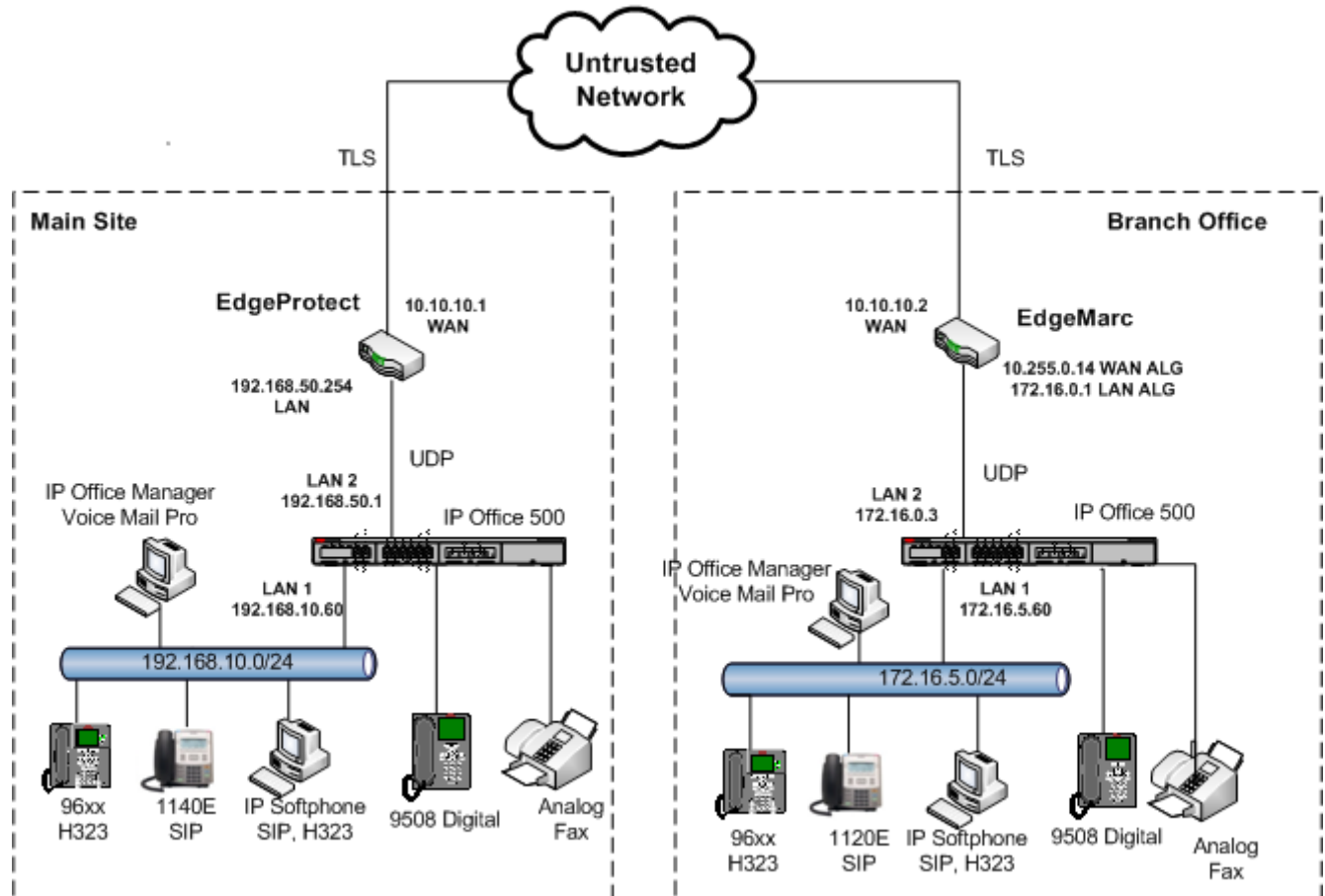


Figure 1. Test Configuration

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.

The screenshot displays the Avaya IP Office configuration interface. On the left, the 'IP Offices' pane shows a tree structure with 'IP500V2 Main' selected. The 'License' pane in the center lists various license types, with 'SIP Trunk Channels' highlighted at the bottom. The 'SIP Trunk Channels' pane on the right shows the 'Licenses' tab with the following details:

Field	Value
License Key	XnMHe6b9DXL42wonZxtw0UgrhsPgbH
License Type	SIP Trunk Channels
License Status	Valid
Instances	255
Expiry Date	Never

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:

IP Offices	System	IP500V2 Main																																																																																																			
BOOTP (4) Operator (3) IP500V2 Main System (1) Line (20) Control Unit (5) Extension (45) User (47) HuntGroup (1) Short Code (63) Service (0) RAS (1) Incoming Call Ro WanPort (0) Directory (0) Time Profile (0) Firewall Profile (1) IP Route (4)	Name IP500V2 Main	<table border="1"><thead><tr><th>System</th><th>LAN1</th><th>LAN2</th><th>DNS</th><th>Voicemail</th><th>Telephony</th><th>Directory Services</th><th>System Events</th><th>SMTP</th></tr></thead><tbody><tr><td colspan="9">LAN Settings VoIP Network Topology SIP Registrar</td></tr><tr><td colspan="2">IP Address</td><td colspan="7">192 . 168 . 50 . 1</td></tr><tr><td colspan="2">IP Mask</td><td colspan="7">255 . 255 . 255 . 0</td></tr><tr><td colspan="2">Primary Trans. IP Address</td><td colspan="7">0 . 0 . 0 . 0</td></tr><tr><td colspan="2">Firewall Profile</td><td colspan="7"><None></td></tr><tr><td colspan="2">RIP Mode</td><td colspan="7">None</td></tr><tr><td colspan="2">Enable NAT</td><td colspan="7"><input type="checkbox"/></td></tr><tr><td colspan="2">Number Of DHCP IP Addresses</td><td colspan="7">200</td></tr><tr><td colspan="2">DHCP Mode</td><td colspan="7"><input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled</td></tr><tr><td colspan="2"></td><td colspan="7">Advanced</td></tr></tbody></table>	System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	LAN Settings VoIP Network Topology SIP Registrar									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		<input type="checkbox"/>							Number Of DHCP IP Addresses		200							DHCP Mode		<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled									Advanced						
System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP																																																																																													
LAN Settings VoIP Network Topology SIP Registrar																																																																																																					
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		<input type="checkbox"/>																																																																																																			
Number Of DHCP IP Addresses		200																																																																																																			
DHCP Mode		<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled																																																																																																			
		Advanced																																																																																																			

For the Branch Office:

IP Offices	System	IP500V2 Branch																																																																																																			
BOOTP (4) Operator (3) IP500V2 Branch System (1) Line (3) Control Unit (4) Extension (27) User (29) HuntGroup (1) Short Code (57) Service (0) RAS (1) Incoming Call Rout WanPort (0) Directory (0) Time Profile (0) Firewall Profile (1) IP Route (2)	Name IP500V2 Bra	<table border="1"><thead><tr><th>System</th><th>LAN1</th><th>LAN2</th><th>DNS</th><th>Voicemail</th><th>Telephony</th><th>Directory Services</th><th>System Events</th><th>SMTP</th></tr></thead><tbody><tr><td colspan="9">LAN Settings VoIP Network Topology SIP Registrar</td></tr><tr><td colspan="2">IP Address</td><td colspan="7">172 . 16 . 0 . 3</td></tr><tr><td colspan="2">IP Mask</td><td colspan="7">255 . 255 . 255 . 0</td></tr><tr><td colspan="2">Primary Trans. IP Address</td><td colspan="7">0 . 0 . 0 . 0</td></tr><tr><td colspan="2">Firewall Profile</td><td colspan="7"><None></td></tr><tr><td colspan="2">RIP Mode</td><td colspan="7">None</td></tr><tr><td colspan="2">Enable NAT</td><td colspan="7"><input type="checkbox"/></td></tr><tr><td colspan="2">Number Of DHCP IP Addresses</td><td colspan="7">1</td></tr><tr><td colspan="2">DHCP Mode</td><td colspan="7"><input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled</td></tr><tr><td colspan="2"></td><td colspan="7">Advanced</td></tr></tbody></table>	System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	LAN Settings VoIP Network Topology SIP Registrar									IP Address		172 . 16 . 0 . 3							IP Mask		255 . 255 . 255 . 0							Primary Trans. IP Address		0 . 0 . 0 . 0							Firewall Profile		<None>							RIP Mode		None							Enable NAT		<input type="checkbox"/>							Number Of DHCP IP Addresses		1							DHCP Mode		<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled									Advanced						
System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP																																																																																													
LAN Settings VoIP Network Topology SIP Registrar																																																																																																					
IP Address		172 . 16 . 0 . 3																																																																																																			
IP Mask		255 . 255 . 255 . 0																																																																																																			
Primary Trans. IP Address		0 . 0 . 0 . 0																																																																																																			
Firewall Profile		<None>																																																																																																			
RIP Mode		None																																																																																																			
Enable NAT		<input type="checkbox"/>																																																																																																			
Number Of DHCP IP Addresses		1																																																																																																			
DHCP Mode		<input type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Dialin <input checked="" type="radio"/> Disabled																																																																																																			
		Advanced																																																																																																			

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.

The screenshot shows the Avaya IP Office configuration interface, specifically the VoIP tab. The interface is divided into several sections:

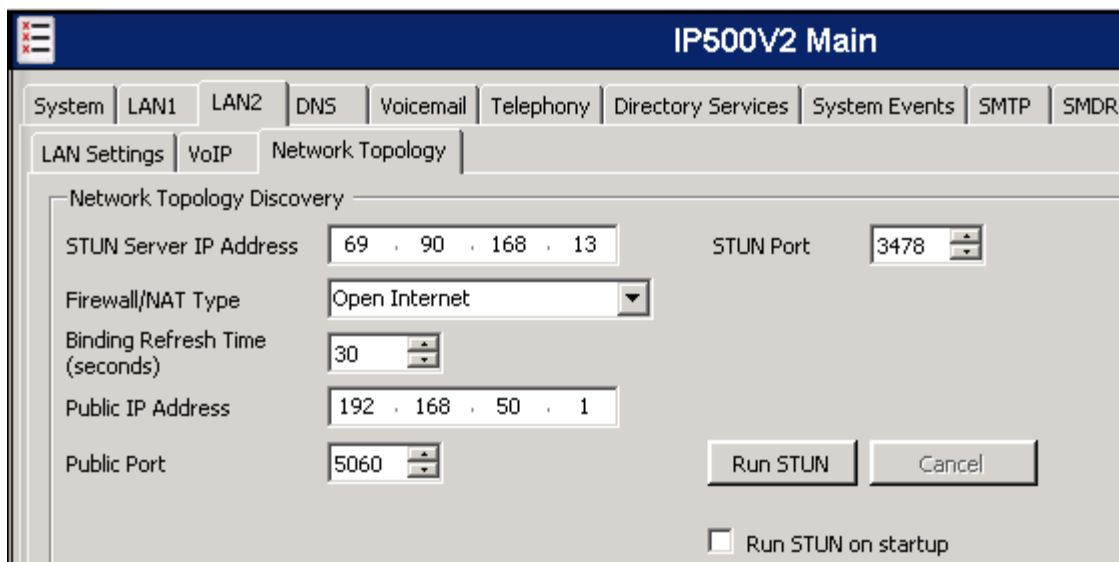
- System Settings:** Includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, and SMTP.
- LAN Settings:** Includes tabs for LAN Settings, VoIP, and Network Topology.
- VoIP Settings:**
 - ☐ H.323 Gatekeeper Enable
 - ☒ SIP Trunks Enable
 - ☐ SIP Registrar Enable
- RTP Port Number Range:**
 - ☐ H.323 Auto-create Extn
 - ☐ H.323 Auto-create User
 - ☐ H.323 Remote Extn Enable
 - ☒ Enable RTCP Monitoring On Port 5005
- DiffServ Settings:**
 - DSCP(Hex): 88, DSCP Mask (Hex): FC, SIG DSCP (Hex): 88
 - DSCP: 46, DSCP Mask: 63, SIG DSCP: 34
- 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: (empty field)
- RTP Keepalives:**
 - Scope: Disabled, Periodic timeout: 0
 - Initial keepalives: Disabled

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

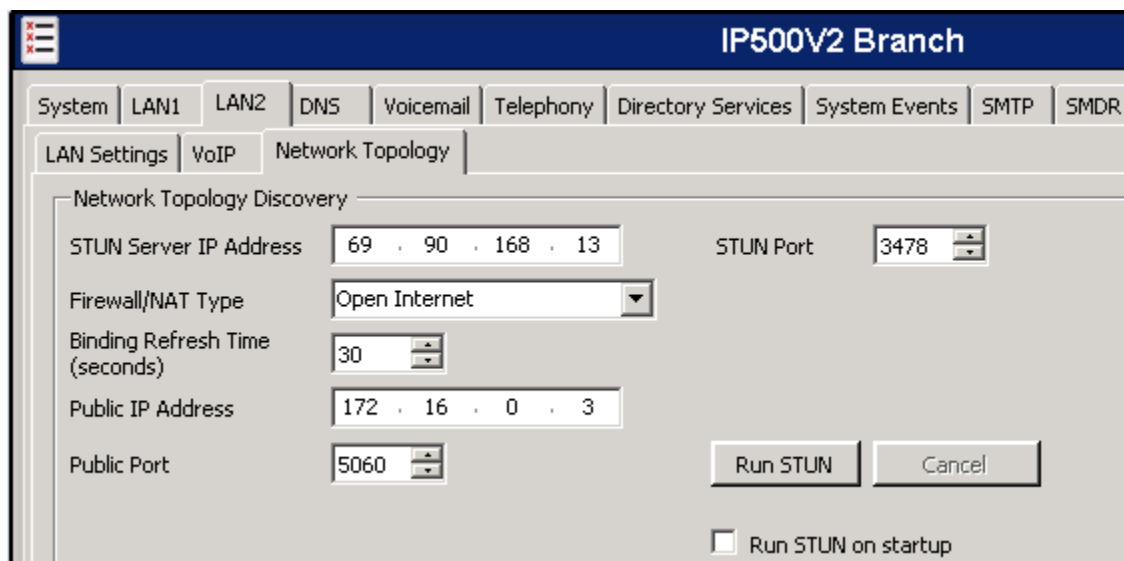
- Select the **Firewall/NAT Type** from the pull-down menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used.
- Set **Binding Refresh Time (seconds)** to **30**. This value determines the frequency at which Avaya IP Office will send SIP OPTIONS 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:



The screenshot shows the 'IP500V2 Main' configuration window. The 'Network Topology' tab is selected. The 'Network Topology Discovery' section contains the following settings: STUN Server IP Address (69 . 90 . 168 . 13), STUN Port (3478), Firewall/NAT Type (Open Internet), Binding Refresh Time (seconds) (30), Public IP Address (192 . 168 . 50 . 1), and Public Port (5060). There are 'Run STUN' and 'Cancel' buttons, and a checkbox for 'Run STUN on startup' which is unchecked.



The screenshot shows the 'IP500V2 Branch' configuration window. The 'Network Topology' tab is selected. The 'Network Topology Discovery' section contains the following settings: STUN Server IP Address (69 . 90 . 168 . 13), STUN Port (3478), Firewall/NAT Type (Open Internet), Binding Refresh Time (seconds) (30), Public IP Address (172 . 16 . 0 . 3), and Public Port (5060). There are 'Run STUN' and 'Cancel' buttons, and a checkbox for 'Run STUN on startup' which is unchecked.

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.

The screenshot shows the 'IP500V2' configuration window with the 'Telephony' tab selected. The left pane shows a tree view of system components. The main area contains settings for analogue extensions and companding law. Under 'Analogue Extensions', there are dropdowns for 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), and 'Default Ring Back Sequence' (Ring Type 2). There are also input fields for '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), and 'Default Name Priority' (Favor Trunk). The 'Companding Law' section has two sub-sections: 'Switch' and 'Line'. Both have radio buttons for 'U-Law' (selected) and 'A-Law'. Below this, there are several checkboxes: 'DSS Status' (unchecked), 'Auto Hold' (checked), 'Dial By Name' (checked), 'Show Account Code' (checked), 'Inhibit Off-Switch Forward/Transfer' (unchecked), 'Restrict Network Interconnect' (unchecked), 'Drop External Only Impromptu Conference' (unchecked), 'Visually Differentiate External Call' (unchecked), 'Unsupervised Analog Trunk Disconnect Handling' (unchecked), and 'High Quality Conferencing' (checked).

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.

The screenshot shows the 'IP500V2' configuration window with the 'Codecs' tab selected. The main area is divided into three sections: 'Available Codecs', 'Default Codec Selection', and 'Selected'. The 'Available Codecs' list contains: G.711 ULAW 64K (checked), G.711 ALAW 64K (checked), G.722 64K (unchecked), G.729(a) 8K CS-ACELP (checked), and G.723.1 6K3 MP-MLQ (checked). The 'Default Codec Selection' section has an 'Unused' list (empty) and a 'Selected' list containing: G.729(a) 8K CS-ACELP, G.711 ULAW 64K, G.711 ALAW 64K, and G.723.1 6K3 MP-MLQ. Between the 'Unused' and 'Selected' lists are buttons for moving codecs: '>>' (top), '<<' (bottom), and up/down arrows in the middle.

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:

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials
Line Number	18				
ITSP Domain Name	192.168.50.1		In Service	<input checked="" type="checkbox"/>	
			Use Tel URI	<input type="checkbox"/>	
Prefix			Check OOS	<input checked="" type="checkbox"/>	
National Prefix	0		Call Routing Method	Request URI	
Country Code			Originator number for forwarded and twinning calls		
International Prefix	00		Name Priority	System Default	
Send Caller ID	Diversion Header				
Association Method	By Source IP address				
<input checked="" type="checkbox"/> REFER Support					
Incoming	Always				
Outgoing	Always				

Branch Site:

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials
Line Number	17				
ITSP Domain Name	172.16.0.3		In Service	<input checked="" type="checkbox"/>	
Prefix			Use Tel URI	<input type="checkbox"/>	
National Prefix	0		Check OOS	<input checked="" type="checkbox"/>	
Country Code			Call Routing Method	Request URI	
International Prefix	00		Originator number for forwarded and twinning calls		
Send Caller ID	Diversion Header		Name Priority	System Default	
Association Method	By Source IP address				
<input checked="" type="checkbox"/> REFER Support					
Incoming	Always				
Outgoing	Always				

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.

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials
ITSP Proxy Address					
Network Configuration					
Layer 4 Protocol	UDP		Send Port	5060	
Use Network Topology Info	LAN 2		Listen Port	5060	
Explicit DNS Server(s)	0 . 0 . 0 . 0		0 . 0 . 0 . 0		
Calls Route via Registrar	<input checked="" type="checkbox"/>				

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**.

The screenshot shows the 'SIP Line' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' field is set to '172.16.0.1'. Under the 'Network Configuration' section, 'Layer 4 Protocol' is set to 'UDP', 'Send Port' is '5060', 'Use Network Topology Info' is set to 'LAN 2', and 'Listen Port' is '5060'. The 'Explicit DNS Server(s)' fields are both set to '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is checked.

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:

The screenshot shows the 'SIP Line - Line 18' configuration window with the 'SIP URI' tab selected. The 'Edit Channel' section contains the following fields: 'Via' is '192.168.50.1'; 'Local URI', 'Contact', 'Display Name', and 'PAI' are all set to 'Use Internal Data'; 'Registration' is set to '0: <None>'; 'Incoming Group' is '18'; 'Outgoing Group' is '18'; and 'Max Calls per Channel' is '10'. 'OK' and 'Cancel' buttons are visible on the right.

Branch Office:

The screenshot shows the 'SIP Line - Line 17*' configuration window with the 'Edit Channel' tab selected. The window has tabs for SIP Line, Transport, SIP URI, VoIP, T38 Fax, and SIP Credentials. The 'Edit Channel' section contains the following fields:

- Via: 172.16.0.3
- Local URI: Use Internal Data (dropdown)
- Contact: Use Internal Data (dropdown)
- Display Name: Use Internal Data (dropdown)
- PAI: Use Internal Data (dropdown)
- Registration: 0: <None> (dropdown)
- Incoming Group: 17
- Outgoing Group: 17
- Max Calls per Channel: 10 (spinner)

Buttons for OK and Cancel are located in the top right corner.

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.

The screenshot shows the 'SIP Line - Line 17*' configuration window with the 'VoIP' tab selected. The window has tabs for SIP Line, Transport, SIP URI, VoIP, T38 Fax, and SIP Credentials. The 'VoIP' section contains the following fields:

- Codec Selection: Custom (dropdown)
- Unused codecs list: G.711 ALAW 64K, G.723.1 6K3 MP-MLQ
- Selected codecs list: G.729(a) 8K CS-ACELP, G.711 ULAW 64K
- Buttons: >>, <<, <-, >+, >>, <<<, >>>
- Fax Transport Support: T38 Fallback (dropdown)
- Call Initiation Timeout (s): 4 (spinner)
- DTMF Support: RFC2833 (dropdown)
- Checkboxes: VoIP Silence Suppression (unchecked), Re-invite Supported (checked), Use Offerer's Preferred Codec (unchecked), Codec Lockdown (unchecked), PRACK/100rel Supported (unchecked)

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

The screenshot shows a configuration window with several tabs: SIP Line, Transport, SIP URI, VoIP, T38 Fax, and SIP Credentials. The T38 Fax tab is selected. The settings are as follows:

- T38 Fax Version: 3
- Transport: UDPTL
- Redundancy section:
 - Low Speed: 0
 - High Speed: 0
- TCF Method: Trans TCF
- Max Bit Rate (bps): 14400
- EFlag Start Timer (msecs): 2600
- EFlag Stop Timer (msecs): 2300
- Tx Network Timeout (secs): 150
- ☒ Use Default Values
- Advanced options section:
 - ☒ Scan Line Fix-up
 - ☒ TFOP Enhancement
 - ☐ Disable T30 ECM
 - ☐ Disable EFlags For First DIS
 - ☐ Disable T30 MR Compression
 - ☐ NSF Override
 - Country Code: 0
 - Vendor Code: 0

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:

Code	Tel
*35*N#	N
*36	
*37*N#	N
*38*N#	N
*39	1
*40	1
*41	1
*42	2
*43	2
*44	2
*45*N#	N

Short Code

Code: 9N;

Feature: Dial

Telephone Number: N"@172.16.0.3"

Line Group ID: 18

Locale: United States (US English)

Force Account Code: ☐

Branch Office:

Code	Tel
*15	
*16	
*17	
*18	
*19	
*20*N#	
*21*N#	
*29	
*30	
*31	

Short Code

Code: 9N;

Feature: Dial

Telephone Number: N"@192.168.50.1"

Line Group ID: 17

Locale: United States (US English)

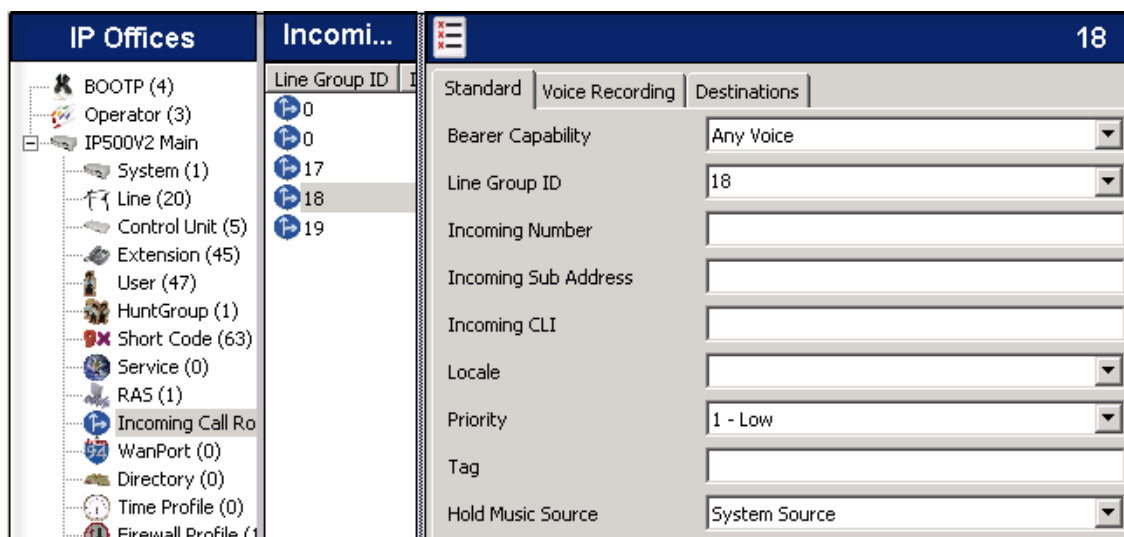
Force Account Code: ☐

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 below:

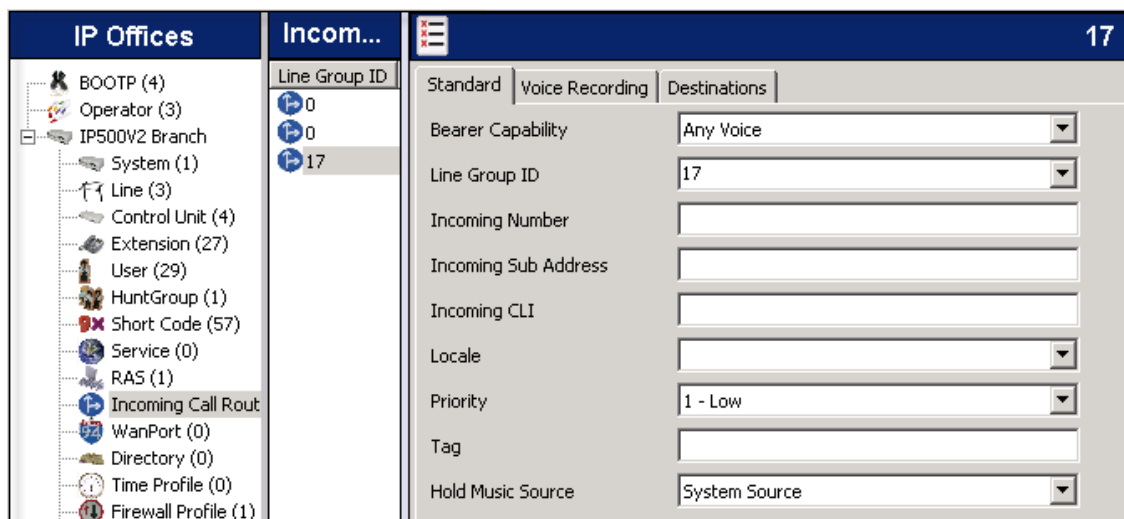
- Set **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5**.
- Default values may be used for all other parameters.

Main site:



IP Offices	Incomi...	Standard	Voice Recording	Destinations
BOOTP (4)	Line Group ID	Bearer Capability		Any Voice
Operator (3)	0	Line Group ID		18
IP500V2 Main	0	Incoming Number		
System (1)	17	Incoming Sub Address		
Line (20)	18	Incoming CLI		
Control Unit (5)	19	Locale		
Extension (45)		Priority		1 - Low
User (47)		Tag		
HuntGroup (1)		Hold Music Source		System Source
Short Code (63)				
Service (0)				
RAS (1)				
Incoming Call Ro				
WanPort (0)				
Directory (0)				
Time Profile (0)				
Firewall Profile (1)				

Branch Office:



IP Offices	Incomi...	Standard	Voice Recording	Destinations
BOOTP (4)	Line Group ID	Bearer Capability		Any Voice
Operator (3)	0	Line Group ID		17
IP500V2 Branch	0	Incoming Number		
System (1)	17	Incoming Sub Address		
Line (3)		Incoming CLI		
Control Unit (4)		Locale		
Extension (27)		Priority		1 - Low
User (29)		Tag		
HuntGroup (1)		Hold Music Source		System Source
Short Code (57)				
Service (0)				
RAS (1)				
Incoming Call Rout				
WanPort (0)				
Directory (0)				
Time Profile (0)				
Firewall Profile (1)				

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.

Standard	Voice Recording	Destinations	
	TimeProfile	Destination	
▶	Default Value	.	

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.

EDGEWATER NETWORKS, INC. [Help](#)

Configuration Menu

- **Network**
 - Subinterfaces
 - VLAN Configuration
 - WAN VLAN Configuration
- DHCP Relay
- DHCP Server
- NAT
- Security
- 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
 - Management Interface
 - Network Information
 - Network Restart
 - Network Test

Network

Networking configuration information for the public and private networks.

LAN Interface Settings:

IP Address:

Subnet Mask:

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:

Subnet Mask:

Network Settings:

Default Gateway:

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**.

<ul style="list-style-type: none">◆ Security<ul style="list-style-type: none">▶ Certificate Store▶ HTTPS Configuration▶ MOTD▶ Pass-Through Rules▶ Session Management▶ System Audit▶ Trusted Hosts▶ User Management◆ Survivability◆ Test UA◆ Traffic Shaper◆ VoIP ALG◆ VoIP Traversal◆ VPN◆ WAN Link◆ Redundancy◆ System<ul style="list-style-type: none">▶ Backup / Restore▶ Clients List▶ Dynamic DNS▶ File Download▶ File Server▶ High Availability▶ Management Interface▶ Network Information▶ Network Restart▶ Network Test Tools▶ Proxy ARP▶ RADIUS Settings▶ Reboot System▶ Route▶ Services Configuration▶ Set Link▶ System Information▶ System Time	<div>Submit Reset Apply Later</div> <div><h3>Create a Certificate</h3><p>Certificate Name: <input type="text" value="voip_traversal_CA"/></p><p>Certificate Type: <input type="text" value="CA Certificate"/></p><p>Key Size: <input type="text" value="1024"/></p><p>Certificate Authority: <input type="text" value="Self-Signed"/></p><p>Country Name (2 letter code): <input type="text" value="US"/></p><p>State or Province (full name): <input type="text" value="FL"/></p><p>Locality Name (e.g., City): <input type="text" value="Miami"/></p><p>Organization (e.g., Company): <input type="text" value="Avaya"/></p><p>Organization Unit: <input type="text" value="SIL"/></p><p>Common Name: <input type="text"/></p><p>Email: <input type="text"/></p><p><i>Password is optional</i></p><p>Password: <input type="text"/></p><p>Password (Verify): <input type="text"/></p><div>Create Certificate Reset</div></div>
---	--

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:

Certificate Type:

Key Size:

Certificate Authority:

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).

Create a Certificate

Certificate Name:

Certificate Type:

Key Size:

Certificate Authority:

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

SSL/TLS Certificate Store

[Help](#)

Configuration Menu

- Network
- DHCP Relay
- DHCP Server
- NAT
- Security
 - Certificate Store
 - HTTPS

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

6.1.3. VoIP Traversal

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

<ul style="list-style-type: none">◆ Test UA◆ Traffic Shaper◆ VoIP ALG◆ VoIP Traversal<ul style="list-style-type: none">▶ Authentication▶ Clients▶ Firewall▶ Routes	Select Operating Mode Select whether this VoIP Traversal system should operate as an Internal Client, External Server, or Remote Client. <ul style="list-style-type: none"><input type="radio"/> Disabled<input type="radio"/> Internal Client<input checked="" type="radio"/> External Server<input type="radio"/> 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:	<input type="text" value="10.255.0.0"/>
Traversal Network Mask (bits):	<input type="text" value="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:	<input type="text" value="voip_traversal_CA"/>
Server Certificate:	<input type="text" value="voip_traversal_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**.

**EDGEWATER
NETWORKS, INC.**


**Configuration
Menu**

- ◆ [Network](#)
- ◆ [DHCP Relay](#)
- ◆ [DHCP Server](#)
- ◆ [NAT](#)
- ◆ [Security](#)
- ◆ [Survivability](#)
- ◆ [Test UA](#)
- ◆ [Traffic Shaper](#)
- ◆ [VoIP ALG](#)
- ◆ [VoIP Traversal](#)
 - [Authentication](#)
 - [Clients](#)
 - [Firewall](#)
 - [Routes](#)

VoIP Traversal Routes

[Help](#)

VoIP Traversal Routes defines networks the system will use to route traffic to the internal subnets. The system will also push these networks as routes to connecting VPN clients. Any route added here will cause the VPN client to send traffic that matches this network through the VPN tunnel.

Destination	Network Mask (Bits)
 192.168.50.0	24

Add a new Route Entry

Destination:

Network Mask (Bits):

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.

EDGEWATER NETWORKS, INC. **Authentication** [Help](#)

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.

User	Password
Add a new User	
User Name:	<input type="text"/>
Password:	<input type="text"/>
<input type="button" value="Add"/>	<input type="button" value="Clear"/>

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

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


User	Password
<input type="button" value="x"/> remote	remote123

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.

**Network**[Help](#)

Networking configuration information for the public and private networks.

LAN Interface Settings:
IP Address:
Subnet Mask:
IPv6 Address/Prefix:
Enable VLAN support ☒
Default VLAN ID:
[VLAN Configuration](#)

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:
Subnet Mask:

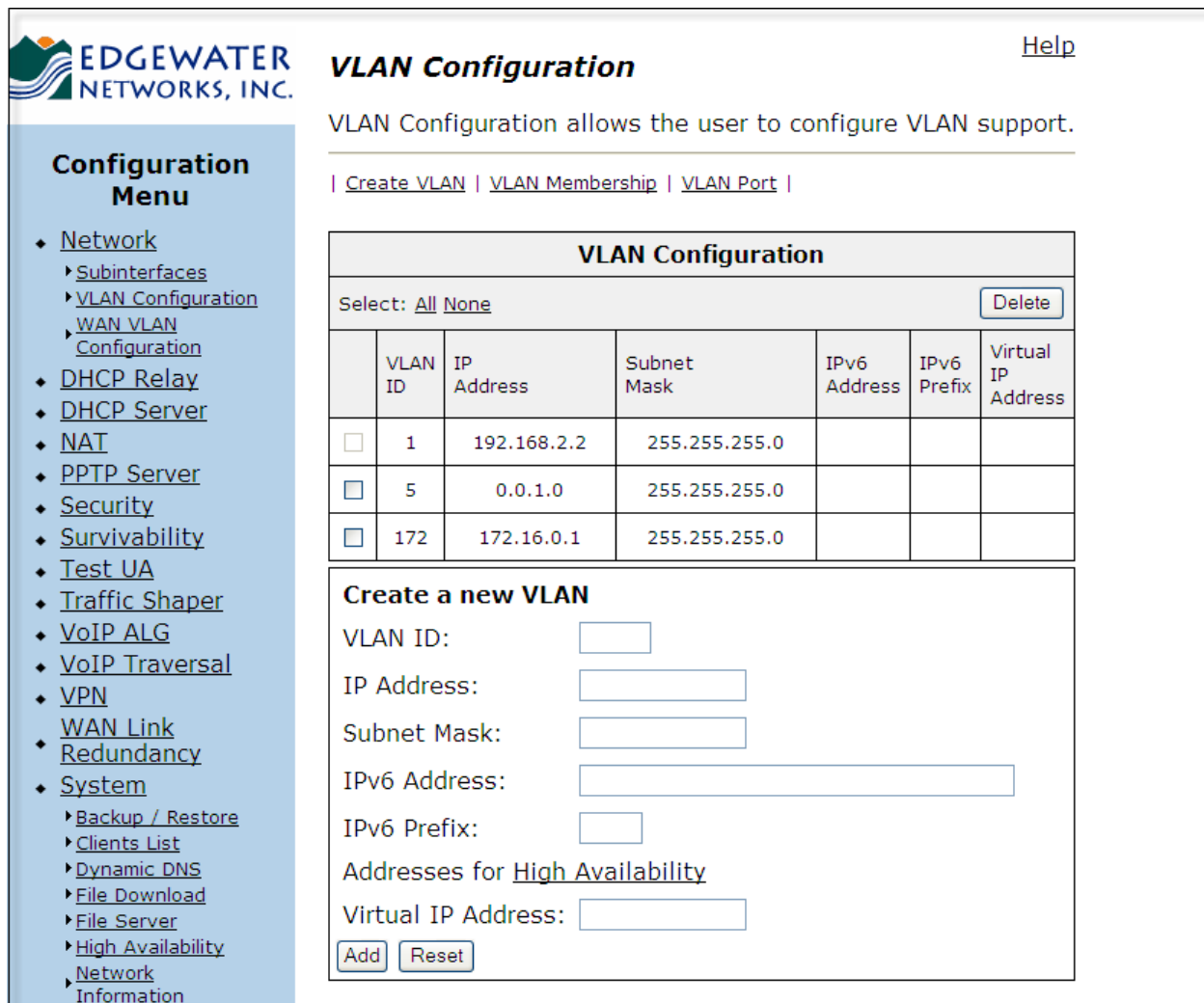
Network Settings:
Default Gateway:

Configuration Menu

- Network
 - Subinterfaces
 - VLAN Configuration
 - WAN VLAN Configuration
- DHCP Relay
- DHCP Server
- NAT
- PPTP Server
- Security
- 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

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.



EDGEWATER NETWORKS, INC. [Help](#)

VLAN Configuration

VLAN Configuration allows the user to configure VLAN support.

[Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN Configuration						
Select: All None Delete						
	VLAN ID	IP Address	Subnet Mask	IPv6 Address	IPv6 Prefix	Virtual IP Address
<input type="checkbox"/>	1	192.168.2.2	255.255.255.0			
<input type="checkbox"/>	5	0.0.1.0	255.255.255.0			
<input type="checkbox"/>	172	172.16.0.1	255.255.255.0			

Create a new VLAN

VLAN ID:

IP Address:

Subnet Mask:

IPv6 Address:

IPv6 Prefix:

Addresses for [High Availability](#)

Virtual IP Address:

[Add](#) [Reset](#)

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.

EDGEWATER NETWORKS, INC.

VLAN Port Membership [Help](#)

VLAN Port Membership allows the user to assign ports as members of a VLAN.

| [Create VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN ID: 172 ▼

VLAN Port Membership	
Select: All None	
Port Number	Member
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>

[Submit](#) [Reset](#) [Apply Later](#)

Configuration Menu

- Network
 - Subinterfaces
 - VLAN Configuration
 - WAN VLAN Configuration
- DHCP Relay
- DHCP Server
- NAT
- PPTP Server
- Security
- Survivability
- Test UA
- Traffic Shaper
- VoIP ALG
- VoIP Traversal
- VPM

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.

Add a Certificate

Certificate Name:

Certificate Type: CA Certificate ▼

Select Certificate File: [Browse...](#)

Select Key File: [Browse...](#)

Password:

[Add Certificate](#) [Reset](#)

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**.

SSL/TLS Certificate Store [Help](#)

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

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:
 External Server Port:

Authentication

Enable Authentication: ☒
 User:
 Password:

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:
 Client Certificate:

Cipher

Select the cipher to use for the tunneled data

Cipher:

LAN-side VLAN

Select the LAN-side VLAN to bridge with the tunnel

Use VLAN:

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:

The screenshot shows the 'VoIP Traversal' status page. On the left is a 'Configuration Menu' with links: Network, DHCP Relay, DHCP Server, NAT, PPTP Server, and Security. The main area shows a diagram with 'External Server' and 'This System', each with a green globe icon and a green arrow pointing from 'This System' to 'External Server'. The top right shows 'Current time: Wed Mar 7 15:08:18 2012' and a 'Help' link. A 'Refresh Status' link is also present.

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 screenshot shows the 'VoIP Traversal' status page from the EdgeProtect interface. The 'Configuration Menu' on the left includes: Network, DHCP Relay, DHCP Server, NAT, Security, and Survivability. The main diagram shows 'This System' (with IP address 10.255.0.4) and 'Remote Clients', each with a green globe icon and a green arrow pointing from 'Remote Clients' to 'This System'. The top right shows 'Current time: Wed Mar 7 14:55:35 2012' and a 'Help' link. A 'Refresh Status' link is also present.

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.

The screenshot shows the 'VoIP ALG' configuration page. On the left is a 'Configuration Menu' with a tree structure: Network, DHCP Relay, DHCP Server, NAT, PPTP Server, Security, Survivability, Test UA, Traffic Shaper, and VoIP ALG (selected). Under VoIP ALG, there are sub-items: H.323, MGCP, SIP, and a selected item (likely ALG). The main content area is titled 'VoIP ALG' and includes a 'Help' link. It contains the following settings: 'ALG allows the system to recognize and register network devices.'; 'Since VLAN support is enabled, you must select a VLAN for the ALG to support. The ALG can only support one VLAN.'; 'ALG LAN using VLAN ID' set to 172; 'Enable LLDP' checked; 'LLDP Broadcast Interval (sec)' set to 30; 'IPv4 only.'; 'TFTP Server IP address' set to 0.0.0.0; a note about alias addresses; 'Use ALG Alias IP Addresses' unchecked; 'ALG LAN Interface IP Address' set to 172.16.0.1; 'ALG LAN Interface IPv6 Address' set to 10.255.0.14; and 'ALG WAN Interface IP Address' set to 10.255.0.14.

EDGEWATER NETWORKS, INC. **VoIP ALG** [Help](#)

ALG allows the system to recognize and register network devices.

Since VLAN support is enabled, you must select a VLAN for the ALG to support. The ALG can only support one VLAN.

ALG LAN using VLAN ID: 172

Enable LLDP: ☒

LLDP Broadcast Interval (sec): 30

IPv4 only.

TFTP Server IP address: 0.0.0.0

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports. The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

Use ALG Alias IP Addresses: ☐

ALG LAN Interface IP Address: 172.16.0.1

ALG LAN Interface IPv6 Address: 10.255.0.14

ALG WAN Interface IP Address: 10.255.0.14

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**.

The screenshot shows the 'SIP Settings' configuration page. On the left is a 'Configuration Menu' with a tree structure: Network, DHCP Relay, DHCP Server, NAT, PPTP Server, Security, Survivability, Test UA, Traffic Shaper, and VoIP ALG (selected). Under VoIP ALG, there are sub-items: H.323, MGCP, SIP, and a selected item (likely ALG). The main content area is titled 'SIP Settings' and includes a 'Help' link. It contains the following settings: 'SIP protocol settings.'; 'The SIP Server settings specify the address and port that all client traffic shall be forwarded to.'; 'SIP Server Address' set to 192.168.50.1; 'SIP Server Port' set to 5060; 'Use Custom Domain' unchecked; 'SIP Server Domain' empty; 'List of SIP Servers' with a 'Create' button; 'Enable Multi-homed Outbound Proxy Mode' unchecked; 'Enable Transparent Proxy Mode' unchecked; 'Limit Outbound to listed Proxies / SIP Servers' checked; and 'Limit Inbound to listed Proxies / SIP Servers' checked. There is also a section for 'Allowed SIP Proxies' with explanatory text.

EDGEWATER NETWORKS, INC. **SIP Settings** [Help](#)

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Address: 192.168.50.1

SIP Server Port: 5060

Use Custom Domain: ☐

SIP Server Domain:

List of SIP Servers: [Create](#)

Enable Multi-homed Outbound Proxy Mode: ☐

Enable Transparent Proxy Mode: ☐

Limit Outbound to listed Proxies / SIP Servers: ☒


Limit Inbound to listed Proxies / SIP Servers: ☒

Allowed SIP Proxies

This is the list of proxies or registrars that are allowed when enabling the "Limit Outbound" (for transparent mode only) and "Limit Inbound" (for transparent as well as non-transparent mode) options. The SIP Server Address above is always included and does not have to be in this list.

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**.



[Help](#)

ALG Trunking Configuration

Configuration of SIP trunking devices.

SIP Trunking devices

A SIP trunking device can be a PSTN gateway, or similar device, that does not issue REGISTER messages. Calls will be forwarded to the device based on the dial-plan rules below.

If VLANs are enabled, the SIP trunking device needs to be in the same VLAN as defined in the VoIP ALG page.

SIP Trunking Devices			
Select: All None Delete			
	Address	Port	Name
<input type="checkbox"/>	172.16.0.3	5060	IP Office Branch

Add a trunking device

Action: Add new trunking device

Name:

Address:

Port:

[Commit](#) [Reset](#)

Configuration Menu

- ◆ [Network](#)
- ◆ [DHCP Relay](#)
- ◆ [DHCP Server](#)
- ◆ [NAT](#)
- ◆ [PPTP Server](#)
- ◆ [Security](#)
- ◆ [Survivability](#)
- ◆ [Test UA](#)
- ◆ [Traffic Shaper](#)
- ◆ [VoIP ALG](#)
 - [H.323](#)
 - [MGCP](#)
 - [SIP](#)
 - [ALG](#)
 - [B2BUA](#)
- ◆ [VoIP Traversal](#)
- ◆ [VPN](#)
- ◆ [WAN Link](#)
- ◆ [Redundancy](#)
- ◆ [System](#)
 - [Backup / Restore](#)
 - [Clients List](#)

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**.

Dial Rules						
Select: All None						<input type="button" value="Delete"/>
	Type	Party	Pattern - match	Strip	Add	Trunking device
<input type="checkbox"/>	Inbound		Default Rule			IP Office Branch (172.16.0.3:5060)

Add a rule

Action: Add new rule ▼

Type: Inbound ▼

Call Party: Called ▼

Default rule: ☐

Pattern-match (if not default):

Strip digits:

Add string:

Trunking device: IP Office Branch (172.16.0.3:5060) ▼

Note: "Use SIP proxy as secondary target" rule can be configured on the B2BUA page

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**.

EDGEWATER NETWORKS, INC. **Route** [Help](#)

The Route page is used to add or delete static routes to hosts or networks.

Static Routes			
Select: All None Delete			
	IP Network	Network Mask	Gateway
<input type="checkbox"/>	172.16.0.0	255.255.255.0	10.255.0.14

Add a Static Route

IP Network:

Network Mask:

Gateway:


[Add](#) [Reset](#)

Configuration Menu

- [Network](#)
- [DHCP Relay](#)
- [DHCP Server](#)
- [NAT](#)
- [Security](#)
- [Survivability](#)
- [Test UA](#)
- [Traffic Shaper](#)
- [VoIP ALG](#)
- [VoIP Traversal](#)
- [VPN](#)
- [WAN Link](#)
- [Redundancy](#)
- [System](#)
 - [Backup / Restore](#)
 - [Clients List](#)

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**.



[Help](#)

Configuration Menu

- ◆ [Network](#)
- ◆ [DHCP Relay](#)
- ◆ [DHCP Server](#)
- ◆ [NAT](#)
- ◆ [PPTP Server](#)
- ◆ [Security](#)
- ◆ [Survivability](#)

Route

The Route page is used to add or delete static routes to hosts or networks.

Static Routes

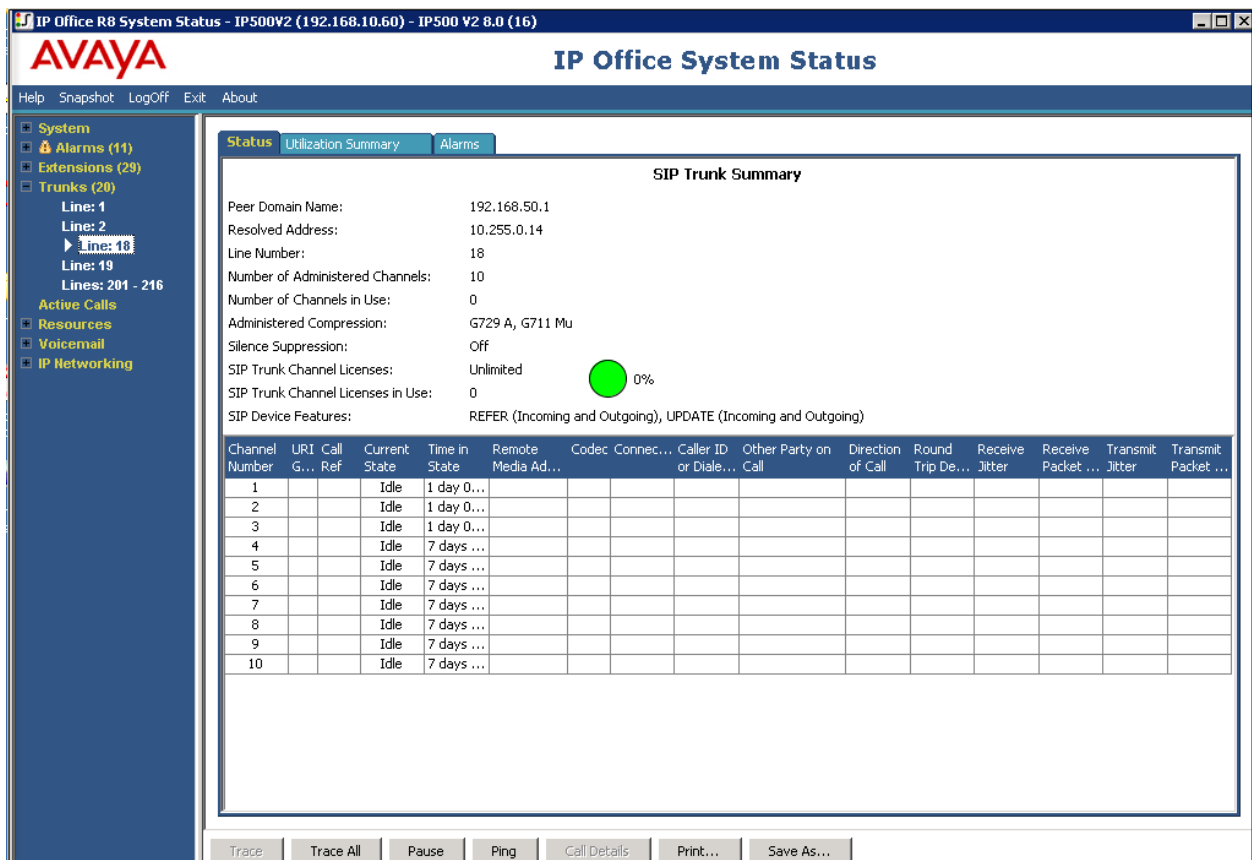
Select: [All](#) [None](#)
Delete

	IP Network	Network Mask	Gateway
<input type="checkbox"/>	192.168.50.0	255.255.255.0	10.255.0.4

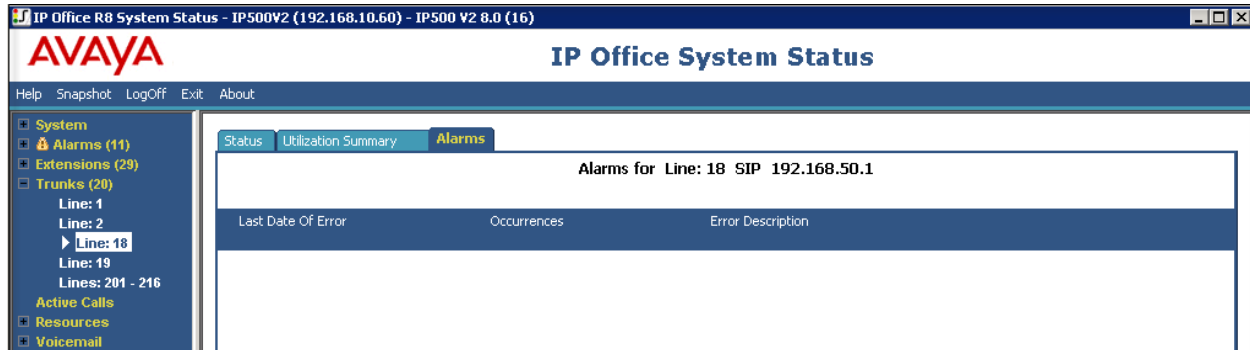
7. Verification Steps

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>

©2012 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.