VoIP 2320

Local Area Network (LAN) Architecture for Hosted Voice Services

November 2011

Version 12.1

Table of Contents

Overview

The ***VOIP2320*** Network Performance Program (NPP) is a quality-control initiative for the ***VOIP2320*** subscriber community. The program was created to ensure that ***VOIP2320*** retail partners exceed the business customer's expectations for high-quality communications services on a 24-7 basis. Cornerstones of the Network Performance Platform include standardization that aggregates best practices garnered from experience serving tens of thousands of end-users. In that effort, this document is intended to define the customer premise network architectures that have been identified as best-practices to accomplish those goals.

To ensure that the highest-quality service is delivered to every subscriber, it is important to review the layout and design of the customer's Internal IP network, or Local Area Network (LAN). Of particular concern is the integration of SIP-enabled devices onto the LAN with respect to the presence of customer firewalls and NAT traversal. These critical items are the root cause of a large portion of LAN integration challenges and ***VOIP2320*** believes the approach defined in this document is the correct model to appropriately address them.

The philosophy behind the NPP program regarding LAN design is to create a predictable, controlled LAN design that accommodates VOIP-specific requirements while allowing flexibility to end-subscribers. In particular, end-subscribers need the ability to deploy security, private networks (VPNs), hosting DMZ and IP circuit redundancy on the same IP network as VOIP services.

This document will define a total of 5 LAN designs that provide solutions to address these requirements when they arise during an end-customer installation. These designs are intended to address single location installations that will have direct broadband Internet access. Larger customer installations involving private WAN IP transport or aggregated Internet access across multiple locations will likely involve additional design considerations. If a customer opportunity arises outside the scope of this document, please engage ***VOIP2320*** for assistance.

The basic philosophy of all LAN designs endorsed by VOIP2320 includes the following three requirements:

1. **The availability of at least a single static (in some cases multiple), Public IP address(es) from the broadband service provider. Larger Public IP subnets are supportable as well.**
2. **The integration of an Edgewater Networks brand EdgeMarc family router, this router would be provisioned with the public IP address required above. See appendix for configurations.**
3. **VOIP2320 Certified SIP-enabled phones/endpoints will be on a common layer-2 Ethernet segment directly to the LAN interface(s) of the EdgeMarc router. Explicitly stated: "UNDER NO CIRCUMSTANCES WILL VOIP TRAFFIC TRAVERSE A NON-EDGEMARC CUSTOMER FIREWALL".**

In addition to the mandatory requirements above, additional design considerations are included to accommodate the co-existence of the following network elements:

- Customer Firewall/screening routers for data applications
- Hosted email and web servers (DMZ)
- VPN concentrators
- Multiple Broadband Connections
- VLANs

Benefits of the NPP LAN Design Requirements

Public IP Address

The requirement for a static, publicly routable IP address at the service location of the voice services fulfills two needs:

- First, it ensures that no more than a single NAT-traversal occurs when SIP signaling and RTP audio packets are entering or leaving the customer LAN. NAT-traversal for these traffic types from one IP network to another has the potential to create a "state-of-confusion" to the far-end source for inbound traffic or the recipient for outbound traffic. A solution to address the "state-of-confusion" for a single NAT traversal is an inherent attribute of the designs defined in this document. However, the potential presence of multiple NAT-traversal hops is not supportable, which dictates the public IP address requirement.

- Second, by assigning a static, public IP address to the customer premise, it can be used to enable additional services by ***VOIP2320***. Specifically, the customer premise can be build into a Network Management System run by ***VOIP2320***. This system, EdgeView, works in conjunction with the EdgeMarc routers to enable CPE configuration services, call monitoring, reporting and service troubleshooting tools. More detail on these features is described below under the EdgeMarc routers.

EdgeMarc Router Family

The requirement for EdgeMarc routers is an enabler for a number of features. However, most importantly EdgeMarc routers include standardized SIP Application-Layer-Gateway (ALG) functionality that has been custom tuned to ***VOIP2320*** specifications. ***This is a vital requirement of service delivery reliability.*** While there are countless other devices that claim this functionality, the reality is there in no standardization for SIP ALG functionality and many vendor's products result in unpredictable or even harmful behavior. Simply stated: ***VOIP2320*** knows an EdgeMarc will work, while other SIP ALGs might work. While adapting/tweaking various equipment to an installation is possible, ***VOIP2320*** intends to avoid making each customer installation a "science project" and instead adopting a uniform approach for installations. The minimal effort invested in this approach during customer installations pays dividends in reduced service troubleshooting and customer dissatisfaction.

In addition to standardized SIP ALG functionality, there are several beneficial attributes of the EdgeMarc platform that do not exist with other vendors:

- Automation of CPE configuration via the ***VOIP2320*** Plug-n-Dial platform. EdgeMarc routers enable out-of-the-box configuration of phones and ATAs to pre-provisioned user accounts by interacting with a hosted CPE configuration server on the phones behalf. Simply stated: There is no need to pre-configure a phone prior to delivery to the subscriber's premise.
- Additionally, as mentioned under the IP address section, ***VOIP2320*** hosts a Network Management System for EdgeMarcs that includes functionality such as MOS statistics, LAN/WAN problem isolation, and signaling capture.

Layer-2 Connection to EdgeMarc Router

The last of the LAN design requirements is to ensure that the placement of SIP-enabled IP phones or Analog Telephone adaptors (ATA) are placed in the network correctly with regard to the EdgeMarc router. In order for the EdgeMarc to properly allow SIP messaging from a SIP device to the Public IP space, as mentioned in Item 1 (above) only a single NAT-traversal can take place. This means that the SIP devices need a direct Layer-2 Ethernet connection directly to the LAN interface(s) of the EdgeMarc. This can be done a number of different ways, which include:

- direct cat-5 cable connect to a LAN port of the EdgeMarc
- Ethernet switch connectivity (non-VLAN)
- Use of 802.1q VLAN tagging.

The important consideration here is that there is not an intermediate Layer-3 device between any SIP-enabled endpoint and the LAN interface(s) of the EdgeMarc.

Assumptions & Conditions

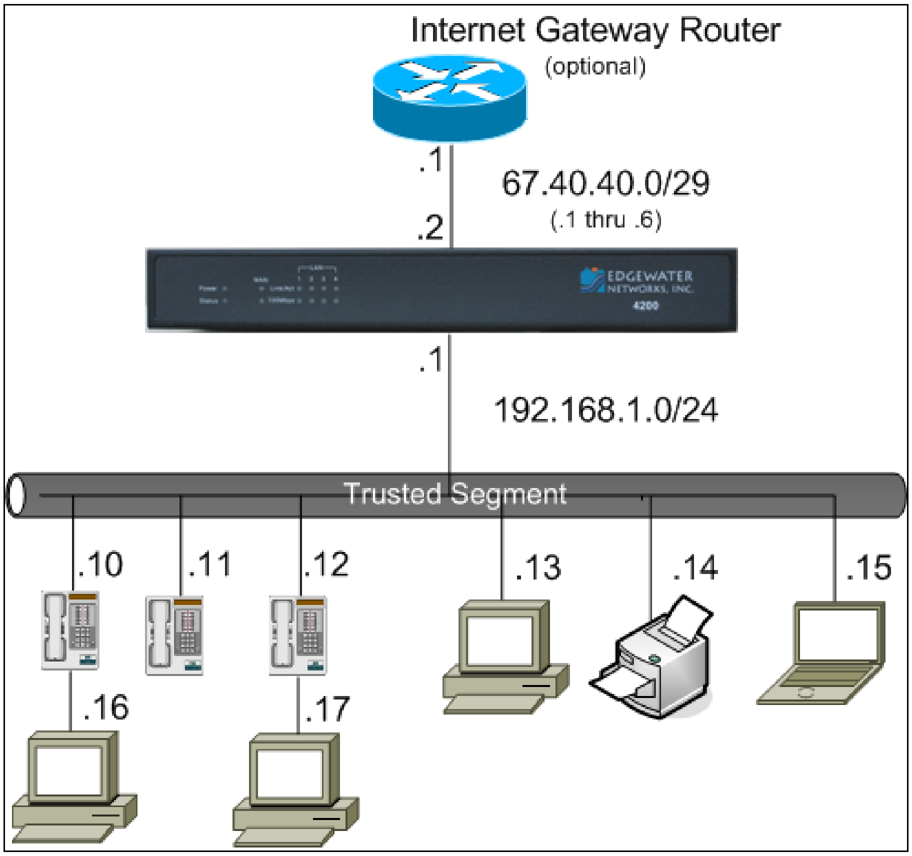
The following assumptions and conditions are made in regard to the information in this document -

- The VOIP services will be based on the SIP protocol.
- This document assumes reader has a working knowledge of the ***VOIP2320*** feature servers, including applicable training.
- This document is intended to identify valid technical solutions for enabling VOIP services and is not intended to imply ***VOIP2320*** support for ancillary network services available in the EdgeMarc router or via 3rd party devices. These include VPN, data firewall, LAN-gateway survivability, email, or web-hosting.
- Installation is for a single location with a single broadband access to the public Internet or, a collection of sites that each has a single broadband access to the public Internet.
- The Internet Gateway Router must support 100Mb full duplex mode on the interface that the Edgemarc is connected.

Network 1.1 - Flat LAN, integrated EdgeMarc

EdgeMarc models supported

- 4200
- 4300T
- 4500E, 4500T4



Topology Characteristics

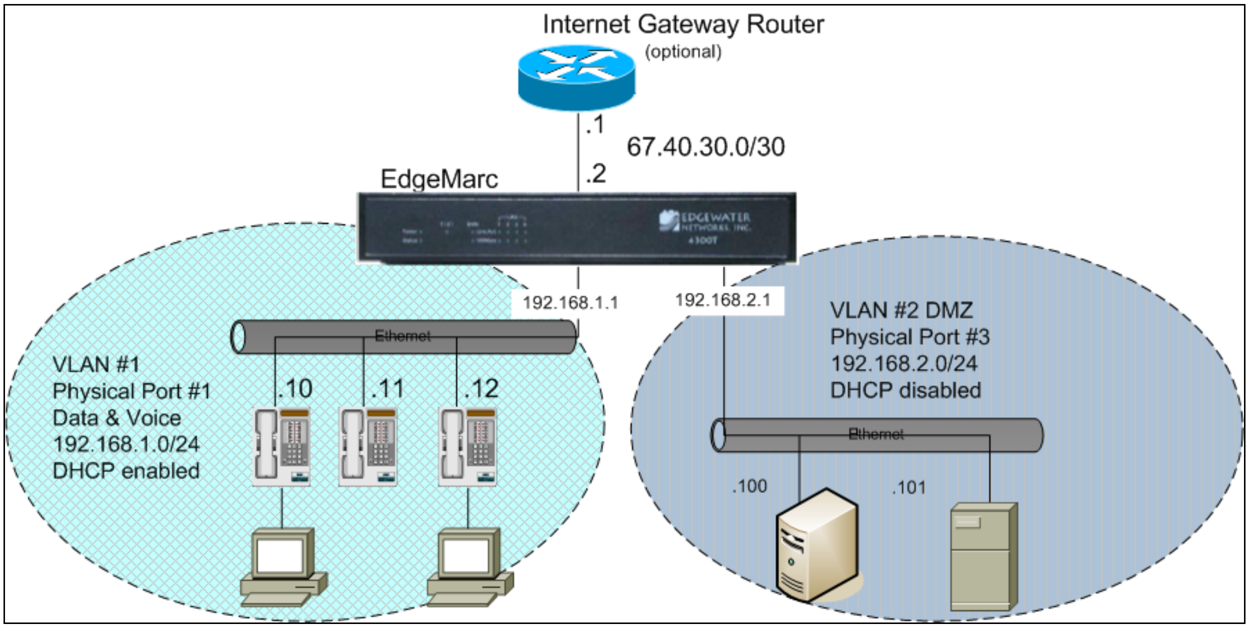
This is simplest of the available network designs. It is a flat-LAN design and can be used when a customer simply has a layer-2 Ethernet switch and no firewall.

- EdgeMarc provides ALG functionality to phones
- EdgeMarc provides NAT, Firewall, Traffic Shaping, and DHCP to PCs and phones
- Phones and PCs share same IP subnet, assigned by DHCP
- EdgeMarc is SIP Proxy to phones
- EdgeMarc WAN interface is provided a public (un-NATed) IP address

Network 2.1 - Flat LANs, integrated EdgeMarc w/DMZ

EdgeMarc model supported

- 4300T
- 4500E, 4500T4



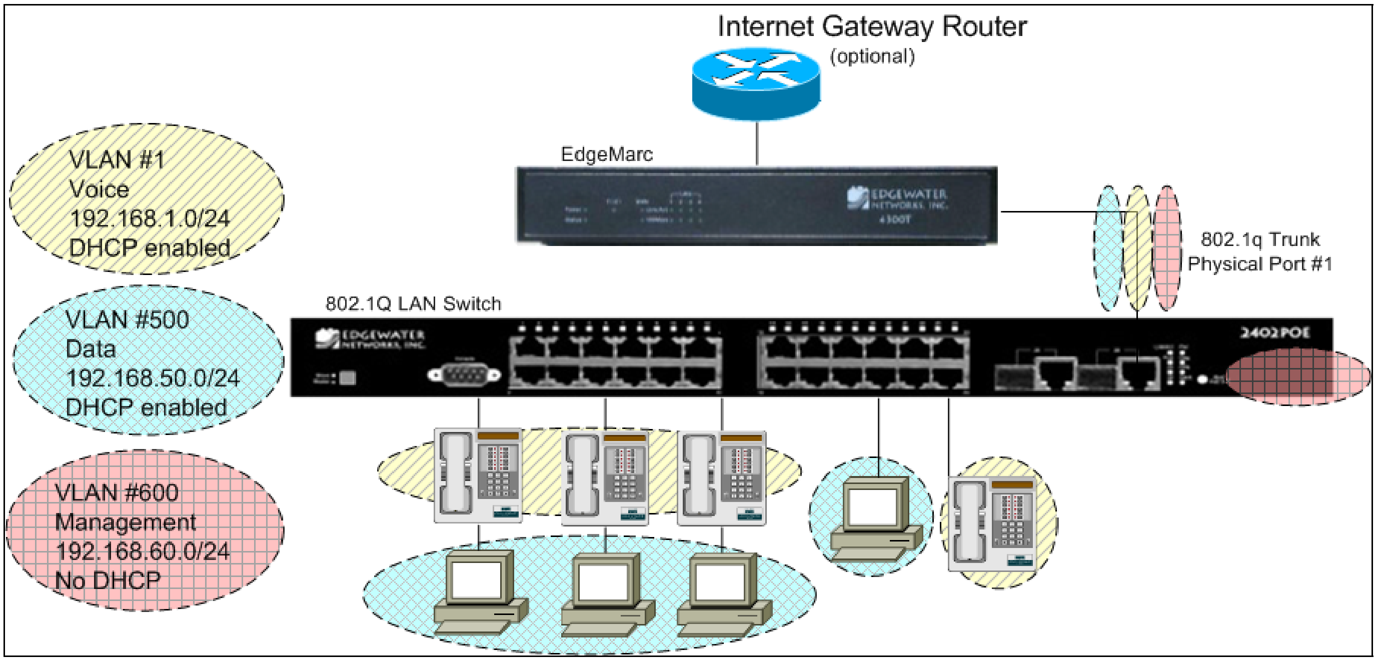
Topology Characteristics

- EdgeMarc provides ALG functionality to phones
- EdgeMarc provides NAT, Firewall, Traffic Shaping, and DHCP to PCs and phones
- Phones and PCs share same IP subnet, assigned by DHCP
- EdgeMarc is SIP Proxy to phones
- The EdgeMarc provides “Static NAT” mappings in DMZ to the publicly-accessible servers OR provides public addresses to servers.
- If Static NAT, then individual IP ports can be statically mapped to the servers, such as port 25 (SMTP) and port 80 (WWW).
- Servers are firewalled from other IP ports (optional)
- WAN interface has at least one IP address:
- The EdgeMarc is assigned one IP address from the WAN subnet
- Other public address(es), can be routed or bridged to LAN-side servers, if desired.
- EdgeMarc LAN interface uses two VLANs
  - One VLAN with a private subnet for phones and PCs. This LAN uses standard 802.1 (untagged) frames.
  - Another VLAN with a separate subnet for servers. This LAN uses standard 802.1 (untagged) frames.

Network 3.1 - VLAN switch, integrated EdgeMarc

EdgeMarc model supported

- 4300T
- 4500E, 4500T4



Topology Characteristics

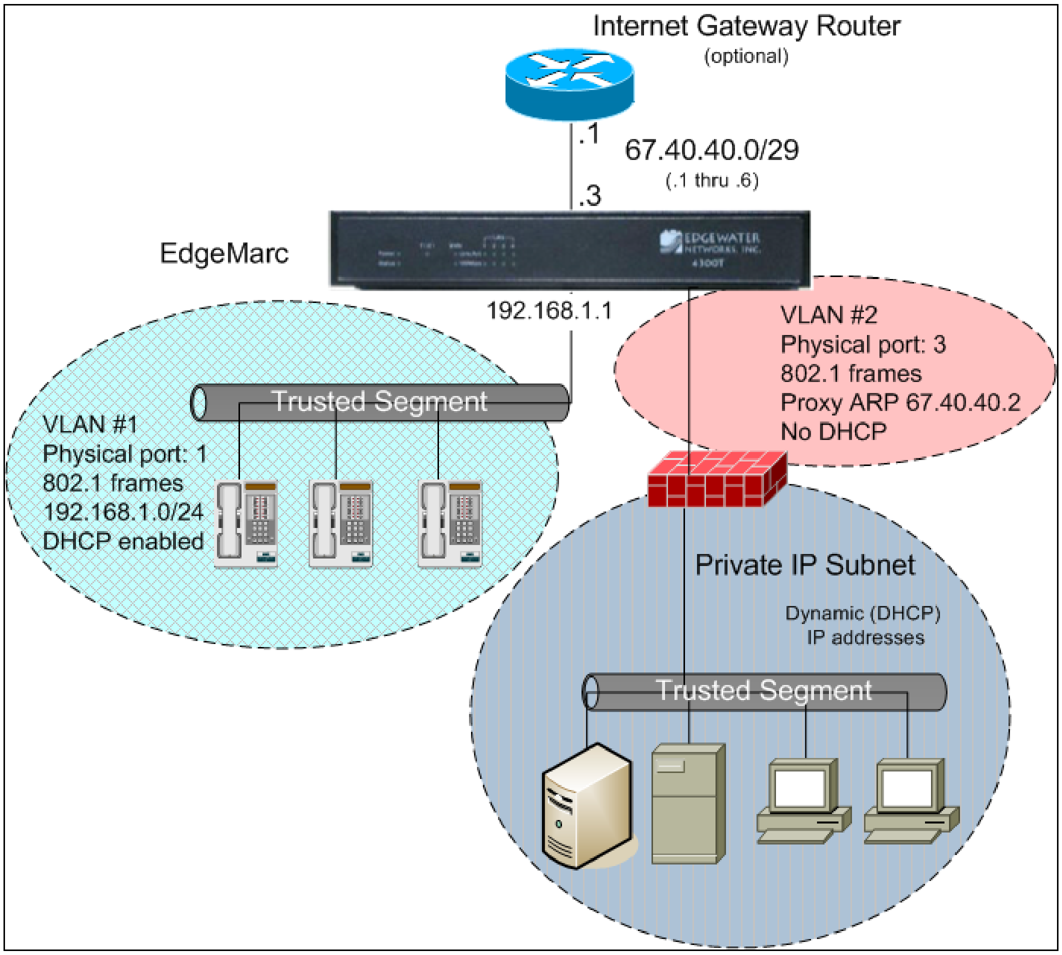
- EdgeMarc provides ALG functionality to phones
- EdgeMarc provides NAT, Firewall, Traffic Shaping, and DHCP to PCs and phones
- Phones and PCs have separate subnets, each assigned by DHCP
- EdgeMarc is SIP Proxy to phones
- VLAN switch provides 802.1 (standard Ethernet) and 802.1q (VLAN tagged Ethernet) frames to phones and PCs, as appropriate
- The EdgeMarc-to-Switch link is a “trunk” (ie 802.1q) link
- WAN interface is provided a public (un-NATed) IP address
- EdgeMarc LAN interface uses three VLANs
- One VLAN for management of the Switch. None of the end-user devices join this VLAN.
- One VLAN for voice traffic to phones. For phones that support VLANs, the switch ports use 802.1q frames for this VLAN.
- One VLAN for data to PCs. This VLAN uses standard 802.1 frames, since few PC NICs support tagged packets.

Network 4.1 - Independent Voice & Data LANs, LAN-side 3rd-party data firewall

EdgeMarc model supported

- 4300T
- 4500E, 4500T4

EdgeMarc provides firewall services for phones. An alternate firewall, on the LAN side of the EdgeMarc is used to firewall PCs and servers. The EdgeMarc connects to a CPE Internet Gateway Router or directly to the Internet. Two drops per cube/desk are used.
Using the EdgeMarc's **Proxy ARP** feature, it is possible to drop in the EdgeMarc without making any configuration changes to the customer's firewall. To do this the customer's ISP must provide at least two public IP addresses. The current IP address will (continue to) be used by the customer's firewall device. A new one will be assigned to the EdgeMarc.



Topology Characteristics

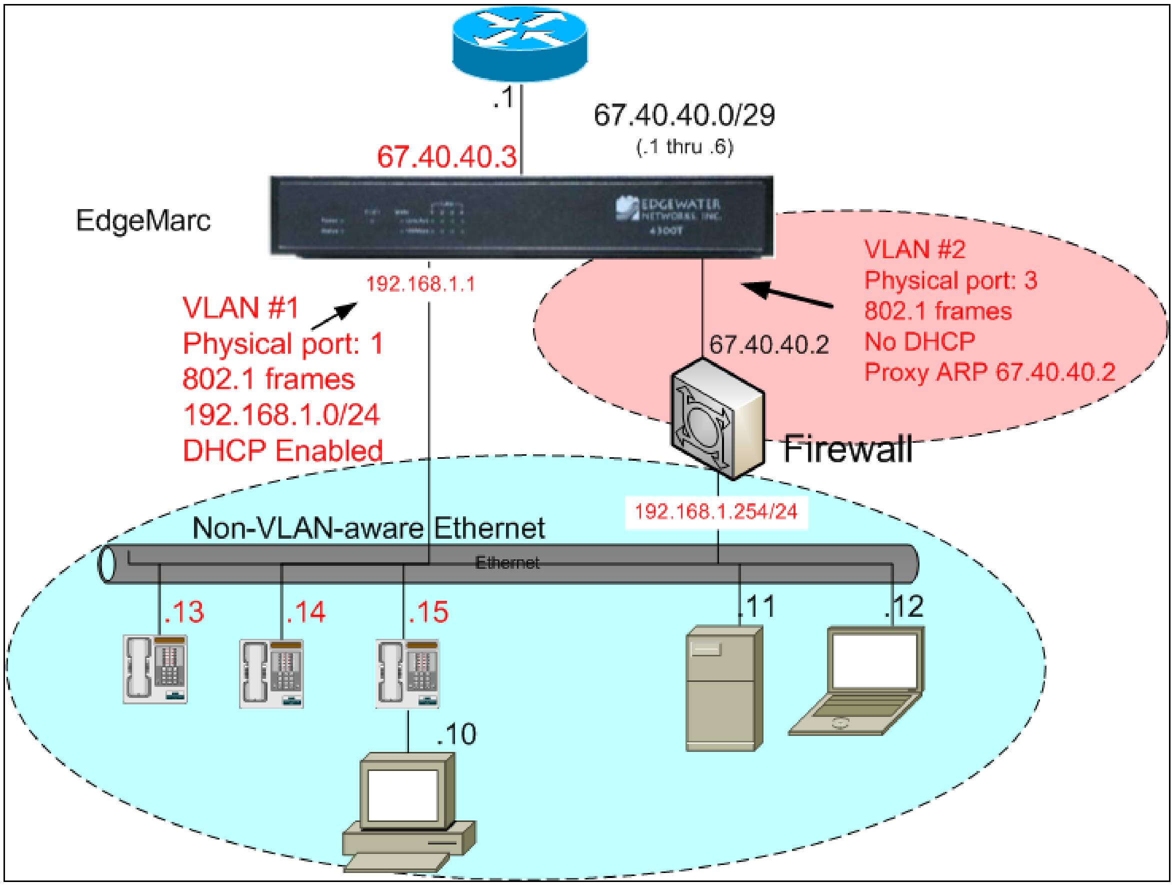
- EdgeMarc provides Traffic Shaping to phones and PCs
- EdgeMarc provides ALG, Firewall and DHCP to phones
- 3rd-party firewall provides NAT, Firewall, and DHCP to PCs and servers
- WAN interface has at least two IP addresses:
- The EdgeMarc is assigned one IP address from the WAN subnet
- Other public address(es), can be routed or bridged to LAN-side firewall.
- EdgeMarc LAN interface uses two VLANs
- One VLAN with a private subnet for phones and PCs. This LAN uses standard 802.1 (untagged) frames.
- Another VLAN with a separate subnet for the 3rd-party firewall. This LAN uses standard 802.1 (untagged) frames.
- Two Ethernet drops per location

Network 5.1 - Flat LAN, LAN-side 3rd-party firewall

EdgeMarc model supported

- 4300T
- 4500E, 4500T4

This design is similar to the one above, except a single drop is used to each location. All devices share the same LAN.
Using the EdgeMarc's **Proxy ARP** feature, it is possible to drop in the EdgeMarc without making any configuration changes to the customer's firewall. To do this the customer's ISP must provide at least two public IP addresses. The current IP address will (continue to) be used by the customer's firewall device. A new one will be assigned to the EdgeMarc.



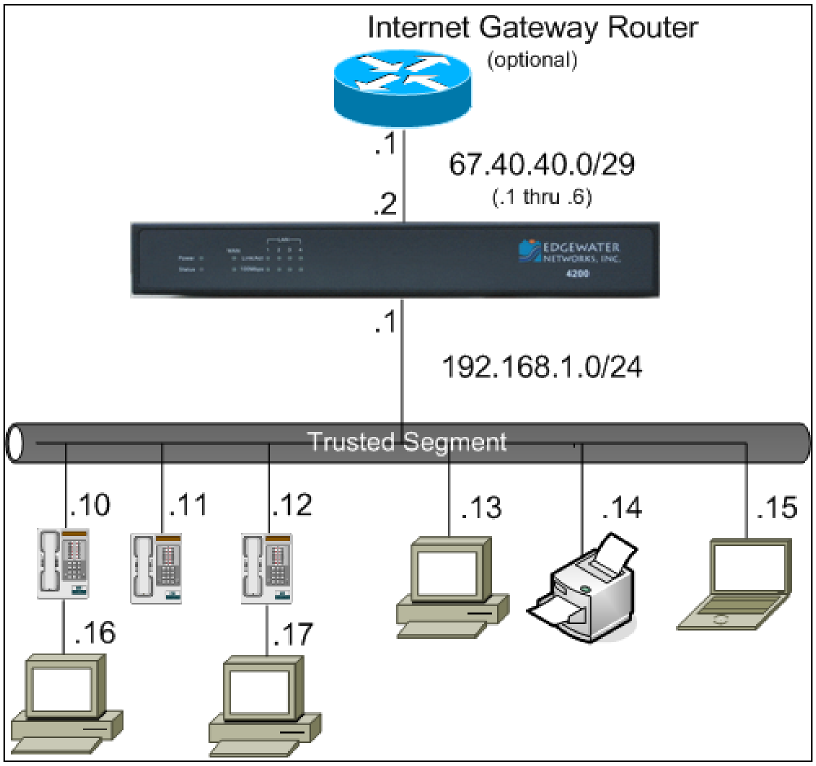
Topology Characteristics

- EdgeMarc provides ALG functionality to phones
- EdgeMarc is SIP Proxy to phones
- EdgeMarc provides Traffic Shaping to phones and PCs
- EdgeMarc provides firewall to phones

- 3rd-party firewall provides NAT, Firewall and DHCP to PCs and phones
- Phones and PCs share same IP subnet, assigned by DHCP
- Default router for PC and phones is 3rd-party firewall
- WAN interface has at least two IP addresses:
- The EdgeMarc is assigned one IP address from the WAN subnet
- Other address(es), including the one already being used by the 3rd-party Firewall/VPN device, are bridged through the EdgeMarc to its LAN interface.
- EdgeMarc LAN interface uses two VLANs
- One VLAN with private subnet for phones, and shared by PCs. This LAN uses standard 802.1 (untagged) frames.
- One VLAN with a public subnet for the 3rd-party VPN / Firewall device. This LAN uses standard 802.1 (untagged) frames.

Appendix A - EdgeMarc Configurations

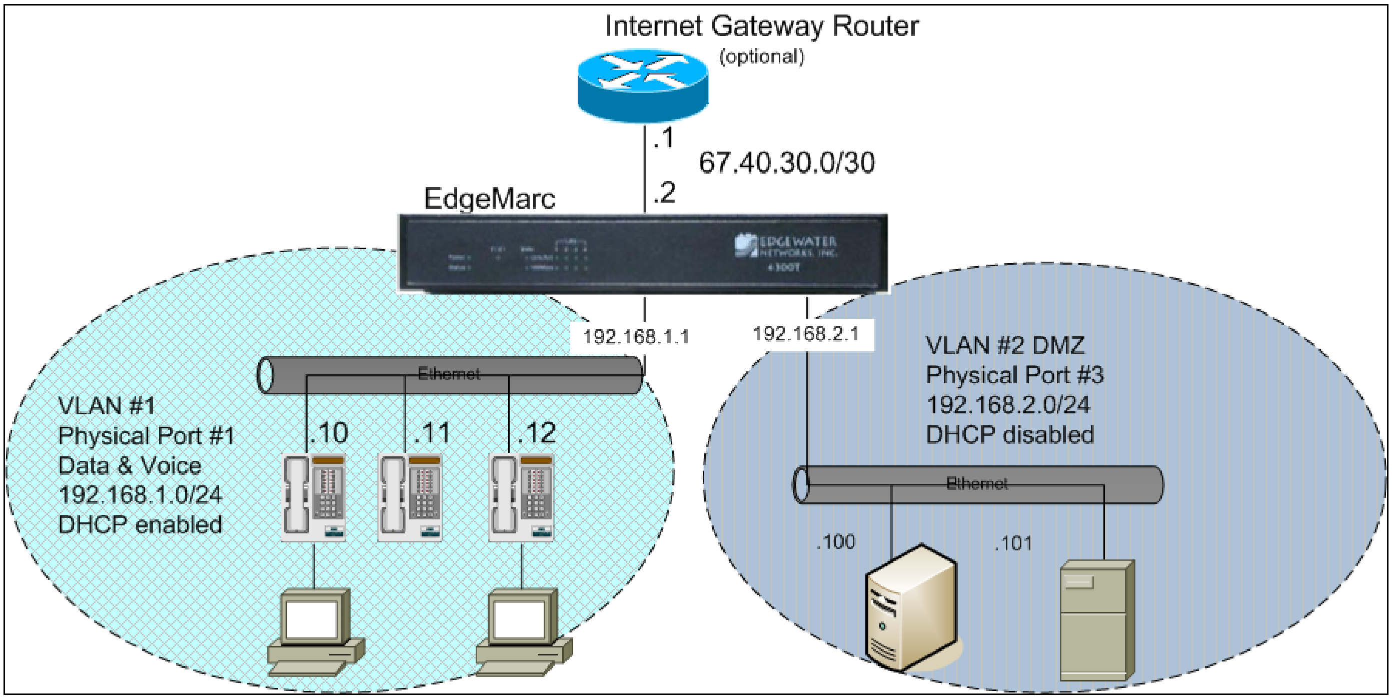
Network 1.1 - Flat LAN, integrated EdgeMarc firewall



Configuration Steps

1) Enable Network (see screenshot #2)
   a. LAN IP address 192.168.1.1
   b. If T1, WAN-Interface T1 (see screenshot #5)
   c. WAN-Interface Static IP address X.X.X.X/X.X.X.X
   d. Set Default Gateway & DNS IP addresses
2) Upgrade firmware to ***VOIP2320*** spec (see screenshot #15a,15b,15c)
3) Enable DHCP (see screenshot #11)
4) Enable Firewall (see screenshot #13)
5) Enable NAT (see screenshot #6)
6) Enable Traffic Shaping (see screenshot #10)
7) Enable ALG functionality Main Screen (see screenshot #7)
8) Enable ALG functionality, SIP Settings (see screenshot #9)
9) Enable Survivability (see screenshot #16a,16b)

Network 2.1 - Flat LANs, integrated EdgeMarc firewall w/DMZ

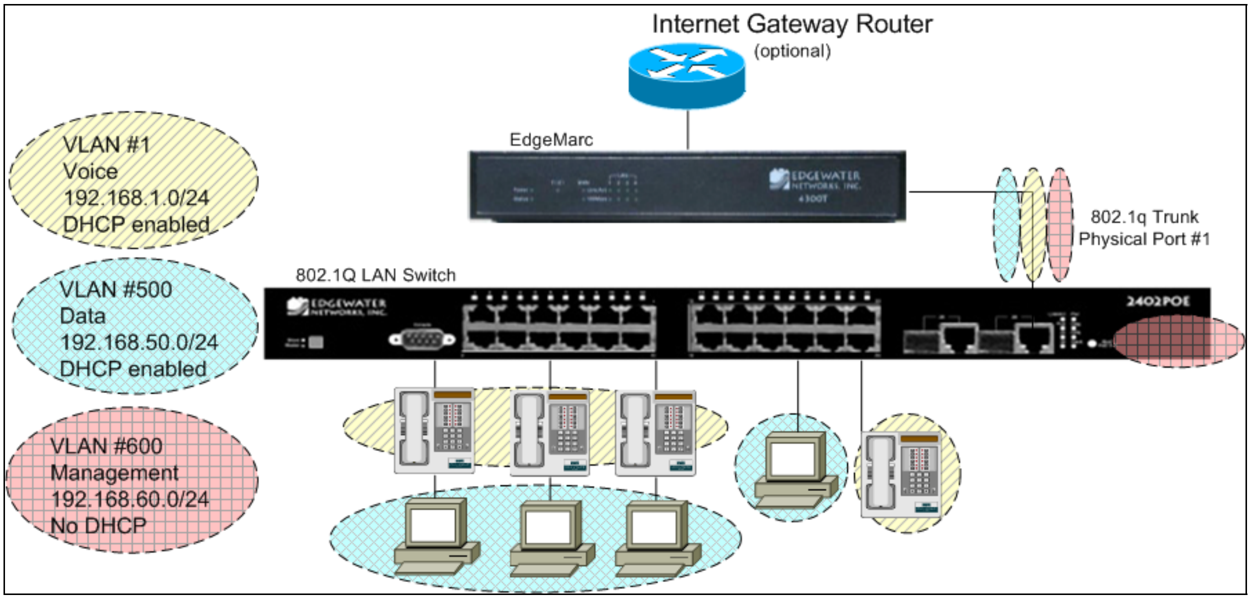


Configuration Steps

1) VLAN Configuration (see screenshot #4a). (Configure VLANs prior to enabling them)
   a) Set the four LAN ports to 802.1
   b) Modify VLAN 1 as:
      i) IP address: 192.168.1.1 with mask 255.255.255.0
      ii) Assign to Physical LAN ports: 1, 2 and 4
   c) Add a VLAN with: ID: 2
      i) IP address: 192.168.2.1 with mask 255.255.255.0
      ii) Associate VLAN 2 with physical LAN port 3
2) Enable Network (Make sure your configuration PC is plugged into one of ports 1, 2 or 4)
   a) If T1, WAN-Interface T1 (see screenshot #5)
   b) WAN-Interface Static IP address X.X.X.X/X.X.X.X (see screenshot #3)
   c) Set Default Gateway & DNS IP addresses
   d) Select Enable VLAN checkbox
3) Upgrade firmware to ***VOIP2320*** spec (see screenshot #15a, 15b,)15c
4) Enable DHCP on VLAN 1 (see screenshot #12)
5) Enable Firewall (see screenshot #13)
6) Enable NAT (see screenshot #6)
7) Enable Traffic Shaping (see screenshot #10)
8) Enable VOIP ALG functionality (see screenshot #8)
   a) Specify VLAN 1 for the ALG
9) Enable ALG functionality, SIP Settings (see screenshot #9)

10) Enable Survivability (see screenshot #16a,16b)

Network 3.1 - VLAN switch, integrated EdgeMarc firewall

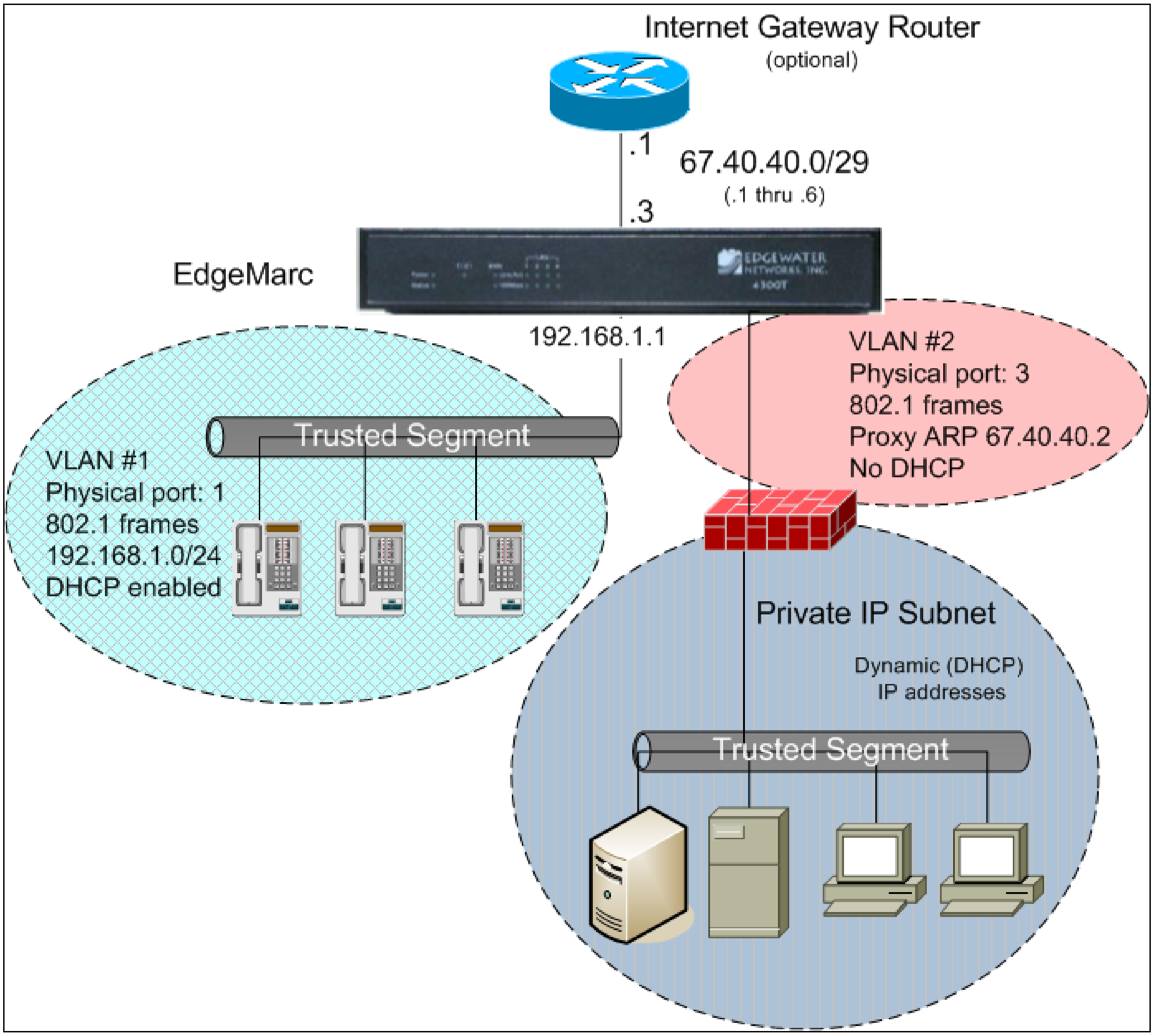


Implementation Steps

1) VLAN Configuration (Screenshot #4b)(Configure VLANs prior to enabling them)
    a. Set LAN Port 1 to 802.1q framing.
    b. Set LAN Ports 2, 3 and 4 to 802.1 framing.
    c. Use VLAN 1 as Voice VLAN:
        i. Assign IP Address: 192.168.1.1 with mask 255.255.255.0
    d. Add a VLAN for Data with:ID: 500
        i. Assign IP address: 192.168.50.1 with mask 255.255.255.0
    e. Add a VLAN for Management with:ID: 600 (optional)
        i. Assign IP address: 192.168.60.1 with mask 255.255.255.0
    f. Associate VLAN 1 with LAN ports 1 and 4
    g. Associate VLANs 500 and 600 with LAN port 1
    h. When done, the VLAN screen should appear like image #4b
2) Enable Network (Make sure your configuration PC is plugged into port 4)
    a. WAN-Interface Static IP address X.X.X.X/X.X.X.X (see screenshot #3)
    b. If T1, WAN-Interface T1 (see screenshot #5)
    c. Select Enable VLAN checkbox
3) Upgrade firmware to ***VOIP2320*** spec (see screenshot #15a, 15b, 1)5c
4) Enable DHCP on VLANs 1 and 500 (screenshot #12)
5) Enable Firewall (screenshot #13)
6) Enable NAT (screenshot #6)
7) Enable Traffic Shaping (screenshot #10)
8) Enable VOIP ALG functionality Main Screen (screenshot #8)
    a. Specify VLAN 1 for the ALG
9) Enable ALG functionality, SIP Settings (screenshot #9)

10) Enable Survivability (see screenshot #16a,16b)

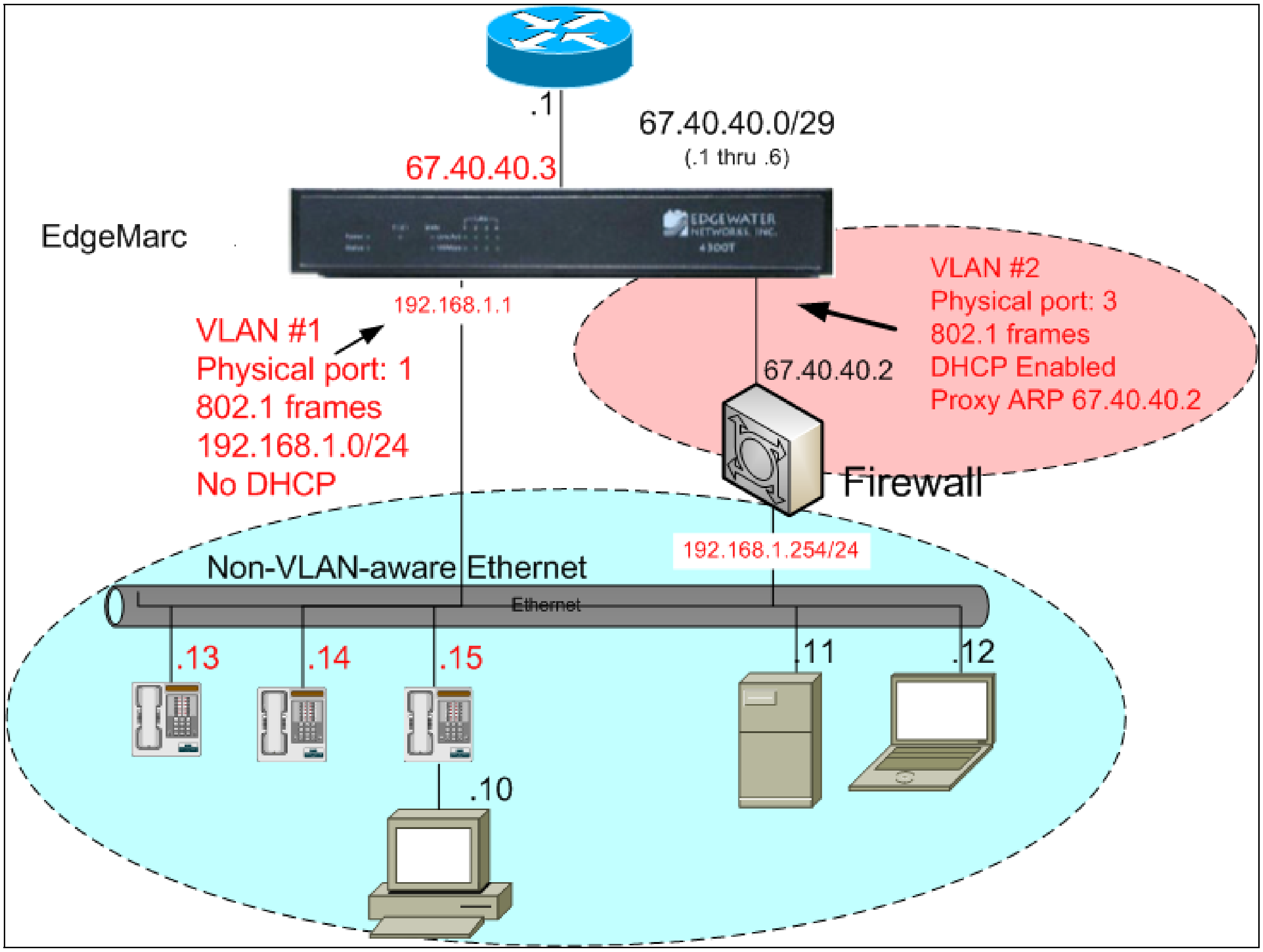
Network 4.1 - Independent Voice & Data LANs, LAN-side 3rd-party data firewall



1) VLAN Configuration (see screenshot #4c).
   a. Configure VLANs (prior to enabling them)
   b. Set the four LAN ports to 802.1
   c. Modify VLAN 1 as:
      i. Address: 192.168.1.1 with mask 255.255.255.0
   d. Add a VLAN with: ID: 2
      i. IP address: 0.0.0.0 with mask 0.0.0.0
   e. Associate VLAN 1 with LAN ports 1, 2 and 4
   f. Associate VLAN 2 with LAN port 3
   g. When complete, VLAN configuration should appear as screenshot #4c.

2) Enable Network (Make sure your configuration PC is plugged into port #1, 2 or 4)
   a. WAN-Interface Static IP address X.X.X.X/X.X.X.X (see screenshot #3)
   b. If T1, WAN-Interface T1 (see screenshot #5)
   c. Select Enable VLAN Checkbox
3) Upgrade firmware to ***VOIP2320*** spec (see screenshot #15a, 15b, 15c)
4) Enable DHCP on VLAN 1 (see screenshot #12)
5) Enable Firewall (see screenshot #13)
6) Enable NAT (see screenshot #6)
7) Enable Traffic Shaping (see screenshot #10)
8) Enable VOIP ALG functionality Main Screen (see screenshot #8)
   a. Specify VLAN 1 for the ALG
9) Enable VOIP ALG functionality, SIP Settings (see screenshot #9)
10) Proxy ARP (Proxy ARP bridges the external Firewall's IP address from the EdgeMarc's WAN interface to its LAN interface.)
    a. Enter The Public IP address to Proxy ARP X.X.X.X/X.X.X.X
    b. Select the VLAN 2 Interface to assign Proxy ARP to.
    c. Enter the WAN default gateway Public IP address X.X.X.X/X.X.X.X
    d. Select WAN interface for Respond to ARP requests from:
    e. When complete, proxy ARP settings should appear like screenshot #14
11) Enable Survivability (see screenshot #16a,16b)

Network 5.1 - Flat LAN, LAN-side 3rd-party firewall



Implementation Steps

1) VLAN Configuration (see screenshot #4d)
   a. Set the four LAN ports to 802.1
   b. Modify VLAN #1 as:
      i. IP address: 192.168.1.1 with mask 255.255.255.0
      ii. Assign VLAN 1 to Physical ports: 1, 2 and 4
   c. Add a VLAN with: ID: 2
      i. IP address: 0.0.0.0 with mask 0.0.0.0
   d. Associate VLAN 2 with Physical LAN port 3
   e. When done, the VLAN screen should appear like #4d
2) Enable Network (Make sure your configuration PC is plugged into port #1, 2 or 4)
   a. WAN-Interface Static IP address X.X.X.X/X.X.X.X (see screenshot #3)
   b. If T1, WAN-Interface T1 (see screenshot #5)
   c. Select Enable VLAN Checkbox
3) Upgrade firmware to ***VOIP2320*** spec (see screenshot #15)a-d

4) Enable Firewall (see screenshot #13)

5) Enable NAT (see screenshot #6)
6) Enable VOIP ALG functionality Main Screen (see screenshot #8)
    a. Specify VLAN #1 for the ALG
7) Enable VOIP ALG functionality, SIP Settings (see screenshot #9)
8) Enable Traffic Shaping (see screenshot #10)
9) Define LAN IP address of 3rd Party firewall as 192.168.1.254/24
10) Enable DHCP on 3rd party Firewall
    a. Define Gateway IP as 192.168.1.254 (Firewall LAN IP)
    b. Only one DHCP server should be active in the network.
11) Proxy ARP (Proxy ARP bridges the external Firewall's IP address from the EdgeMarc's WAN interface to its LAN interface.)
    a. Enter The Public IP address to Proxy ARP X.X.X.X/X.X.X.X
    b. Select the VLAN 2 Interface to assign Proxy ARP to.
    c. Enter the WAN default gateway Public IP address X.X.X.X/X.X.X.X
    d. Select WAN interface for Respond to ARP requests from:
    e. When complete, proxy ARP settings should appear like screenshot #14
12) Enable Survivability (see screenshot #16a,16b)

Note: If using a 3rd-party DHCP server, phones expect a combination of DHCP Options 66, 150 and 151 for VoIP parameters. See Edgewater knowledgebase article: *90562 : DHCP parameters supported by EdgeMarc*.

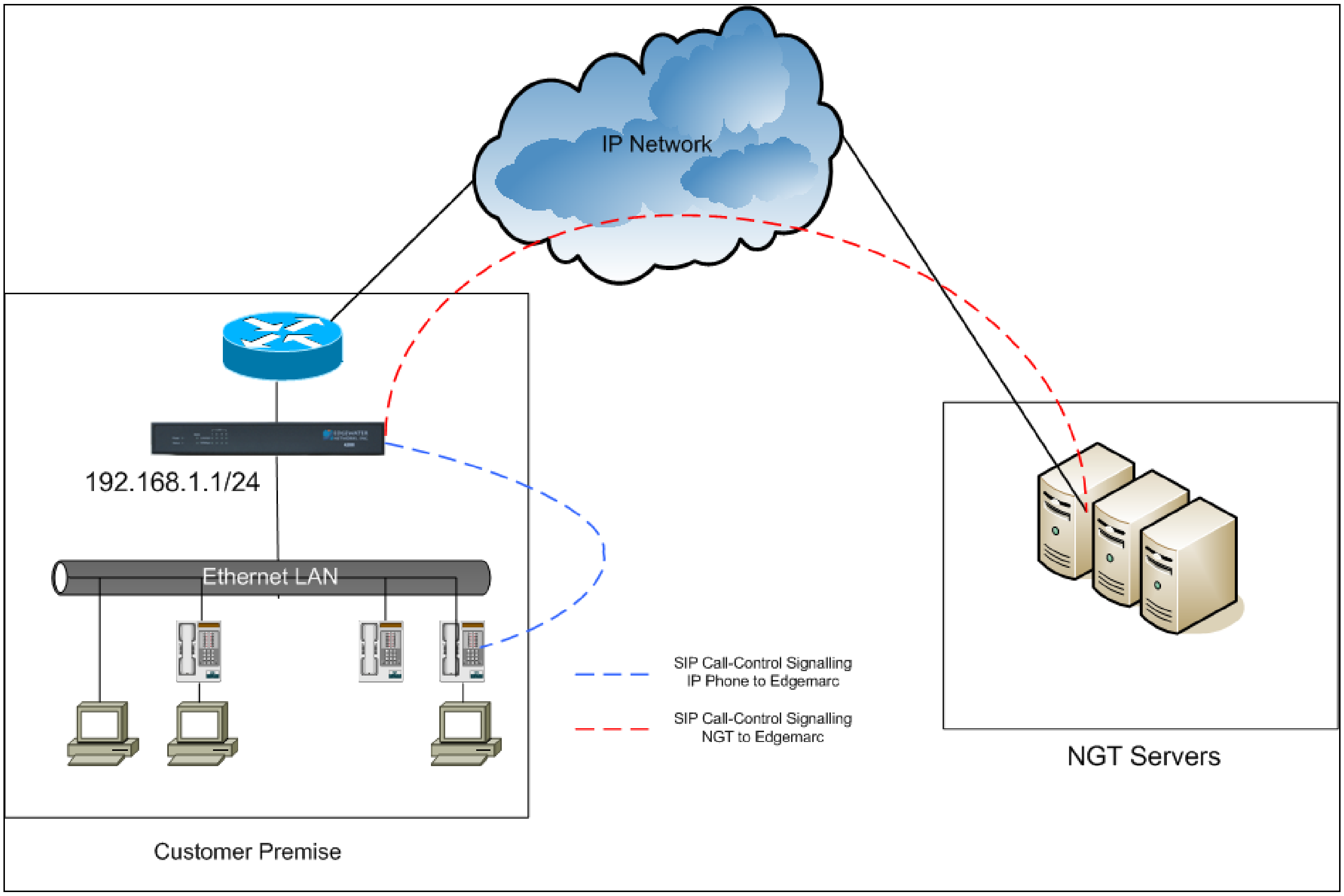
Appendix B - SIP Device and VLAN Switch Configurations

SIP Device Configuration

One of the key attributes that the EdgeMarc router provides to enabling VoIP services is that it performs the function of an Application Layer Gateway (ALG) to the SIP-enabled IP devices on the customer premise. What occurs in this scenario is that the SIP device uses the EdgeMarc as its SIP proxy server and the EdgeMarc then propagates any messaging from the phone to the ***VOIP2320*** network. This 2-step SIP messaging model is displayed in the diagram below.

This architecture means that for all physical SIP-devices on the customer LAN, the appropriate SIP Proxy Server setting will be to assign it to the LAN IP address of the EdgeMarc router itself. The standardized IP address assignment in all of the LAN designs in this document is “192.168.1.1”. This setting should be used for configurations of IP phones and ATAs.

SIP CPE CONFIGURATION:
SIP PROXY SERVER =192.168.1.1


IP Network
192.168.1.1/24
Ethernet LAN
SIP Call-Control Signalling IP Phone to Edgemarc
SIP Call-Control Signalling NGT to Edgemarc
NGT Servers
Customer Premise

VLAN Switch and Phone Configuration for Network 3.1

When Network Design 3.1 is used as a deployment solution, special consideration will need to be applied to the configuration of the SIP devices as well as the LAN switch. Network 3.1 is based-upon the use of VLAN tagging, or 802.1q. This allows for the ability to connect 2 IP devices (for example, a PC and an IP phone) to the same physical Cat-5 cable but logically separate traffic onto 2 unique IP subnets. By doing this, separate routing and security can be applied to each IP subnet. So, of particular concern is that the LAN switch utilized is able to support the use 802.1q VLAN technology. ***VOIP2320*** has not chosen to require the use of specific VLAN switch equipment, however this functional will need to be available when using this network design.

VLAN tagging uses the insertion of an ancillary header in the Ethernet frame that identifies the appropriate VLAN to associate a packet to. The IEEE has defined an optional tag for 802.x networks which can convey additional Layer 2 information. This four-byte tag is inserted between the MAC addresses and Ethertype fields of the Ethernet frame, and the Maximum Transmission Unit (MTU) of a tag-enabled interface is increased by four so that the use of tags does not cause a decrease in the MTU available to Layer 3 protocols (such as IP). The first two bytes of the tag are statically defined to the Ethertype for tags, so that tagged frames can be distinguished from untagged frames. Twelve bits optionally encode a VLAN number (0-4095), and three bits encode the QoS value (0-7). Each Ethernet link has a “native VLAN” which is assumed for all frames which do not have a tag or which have a VLAN number of 0 in the tag.

So when configuring the 3.1 Network for the first time, before the phones and PCs will properly function you will need to verify that the proper VLAN configurations are setup in your phones and VLAN switch. First, the phones will need to be setup to function on VLAN ID #1, as it is defined as the Voice VLAN. Secondly, because the PCs generally will not support VLAN tagging your switch will need to be setup to default untagged packets to the Data VLAN assignment of VLAN ID #500. Lastly, you will need to create a VLAN trunk port on your switch to aggregate traffic back to the EdgeMarc. This port will need to be associated with all 3 VLANs, #1-Voice, #500-Data & #600 ***VOIP2320*** (if applicable).

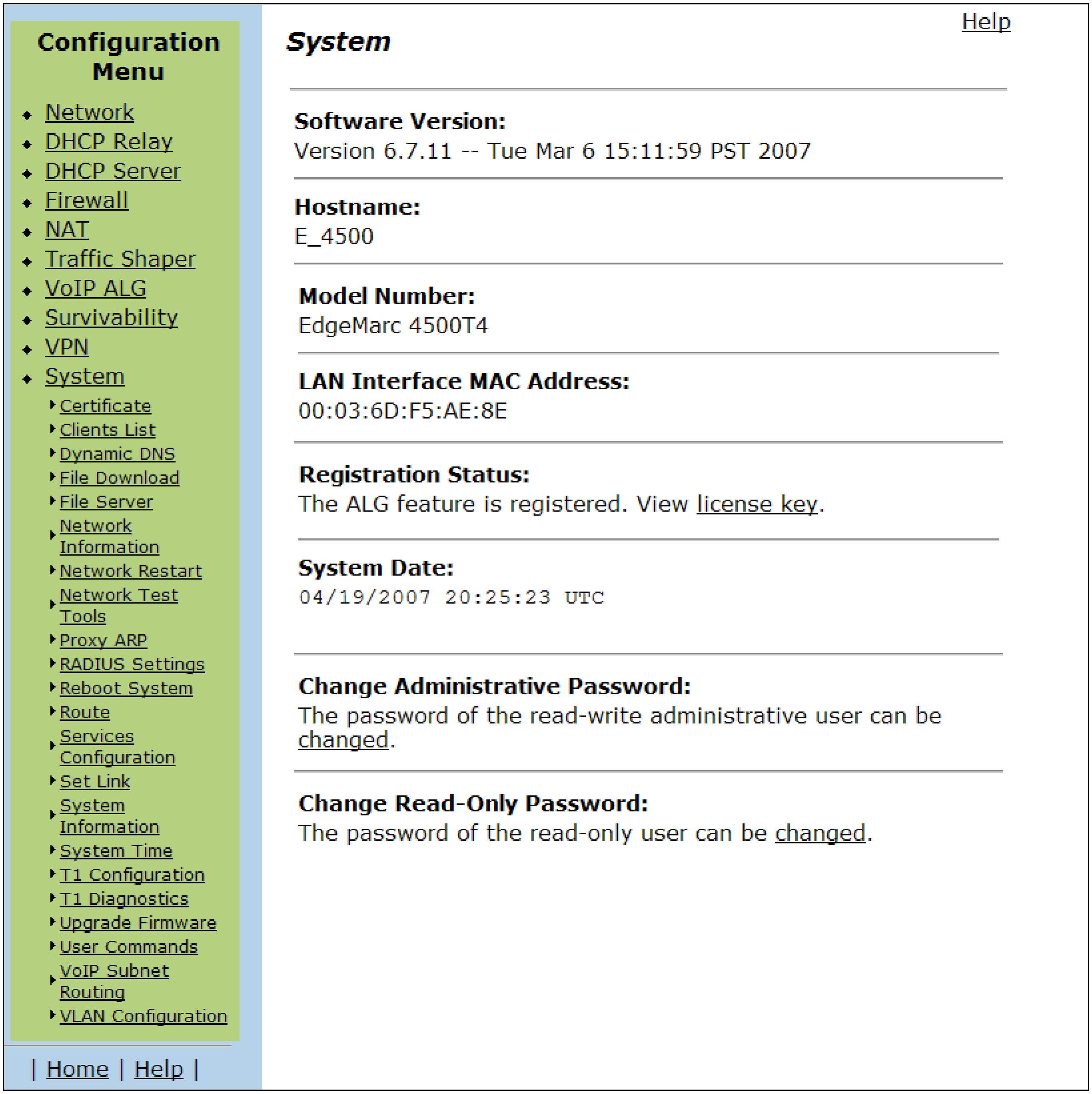
Pre-Configuration Requirements for Network 3.1

- **Phones need to be setup to VLAN ID #1**
- **VLAN Switch needs to default Untagged Packets to VLAN ID #500 for all PCs connected to it.**
- **Configure a VLAN trunk port on your switch. Assign to VLAN #1, #500, and #600(if applicable). All VLANs packets should be tagged on the VLAN Trunk port. Connect this switch port to physical LAN port #1 of the EdgeMarc.**

EdgeMarc Configuration Screenshots

Screenshot #1, EdgeMarc Main Menu

- Select left column Menu options to navigate configuration screens



System

Software Version:
Version 6.7.11 -- Tue Mar 6 15:11:59 PST 2007

Hostname:
E_4500

Model Number:
EdgeMarc 4500T4

LAN Interface MAC Address:
00:03:6D:F5:AE:8E

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

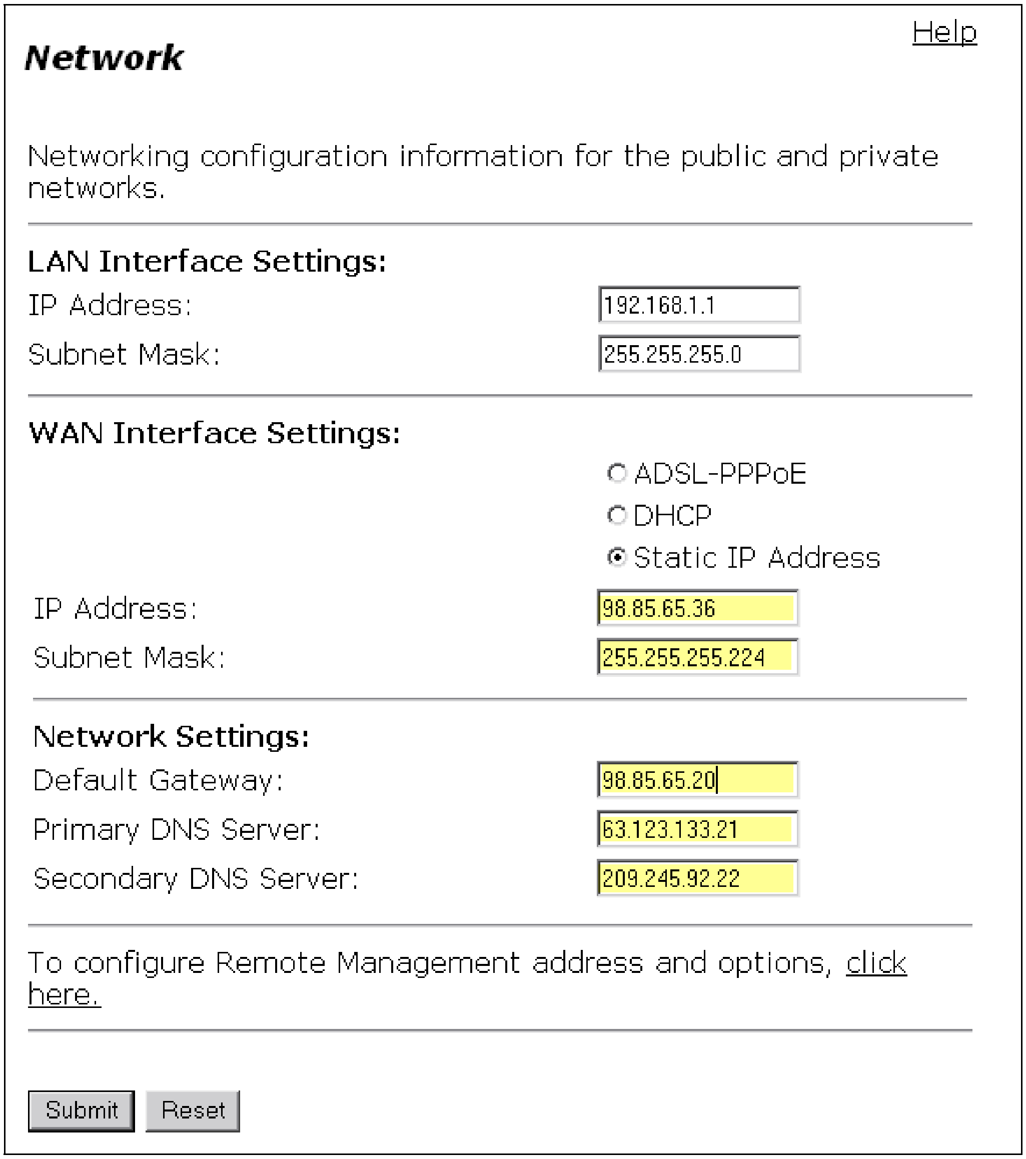
System Date:
04/19/2007 20:25:23 UTC

Change Administrative Password:
The password of the read-write administrative user can be changed.

Change Read-Only Password:
The password of the read-only user can be changed.

Screenshot #2, Network Settings Main Screen, No VLAN

- Default LAN IP address defaults to 192.168.1.1/255.255.255.0
    - Change only if necessary. Configuration examples assume no change.
- Select the correct WAN Interface Option
    - If static, then enter the IP address and mask
    - If T1, enter the static IP and mask, then follow link to T1 configuration
- Enter Default gateway IP address
- Enter at least a Primary DNS Server, Secondary if available



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

WAN Interface Settings:

○ ADSL-PPPoE
○ DHCP
● Static IP Address

IP Address:	98.85.65.36
Subnet Mask:	255.255.255.224

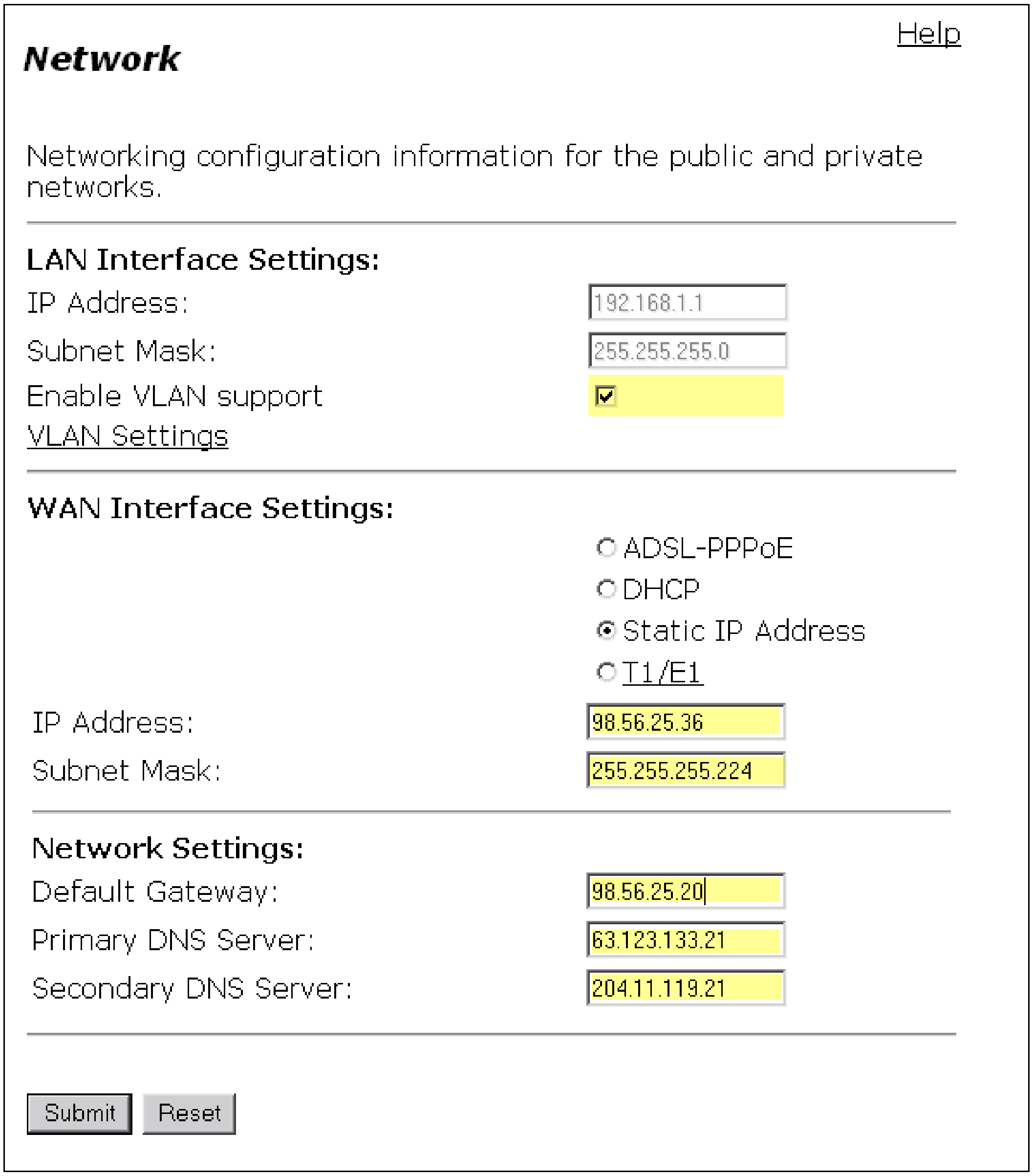
Network Settings:

Default Gateway:	98.85.65.20
Primary DNS Server:	63.123.133.21
Secondary DNS Server:	209.245.92.22

To configure Remote Management address and options, click here.

Screenshot #3, Network Settings Main Screen, with VLANs

- Default LAN IP address defaults to 192.168.1.1/255.255.255.0
    - Change only if necessary. Configuration examples assume no change.
    - Check Enable VLAN support only after VLAN configuration is complete
- Select the correct WAN Interface Option
    - If static, then enter the IP address and mask
    - If T1, enter the static IP and mask, then follow link to T1 configuration
- Enter Default gateway IP address
- Enter at least a Primary DNS Server, Secondary if available



Help

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
Enable VLAN support	☑

VLAN Settings

WAN Interface Settings:

○ ADSL-PPPoE
○ DHCP
● Static IP Address
○ T1/E1

IP Address:	98.56.25.36
Subnet Mask:	255.255.255.224

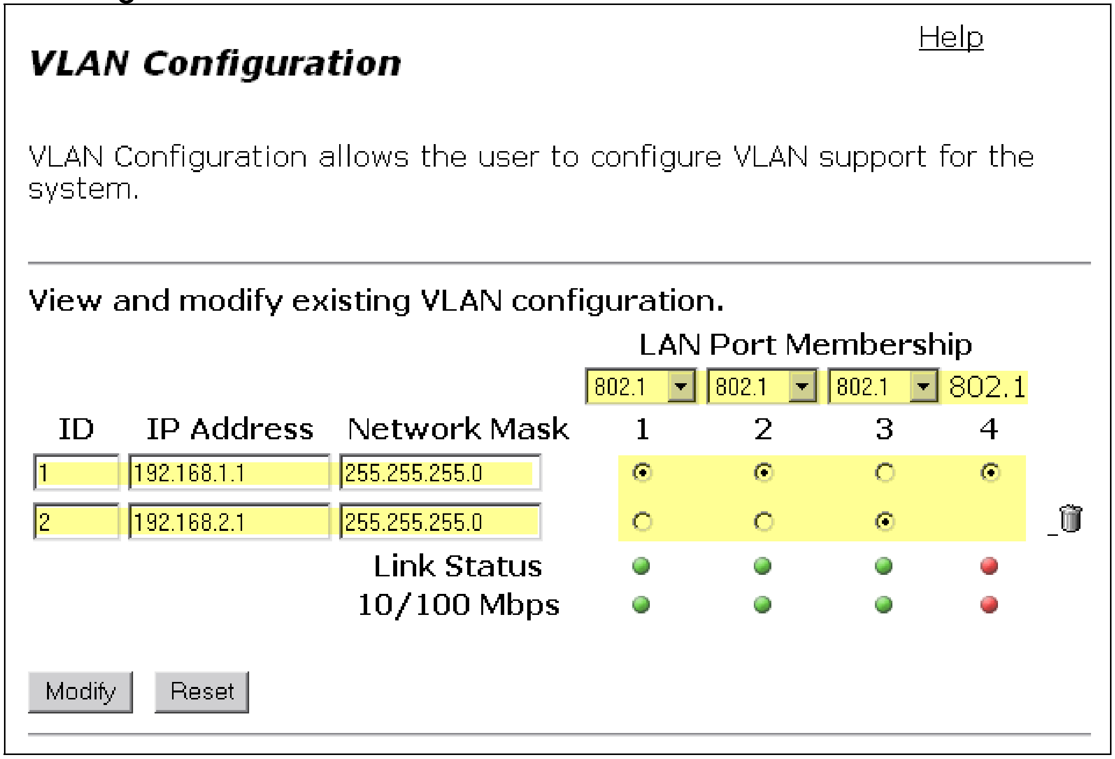
Network Settings:

Default Gateway:	98.56.25.20
Primary DNS Server:	63.123.133.21
Secondary DNS Server:	204.11.119.21

Screenshot #4 (a-d), VLAN Configuration

Screenshot 4a-VLAN Configuration for Network 2.1
Screenshot 4b-VLAN Configuration for Network 3.1
Screenshot 4c-VLAN Configuration for Network 4.1
Screenshot 4d-VLAN Configuration for Network 5.1

4a, VLAN Configuration for Network 2.1



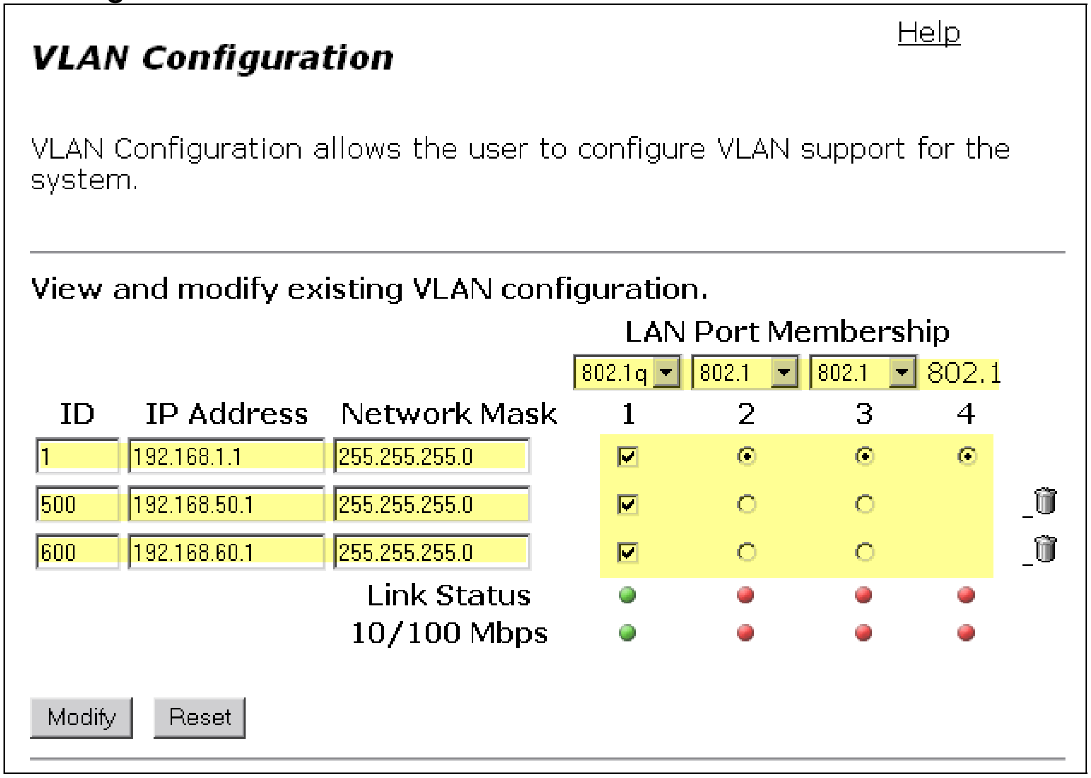
VLAN Configuration

VLAN Configuration allows the user to configure VLAN support for the system.

View and modify existing VLAN configuration.

			LAN Port Membership			
			802.1	802.1	802.1	802.1
ID	IP Address	Network Mask	1	2	3	4
1	192.168.1.1	255.255.255.0	●	●	○	●
2	192.168.2.1	255.255.255.0	○	○	●	
		Link Status	🟢	🟢	🟢	🔴
		10/100 Mbps	🟢	🟢	🟢	🔴

4b, VLAN Configuration for Network 3.1



Help

VLAN Configuration

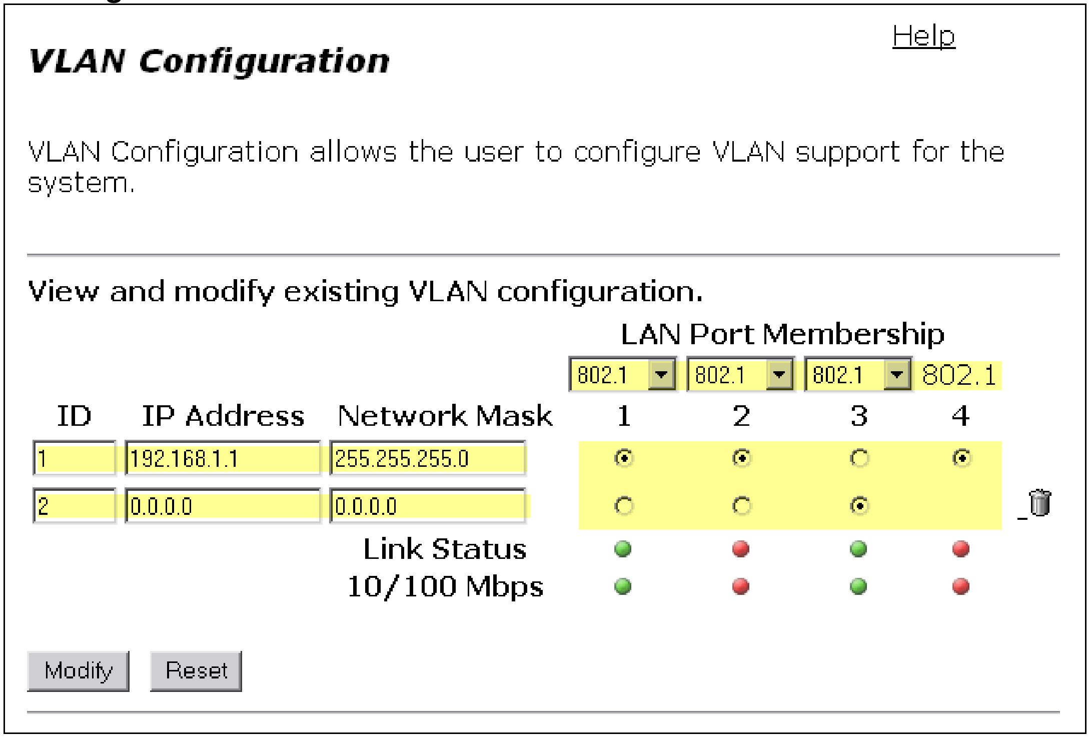
VLAN Configuration allows the user to configure VLAN support for the system.

View and modify existing VLAN configuration.

			LAN Port Membership				
			802.1q	802.1	802.1	802.1	
ID	IP Address	Network Mask	1	2	3	4	
1	192.168.1.1	255.255.255.0	☑	●	●	●	
500	192.168.50.1	255.255.255.0	☑	○	○		🗑
600	192.168.60.1	255.255.255.0	☑	○	○		🗑
		Link Status	🟢	🔴	🔴	🔴	
		10/100 Mbps	🟢	🔴	🔴	🔴	

Modify Reset

4c, VLAN Configuration for Network 4.1



Help

VLAN Configuration

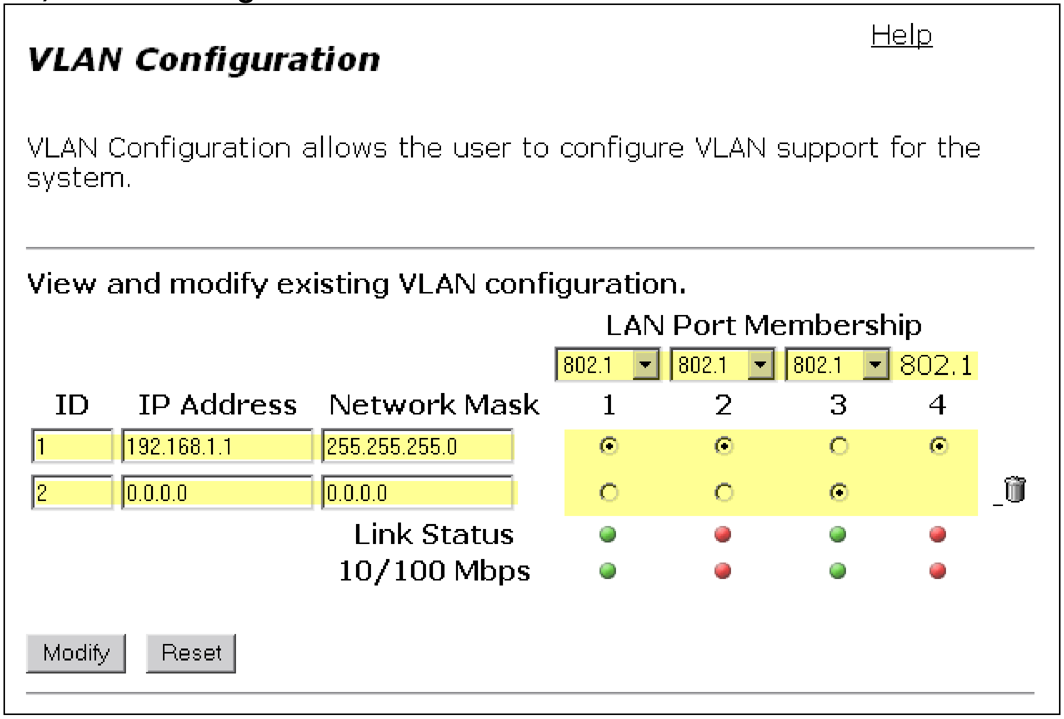
VLAN Configuration allows the user to configure VLAN support for the system.

View and modify existing VLAN configuration.

			LAN Port Membership				
			802.1	802.1	802.1	802.1	
ID	IP Address	Network Mask	1	2	3	4	
1	192.168.1.1	255.255.255.0	●	●	○	●	
2	0.0.0.0	0.0.0.0	○	○	●		🗑
		Link Status	🟢	🔴	🟢	🔴	
		10/100 Mbps	🟢	🔴	🟢	🔴	

Modify Reset

4d, VLAN Configuration for Network 5.1



VLAN Configuration

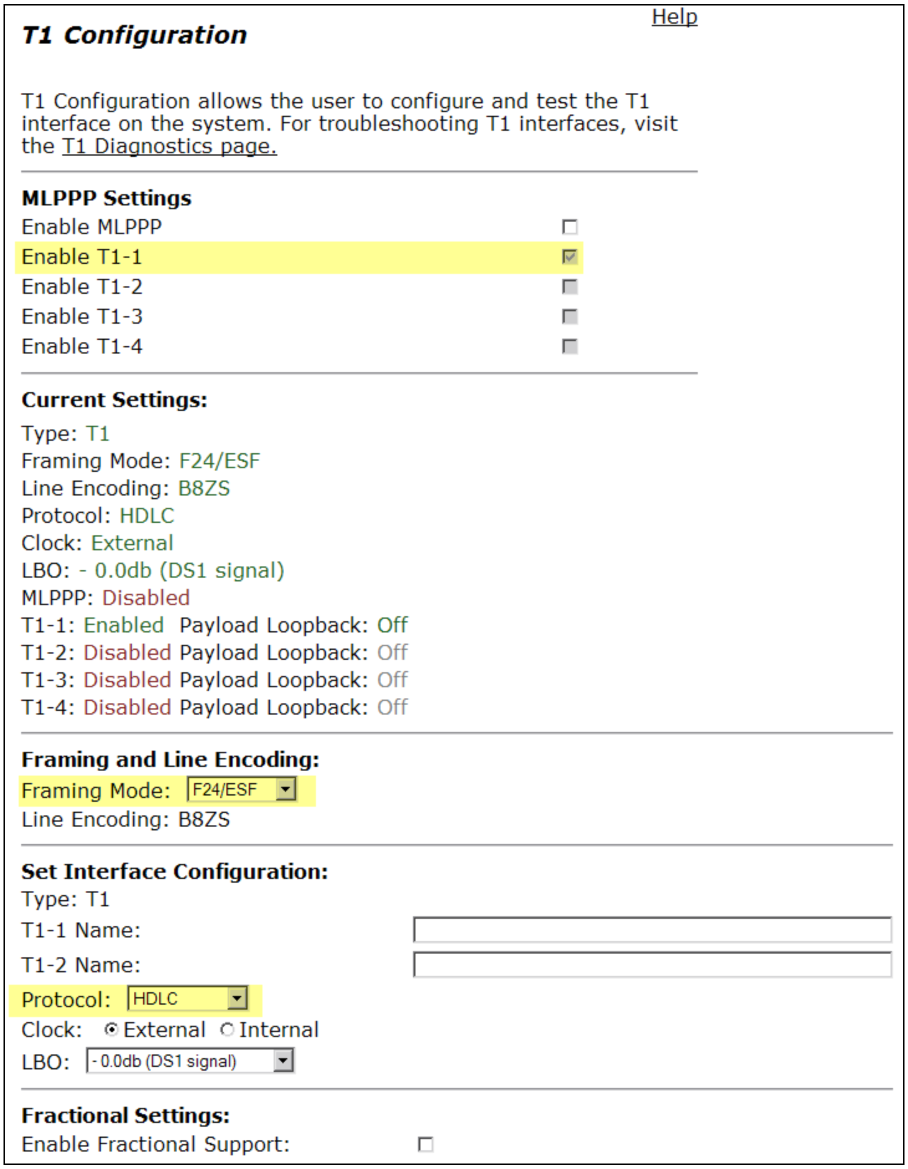
VLAN Configuration allows the user to configure VLAN support for the system.

View and modify existing VLAN configuration.

			LAN Port Membership			
			802.1	802.1	802.1	802.1
ID	IP Address	Network Mask	1	2	3	4
1	192.168.1.1	255.255.255.0	●	●	○	●
2	0.0.0.0	0.0.0.0	○	○	●	
		Link Status	🟢	🔴	🟢	🔴
		10/100 Mbps	🟢	🔴	🟢	🔴

Screenshot #5, Network Settings T1 Configuration, Sub-screen

- Select T1 Protocol from pull down list
- Enter appropriate T1 protocol settings (to be defined by T1 Service Provider)



T1 Configuration Help

T1 Configuration allows the user to configure and test the T1 interface on the system. For troubleshooting T1 interfaces, visit the T1 Diagnostics page.

MLPPP Settings

Enable MLPPP ☐
Enable T1-1 ☑
Enable T1-2 ☐
Enable T1-3 ☐
Enable T1-4 ☐

Current Settings:

Type: T1
Framing Mode: F24/ESF
Line Encoding: B8ZS
Protocol: HDLC
Clock: External
LBO: - 0.0db (DS1 signal)
MLPPP: Disabled
T1-1: Enabled Payload Loopback: Off
T1-2: Disabled Payload Loopback: Off
T1-3: Disabled Payload Loopback: Off
T1-4: Disabled Payload Loopback: Off

Framing and Line Encoding:

Framing Mode: F24/ESF ▾
Line Encoding: B8ZS

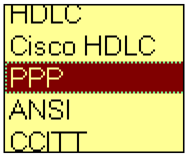
Set Interface Configuration:

Type: T1
T1-1 Name:
T1-2 Name:
Protocol: HDLC ▾
Clock: ● External ○ Internal
LBO: - 0.0db (DS1 signal) ▾

Fractional Settings:

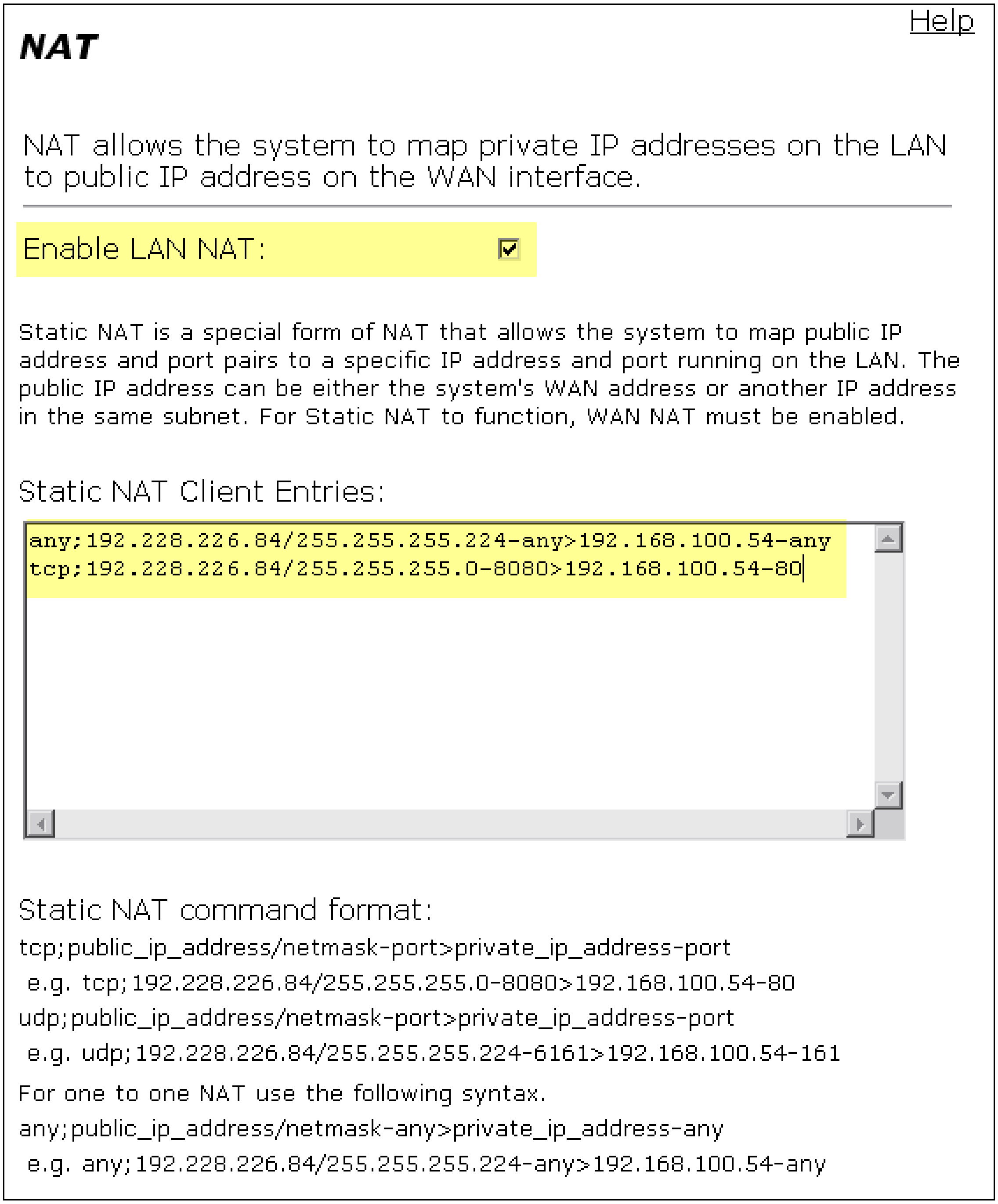
Enable Fractional Support: ☐

Select T1 Protocol Option from pull down:



Screenshot #6, NAT Settings

- Select-Enable LAN NAT
- If necessary, enter static NAT Client Entries



NAT

NAT allows the system to map private IP addresses on the LAN to public IP address on the WAN interface.

Enable LAN NAT: ☑

Static NAT is a special form of NAT that allows the system to map public IP address and port pairs to a specific IP address and port running on the LAN. The public IP address can be either the system's WAN address or another IP address in the same subnet. For Static NAT to function, WAN NAT must be enabled.

Static NAT Client Entries:

```
any;192.228.226.84/255.255.255.224-any>192.168.100.54-any
tcp;192.228.226.84/255.255.255.0-8080>192.168.100.54-80
```

Static NAT command format:

tcp;public_ip_address/netmask-port>private_ip_address-port

e.g. tcp;192.228.226.84/255.255.255.0-8080>192.168.100.54-80

udp;public_ip_address/netmask-port>private_ip_address-port

e.g. udp;192.228.226.84/255.255.255.224-6161>192.168.100.54-161

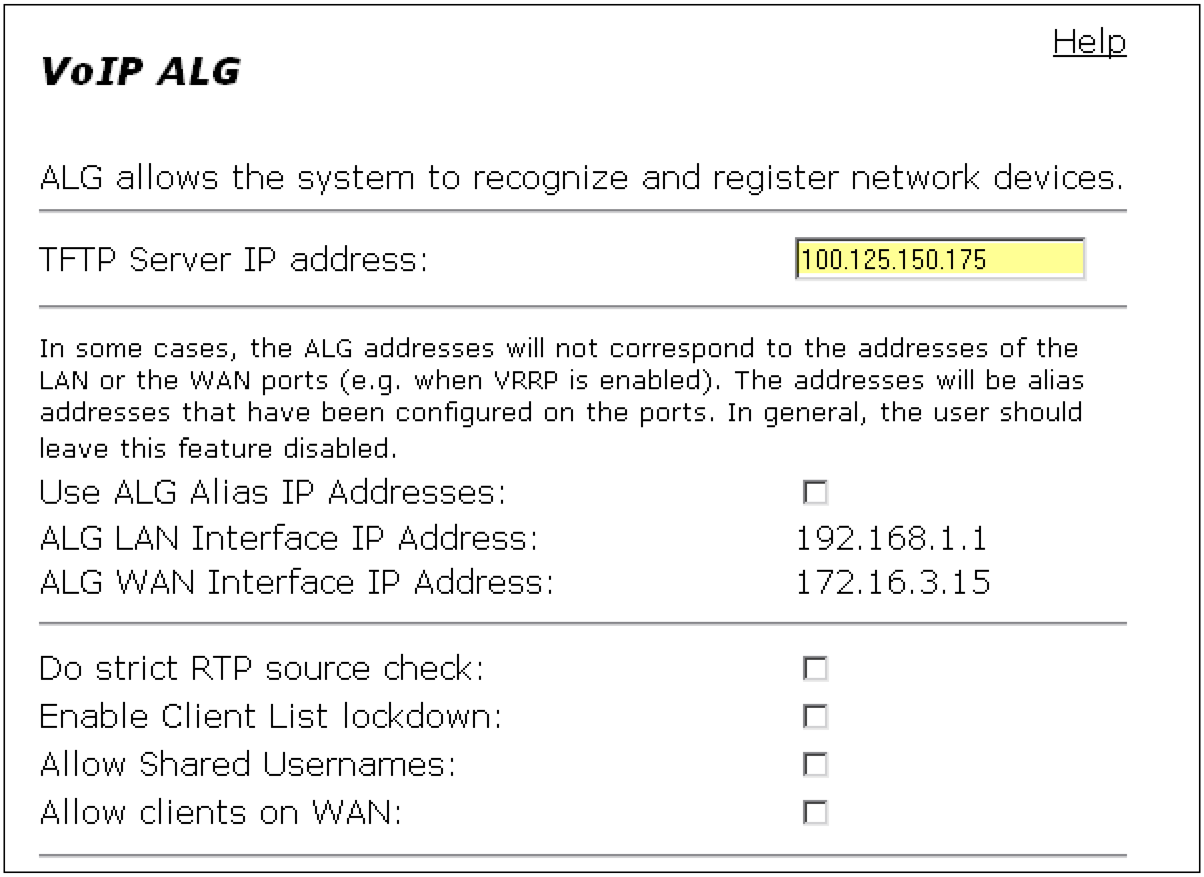
For one to one NAT use the following syntax.

any;public_ip_address/netmask-any>private_ip_address-any

e.g. any;192.228.226.84/255.255.255.224-any>192.168.100.54-any

Screenshot #7, VOIP ALG, Main Screen, No VLANs

- The TFTP Server address should be set to the WAN-side Public TFTP server if the EdgeMarc's built-in TFTP/FTP Server function is not enabled. Otherwise, leave the TFTP Server IP as default 0.0.0.0.



VoIP ALG

ALG allows the system to recognize and register network devices.

TFTP Server IP address: 100.125.150.175

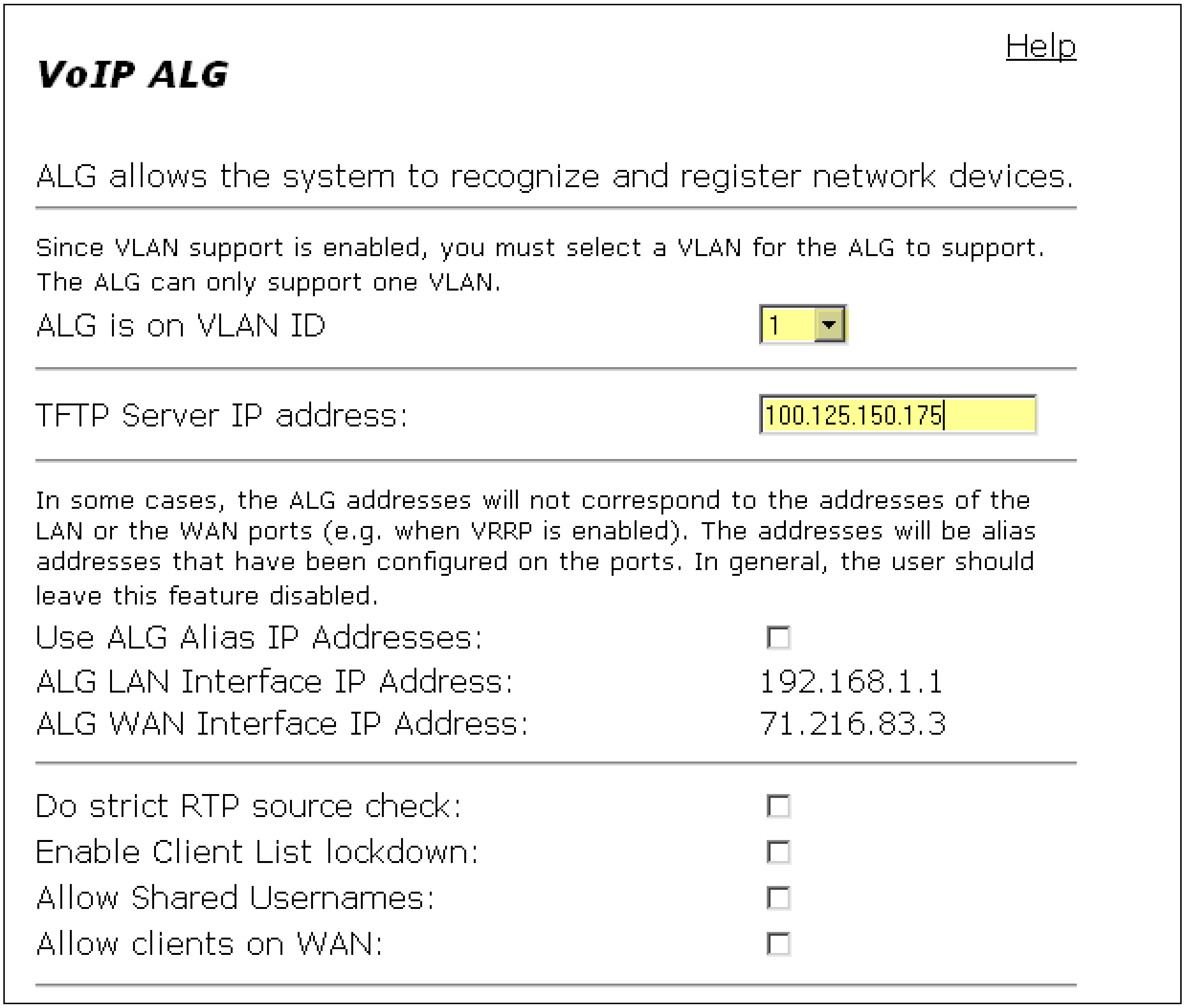
In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports (e.g. when VRRP is enabled). The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

Use ALG Alias IP Addresses: □
ALG LAN Interface IP Address: 192.168.1.1
ALG WAN Interface IP Address: 172.16.3.15

Do strict RTP source check: □
Enable Client List lockdown: □
Allow Shared Usernames: □
Allow clients on WAN: □

Screenshot #8, VOIP ALG-Main Screen, with VLANs

- Select the VLAD ID to apply the VOIP ALG functionality to.
  - To be done only after VLAN configuration
- The TFTP Server address should be set to the WAN-side Public TFTP server if the EdgeMarc's built-in TFTP/FTP Server function is not enabled. Otherwise, leave the TFTP Server IP as default 0.0.0.0.



VoIP ALG

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 is on VLAN ID: 1

TFTP Server IP address: 100.125.150.175

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports (e.g. when VRRP is enabled). 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: 192.168.1.1

ALG WAN Interface IP Address: 71.216.83.3

Do strict RTP source check: □

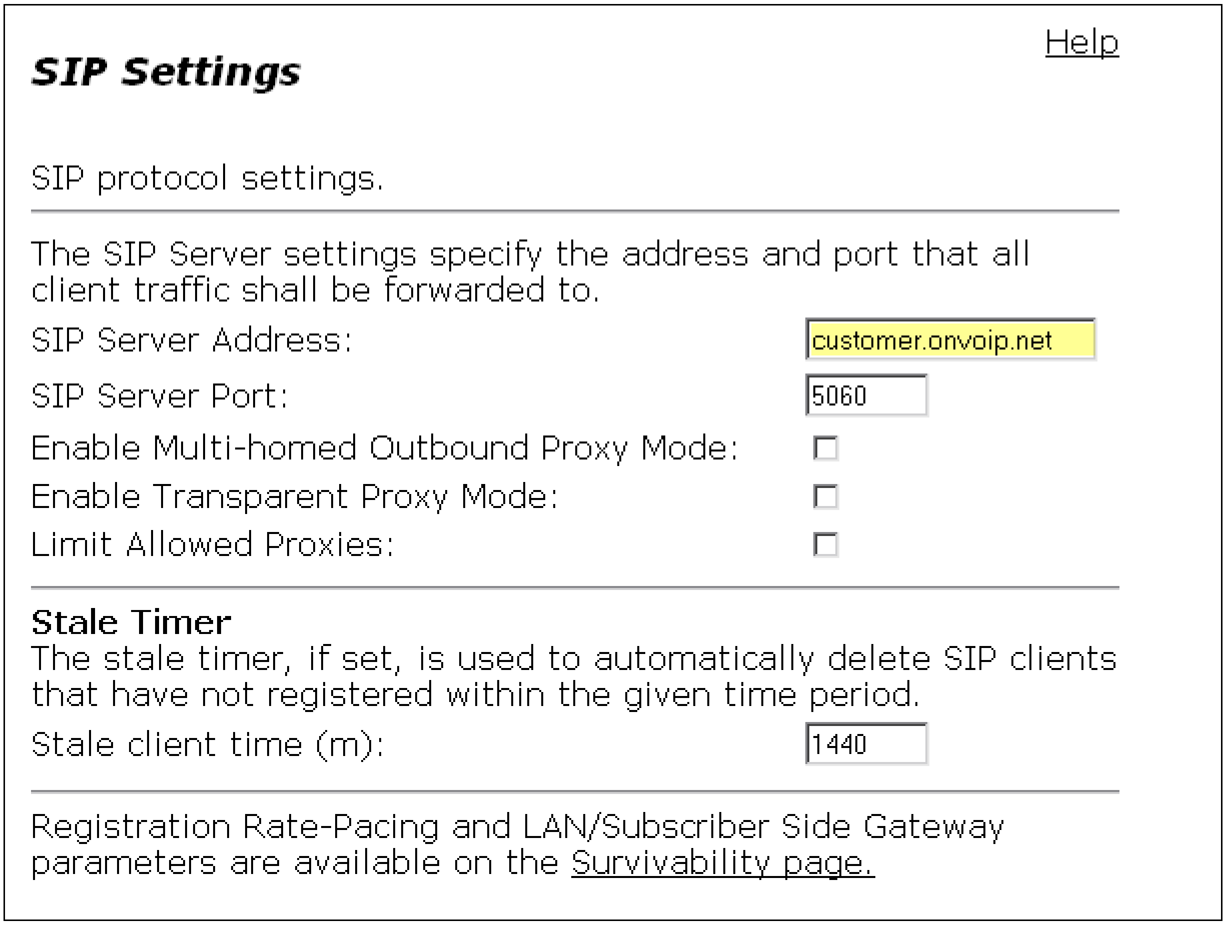
Enable Client List lockdown: □

Allow Shared Usernames: □

Allow clients on WAN: □

Screenshot #9, VOIP ALG, SIP Settings Sub-screen

- Enter your specific assigned value for the **SIP Server Address** as: ***.onvoip.net.***
- Screenshot entry is only an example.



SIP Settings

SIP protocol settings.

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

SIP Server Address:	customer.onvoip.net
SIP Server Port:	5060
Enable Multi-homed Outbound Proxy Mode:	□
Enable Transparent Proxy Mode:	□
Limit Allowed Proxies:	□

Stale Timer
The stale timer, if set, is used to automatically delete SIP clients that have not registered within the given time period.

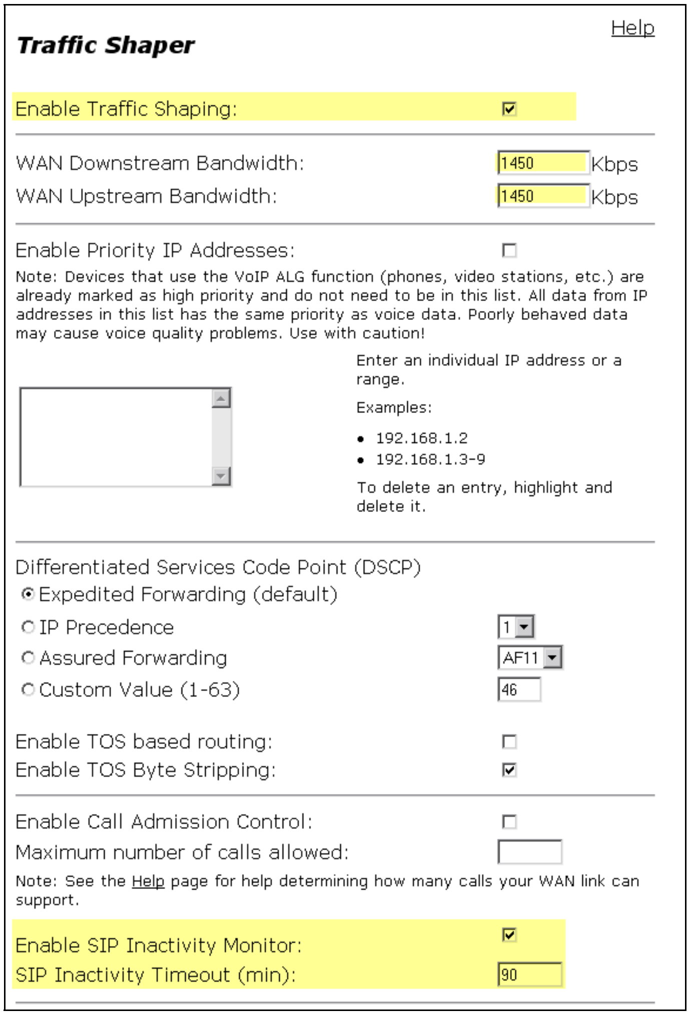
Stale client time (m):	1440

Registration Rate-Pacing and LAN/Subscriber Side Gateway parameters are available on the Survivability page.

Screenshot #10, Traffic Shaper

- Select Enable Traffic Shaping checkbox
- Set Upstream and Downstream bandwidth
- Select Enable TOS Byte Stripping checkbox
- Enable Call Admission Control Do not check! (Use BroadSoft Call Capacity Mgmt instead)

Note: The actual available bandwidth can be determined by disabling the Traffic Shaper and running a speed test from a LAN-side PC to an Internet testing service, such as dslreports.com. Set the Traffic Shaper's bandwidth to approximately 95% of the lower upstream and 95% of the lower downstream values provided by the test report.



Traffic Shaper

Help

Enable Traffic Shaping: ☑

WAN Downstream Bandwidth: 1450 Kbps
WAN Upstream Bandwidth: 1450 Kbps

Enable Priority IP Addresses: □

Note: Devices that use the VoIP ALG function (phones, video stations, etc.) are already marked as high priority and do not need to be in this list. All data from IP addresses in this list has the same priority as voice data. Poorly behaved data may cause voice quality problems. Use with caution!

Enter an individual IP address or a range.

Examples:

- 192.168.1.2
- 192.168.1.3-9

To delete an entry, highlight and delete it.

Differentiated Services Code Point (DSCP)
● Expedited Forwarding (default)
○ IP Precedence 1
○ Assured Forwarding AF11
○ Custom Value (1-63) 46

Enable TOS based routing: □
Enable TOS Byte Stripping: ☑

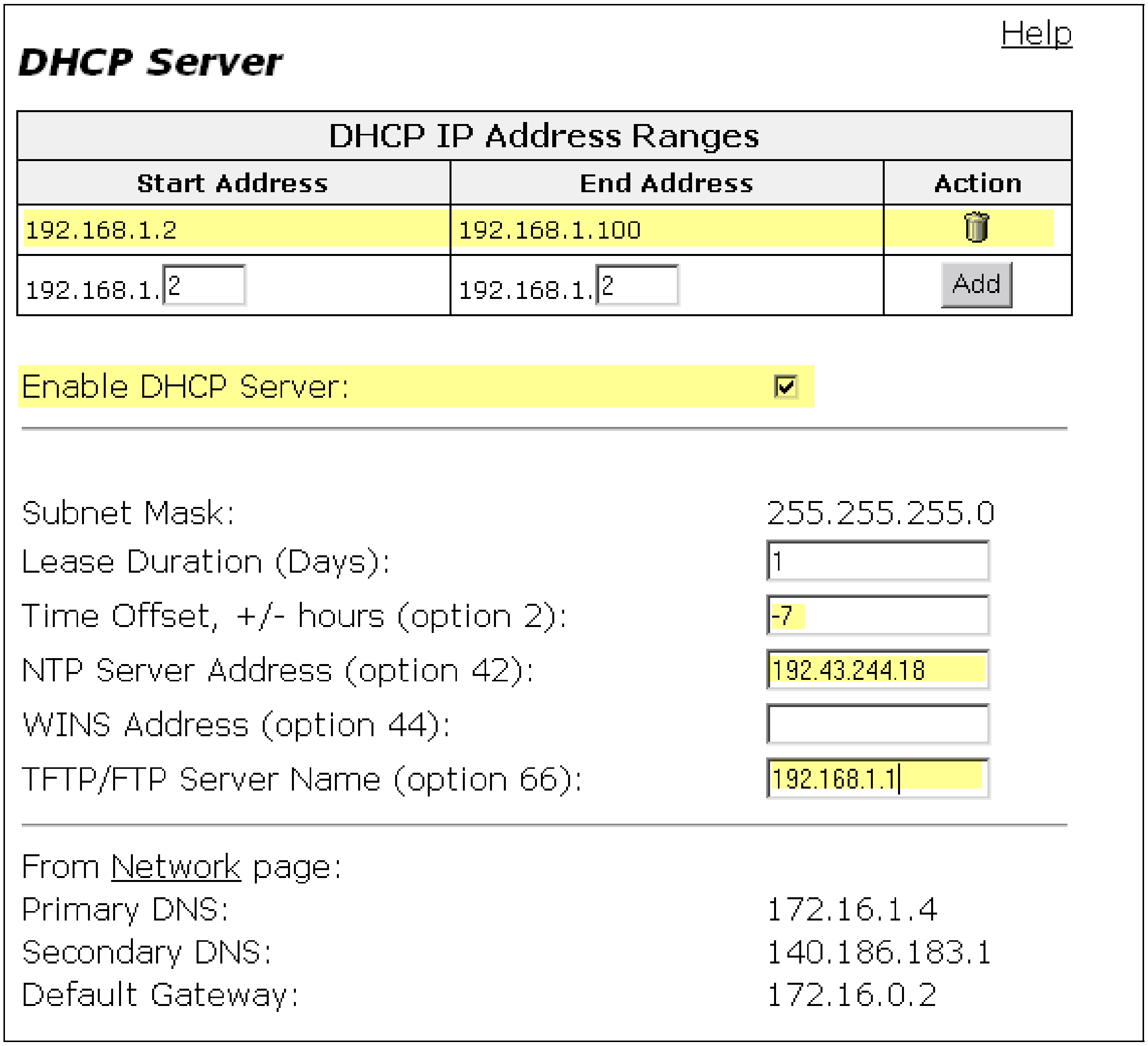
Enable Call Admission Control: □
Maximum number of calls allowed:

Note: See the Help page for help determining how many calls your WAN link can support.

Enable SIP Inactivity Monitor: ☑
SIP Inactivity Timeout (min): 90

Screenshot #11, DHCP Server, No VLANs

- Select checkbox for Enable DHCP Server
- Define a DHCP range for dynamic assignment
  - Press “Add:
- Set the proper timezone offset from GMT (-5 = EST, -8 = PST)
- Set a SNTP (Network Time Server) IP address or server name
- Set a TFTP/FTP Server Name (option 66). If TFTP is used, then this value must be the LAN Interface of the EdgeMarc (192.168.1.1). If FTP is used, then this value must be the actual FTP Server address.



DHCP Server

DHCP IP Address Ranges		
Start Address	**End Address**	**Action**
192.168.1.2	192.168.1.100	🗑
192.168.1.2	192.168.1.2	Add

Enable DHCP Server: ☑

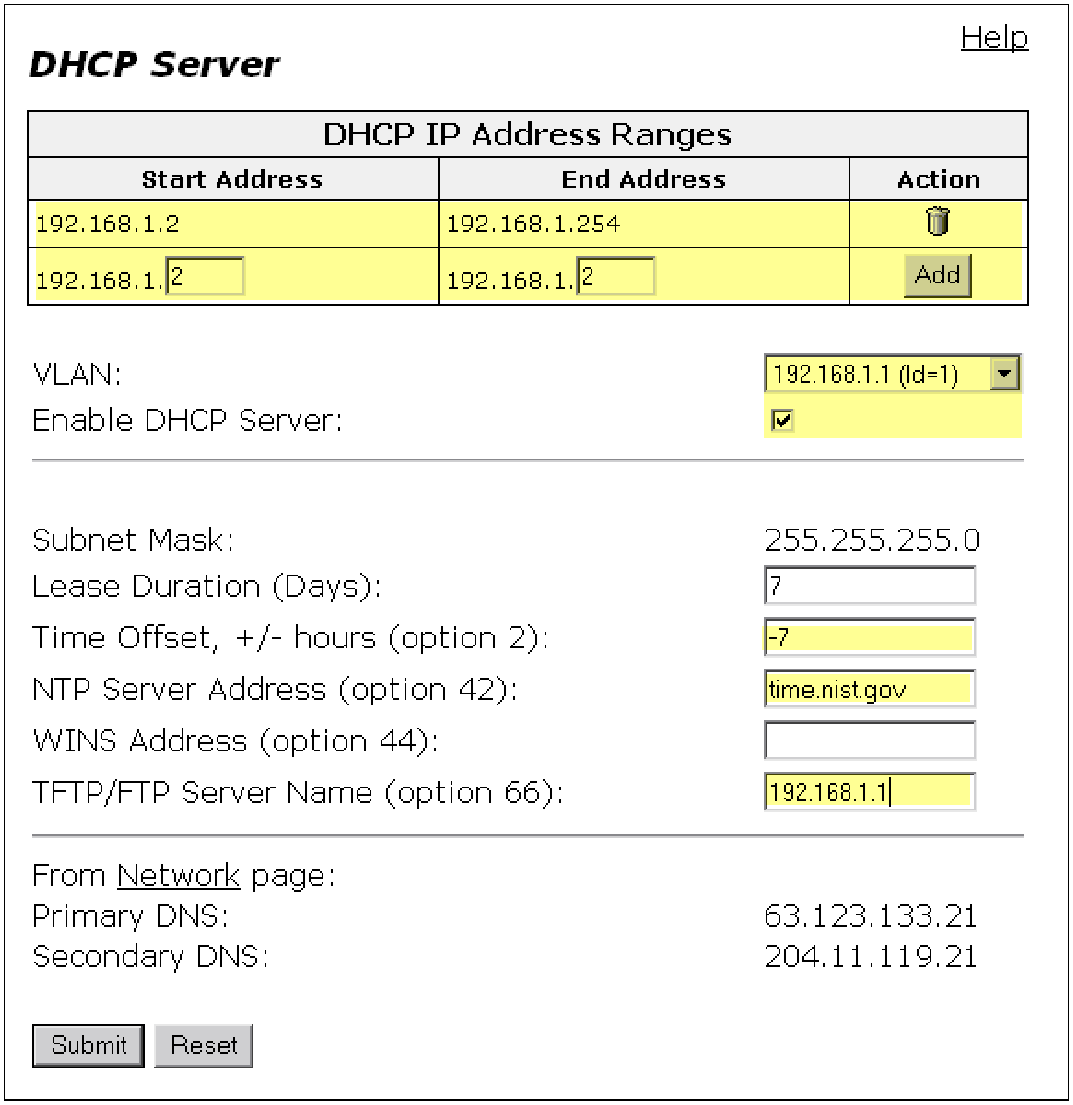
Subnet Mask:	255.255.255.0
Lease Duration (Days):	1
Time Offset, +/- hours (option 2):	-7
NTP Server Address (option 42):	192.43.244.18
WINS Address (option 44):	
TFTP/FTP Server Name (option 66):	192.168.1.1

From Network page:

Primary DNS:	172.16.1.4
Secondary DNS:	140.186.183.1
Default Gateway:	172.16.0.2

Screenshot #12, DHCP Server, with VLANs

- Select checkbox for Enable DHCP Server
- Select VLAN ID from pull down to assign DHCP server
- Define a DHCP range for dynamic assignment
  - Press “Add”
- Set the proper timezone offset from GMT (-5 = EST, -8 = PST)
- Set a SNTP (Network Time Server) IP address or server name
- Set a TFTP/FTP Server Name (option 66). If TFTP is used, then this value must be the LAN Interface of the EdgeMarc (192.168.1.1). If FTP is used, then this value must be the actual FTP Server address.



Help

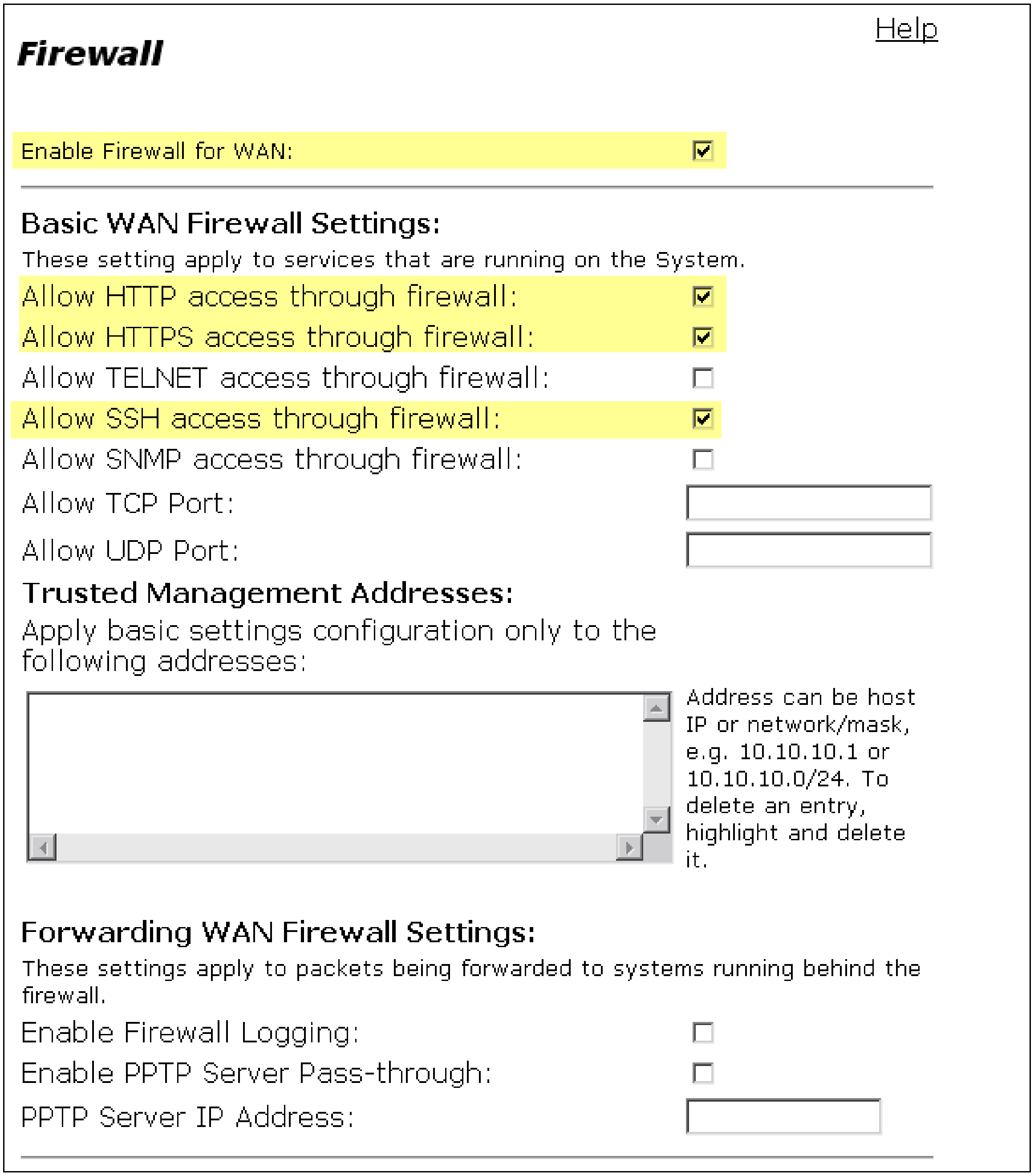
DHCP Server

DHCP IP Address Ranges		
Start Address	**End Address**	**Action**
192.168.1.2	192.168.1.254	🗑
192.168.1.2	192.168.1.2	Add

VLAN:	192.168.1.1 (Id=1) ▾
Enable DHCP Server:	☑
Subnet Mask:	255.255.255.0
Lease Duration (Days):	7
Time Offset, +/- hours (option 2):	-7
NTP Server Address (option 42):	time.nist.gov
WINS Address (option 44):	
TFTP/FTP Server Name (option 66):	192.168.1.1
From Network page:	
Primary DNS:	63.123.133.21
Secondary DNS:	204.11.119.21

Screenshot #13, Firewall Settings

- Enable HTTP, HTTPs and SSH access from WAN side for debug/management access.



Firewall

Enable Firewall for WAN: ☑

Basic WAN Firewall Settings:

These setting apply to services that are running on the System.

Allow HTTP access through firewall: ☑

Allow HTTPS access through firewall: ☑

Allow TELNET access through firewall: ☐

Allow SSH access through firewall: ☑

Allow SNMP access through firewall: ☐

Allow TCP Port:

Allow UDP Port:

Trusted Management Addresses:

Apply basic settings configuration only to the following addresses:

Address can be host IP or network/mask, e.g. 10.10.10.1 or 10.10.10.0/24. To delete an entry, highlight and delete it.

Forwarding WAN Firewall Settings:

These settings apply to packets being forwarded to systems running behind the firewall.

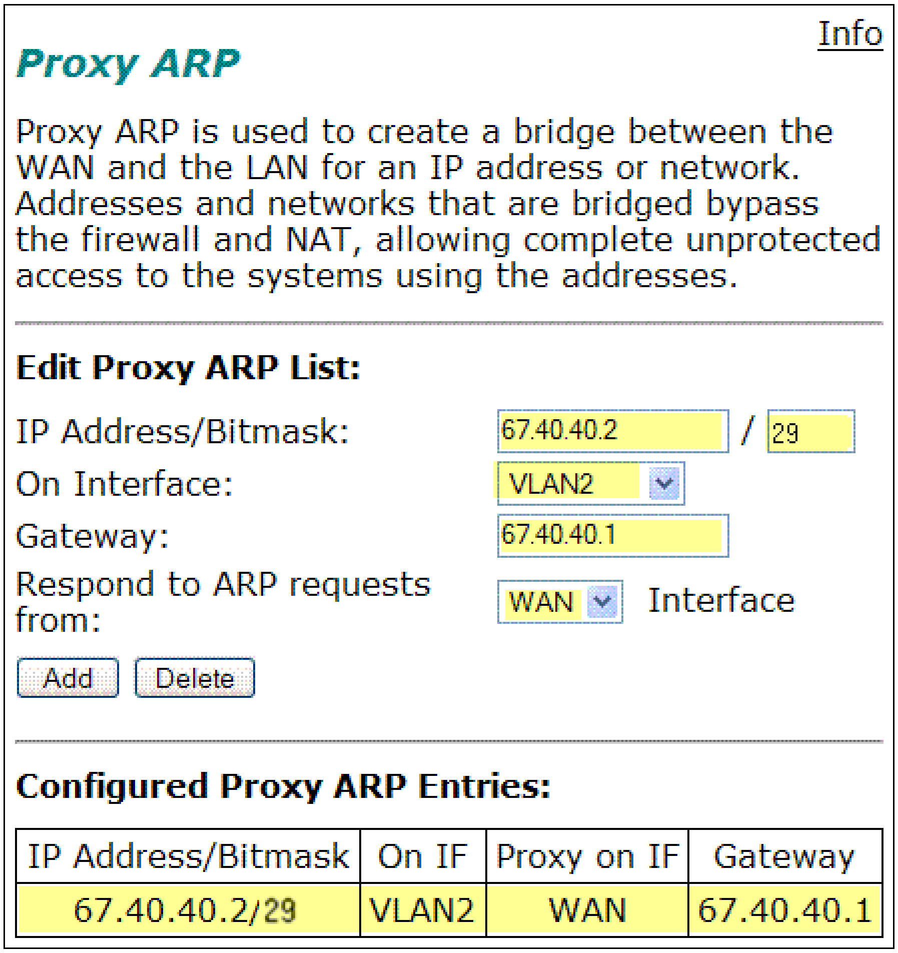
Enable Firewall Logging: ☐

Enable PPTP Server Pass-through: ☐

PPTP Server IP Address:

Screenshot #14, Proxy ARP

- Enter Public IP address and bitmask to be assigned to LAN-side 3rd-party device
  - Example: 67.40.40.2/29
  - Must be on same IP subnet as the WAN Public IP address
- Select the VLAN2 Interface
- Enter the Default Gateway IP address
  - Must match the Default Gateway IP on the Network Settings page
  - Example: 67.40.40.1
- Select WAN interface for Respond to ARP requests from:



Proxy ARP

Proxy ARP is used to create a bridge between the WAN and the LAN for an IP address or network. Addresses and networks that are bridged bypass the firewall and NAT, allowing complete unprotected access to the systems using the addresses.

Edit Proxy ARP List:

IP Address/Bitmask:	67.40.40.2 / 29
On Interface:	VLAN2
Gateway:	67.40.40.1
Respond to ARP requests from:	WAN Interface

Configured Proxy ARP Entries:

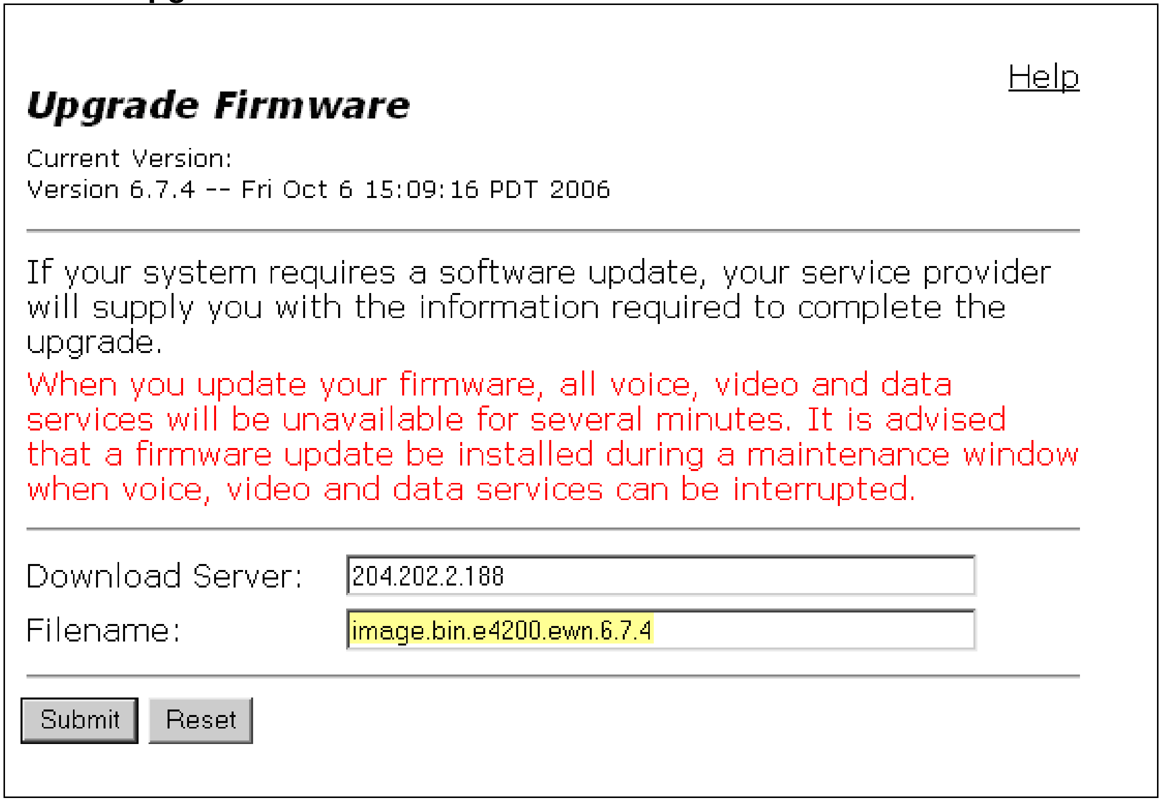
IP Address/Bitmask	On IF	Proxy on IF	Gateway
67.40.40.2/29	VLAN2	WAN	67.40.40.1

Screenshot #15 (a-c), Firmware Upgrade

- Enter firmware upgrade statement to comply with current ***VOIP2320*** version spec (15a)
  - Check ***VOIP2320*** Resource center for current version support
  - Example #1: Model 4200 to firmware code 6.7.4
    - Enter text: “image.bin.e4200.ewn.6.7.4”
  - Example #2: Model 4300 to firmware code 6.7.5
    - Enter text : “image.bin.e4300.ewn.6.7.5”
  - Example #3: Model 4500 to firmware code 6.7.11
    - Enter text : “image.bin.e4500.ewn.6.7.11”

- Monitor Progress screens (15b)
- Unit will reboot when complete (15c)

15a-Firmware Upgrade statement



Upgrade Firmware

Help

Current Version:
Version 6.7.4 -- Fri Oct 6 15:09:16 PDT 2006

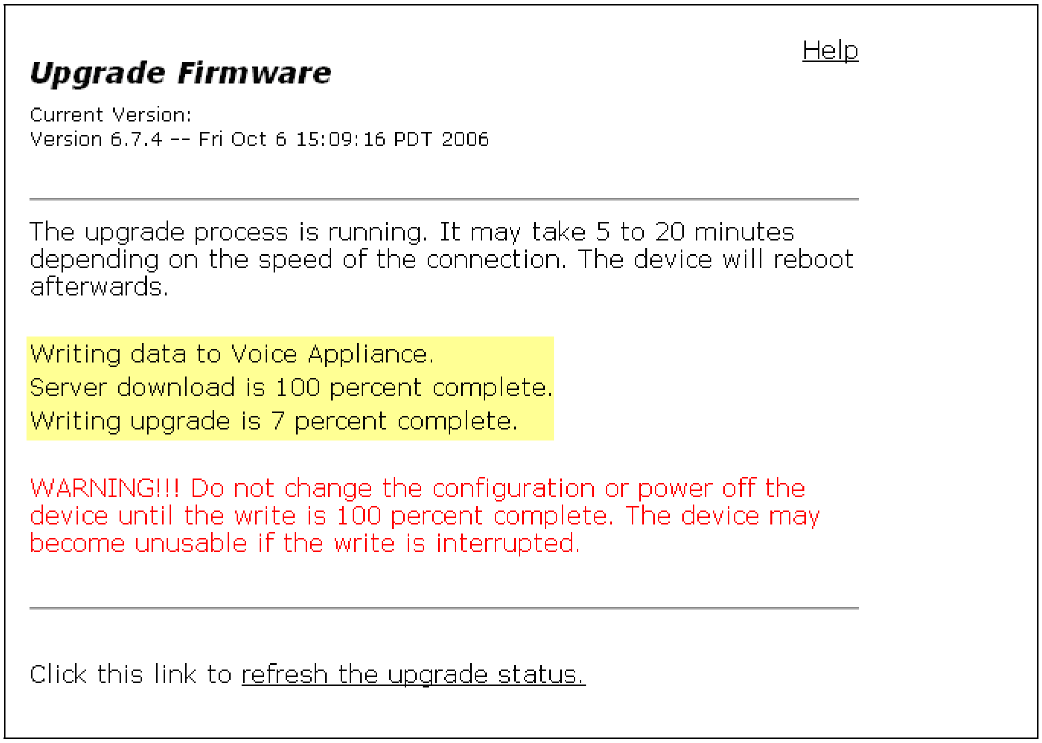
If your system requires a software update, your service provider will supply you with the information required to complete the upgrade.

When you update your firmware, all voice, video and data services will be unavailable for several minutes. It is advised that a firmware update be installed during a maintenance window when voice, video and data services can be interrupted.

Download Server: 204.202.2.188

Filename: image.bin.e4200.ewn.6.7.4

15b-Firmware download & write



Upgrade Firmware

Current Version:
Version 6.7.4 -- Fri Oct 6 15:09:16 PDT 2006

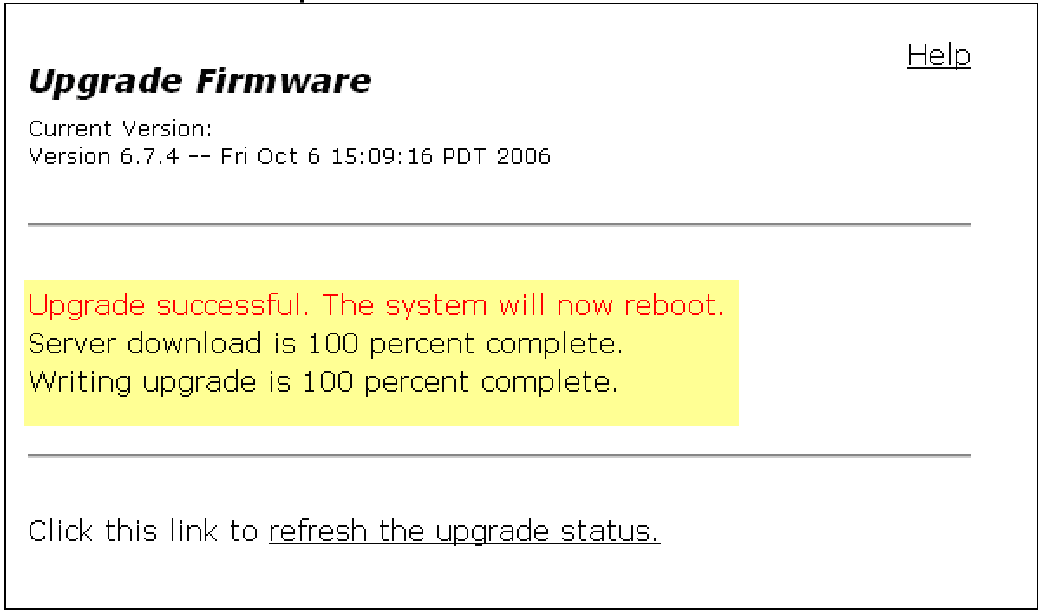
The upgrade process is running. It may take 5 to 20 minutes depending on the speed of the connection. The device will reboot afterwards.

Writing data to Voice Appliance.
Server download is 100 percent complete.
Writing upgrade is 7 percent complete.

WARNING!!! Do not change the configuration or power off the device until the write is 100 percent complete. The device may become unusable if the write is interrupted.

Click this link to refresh the upgrade status.

15c-Firmware Download Complete & Reboot



Upgrade Firmware

Current Version:
Version 6.7.4 -- Fri Oct 6 15:09:16 PDT 2006

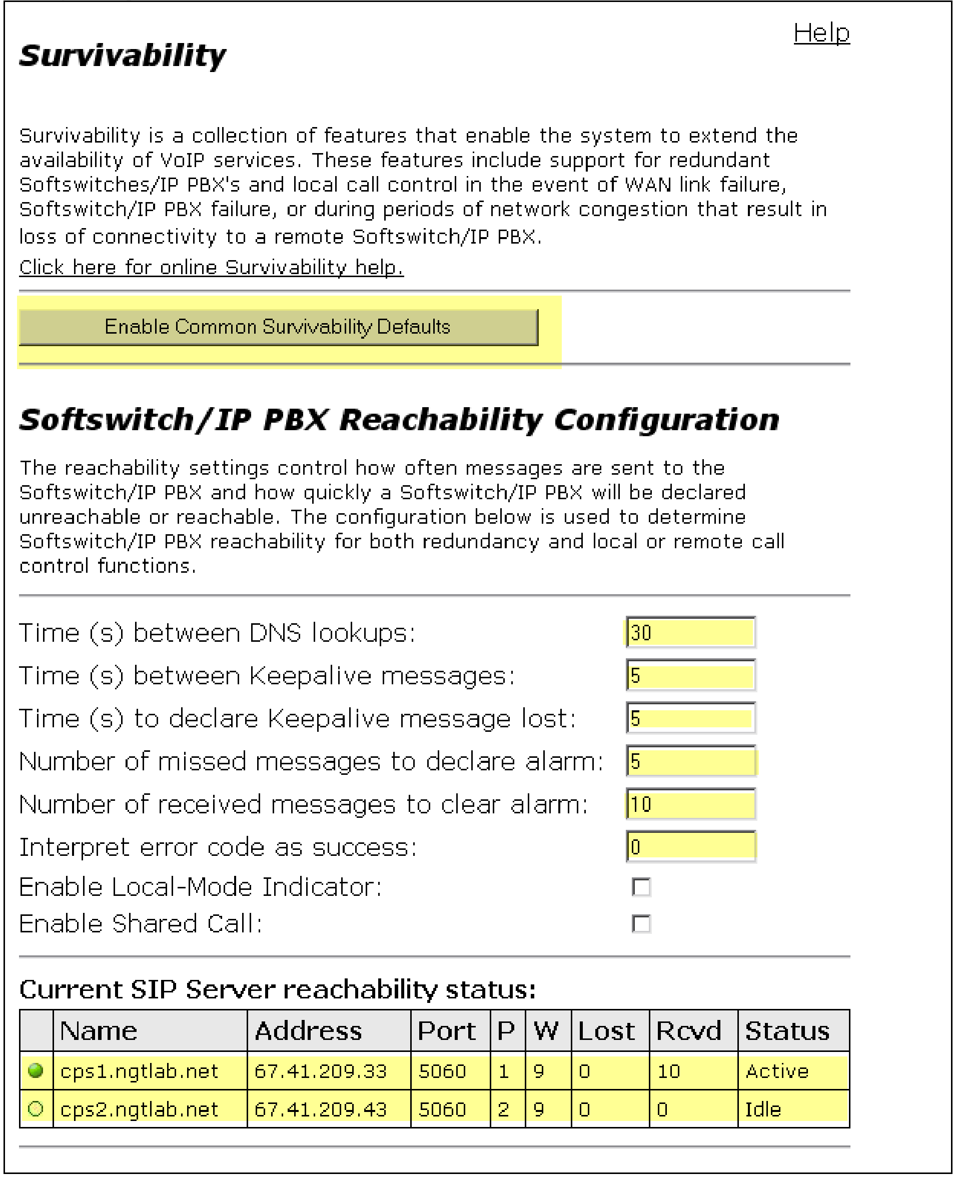
Upgrade successful. The system will now reboot.
Server download is 100 percent complete.
Writing upgrade is 100 percent complete.

Click this link to refresh the upgrade status.

Screenshot #16 (a-b), Survivability

- Click "Enable Common Survivability Defaults" button
  - This automatically defines the ***VOIP2320*** survivability settings
- Confirm redundant SIP Server reachability (16a)
  - 2 Servers will be identified. 1 active, 1 Idle.
  - Green button indicates active server
- Confirm all highlighted settings are as shown in 16a & 16b

16a –Survivability Top View



Help

Survivability

Survivability is a collection of features that enable the system to extend the availability of VoIP services. These features include support for redundant Softswitches/IP PBX's and local call control in the event of WAN link failure, Softswitch/IP PBX failure, or during periods of network congestion that result in loss of connectivity to a remote Softswitch/IP PBX.

Click here for online Survivability help.

Enable Common Survivability Defaults

Softswitch/IP PBX Reachability Configuration

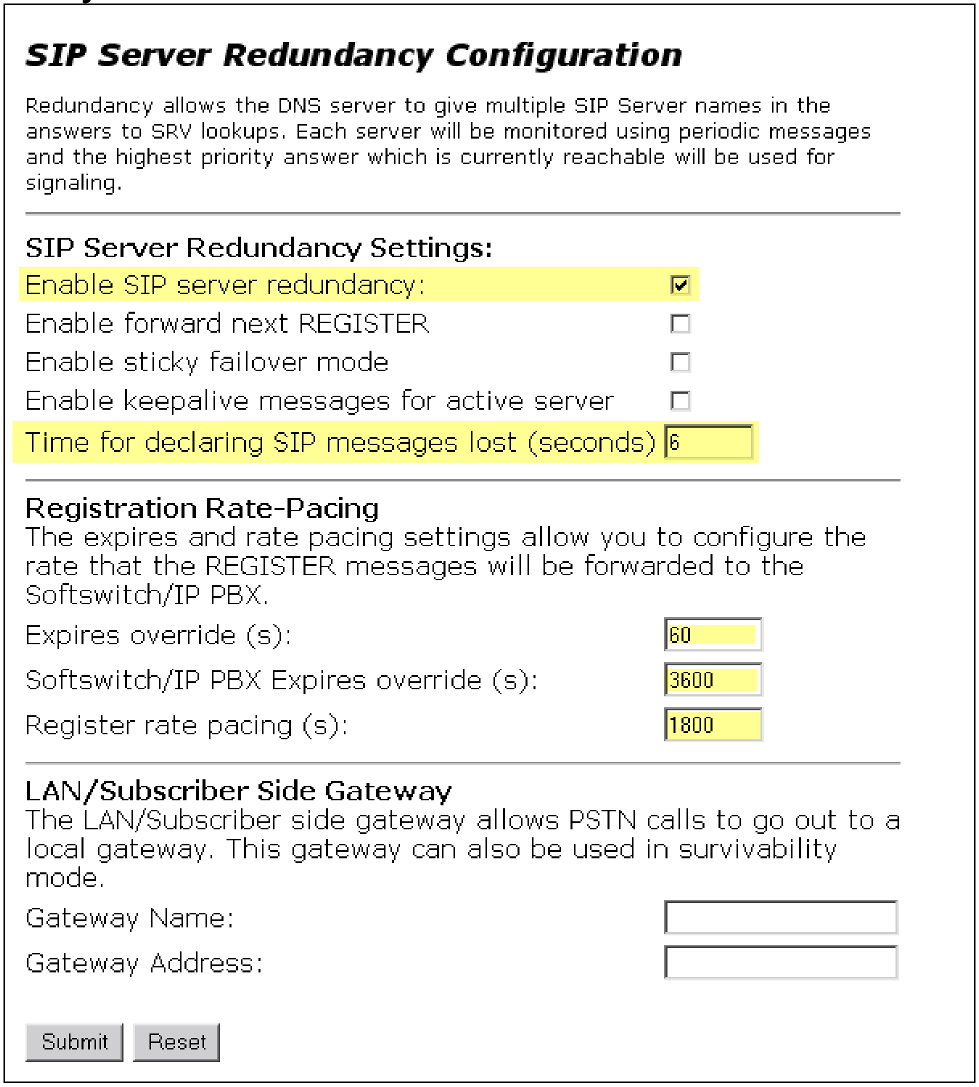
The reachability settings control how often messages are sent to the Softswitch/IP PBX and how quickly a Softswitch/IP PBX will be declared unreachable or reachable. The configuration below is used to determine Softswitch/IP PBX reachability for both redundancy and local or remote call control functions.

Time (s) between DNS lookups:	30
Time (s) between Keepalive messages:	5
Time (s) to declare Keepalive message lost:	5
Number of missed messages to declare alarm:	5
Number of received messages to clear alarm:	10
Interpret error code as success:	0
Enable Local-Mode Indicator:	□
Enable Shared Call:	□

Current SIP Server reachability status:

	Name	Address	Port	P	W	Lost	Rcvd	Status
●	cps1.ngtlab.net	67.41.209.33	5060	1	9	0	10	Active
○	cps2.ngtlab.net	67.41.209.43	5060	2	9	0	0	Idle

16b – Survivability Bottom View



SIP Server Redundancy Configuration

Redundancy allows the DNS server to give multiple SIP Server names in the answers to SRV lookups. Each server will be monitored using periodic messages and the highest priority answer which is currently reachable will be used for signaling.

SIP Server Redundancy Settings:

Enable SIP server redundancy: ☑
Enable forward next REGISTER ☐
Enable sticky failover mode ☐
Enable keepalive messages for active server ☐
Time for declaring SIP messages lost (seconds) 6

Registration Rate-Pacing

The expires and rate pacing settings allow you to configure the rate that the REGISTER messages will be forwarded to the Softswitch/IP PBX.

Expires override (s): 60
Softswitch/IP PBX Expires override (s): 3600
Register rate pacing (s): 1800

LAN/Subscriber Side Gateway

The LAN/Subscriber side gateway allows PSTN calls to go out to a local gateway. This gateway can also be used in survivability mode.

Gateway Name:
Gateway Address:

Definitions

The following definitions may assist with understanding terminology used within this document.

ALG

Application Layer Gateway. The component within an EdgeMarc that provides the base VoIP functionality, including private-to-public IP address translation and inbound dial-number mappings.

DHCP

Dynamic Host Configuration Protocol. Protocol for assignment of IP addresses to devices. Used to assign unique IPs to LAN devices such as PCs and Phones. One DHCP server is allowed per Ethernet (Virtual) LAN.

802.1 Framing

Standard Ethernet header framing. Used in flat (non-VLAN) Ethernet networks.

802.1q Framing

Extension to Ethernet framing used in VLAN (Virtual LAN) networks. Provides a VLAN ID in the header of the Ethernet packet. Ethernet links that include the 802.1q tag are sometimes called Trunk links.

Firewall

A piece of hardware and/or software which functions in a networked environment to prevent Some communications forbidden by the security policy

LAN

Local Area Network. A computer network covering a local area, like a home, office, or building. Current LANs are most likely to be based on switched IEEE 802.3 Ethernet running at 10, 100 or 1,000 Mbit/s or on wireless technology

MOS

Mean Opinion Score. A measurement of quality of the audio heard by the listener on a phone call. Scores range from 1 to 4.4. Toll quality audio is generally considered to have a MOS rating of 4 and above.

NAT

Network Address Translation (also including Port Address Translation when used in this document). Allows one public IP address to be shared by many LAN-side endpoints, each having unique private IP addresses. When active, NAT will change the Layer-3 IP address and/or Layer-4 Port number after a packet has been generated by another device. This action often breaks VoIP protocols.

Proxy

Many definitions, but as used in this document refers to the address translation function of the EdgeMarc's ALG. The phones on the LAN side of the EdgeMarc view the EM as the softswitch; the softswitch sees the Edgemarc's WAN IP address as a large multi-line phone. The ALG performs an IP address translation function and a phone number mapping function to translate VoIP signaling protocol and audio RTP from one side of the EdgeMarc to the other.

SIP

Session Initiation Protocol. An IP telephony signaling protocol developed by the IETF. Primarily used for voice over IP (VoIP) calls, SIP can also be used for video or any media type.

SIP is a text-based protocol that is based on HTTP and MIME, which makes it suitable and very flexible for integrated voice-data applications. SIP is designed for realtime transmission, uses fewer resources and is considerably less complex than H.323. Its addressing scheme uses URLs and is human readable; for example: sip:john.doe@company.com.

SIP relies on the session description protocol (SDP) for session description and the realtime transport protocol (RTP) for actual transport.

SIP Proxy

The softswitch from/to which all SIP signaling is sent and received. In other words, the ***VOIP2320*** VOIP platform.

Traffic Shaper

Component of VOS providing prioritization of voice and signaling traffic over other “data” traffic. It also provides outbound bandwidth shaping so that no queuing occurs upstream of the EdgeMarc as well as throttling of inbound TCP data traffic to avoid swamping of inbound voice.

VOS

Voice Operating System for the EdgeMarc router(s). Includes all the software functionality provided by Edgewater; both Edgewater developed software as well as the Linux O/S and other open-source packages.

WAN

Wide Area Network. A computer network covering a broad geographical area. WANs are used to connect local area networks (LANs) together, so that users and computers in one location can communicate with users and computers in other locations. The largest and most well-known example of a WAN is the Internet.

Additional Documentation

- ***VOIP2320*** Configuration Guide EdgeMarc
  http://voip2320.com/index-4.html

- Edgewater Networks 4200 Series Converged Network Appliance Users Manual
  http://www.edgewaternetworks.com/index.html

- Edgewater Networks 4300 Series Converged Network Appliance Users Manual
  http://www.edgewaternetworks.com/index.html